管理員指南

AWS Service Catalog

AWS Service Catalog: 管理員指南

Table of Contents

什麼是 Service Catalog？ 1
影片：簡介 AWS Service Catalog 1
概觀 2
使用者 2
產品 2
HashiCorp Terraform 開放原始碼和 Terraform 雲端支援 2
佈建產品 3
產品組合 3
版本控制 3
許可 3
Constraints 4
初始管理者工作流程 4
初始最終使用者工作流程 4
配額 5
AWS Organizations 5
限制條件配額 5
產品組合配額 5
產品配額 6
佈建產品配額 6
區域配額 6
服務動作配額 6
TagOptions 配額 6
設定 7
註冊 AWS 帳戶 7
建立具有管理存取權的使用者 7
將許可授予管理員 9
將許可授予最終使用者 11
安裝和設定 Terraform 佈建引擎 12
佇列判斷 12
將混淆代理人新增至 Terraform 佈建引擎 13
開始使用 17
入門資源庫 17
先決條件 18
進一步了解 18

CloudFormation 產品入門 18
步驟 1：下載範本 19
步驟 2：建立金鑰對 23
步驟 3：建立產品組合 24
步驟 4：在產品組合中建立新的產品 24
步驟 5：新增範本限制條件 25
步驟 6：新增啟動限制條件 26
步驟 7：授予最終使用者對產品組合的存取權 28
步驟 8：測試最終使用者體驗 29
Terraform 產品入門 30
更新至外部產品類型 31
先決條件：設定 Terraform 佈建引擎 32
步驟 1：Terraform 組態檔案下載 33
步驟 2：建立 Terraform 產品 34
步驟 3：建立產品組合 35
步驟 4：將產品新增至產品組合 36
步驟 5：建立啟動角色 36
步驟 6：新增啟動限制條件 39
步驟 7：授予最終使用者存取權 40
步驟 8：與最終使用者共用產品組合 41
步驟 9：測試最終使用者體驗 41
步驟 10：監控 Terraform 佈建操作 42
安全 44
資料保護 44
使用加密來保護資料 45
身分和存取權管理 46
目標對象 46
的身分型政策範例 AWS Service Catalog 46
AWS 受管政策 52
使用服務連結角色 60
對 AWS Service Catalog 身分和存取進行故障診斷 65
控制存取 66
記錄和監控 67
合規驗證 67
恢復能力 68
基礎設施安全性 68

安全最佳實務 68
管理目錄 70
管理產品組合 70
建立、檢視和刪除產品組合 71
檢視產品組合詳細資訊 71
建立和刪除產品組合 71
新增 產品 72
新增限制條件 74
授予存取權限給使用者 75
共用產品組合 76
共用和匯入產品組合 83
管理產品 86
檢視產品頁面 86
建立產品 87
將產品新增至產品組合 89
更新產品 89
從外部儲存庫將產品同步至範本檔案 91
刪除產品 98
管理版本 105
使用限制 106
啟動限制條件 107
通知限制條件 112
標籤更新限制 113
堆疊集限制 113
範本限制條件 114
使用服務動作 118
先決條件 118
步驟 1：設定最終使用者許可 119
步驟 2：建立服務動作 120
步驟 3：將服務動作與產品版本建立關聯 121
步驟 4：測試最終使用者體驗 121
步驟 5：使用 管理服務動作 AWS CloudFormation 121
步驟 6：故障診斷 122
將 AWS Marketplace 產品新增至您的產品組合 123
使用 管理 AWS Marketplace 產品 AWS Service Catalog 124
手動管理和新增 AWS Marketplace 產品 124

使用 CloudFormation StackSets 129
堆疊集與堆疊執行個體 129
堆疊集限制 129
管理預算 130
先決條件 130
建立預算 132
關聯預算 133
檢視預算 133
取消關聯預算 133
管理佈建產品 135
以管理員身分管理佈建產品 135
變更佈建產品擁有者 136
另請參閱 136
更新已佈建產品的範本 136
教學：識別使用者資源分配 137
管理 Terraform 開放原始碼產品狀態錯誤 141
狀態錯誤範例 141
管理 Terraform 開放原始碼產品狀態檔案 142
管理標籤 144
AutoTags 144
TagOption 資料庫 145
啟動具有 TagOption 的產品 146
管理 TagOption 150
搭配 AWS Organizations 標籤政策使用 TagOptions 152
外部引擎 155
考量事項 156
參數剖析 156
佈建中 158
更新中 161
終止 164
標記 165
監控 167
監控工具 167
自動化工具 167
CloudWatch Metrics 168
啟用 CloudWatch 指標 168

可用的指標與維度 168
檢視 AWS Service Catalog 指標 169
CloudTrail 日誌 170
AWS Service Catalog CloudTrail 中的資訊 170
了解 AWS Service Catalog 日誌檔案項目 171
主控台品牌 173
AWS 區域 支援主控台品牌 173
文件歷史記錄 176
舊版更新 177
..... clxxxi

什麼是 Service Catalog？

Service Catalog 可讓組織建立和管理已核准的 IT 服務目錄 AWS。這些 IT 服務可以包含虛擬機器映像、伺服器、軟體、資料庫等所有項目，以完成多層應用程式架構。

Service Catalog 可讓組織集中管理常見的部署 IT 服務，並協助組織實現一致的控管並滿足合規要求。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

  管理員會從其目錄中組合產品組合、新增要在佈建中使用的限制條件和資源標籤，然後透過 AWS Identity and Access Management (IAM) 使用者和群組授予對產品組合的存取權。
- 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 提供對所有最終使用者動作的程式設計控制，作為使用 的替代方案 AWS 管理主控台。如需詳細資訊，請參閱 Service Catalog 開發人員指南。

影片：簡介 AWS Service Catalog

此影片 (7：27) 說明如何建立、組織和管理精選的產品 AWS 目錄，以及使用許可層級共用產品。因此，最終使用者可以快速佈建核准的 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，您將受益於了解其元件以及管理員和最終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），將它們組織成產品組合，並將存取權授予最終使用者。目錄管理員為 產品準備 CloudFormation 範本、設定限制條件和管理 IAM 角色，以提供進階資源管理。
- 最終使用者 – 從其 IT 部門或經理接收 AWS 登入資料，並使用 AWS 管理主控台 來啟動已獲授予存取權的產品。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

產品是您想要用來部署的 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 AWS Marketplace 產品。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，或是其中的任何項目。

您可以透過匯入 AWS CloudFormation 範本來建立產品。 AWS CloudFormation 範本定義 AWS 產品所需的資源、資源之間的關係，以及最終使用者可以在啟動產品時插入的參數，以設定安全群組、建立金鑰對，以及執行其他自訂。

HashiCorp Terraform 開放原始碼和 Terraform 雲端支援

AWS Service Catalog 可讓您快速地進行自助式佈建，並在其中控管 HashiCorp Terraform 開放原始碼和 Terraform Cloud 組態 AWS。您可以使用 Service Catalog 做為單一工具來大規模組織、管理和分發 Terraform 組態 AWS。您可以存取 Service Catalog 金鑰功能，包括標準化和預先核准的 Terraform 範本目錄、存取控制、最低權限佈建、版本控制、標記，以及與數千個 AWS 帳戶共用。您的最終使用者會看到他們可以存取的產品和版本的簡單清單，然後可以在單一動作中部署這些產品。

若要進一步了解並完成 Terraform 產品教學課程，請檢閱 Terraform 產品入門。

佈建產品

AWS CloudFormation 堆疊可讓您以單一單位佈建、標記、更新和終止產品執行個體，讓您更輕鬆地管理產品的生命週期。 AWS CloudFormation 堆疊包含以 JSON 或 YAML 格式撰寫的 AWS CloudFormation 範本，及其相關聯的資源集合。佈建產品是一個堆疊。當最終使用者啟動產品時，Service Catalog 佈建的產品執行個體是具有執行產品所需資源的堆疊。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組合。產品組合會協助管理可使用特定產品的人與其使用方法。使用 Service Catalog，您可以為組織中每種類型的使用者建立自訂產品組合，並選擇性地授予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以額外的限制來分配您的產品組合，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) 許可來控制誰可以檢視和修改您的目錄。IAM 許可可以指派給 IAM 使用者、群組和角色。

當使用者啟動已指派 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 CloudFormation。透過將 IAM 角色指派給每個產品，您可以避免授予使用者執行未核准操作的許可，並讓他們能夠使用 目錄佈建資源。

Constraints

限制會控制您可以為產品部署特定 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。有不同類型的 AWS Service Catalog 限制條件：啟動限制條件、通知限制條件和範本限制條件。

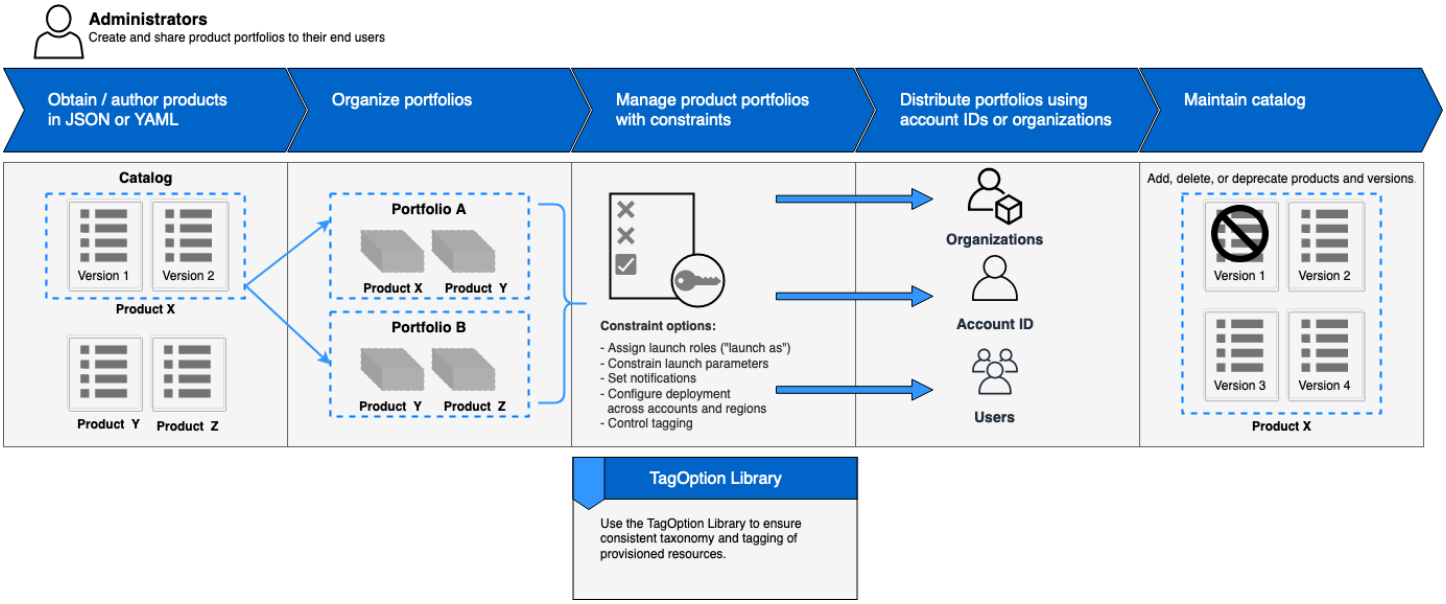
透過啟動限制，您可為產品組合中的產品指定角色。使用此角色在啟動時佈建資源，因此您可以限制使用者許可，而不會影響使用者從目錄中佈建產品的能力。

通知限制條件可讓您使用 Amazon SNS 主題取得堆疊事件的通知。

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。

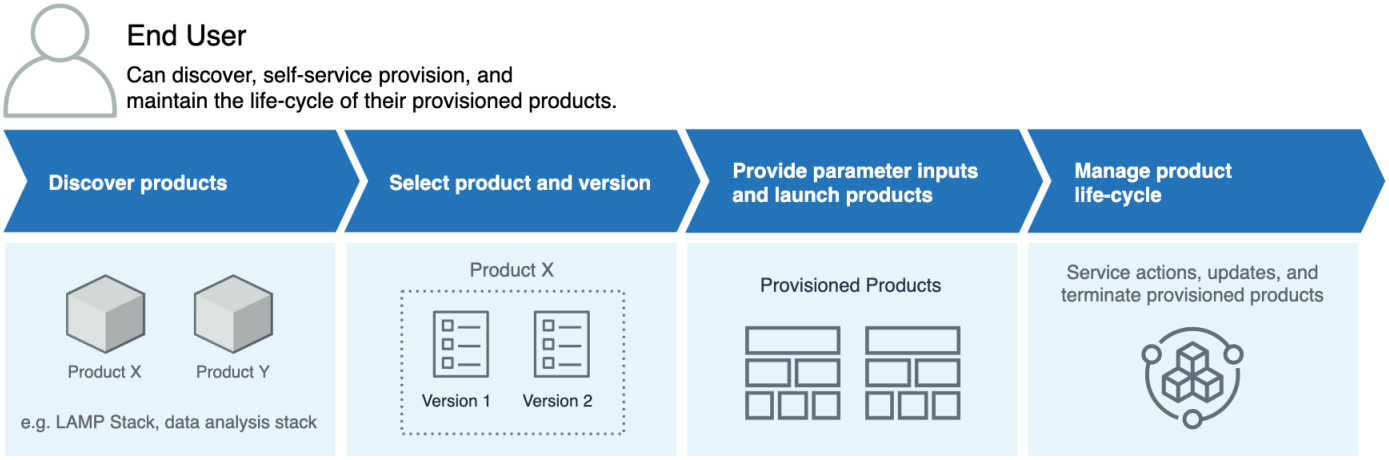
初始管理者工作流程

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

此圖表顯示最終使用者的初始工作流程。



AWS Service Catalog 預設服務配額

AWS 您的帳戶具有下列預設配額 AWS Organizations：限制條件、產品組合、產品、佈建產品、區域、服務動作和 TagOptions。

AWS Organizations

- AWS Service Catalog 每個組織的委派管理員：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

- 每個資源的 TagOptions：25
- 每個 TagOption 的值：25

設定 AWS Service Catalog

開始使用 之前 AWS Service Catalog，請先完成下列任務。

主題

- 註冊 AWS 帳戶
- 建立具有管理存取權的使用者
- 將許可授予 AWS Service Catalog 管理員
- 將許可授予 AWS Service Catalog 最終使用者
- 安裝和設定 Terraform 佈建引擎

註冊 AWS 帳戶

如果您沒有 AWS 帳戶，請完成下列步驟來建立一個。

註冊 AWS 帳戶

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

   部分註冊程序需接收來電或簡訊，並在電話鍵盤輸入驗證碼。

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

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

建立具有管理存取權的使用者

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

保護您的 AWS 帳戶根使用者

1. 選擇根使用者並輸入 AWS 帳戶 您的電子郵件地址，以帳戶擁有者AWS 管理主控台身分登入 。在下一頁中，輸入您的密碼。

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

2. 若要在您的根使用者帳戶上啟用多重要素驗證 (MFA)。

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

建立具有管理存取權的使用者

1. 啟用 IAM Identity Center。

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

2. 在 IAM Identity Center 中，將管理存取權授予使用者。

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

以具有管理存取權的使用者身分登入

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

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

指派存取權給其他使用者

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

   如需指示，請參閱《AWS IAM Identity Center 使用者指南》中的建立許可集。

2. 將使用者指派至群組，然後對該群組指派單一登入存取權。

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

主題

- 將許可授予 AWS Service Catalog 管理員
- 將許可授予 AWS Service Catalog 最終使用者
- 安裝和設定 Terraform 佈建引擎

若要提供存取權，請新增權限至您的使用者、群組或角色：

- 中的使用者和群組 AWS IAM Identity Center：

  建立權限合集。請按照《AWS IAM Identity Center 使用者指南》中的建立權限合集說明進行操作。
- 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。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。請按照《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》的新增許可到使用者 (主控台) 中的指示。

將許可授予 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，才能執行下列任務：

- 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 擔任的 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連接至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. 前往 https://console.aws.amazon.com/iam/ 開啟 IAM 主控台。

2. 在導覽窗格中，選擇存取管理，然後選擇使用者。如果您已建立要用作目錄管理員的 IAM 使用者，請選擇使用者名稱，然後選擇新增許可。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. 對於使用者名稱，輸入 **ServiceCatalogAdmin**。

   c. 選擇 Programmatic access (程式設計存取) 和 AWS 管理主控台 存取。

   d. 選擇 Next: Permissions (下一步：許可)。

3. 選擇直接連接現有政策。

4. 選擇建立政策，然後執行下列動作：

   a. 選擇 JSON 標籤。

   b. 複製下列範例政策，並將其貼到政策文件中：

```
{
    "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. （選用）選擇新增標籤，將鍵/值對與資源建立關聯。您最多可新增 50 個標籤。

> **Note**
>
> 標籤是您可以新增至資源的鍵/值對。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，以存取 AWS Service Catalog 存放在 Amazon S3 中的範本。如需詳細資訊，請參閱《Amazon Simple Storage Service 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`**政策的核取方塊，然後選擇下一步：檢閱。
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。

將許可授予 AWS Service Catalog 最終使用者

在最終使用者可以使用 之前 AWS Service Catalog，您必須授予 AWS Service Catalog 最終使用者主控台檢視的存取權。若要授予存取權，請將政策連接到最終使用者所使用的 IAM 使用者、群組或角色。在下列程序中，我們會將**`AWSServiceCatalogEndUserFullAccess`**政策連接至 IAM 群組。

將權限授予最終使用者群組

1. 前往 https://console.aws.amazon.com/iam/ 開啟 IAM 主控台。
2. 在導覽窗格中，選擇 User groups (使用者群組)。
3. 選擇建立群組並執行下列動作：
   a. 針對使用者群組名稱，輸入 **Endusers**。
   b. 在搜尋欄位中，輸入 **AWSServiceCatalog** 以篩選政策清單。
   c. 選取**AWSServiceCatalogEndUserFullAccess**政策的核取方塊。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. 選擇新增使用者並執行下列動作：
   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。
   c. 選擇下一步：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

若要搭配 成功使用 Terraform 產品 AWS Service Catalog，您必須在您要管理 Terraform 產品的相同帳戶中安裝和設定 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，安裝並設定 Terraform 佈建引擎所需的程式碼和基礎設施。 AWS Service Catalog此一次性設定大約需要 30 分鐘。 AWS Service Catalog 提供 GitHub 儲存庫，其中包含有關安裝和設定 Terraform 佈建引擎的說明。

佇列判斷

當您呼叫佈建操作時， 會 AWS Service Catalog 準備承載訊息，以傳送至佈建引擎中的相關佇列。為了建置佇列的 ARN， AWS Service Catalog 會做出下列假設：

- 佈建引擎位於產品擁有者的帳戶
- 佈建引擎位於 AWS Service Catalog 與 進行呼叫的相同區域
- 佈建引擎佇列遵循以下詳述的文件化命名結構描述

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

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

將混淆代理人新增至 Terraform 佈建引擎

端點上的混淆代理人內容索引鍵，以限制**`lambda:Invoke`**操作的存取

AWS Service Catalog由提供的引擎建立的參數剖析器 Lambda 函數具有存取政策，僅授予跨帳戶`lambda:Invoke`許可給 AWS Service Catalog 服務主體：

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "servicecatalog.amazonaws.com"
            },
            "Action": "lambda:InvokeFunction",
            "Resource": "arn:aws:lambda:us-
east-1:111122223333:function:ServiceCatalogTerraformOSParameterParser"
        }
    ]
}
```

這應該是與 整合 AWS Service Catalog 以正常運作所需的唯一許可。不過，您可以使用`aws:SourceAccount`混淆代理人內容索引鍵進一步限制這一點。當 AWS Service Catalog 傳送訊息至這些佇列時， 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，您可以使用如下所示的條件，將引擎限制為僅允許源自 000000000000 和 111111111111 的請求：

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "servicecatalog.amazonaws.com"
            },
            "Action": "lambda:InvokeFunction",
            "Resource": "arn:aws:lambda:us-
east-1:111122223333:function:ServiceCatalogTerraformOSParameterParser",
            "Condition": {
                "StringLike": {
                    "aws:SourceAccount": [
                        "000000000000",
                        "111111111111"
                    ]
                }
            }
        }
    ]
}
```

端點上的混淆代理人內容索引鍵，以限制**sqs:SendMessage**操作的存取

佈建操作會擷取由 AWS Service Catalog提供的引擎建立的 Amazon SQS 佇列，其存取政策只會授與跨帳戶 `sqs:SendMessage` (和相關聯的 KMS) 許可給 AWS Service Catalog 服務主體：

JSON

```
{
    "Version":"2012-10-17",
    "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-1:111122223333: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:ReEncryptFrom",
                "kms:ReEncryptTo",
                "kms:GenerateDataKey"
            ],
            "Resource": "arn:aws:kms:us-east-1:111122223333:key/key_id"
        }
    ]
}
```

這應該是與 整合 AWS Service Catalog 以正常運作所需的唯一許可。不過，您可以使用`aws:SourceAccount`混淆代理人內容索引鍵進一步限制這一點。當 AWS Service Catalog 傳送訊息到這些佇列時， 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，您可以使用如下所示的條件，將引擎限制為僅允許源自 000000000000 和 111111111111 的請求：

JSON

```
{
```

```
    "Version":"2012-10-17",
    "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-1:111122223333: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:ReEncryptFrom",
                "kms:ReEncryptTo",
                "kms:GenerateDataKey"
            ],
            "Resource": "arn:aws:kms:us-east-1:111122223333:key/key_id"
        }
    ]
}
```

開始使用

您可以使用 AWS Service Catalog 入門程式庫中架構良好的其中一個產品範本，或依照其中一個入門教學課程中的步驟來開始使用 。

在教學課程中，您會以目錄管理員和最終使用者身分執行任務。身為目錄管理員，您可以建立產品組合，然後建立產品。身為最終使用者，您可以驗證您可以存取最終使用者主控台並啟動產品。產品為下列其中一項：

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

> **Note**
>
> 開始之前，請確定您已完成 中的動作項目設定 AWS Service Catalog。

主題

- 入門資源庫
- CloudFormation 產品入門
- Terraform 產品入門

入門資源庫

AWS Service Catalog 提供架構良好的產品範本入門程式庫，讓您可以快速入門。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

- 先決條件
- 進一步了解

先決條件

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 CloudFormation 範本所需的許可。如需詳細資訊，請參閱使用 控制存取 AWS Identity and Access Management。
- 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

如需架構良好的詳細資訊，請參閱 AWS Well-Architected。

CloudFormation 產品入門

您可以使用 AWS Service Catalog 入門程式庫中架構良好的其中一個產品範本，或依照入門教學課程中的步驟來開始使用 。

在教學課程中，您會以目錄管理員和最終使用者身分執行任務。身為目錄管理員，您可以建立 porfolio，然後建立產品。身為最終使用者，您可以驗證您可以存取最終使用者主控台並啟動產品。產品是在 Amazon Linux 上執行的雲端開發環境，以定義產品可使用之 AWS 資源的 CloudFormation 範本為基礎。

> **Note**
>
> 開始之前，請確定您已完成 中的動作項目設定 AWS Service Catalog。

主題

- 步驟 1：下載 CloudFormation 範本
- 步驟 2：建立金鑰對
- 步驟 3：建立產品組合
- 步驟 4：在產品組合中建立新的產品
- 步驟 5：新增範本限制條件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：授予最終使用者對產品組合的存取權

- 步驟 8：測試最終使用者體驗

步驟 1：下載 CloudFormation 範本

您可以使用 CloudFormation 範本來設定和佈建產品組合和產品。這些範本是文字檔案，可以 JSON 或 YAML 格式，並描述您要佈建的資源。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CloudFormation 範本格式。您可以使用編輯器 AWS CloudFormation 或您選擇的文字編輯器來建立和儲存範本。在本教學課程中，我們提供簡單的範本，讓您可以開始使用。範本會啟動針對 SSH 存取設定的單一 Linux 執行個體。

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

範本下載

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

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） – 用來建立此範本的AWS 範本格式版本。最新的範本格式版本為 2010-09-09，目前是唯一有效的值。
- 描述 （選用） – 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 限制條件。

  KeyName 參數可讓您指定最終使用者在啟動產品時必須提供 AWS Service Catalog 的 Amazon Elastic Compute Cloud (Amazon EC2) 金鑰對名稱。您將在下一個步驟中建立金鑰對。
- 中繼資料 （選用） – 提供範本額外資訊的物件。AWS：：CloudFormation：：Interface 金鑰會定義最終使用者主控台檢視顯示參數的方式。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。
- 映射 （選用） – 索引鍵和關聯值的映射，可用於指定條件參數值，類似於查詢資料表。您可以使用資源和輸出區段中的 Fn：：FindInMap 內部函數，將索引鍵比對至對應的值。上述範本包含區域清單，以及對應至每個 AWS 區域的 Amazon Machine Image (AMI)。 AWS Service Catalog 會使用此映射，根據使用者在 中選取 AWS 的區域來決定要使用的 AMI AWS 管理主控台。
- 資源 （必要） – 堆疊資源及其屬性。您可以在範本的資源和輸出區段中參考資源。在上述範本中，我們會指定執行 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類型的資訊來設定執行個體類型和 SSH 存取的金鑰名稱。

  CloudFormation 使用目前的 AWS 區域從先前定義的映射中選取 AMI ID，並為其指派安全群組。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） – 告知使用者產品啟動完成的文字。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。

如需範本結構頁面的詳細資訊，請參閱CloudFormation 《 使用者指南》中的範本參考。

步驟 2：建立金鑰對

若要讓您的最終使用者啟動以本教學課程的範例範本為基礎的產品，您必須建立 Amazon EC2 金鑰對。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。如需金鑰對的詳細資訊，請確定您已登入 AWS 主控台，然後在 Amazon EC2 使用者指南中檢閱 Amazon EC2 金鑰對。Amazon EC2

本教學課程的 CloudFormation 範本 `development-environment.template`包含 `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：建立產品組合。否則，請完成下列步驟。

建立一組金鑰對

1. 前往 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：建立產品組合

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：//https://console.aws.amazon.com/servicecatalog/ 開啟 Service Catalog 主控台。
2. 在左側導覽面板中，選擇產品組合，然後選擇建立產品組合。
3. 輸入下列值：
   - 產品組合名 – **Engineering Tools**
   - 產品組合描述 – **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的產品

建立產品組合之後，您就可以在產品組合中建立產品。在本教學課程中，您會在 Engineering Tool 產品組合中建立名為 Linux Desktop 的產品，這是在 Amazon Linux 上執行的雲端開發環境。

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，請開啟 https：//https://console.aws.amazon.com/servicecatalog/。
2. 選擇並開啟您在步驟 2 中建立的工程工具產品組合。
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，輸入下列內容：
   - 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**
   - Distributor – （空白）
5. 在版本詳細資訊頁面上，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. 在支援詳細資訊區段中，輸入下列內容：

- 電子郵件聯絡 – **ITSupport@example.com**
- 支援連結 – **https://wiki.example.com/IT/support**
- 支援描述 – **Contact the IT department for issues deploying or connecting to this product.**

7. 選擇建立產品。

步驟 5：新增範本限制條件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 CloudFormation 範本 (範本限制條件)。如需詳細資訊，請參閱使用 AWS Service Catalog 限制條件。

將範本限制新增至 Linux 桌面產品，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 使用者指南》中的 T2 執行個體。 Amazon EC2

將範本限制新增至 Linux 桌面產品

1. 在產品組合詳細資訊頁面上，選擇限制條件，然後選擇建立限制條件。
2. 在建立限制頁面上，針對產品選擇 Linux 桌面。然後，針對限制類型，選擇範本。
3. 在 Template 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. 針對限制描述，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

啟動限制會指定最終使用者啟動產品時 AWS Service Catalog 擔任的 IAM 角色。

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

您指派給產品做為啟動限制條件的 IAM 角色必須具有下列許可

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

此啟動限制可讓最終使用者啟動產品，並在啟動後將其管理為佈建產品。如需詳細資訊，請參閱 AWS Service Catalog 啟動限制。

如果沒有啟動限制，您需要將額外的 IAM 許可授予最終使用者，然後他們才能使用 Linux 桌面產品。例如，`ServiceCatalogEndUserAccess`政策會授予存取 AWS Service Catalog 最終使用者主控台檢視所需的最低 IAM 許可。

使用啟動限制可讓您遵循 IAM 最佳實務，將最終使用者 IAM 許可保持在最低限度。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. 請遵循 IAM 使用者指南中 JSON 標籤上建立新政策的指示。
2. 貼上下列 JSON 政策文件：

   - `cloudformation`– 允許建立、讀取、更新、刪除、列出和標記 CloudFormation 堆疊 AWS Service Catalog 的完整許可。

- `ec2`— 允許列出、讀取、寫入、佈建和標記屬於 AWS Service Catalog 產品一部分的 Amazon Elastic Compute Cloud (Amazon EC2) 資源 AWS Service Catalog 的完整許可。根據您要部署 AWS 的資源，此許可可能會變更。
- `ec2`– 為您的 AWS 帳戶建立新的受管政策，並將指定的受管政策連接至指定的 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 需要存取佈建成品。
- `servicecatalog`— 允許代表最終使用者列出、讀取、寫入、標記和啟動資源的 AWS Service Catalog 許可。
- `sns`— 允許 AWS Service Catalog 許可列出、讀取、寫入和標記啟動限制條件的 Amazon SNS 主題。

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

JSON

