



管理員指南

AWS Supply Chain



AWS Supply Chain: 管理員指南

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon 的商標和商業外觀不得用於任何非 Amazon 的產品或服務，也不能以任何可能造成客戶混淆、任何貶低或使 Amazon 名譽受損的方式使用 Amazon 的商標和商業外觀。所有其他非 Amazon 擁有的商標均為其各自擁有者的財產，這些擁有者可能附屬於 Amazon，或與 Amazon 有合作關係，亦或受到 Amazon 贊助。

Table of Contents

什麼是 AWS Supply Chain ?	1
支援的瀏覽器	1
支援的語言	1
.....	1
設定 AWS 帳戶	3
註冊 AWS 帳戶	3
建立具有管理存取權的使用者	3
要使用的先決條件 AWS Supply Chain	5
入門 AWS Supply Chain	6
步驟 1：指派 IAM Identity Center 使用者設定檔	6
步驟 2：建立執行個體	7
使用標準組態	8
使用進階組態	9
步驟 3：選擇 AWS Supply Chain 應用程式擁有者	14
登入 AWS Supply Chain Web 應用程式	15
使用 AWS Supply Chain	17
使用 AWS Supply Chain 主控台	17
更新您的設定檔	18
更新您的帳戶設定檔	18
更新您的組織設定檔	18
管理使用者許可角色	18
新增使用者	19
更新使用者許可	20
刪除使用者	20
建立自訂使用者許可角色	21
刪除執行個體	21
安全	23
資料保護	23
處理的資料 AWS Supply Chain	24
選擇退出偏好設定	24
靜態加密	24
傳輸中加密	25
金鑰管理	25
網際網路流量隱私權	25

如何在 中 使用 AWS Supply Chain 授予 AWS KMS	25
AWS PrivateLink	29
考量事項	29
建立介面端點	29
建立端點政策	30
IAM	31
目標對象	31
使用身分驗證	31
使用政策管理存取權	33
AWS Supply Chain 如何使用 IAM	34
身分型政策範例	38
疑難排解	39
AWS 受管政策	40
AWSSupplyChainFederationAdminAccess	41
政策更新	42
法規遵循驗證	43
恢復能力	44
記錄和監控 AWS 供應鏈	44
AWS Supply Chain CloudTrail 中的資料事件	45
AWS Supply Chain CloudTrail 中的 管理事件	46
Web 應用程式 APIs	46
使用 管理事件 EventBridge	52
AWS Supply Chain 事件	53
傳送 AWS Supply Chain 事件	53
事件詳細參照	54
配額	56
常見問答集 (FAQ)	58
管理支援	60
文件歷史紀錄	61
.....	lxiv

什麼是 AWS Supply Chain ?

AWS Supply Chain 是以雲端為基礎的供應鏈管理應用程式，可統一資料並提供 ML 支援的預測方法，以改善需求預測和庫存可見性。可行的洞見 內建內容協作、需求規劃、供應規劃、n 層供應商可見性、和永續性資訊管理。AWS Supply Chain 可以連線至現有的企業資源規劃 (ERP) 和供應鏈管理系統，並使用 ML 和生成式 AI 將不同的資料轉換和整合到供應鏈資料湖 (SCDL)。AWS Supply Chain 可以改善供應鏈風險管理，無需進行修改、預付授權費用或長期承諾。

主題

- [支援的瀏覽器 AWS Supply Chain](#)
- [支援的語言 AWS Supply Chain](#)

支援的瀏覽器 AWS Supply Chain

在您使用 AWS Supply Chain 之前，請使用下表確認您的瀏覽器是否受到支援。

瀏覽器	支援的版本
Google Chrome	最新三個版本。
Mozilla Firefox ESR	版本在 Firefox 的 生命週期結束日期 之前都會受到支援。有關詳細資訊，請參見 Firefox ESR 發布行事曆 。
Mozilla Firefox	最新三個版本。
Microsoft Edge 和 Edge Chromium	84 版及更新版本。
Safari	macOS 上的 Safari 10 或更新版本。

支援的語言 AWS Supply Chain

AWS Supply Chain 支援下列語言：

- 英文 (美國)
- 英文 (英國)

- 德文
- 西班牙文
- 法文
- 義大利文
- 葡萄牙文
- 簡體中文
- 繁體中文
- 日文
- 韓文

設定 AWS 帳戶

使用本節來建立 AWS 帳戶和建立 IAM 使用者。如需建立 AWS 帳戶的最佳實務資訊，請參閱[建立您的最佳實務 AWS 環境](#)。

主題

- [註冊 AWS 帳戶](#)
- [建立具有管理存取權的使用者](#)

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](#)。

要使用的先決條件 AWS Supply Chain

建立 AWS Supply Chain 執行個體之前，請務必完成下列步驟：

- 您有 AWS 帳戶。若要建立 AWS 帳戶，請參閱 [設定 AWS 帳戶](#)。
- 確定已啟用 IAM Identity Center。若要啟用 IAM Identity Center，請參閱 [啟用 IAM Identity Center](#)。
- 您有必要的管理許可。如需許可的詳細資訊，請參閱進階組態。
- IAM Identity Center 執行個體必須在您要建立 AWS Supply Chain 執行個體的相同區域中啟用。AWS Supply Chain 僅在美國東部（維吉尼亞北部）、美國西部（奧勒岡）、歐洲（法蘭克福）、亞太區域（雪梨）和歐洲（愛爾蘭）區域支援。

如果 AWS Supply Chain 執行個體不在與 IAM Identity Center 區域相同的區域中，[請聯絡我們](#)以取得進一步協助。

- 您必須在 IAM Identity Center 執行個體中至少有一個使用者，才能指派做為 AWS Supply Chain 管理員。您可以將作用中目錄連線至 IAM Identity Center。如需詳細資訊，請參閱 [連線至 Microsoft AD 目錄](#)。
- 新增需要存取 AWS Supply Chain IAM Identity Center 的任何其他使用者。
- 您需要 AWS Key Management Service (AWS KMS) 來建立執行個體。AWS Supply Chain 使用此執行個體 AWS KMS key 來加密所有傳入的資料 AWS Supply Chain。如需 AWS KMS 金鑰的相關資訊，請參閱 [建立金鑰](#)。

入門 AWS Supply Chain

在本節中，您可以學習建立 AWS Supply Chain 執行個體、授予使用者許可角色、登入 AWS Supply Chain Web 應用程式，以及建立自訂使用者許可角色。最多 AWS 帳戶 可以有 10 個 AWS Supply Chain 執行個體處於作用中或初始化狀態。

主題

- [步驟 1：指派 IAM Identity Center 使用者設定檔](#)
- [步驟 2：建立執行個體](#)
- [步驟 3：選擇 AWS Supply Chain 應用程式擁有者](#)
- [登入 AWS Supply Chain Web 應用程式](#)

步驟 1：指派 IAM Identity Center 使用者設定檔

若要建立執行個體並使用 AWS Supply Chain 服務，您需要連接現有的 IAM Identity Center 使用者設定檔或建立新的設定檔。

1. 開啟 [AWS Supply Chain 主控台](#)。您也可以從主要 搜尋 "AWS Supply Chain" AWS 管理主控台。
2. 如有必要，AWS 請選取主控台頂端的選取區域來變更區域。從下拉式清單中選擇您的區域。
3. 選取建立 AWS Supply Chain 執行個體。隨即顯示通知。

Continue with email



We'll check if you have an existing user and help create one if you don't.