```
{
    "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. 在檢閱政策頁面中，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. 對於選取信任的實體，請選擇AWS 服務，然後在其他服務的使用案例下 AWS ，選擇 Service Catalog。選取 Service Catalog 使用案例，然後選擇下一步。
   b. 搜尋 linuxDesktopPolicy 政策，然後選取此選取方塊。
   c. 選擇下一步。
   d. 於角色名稱輸入 **linuxDesktopLaunchRole**。
   e. 選擇建立角色。
8. 在 https：//https://console.aws.amazon.com/servicecatalog 開啟 AWS Service Catalog 主控台。
9. 選擇 Engineering Tools (工程工具) 產品組合。
10. 在產品組合詳細資訊頁面上，選擇限制條件索引標籤，然後選擇建立限制條件。
11. 對於產品，選擇 Linux 桌面，對於限制類型，選擇啟動。
12. 選擇選取 IAM 角色。接著選擇 linuxDesktopLaunchRole，然後選擇建立。

步驟 7：授予最終使用者對產品組合的存取權

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。

先決條件

如果您尚未為最終使用者建立 IAM 群組，請參閱 將許可授予 AWS Service Catalog 最終使用者。

提供存取產品組合

1. 在產品組合詳細資訊頁面上，選擇存取索引標籤。
2. 選擇 Grant access (授與存取權)。
3. 在群組索引標籤上，選取最終使用者的 IAM 群組核取方塊。
4. 選擇新增存取權。

步驟 8：測試最終使用者體驗

若要驗證最終使用者可以成功存取最終使用者主控台檢視並啟動您的產品，請以最終使用者 AWS 身分登入 並執行這些任務。

若要驗證最終使用者是否能存取最終使用者主控台

1. 請遵循 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，選擇您建立`Engineering Tools`產品組合 AWS 的區域。在本教學課程中，選擇 us-east-1 區域。
3. 開啟位於 https：//https://console.aws.amazon.com/servicecatalog/ 的 AWS Service Catalog 主控台，查看：

   - 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。

驗證最終使用者可以啟動 Linux 桌面產品

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。
2. 選擇啟動產品以啟動設定產品的精靈。
3. 在啟動：Linux 桌面頁面上，輸入 **`Linux-Desktop`** 以取得佈建的產品名稱。
4. 在參數頁面上，輸入以下內容，然後選擇下一步：

   - 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 – 為要連線至執行個體的 IP 地址輸入有效的 CIDR 範圍。您可以使用預設值 (0.0.0.0/0) 來允許從任何 IP 地址、IP 地址存取，後面接著 **/32** 來限制僅存取您的 IP 地址，或介於兩者之間。

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。 AWS Service Catalog 啟動產品需要幾分鐘的時間。若要查看目前狀態，請重新整理瀏覽器。產品啟動後，狀態為可清空。

Terraform 產品入門

AWS Service Catalog 啟用快速的自助式佈建，並控管其中的 HashiCorp Terraform 組態 AWS。您可以使用 AWS Service Catalog 做為單一工具來大規模組織、管理和分配 Terraform 組態 AWS。 AWS Service Catalog 支援跨數個主要功能的 Terraform，包括標準化和預先核准的 Terraform 範本目錄、存取控制、版本控制、標記，以及與其他 AWS 帳戶共用。在 中 AWS Service Catalog，您的最終使用者會看到他們可以存取的產品和版本的簡單清單，然後可以在單一動作中部署這些產品。

> **Note**
>
> 為了繼續支援 HashiCorp 技術，由於最近的 Terraform 授權變更， 將先前對 Terraform 開放原始碼的任何參考 AWS Service Catalog 變更為外部。外部產品類型包含對 Terraform Community Edition 的支援，先前稱為 Terraform Open Source。如需將現有 Terraform Open Source 產品和佈建產品遷移至外部產品類型的詳細資訊和說明，請參閱 將現有的 Terraform Open Source 產品和佈建產品更新為外部產品類型。

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

身為目錄管理員，您在中央管理員帳戶 （中樞帳戶） 中工作。Terrafrm Community Edition 和 Terraform Cloud 產品都需要 Terraform 佈建引擎，您可以在 佈建 Terraform Community Edition 的引擎 （外部產品類型） 和 中進一步了解佈建適用於 Terraform Cloud 的引擎。

在教學課程中，您會在管理員帳戶中執行下列任務：

- 使用 Terraform Cloud 或外部產品類型建立 Terraform 產品。Service Catalog 使用外部產品類型來支援 Terraform Community Edition 產品。
- 將產品與產品組合建立關聯
- 建立啟動限制，以允許最終使用者佈建產品

- 標記產品
- 與最終使用者帳戶 （輻條帳戶） 共用產品組合和 Terraform 產品

在教學課程中，您可以使用管理中樞帳戶的組織共用選項來共用產品組合，該帳戶也是組織的管理帳戶。如需組織共用的詳細資訊，請參閱 共用產品組合。

您在教學課程中建立的 Terraform 產品中包含 AWS 的資源是簡單的 Amazon S3 儲存貯體。

> **Note**
>
> 開始之前，請確定您已完成 中的動作項目設定 AWS Service Catalog。

主題

- 將現有的 Terraform Open Source 產品和佈建產品更新為外部產品類型
- 先決條件：設定 Terraform 佈建引擎
- 步驟 1：Terraform 組態檔案下載
- 步驟 2：建立 Terraform 產品
- 步驟 3：建立 AWS Service Catalog 產品組合
- 步驟 4：將產品新增至產品組合
- 步驟 5：建立啟動角色
- 步驟 6：將啟動限制新增至 Terraform 產品
- 步驟 7：授予最終使用者存取權
- 步驟 8：與最終使用者共用產品組合
- 步驟 9：測試最終使用者體驗
- 步驟 10：監控 Terraform 佈建操作

將現有的 Terraform Open Source 產品和佈建產品更新為外部產品類型

為了繼續支援 HashiCorp 技術，由於最近的 Terraform 授權變更， 將任何先前對 Terraform 開放原始碼的參考 AWS Service Catalog 變更為外部。外部產品類型包含對 Terraform Community Edition 的支援，先前稱為 Terraform Open Source。 AWS Service Catalog 不再支援 Terraform Open Source 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 Open Source 產品和佈建產品轉換為外部產品。

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。如需有關更新 Terraform 參考引擎的說明，請檢閱我們的 GitHub 儲存庫。
2. 使用新的外部產品類型重新建立任何現有的 Terraform Open Source 產品。
3. 刪除任何使用 Terraform Open Source 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 Open Source 產品類型的現有佈建產品。

轉換現有產品後，請針對任何使用 tar.gz 組態檔案的新產品使用外部產品類型。

AWS Service Catalog 會視需要支援客戶完成此變更。如果這些變更需要您帳戶的大量工作，或影響關鍵產品工作負載，請聯絡您的 帳戶代表請求協助。

先決條件：設定 Terraform 佈建引擎

在 中建立 Terraform 產品的先決條件是 AWS Service Catalog，您必須在 Service Catalog 管理員帳戶（中樞帳戶）中安裝和設定佈建引擎。Terraform Community Edition 產品（使用外部產品類型）和 Terraform Cloud 產品（使用 Terraform Cloud 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。

佈建 Terraform Community Edition 的引擎（外部產品類型）

AWS Service Catalog 使用外部產品類型來支援 Terraform Community Edition 產品。外部產品類型也支援其他佈建工具，包括 Pulumi、Ansible、Chef 等以佈建引擎的組態為基礎的工具。

對於搭配 HashiCorp 的 Terraform Community Edition 使用外部產品類型 AWS Service Catalog 的產品，您必須在 AWS Service Catalog 管理員帳戶（中樞帳戶）中安裝並設定 Terraform 佈建引擎。 會 AWS 管理此引擎及其資源。

AWS Service Catalog 提供 GitHub 儲存庫，其中包含安裝和設定 AWS所提供 Terraform 佈建引擎的指示。儲存庫包含下列資訊：

- 必要的安裝工具

- 建置程式碼
- 部署至 AWS 帳戶
- 有關佈建工作流程、品質保證和限制的其他資訊

佈建適用於 Terraform Cloud 的引擎

對於搭配 HashiCorp 的 Terraform Cloud 使用 Terraform Cloud 產品類型 AWS Service Catalog 的產品，您必須在 AWS Service Catalog 管理員帳戶（中樞帳戶）中安裝和設定 Terraform 佈建引擎。HashiCorp 會在遠端環境中管理此引擎。

HashiCorp 提供 GitHub 儲存庫，其中包含設定 Terraform Cloud 引擎的說明 AWS Service Catalog。儲存庫包含下列資訊：

- 必要的安裝工具
- 建置程式碼
- 部署至 AWS 帳戶
- 有關佈建工作流程、品質保證和限制的其他資訊

步驟 1：Terraform 組態檔案下載

您可以使用 Terraform 組態檔案來建立和佈建 HashiCorp Terraform 產品。這些組態是純文字檔案，並說明您要佈建的資源。您可以使用您選擇的文字編輯器來建立、更新和儲存組態。若要建立產品，您必須將 Terraform 組態上傳為 tar.gz 檔案。在本教學課程中， AWS Service Catalog 提供簡單的組態檔案，讓您可以開始使用。組態會建立 Amazon S3 儲存貯體。

組態檔案下載

AWS Service Catalog 提供範例simple-s3-bucket.tar.gz組態檔案，供您在本教學課程中使用。

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

組態檔案會在 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）– 管理員使用者（中樞帳戶管理員）可指派以自訂組態的值定義。變數提供一致的界面，以變更指定組態的行為。變數關鍵字後面的標籤是變數的名稱，在相同模組中的所有變數中必須是唯一的。此名稱用於將外部值指派給變數，並從模組中參考變數的值。
- 提供者（選用）– 資源佈建的雲端服務提供者，僅支援 AWS. AWS Service Catalog only AWS作為提供者。因此，Terraform 佈建引擎會將任何其他列出的提供者覆寫為 AWS。
- 資源（必要）– 佈建的 AWS 基礎設施資源。在本教學課程中，Terraform 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傳回的值。您可以使用輸出資料，透過自動化工具設定基礎設施工作流程。

步驟 2：建立 Terraform 產品

安裝 Terraform 佈建引擎後，您就可以在其中建立 HashiCorp Terraform 產品 AWS Service Catalog。在本教學課程中，您會建立包含簡單 Amazon S3 儲存貯體的 Terraform 產品。

建立 Terraform 產品

1. 在 https：//https://console.aws.amazon.com/servicecatalog/ 開啟 AWS Service Catalog 主控台，並以管理員使用者身分登入。
2. 導覽至管理區段，然後選擇產品清單。
3. 選擇建立產品。
4. 在產品詳細資訊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 Community Edition 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 儲存貯體的 Terraform 產品。
- 擁有者 – **IT**
- Distributor – （空白）

6. 在版本詳細資訊窗格中，選擇上傳範本檔案，然後選擇選擇檔案。選取您在 中下載的檔案步驟 1：Terraform 組態檔案下載。
7. 輸入下列資料：

   - 版本名稱 – **v1.0**
   - 版本描述 – **Base Version**

8. 在支援詳細資訊區段中，輸入以下內容，然後選擇建立產品。

   - 電子郵件聯絡 – **ITSupport@example.com**
   - 支援連結 – **https://wiki.example.com/IT/support**
   - 支援描述 – **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， 會在產品頁面上 AWS Service Catalog 顯示確認橫幅。

步驟 3：建立 AWS Service Catalog 產品組合

您可以在 AWS Service Catalog 管理員帳戶（中樞帳戶）中建立產品組合，以便輕鬆進行產品組織，並分發至最終使用者帳戶（輪換帳戶）。

建立產品組合

1. 在 https：//https://console.aws.amazon.com/servicecatalog/ 開啟 AWS Service Catalog 主控台，並以管理員身分登入。
2. 在左側導覽面板中，選擇產品組合，然後選擇建立產品組合。
3. 輸入下列值：

   - 產品組合名 – **S3 bucket**
   - 產品組合描述 – **Sample portfolio for Terraform configurations.**
   - 擁有者 – **IT (it@example.com)**

4. 選擇建立。

步驟 4：將產品新增至產品組合

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。

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 Simple 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 會顯示新增簡單 S3 儲存貯體至產品組合窗格。
3. 選取 S3 儲存貯體產品組合，然後關閉建立啟動限制。稍後您將在教學課程中建立啟動限制。
4. 選擇將產品新增至產品組合。

成功將產品新增至產品組合後， 會在產品清單頁面上 AWS Service Catalog 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 佈建引擎在最終使用者啟動 HashiCorp Terraform 產品時 AWS Service Catalog 可擔任的許可。

您稍後做為啟動限制條件指派給簡單 Amazon S3 儲存貯體 Terraform 產品的 IAM 角色（啟動角色）必須具有下列許可：

- 存取 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:List*`、 `s3:Get*`和 `s3:PutBucketTagging` Amazon S3 操作的存取。
- 在 AWS Service Catalog擁有的 Amazon S3 儲存貯體中讀取對 Amazon S3 範本的存取權
- 存取 `CreateGroup`、`DeleteGroup`、 `ListGroupResources`和資源`Tag`群組操作。這些操作 AWS Service Catalog 可讓 管理資源群組和標籤

在 AWS Service Catalog 管理員帳戶中建立啟動角色

1. 登入 AWS Service Catalog 管理員帳戶時，請遵循 IAM 使用者指南中 JSON 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。此政策必須在您建立啟動角色之前建立，並包含下列許可：

- `s3`— 允許列出、讀取、寫入、佈建和標記 Amazon S3 產品 AWS Service Catalog 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 需要存取佈建成品。
- `resourcegroups`— 允許 AWS Service Catalog 建立、列出、刪除和標記 AWS Resource Groups。
- `tag`— 允許 AWS Service Catalog 標記許可。

> **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：

JSON

```
{
    "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. 在檢閱政策頁面中，針對名稱輸入 **S3ResourceCreationAndArtifactAccessPolicy**。
   d. 選擇建立政策。
4. 在導覽窗格中，選擇角色，然後選擇建立角色。
5. 針對選取信任的實體，選擇自訂信任政策，然後輸入下列 JSON 政策：
6. 選擇下一步。
7. 在政策清單中，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 管理員帳戶中建立啟動角色之後，您還必須在 AWS Service Catalog 最終使用者帳戶中建立相同的啟動角色。最終使用者帳戶中的角色必須具有與管理員帳戶中的角色相同的名稱，並包含相同的政策。

在 AWS Service Catalog 最終使用者帳戶中建立啟動角色

1. 以管理員身分登入最終使用者帳戶，然後遵循 IAM 使用者指南中 JSON 標籤上建立新政策的指示。
2. 重複上述 AWS Service Catalog 管理員帳戶中建立啟動角色的步驟 2-10。

> **Note**
>
> 在 AWS Service Catalog 最終使用者帳戶中建立啟動角色時，請確定您在自訂信任政策**`AccountId`**中使用相同的管理員。

現在您已在管理員和最終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 Terraform 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，最終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 產品的啟動限制建立關聯。

此啟動限制可讓最終使用者啟動產品，並在啟動後將其管理為佈建產品。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 IAM 最佳實務，將最終使用者 IAM 許可保持在最低限度。如需詳細資訊，請參閱《IAM 使用者指南》中的授予最低權限。

將啟動限制指派給產品

1. 在 https：//https://console.aws.amazon.com/servicecatalog 開啟 AWS Service Catalog 主控台。
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. 在產品組合詳細資訊頁面上，選擇限制條件索引標籤，然後選擇建立限制條件。
5. 針對產品，選擇 Simple S3 儲存貯體。 AWS Service Catalog 會自動選取啟動限制類型。
6. 選擇輸入角色名稱，然後選擇 SCLaunch-S3product。
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中，以及使用此啟動限制啟動產品的使用者帳戶中。

步驟 7：授予最終使用者存取權

將啟動限制套用至 HashiCorp Terraform 產品後，您就可以將存取權授予發言帳戶中的最終使用者。

在本教學課程中，您會使用主體名稱共用將存取權授予最終使用者。主體名稱是管理員可以在產品組合中指定的群組、角色和使用者的名稱，然後與產品組合共用。當您共用產品組合時， 會 AWS Service Catalog 驗證這些委託人名稱是否已存在。如果它們確實存在， AWS Service Catalog 會自動將相符的 IAM 主體與共用產品組合建立關聯，以將存取權授予最終使用者。如需詳細資訊，請參閱共用產品組合。

先決條件

如果您尚未為最終使用者建立 IAM 群組，請參閱 將許可授予 AWS Service Catalog 最終使用者。

提供存取產品組合

1. 導覽至產品組合頁面，然後選擇 S3 儲存貯體產品組合。
2. 選擇存取索引標籤，然後選擇授予存取權。
3. 在存取類型窗格中，選擇主體名稱。
4. 在主體名稱窗格中，選取主體名稱類型，然後在輻條帳戶中輸入所需最終使用者的主體名稱。
5. 選擇 Grant access (授與存取權)。

步驟 8：與最終使用者共用產品組合

AWS Service Catalog 管理員可以使用account-to-account共用或 AWS Organizations 共用，將產品組合與最終使用者帳戶分配。在本教學課程中，您要從管理員帳戶 （中樞帳戶） 與組織共用產品組合，這也是組織的管理帳戶。

從管理員中樞帳戶共用產品組合

1. 在 https：//https://console.aws.amazon.com/servicecatalog/ 開啟 AWS Service Catalog 主控台。
2. 在產品組合頁面上，選取 S3 儲存貯體產品組合。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，選擇最終使用者帳戶 （輻條帳戶）。

   您也可以根據組織結構，選取根節點來與整個組織、父組織單位 (OU) 或組織內的子 OU 共用產品組合。如需詳細資訊，請參閱 共用產品組合。
5. 在共用設定窗格中，選擇主體共用。
6. 選擇共用。

成功與最終使用者共用產品組合後，下一步是驗證最終使用者體驗並佈建 Terraform 產品。

步驟 9：測試最終使用者體驗

若要驗證最終使用者可以成功存取最終使用者主控台檢視並啟動您的**Simple S3 bucket**產品，請以最終使用者 AWS 身分登入 並執行以下任務。

若要驗證最終使用者是否能存取最終使用者主控台

- 開啟位於 https：//https://console.aws.amazon.com/servicecatalog/ 的 AWS Service Catalog 主控台，查看：

- 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。

驗證最終使用者可以啟動 Terraform 產品

1. 在主控台的產品區段中，選擇 Simple S3 儲存貯體。
2. 選擇啟動產品以啟動設定產品的精靈。
3. 在啟動簡易 S3 儲存貯體頁面上，輸入 **`Amazon S3 product`** 以取得佈建的產品名稱。
4. 在參數頁面上，輸入以下內容，然後選擇下一步：

   - bucket_name – 提供 Amazon S3 儲存貯體的唯一名稱。例如 **`terraform-s3-product`**。
5. 選擇啟動產品。主控台會顯示 Amazon S3 產品啟動的堆疊詳細資訊頁面。產品的初始狀態為變更中。 AWS Service Catalog 啟動產品需要幾分鐘的時間。若要查看目前狀態，請重新整理瀏覽器。產品成功啟動後，狀態為可用。

   AWS Service Catalog 會建立新的 Amazon S3 儲存貯體，名為 **`terraform-s3-product`**。

步驟 10：監控 Terraform 佈建操作

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

佈建工作流程有兩個狀態機器：

- `ManageProvisionedProductStateMachine` - 在佈建新的 Terraform 產品和更新現有的 Terraform 佈建產品時 AWS Service Catalog 調用此狀態機器。
- `TerminateProvisionedProductStateMachine` - 在終止現有的 Terraform 佈建產品時 AWS Service Catalog 呼叫此狀態機器。

執行監控狀態機器

1. 開啟 AWS 管理主控台，並在安裝 Terraform 佈建引擎的管理員中樞帳戶中以管理員身分登入。
2. 打開 AWS Step Functions。
3. 在左側導覽面板中，選擇狀態機器。
4. 選擇 ManageProvisionedProductStateMachine。

5. 在執行清單中，輸入佈建的產品 ID 來尋找您的執行。

> **Note**
>
> AWS Service Catalog 當您佈建產品時， 會建立佈建的產品 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，您可以檢視佈建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

的雲端安全性 AWS 是最高優先順序。身為 AWS 客戶，您可以受益於資料中心和網路架構，這些架構專為滿足最安全敏感組織的需求而建置。

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

- 雲端的安全性 – AWS 負責保護在 AWS Cloud 中執行 AWS 服務的基礎設施。 AWS 也為您提供可安全使用的服務。在 AWS 合規計劃中，第三方稽核員會定期測試並驗證我們的安全功效。

  若要了解適用的合規計劃 AWS Service Catalog，請參閱AWS 合規計劃範圍內的服務
- 雲端的安全性 – 您的責任取決於您使用 AWS 的服務。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。

本文件可協助您了解如何在使用 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 以符合您的安全與合規目標。也會向您介紹其他 AWS 服務，協助您監控和保護 AWS Service Catalog 資源。

主題

- 中的資料保護 AWS Service Catalog
- 中的 Identity and Access Management AWS Service Catalog
- 在 中記錄和監控 AWS Service Catalog
- 的合規驗證 AWS Service Catalog
- 中的彈性 AWS Service Catalog
- 中的基礎設施安全 AWS Service Catalog
- 的安全最佳實務 AWS Service Catalog

中的資料保護 AWS Service Catalog

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

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

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

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

使用加密來保護資料

靜態加密

AWS Service Catalog 使用 Amazon S3 儲存貯體和使用 Amazon 受管金鑰進行靜態加密的 Amazon DynamoDB 資料庫。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 Transport Layer Security (TLS)，以及呼叫者與 之間傳輸中資訊的用戶端加密 AWS。

您可以透過建立 VPC 端點，從 Amazon Virtual Private Cloud (Amazon VPC) 私下存取 AWS Service Catalog APIs。使用 VPC 端點時，VPC 和 之間的路由 AWS Service Catalog 會由 AWS 網路處理，而不需要網際網路閘道、NAT 閘道或 VPN 連接。

最新一代的 VPC 端點 AWS Service Catalog 採用 技術 AWS PrivateLink，這項 AWS 技術可在 VPCs 中使用具有私有 IPs 的彈性網路介面，在服務之間 AWS 實現私有連線。

中的 Identity and Access Management AWS Service Catalog

存取 AWS Service Catalog 需要登入資料。這些登入資料必須具有存取 AWS 資源的許可，例如 AWS Service Catalog 產品組合或產品。 與 AWS Identity and Access Management (IAM) AWS Service Catalog 整合，可讓您授予 AWS Service Catalog 管理員建立和管理產品所需的許可，以及授予 AWS Service Catalog 最終使用者啟動產品和管理佈建產品所需的許可。這些政策是由 建立和管理 AWS ，或由管理員和最終使用者個別建立和管理。若要控制存取，請將這些政策連接到搭配 使用的使用者、群組和角色 AWS Service Catalog。

目標對象

您使用 AWS Identity and Access Management (IAM) 擁有的許可可以取決於您扮演的角色 AWS Service Catalog。

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

管理員 - 身為 AWS Service Catalog 管理員，您需要管理員主控台和 IAM 許可的完整存取權，才能執行任務，例如建立和管理產品組合和產品、管理限制條件，以及授予最終使用者的存取權。

最終使用者 - 最終使用者可以使用您的產品之前，您需要授予他們許可，讓他們能夠存取 AWS Service Catalog 最終使用者主控台。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，建議您了解如何撰寫政策以管理存取權的詳細資訊 AWS Service Catalog。若要檢視您可以在 IAM 中使用的以 AWS Service Catalog 身分為基礎的政策範例，請參閱 the section called “AWS 受管政策”。

的身分型政策範例 AWS Service Catalog

主題

- 最終使用者的主控台存取
- 最終使用者的產品存取
- 管理佈建產品的範例政策

最終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。當具有這些政策之一的使用者

AWS Service Catalog 在 中選擇時 AWS 管理主控台，最終使用者主控台檢視會顯示他們具有啟動許可的產品。

在最終使用者可以成功啟動 AWS Service Catalog 您授予存取權的產品之前，您必須提供他們額外的 IAM 許可，讓他們能夠使用產品 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)，您必須授予使用者 Amazon RDS 啟動產品的許可。

若要了解如何讓最終使用者在強制執行最低存取 AWS 資源許可的同時啟動產品，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 將這些許可直接授予最終使用者，但如果您想要限制最終使用者對 AWS 資源的存取，則應將政策連接至啟動角色。然後 AWS Service Catalog ，您可以使用 將啟動角色套用至產品的啟動限制。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**
>
> 如果您授予使用者 AWS Service Catalog 管理員的 IAM 許可，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。

最終使用者的產品存取

在最終使用者可以使用您授予存取權的產品之前，您必須提供他們額外的 IAM 許可，以允許他們使用產品 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)，您必須授予使用者 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。您可以直接將這些許可授予 IAM 中的最終使用者，但如果您想要限制最終使用者對 AWS 資源的存取，則應將政策連接至啟動角色。然後 AWS Service Catalog ，您可以使用 將啟動角色套用至產品的啟動限制。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。

管理佈建產品的範例政策

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 –

授予帳戶層級存取權也會授予角色層級存取權和使用者層級存取權，而新增角色層級存取權也會授予使用者層級存取權，但不會授予帳戶層級存取權。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 寫入操作的存取層級：UpdateProvisionedProduct和 TerminateProvisionedProduct，以及讀取操作：ScanProvisionedProducts、 DescribeRecord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
- 最終使用者對佈建產品的存取
- 已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。

JSON