AWS Supply Chain

Email address

Continue

4. 輸入您的電子郵件地址，然後選取繼續。IdC 將驗證電子郵件是否符合現有的使用者。
5. 執行以下任意一項：
 - 如果 IdC 將電子郵件地址與使用者相符 – 選取連接您的身分來源並加入您的團隊。

Note

如果您的組織具有您要用於的已建立 IdC 執行個體，則可以使用此功能 AWS Supply Chain。

- 如果 IdC 找不到與現有使用者的相符項目 – 即會顯示建立新使用者通知。繼續下一個步驟。
6. 在通知中，輸入以下內容，然後選取繼續：
- 電子郵件地址
 - 名字
 - 姓氏

IdC 會自動建立使用者，並將其新增為 AWS Supply Chain 管理員。

7. 執行以下任意一項：
- 若要使用標準組態建立執行個體 – 選取建立。請參閱 [the section called “使用標準組態”](#)。
 - 若要使用自訂組態建立執行個體 – 在進階設定中選取編輯。請參閱 [the section called “使用進階組態”](#)。

步驟 2：建立執行個體

在中建立執行個體會 AWS Supply Chain 建立專用環境，以進行供應鏈管理和分析。若要設定執行個體，您可以設定基本詳細資訊、建立設定，以及定義初始使用者存取許可。

Note

只有 AWS 管理主控台 管理員可以建立執行個體。建立 AWS Supply Chain 執行個體的 AWS 管理主控台 管理員應擁有 下列出的所有許可 [使用 AWS Supply Chain](#)。此管理員應邀請 IAM 使用者做為 AWS Supply Chain 管理員來管理 AWS Supply Chain。

您可以使用兩種方法之一建立執行個體：標準組態或進階組態。標準組態使用自動化程序，以使用預設參數快速建立執行個體。進階組態可讓您透過設定自己的參數來自訂執行個體。

主題

- [使用標準組態](#)

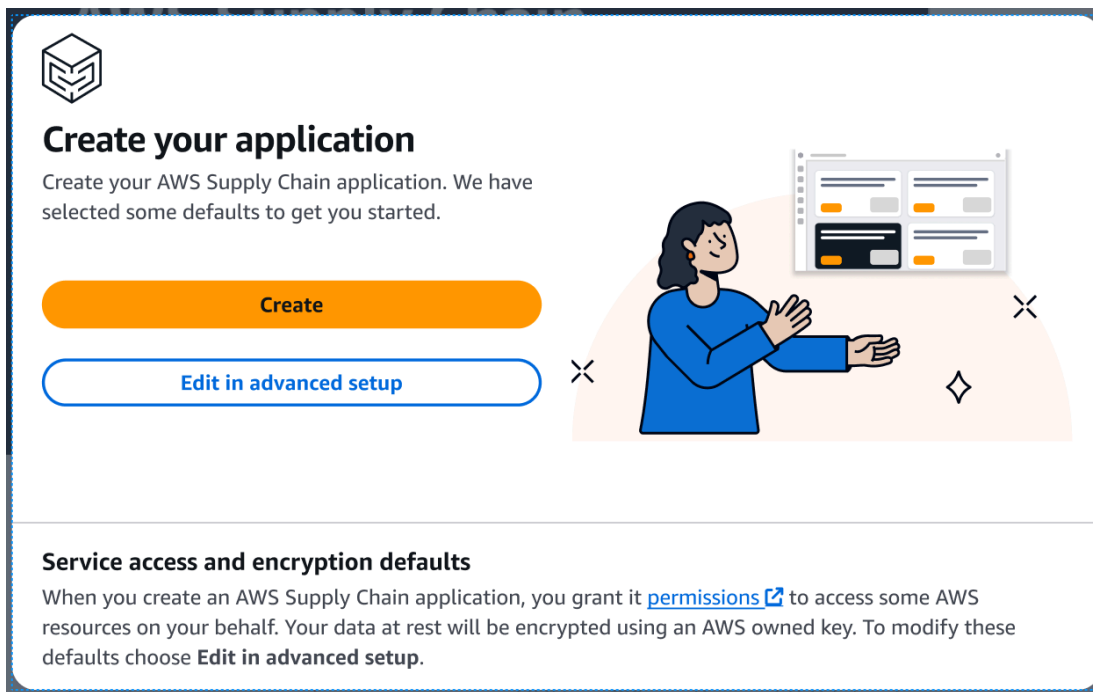
- [使用進階組態](#)

使用標準組態

標準組態會使用預設的安全性和加密設定來建立 AWS Supply Chain 執行個體。執行個體在 AWS 地理區域中運作。如需區域的詳細資訊，請參閱《IAM 使用者指南》中的 [區域和端點](#)，以及《》中的 [區域端點](#) AWS 一般參考。

若要使用預設參數的標準組態建立 AWS Supply Chain 執行個體，請遵循下列步驟。

1. 選取建立。



Create your application

Create your AWS Supply Chain application. We have selected some defaults to get you started.

[Create](#)

[Edit in advanced setup](#)

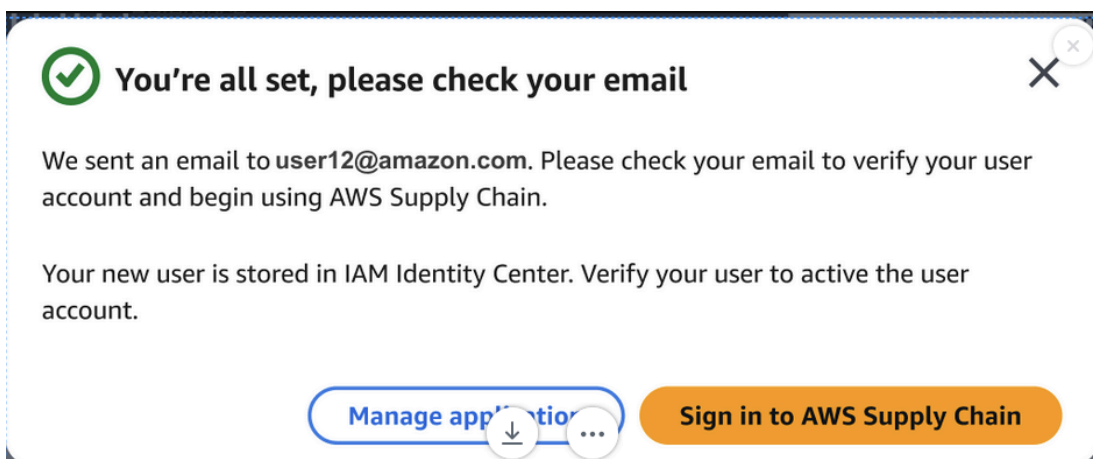
Service access and encryption defaults

When you create an AWS Supply Chain application, you grant it [permissions](#) to access some AWS resources on your behalf. Your data at rest will be encrypted using an AWS owned key. To modify these defaults choose [Edit in advanced setup](#).

[Manage application](#)

[Sign in to AWS Supply Chain](#)

確認隨即出現。



You're all set, please check your email

We sent an email to user12@amazon.com. Please check your email to verify your user account and begin using AWS Supply Chain.