```
{
   "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：

JSON

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

在任何 政策中未指定Condition區塊 AWS Service Catalog ，會被視為與指定"servicecatalog:accountLevel"存取權相同的 。請注意，accountLevel 存取包含 roleLevel 和 userLevel 存取。

最終使用者對佈建產品的存取

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。

JSON

```
{
    "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"
                }
            }
        }
    ]
}
```

已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。

JSON

```
{
    "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"
                }
            }
        }
    ]
}
```

JSON

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

AWS 的 受管政策 AWS Service Catalog AppRegistry

AWS 受管政策： **AWSServiceCatalogAdminFullAccess**

您可以將 AWSServiceCatalogAdminFullAccess 連接到 IAM 實體。AppRegistry 也會將此政策連接至服務角色，以允許 AppRegistry 代表您執行動作。

此政策會授予##許可，以允許完整存取管理員主控台檢視，並授予建立和管理產品和產品組合的許可。

許可詳細資訊

此政策包含以下許可。

- servicecatalog – 允許主體對管理員主控台檢視的完整許可，以及能夠建立和管理產品組合和產品、管理限制、授予最終使用者的存取權，以及在其中執行其他管理任務 AWS Service Catalog。
- cloudformation– 允許列出、讀取、寫入和標記 AWS CloudFormation 堆疊 AWS Service Catalog 的完整許可。
- config– 允許透過 對產品組合、產品和佈建產品的 AWS Service Catalog 有限許可 AWS Config。
- iam– 允許主體檢視和建立建立和管理產品和產品組合所需的服務使用者、gropus 或角色的完整許可。
- ssm – 允許 AWS Service Catalog 使用 AWS Systems Manager 列出和讀取目前 AWS 帳戶和 AWS 區域中的 Systems Manager 文件。

檢視政策：AWSServiceCatalogAdminFullAccess。

AWS 受管政策： **AWSServiceCatalogAdminReadOnlyAccess**

您可以將 AWSServiceCatalogAdminReadOnlyAccess 連接到 IAM 實體。AppRegistry 也會將此政策連接至服務角色，以允許 AppRegistry 代表您執行動作。

此政策授予##許可，允許完整存取管理員主控台檢視。此政策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 – 允許主體對管理員主控台檢視的唯讀許可。

- `cloudformation`– 允許列出和讀取 AWS CloudFormation 堆疊的 AWS Service Catalog 有限許可。
- `config`– 允許透過 對產品組合、產品和佈建產品的 AWS Service Catalog 有限許可 AWS Config。
- `iam`– 允許主體檢視建立和管理產品和產品組合所需的服務使用者、群組或角色的有限許可。
- `ssm` – 允許 AWS Service Catalog 使用 AWS Systems Manager 列出和讀取目前 AWS 帳戶和 AWS 區域中的 Systems Manager 文件。

檢視政策：AWSServiceCatalogAdminReadOnlyAccess。

AWS 受管政策： **AWSServiceCatalogEndUserFullAccess**

您可以將 `AWSServiceCatalogEndUserFullAccess` 連接到 IAM 實體。AppRegistry 也會將此政策連接至服務角色，以允許 AppRegistry 代表您執行動作。

此政策授予###許可，以允許完整存取最終使用者主控台檢視，並授予許可，以啟動產品和管理佈建產品。

許可詳細資訊

此政策包含以下許可。

- `servicecatalog` – 允許主體對最終使用者主控台檢視的完整許可，以及啟動產品和管理佈建產品的能力。
- `cloudformation`– 允許列出、讀取、寫入和標記 AWS CloudFormation 堆疊 AWS Service Catalog 的完整許可。
- `config`– 允許 AWS Service Catalog 有限許可列出和讀取有關產品組合、產品和佈建產品的詳細資訊 AWS Config。
- `ssm` – 允許 AWS Service Catalog 使用 AWS Systems Manager 讀取目前 AWS 帳戶和 AWS 區域中的 Systems Manager 文件。

檢視政策：AWSServiceCatalogEndUserFullAccess。

AWS 受管政策： **AWSServiceCatalogEndUserReadOnlyAccess**

您可以將 `AWSServiceCatalogEndUserReadOnlyAccess` 連接到 IAM 實體。AppRegistry 也會將此政策連接至服務角色，以允許 AppRegistry 代表您執行動作。

此政策授予##許可，允許對最終使用者主控台檢視進行唯讀存取。此政策不會授予啟動產品或管理佈建產品的許可。

許可詳細資訊

此政策包含以下許可。

- `servicecatalog` ：允許主體對最終使用者主控台檢視的唯讀許可。
- `cloudformation`– 允許列出和讀取 AWS CloudFormation 堆疊的 AWS Service Catalog 有限許可。
- `config`– 允許 AWS Service Catalog 有限許可透過 列出和讀取有關產品組合、產品和佈建產品的詳細資訊 AWS Config。
- `ssm` – 允許 AWS Service Catalog 使用 AWS Systems Manager 讀取目前 AWS 帳戶和 AWS 區域中的 Systems Manager 文件。

檢視政策：AWSServiceCatalogEndUserReadOnlyAccess。

AWS 受管政策： **`AWSServiceCatalogSyncServiceRolePolicy`**

AWS Service Catalog 將此政策連接至`AWSServiceRoleForServiceCatalogSync`服務連結角色 (SLR)，允許 AWS Service Catalog 將外部儲存庫中的範本同步至 AWS Service Catalog 產品。

此政策會授予許可，允許有限存取 AWS Service Catalog 動作 （例如 API 呼叫） 和 AWS Service Catalog 依賴的其他 AWS 服務動作。

許可詳細資訊

此政策包含以下許可。

- `servicecatalog` – 允許 AWS Service Catalog 成品同步角色限制對 AWS Service Catalog 公有 APIs存取。
- `codeconnections`– 允許 AWS Service Catalog 成品同步角色限制對 CodeConnections 公有 APIs 存取。
- `cloudformation`– 允許 AWS Service Catalog 成品同步角色限制對 AWS CloudFormation 公有 APIs存取。

檢視政策：AWSServiceCatalogSyncServiceRolePolicy。

服務連結角色詳細資訊

AWS Service Catalog 會將上述許可詳細資訊用於使用者建立或更新使用 CodeConnections AWS Service Catalog 的產品時所建立`AWSServiceRoleForServiceCatalogSync`的服務連結角色。您可以使用 AWS CLI、 AWS API 或透過 AWS Service Catalog 主控台修改此政策。如需如何建立、編輯和刪除服務連結角色的詳細資訊，請參閱使用服務連結角色 (SLRs) AWS Service Catalog。

`AWSServiceRoleForServiceCatalogSync` 服務連結角色中包含的許可 AWS Service Catalog 允許 代表客戶執行下列動作。

- `servicecatalog:ListProvisioningArtifacts` — 允許 AWS Service Catalog 成品同步角色列出同步至儲存庫中範本檔案之指定 AWS Service Catalog 產品的佈建成品。
- `servicecatalog:DescribeProductAsAdmin` — 允許 AWS Service Catalog 成品同步角色使用 `DescribeProductAsAdmin` API 來取得 AWS Service Catalog 產品的詳細資訊，及其與儲存庫中範本檔案同步的相關佈建成品。成品同步角色會使用來自此呼叫的輸出來驗證佈建成品的產品服務配額限制。
- `servicecatalog:DeleteProvisioningArtifact` — 允許 AWS Service Catalog 成品同步角色刪除佈建的成品。
- `servicecatalog:ListServiceActionsForProvisioningArtifact` — 允許 AWS Service Catalog 成品同步角色判斷服務動作是否與佈建成品相關聯，並確保如果與服務動作相關聯，則不會刪除佈建成品。
- `servicecatalog:DescribeProvisioningArtifact` — 允許 AWS Service Catalog 成品同步角色從 `DescribeProvisioningArtifact` API 擷取詳細資訊，包括`SourceRevisionInfo`輸出中提供的遞交 ID。
- `servicecatalog:CreateProvisioningArtifact` — 如果偵測到對外部儲存庫中的來源範本檔案進行變更 （ 例如，遞交 git-push)，允許 AWS Service Catalog 成品同步角色建立新的佈建成品。
- `servicecatalog:UpdateProvisioningArtifact` — 允許 AWS Service Catalog 成品同步角色更新已連線或同步產品的佈建成品。
- `codeconnections:UseConnection` — 允許 AWS Service Catalog 成品同步角色使用現有的連線來更新和同步產品。
- `cloudformation:ValidateTemplate` — 允許 AWS Service Catalog 成品同步角色限制對的存取 AWS CloudFormation ，以驗證外部儲存庫中使用的範本的範本格式，並驗證 是否可以 CloudFormation 支援範本。

AWS 受管政策： **AWSServiceCatalogOrgsDataSyncServiceRolePolicy**

AWS Service Catalog 將此政策連接到AWSServiceRoleForServiceCatalogOrgsDataSync服務連結角色 (SLR) AWS Service Catalog ，允許 與 同步 AWS Organizations。

此政策會授予許可，允許有限存取 AWS Service Catalog 動作 （ 例如 API 呼叫 ） 和 AWS Service Catalog 依賴的其他 AWS 服務動作。

許可詳細資訊

此政策包含以下許可。

- organizations— 允許 AWS Service Catalog 資料同步角色限制對 AWS Organizations 公有 APIs 存取。

檢視政策：AWSServiceCatalogOrgsDataSyncServiceRolePolicy。

服務連結角色詳細資訊

AWS Service Catalog 會將上述許可詳細資訊用於使用者啟用 AWS Organizations 共用產品組合存取或建立產品組合共用時所建立AWSServiceRoleForServiceCatalogOrgsDataSync的服務連結角色。您可以使用 AWS CLI、 AWS API 或透過 AWS Service Catalog 主控台修改此政策。如需如何建立、編輯和刪除服務連結角色的詳細資訊，請參閱使用服務連結角色 (SLRs) AWS Service Catalog。

AWSServiceRoleForServiceCatalogOrgsDataSync 服務連結角色中包含的許可 AWS Service Catalog 允許 代表客戶執行下列動作。

- organizations:DescribeAccount — 允許 AWS Service Catalog Organizations Data Sync 角色擷取指定帳戶的 AWS Organizations相關資訊。
- organizations:DescribeOrganization — 允許 AWS Service Catalog Organizations Data Sync 角色擷取有關使用者帳戶所屬組織的資訊。
- organizations:ListAccounts — 允許 AWS Service Catalog Organizations Data Sync 角色列出使用者組織中的帳戶。
- organizations:ListChildren — 允許 AWS Service Catalog Organizations Data Sync 角色列出指定父 OU 或根中包含的所有組織單位 (UOs) 或帳戶。
- organizations:ListParents — 允許 AWS Service Catalog Organizations Data Sync 角色列出做為指定子 OUs 或帳戶之直接父項的根或 OU。
- organizations:ListAWSServiceAccessForOrganization — 允許 AWS Service Catalog Organizations Data Sync 角色擷取使用者啟用與其組織整合 AWS 的服務清單。

已棄用的政策

下列管理的政策已作廢。

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

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。

若要從已棄用的政策遷移到目前的政策，請參閱AWS Identity and Access Management 《使用者指南》中的新增和移除 IAM 身分許可。

AWS 受管政策的 AppRegistry 更新

檢視自此服務開始追蹤這些變更以來 AppRegistry AWS 受管政策更新的詳細資訊。如需此頁面變更的自動提醒，請訂閱 AppRegistry 文件歷史記錄頁面上的 RSS 摘要。

變更	描述	Date
AWSServiceCatalogSyncServiceRolePolicy – 更新受管政策	AWS Service Catalog 已更新`AWSServiceCatalogSyncServiceRolePolicy` 政策以`codestar-connections` 變更為`codeconnections` 。	2024 年 5 月 7 日
AWSServiceCatalogAdminFullAccess – 更新受管政策	AWS Service Catalog 已更新`AWSServiceCatalogAdminFullAccess` 政策，以包含 AWS Service Catalog 管理員在其帳戶中建立`AWSServiceRoleForServiceCatalogOrgsDataSync` 服務連結角色 (SLR) 所需的許可。	2023 年 4 月 14 日

變更	描述	Date
AWSServiceCatalogOrgsDataSyncServiceRolePolicy – 新的受管政策	AWS Service Catalog 新增了連接到AWSServiceRoleForServiceCatalogOrgsDataSync 服務連結角色 (SLR) 的 AWSServiceCatalogOrgsDataSyncServiceRolePolicy ，AWS Service Catalog 允許 與 同步 AWS Organizations。此政策允許有限存取 AWS Service Catalog 動作（例如 API 呼叫），以及 AWS Service Catalog 所依賴的其他 AWS 服務動作。	2023 年 4 月 14 日
AWSServiceCatalogAdminFullAccess – 更新受管政策	AWS Service Catalog 已更新AWSServiceCatalogAdminFullAccess 政策，納入 AWS Service Catalog 管理員的所有許可，並建立與 AppRegistry 的相容性。	2023 年 1 月 12 日
AWSServiceCatalogSyncServiceRolePolicy – 新受管政策	AWS Service Catalog 已新增 政策，該AWSServiceCatalogSyncServiceRolePolicy 政策會連接至AWSServiceRoleForServiceCatalogSync 服務連結角色 (SLR)。此政策允許 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

變更	描述	Date
AWSServiceRoleForServiceCatalogSync – 新的服務連結角色	AWS Service Catalog 已新增`AWSServiceRoleForServiceCatalogSync` 服務連結角色 (SLR)。需要此角色 AWS Service Catalog 才能使用 CodeConnections，以及建立、更新和描述產品的 AWS Service Catalog 佈建成品。	2022 年 11 月 18 日
AWSServiceCatalogAdminFullAccess – 更新了受管政策	AWS Service Catalog 已更新`AWSServiceCatalogAdminFullAccess` 政策，以包含 AWS Service Catalog 管理員的所有必要許可。政策會識別管理員可以對所有 AWS Service Catalog 資源採取的特定動作，例如建立、描述、刪除等。此外，政策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` 政策作為範本，以允許或拒絕根據標籤對 AWS Service Catalog 資源執行的動作。如需 ABAC 的詳細資訊，請參閱《》中的什麼是 ABAC for AWSAWS Identity and Access Management。	2022 年 9 月 30 日
AppRegistry 已開始追蹤變更	AppRegistry 開始追蹤其 AWS 受管政策的變更。	2022 年 9 月 15 日

使用 的服務連結角色 AWS Service Catalog

AWS Service Catalog use AWS Identity and Access Management (IAM) 服務連結角色。服務連結角色是直接連結至 的唯一 IAM 角色類型 AWS Service Catalog。服務連結角色由 預先定義， AWS Service Catalog 並包含該服務代表您呼叫其他 AWS 服務所需的所有許可。

服務連結角色可讓您更 AWS Service Catalog 輕鬆地設定，因為您不必手動新增必要的許可。 AWS Service Catalog 會定義其服務連結角色的許可，除非另有定義，否則只能 AWS Service Catalog 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。這可保護您的 AWS Service Catalog 資源，因為您不會不小心移除存取資源的許可。

如需有關支援服務連結角色的其他 服務的資訊，請參閱 AWS 服務與 IAM 搭配使用，並在服務連結角色欄中尋找具有是的服務。選擇具有連結的是，以檢視該服務的服務連結角色文件。

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** – 必須使用此服務連結角色 AWS Service Catalog ， 才能使用 CodeConnections 並建立、更新和描述 AWS Service Catalog 產品的佈建成品。

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

- `sync.servicecatalog.amazonaws.com`

名為 AWSServiceCatalogSyncServiceRolePolicy 的角色許可政策允許 對指定的資源 AWS Service Catalog 完成下列動作：

- 動作：`CodeConnections` 上的 `Connection`
- 動作：`ProvisioningArtifact` AWS Service Catalog 產品在 `Create, Update, and Describe`上的

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 當您在 AWS CLI、 或 AWS API 中建立 CodeConnections 時 AWS 管理主控台， 會自動為您建立服務連結角色。

> **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 AWS Service Catalog 服務，當服務連結角色開始支援服務時， 會在您的帳戶中 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 CodeConnections 時， 會再次為您 AWS Service Catalog 建立服務連結角色。

您也可以使用 IAM 主控台建立具有同步 AWS Service Catalog 產品使用案例的服務連結角色。在 AWS CLI 或 AWS API 中，使用服務名稱建立sync.servicecatalog.amazonaws.com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 組織需要此服務連結角色才能保持同步 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受管政策之外，AWSServiceRoleForServiceCatalogOrgsDataSync服務連結角色還要求您使用下列信任政策： ???

JSON

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

名為 AWSServiceCatalogOrgsDataSyncServiceRolePolicy 的角色許可政策允許 對指定的資源 AWS Service Catalog 完成下列動作：

- 動作：Organizations accounts 上的 DescribeAccount、DescribeOrganization 和 ListAWSServiceAccessForOrganization
- 動作：Organizations accounts 上的 ListAccounts、ListChildren 和 ListParent

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 會將您啟用 與 共用 AWS Organizations或 的動作共用產品組合視為 代表您在背景建立 SLR AWS Service Catalog 的許可。

AWS Service Catalog 當您在 AWS CLI、 EnableAWSOrganizationsAccess或 AWS API CreatePortfolioShare中請求 或 時 AWS 管理主控台， 會自動為您建立服務連結角色。

> **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。當您請求 `EnableAWSOrganizationsAccess`或 時`CreatePortfolioShare`， 會再次為您 AWS Service Catalog 建立服務連結角色。

編輯 的服務連結角色 AWS Service Catalog

AWS Service Catalog 不允許您編輯 `AWSServiceRoleForServiceCatalogSync`或`AWSServiceRoleForServiceCatalogOrgsDataSync`服務連結角色。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。

刪除 的服務連結角色 AWS Service Catalog

您可以使用 IAM 主控台、CLI AWS 或 AWS API 來手動刪除 `AWSServiceRoleForServiceCatalogSync`或 `AWSServiceRoleForServiceCatalogOrgsDataSync` SLR。若要這麼做，您必須先手動移除使用服務連結角色的所有資源（例如，同步至外部儲存庫的任何 AWS Service Catalog 產品），然後才能手動刪除服務連結角色。

AWS Service Catalog 服務連結角色支援的區域

AWS Service Catalog 支援在提供服務的所有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	中的支援 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

區域名稱	區域身分	中的支援 AWS Service Catalog
美國西部 (奧勒岡)	us-west-2	是
Africa (Cape Town)	af-south-1	是
亞太地區 (香港)	ap-east-1	是
亞太地區 (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
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
Europe (Stockholm)	eu-north-1	是
Middle East (Bahrain)	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

區域名稱	區域身分	中的支援 AWS Service Catalog
AWS GovCloud （美國西部）	us-gov-west-1	否

對 AWS Service Catalog 身分和存取進行故障診斷

使用以下資訊來協助您診斷和修正使用 AWS Service Catalog 和 IAM 時可能遇到的常見問題。

主題

- 我無權在 中執行動作 AWS Service Catalog
- 我未獲得執行 iam:PassRole 的授權
- 我想要允許 AWS 帳戶外的人員存取我的 AWS Service Catalog 資源