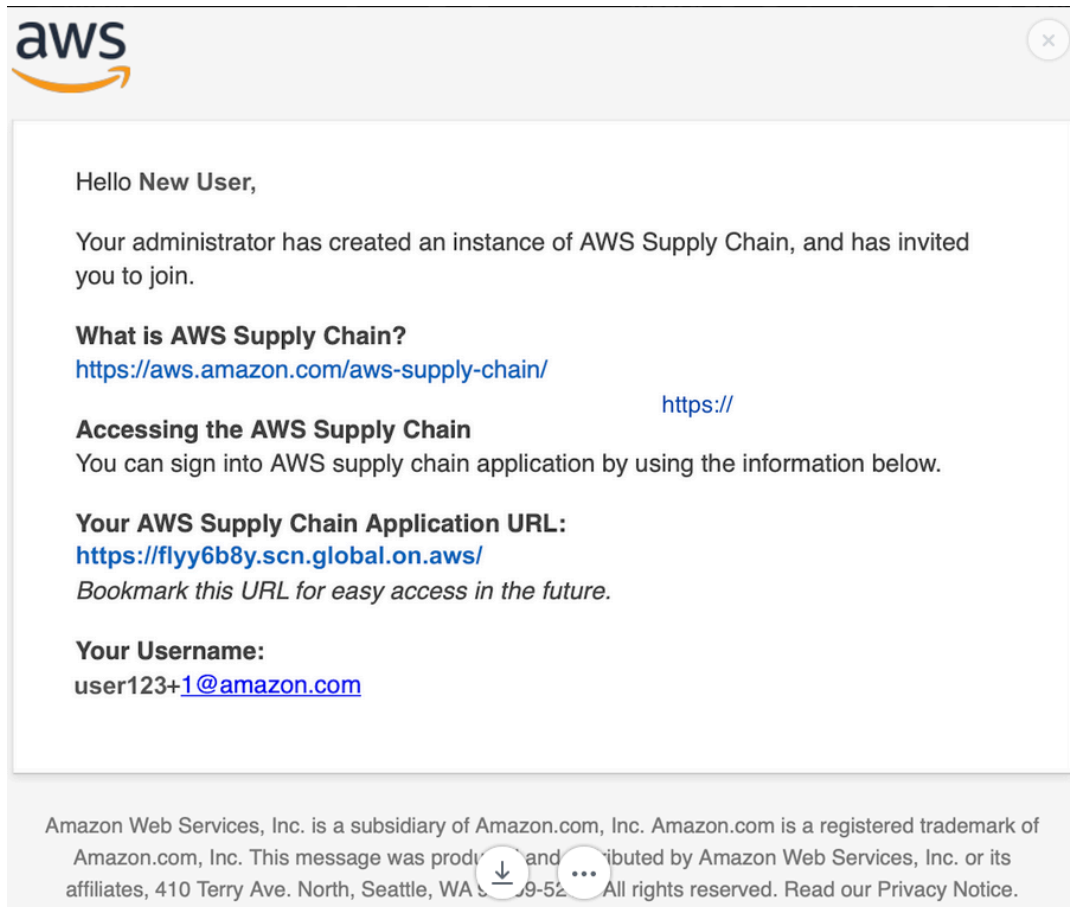
Your new user is stored in IAM Identity Center. Verify your user to activate the user account.

[Manage application](#)

[Sign in to AWS Supply Chain](#)

2. 檢查您的電子郵件是否有下列項目：

- 來自 IdC 團隊的電子郵件。
- Identity Management 團隊的電子郵件。

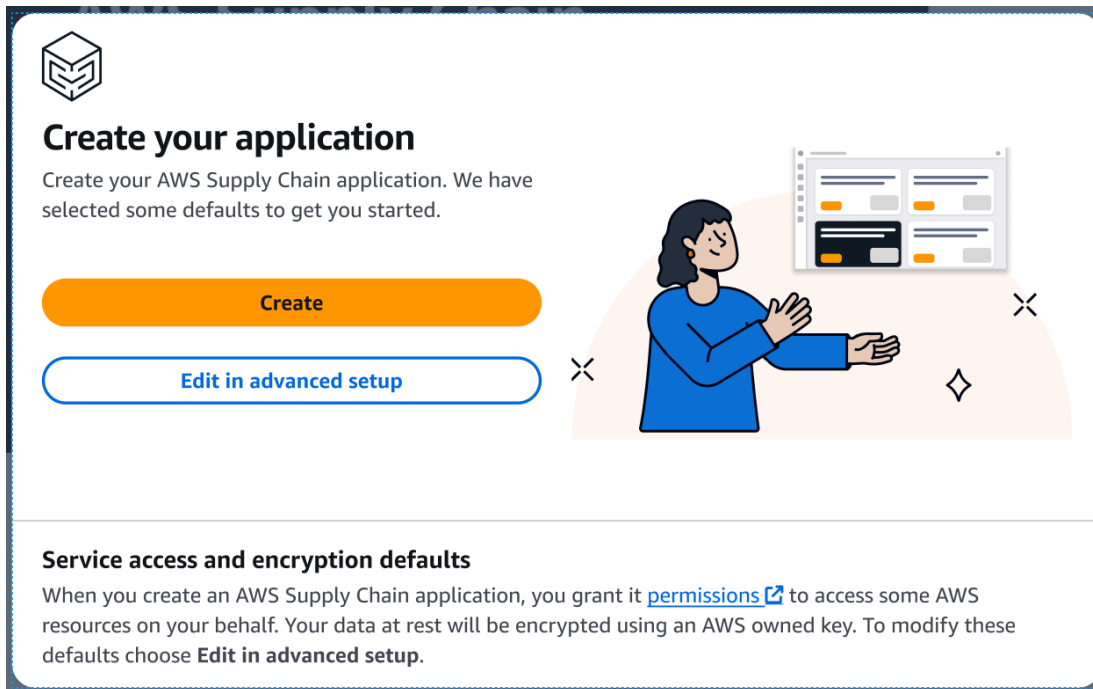


3. 收到邀請電子郵件後，請登入 AWS Supply Chain。請參閱 [the section called “登入 AWS Supply Chain Web 應用程式”](#)。

使用進階組態

進階組態可讓您透過設定自己的參數來自訂執行個體。若要使用預設參數的進階組態建立 AWS Supply Chain 執行個體，請遵循下列步驟。

1. 在進階設定中選取編輯。



Create your application

Create your AWS Supply Chain application. We have selected some defaults to get you started.

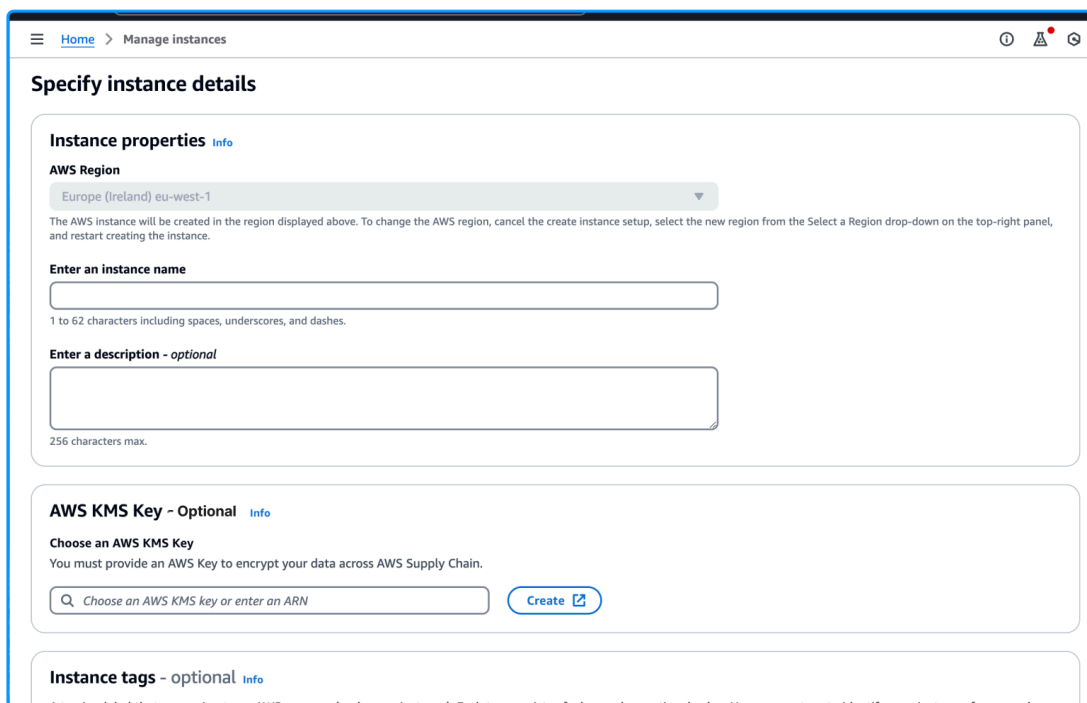
Create

Edit in advanced setup

Service access and encryption defaults

When you create an AWS Supply Chain application, you grant it [permissions](#) to access some AWS resources on your behalf. Your data at rest will be encrypted using an AWS owned key. To modify these defaults choose **Edit in advanced setup**.