我無權在 中執行動作 AWS Service Catalog

如果 AWS 管理主控台 告訴您無權執行 動作，則必須聯絡您的管理員尋求協助。您的管理員是為您提供簽署憑證的人員。當 mateojackson 使用者嘗試使用主控台檢視虛構 my-example-widget 資源的詳細資訊，但沒有虛構`aws:GetWidget`許可時，會發生下列範例錯誤。

```
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。您的管理員是為您提供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。

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

當名為 marymajor 的使用者嘗試使用主控台在其中執行動作時，會發生下列範例錯誤 AWS Service Catalog。不過， 動作需要服務具有服務角色授予的許可。Mary 沒有將角色傳遞給服務的許可。

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

在這種情況下，Mary 要求她的管理員更新她的政策，以允許她執行 iam：PassRole 動作。

我想要允許 AWS 帳戶外的人員存取我的 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：

- 若要了解 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 ManagementAWS Service Catalog》中的 。
- 若要了解如何在您擁有的 AWS 帳戶中提供資源的存取權，請參閱《IAM 使用者指南》中的為您擁有的另一個 AWS 帳戶中的 IAM 使用者提供存取權。
- 若要了解如何將資源的存取權提供給第三方 AWS 帳戶，請參閱《IAM 使用者指南》中的將存取權提供給第三方擁有 AWS 的帳戶。
- 如需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 產品組合為您的管理員提供最終使用者群組的存取控制層級。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”。

Constraints

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 啟動限制可讓您進一步控制最終使用者所需的許可。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 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”。

在 中記錄和監控 AWS Service Catalog

AWS Service Catalog 與 整合 AWS CloudTrail，此服務會擷取所有 AWS Service Catalog API 呼叫，並將日誌檔案交付至您指定的 Amazon S3 儲存貯體。如需詳細資訊，請參閱使用 CloudTrail 記錄 AWS Service Catalog API 呼叫。

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

的合規驗證 AWS Service Catalog

第三方稽核人員 AWS Service Catalog 會在多個合規計畫中評估 的安全性和 AWS 合規性，包括下列項目：

- 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 AWS 的服務清單，請參閱合規計劃範圍內的 AWS 服務。 如需一般資訊，請參閱AWS 合規計劃。

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 取決於資料的機密性、您公司的合規目標，以及適用的法律和法規。 AWS 提供這些資源來協助合規：

- 安全與合規快速入門指南 – 這些部署指南討論架構考量，並提供在其中部署以安全與合規為重心的基準環境的步驟 AWS。
- HIPAA 安全與合規架構白皮書 – 此白皮書說明公司如何使用 AWS 來建立符合 HIPAA 規範的應用程式。
- AWS 合規資源 – 此工作手冊和指南集合可能適用於您的產業和位置。
- AWS Config – AWS 此服務會評估資源組態符合內部實務、產業準則和法規的程度。

- AWS Security Hub CSPM – AWS 此服務提供 內安全狀態的全方位檢視 AWS ，可協助您檢查是否符合安全產業標準和最佳實務。

中的彈性 AWS Service Catalog

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

如需 AWS 區域和可用區域的詳細資訊，請參閱 AWS 全球基礎設施。

除了 AWS 全球基礎設施之外， AWS Service Catalog 還提供 AWS Service Catalog 自助式動作。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。如需詳細資訊，請參閱 the section called “使用服務動作”。

中的基礎設施安全 AWS Service Catalog

作為受管服務， AWS Service Catalog 受到 AWS 全球網路安全的保護。如需 AWS 安全服務以及 如何 AWS 保護基礎設施的相關資訊，請參閱AWS 雲端安全。若要使用基礎設施安全的最佳實務來設計您的 AWS 環境，請參閱安全支柱 AWS Well-Architected Framework 中的基礎設施保護。

您可以使用 AWS 發佈的 API 呼叫， AWS Service Catalog 透過網路存取 。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。

使用 AWS Service Catalog，您可以控制資料存放所在的區域。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。

的安全最佳實務 AWS Service Catalog

AWS Service Catalog 提供許多安全功能，供您在開發和實作自己的安全政策時考慮。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 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 會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 類型的 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 套用第二個更嚴格的限制條件 (t1.micro 和 m1.small)。

當您將 IAM 政策連接至啟動角色時，可以限制最終使用者對 AWS 資源的存取。然後 AWS Service Catalog ，您可以使用 建立啟動限制，以在啟動產品時使用 角色。

若要進一步了解 的 受管政策 AWS Service Catalog，請參閱 AWS 的 受管政策 AWS Service Catalog。

管理目錄

AWS Service Catalog 提供從管理員主控台管理產品組合、產品和限制條件的介面。

> **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，請參閱中的 Identity and Access Management AWS Service Catalog。

任務

- 管理產品組合
- 管理產品
- 使用 AWS Service Catalog 限制條件
- AWS Service Catalog 服務動作
- 將 AWS Marketplace 產品新增至您的產品組合
- 使用 CloudFormation StackSets
- 管理預算

管理產品組合

您可以在管理員主控台的產品組合頁面上 AWS Service Catalog 建立、檢視和更新產品組合。

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

- 共用和匯入產品組合

建立、檢視和刪除產品組合

產品組合頁面會顯示您在目前區域中建立的產品組合清單。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。

檢視產品組合頁面

1. 在 https：//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. 如果您是新手 AWS Service Catalog，您會看到 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產品組合，然後前往產品組合頁面。

使用 時 AWS Service Catalog，您可以隨時返回產品組合頁面；在導覽列中選擇服務目錄，然後選擇產品組合。

檢視產品組合詳細資訊

在 AWS Service Catalog 管理員主控台中，產品組合詳細資訊頁面會列出產品組合的設定。使用此頁面以管理產品組合中的產品、授予使用者產品的存取權與套用 TagOptions 及限制。

檢視 Portfolio details (產品組合詳細資訊) 頁面

1. 在 https：//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

使用產品組合頁面來建立和刪除產品組合。

新建產品組合

1. 在左側導覽功能表中，選擇產品組合。
2. 選擇建立產品組合。
3. 在建立產品組合頁面上，輸入請求的資訊。
4. 選擇 Create. AWS Service Catalog created 產品組合並顯示產品組合詳細資訊。

刪除產品組合

> **Note**
>
> 您只能刪除本機產品組合。您可以移除匯入（共用）的產品組合，但無法刪除匯入的產品組合。

您必須先移除其所有產品、限制條件、群組、角色、使用者、共用和 TagOptions，才能刪除產品組合。若要這樣做，請開啟產品組合以顯示產品組合詳細資訊。然後選擇要移除的標籤。

> **Note**
>
> 若要避免錯誤，請先移除產品組合的限制條件，再移除任何產品。

1. 在左側導覽功能表中，選擇產品組合。
2. 選取您要刪除的產品組合。
3. 選擇 刪除。您只能刪除本機產品組合。如果您嘗試刪除匯入（共用）的產品組合，則動作功能表無法使用。
4. 在確認視窗中，選擇 Delete (刪除)。

新增 產品

您可以將新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建立關聯，以將產品新增至產品組合。

> **Note**
>
> 建立 AWS Service Catalog 產品時，您可以上傳 CloudFormation 範本或 Terraform 組態檔案。 CloudFormation 範本存放在 Amazon Simple Storage Service (Amazon S3) 儲存貯體中，儲存貯體名稱開頭為 "cf-templates-"。在佈建產品時，您還必須具有從其他儲存貯體擷取物件的許可。如需詳細資訊，請參閱建立 產品。

新增新產品

您可以從產品組合詳細資訊頁面直接新增新產品。當您從此頁面建立產品時， 會將其 AWS Service Catalog 新增至目前選取的產品組合。

若要新增一個新產品

1. 導覽至產品組合頁面，然後選擇您要新增產品的產品組合名稱。
2. 在產品組合詳細資訊頁面上，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。
   - 產品描述 （選用 ） – 產品描述。此描述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。此描述會顯示在產品清單中，以協助您選擇正確的產品。
   - 擁有者或經銷商 – 擁有者的名稱或電子郵件地址。經銷商的聯絡資訊為選用。
   - Vendor （選用 ） – 應用程式發佈者的名稱。此欄位可讓您排序產品清單，以更輕鬆地尋找產品。
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 CloudFormation 產品，請選擇您自己的範本檔案、本機磁碟機的 CloudFormation 範本，或指向存放在 Amazon S3 中的範本的 URL、現有的 CloudFormation 堆疊 ARN 範本，或存放在外部儲存庫中的範本檔案。

     對於 Teraform 產品，請選擇您自己的範本檔案、本機磁碟機中的 tar.gz 組態檔案，或指向存放在 Amazon S3 中的範本的 URL，或儲存在外部儲存庫中的 tar.gz 組態檔案。
   - 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。
   - 支援連結 （選用 ） – 網站 URL，使用者可以在此找到支援資訊或檔案票證。URL 必須以 `http://`或 `https://` 開頭。管理員負責維護支援資訊的準確性和存取權。
   - 支援描述 （選用 ） – 說明您應該如何使用電子郵件聯絡人和支援連結。
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、產品組合詳細資訊頁面或產品清單頁面。

若要新增現有產品到產品組合中

1. 導覽至產品組合頁面。
2. 選擇產品組合。然後選擇動作 - 將產品新增至產品組合。
3. 選擇產品，然後選擇將產品新增至產品組合。

從產品組合中移除產品

當您不想再使用產品時，請將其從產品組合中移除。產品仍可從產品頁面在您的目錄中取得，而且您仍然可以將產品新增至其他產品組合。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. 導覽至產品組合頁面，然後選擇包含產品的產品組合。產品組合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

您應該新增限制條件，以控制使用者與 產品的互動方式。如需 AWS Service Catalog 支援限制類型的詳細資訊，請參閱 使用 AWS Service Catalog 限制條件。

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：//https://console.aws.amazon.com/servicecatalog/ 開啟 Service Catalog 主控台。
2. 選擇產品組合，然後選取產品組合。
3. 在產品組合詳細資訊頁面中，展開建立限制條件區段，然後選擇新增限制條件。
4. 針對產品，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 角色指派給用來佈建 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 – 可讓您限制最終使用者在啟動產品時可用的選項。範本包含 JSON 格式的文字檔案，其中包含一或多個規則。規則會新增至產品使用的 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 CloudFormation StackSets 設定跨帳戶和區域的產品部署。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。如需詳細資訊，請參閱AWS Service Catalog 標籤更新限制。

6. 選擇繼續，然後輸入必要的資訊。

若要編輯限制條件

1. 登入 AWS 管理主控台 ，並在 https：//https://console.aws.amazon.com/catalog/ 開啟 AWS Service Catalog 管理員主控台。
2. 選擇產品組合，然後選取產品組合。
3. 在產品組合詳細資訊頁面中，展開建立限制條件區段，然後選取要編輯的限制條件。
4. 選擇編輯限制條件。
5. 視需要編輯限制條件，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產品組合。為許多使用者提供產品組合存取權的最佳方法是將使用者放在 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，使用者還必須能夠存取 AWS Service Catalog 最終使用者主控台。您可以透過在 IAM 中套用許可來授予對 主控台的存取權。如需詳細資訊，請參閱中的 Identity and Access Management AWS Service Catalog。

如果您想要與其他帳戶共用產品組合及其委託人，您可以將委託人名稱（群組、角色或使用者）與產品組合建立關聯。委託人名稱會與產品組合共用，並在收件人帳戶中用於授予最終使用者的存取權。

若要授予產品組合的存取權限給使用者或群組

1. 在 https：//https://console.aws.amazon.com/servicecatalog/ 開啟 Service Catalog 主控台。
2. 從導覽窗格中，選擇管理，然後選擇產品組合。
3. 選擇您要授予群組、角色或使用者存取權的產品組合。 AWS Service Catalog 導向至產品組合詳細資訊頁面。
4. 在產品組合詳細資訊頁面上，選擇存取索引標籤。
5. 在產品組合存取下，選擇授予存取權。
6. 針對類型，選擇主體名稱，然後選取群組/、角色/或使用者/、類型。您最多可以新增 9 個主體名稱。
7. 選擇授予存取權，將委託人與目前的產品組合建立關聯。

若要移除對產品組合的存取權限

1. 在產品組合詳細資訊頁面上，選擇群組、角色或使用者名稱。
2. 選擇移除存取權。

共用產品組合

若要讓另一個 AWS 帳戶的 AWS Service Catalog 管理員將您的產品分發給最終使用者，請使用account-to-account共用或 與他們共用您的 AWS Service Catalog 產品組合 AWS Organizations。

當您使用account-to-account共用產品組合時，您會共用該產品組合的參考。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。

收件人無法變更產品或限制條件，但可以為最終使用者新增 AWS Identity and Access Management 存取權。

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

帳戶對帳戶共用

若要完成這些步驟，您必須取得目標帳戶的帳戶 ID AWS 。您可以在 AWS 管理主控台 目標帳戶的 中的我的帳戶頁面上找到 ID。

與 AWS 帳戶共用產品組合

1. 在 https：//https://console.aws.amazon.com/servicecatalog/ 開啟 Service Catalog 主控台。
2. 在左側導覽功能表中，選擇產品組合，然後選取您要共用的產品組合。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 AWS 的帳戶的帳戶 ID。（選用）選取 TagOption 共用。然後，選擇共用。
4. 將 URL 傳送給目標帳戶的 AWS Service Catalog 管理員。URL 會開啟匯入產品組合頁面，並自動提供共用產品組合的 ARN。

匯入一個產品組合

如果另一個 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，以便您可以將其產品分發給最終使用者。

如果產品組合是透過 共用，則不需要匯入產品組合 AWS Organizations。

若要匯入產品組合，您必須從管理員取得產品組合 ID。

若要檢視所有匯入的產品組合，請開啟位於 https：//https://console.aws.amazon.com/servicecatalog/ 的 AWS Service Catalog 主控台。在產品組合頁面上，選取匯入標籤。檢閱匯入的產品組合資料表。

與 共用 AWS Organizations

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

首先，您必須決定要從管理帳戶或委派管理員帳戶共用。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《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，可以與組織共用產品組合。

使用組織結構與組織共用產品組合

1. 在 https：//https://console.aws.amazon.com/servicecatalog/ 開啟 AWS Service Catalog 主控台。
2. 在產品組合頁面上，選取您要共用的產品組合。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。

   您可以選擇根節點，與整個組織、父組織單位 (OU)、子 OU 或組織內 AWS 的帳戶共用產品組合。

   共用到父 OU 會將產品組合共用到該父 OU 內的所有帳戶和子 OU。

   您只能選取檢視 AWS 帳戶，以查看組織中所有 AWS 帳戶的清單。

輸入組織節點的 ID，與組織共用產品組合

1. 在 https：//https://console.aws.amazon.com/servicecatalog/ 開啟 AWS Service Catalog 主控台。
2. 在產品組合頁面上，選取您要共用的產品組合。在動作功能表中，選取共用。
3. 選取組織節點。

   選取您要與整個組織、組織內的帳戶 AWS 或 OU 共用。

   輸入您選取的組織節點 ID，您可以在 AWS Organizations 主控台中找到該 ID，網址為 https：// 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和取消註冊為組織的委派管理員。

委派管理員可以像管理帳戶一樣在其組織中共用 AWS Service Catalog 資源。他們有權建立、刪除和共用產品組合。

若要註冊或取消註冊委派管理員，您必須從管理帳戶使用 API 或 CLI。如需詳細資訊，請參閱 AWS Organizations API 參考中的 RegisterDelegatedAdministrator 和 DeregisterDelegatedAdministrator。

> **Note**
>
> 管理員必須先呼叫 ，才能指定委派代表 EnableAWSOrganizationsAccess。

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

如果成員取消註冊為委派管理員，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**
>
> 如果委派管理員建立的產品組合和共用在委派管理員取消註冊後未移除，請再次註冊和取消註冊委派管理員。此動作會移除該帳戶建立的產品組合和共用。

在組織內移動帳戶

如果您在組織內移動帳戶，與帳戶共用的 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產品組合。

在共用產品組合時共用 TagOptions

身為管理員，您可以建立共享以包含 TagOptions。TagOptions 是金鑰/值對，可讓管理員：

- 定義和強制執行標籤的分類。
- 定義標籤選項並將其與產品和產品組合建立關聯。
- 與其他帳戶共用與產品組合和產品相關聯的標籤選項。

當您在主要帳戶中新增或移除標籤選項時，變更會自動出現在收件人帳戶中。在收件人帳戶中，當最終使用者使用 TagOptions 佈建產品時，他們必須為成為佈建產品上標籤的標籤選擇值。

在收件人帳戶中，管理員可以將其他本機 TagOptions 與其匯入的產品組合建立關聯，以強制執行該帳戶特有的標記規則。

> **Note**
>
> 若要共用產品組合，您需要消費者 AWS 的帳戶 ID。在 主控台的我的 AWS 帳戶尋找帳戶 ID。

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

在共用產品組合時共用 TagOptions

1. 在左側導覽功能表中，選擇產品組合。
2. 在本機產品組合中，選擇並開啟產品組合。
3. 從上面的清單中選擇共用，然後選擇共用按鈕。
4. 選擇與其他 AWS 帳戶或組織共用。
5. 輸入 12 位數帳戶 ID 號碼，選取啟用，然後選擇共用。

   您共用的帳戶會顯示在與 共用的帳戶區段中。它指出是否已啟用 TagOptions。

您也可以更新產品組合共享以包含 TagOptions。屬於產品組合和產品的所有 TagOptions 現在都會共用到此帳戶。

更新產品組合共享以包含 TagOptions

1. 在左側導覽功能表中，選擇產品組合。
2. 在本機產品組合中，選擇並開啟產品組合。
3. 從上述清單中選擇共用。
4. 在與 共用的帳戶中，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用 TagOptions。您共用的帳戶會顯示在與 共用的帳戶區段中。

   當您選取取消共用時，請確認您不想再共用帳戶。

在共用產品組合時共用主體名稱

身為管理員，您可以建立包含主體名稱的產品組合共享。主體名稱是管理員可以在產品組合中指定的群組、角色和使用者的名稱，然後與產品組合共用。當您共用產品組合時， 會 AWS Service Catalog 驗證這些委託人名稱是否已存在。如果它們確實存在， AWS Service Catalog 會自動將相符的 IAM 主體與共用產品組合建立關聯，以將存取權授予使用者。

> **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。對於收件人帳戶中非 AWS Service Catalog 管理員但仍能夠建立主體 （使用者/角色） 的使用者，該使用者可以建立符合產品組合主體名稱關聯的 IAM 主體。雖然此使用者可能不知道透過哪些委託人名稱建立關聯 AWS Service Catalog，但他們可能可以猜測使用者。如果此潛在的呈報路徑是問題，則 AWS Service Catalog 建議使用 `PrincipalType`做為 `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。

當您在主要帳戶中新增或移除主體名稱時， AWS Service Catalog 會自動將這些變更套用到收件人帳戶中。然後，收件人帳戶中的使用者可以根據其角色執行任務：

- 最終使用者可以佈建、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，以將存取權授予該帳戶特定的最終使用者。

> **Note**
>
> 主體名稱共用僅適用於 AWS Organizations。

在共用產品組合時共用主體名稱

1. 在左側導覽功能表中，選擇產品組合。
2. 在本機產品組合中，選擇您要共用的產品組合。
3. 在動作功能表中，選擇共用。
4. 選取 中的組織 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，啟用主體共用選項。

您也可以更新產品組合共享，以包含主體名稱共享。這會與收件人帳戶共用屬於該產品組合的所有主體名稱。

更新產品組合共用以啟用或停用主體名稱

1. 在左側導覽功能表中，選擇產品組合。
2. 在本機產品組合中，選擇您要更新的產品組合。
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體共用。 AWS Service Catalog 然後在收件人帳戶中共用主體名稱。

如果您想要停止與收件人帳戶共用主體名稱，請停用主體共用。

共用主體名稱時使用萬用字元

AWS Service Catalog 支援使用萬用字元將產品組合存取權授予 IAM 主體（使用者、群組或角色）名稱，例如「*」或「？」。使用萬用字元模式可讓您一次涵蓋多個 IAM 主體名稱。ARN 路徑和主體名稱允許無限萬用字元。

可接受的萬用字元 ARN 範例：

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

無法接受萬用字元 ARN 的範例：

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

在 IAM Principal ARN 格式 (**arn:partition:iam:::resource-type/resource-path/resource-name**) 中，有效值包括 user/、group/ 或 role/。只有在 resource-id 區段中的 resource-type 之後，才允許使用 "？" 和 "*"。您可以在 resource-id 內的任何位置使用特殊字元。

"*" 字元也符合 "/" 字元，允許在 resource-id 中形成路徑。例如：

arn:aws:iam:::role/*/ResourceName_? 同時符合 **arn:aws:iam:::role/pathA/pathB/ResourceName_1**和 **arn:aws:iam:::role/pathA/ResourceName_1**。

共用和匯入產品組合

若要將您的 AWS Service Catalog 產品提供給不在 中的使用者 AWS 帳戶，例如屬於其他組織或 AWS 帳戶 組織中其他 的使用者，您可以與他們共用您的產品組合。您可以透過多種方式共用，包括account-to-account共用、組織共用，以及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。如果您想要共用參考 (產品組合的匯入版本，會與原始版本保持同步)，您可以使用帳戶對帳戶共用，也可以使用 AWS Organizations來共用。

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

當您使用account-to-account共用來共用產品組合，或者 AWS Organizations，您可以允許 AWS Service Catalog 另一個 AWS 帳戶的管理員將產品組合匯入其帳戶，並將產品分發給該帳戶中的最終使用者。

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。收件人管理員是您共享產品組合的管理員，無法變更產品或限制條件，但可為最終使用者新增 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。

收件人管理員可以透過下列方式，將產品分發給屬於其 AWS 帳戶的最終使用者：

- 將使用者、群組和角色新增至匯入的產品組合。
- 透過將匯入產品組合中的產品新增至本機產品組合，這是收件人管理員建立且屬於其 AWS 帳戶的個別產品組合。然後，收件人管理員會將使用者、群組和角色新增至該本機產品組合。最初套用至共用產品組合中產品的任何限制也會出現在本機產品組合中。本機產品組合收件人管理員可以新增其他限制條件，但無法移除最初從共用產品組合匯入的限制條件。

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。

啟動角色是在最終使用者啟動產品時， AWS Service Catalog 用來佈建 AWS 資源 （例如 Amazon EC2 執行個體或 Amazon RDS 資料庫） 的 IAM 角色。身為管理員，您可以選擇指定特定的啟動角色 ARN 或本機角色名稱。如果您使用角色 ARN，即使最終使用者所屬的帳戶與 AWS 擁有啟動角色的帳戶不同，也會使用該角色。如果您使用本機角色名稱，則會使用最終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 AWS 的帳戶會佈建 AWS 資源，而此帳戶會產生這些資源的使用費。如需詳細資訊，請參閱AWS Service Catalog 定價。

此影片說明如何在 中跨帳戶共用產品組合 AWS Service Catalog。

在 中跨帳戶共用 (https://www.youtube.com/embed/BVSohYOppjk%22%3EShare) 產品組合 AWS Service Catalog。

> **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**
>
> 產品組合匯入必須在管理與相依帳戶之間的相同區域中進行。

共用的和匯入的產品組合之間的關係

此資料表摘要說明匯入的產品組合與共用產品組合之間的關係，以及匯入產品組合的管理員可以和不可以對該產品組合及其產品採取的動作。

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。 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	將匯入的產品新增到本機產品組合。產品會與共用的產品組合保持同步。	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
	傳播到匯入的產品組合。		
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中移除啟動限制，變更會傳播到產品的所有匯入執行個體。 如果收件人管理員將匯入的產品新增至其本機產品組合，則匯入的啟動限制不會轉移到共用產品組合。	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限制條件。	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。
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。 如果收件人管理員將匯入的產品新增至本機產品組合，則匯入的範本限制不會轉移到本機產品組合。	在本機產品組合中，管理員可以新增限制本機產品的範本限制條件。	移除已匯入的範本限制條件。

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
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、根據更新後的範本建立新版本來更新產品，並將產品分組到產品組合中，以將它們分發給使用者。

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。當您分發更新時，最終使用者可以更新現有的佈建產品。

任務

- 檢視產品頁面
- 建立產品
- 將產品新增至產品組合
- 更新產品
- 從 GitHub、GitHub Enterprise 或 Bitbucket 將產品同步至範本檔案
- 刪除產品
- 管理版本

檢視產品頁面

您可以從 AWS Service Catalog 管理員主控台中的產品清單頁面管理產品。

檢視產品清單頁面

1. 在 https：//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 管理員主控台中的產品頁面建立產品。

> **Note**
>
> 建立 Terraform 產品需要額外的組態，包括 Terraform 佈建引擎和啟動角色。如需詳細資訊，請檢閱 Terraform 產品入門。

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 支援 CloudFormation、Terraform Cloud 和外部 （支援 Terraform Community Edition) 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。
   - 產品描述 – 描述會顯示在產品清單中，以協助您選擇正確的產品。
   - 擁有者 – 發佈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。
   - Distributor （選用） – 應用程式發佈者的名稱。此欄位可讓您排序產品清單，以更輕鬆地尋找產品。
4. 版本詳細資訊可讓您新增範本檔案並建置產品。輸入下列資料：
   - 選擇方法 – 新增範本檔案有四種方式。
     - 使用本機範本檔案 - 從本機磁碟機上傳 CloudFormation 範本或 Terraform tar.gz 組態檔案。
     - 使用 Amazon S3 URL - 指定指向存放在 Amazon S3 中的 CloudFormation 範本或 Terraform tar.gz 組態檔案的 URL。如果您指定 Amazon S3 URL，則必須以 開頭`https://`。
     - 使用外部儲存庫 - 指定您的 GitHub、GitHub Enterprise 或 Bitbucket 程式碼儲存庫。 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在 Tar 中封存並以 Gzip 壓縮的單一檔案。
     - 使用現有的 CloudFormation 堆疊 - 輸入現有 CloudFormation 堆疊的 ARN。此方法不支援 Terraform Cloud 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。
   - 描述 （選用） – 產品版本的描述，包括此版本與其他版本的差異。

- 指引 – 在產品詳細資訊頁面上的版本索引標籤中受管。在建立產品工作流程期間建立產品版本時，該版本的指引會設為預設。若要進一步了解指引，請參閱管理版本。

5. 支援詳細資訊可識別您公司內的組織，並提供支援聯絡窗口。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。
   - 支援連結 （選用） – 網站 URL，使用者可以在此找到支援資訊或檔案票證。URL 必須以 `http://`或 `https://` 開頭。管理員負責維護支援資訊的準確性和存取權。
   - 支援描述 （選用） – 說明您應該如何使用電子郵件聯絡人和支援連結。

6. 管理標籤 （選用） – 除了使用標籤來分類資源之外，您也可以使用它們來驗證建立此資源的許可。

7. 建立產品 – 當您完成表單時，請選取建立產品。幾秒鐘後，產品會出現在產品清單頁面上。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 AWS Service Catalog ，並交付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：建立部署到的管道 AWS Service Catalog。

您可以在 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。這些屬性可以定義值的最小和最大長度、最小和最大值、允許的值，以及規則表達式。如果提供的值不符合參數屬性， 會在佈建期間 AWS Service Catalog 發出警告。若要進一步了解參數屬性，請參閱CloudFormation 《 使用者指南》中的參數。

疑難排解

您必須具有從 Amazon S3 儲存貯體擷取物件的許可。否則，您可能會在啟動或更新產品時遇到下列錯誤。

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

如果您遇到此訊息，請確定 具有從下列儲存貯體擷取物件的許可：

- 存放佈建成品範本的儲存貯體。
- 以 "cf-templates-*" 開頭的儲存貯體，以及 AWS Service Catalog 存放佈建成品範本的 。
- 以 "sc-*" 開頭的內部儲存貯體，以及 AWS Service Catalog 存放中繼資料的位置。您無法從您的帳戶看到此儲存貯體。

下列範例政策顯示從先前提及的儲存貯體擷取物件所需的最低許可。