執行個體屬性頁面隨即出現。



Home > Manage instances

Specify instance details

Instance properties [Info](#)

AWS Region

Europe (Ireland) eu-west-1

The AWS instance will be created in the region displayed above. To change the AWS region, cancel the create instance setup, select the new region from the Select a Region drop-down on the top-right panel, and restart creating the instance.

Enter an instance name

1 to 62 characters including spaces, underscores, and dashes.

Enter a description - optional

256 characters max.

AWS KMS Key - Optional [Info](#)

Choose an AWS KMS Key

You must provide an AWS Key to encrypt your data across AWS Supply Chain.

Create


Instance tags - optional [Info](#)

A key-value label that you assign to an AWS resource (such as an instance). Each tag consists of a key and an optional value. You can use tags to identify your instances, for example,

2. 在執行個體屬性頁面上輸入以下內容：


- 名稱 – 輸入執行個體名稱。
- 描述 – 輸入 AWS Supply Chain 執行個體的描述（例如生產執行個體、測試執行個體等）。

- AWS KMS 金鑰（選用）– 您可以選擇使用預設 AWS KMS 金鑰（建議）或提供您自己的 AWS KMS 金鑰。如需詳細資訊，請參閱[the section called “使用自訂 AWS KMS 金鑰”](#)。
- 執行個體標籤 – 您可以將標籤新增至執行個體，以用於識別。例如，您可以新增標籤來定義您要建立的執行個體類型（例如生產、測試、UTA 等）。

 Note

如果您計劃使用 S/4 Hana 資料連線，請確定您提供的 AWS KMS 金鑰具有具有相關聯值為的 `aws-supply-chain-access` 標籤 `true`。

3. 選取建立執行個體。
4. （選用）建立 AWS Supply Chain 執行個體後，如果您選擇在 AWS KMS 金鑰下使用自己的 AWS KMS 金鑰，請更新 KMS 政策以允許 AWS Supply Chain 存取您的 AWS KMS 金鑰。

 Note

以您的 和執行個體 ID 取代 *YourAccountNumber* AWS 帳戶 和 *YourInstanceID*。
AWS Supply Chain

```
{  
  
  "Sid": "Allow AWS Supply Chain to access the AWS KMS Key",  
  "Effect": "Allow",  
  "Principal": {  
    "AWS": "arn:aws:iam::YourAccountNumber:role/service-role/scn-instance-  
role-YourInstanceID"  
  },  
  "Action": [  
    "kms:Encrypt",  
    "kms:Decrypt",  
    "kms:GenerateDataKey"  
  ],  
  "Resource": "*"   
}
```

使用自訂 AWS KMS 金鑰

您可以在建立執行個體時使用自己的 AWS KMS 金鑰。如果您想要管理自己的金鑰，但不想使用現有的金鑰，您可以建立新的金鑰。

Note

使用 AWS 擁有的金鑰是 AWS Supply Chain 執行個體的建議預設設定。

使用現有的 AWS KMS 金鑰

1. 選擇自訂加密設定。
2. 前往選擇 AWS KMS 金鑰。
3. 在提供的欄位中輸入您的金鑰。
4. 選取 Update (更新)。

建立 AWS KMS 金鑰

1. 選取建立。
2. 請遵循[建立 KMS 金鑰](#)中的步驟。
3. 使用下列許可更新新金鑰。
 - 定義金鑰管理許可：保持未核取狀態
 - 定義金鑰使用許可：保持未核取狀態
 - 更新金鑰政策：編輯金鑰政策並取代為：
JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Enable IAM User Permissions",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:root"
      },
      "Action": "kms:*",
```