```
{
          "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-*/*"
          ]
      }
```

將產品新增至產品組合

您可以將產品新增至任意數量的產品組合。產品更新時，包含產品的所有產品組合（包括共用產品組合）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，選擇將產品新增至產品組合。系統會將您導向至將***name-of-product***新增至產品組合頁面。
3. 選擇產品組合，然後選擇將產品新增至產品組合。

將 Terraform 產品新增至產品組合時，產品需要啟動限制條件。您必須從帳戶選取 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，且帳戶使用啟動限制，則帳戶會針對 IAM 角色使用該名稱。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較少的資源。如需詳細資訊和說明，請參閱 步驟 6：將啟動限制新增至 Terraform 產品

產品組合可以包含許多混合 CloudFormation 和 Terraform 產品類型的產品。

更新產品

當您更新產品的範本時，您會建立新的產品版本。新的產品版本會自動提供給有權存取包含產品的產品組合的所有使用者。

> **Note**
>
> 更新現有產品時，您無法變更產品類型 (CloudFormation 或 Teraform)。例如，如果您更新 CloudFormation 產品，則無法將現有 CloudFormation 範本取代為 Terraform tar.gz 組態檔案。您必須使用新的 CloudFormation 範本檔案更新現有的 CloudFormation 範本檔案。

目前執行先前產品版本的佈建產品的最終使用者可以將其佈建產品更新為新版本。當產品有新版本可用時，使用者可以使用佈建產品清單或佈建產品詳細資訊頁面上的更新佈建產品命令。

在建立新的產品版本之前， AWS Service Catalog 建議您在 Terraform 引擎中 CloudFormation 或在中測試產品更新，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訊頁面。
3. 在產品詳細資訊頁面上，展開版本索引標籤，然後選擇建立新版本。
4. 在版本詳細資訊下，執行下列動作：
   - 選擇範本 – 新增範本檔案有四種方式。

     使用本機範本檔案 - 從本機磁碟機上傳 CloudFormation 範本或 Terraform tar.gz 組態檔案。

     使用 Amazon S3 URL - 指定指向存放在 Amazon S3 中的 CloudFormation 範本或 Terraform tar.gz 組態檔案的 URL。如果您指定 Amazon S3 URL，必須以 https：// 開頭。

     使用外部儲存庫 - 指定您的 GitHub、GitHub Enterprise 或 Bitbucket 程式碼儲存庫。 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在 Tar 中封存並以 Gzip 壓縮的單一檔案。

     使用現有的 CloudFormation 堆疊 - 輸入現有 CloudFormation 堆疊的 ARN。此方法不支援 Terraform Cloud 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。
   - 描述（選用）– 產品版本的描述，包括此版本與先前版本的差異。
5. 選擇建立產品版本。

您也可以使用 CodePipeline 建立和設定管道，將產品範本部署到其中 AWS Service Catalog，並在來源儲存庫中交付變更。如需詳細資訊，請參閱教學課程：建立部署到的管道 AWS Service Catalog。

從 GitHub、GitHub Enterprise 或 Bitbucket 將產品同步至範本檔案

AWS Service Catalog 可讓您將產品同步至透過外部儲存庫提供者管理的範本檔案。 AWS Service Catalog 是指具有此類範本連線的產品，做為 Git 同步產品。儲存庫選項包括 GitHub、GitHub Enterprise 或 Bitbucket。使用外部儲存庫帳戶授權 AWS 帳戶 之後，您可以建立新的 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。當對範本檔案進行變更並在儲存庫中遞交時 （例如，使用 git-push)， 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許可
- 建立帳戶連線
- 檢視 Git 同步產品連線
- 更新 Git 同步產品連線
- 刪除 Git 同步產品連線
- 從 GitHub、GitHub Enterprise 或 Bitbucket 將 Terraform 產品同步至範本檔案
- AWS 區域 支援 Git 同步產品

將產品同步至外部範本檔案所需的許可

您可以使用下列 AWS Identity and Access Management (IAM) 政策做為範本，讓 AWS Service Catalog 管理員從外部儲存庫將產品同步至範本檔案。此政策包含 CodeConnections 和 的必要許可 AWS Service Catalog。 AWS Service Catalog 建議您複製以下範本政策，並在 AWS Service Catalog `AWSServiceCatalogAdminFullAccess`啟用儲存庫同步產品時使用 受管政策。

JSON

```
{
    "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儲存庫詳細資訊。您可以使用 AWS Service Catalog 主控台、CodeConnections 主控台、 AWS Command Line Interface (CLI) 或 CodeConnections APIs 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 來建立同步 AWS Service Catalog 產品。 AWS Service Catalog 管理員可以根據儲存庫和分支中的範本檔案建立新的或更新現有 AWS Service Catalog 產品。如果在儲存庫中遞交變更， 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，並指派已棄用的狀態。

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 AWS Service Catalog 允許 偵測遞交至儲存庫的任何範本檔案變更。SLR 也允許 AWS Service Catalog 自動為同步產品建立新的產品版本。如需 SLR 許可和功能的詳細資訊，請參閱 的服務連結角色 AWS Service Catalog。

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. 在版本詳細資訊中，選擇使用 AWS CodeStar 提供者指定程式碼儲存庫，然後選擇建立新的 AWS CodeStar 連線連結。
4. 建立連線後，請重新整理連線清單，然後選取新的連線。指定儲存庫詳細資訊，包括儲存庫、分支和範本檔案路徑。

   如需使用 Terraform 組態檔案的資訊，請參閱 從 GitHub、GitHub Enterprise 或 Bitbucket 將 Terraform 產品同步至範本檔案。

   a. （建立新的 AWS Service Catalog 產品資源時為選用）在支援詳細資訊區段中，新增產品的中繼資料。

   b. （建立新的 AWS Service Catalog 產品資源時選用）在標籤區段中，選擇新增標籤，然後輸入金鑰和值對。
5. 選擇建立新產品。

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 git 受管產品。
2. 輸入常見產品詳細資訊。
3. 在外部儲存庫詳細資訊中，選取AWS CodeStar 連線，然後指定儲存庫和分支。
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，並視需要繼續新增產品。
5. 新增所有必要的產品後，請選擇大量建立產品。

將現有 AWS Service Catalog 產品連線至外部儲存庫

1. 在 AWS Service Catalog 主控台左側導覽面板中，選擇產品清單，然後選擇將產品連線至外部儲存庫。

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，然後指定儲存庫、分支和範本檔案路徑。
4. 選擇下一步。
5. 在檢閱和提交頁面上，驗證連線詳細資訊，然後選擇將產品連線至外部儲存庫。

檢視 Git 同步產品連線

您可以使用 AWS Service Catalog 主控台、API 或 AWS CLI 來檢視儲存庫連線詳細資訊。對於連結至範本檔案 AWS Service Catalog 的產品，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 APIs 中擁有 IAM 許可，才能檢視儲存庫詳細資訊。如需這些 IAM 許可所需政策的詳細資訊，請參閱將 AWS Service Catalog 產品同步至範本檔案的必要許可。

使用 檢視連線和儲存庫詳細資訊 AWS 管理主控台

1. 在左側導覽面板中，選擇產品清單。
2. 從清單中選擇產品。
3. 在產品頁面上，導覽至產品來源詳細資訊區段。
4. 若要檢視產品版本的來源修訂 ID，請選擇建立的最後一個版本連結。版本詳細資訊區段會顯示來源修訂版 ID。

使用 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 同步產品連線

您可以使用 AWS Service Catalog 主控台、 AWS Service Catalog API 或 更新現有的帳戶連線和 Git 同步產品 AWS CLI。

若要了解如何將現有 AWS Service Catalog 產品連線至範本檔案，請參閱建立新的 Git 同步產品連線。

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，請選取產品，導覽至產品來源詳細資訊區段，然後選擇編輯詳細資訊。
   - 若要更新多個產品，請選擇將產品連接到外部儲存庫，選取最多十個產品，然後選擇下一步。
2. 在產品來源詳細資訊區段中，執行下列更新：
   - 指定連線。
   - 指定儲存庫。
   - 指定分支。
   - 為範本檔案命名。
3. 選擇儲存變更。

> **Note**
>
> 對於尚未連接到外部儲存庫的產品，您可以在選取產品後，使用在產品資訊頁面頂端的提醒中顯示的連接到外部儲存庫選項。

您也可以使用 AWS Service Catalog 主控台或 AWS CLI 來

- 將現有 AWS Service Catalog 產品連接到外部儲存庫中的範本檔案
- 更新產品中繼資料，包括產品名稱、描述和標籤。
- 重新設定 （更新同步以使用不同的儲存庫來源） 先前連線 AWS Service Catalog 產品的連線。

使用 AWS Service Catalog 主控台更新連線和儲存庫詳細資訊

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儲存庫的產品。

2. 在產品來源詳細資訊區段中，選擇編輯產品來源。
3. 在產品來源詳細資訊區段中，指定新的所需儲存庫。
4. 選擇儲存變更。

使用 更新連線和儲存庫詳細資訊 AWS CLI

從 AWS CLI 執行 `$ aws servicecatalog update-product`和 `$ aws servicecatalog update-provisioning-artifact`命令。

刪除 Git 同步產品連線

您可以使用 AWS Service Catalog 主控台、CodeConnections API 或 刪除 AWS Service Catalog 產品和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 AWS Service Catalog 產品會切換到定期受管產品。中斷連線產品後，如果範本檔案已變更並遞交至先前連線的儲存庫，則不會反映變更。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 AWS Service Catalog 產品。

使用 AWS Service Catalog 主控台中斷連接 Git 同步產品

1. 在 中 AWS 管理主控台，從左側導覽面板中選擇產品清單。
2. 從清單中選擇產品。
3. 在產品頁面上，導覽至產品來源詳細資訊區段。
4. 選擇中斷連線。
5. 確認動作，然後選擇中斷連線。

使用 中斷連接 Git 同步產品 AWS CLI

從 AWS CLI執行 `$ aws servicecatalog update-product`命令。
在`ConnectionParameters`輸入中，移除指定的連線。

使用 CodeConnections API 或 刪除連線 AWS CLI

在 CodeConnections API 或 中 AWS CLI，執行 `$ aws codestar-connections delete-connection`命令。

從 GitHub、GitHub Enterprise 或 Bitbucket 將 Terraform 產品同步至範本檔案

使用 Terraform 組態檔案建立 Git 同步產品時，檔案路徑只接受 tar.gz 格式。檔案路徑中不接受 Terraform 資料夾格式。

AWS 區域 支援 Git 同步產品

AWS Service Catalog 支援 中的 Git 同步 produtc， AWS 區域 如下表所示。

AWS 區域 名稱	AWS 區域 身分	支援 Git 同步產品
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
Africa (Cape Town)	af-south-1	否
亞太地區 (香港)	ap-east-1	否
亞太地區 (雅加達)	ap-southeast-3	否
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

AWS 區域 名稱	AWS 區域 身分	支援 Git 同步產品
Europe (Paris)	eu-west-3	是
Europe (Stockholm)	eu-north-1	是
Middle East (Bahrain)	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

當您刪除產品時， 會從包含產品的每個產品組合 AWS Service Catalog 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、TagOptions 和服務動作。

> **Important**
>
> 產品刪除後就無法復原。

使用 AWS Service Catalog 主控台刪除產品

1. 導覽至產品組合頁面，然後選取包含您要刪除之產品的產品組合。
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. 對於沒有相關聯資源的產品，請在文字方塊中輸入 Delete 以確認您要刪除的產品，然後選擇 Delete。

   對於具有相關聯資源的產品，請繼續步驟 4。
4. 在刪除產品視窗中，檢閱關聯表格，其中會顯示所有產品關聯的資源。當您刪除產品時， AWS Service Catalog 嘗試取消這些資源的關聯。
5. 確認您想要刪除產品，並在文字方塊中輸入 Delete 來移除所有相關聯的資源。

6. 選擇取消關聯並刪除。

如果 AWS Service Catalog 無法取消所有產品資源的關聯，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，以及每個失敗的描述。如需在刪除產品時解決失敗資源取消關聯的詳細資訊，請參閱在以下刪除產品時解決失敗的資源取消關聯。

主題

- 使用 刪除產品 AWS CLI
- 解決刪除產品時失敗的資源取消關聯

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。是一種 AWS CLI 開放原始碼工具，可讓您使用命令列 Shell 中的 命令與 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 AWS CLI ，以縮短您經常使用的命令或指令碼。

先決條件

- 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和組態基本概念。使用最低 AWS CLI 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，讓您能夠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、標籤選項和服務動作。使用 CLI 刪除產品時，CLI `force-delete-product` 別名可讓您呼叫 `Disassociate` API 來取消關聯任何會阻止 `DeleteProduct` API 的資源。這可避免個別取消關聯的個別呼叫。

> **Note**
>
> 以下程序中顯示的檔案路徑可能會根據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 AWS CLI 刪除 AWS Service Catalog 產品時，CLI `force-delete-product` 別名可讓您呼叫 `Disassociate` API，以取消任何會阻止`DeleteProduct`呼叫的資源的關聯。

在 AWS CLI 組態資料夾中建立 **`alias`** 檔案

1. 在 AWS CLI 主控台中，導覽至 configuraiton 資料夾。根據預設，組態資料夾路徑`~/.aws/`位於 Linux 和 macOS `%USERPROFILE%\.aws\`或 Windows。
2. `cli` 使用檔案導覽或在您偏好的終端機中輸入下列命令來建立名為 的子資料夾：

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

   產生的`cli`資料夾預設路徑位於 `~/.aws/cli/` Linux 和 MacOS `%USERPROFILE%\.aws\cli`或 Windows。
3. 在新`cli`資料夾中，建立名為 `alias` 且沒有副檔名的文字檔案。您可以使用`alias`檔案導覽或在偏好的終端機中輸入下列命令來建立檔案：

   ```
   $ touch ~/.aws/cli/alias
   ```
4. 在第一行`[toplevel]`輸入 。
5. 儲存檔案。

接下來，您可以透過手動將別名指令碼貼入 `alias` 檔案，或使用終端機視窗中的命令，將 force-delete-product 別名新增至 檔案。

手動將 force-delete-product 別名新增至您的**`alias`**檔案

1. 在 AWS CLI 主控台中，導覽至您的 AWS CLI 組態資料夾並開啟 `alias` 檔案。
2. 將下列程式碼別名輸入 檔案，位於 `[toplevel]`行下方：

   ```
   [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 別名新增至您的**alias**檔案

1. 開啟終端機視窗並執行下列命令

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

2. 將別名指令碼貼到終端機視窗，然後按 CTRL+D 結束cat命令。

呼叫 force-delete-product 別名

1. 在終端機視窗中，執行下列命令來呼叫刪除產品別名

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

   以下範例顯示force-delete-product別名命令及其產生的回應

   ```
               $ 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 以確認您想要刪除產品。

成功刪除產品後，終端機視窗會顯示下列結果

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

其他資源

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

- 《 AWS Command Line Interface (CLI) AWS CLI 使用者指南》中的建立和使用別名。
- AWS CLI 別名儲存庫 git 儲存庫。
- 刪除 AWS Service Catalog 產品。
- AWS re：Invent 2016：YouTube 上的有效 AWS CLI 使用者。 YouTube

解決刪除產品時失敗的資源取消關聯

如果您之前因資源取消關聯例外狀況而嘗試刪除產品失敗，請檢閱下列例外狀況清單及其解決方法。

> **Note**
>
> 如果您在收到失敗的資源取消關聯訊息之前關閉刪除產品視窗，您可以遵循繼續執行刪除產品區段中的步驟一到三，以再次開啟視窗。

解決失敗的資源取消關聯

在刪除產品視窗中，檢閱關聯資料表狀態欄。識別失敗的資源取消關聯例外狀況和建議的解決方案：

狀態例外類型	原因	Resolution
產品產品-****	AWS Service Catalog 無法刪除產品，因為產品仍有關聯的 TagOptions、預算、至少一個 `ProvisioningArtifact` 有關聯的動作、產品仍指派給產品組合、產品有使用者，或產品有限制條件。	嘗試再次刪除產品。
使用者： `username` 未獲授權執行：	嘗試刪除產品的使用者沒有取消產品資源關聯的必要許可。	AWS Service Catalog 建議聯絡您的 帳戶管理員，以取得有關取消關聯您目前沒有取消關聯的許可產品資源的詳細資訊。

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 CloudFormation 範本、標題、描述、狀態和指引。

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 - 從版本清單中移除已刪除的版本。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 - 根據預設，產品版本沒有任何指引。最終使用者可以使用該版本來更新和啟動佈建產品。
- 已棄用 - 使用者無法使用已棄用的產品版本啟動新的佈建產品。如果先前啟動的 p 佈建產品使用現已棄用版本，使用者只能使用現有版本或新版本更新該佈建產品。

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 限制條件

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。

Constraints

- 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

啟動限制條件指定最終使用者啟動、更新或終止產品時 AWS Service Catalog 擔任的 AWS Identity and Access Management (IAM) 角色。IAM 角色是使用者或服務 AWS 可暫時擔任以使用 AWS 服務的許可集合。如需簡介範例，請參閱：

- CloudFormation 產品類型： 步驟 6：新增啟動限制以指派 IAM 角色
- Terraform 開放原始碼或 Terraform Cloud 產品類型： 步驟 5：建立啟動角色

啟動限制條件適用於產品組合中的產品（產品產品組合關聯）。啟動限制不適用於產品組合層級或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 登入資料來啟動和管理產品。若要這樣做，他們必須擁有 的許可 CloudFormation、產品使用 AWS 的服務，以及 AWS Service Catalog。透過使用啟動角色，您可以改為將最終使用者的許可限制為該產品所需的最低許可。如需有關最終使用者權限的詳細資訊，請參閱 中的 Identity and Access Management AWS Service Catalog。

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條件的 IAM 角色必須具有使用下列項目的許可：

對於 Cloudformation 產品

- `arn:aws:iam::aws:policy/AWSCloudFormationFullAccess` CloudFormation 受管政策

- 產品 AWS CloudFormation 範本中的服務
- 讀取服務擁有的 Amazon S3 儲存貯體中的 AWS CloudFormation 範本存取權。

對於 Terraform 產品

- 產品 Amazon S3 範本中的服務
- 在服務擁有的 Amazon S3 儲存貯體中讀取對 Amazon S3 範本的存取權。
- `resource-groups:Tag`在 Amazon EC2 執行個體中標記（在執行佈建操作時由 Terraform 佈建引擎擔任）
- `resource-groups:CreateGroup` 用於資源群組標記（由 擔任 AWS Service Catalog ，以建立資源群組並指派標籤）

IAM 角色的信任政策必須允許 AWS Service Catalog 擔任該角色。在下列程序中，當您選取 AWS Service Catalog 做為角色類型時，會自動設定信任政策。如果您不是使用 主控台，請參閱如何搭配 IAM 角色使用信任政策中為擔任角色 AWS 的服務建立信任政策一節。 https://aws.amazon.com/blogs/security/how-to-use-trust-policies-with-iam-roles/

> **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，如授予許可給 AWS Service Catalog 最終使用者一節中的內嵌政策步驟所示。

> **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 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. 前往 https://console.aws.amazon.com/iam/ 開啟 IAM 主控台。

   Terraform 產品需要額外的啟動角色組態。如需詳細資訊，請參閱 Terraform Open Source 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**
>
> 當您設定啟動限制條件的啟動角色時，您必須使用此字串：`"s3:ExistingObjectTag/servicecatalog:provisioning":"true"`。

5. 針對產品使用的每個額外服務，將一行新增至政策。例如，若要新增 Amazon Relational Database Service (Amazon RDS) 的許可，請在`Action`清單中最後一行的結尾輸入逗號，然後新增下列行：

```
"rds:*"
```

6. 選擇 Apply Policy (套用政策)

套用啟動限制

設定啟動角色之後，請將角色指派給產品做為啟動限制條件。此動作 AWS Service Catalog 會指示 在最終使用者啟動產品時擔任該角色。

將角色指派至產品

1. 在 https：//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，您可以從您的帳戶選取 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，且帳戶使用啟動限制，則帳戶會針對 IAM 角色使用該名稱。此方法可讓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較少的資源。

   > **Note**
   >
   > 指定的角色名稱必須存在於建立啟動限制的帳戶中，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)。

新增混淆代理人以啟動限制條件

AWS Service Catalog 支援使用擔任角色請求執行APIs 的混淆代理人保護。當您新增啟動限制條件時，您可以使用啟動角色信任政策中的 `sourceAccount`和 `sourceArn`條件來限制啟動角色存取。它可確保由信任的來源呼叫啟動角色。

在下列範例中， AWS Service Catalog 最終使用者屬於帳戶 111111111111。當 AWS Service Catalog 管理員LaunchConstraint為產品建立 時，最終使用者可以在啟動角色信任政策中指定下列條件，將擔任角色限制為帳戶 111111111111。

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

}
```

使用 佈建產品的使用者LaunchConstraint必須具有相同的 AccountId (111111111111)。如果沒有，操作會失敗並顯示AccessDenied錯誤，防止啟動角色濫用。

以下 AWS Service Catalog APIs受到混淆代理人保護：

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

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

驗證啟動限制條件

若要驗證 AWS Service Catalog 使用 角色來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，最終使用者。

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 Resource Name (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 Terraform Open Source 或 Terraform Cloud 產品的通知限制條件。

通知限制條件會指定 Amazon SNS 主題，以接收堆疊事件的通知。

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：//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，並將限制類型設定為通知。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 Open Source 產品的標籤更新限制條件。

透過標籤更新限制， AWS Service Catalog 管理員可以允許或不允許最終使用者更新與佈建產品相關聯資源的標籤。如果允許標籤更新，則與產品或產品組合相關聯的新標籤將在佈建產品更新期間套用至佈建的資源。

啟用產品的標籤更新

1. 在 https：//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. 選擇限制條件索引標籤，然後選擇新增限制條件。
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 Open Source 產品的堆疊集限制。
> - StackSets 目前不支援 AutoTags。 CloudFormation StackSets

堆疊集限制允許您使用 CloudFormation StackSets，設定產品的部署選項。您可以指定多個帳戶和區域的產品啟動。最終使用者可以管理這些帳戶，並判斷產品部署的位置和部署順序。

套用堆疊集限制至產品

1. 在 https：//https://console.aws.amazon.com/servicecatalog/ 開啟 Service Catalog 主控台。
2. 使用您想要的產品選擇產品組合。
3. 選擇限制條件索引標籤，然後選擇建立限制條件。
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、區域和許可。
   - 在帳戶設定中，識別您要建立產品的帳戶。
   - 在區域設定中，選擇要部署產品的地理區域，以及您希望在這些區域中部署這些產品的順序。
   - 在許可中，選擇 IAM StackSet 管理員角色來管理您的目標帳戶。如果您未選擇角色，StackSets 會使用預設 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 Terraform Open Source 或 Terraform Cloud 產品的範本限制條件。

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。您可以將範本限制條件套用至 AWS Service Catalog 產品組合中的產品。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。

範本限制條件由一或多個規則組成，這些規則會縮小產品基礎 CloudFormation 範本中定義之參數的允許值。 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 CloudFormation 範本參數的詳細資訊，請參閱CloudFormation 《 使用者指南》中的參數。

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 管理員主控台中將規則寫入為 JSON 文字來定義範本限制規則。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：//https://console.aws.amazon.com/servicecatalog/ 開啟 Service Catalog 主控台。
2. 在產品組合頁面上，選擇包含您要套用範本限制的產品的產品組合。
3. 展開限制條件區段，然後選擇新增限制條件。
4. 在選取產品和類型視窗中，針對產品選擇您要定義範本限制的產品。然後，針對限制類型，選擇範本。選擇繼續。
5. 在範本限制條件建置器頁面上，使用 JSON 編輯器或規則建置器界面編輯限制條件規則。

   - 若要編輯規則的 JSON 程式碼，請選擇限制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。

     若要使用規則建置器界面建置規則，請選擇規則建置器標籤。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。

     完成規則的建置後，請選擇新增規則。規則會出現在規則建置器索引標籤的表格中。若要檢閱和編輯 JSON 輸出，請選擇限制文字編輯器索引標籤。
6. 當您完成編輯限制條件的規則時，請選擇提交。若要查看限制條件，請前往產品組合詳細資訊頁面並展開限制條件。

範本限制規則

定義 AWS Service Catalog 產品組合中範本限制的規則說明最終使用者何時可以使用範本，以及他們可以為用於建立其嘗試使用之產品之 CloudFormation 範本中宣告的參數指定哪些值。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，您可以新增規則來驗證最終使用者是否在指定的 VPC 中指定有效的子網路，或測試環境使用的`m1.small`執行個體類型。在建立產品資源之前，CloudFormation 會使用規則來驗證參數值。

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 時， 會 CloudFormation 評估宣告，以在建立或更新堆疊之前檢查子網路參數值是否在該 VPC 中。如果參數值無效，則 CloudFormation 立即無法建立或更新堆疊。如果使用者未指定 VPC， CloudFormation 則不會檢查子網路參數值。

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。

如需定義規則條件和聲明的規則特定內部函數資訊，請參閱AWS CloudFormation 《 使用者指南》中的AWS 規則函數。

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 Terraform Open Source 或 Terraform Cloud 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 停止和重新啟動，您也可以定義自訂動作。

在本教學課程中，您會為最終使用者提供重新啟動 Amazon EC2 執行個體的能力。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。

先決條件

本教學假設您擁有完整的 AWS 管理員許可、已經熟悉 AWS Service Catalog，而且已經擁有一組基本產品、產品組合和使用者。如果您不熟悉 AWS Service Catalog，請先完成設定 和 開始使用任務，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：使用 管理服務動作 AWS CloudFormation
- 步驟 6：故障診斷

步驟 1：設定最終使用者許可

最終使用者必須擁有必要的許可，才能檢視和執行特定的服務動作。在此範例中，最終使用者需要存取 AWS Service Catalog 服務動作功能和執行 Amazon EC2 重新啟動的許可。

更新權限

1. 開啟位於 https：//https://console.aws.amazon.com/iam/ 的 AWS Identity and Access Management (IAM) 主控台。
2. 從功能表中，尋找使用者群組。
3. 選擇最終使用者將用於存取 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。在此範例中，我們透過選取為群組佈建 AWS Service Catalog 和終止許可建立的自訂政策，將許可新增至現有政策。
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：

   JSON

```
{
 "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擁有在 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

接著，建立服務動作以重新啟動 Amazon EC2 執行個體。

1. 在 https：//https://console.aws.amazon.com/sc/ 開啟 AWS Service Catalog 主控台。
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. 在建立動作頁面上，選擇 AWS Systems Manager 文件以定義服務動作。Amazon EC2 執行個體重新啟動動作是由 AWS Systems Manager 文件定義，因此我們會在下拉式功能表 Amazon 文件上保留預設選項。
5. 搜尋並選擇 AWS-RestartEC2Instance 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-RestartEC2instance，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 AWS Service Catalog 儀表板的導覽窗格中，選擇佈建產品清單。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. 在佈建產品詳細資訊頁面上，選擇右上角的動作，然後選擇 AWS-RestartEC2instance 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：使用 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::CloudFormationProduct ProvisioningArtifactProperties
- AWS::ServiceCatalog::ServiceActionAssociation

> **Note**
>
> 如果您管理服務動作與 CloudFormation 資源的關聯，請勿透過 AWS Command Line Interface 或 新增或移除服務動作 AWS 管理主控台。當您執行堆疊更新時，在 外部 CloudFormation 對服務動作所做的任何變更都會遭到取代。

步驟 6：故障診斷

如果您的服務動作執行失敗，您可以在佈建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。

呼叫 StartAutomationExecution 作業時發生錯誤 (ThrottlingException)

服務動作執行是由後端服務調節，例如 SSM。

假設角色時拒絕存取

AWS Service Catalog 無法擔任服務動作定義中指定的角色。請確定 servicecatalog.amazonaws.com 委託人或 servicecatalog.us-east-1.amazonaws.com 等區域委託人被允許列在角色的信任政策中。

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

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

在佈建的產品中找不到具有 ***TargetType*** 類型的任何資源

佈建的產品不包含任何符合 SSM 文件中所指定目標類型的資源，例如 AWS：：EC2：：Instance。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，SSM 遇到不明的例外狀況。

無法擷取角色的認證

AWS Service Catalog 擔任指定角色時遇到未知錯誤。

參數在 {***InvalidValue***1}、{ValidValue2} 中找不到值 "InvalidValue" ***ValidValue1ValidValue2***

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

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

傳遞給 SSM 的 參數值對文件上的 類型無效。

未在服務動作定義中定義參數

參數已傳遞至 AWS Service Catalog 未在服務動作定義中定義的 。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。*#####*如需診斷詳細資訊，請參閱 Automation Service 故障診斷指南。

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。

不允許參數的下列值，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。

SSM 自動化文件未定義的 TargetType

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

將 AWS Marketplace 產品新增至您的產品組合

您可以將 AWS Marketplace 產品新增至您的產品組合，讓這些產品可供最終 AWS Service Catalog 使用者使用。

AWS Marketplace 是線上商店，您可以在其中尋找、訂閱並立即開始使用大量軟體和服務。中的產品類型 AWS Marketplace 包括資料庫、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 可在 取得https://aws.amazon.com/marketplace。請注意，您無法將軟體即服務 (SaaS) 產品從 新增至 AWS Marketplace AWS Service Catalog。

您可以使用 範本將產品 CloudFormation 複製到 AWS Service Catalog，然後將產品新增至產品組合，以將產品分發給 AWS Marketplace AWS Service Catalog 最終使用者。

> **Note**
>
> AWS Service Catalog 不支援使用 Terraform Open Source 或 Terraform Cloud AWS Marketplace 產品範本將產品分發給 AWS Service Catalog 最終使用者。

AWS Marketplace AWS Service Catalog 直接支援 或使用手動選項訂閱和新增產品。我們建議您使用專為 設計的功能來新增產品 AWS Service Catalog。

使用 管理 AWS Marketplace 產品 AWS Service Catalog

您可以使用自訂界面 AWS Service Catalog ，將訂閱 AWS Marketplace 的產品直接新增至 。在 AWS Marketplace 中，選擇 Service Catalog (服務目錄)。如需詳細資訊，請參閱 AWS Marketplace 說明和常見問答集中的將產品複製到 AWS Service Catalog 。

手動管理和新增 AWS Marketplace 產品

完成下列步驟以訂閱 AWS Marketplace 產品、在 CloudFormation 範本中定義該產品，並將範本新增至 AWS Service Catalog 產品組合。

訂閱 AWS Marketplace 產品

1. 前往 AWS Marketplace 。 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. 選擇繼續以檢視履行頁面，然後選擇手動啟動索引標籤。

   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、支援的 AWS 區域和產品用於每個 AWS 區域的 Amazon Machine Image (AMI) ID。請注意，部分選擇將會影響成本。您將使用此資訊在後續步驟中自訂 CloudFormation 範本。
4. 選擇 [接受條款] 以訂閱該產品。

訂閱產品後，您可以隨時選擇您的軟體，然後選擇產品， AWS Marketplace 以存取 中產品履行頁面上的資訊。

在 CloudFormation 範本中定義您的 AWS Marketplace 產品

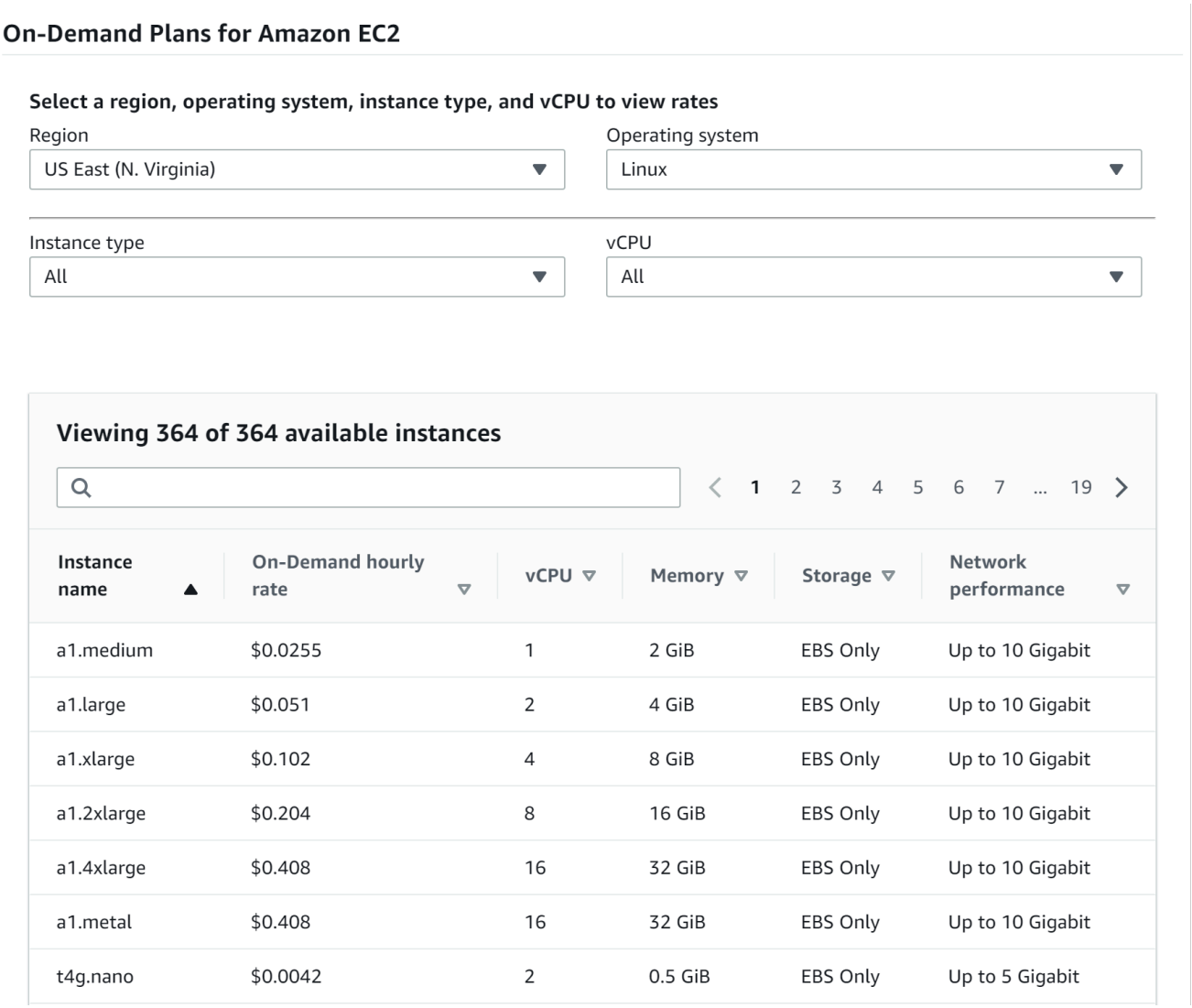
若要完成下列步驟，您將使用其中一個 CloudFormation 範例範本做為起點，而且您將自訂範本，使其代表您 AWS Marketplace 的產品。若要存取範例範本，請參閱 https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/cfn-sample-templates.html 使用者指南中的AWS CloudFormation 範例範本。

1. 在 CloudFormation 使用者指南的範例範本頁面上，為您的產品選擇 AWS 區域。您的 AWS Marketplace 產品必須支援 AWS 區域。您可以在 AWS Marketplace的產品履行頁面上檢視受支援的區域。
2. 若要檢視適合該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 中的產品履行頁面上 AWS Marketplace，檢視定價詳細資訊區段中支援的 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. 在範本的 Mappings區段中，編輯AWSRegionArch2AMI映射，將每個 AWS 區域與您產品的對應架構和 AMI ID 建立關聯。

a. 在 中的產品履行頁面上 AWS Marketplace，檢視您的產品用於每個 AWS 區域的 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 區域的映射。

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 區域和架構映射，從其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 AWS Service Catalog 產品組合。如果您希望進行其他變更，請參閱使用 CloudFormation 範本以進一步了解範本的詳細資訊。

將 AWS Marketplace 產品新增至 AWS Service Catalog 產品組合

1. 登入 AWS 管理主控台 並導覽至 AWS Service Catalog 管理員主控台，網址為 https：//https://console.aws.amazon.com/servicecatalog/。
2. 在產品組合頁面上，選擇您要新增產品的 AWS Marketplace 產品組合。
3. 在產品組合詳細資訊頁面上，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，驗證摘要是否正確，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 CloudFormation StackSets

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

您可以使用 CloudFormation StackSets 跨多個 AWS 區域 和 帳戶啟動 AWS Service Catalog 產品。您可以指定產品在其中循序部署的順序 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 CloudFormation StackSets。

堆疊集與堆疊執行個體

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

堆疊執行個體是指 AWS 區域內目標帳戶中的堆疊，並且只與一個堆疊集相關聯。

如需詳細資訊，請參閱 StackSets 概念。

堆疊集限制

在 中 AWS Service Catalog，您可以使用堆疊集限制條件來設定產品部署選項。

AWS Service Catalog 支援兩個 AWS GovCloud (US) Regions： AWS GovCloud （美國西部） 和 AWS GovCloud （美國東部） 中產品的堆疊集限制。

如需詳細資訊，請參閱AWS Service Catalog 堆疊集限制。

管理預算

您可以使用 AWS Budgets 來追蹤其中的服務成本和用量 AWS Service Catalog。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 Open Source 產品的預算。

AWS 預算可讓您設定自訂預算，在成本或用量超過 （或預測超過） 預算金額時提醒您。如需 AWS Budgets 的相關資訊，請參閱 https://aws.amazon.com/aws-cost-management/aws-budgets。

任務

- 先決條件
- 建立預算
- 關聯預算
- 檢視預算
- 取消關聯預算

先決條件

在使用 AWS Budgets 之前，您需要在 AWS 帳單與成本管理 主控台中啟用成本分配標籤。如需詳細資訊，請參閱「AWS 帳單與成本管理 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 Budgets 功能的任何使用者或群組啟用 AWS 帳單與成本管理 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，您可以讓使用者能夠建立 Amazon SNS 通知，如以下政策範例所示。

建立預算政策

1. 前往 https://console.aws.amazon.com/iam/ 開啟 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。

   JSON

```
{
    "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-1:123456789012:*"
            ]
        }
    ]
}
```

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) 以查看政策授與的許可，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 《 使用者指南》中的建立和連接客戶受管政策。

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，並允許您對其採取動作。若要建立預算，請先決定要與預算建立關聯的產品或產品組合。

若要建立預算

1. 在 https：//https://console.aws.amazon.com/servicecatalog/ 開啟 Service Catalog 主控台。
2. 選擇產品清單或產品組合。
3. 選取您要新增預算的產品或產品組合。
4. 開啟動作功能表，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。

   標籤有兩種類型：AutoTags 和 TagOptions。AutoTags 會識別啟動產品的產品組合、產品和使用者。 會自動將這些標籤 AWS Service Catalog 套用至佈建的資源。TagOption 是在 中管理的管理員定義鍵/值對 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 “先決條件”。
6. 選擇建立。 AWS Budgets系統會將您導向至設定預算頁面。請依照建立預算中的步驟繼續設定您的預算。

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

關聯預算

每個產品組合或產品都可以有一個相關聯的預算。每個預算都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，您可以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。為了讓產品組合或產品上發生的支出反映在預算上，您必須在預算和產品組合或產品上關聯相同的標籤。

> **Note**
>
> 如果您從中刪除預算 AWS Budgets，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資訊。

關聯預算

1. 在 https：//https://console.aws.amazon.com/servicecatalog/ 開啟 Service Catalog 主控台。
2. 選擇產品清單或產品組合。
3. 選取您要與預算建立關聯的產品或產品組合。
4. 開啟動作功能表，然後選擇關聯預算。
5. 在預算關聯頁面上，選取現有的預算，然後選擇繼續。
6. 產品或產品組合資料表現在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和產品清單頁面上檢視預算的相關資訊。如果預算與產品組合相關聯，您可以在產品組合和產品組合詳細資訊頁面上檢視預算的相關資訊。

產品組合和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，系統會將您導向詳細資訊頁面。產品組合詳細資訊和產品詳細資訊頁面包含包含相關預算詳細資訊的區段。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 AWS 預算中刪除預算，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資訊。

取消關聯預算

1. 開啟位於 https：//https://console.aws.amazon.com/servicecatalog/ 的 Service Catalog 主控台。
2. 選擇產品清單或產品組合。
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，選擇取消預算的關聯。確認提醒隨即出現。
5. 在您確認想要從產品或產品組合取消預算之後，請選擇確認。

管理佈建產品

AWS Service Catalog 提供用於管理佈建產品的介面。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

- 以管理員身分管理佈建產品
- 變更佈建產品擁有者
- 更新已佈建產品的範本
- 教學：識別使用者資源分配
- 管理 Terraform 開放原始碼產品狀態錯誤
- 管理 Terraform 開放原始碼產品狀態檔案

以管理員身分管理佈建產品

若要管理帳戶的所有佈建產品，您必須擁有 `AWSServiceCatalogAdminFullAccess`或同等的 IAM 許可，才能存取佈建產品寫入操作。如需詳細資訊，請參閱中的 Identity and Access Management AWS Service Catalog。

> **Tip**
>
> 對於靜態佈建產品鏈結，您必須在佈建產品之前，參考產品成品範本中的佈建產品輸出。如需詳細資訊，包括範例，請參閱下列內容：
>
> - AWS CloudFormation 《 使用者指南》中的 AWS::ServiceCatalog::CloudFormationProvisionedProduct。
> - 《 AWS Service Catalog 開發人員指南》中的 DescribeProvisioningParameters (ProvisioningArtifactOutputKeys)。

檢視並管理所有佈建產品

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

   如果您已登入 AWS Service Catalog 主控台，請選擇 Service Catalog，然後選擇最終使用者。
2. 如有必要，請向下捲動至佈建產品區段。

3. 在佈建產品區段中，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，此功能可供使用 `AWSServiceCatalogAdminFullAccess`受管政策的管理員使用。您可以透過授予最終使用者在 AWS Identity and Access Management (IAM) 中的`servicecatalog:UpdateProvisionedProductProperties`許可，為最終使用者啟用此功能。

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，然後選擇變更佈建產品擁有者。 您也可以在佈建產品的詳細資訊頁面上的動作選單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

您可以將佈建產品的目前範本變更為不同的範本。例如，如果您在 Service Catalog 中有 EC2 產品，您可以更新該 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**
>
> 佈建的 Terraform 開放原始碼或 Terraform 雲端產品不支援更新範本。如果您想要為現有的 Terraform 產品使用不同的範本，您必須刪除產品，然後使用所需的範本建立新的產品。

更新佈建產品的範本

1. 在左側導覽功能表中，選擇佈建產品。
2. 在佈建產品中，選擇佈建產品，然後選取動作、更新。

   請注意，您也可以在佈建產品詳細資訊頁面中選取動作、更新。
3. （選用）在產品詳細資訊中，選擇變更產品。

   在變更產品中，請注意此警告：

   變更產品會將此佈建產品更新為不同的產品範本。這可能會終止資源並建立新的資源。

   您可以將佈建的產品更新為相同產品中的不同版本。
4. （選用）在產品中，選擇您要使用不同範本更新的產品。然後選擇變更。

   在產品詳細資訊中，請注意此警告：

   【產品名稱】 將從 【目前範本名稱】 更新為 【新範本名稱】。不過，您佈建產品的名稱 【佈建產品名稱】 不會變更。

   您可以將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。

   在佈建產品詳細資訊中，您可以查看更新的詳細資訊。佈建的產品名稱不會變更，但佈建的產品現在有不同的範本。

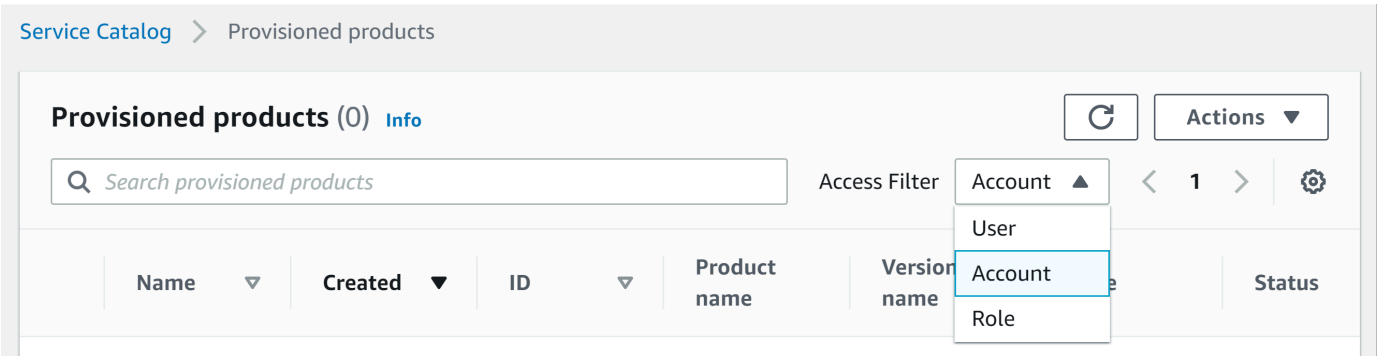
教學：識別使用者資源分配

您可以使用 AWS Service Catalog 主控台來識別佈建產品的使用者，以及與產品相關聯的資源。本教學可協助將此範例翻譯為您自己特定的佈建產品。

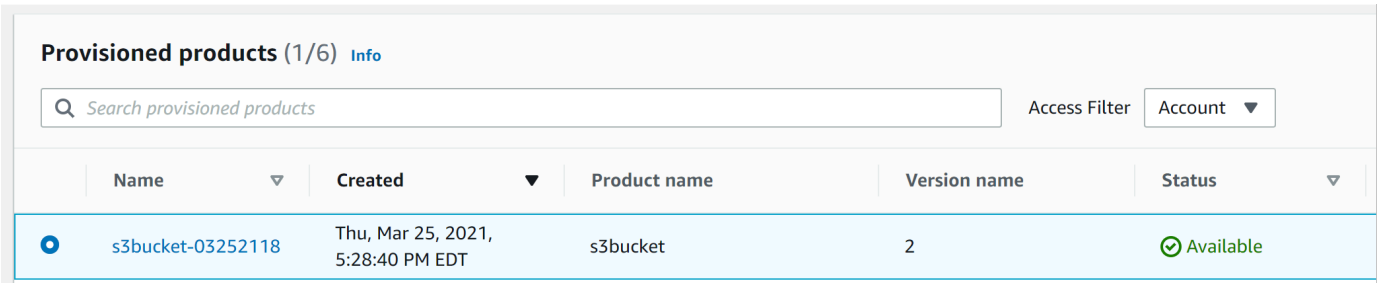
若要管理帳戶所有的佈建產品，您需 `AWSServiceCatalogAdminFullAccess` 或佈建產品寫入操作的相同存取。如需詳細資訊，請參閱《 管理員指南》中的 Identity and Access Management。 AWS Service Catalog

為了識別佈建產品及相關資源的使用者

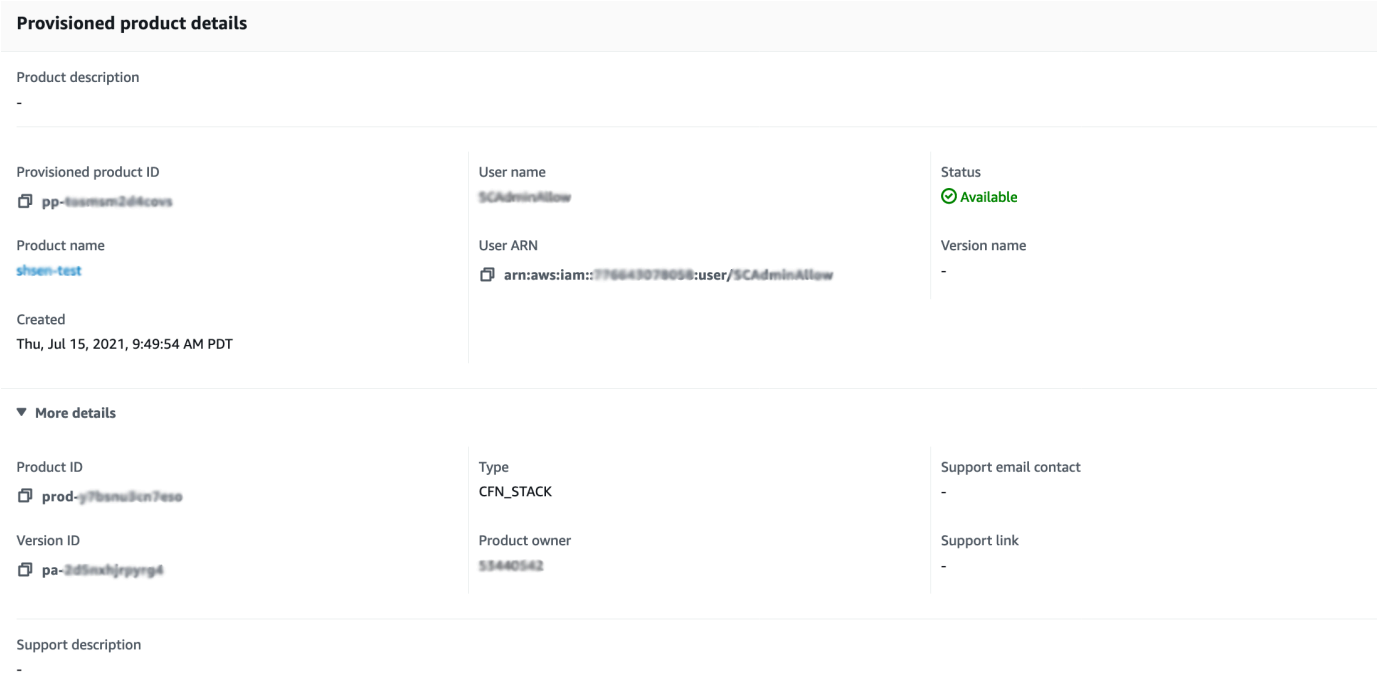
1. 開啟 https：//https://console.aws.amazon.com/servicecatalog。
2. 在左側導覽功能表中，選擇佈建產品。
3. 在存取篩選條件下拉式功能表中，選擇帳戶。



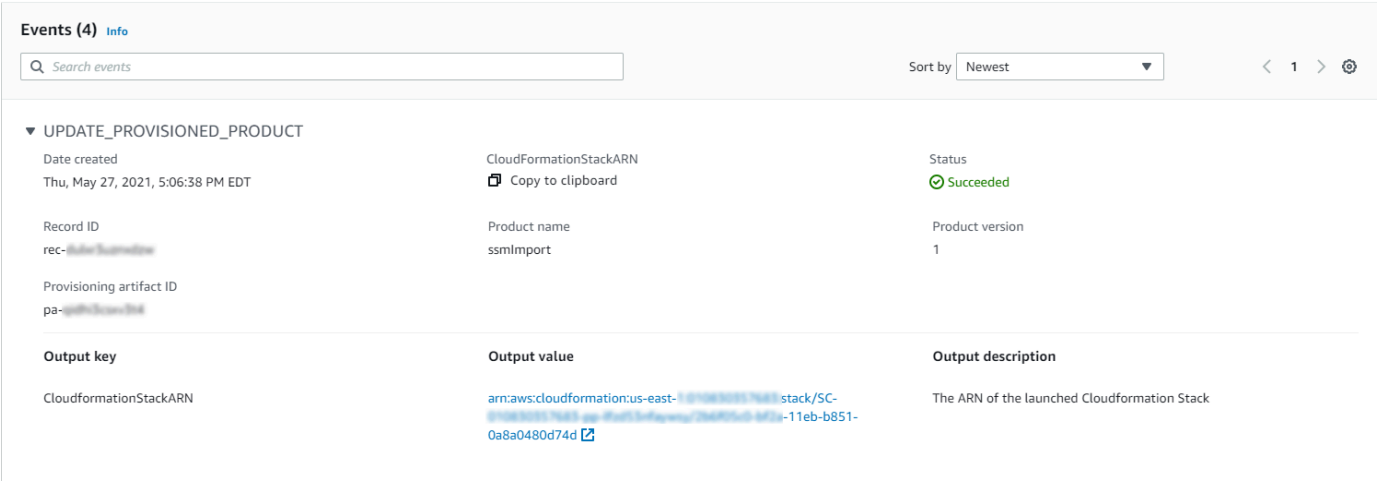
4. 在帳戶檢視中，選擇並開啟佈建產品以顯示其詳細資訊。



您可以查看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 來識別與此啟動對應的 AWS CloudTrail 記錄，並識別請求的使用者（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 `CloudformationStackARN`值來識別 CloudFormation 事件，以尋找所建立資源的相關資訊。您也可以使用 CloudFormation API 來取得此資訊。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 命令列參考。

管理 Terraform 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，允許每個佈建產品繼續至 `UpdateProvisionedProduct`。發生這種情況時：

- `UpdateProvisionedProduct` 不會嘗試更新或更正標籤，或建立或修改資源群組。
- `UpdateProvisionedProduct` 在決定是否應該將佈建產品設定為 `AVAILABLE`或 時， 不會考慮先前佈建操作的失敗`TAINTED`。

AWS Service Catalog 只會在 期間套用標籤`ProvisionProduct`。任何因`ProvisionProduct`操作失敗而導致的失敗標記都不會自動解決。

狀態錯誤範例

範例 1： AWS Service Catalog 未在 期間建立資源群組 `ProvisionProduct`

在下列案例中，即使沒有支援的資源群組，而且沒有將任何標籤套用至資源，您仍有處於 `AVAILABLE` 狀態的佈建產品。

1. 您的動作會啟動 ProvisionProduct。
2. Terraform 佈建引擎會以ProvisionProduct工作流程失敗回應 ，且不提供 ResourceIdentifier。
3. ProvisionProduct 工作流程不會建立資源群組，然後將佈建的產品狀態設定為 ERROR。
4. 然後，您可以啟動 UpdateProvisionedproduct操作。
5. Terraform 佈建引擎回應指出「成功」。
6. 因此，UpdateprovisionedProduct工作流程會將佈建的產品狀態設定為 AVAILABLE，但不會建立資源群組，或嘗試套用任何標籤。