```

        "Resource": "*"
    },
    {
        "Sid": "Allow access through SecretManager for all principals
in the account that are authorized to use SecretManager",
        "Effect": "Allow",
        "Principal": {
            "AWS": "*"
        },
        "Action": [
            "kms:Encrypt",
            "kms:Decrypt",
            "kms:ReEncrypt*",
            "kms:GenerateDataKey*",
            "kms:CreateGrant",
            "kms:DescribeKey",
            "kms:GenerateDataKeyWithoutPlaintext",
            "kms:ReEncryptFrom",
            "kms:ReEncryptTo"
        ],
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "kms:ViaService": "secretsmanager.us-
east-1.amazonaws.com",
                "kms:CallerAccount": "YourAccountNumber"
            }
        }
    },
    {
        "Sid": "Allow AWS Supply Chain to access the AWS KMS Key",
        "Effect": "Allow",
        "Principal": {
            "Service": "scn.Region.amazonaws.com"
        },
        "Action": [
            "kms:Encrypt",
            "kms:GenerateDataKeyWithoutPlaintext",
            "kms:ReEncryptFrom",
            "kms:ReEncryptTo",
            "kms:Decrypt",
            "kms:GenerateDataKey",
            "kms:DescribeKey",
            "kms:CreateGrant",

```

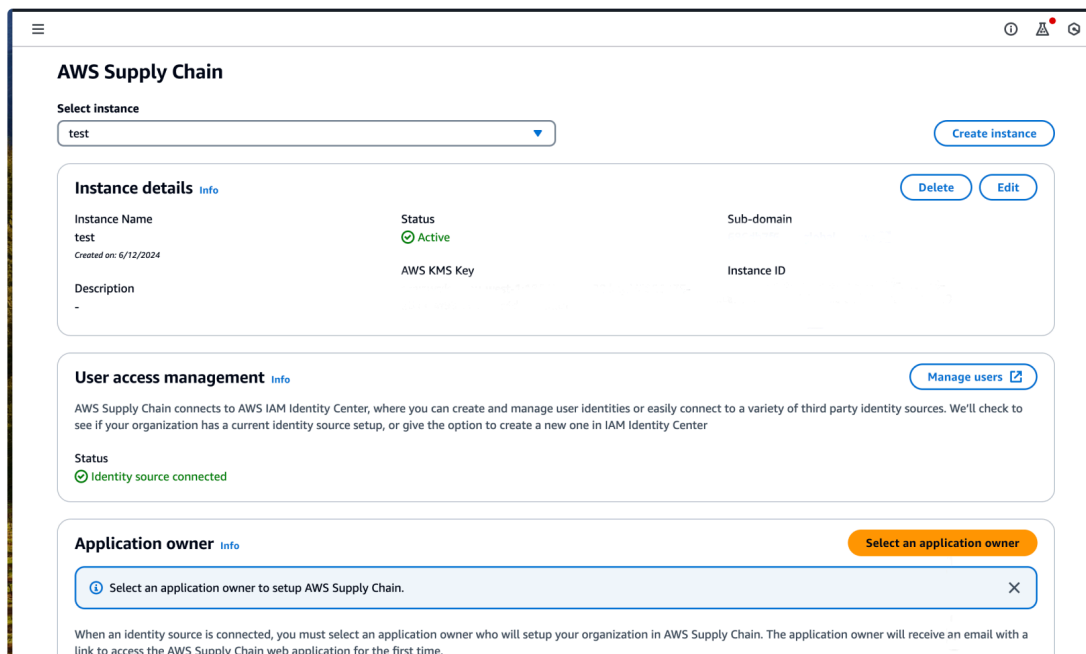
```
        "kms:RetireGrant"
      ],
      "Resource": "*"
    }
  ]
}
```

步驟 3：選擇 AWS Supply Chain 應用程式擁有者

身為 AWS 主控台管理員，您可以選擇 AWS Supply Chain 應用程式擁有者來管理 AWS Supply Chain Web 應用程式存取。AWS Supply Chain 應用程式擁有者可以新增或移除 AWS Supply Chain Web 應用程式的使用者許可角色。

建立執行個體並連接身分來源後，請依照下列步驟選擇 AWS Supply Chain 應用程式擁有者。

1. 開啟 AWS Supply Chain 主控台儀表板。
2. 前往選取應用程式擁有者，然後選取要成為 AWS Supply Chain 應用程式擁有者的使用者。搜尋結果只會顯示符合搜尋條件的使用者。

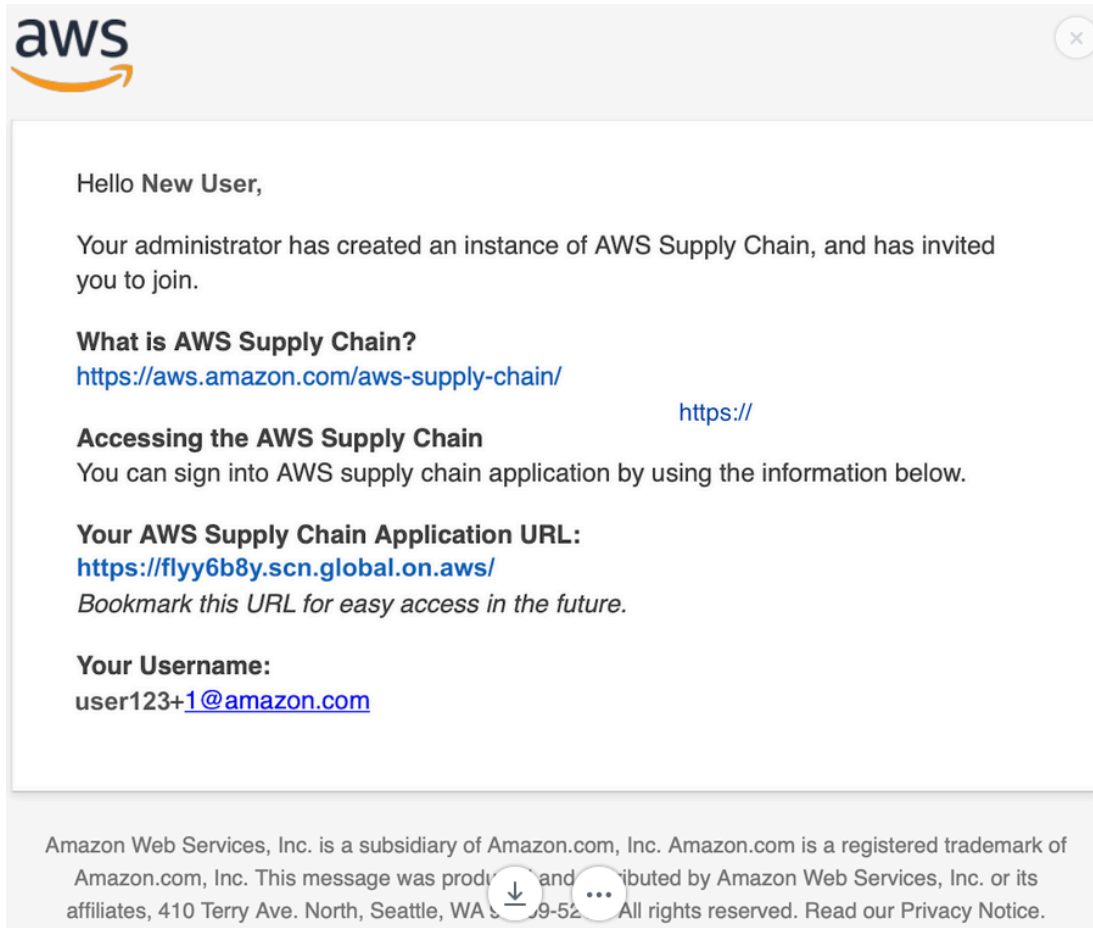


3. (選用) 選擇前往 IAM Identity Center 以新增更多使用者。如需新增使用者的詳細資訊，請參閱 AWS IAM Identity Center 使用者指南中的 [管理您的身分來源](#)，如需使用者許可角色的詳細資訊，請參閱 [使用者許可角色](#)。

Note

您一次只能從 AWS Supply Chain 主控台新增一個使用者。您無法將群組新增為其中的應用程式擁有者 AWS Supply Chain。

4. 選擇傳送邀請。一封電子郵件會傳送給 Web 應用程式管理員。一旦 Web 應用程式管理員收到邀請電子郵件，他們將能夠選取應用程式 URL 並登入 AWS Supply Chain。



在 AWS Supply Chain 主控台儀表板上，您會看到應用程式擁有者下列出的使用者。

選擇在 AWS Supply Chain 中管理，以在 AWS Supply Chain Web 應用程式中新增和移除使用者


登入 AWS Supply Chain Web 應用程式

身為 AWS Supply Chain 管理員，您應該已收到 AWS Supply Chain Web 應用程式的電子郵件邀請。

1. 您可以在電子郵件 AWS Supply Chain 或主控台儀表板中選擇連結，在子網域下，選擇 Web URL。

AWS Supply Chain Web 應用程式登入頁面隨即出現。

2. 輸入 AWS IAM Identity Center 使用者登入資料，然後選擇登入。

 Note

當您第一次登入時，系統只會要求您完成帳戶和組織的設定檔。

3. 在完成設定檔頁面上，輸入您的任務標題和時區。選擇下一步。
4. 在讓我們新增您的組織資訊頁面上，輸入組織名稱，然後選擇總部位置。或者，您可以新增公司標誌。選擇下一步。
5. 在設定團隊成員頁面上 AWS Supply Chain，選取您要存取 AWS Supply Chain Web 應用程式的使用者。選擇 Invite Users (邀請使用者)。如需 AWS Supply Chain 使用者許可角色的資訊，請參閱 [管理使用者許可角色](#)。
6. 如果稍後想要新增使用者，您可以選擇立即略過。

加入完成頁面隨即出現。

7. 您新增的每個使用者都會收到電子郵件訊息，其中包含前往的連結 AWS Supply Chain，或者您可以選擇複製連結並將連結傳送給使用者。
8. 選擇繼續前往首頁以檢視 AWS Supply Chain 儀表板。

使用 AWS Supply Chain

AWS Supply Chain 是以雲端為基礎的應用程式，可協助您了解供應鏈網路、快速做出明智的決策，並改善供應鏈彈性。使用 AWS Supply Chain，您可以連接不同的資料來源、使用機器學習產生洞見，以及與內部團隊和外部合作夥伴協作。本節將引導您完成一些 AWS Supply Chain 基本函數。

主題

- [使用 AWS Supply Chain 主控台](#)
- [更新您的設定檔](#)
- [管理使用者許可角色](#)
- [刪除執行個體](#)

使用 AWS Supply Chain 主控台

使用 主控台是管理服務資源和組態的最簡單方式。主控台提供直覺式的 Web 型界面，您可以在其中檢視、建立、修改和監控您的 資源。本節說明如何存取和導覽主控台，以執行常見的管理任務。

Note

如果 AWS 您的帳戶是 AWS 組織的成員帳戶，並包含服務控制政策 (SCP)，請確定組織的 SCP 將下列許可授予該成員帳戶。如果組織的 SCP 政策未包含下列許可，AWS Supply Chain 執行個體建立將會失敗。

若要存取 AWS Supply Chain 主控台，您必須擁有一組最低的許可。這些許可必須允許您列出和檢視中 AWS Supply Chain 資源的詳細資訊 AWS 帳戶。如果您建立比最基本必要許可更嚴格的身分型政策，則對於具有該政策的實體 (使用者或角色) 而言，主控台就無法如預期運作。