範例 2： AWS Service Catalog 在 期間建立新資源 UpdateProvisionedProduct

在下列案例中，即使新資源未套用任何標籤，您仍有處於 AVAILABLE 狀態的佈建產品。

1. 您的動作會啟動 ProvisionProduct。
2. Terraform 佈建引擎回應指出「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. 您會在建立新資源的新成品UpdateProvisionedProduct上啟動 。
5. Terraform 佈建引擎回應指出「成功」。
6. UpdateProvisionedProduct 工作流程會將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。

狀態錯誤解決方案

AWS Service Catalog 確保為所有TAINTED從 設定為 的佈建產品建立資源群組ProvisionProduct。如果 Terraform 佈建引擎未傳回 ResourceIdentifier，或如果 AWS Service Catalog 無法建立資源群組，則佈建產品會設為 ERROR 狀態，強制您終止。

管理 Terraform 開放原始碼產品狀態檔案

每個 Terraform 開放原始碼佈建產品都有單一狀態檔案。佈建的產品與其狀態檔案之間有 1：1 的關係。檔案存放在名為 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 物件金鑰下。

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。根據預設， AWS Service Catalog 管理員可以查看狀態檔案的清單，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 中管理標籤 AWS Service Catalog

AWS Service Catalog 提供標籤，讓您可以將資源分類。標籤有兩種類型：AutoTags 和 TagOptions。

AutoTags 是識別 中佈建資源來源相關資訊的標籤，由 AWS Service Catalog 自動套用至 AWS Service Catalog 佈建資源。

TagOptions 是在 中管理的鍵/值對 AWS Service Catalog ，可作為建立 AWS 標籤的範本。

主題

- AWS Service Catalog AutoTags
- AWS Service Catalog TagOption 程式庫

AWS Service Catalog AutoTags

> **Note**
>
> AWS Service Catalog 不支援 Terraform Open Source 產品的 AutoTags。

AutoTags 是識別 中佈建資源來源相關資訊的標籤，由 AWS Service Catalog 自動套用至 AWS Service Catalog 佈建資源。

AutoTags 包含產品組合、產品、使用者、產品版本和佈建產品之唯一識別符的標籤。這提供一組標籤，反映客戶在目錄中設定的 AWS Service Catalog 結構。AutoTags 不會與客戶的 50 個標籤限制衝突。

> **Note**
>
> AWS Service Catalog 不支援 Terraform Open Source 產品的 AutoTags。

AWS Service Catalog AutoTags 可協助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 來識別啟動後操作的資源，例如設定 AWS Config 規則。您可以在用於佈建之下游服務的標籤區段中檢視佈建資源的 AutoTags CloudFormation，例如 Amazon EC2 和 Amazon S3。

> **Note**
>
> AWS Service Catalog 將 AutoTags 套用至佈建的資源後，不會更新 AutoTags。如果您將佈建產品更新為不同的產品、佈建成品或新的啟動路徑，現有的 AutoTags仍會顯示原始值。

AutoTag 詳細資訊

- 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。
- aws:servicecatalog:provisioningPrincipalArn – 建立佈建產品的佈建委託人 (使用者) 的 ARN。
- aws:servicecatalog:provisionedProductArn – 佈建產品 ARN。
- aws:servicecatalog:provisioningArtifactIdentifier – 原始佈建成品 (產品版本) 的 ID。

AWS Service Catalog TagOption 程式庫

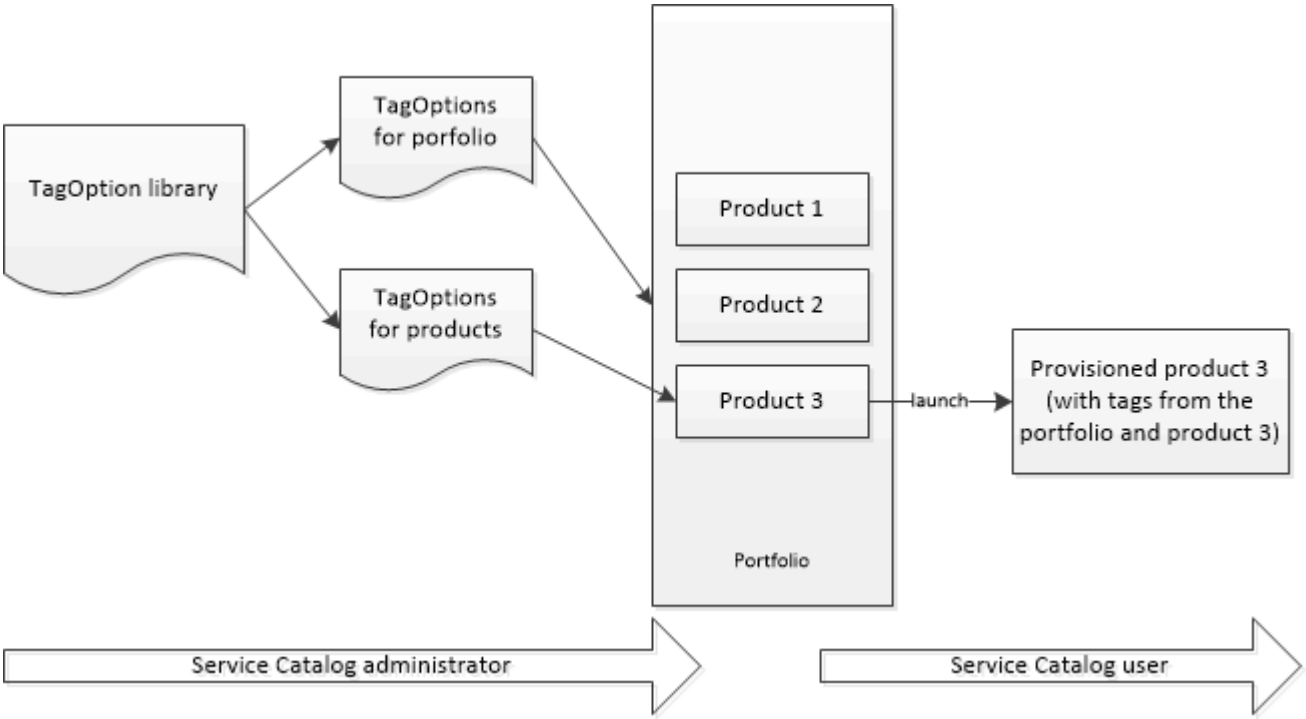
為了讓管理員能夠輕鬆地管理佈建產品上的標籤，AWS Service Catalog 提供了 TagOption 資料庫。TagOption 是在 AWS Service Catalog中受管的金鑰/值對組。它不是 AWS 標籤，而是做為根據 TagOption 建立 AWS 標籤的範本。

AWS Service Catalog 不支援 Terraform Open Source 或 Terraform Cloud 產品的 TagOptions。

TagOption 資料庫讓執行下列的動作變得更輕鬆：

- 一致的分類
- 資源的適當標記 AWS Service Catalog
- 針對允許的標籤定義使用者可選的選項

管理員可以建立 TagOption 與產品組合和產品的關聯。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，並將其套用至佈建的產品，如下圖所示。



運用 TagOption 資料庫，您可以停用 TagOption，並保留其與產品組合或產品的關聯，然後在需要時重新加以啟動。這種方式不僅有助於維持資料庫的完整性，也可讓您針對可能是間歇性使用或只在特殊情況下使用的 TagOption，來進行管理。

您可以使用 AWS Service Catalog 主控台或 TagOptions 程式庫 API 來管理 TagOption。如需詳細資訊，請參閱 Service Catalog API 參考。

目錄

- 啟動具有 TagOption 的產品
- 管理 TagOption
- 搭配 AWS Organizations 標籤政策使用 TagOptions

啟動具有 TagOption 的產品

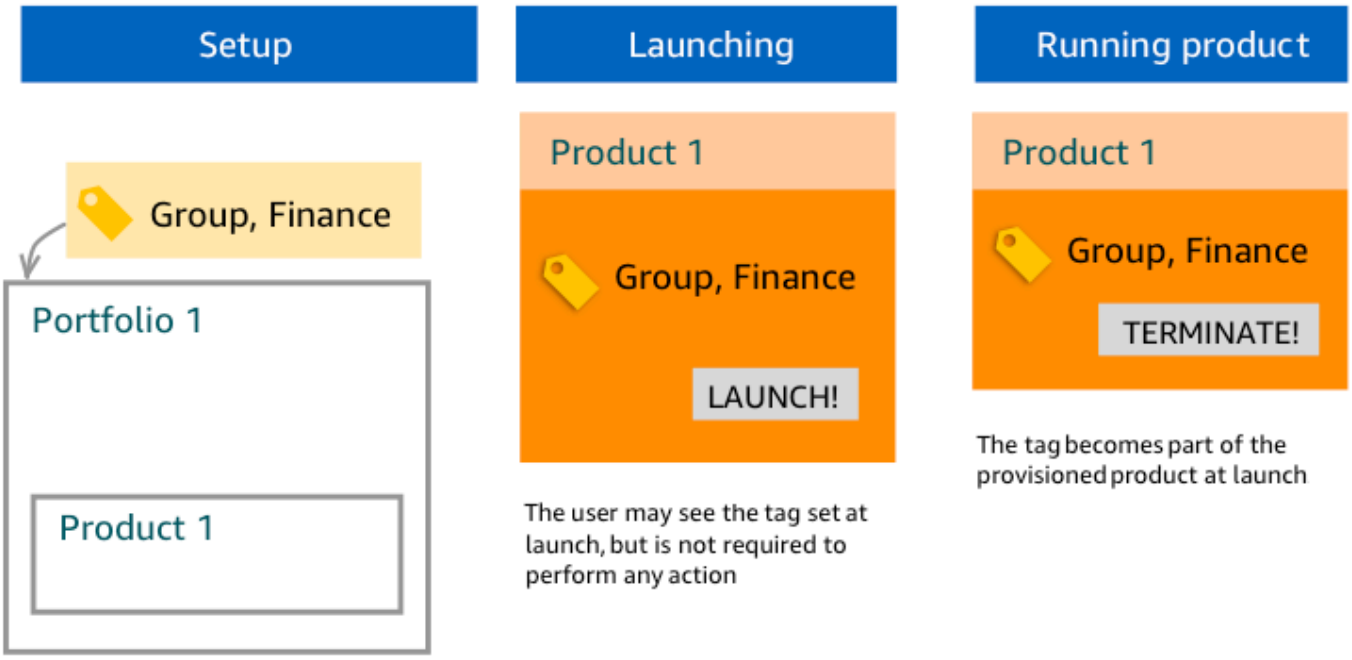
當使用者啟動具有 TagOptions 的產品時， 會代表您 AWS Service Catalog 執行下列動作：

- 收集產品所有的 TagOption 和啟動產品組合。
- 確保在佈建產品的標籤中，只使用具備唯一金鑰的 TagOption。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。

下列的使用案例示範了 TagOption 在啟動期間的運作方式。

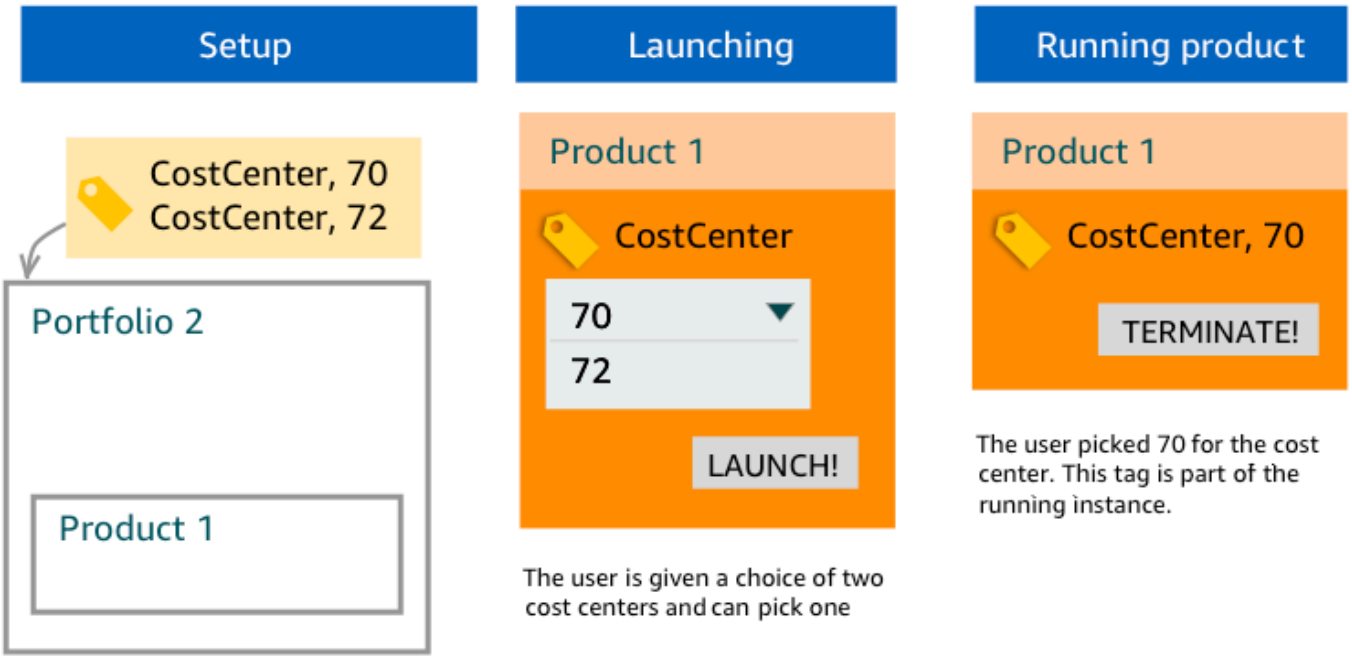
範例 1：唯一的 TagOption 金鑰

管理員建立了 TagOption[Group=Finance] (TagOption[分組=金融])，然後建立其與 Portfolio1 (產品組合 1) 的關聯，此產品組合具有 Product1 (產品 1)，而且未包含 TagOption。當使用者啟動佈建的產品時，單一的 TagOption 變成 Tag[Group=Finance] (標籤[分組=金融])，如下所示：



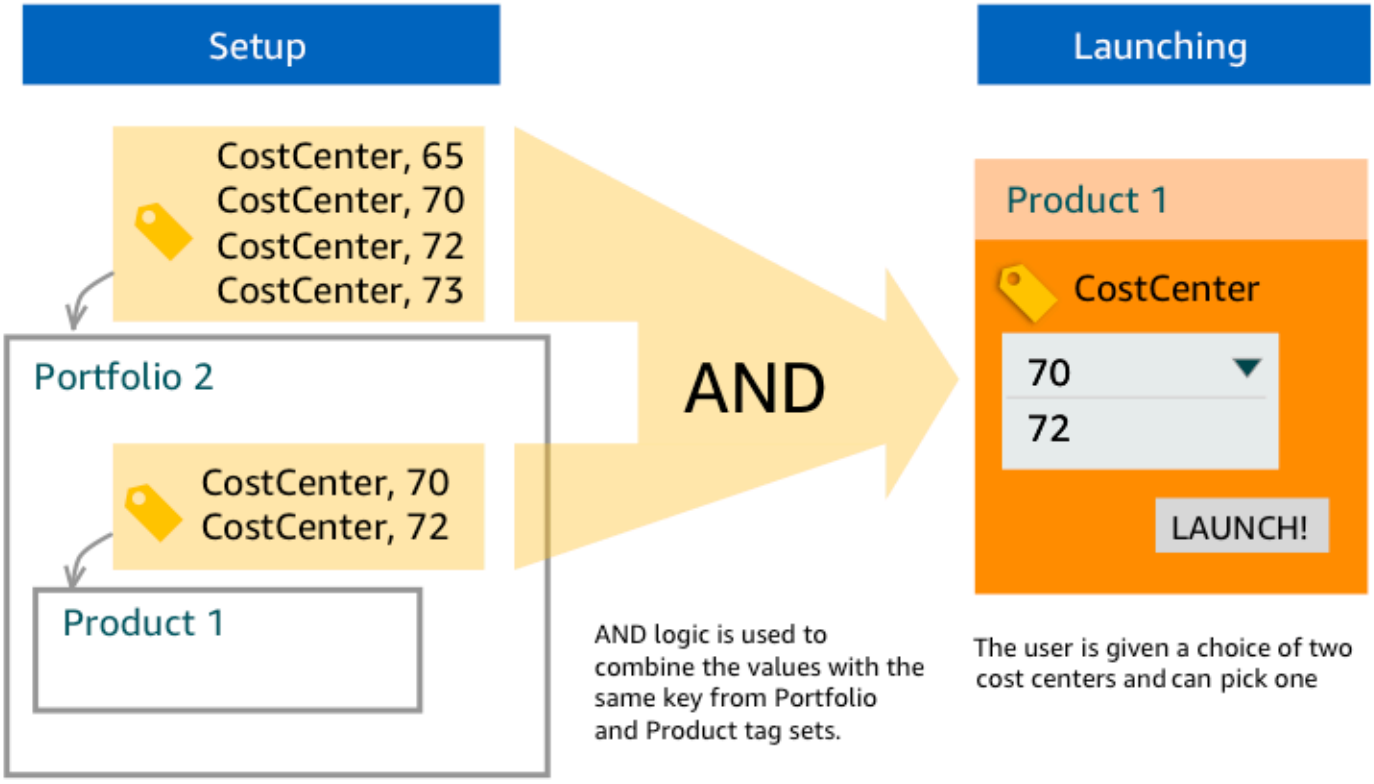
範例 2：產品組合中的一組 TagOption，具備相同的金鑰

管理員在產品組合中放置了具有相同金鑰的兩個 TagOption，而在該產品組合中的任何產品上，都沒有相同金鑰的 TagOption。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。



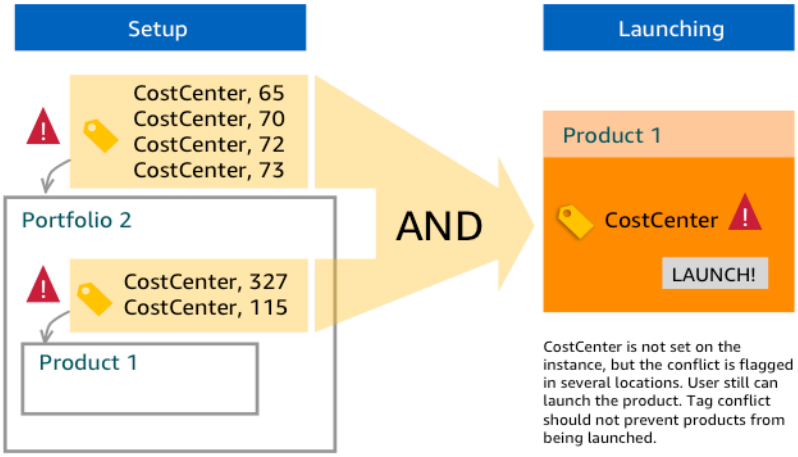
範例 3：在產品組合中以及該產品組合的產品中，皆使用了一組具備相同金鑰的 TagOption

管理員已將數個具有相同索引鍵的 TagOptions 放置在產品組合上，而且該產品組合內的產品也有數個具有相同索引鍵的 TagOptions。 會從 TagOptions 的彙總（邏輯 AND 操作）AWS Service Catalog 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：多個 TagOption 具備相同的金鑰和衝突的值

管理員已將數個具有相同索引鍵的 TagOptions 放置在產品組合上，而且該產品組合中的產品也有數個 TagOptions 具有相同索引鍵的 TagOptions。 會從 TagOptions 的彙總（邏輯 AND 操作）AWS Service Catalog 建立一組值。如果彙總找不到索引鍵的值， 會 AWS Service Catalog 建立具有相同索引鍵和 值的標籤`sc-tagconflict-`*`portfolioid`*`-`*`productid`*，其中 *`portfolioid`*和 *`productid`*是產品組合和產品的 ARNs。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 TagOption

身為管理員，您可以執行下列動作來管理 TagOptions 程式庫中的 TagOptions：

- 建立和刪除
- 啟用或停用
- 關聯或取消關聯
- 編輯

在主控台中建立 TagOptions

1. 在 https：//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 程式庫。
3. 在建立新的 TagOption 中，輸入索引鍵和值，然後選擇新增。

   建立新的 TagOption 之後，它會依索引鍵/值對分組，並在 TagOptions 清單中依字母順序排序。

   若要使用 AWS Service Catalog API 建立 TagOption，請參閱 CreateTagOption。

在主控台中刪除 TagOptions

1. 在 https：//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 程式庫，然後選擇動作。
3. 選取刪除並確認刪除。

在主控台中啟用或停用一或多個 TagOptions

1. 在 https：//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 程式庫，然後選擇動作。
3. 若要啟用，請選擇您想要的非作用中 TagOption。然後選擇動作，然後從下拉式功能表中選取啟用，然後確認您的選擇。

   若要停用，請選擇您想要的作用中 TagOption。然後選擇動作，然後從下拉式功能表中選取停用，然後確認您的選擇。

在主控台中建立或取消一或多個 TagOptions 與產品組合的關聯

1. 在 https：//https://console.aws.amazon.com/servicecatalog/ 開啟 Service Catalog 主控台。
2. 在左側導覽功能表中，選擇產品組合，然後開啟您要關聯或取消關聯的產品組合。
3. 選擇 TagOptions 索引標籤，然後選取一或多個要與產品組合建立關聯或取消關聯的 TagOptions。
4. 選擇動作。然後選取關聯或取消關聯，然後確認您的選擇。

將一或多個 TagOptions 與主控台中的產品建立關聯或取消關聯

1. 開啟 AWS Service Catalog 主控台，網址為：https：//https://console.aws.amazon.com/servicecatalog/。
2. 在左側導覽選單的管理下，選擇產品。然後開啟您要關聯或取消關聯的產品。
3. 選擇 TagOptions 索引標籤，然後選取一或多個要與產品組合建立關聯或取消關聯的 TagOptions。
4. 選擇動作。然後選取關聯或取消關聯，然後確認您的選擇。

> **Note**
>
> 若要使用 AWS Service Catalog API 將 TagOptions 與產品組合或產品建立關聯，請參閱 AssociateTagOptionWithResource。
> 若要使用 AWS Service Catalog API 移除 （取消關聯） TagOptions，請參閱 DisassociateTagOptionFromResource。

在主控台中編輯 TagOptions 的值

1. 在 https：//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 程式庫。
3. 選擇 TagOption 並開啟 值。（此值為超連結。）然後選擇 Edit (編輯)。
4. 在值欄位中，編輯值，然後選擇儲存變更。

搭配 AWS Organizations 標籤政策使用 TagOptions

本主題提供 AWS Organizations 和 TagOptions 的標籤政策的簡短概觀 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。

適用於 的 TagOptions AWS Service Catalog 適用於佈建產品 (CloudFormation 堆疊），而 AWS Organizations 適用於 AWS 的帳戶和組織單位 (OU) 或組織根目錄的標籤政策。例如，如果您將標籤政策連接到 OU，相同的標籤政策會套用至該 OU 中的所有帳戶。如果您同時使用這兩個標記功能，您應該設定它們，使其不會衝突。

標籤政策

標籤政策可讓您定義如何在帳戶中的資源上使用標籤 AWS 的規則 AWS Organizations。您可以使用標籤政策來建立和維護在帳戶層級標記 AWS 資源的一致方法。

標籤政策提供一種簡單的方法，以確保使用者套用一致的標籤、稽核標記的資源，以及維護適當的資源分類。您也可以定義標籤索引鍵的大寫方式，以及您想要允許的值。例如，您可以要求帳戶中的所有 EC2 執行個體必須將標籤金鑰設定為 ，**`CostCenter`**且該標籤的值為 **`Data Insights`**或 **`Marketing`**。

標籤政策可讓您選取選項來強制執行標記規則、防止標籤的不合規操作，以及指定強制執行適用的資源類型。如果您未選擇強制執行選項，標籤政策可讓您建立或變更不合規標籤，但在 AWS Organizations 主控台中將其報告為不合規。

如需如何設定帳戶層級標記強制執行的詳細資訊，請參閱 中的標記政策AWS Organizations。

TagOptions

TagOptions 是一種標記功能，如果已套用至相關聯的產品，則會 AWS Service Catalog 套用至 CloudFormation 堆疊層級的佈建產品。 AWS Service Catalog 會提供 TagOptions 程式庫，您可以在其中定義要與 AWS Service Catalog 產品建立關聯的鍵值對。啟動 AWS Service Catalog 產品時，您必須為與該產品組合或產品相關聯的現有 TagOption 金鑰選擇 TagOption TagOption 值，才能啟動該產品。由於您在產品組合或產品層級設定 TagOptions，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。

如需如何在 中設定 TagOptions 的詳細資訊 AWS Service Catalog，請參閱 AWS Service Catalog TagOption Library。

避免 AWS Organizations 標籤政策與 AWS Service Catalog TagOptions 之間的衝突

如果您為組織中的帳戶設定 AWS Organizations 標籤政策，建議您執行下列動作：

- 與同時管理 AWS Service Catalog 產品組合和產品的 TagOptions 的管理員共用合規標籤的需求。
- 與最終使用者共用合規標籤的需求，這些最終使用者可能會在 中啟動產品， AWS Service Catalog 並將選用的最終使用者標籤附加至其產品啟動。

假設您想要在 中啟動 AWS Service Catalog 使用 TagOption 金鑰 的產品`city`，而且您有一個標籤政策，要求 的標籤金鑰`city`具有美國城市的標籤值，例如 **`Atlanta`**、 **`San Francisco`**或 **`Austin`**。AWS Service Catalog 不允許您在沒有為產品所需的 TagOption 金鑰選取 TagOption 值的情況下啟動產品。

在這種情況下，如果您有包含南美洲城市`city`的 TagOption 金鑰的 TagOption TagOption 值，例如 **`Rio de Janeiro`**或 **`Buenos Aires`**， AWS Service Catalog 則 不會啟動產品。反之，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。

下表提供案例，說明如何解決同時使用標籤政策和 TagOptions 時可能遇到的標記衝突問題。

案例	Reason	解決方案
如果在標籤政策中檢查了標籤強制執行，產品因為標籤不合規而無法啟動。	使用尚未新增至標籤政策中合規標籤允許清單的索引鍵和值指定 TagOptions。 新增不符合標籤政策的選用自訂標籤。	如果您在標籤政策標籤索引鍵大寫強制執行中設定特定的大寫結構描述，請確定您的 TagOptions 標籤索引鍵和選用的自訂標籤索引鍵與您在標籤政策中指定的索引鍵一致。 請注意，在標籤政策中取消核取標籤索引鍵大寫強制執行方塊時，會導致所有小寫標籤索引鍵都合規，並確保您的 TagOptions 標籤索引鍵和選用的自訂標籤索引鍵與標籤政策中所需的索引鍵一致（例如全部小寫）。
由於標籤索引鍵大小寫不一致，產品無法啟動。	在與您的標籤政策大寫強制執行規則不一致的 TagOptions 金鑰中指定大寫。	正確設定標籤政策。如果您未指定標籤索引鍵大小寫合規，則預設標籤索引鍵大小寫都是小寫。

案例	Reason	解決方案
		此外，如果您未在標籤政策中指定標籤索引鍵大寫合規，請確定 中的 TagOptions 標籤索引鍵 AWS Service Catalog 都是小寫的，以符合強制執行規則。 如果您使用的標籤政策未啟用大寫合規，則該標籤政策只會將所有小寫標籤索引鍵視為合規。
由於標籤值不相容，產品無法啟動。	為不在標籤政策標籤值合規允許清單中的產品啟動選取 TagOptions 標籤值。	將 TagOptions 與您的產品和產品組合建立關聯，這些產品和產品組合符合您在清單標籤政策標籤值合規允許的標籤值中的需求。

的外部引擎 AWS Service Catalog

在 中 AWS Service Catalog，外部引擎會透過 EXTERNAL產品類型來表示。EXTERNAL 產品類型允許整合第三方佈建引擎，例如 Terraform。您可以使用外部引擎，將 Service Catalog 的功能延伸到原生 AWS CloudFormation 範本之外，以使用其他教學做為程式碼 (IaC) 工具。

EXTERNAL 產品類型可讓您使用 Service Catalog 熟悉的界面管理和部署資源，同時利用所選 IaC 工具的特定功能和語法。

若要在 Service Catalog 中啟用EXTERNAL產品類型，您必須在帳戶中定義一組標準資源。這些資源稱為 引擎。Service Catalog 在成品剖析和佈建操作中的特定點將任務委派給引擎。

佈建成品代表 Service Catalog 內產品的特定版本，可讓您管理和部署一致的資源。

當您針對EXTERNAL產品類型的佈建成品呼叫 AWS Service CatalogDescribeProvisioningArtifact 或 DescribeProvisioningParameters 操作時，Service Catalog 會在引擎中叫用 AWS Lambda 函數。這是從提供的佈建成品中擷取參數清單並將其傳回的必要項目 AWS Service Catalog。這些參數將在稍後做為佈建程序的一部分使用。

當您呼叫 ProvisionProduct 佈建EXTERNAL佈建成品時，Service Catalog 會先在內部執行一些動作，然後將訊息傳送至引擎中的 Amazon SQS 佇列。接著，引擎會擔任提供的啟動角色 （您指派給產品的 IAM 角色做為啟動限制）、根據提供的佈建成品佈建資源，以及叫用 NotifyProvisionProductEngineWorkflowResult API 來報告成功或失敗。

UpdateProvisionedProduct 和 TerminateProvisionedProduct 的呼叫處理方式類似，每個呼叫都有不同的佇列和通知 APIs：

- NotifyProvisionProductEngineWorkflowResult
- NotifyUpdateProvisionedProductEngineWorkflowResult
- NotifyTerminateProvisionedProductEngineWorkflowResult。

主題

- 考量事項
- 參數剖析
- 佈建中
- 更新中
- 終止

- 標記

考量事項

每個中樞帳戶僅限一個外部引擎

每個 Service Catalog 中樞帳戶只能使用一個EXTERNAL佈建引擎。Service Catalog 中hub-and-spoke模型允許中樞帳戶建立基準產品並共用產品組合，同時輻條帳戶匯入產品組合並利用產品。

此限制是 ，因為 EXTERNAL只能路由到帳戶中的一個引擎。如果管理員想要擁有多個外部引擎，管理員必須在不同的中樞帳戶中設定外部引擎 （ 以及產品組合和產品 ）。

外部引擎僅支援具有啟動限制的啟動角色

EXTERNAL 佈建成品僅支援使用使用啟動限制條件指定的啟動角色進行佈建。啟動限制條件會指定 Service Catalog 在最終使用者啟動、更新或終止產品時所擔任的 IAM 角色。如需啟動限制的詳細資訊，請參閱AWS Service Catalog 啟動限制。

參數剖析

EXTERNAL 佈建成品可以是任何格式。這表示建立EXTERNAL產品類型時，引擎需要從提供的佈建成品中擷取參數清單，並將其傳回 Service Catalog。這可透過在您的帳戶中建立 Lambda 函數來完成，該函數可接受下列請求格式、處理佈建成品，並傳回下列回應格式。

> **Important**
>
> Lambda 函數必須命名為 `ServiceCatalogExternalParameterParser`。

請求語法：

```
{
    "artifact": {
        "path": "string",
        "type": "string"
    },
    "launchRoleArn": "string"
}
```

欄位	類型	必要	Description
成品	object	是	要剖析之成品的詳細資訊。
成品/路徑	string	是	剖析器從中下載成品的位置。例如，對於 AWS_S3，這是 Amazon S3 URI。
成品/類型	string	是	成品類型。允許的值：AWS_S3。
launchRole	string	否	下載成品時要擔任之啟動角色的 Amazon Resource Name (ARN)。如果未提供啟動角色，則會使用 Lambda 的執行角色。

回應語法：

```
{
    "parameters": [
        {
            "key": "string"
            "defaultValue": "string",
            "type": "string",
            "description": "string",
            "isNoEcho": boolean
        },
    ]
}
```

欄位	類型	必要	Description
parameters	列出	是	Service Catalog 要求最終使用者在佈建

欄位	類型	必要	Description
			產品或更新佈建產品時提供的參數清單。如果成品中未定義參數，則會傳回空白清單。
金鑰	string	是	參數索引鍵。
defaultValue	string	否	如果最終使用者未提供值，則為 參數的預設值。
type	string	是	引擎參數值的預期類型。例如，字串、布林值或映射。允許的值專屬於每個引擎。Service Catalog 會將每個參數值以字串形式傳遞至引擎。
描述	string	否	參數的描述。建議這易於使用。
isNoEcho	布林值	編號	判斷日誌中是否未回應參數值。預設值為 false （參數值會回應）。

佈建中

對於 ProvisionProduct 操作，Service Catalog 會將資源的實際佈建委派給引擎。引擎負責連接您選擇的 IaC 解決方案 （例如 Terraform)，以佈建成品中定義的資源。引擎也負責通知 Service Catalog 結果。

Service Catalog 會將所有佈建請求傳送至您帳戶中名為 的 Amazon SQS 佇列`ServiceCatalogExternalProvisionOperationQueue`。

請求語法：

```
{
    "token": "string",
    "operation": "string",
    "provisionedProductId": "string",
    "provisionedProductName": "string",
    "productId": "string",
    "provisioningArtifactId": "string",
    "recordId": "string",
    "launchRoleArn": "string",
    "artifact": {
        "path": "string",
        "type": "string"
    },
    "identity": {
        "principal": "string",
        "awsAccountId": "string",
        "organizationId": "string"
    },
    "parameters": [
        {
            "key": "string",
            "value": "string"
        }
    ],
    "tags": [
        {
            "key": "string",
            "value": "string"
        }
    ]
}
```

欄位	類型	必要	Description
token	string	是	識別此操作的字符。權杖必須傳回 Service Catalog，以通知執行結果。

欄位	類型	必要	Description
operation	string	是	此欄位必須PROVISION_PRODUCT 用於此操作。
provisionedProductId	string	是	佈建產品的 ID。
provisionedProductName	string	是	佈建產品的名稱。
productId	string	是	產品的 ID。
provisioningArtifactId	string	是	佈建成品的 ID。
recordId	string	是	此操作的 Service Catalog 記錄 ID。
launchRoleArn	string	是	用於佈建資源之 IAM 角色的 Amazon Resource Name (ARN)。
成品	object	是	定義如何佈建資源的成品詳細資訊。
成品/路徑	string	是	引擎從中下載成品的位置。例如，對於 AWS_S3，這是 Amazon S3 URI。
成品/類型	string	是	成品類型。允許的值：AWS_S3。
身分	string	否	目前未使用 欄位。

欄位	類型	必要	Description
parameters	列出	是	使用者輸入 Service Catalog 做為此操作輸入的參數鍵值對清單。
標籤	列出	是	使用者輸入 Service Catalog 做為標籤的 key-value-pairs 清單，以套用至佈建的資源。

工作流程結果通知：

使用 API 詳細資訊頁面上指定的回應物件叫用 NotifyProvisionProductEngineWorkflowResult API。

更新中

針對 UpdateProvisionedProduct 操作，Service Catalog 會將資源的實際更新委派給引擎。引擎負責與您選擇的 IaC 解決方案 （例如 Terraform) 連接，以更新成品中定義的資源。引擎也負責通知 Service Catalog 結果。

Service Catalog 會將所有更新請求傳送至您帳戶中名為 的 Amazon SQS 佇列`ServiceCatalogExternalUpdateOperationQueue`。

請求語法：

```
{
    "token": "string",
    "operation": "string",
    "provisionedProductId": "string",
    "provisionedProductName": "string",
    "productId": "string",
    "provisioningArtifactId": "string",
    "recordId": "string",
    "launchRoleArn": "string",
    "artifact": {
        "path": "string",
```

```
        "type": "string"
    },
    "identity": {
        "principal": "string",
        "awsAccountId": "string",
        "organizationId": "string"
    },
    "parameters": [
        {
            "key": "string",
            "value": "string"
        }
    ],
    "tags": [
        {
            "key": "string",
            "value": "string"
        }
    ]
}
```

欄位	類型	必要	Description
token	string	是	識別此操作的字符。權杖必須傳回 Service Catalog，以通知執行結果。
operation	string	是	此欄位必須UPDATE_PROVISION_PRODUCT 用於此操作。
provisionedProductId	string	是	佈建產品的 ID。
provisionedProductName	string	是	佈建產品的名稱。
productId	string	是	產品的 ID。

欄位	類型	必要	Description
provisioningArtifactId	string	是	佈建成品的 ID。
recordId	string	是	此操作的 Service Catalog 記錄 ID。
launchRoleArn	string	是	用於佈建資源之 IAM 角色的 Amazon Resource Name (ARN)。
成品	object	是	定義如何佈建資源的成品詳細資訊。
成品/路徑	string	是	引擎從中下載成品的位置。例如，對於 AWS_S3，這是 Amazon S3 URI。
成品/類型	string	是	成品類型。允許的值：AWS_S3。
身分	string	否	目前未使用 欄位。
parameters	列出	是	使用者輸入 Service Catalog 做為此操作輸入的參數鍵值對清單。
標籤	列出	是	使用者輸入 Service Catalog 做為標籤的 key-value-pairs 清單，以套用至佈建的資源。

工作流程結果通知：

使用 API 詳細資訊頁面上指定的回應物件叫用 NotifyUpdateProvisionedProductEngineWorkflowResult API。

終止

對於 TerminateProvisionedProduct 操作，Service Catalog 會將實際終止的資源委派給引擎。引擎負責與您選擇的 IaC 解決方案 （ 例如 Terraform) 連接，以終止成品中定義的資源。引擎也負責通知 Service Catalog 結果。

Service Catalog 會將所有終止請求傳送至您帳戶中名為 的 Amazon SQS 佇列`ServiceCatalogExternalTerminateOperationQueue`。

請求語法：

```
{
    "token": "string",
    "operation": "string",
    "provisionedProductId": "string",
    "provisionedProductName": "string",
    "recordId": "string",
    "launchRoleArn": "string",
    "identity": {
        "principal": "string",
        "awsAccountId": "string",
        "organizationId": "string"
    }
}
```

欄位	類型	必要	Description
token	string	是	識別此操作的字符。權杖必須傳回 Service Catalog，以通知執行結果。
operation	string	是	此欄位必須`TERMINATE_PROVISIO`

欄位	類型	必要	Description
			N_PRODUCT 用於此操作。
provisionedProductId	string	是	佈建產品的 ID。
provisionedProduct Name	string	是	佈建產品的名稱。
recordId	string	是	此操作的 Service Catalog 記錄 ID。
launchRoleArn	string	是	用於佈建資源之 IAM 角色的 Amazon Resource Name (ARN)。
身分	string	否	目前未使用 欄位。

工作流程結果通知：

使用 API 詳細資訊頁面上指定的回應物件叫用 NotifyTerminateProvisionedProductEngineWorkflowResult API。

標記

若要透過資源群組管理標籤，您的啟動角色需要下列其他許可陳述式：

```
{
    "Effect": "Allow",
    "Action": [
        "resource-groups:CreateGroup",
        "resource-groups:ListGroupResources"
    ],
    "Resource": "*"
},
{
    "Effect": "Allow",
    "Action": [
```

```
        "tag:GetResources",
        "tag:GetTagKeys",
        "tag:GetTagValues",
        "tag:TagResources",
        "tag:UntagResources"
    ],
    "Resource": "*"
}
```

> **Note**
>
> 啟動角色還需要對成品中特定資源的標記許可，例如 `ec2:CreateTags`。

在 中監控 AWS Service Catalog

您可以使用 Amazon CloudWatch 來監控 AWS Service Catalog 資源，Amazon CloudWatch 會收集原始資料並將其處理 AWS Service Catalog 為可讀指標。這些統計資料會記錄兩週，讓您可以存取歷史資訊，並更清楚您的服務效能。 AWS Service Catalog 指標資料會在 1 分鐘內自動傳送至 CloudWatch。如需有關 CloudWatch 的詳細資訊，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 指標。

監控是維護 和 AWS 解決方案的可靠性、可用性 AWS Service Catalog 和效能的重要部分。您應該從 AWS 解決方案的所有部分收集監控資料，以便在發生多點失敗時更輕鬆地偵錯。開始監控之前 AWS Service Catalog，您應該建立監控計畫，其中包含下列問題的答案：

- 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 提供各種可用來監控的工具 AWS Service Catalog。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。

CloudWatch 警示會在您指定的期間內監看單一指標，並根據指標在多個期間內相對於指定閾值的值執行一或多個動作。此動作是傳送到 Amazon Simple Notification Service (Amazon SNS) 主題或 Amazon EC2 Auto Scaling 政策的通知。CloudWatch 警示不會只因處於特定狀態就調用動作，狀態必須已變更並已維持一段指定的時間。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 指標。

AWS Service Catalog CloudWatch 指標

您可以使用 Amazon CloudWatch 來監控您的 AWS Service Catalog 資源，Amazon CloudWatch 會收集原始資料並將其處理 AWS Service Catalog 為可讀指標。這些統計資料會記錄兩週，讓您可以存取歷史資訊，並更清楚您的服務效能。 AWS Service Catalog 指標資料會在 1 分鐘內自動傳送至 CloudWatch。如需有關 CloudWatch 的詳細資訊，請參閱《Amazon CloudWatch 使用者指南》。

主題

- 啟用 CloudWatch 指標
- 可用的指標與維度
- 檢視 AWS Service Catalog 指標

啟用 CloudWatch 指標

Amazon CloudWatch 指標預設為啟用。

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	Description
`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。維度會以個別記錄的形式發佈在 CloudWatch 日誌中。 單位：`Count` 有效統計資料：`Minimum`、`Maximum`、`Sum`、 `Average` 維度：`State`、`PPState`、`ProductId` 、 `ProvisioningArtifactId`
`ProductProvisioningOperation`	在產品 ID 上執行的操作數量`provisioningArtifactId` 。維度會在 CloudWatch 日誌中發佈為一筆記錄。

指標	Description
	單位：Count 有效統計資料：Minimum、Maximum、Sum、 Average 維度：State、PPState、ProductId 、 ProvisioningArtifactId

AWS Service Catalog 指標的維度

AWS Service Catalog 會將下列維度傳送至 Amazon CloudWatch。

維度	Description
PPState	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：可用、固定、錯誤
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。
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

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 資源的精細且可自訂顯示，以及服務中執行中的任務數量。

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 CloudWatch 主控台提供 AWS Service Catalog 指標的詳細檢視，您可以量身打造符合需求的檢視。如需 Amazon CloudWatch 的詳細資訊，請參閱《Amazon CloudWatch 使用者指南》。

若要在 Amazon CloudWatch 主控台中檢視指標

1. 在 https://console.aws.amazon.com/cloudwatch/ 開啟 Amazon CloudWatch 主控台。
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 記錄 AWS Service Catalog API 呼叫 AWS CloudTrail

AWS Service Catalog 已與 服務整合 AWS CloudTrail，此服務可提供使用者、角色或 AWS 服務在其中採取之動作的記錄 AWS Service Catalog。CloudTrail 會將 AWS Service Catalog 的所有 API 呼叫擷取為事件。擷取的呼叫包括來自 主控台的 AWS Service Catalog 呼叫，以及對 AWS Service Catalog API 操作的程式碼呼叫。如果您建立線索，您可以將 CloudTrail 事件持續交付至 Amazon S3 儲存貯體，包括 的事件 AWS Service Catalog。即使您未設定追蹤，依然可以透過 CloudTrail 主控台中的事件歷史記錄檢視最新事件。您可以使用 CloudTrail 所收集的資訊來判斷提出的請求 AWS Service Catalog、提出請求的 IP 地址、提出請求的人員、提出請求的時間，以及其他詳細資訊。

若要進一步了解 CloudTrail，請參閱AWS CloudTrail 《使用者指南》。

AWS Service Catalog CloudTrail 中的資訊

AWS 您的帳戶會在您建立時啟用 CloudTrail。當活動在 中發生時 AWS Service Catalog，該活動會與事件歷史記錄中的其他服務 AWS 事件一起記錄在 CloudTrail 事件中。您可以在 AWS 帳戶中檢視、搜尋和下載最近的事件。如需詳細資訊，請參閱「使用 CloudTrail 事件歷史記錄檢視事件」。

若要持續記錄您 AWS 帳戶中的事件，包括 的事件 AWS Service Catalog，請建立追蹤。線索能讓 CloudTrail 將日誌檔案交付至 Amazon S3 儲存貯體。依預設，當您在主控台中建立追蹤時，該追蹤會套用至所有的 AWS 區域。線索會記錄 AWS 分割區中所有區域的事件，並將日誌檔案傳送到您指定的 Amazon S3 儲存貯體。此外，您可以設定其他 AWS 服務，以進一步分析和處理 CloudTrail 日誌中所收集的事件資料。如需詳細資訊，請參閱下列內容：

- 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
- 從多個區域接收 AWS CloudTrail日誌檔案，以及從多個帳戶接收 AWS CloudTrail 日誌檔案

CloudTrail 會記錄所有 AWS Service Catalog 動作。例如，對 `CreatePortfolio`、`CreateProduct` 和 `UpdateProvisionedProduct` 動作發出的呼叫會在 CloudTrail 記錄檔案中產生專案。

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

- 是否使用根或 AWS Identity and Access Management (IAM) 使用者登入資料提出請求。
- 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。
- 請求是否由其他 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，能讓事件以日誌檔案的形式交付到您指定的 Amazon S3 儲存貯體。CloudTrail 日誌檔案包含一或多個日誌專案。一個事件為任何來源提出的單一請求，並包含請求動作、請求的日期和時間、請求參數等資訊。CloudTrail 日誌檔並非依公有 API 呼叫的堆疊追蹤排序，因此不會以任何特定順序出現。下列範例顯示示範 `CreateApplication` API 的 CloudTrail 日誌項目。

```
{
    "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"
}
```

主控台品牌偏好設定

AWS Service Catalog 允許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來指定公司名稱、標誌影像，以及各種網站元件的主要和次要（重點）顏色。管理員和最終使用者在使用主控台時都可看見這些品牌偏好設定。

主控台品牌偏好設定可增強帳戶的外觀，並完成下列動作：

- 在主控台和內部應用程式之間建立無縫的視覺化轉換
- 區分同一公司內不同內部團隊所使用的帳戶
- 跨多個環境區分帳戶，例如開發、預備或生產

> **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. 在左側導覽功能表中，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 支援主控台品牌的區域清單，請檢閱AWS 區域 主控台品牌支援。

AWS 區域 支援主控台品牌偏好設定

AWS Service Catalog 支援下表 AWS 區域 所列 中的主控台品牌偏好設定。

AWS 區域 名稱	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 名稱	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	
Africa (Cape Town)	af-south-1	
亞太地區 (香港)	ap-east-1	
亞太地區 (雅加達)	ap-southeast-3	
亞太區域 (孟買)	ap-south-1	
亞太地區 (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	
Europe (Paris)	eu-west-3	
歐洲 (斯德哥爾摩)	eu-north-1	
Middle East (Bahrain)	me-south-1	
南美洲 (聖保羅)	sa-east-1	

AWS 區域 名稱	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

下表說明 文件的重要變更 AWS Service Catalog。如需有關此文件更新的通知，您可以訂閱 RSS 訂閱源。

- API 版本：2014 年 11 月 12 日
- 文件最近更新時間：2024 年 5 月 16 日

變更	描述	日期
的外部引擎 AWS Service Catalog	AWS Service Catalog 新增外部引擎的新文件。外部引擎透過 EXTERNAL產品類型表示。EXTERNAL 產品類型允許整合第三方佈建引擎，例如 Terraform。您可以使用外部引擎，將 Service Catalog 的功能延伸到原生 AWS CloudFormation 範本之外，以使用其他教學做為程式碼 (IaC) 工具。如需詳細資訊，請參閱 的外部引擎 AWS Service Catalog。	2024 年 5 月 16 日
安全 IAM 更新	AWS Service Catalog 會更新AWSServiceCatalogSyncServiceRolePolicy 政策以codestar-connections 變更為 codeconnections 。如需詳細資訊，請參閱 AWS Service Catalog AppRegistry的AWS 受管政策。	2024 年 5 月 7 日

舊版更新

下表說明 2024 年 4 月 25 AWS Service Catalog 日之前的文件發行歷史記錄。

功能	Description	發行日期
AWS Service Catalog	若要了解 Hashicorp 對 Terraform 授權的變更和外部產品類型的更新，請檢閱 將現有的 Terraform Open Source 產品和佈建產品更新為外部產品類型。	2023 年 10 月 20 日
AWS Service Catalog	若要了解如何與 共用產品組合 AWS Organizations並允許 AWS Service Catalog 同步 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	若要了解如何管理 git 連線的產品 AWS Service Catalog ，並允許 將外部儲存庫中的範本同步至您的 AWS Service Catalog 產品，請參閱 AWSServiceCatalogSyncServiceRolePolicy 政策和 AWSServiceRoleForServiceCatalogSync 服務連結角色。	2022 年 11 月 18 日
AWS Service Catalog AppRegistry	若要了解 AppRegistry 如何協助存放您的 AWS 應用程式、其相關聯的資源集合和應用	2022 年 6 月 15 日

功能	Description	發行日期
	程式屬性群組，請參閱 AWS Service Catalog AppRegistry。	
AWS Service Management Connector	若要了解 Connectors for Jira Service Management 和 ServiceNow，請參閱 AWS Service Management Connector。	2022 年 6 月 9 日
適用於 Jira Service Management 的連接器	若要了解 Connector for Jira Service Management 的更新，請參閱 AWS Service Management Connector for Jira Service Management。	2021 年 5 月 25 日
Connector for ServiceNow	若要了解 Connector for ServiceNow 的更新，請參閱 AWS Service Management Connector for ServiceNow。	2021 年 4 月 7 日
Connector for ServiceNow	若要了解 Connector for ServiceNow 的更新，請參閱 AWS Service Management Connector for ServiceNow。	2020 年 9 月 24 日
AWS Service Quotas	若要了解 AWS Service Catalog 如何使用 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	若要了解 提供的架構良好的產品範本程式庫 AWS Service Catalog，請參閱 入門資源庫	2020 年 3 月 10 日

功能	Description	發行日期
版本指引	若要了解產品版本指南，請參閱版本指南。	2019 年 12 月 17 日
Jira 服務台的連接器	若要開始使用 Connector for Jira 服務台，請參閱 AWS Service Management Connector for Jira 服務台。	2019 年 11 月 21 日
Connector for ServiceNow	若要了解 Connector for ServiceNow 的更新，請參閱 AWS Service Management Connector for ServiceNow。	2019 年 11 月 18 日
新增安全性章節	若要了解 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
變更佈建的產品擁有者	若要了解如何變更佈建產品的擁有者，請參閱變更佈建產品擁有者。	2019 年 10 月 31 日
新的資源更新限制條件	若要了解如何使用 RESOURCE_UPDATE 限制條件來更新佈建產品中的標籤，請參閱AWS Service Catalog 標籤更新限制條件。	2019 年 4 月 17 日
Connector for ServiceNow	若要開始使用 Connector for ServiceNow，請參閱 AWS Service Management Connector for ServiceNow。	2019 年 3 月 19 日

功能	Description	發行日期
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
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	若要了解 Amazon CloudWatch 指標，請參閱 AWS Service CatalogAmazon CloudWatch。	2018 年 9 月 26 日
支援 TagOptions	若要管理標籤，請參閱 AWS Service Catalog TagOption Library。	2017 年 28 月 6 日
匯入一個產品組合	若要匯入從另一個 AWS 帳戶共用的產品組合，請參閱匯入產品組合。	2016 年 2 月 16 日
許可資訊更新	若要授予最終使用者主控台檢視的存取權，請參閱最終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。