對於僅呼叫 AWS CLI 或 AWS API 的使用者，您不需要允許最低主控台許可。反之，只需允許存取符合他們嘗試執行之 API 操作的動作就可以了。

主控台管理員需要下列許可，才能成功建立和更新 AWS Supply Chain 執行個體。

JSON

`key_arn` 指定您想要用於 AWS Supply Chain 執行個體的金鑰。如需最佳實務和限制僅存取您想要使用的金鑰 AWS Supply Chain，請參閱在 [IAM 政策陳述式中指定 KMS 金鑰](#)。若要代表所有 KMS 金鑰，請單獨使用萬用字元 ("*")。

更新您的設定檔

您可以隨時在 AWS Supply Chain Web 應用程式上更新您的帳戶和組織設定檔。

更新您的帳戶設定檔

若要更新您的帳戶設定檔，請遵循下列步驟。

1. 在 AWS Supply Chain Web 應用程式儀表板的左側導覽窗格中，選擇設定圖示。
2. 選擇帳戶設定檔。

帳戶設定檔頁面隨即出現。

3. 更新帳戶資訊，然後選擇儲存。

更新您的組織設定檔

若要更新組織設定檔，請遵循下列步驟。

1. 在 AWS Supply Chain Web 應用程式儀表板的左側導覽窗格中，選擇設定圖示。
2. 選擇組織，然後選擇組織設定檔。

組織設定檔頁面隨即出現。

3. 更新組織標誌或總部位置，然後選擇儲存。

管理使用者許可角色

身為 AWS Supply Chain 管理員，您可以使用預設使用者許可角色或建立自訂許可角色。AWS Supply Chain 具有下列預設使用者許可角色：

- 管理員 – 建立、檢視和管理所有資料和使用者許可的存取權。
- 資料分析師 – 建立、檢視和管理所有資料連線的存取權。
- 庫存管理員 – 建立、檢視和管理 Insights 的存取權。

- 需求規劃工具 – 建立、檢視和管理預測、覆寫和發佈需求計畫的存取權。
- 合作夥伴資料管理員 – 存取以管理和檢視合作夥伴、管理和檢視資料請求，以及檢視永續性資料。
- 供應規劃工具 – 管理和檢視供應計畫的存取權。

Note

身為 AWS Supply Chain 管理員，在新增使用者之前，請注意下列事項：

- 每個預設使用者許可角色都定義一組許可。您可以將使用者新增至預設使用者許可角色，或建立自訂許可角色。
- 一個使用者只能指派給一個使用者許可角色。
- 您無法編輯或刪除預設使用者許可角色。
- 當您編輯您建立的自訂許可角色時，會更新自訂許可角色下所有使用者的許可。
- 當您刪除您建立的自訂許可角色時，自訂許可角色下的所有使用者都將失去存取權 AWS Supply Chain。
- 不支援在 中新增群組 AWS Supply Chain。

主題

- [新增使用者](#)
- [更新使用者許可](#)
- [刪除使用者](#)
- [建立自訂使用者許可角色](#)

新增使用者

身為 AWS Supply Chain 管理員，您可以新增使用者來存取 AWS Supply Chain Web 應用程式。使用者必須先新增至 IAM Identity Center (IdC)，然後才能新增至其中 AWS Supply Chain。如需將使用者新增至 IdC 的詳細資訊，請參閱[指派使用者存取權](#)。

將使用者新增至 IdC 後，請依照下列步驟新增使用者。

1. 選擇 AWS Supply Chain 儀表板上的設定圖示。
2. 選取使用者和許可。

3. 選取使用者、使用者。管理使用者頁面隨即出現。
4. 選取新增使用者。新增使用者頁面隨即出現。
5. 從新增使用者（們）下拉式功能表中選取使用者。
6. 從選取角色下拉式功能表下的 中選取使用者的角色。
7. 選取新增。

更新使用者許可

若要更新目前使用者 AWS Supply Chain 的使用者許可角色，請遵循下列步驟。

1. 在 AWS Supply Chain 儀表板的左側導覽窗格中，選擇設定圖示。
2. 選擇許可，然後選擇使用者。

管理使用者頁面隨即出現。

3. 在管理使用者頁面上，選取要更新其使用者許可角色的使用者或群組，然後從許可角色下拉式功能表中選取其中一個許可角色。

Note

視您指派的角色許可而定，儀表板 AWS Supply Chain 會自訂。如需詳細資訊，請參閱[建立自訂使用者許可角色](#)。

4. 選擇 Save (儲存)。

刪除使用者

身為 AWS Supply Chain 管理員，您可以從 AWS Supply Chain Web 應用程式刪除使用者。請依照下列步驟刪除使用者。

1. 在 AWS Supply Chain 儀表板的左側導覽窗格中，選擇設定圖示。
2. 選擇許可，然後選擇使用者。

管理使用者頁面隨即出現。

3. 在管理使用者頁面上，選取您要刪除的使用者，然後選擇刪除圖示。

建立自訂使用者許可角色

除了預設的使用者許可角色之外，您還可以建立自訂使用者許可角色，以包含多個許可角色，並新增特定位置和產品。請依照下列步驟建立新的許可角色。

1. 在 AWS Supply Chain 儀表板的左側導覽窗格中，選擇設定圖示。選擇許可，然後選擇許可角色。

許可角色頁面隨即出現。

2. 選擇 Create New Role (建立新角色)。
3. 在管理許可角色頁面的角色名稱下，輸入名稱。
4. 移動滑桿以選取使用者許可角色。
 - 管理 – 指派具有管理許可的使用者可以新增、編輯和管理資訊。
 - 檢視 – 指派具有檢視許可的使用者只能檢視目前資訊。

5.  Note

如果您的執行個體連接到資料來源，您只能選擇位置存取和產品存取下的產品和位置。例如，您可以建立自訂的 Admin 使用者，只用來管理西雅圖位置的 avocados，也可以建立 Insight 使用者，只用來管理西雅圖位置的 avocados 洞見。

在位置存取下，搜尋您在搜尋列中輸入的區域，然後選取區域。

6. 在產品存取下，在您於搜尋列中輸入時搜尋產品，然後選取產品。
7. 選擇儲存。

刪除執行個體

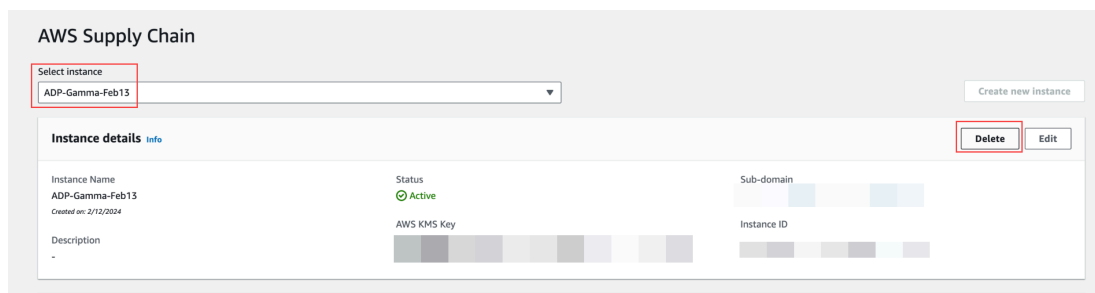
若要刪除執行個體，請遵循下列步驟。

Note

當您刪除執行個體時，不會自動刪除 Amazon S3 儲存貯體中的資訊。

1. 在開啟 AWS Supply Chain 主控台 <https://console.aws.amazon.com/scn/home>。

- 在 AWS Supply Chain 主控台儀表板的下拉式清單中，選取您要刪除的執行個體。



- 選擇 刪除。
- 在刪除 AWS Supply Chain 執行個體頁面的確認下，輸入 **delete**以確認您要刪除執行個體。
- 選擇 刪除。執行個體刪除開始，一旦刪除執行個體，您會看到確認訊息。

Note

刪除執行個體後，AWS Supply Chain 會自動刪除與 Amazon Q in 相關的資訊。

中的安全性 AWS Supply Chain

的雲端安全 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，這些架構是為滿足最安全敏感組織的需求而 AWS 建置的。

安全性是您和 之間的共同責任 AWS。[共同責任模型](#)將此描述為雲端安全性和雲端安全性：

- 雲端的安全性 – AWS 負責保護在 AWS 服務 中執行的基礎設施 AWS 雲端。AWS 也為您提供可安全使用的服務。在 [AWS 合規計劃](#) 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 Supply Chain，請參閱[AWS 合規計劃範圍內的服務](#)。
- 雲端安全性 – 您使用 AWS 服務 的 決定您的責任。您也必須負責其他因素。包括資料的敏感度、您的要求，以及適用的法律和法規。

本文件可協助您了解如何在使用 時套用共同責任模型 AWS Supply Chain。下列主題說明如何設定 AWS Supply Chain 以符合您的安全和合規目標。您也會了解如何使用其他 AWS 服務 來協助您監控和保護 AWS Supply Chain 資源。

主題

- [中的資料保護 AWS Supply Chain](#)
- [AWS Supply Chain 使用介面端點 \(AWS PrivateLink\) 存取](#)
- [適用於 的 IAM AWS Supply Chain](#)
- [AWS 的 受管政策 AWS Supply Chain](#)
- [的合規驗證 AWS Supply Chain](#)
- [中的彈性 AWS Supply Chain](#)
- [記錄和監控 AWS Supply Chain](#)
- [使用 管理 AWS Supply Chain 事件 Amazon EventBridge](#)

中的資料保護 AWS Supply Chain

AWS [共同責任模型](#)適用於 中的資料保護 AWS Supply Chain。如此模型所述，AWS 負責保護執行所有的 全球基礎設施 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 Supply Chain 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。

處理的資料 AWS Supply Chain

為了限制特定 AWS Supply Chain 執行個體的授權使用者可存取的資料，持有於 AWS Supply Chain 內的資料會依 AWS 您的帳戶 ID 和 AWS Supply Chain 執行個體 ID 分隔。

AWS 供應鏈會處理各種供應鏈資料，例如使用者資訊、從資料連接器擷取的資訊，以及庫存詳細資訊。

選擇退出偏好設定

我們可能會使用和存放由 處理的內容 AWS Supply Chain，如 [AWS 服務條款](#)所述。如果您想要選擇退出 AWS Supply Chain 以使用或儲存內容，您可以在 AWS Organizations 中建立選擇退出政策。如需建立選擇退出政策的詳細資訊，請參閱 [AI 服務選擇退出政策語法和範例](#)。

靜態加密

分類為 PII 的聯絡資料，或代表客戶內容的資料，包括由 AWS Supply Chain 存放之 Amazon Q 中使用的內容 AWS Supply Chain，會靜態加密（即在放入、存放或儲存到磁碟之前），其金鑰有時間限制且特定於 AWS Supply Chain 執行個體。

Amazon S3 伺服器端加密用於使用每個客戶帳戶唯一的資料金鑰加密所有主控台和 Web 應用程式 AWS Key Management Service 資料。如需的相關資訊 AWS KMS keys，請參閱《AWS Key Management Service 開發人員指南》中的[什麼是 AWS Key Management Service？](#)。

Note

AWS Supply Chain 功能 供應規劃和 N 層可見性不支援使用提供的 KMS-CMK data-at-rest。

傳輸中加密

資料包括與 AWS Supply Chain AWS Supply Chain 交換之 Amazon Q 中使用的內容，會在使用者網頁瀏覽器與 AWS Supply Chain 之間使用業界標準的 TLS 加密進行傳輸時受到保護。

金鑰管理

AWS Supply Chain 部分支援 KMS-CMK。

如需在 中更新 AWS KMS 金鑰的資訊 AWS Supply Chain，請參閱 [步驟 2：建立執行個體](#)。

網際網路流量隱私權

Note

AWS Supply Chain 不支援 PrivateLink。

的虛擬私有雲端 (VPC) 端點 AWS Supply Chain 是 VPC 內的邏輯實體，僅允許連線 AWS Supply Chain。VPC 會將請求路由至，AWS Supply Chain 並將回應路由回 VPC。如需詳細資訊，請參閱《[VPC 使用者指南](#)》中的 [VPC 端點](#)。

如何在 中使用 AWS Supply Chain 授予 AWS KMS

AWS Supply Chain 需要[授予](#)才能使用您的客戶受管金鑰。

AWS Supply Chain 會使用 CreateInstance 操作期間傳遞的 AWS KMS 金鑰來建立數個授予。會傳送 [CreateGrant](#) 請求給 來代表您 AWS Supply Chain 建立授予 AWS KMS。中的授予 AWS KMS 用於授予客戶帳戶中 AWS KMS 金鑰的 AWS Supply Chain 存取權。

Note

AWS Supply Chain 使用自己的授權機制。使用者新增至 後 AWS Supply Chain，您就無法使用 AWS KMS 政策拒絕列出相同的使用者。

AWS Supply Chain 會針對下列項目使用 授予：

- 將 GenerateDataKey 請求傳送至 ，AWS KMS 以[加密](#)存放在執行個體中的資料。
- 將解密請求傳送至 AWS KMS ，以讀取與執行個體相關聯的加密資料。
- 新增 DescribeKey、CreateGrant 和 RetireGrant 許可，以便在將資料傳送至 Amazon Forecast 等 AWS 其他服務時確保資料的安全。

您可以隨時撤銷授予的存取權，或移除服務對客戶受管金鑰的存取權。如果您這麼做，AWS Supply Chain 您將無法存取客戶受管金鑰加密的任何資料，這會影響依賴該資料的操作。

監控 的加密 AWS Supply Chain

下列範例是 Encrypt、和 AWS CloudTrail 的事件GenerateDataKey，Decrypt用於監控 呼叫的 KMS 操作 AWS Supply Chain，以存取客戶受管金鑰加密的資料：

Encrypt

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AWSService",
    "invokedBy": "scn.amazonaws.com"
  },
  "eventTime": "2024-03-06T22:39:32Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "Encrypt",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "172.12.34.56"
  "userAgent": "Example/Desktop/1.0 (V1; OS)",
  "requestParameters": {
    "encryptionAlgorithm": "SYMMETRIC_DEFAULT",
    "keyId": "arn:aws:kms:us-east-1:123456789:key/1234abcd-11ab-22bc-33ef-123456sample"
  }
}
```

```

},
"responseElements": null,
"requestID": "12a345n4-78a4-8888-0000-a000-6q000yy666rr",
"eventID": "12a345n4-78a4-8888-0000-a000-6q000yy666rr",
"readOnly": true,
"resources": [
  {
    "accountId": account ID,
    "type": "AWS::KMS::Key",
    "ARN": "arn:aws:kms:us-
east-1:123456789:key/1234abcd-11ab-22bc-33ef-123456sample"
  }
],
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "112233445566",
"sharedEventID": "fdf9ee0f-e43f-4e43-beac-df69067edb8b",
"eventCategory": "Management"
}

```

GenerateDataKey

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AWSService",
    "invokedBy": "scn.amazonaws.com"
  },
  "eventTime": "2024-03-06T22:39:32Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "GenerateDataKey",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "172.12.34.56"
  "userAgent": "Example/Desktop/1.0 (V1; OS)",
  "requestParameters": {
    "encryptionContext": {
      "aws:s3:arn": "arn:aws:s3:::test/rawEvent/bf6666c1-111-48aaca-b6b0-
dsadsadsa3432423/noFlowName/scn.data.inboundorder/20240306_223934_536"
    },
    "keyId": "arn:aws:kms:us-
east-1:123456789:key/1234abcd-11ab-22bc-33ef-123456sample",

```

```

    "keySpec": "AES_222"
  },
  "responseElements": null,
  "requestID": "12a345n4-78a4-8888-0000-a000-6q000yy666rr",
  "eventID": "12a345n4-78a4-8888-0000-a000-6q000yy666rr",
  "readOnly": true,
  "resources": [
    {
      "accountId": account ID,
      "type": "AWS::KMS::Key",
      "ARN": "arn:aws:kms:us-east-1:123456789:key/1234abcd-11ab-22bc-33ef-123456sample"
    }
  ],
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "112233445566",
  "sharedEventID": "fdf9ee0f-e43f-4e43-beac-df69067edb8b",
  "eventCategory": "Management"
}

```

Decrypt

```

  {
    "eventVersion": "1.08",
    "userIdentity": {
      "type": "AWSService",
      "invokedBy": "scn.amazonaws.com"
    },
    "eventTime": "2024-03-06T22:39:32Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "172.12.34.56"
    "userAgent": "Example/Desktop/1.0 (V1; OS)",
    "requestParameters": {
      "keyId": "arn:aws:kms:us-east-1:123456789:key/1234abcd-11ab-22bc-33ef-123456sample",
      "encryptionAlgorithm": "SYMMETRIC_DEFAULT"
    },
    "responseElements": null,
  }

```

```
"requestID": "12a345n4-78a4-8888-0000-a000-6q000yy666rr",
"eventID": "12a345n4-78a4-8888-0000-a000-6q000yy666rr",
"readOnly": true,
"resources": [
  {
    "accountId": account ID,
    "type": "AWS::KMS::Key",
    "ARN": "arn:aws:kms:us-
east-1:123456789:key/1234abcd-11ab-22bc-33ef-123456sample"
  }
],
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "112233445566",
"sharedEventID": "fdf9ee0f-e43f-4e43-beac-df69067edb8b",
"eventCategory": "Management"
}
```

AWS Supply Chain 使用介面端點 (AWS PrivateLink) 存取

您可以使用在 VPC 和 之間 AWS PrivateLink 建立私有連線 AWS Supply Chain。您可以 AWS Supply Chain 像在 VPC 中一樣存取，無需使用網際網路閘道、NAT 裝置、VPN 連線或 Direct Connect 連線。VPC 中的執行個體不需要公有 IP 地址即可存取 AWS Supply Chain。

您可以建立由 AWS PrivateLink 提供支援的介面端點來建立此私有連線。我們會在您為介面端點啟用的每個子網中建立端點網路介面。這些是請求者管理的網路介面，可作為目的地為 AWS Supply Chain 之流量的進入點。

如需詳細資訊，請參閱《AWS PrivateLink 指南》中的[AWS 服務 透過 存取 AWS PrivateLink](#)。

的考量事項 AWS Supply Chain

在您設定的介面端點之前 AWS Supply Chain，請檢閱 AWS PrivateLink 指南中的[考量事項](#)。

AWS Supply Chain 支援透過介面端點呼叫其所有 API 動作。

建立的介面端點 AWS Supply Chain

您可以使用 Amazon VPC AWS Supply Chain 主控台或 AWS Command Line Interface () 建立的介面端點 AWS CLI。如需詳細資訊，請參閱《AWS PrivateLink 指南》中的[建立介面端點](#)。

AWS Supply Chain 使用下列服務名稱建立 的介面端點：

```
com.amazonaws.region.scn
```

如果您為介面端點啟用私有 DNS，您可以使用 AWS Supply Chain 其預設的區域 DNS 名稱向 提出 API 請求。例如：`scn.region.amazonaws.com`。

為您的介面端點建立端點政策

端點政策為 IAM 資源，您可將其連接至介面端點。預設端點政策允許 AWS Supply Chain 透過介面端點完整存取。若要控制 AWS Supply Chain 從 VPC 允許存取的，請將自訂端點政策連接至介面端點。

端點政策會指定以下資訊：

- 可執行動作的主體 (AWS 帳戶、IAM 使用者和 IAM 角色)
- 可執行的動作
- 可以對其執行動作的資源

如需詳細資訊，請參閱「AWS PrivateLink 指南」中的[使用端點政策控制對服務的存取](#)。

範例：AWS Supply Chain 動作的 VPC 端點政策

以下是自訂端點政策的範例。將此政策附加至介面端點後，此政策會針對所有資源上的所有主體，授予列出的 AWS Supply Chain 動作的存取權限。

```
{
  "Statement": [
    {
      "Principal": "*",
      "Effect": "Allow",
      "Action": [
        "scn:action-1",
        "scn:action-2",
        "scn:action-3"
      ],
      "Resource": "*"
    }
  ]
}
```

```
]
}
```

適用於 的 IAM AWS Supply Chain

AWS Identity and Access Management (IAM) 是 AWS 服務，可協助管理員安全地控制對 AWS 資源的存取。IAM 管理員可控制誰可以進行驗證（登入）和授權（具有許可）來使用 AWS Supply Chain 資源。IAM 是 AWS 服務 您可以免費使用的。

主題

- [目標對象](#)
- [使用身分驗證](#)
- [使用政策管理存取權](#)
- [AWS Supply Chain 如何使用 IAM](#)
- [的身分型政策範例 AWS Supply Chain](#)
- [對 AWS Supply Chain 身分和存取進行故障診斷](#)

目標對象

使用方式 AWS Identity and Access Management (IAM) 會根據您的角色而有所不同：

- 服務使用者 — 若無法存取某些功能，請向管理員申請所需許可 (請參閱 [對 AWS Supply Chain 身分和存取進行故障診斷](#))
- 服務管理員 — 負責設定使用者存取權並提交相關許可請求 (請參閱 [AWS Supply Chain 如何使用 IAM](#))
- IAM 管理員 — 撰寫政策以管理存取控制 (請參閱 [的身分型政策範例 AWS Supply Chain](#))

使用身分驗證

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

您可以使用身分來源的登入資料，例如 AWS IAM Identity Center (IAM Identity Center)、單一登入身分驗證或 Google/Facebook 登入資料，以聯合身分的形式登入。如需有關登入的詳細資訊，請參閱《AWS 登入 使用者指南》中的 [如何登入您的 AWS 帳戶](#)。

對於程式設計存取，AWS 提供 SDK 和 CLI 以密碼編譯方式簽署請求。如需詳細資訊，請參閱《IAM 使用者指南》中的 [API 請求的AWS 第 4 版簽署程序](#)。

AWS 帳戶 根使用者

當您建立時 AWS 帳戶，您會從一個名為 AWS 帳戶 theroot 使用者的登入身分開始，該身分可完整存取所有 AWS 服務和資源。強烈建議不要使用根使用者來執行日常任務。有關需要根使用者憑證的任務，請參閱《IAM 使用者指南》中的 [需要根使用者憑證的任務](#)。

聯合身分

最佳實務是要求人類使用者使用聯合身分提供者，以 AWS 服務使用臨時憑證存取。

聯合身分是您企業目錄、Web 身分提供者的使用者，或是 AWS 服務使用身分來源的憑證 Directory Service 存取的使用者。聯合身分會擔任角色，而該角色會提供臨時憑證。

若需集中化管理存取權限，建議使用 AWS IAM Identity Center。如需詳細資訊，請參閱 AWS IAM Identity Center 使用者指南中的 [什麼是 IAM Identity Center ?](#)。

IAM 使用者和群組

IAM 使用者 https://docs.aws.amazon.com/IAM/latest/UserGuide/id_users.html 是一種身分具備單人或應用程式的特定許可權。建議以臨時憑證取代具備長期憑證的 IAM 使用者。如需詳細資訊，請參閱《IAM 使用者指南》中的 [要求人類使用者使用聯合身分提供者來 AWS 使用臨時憑證存取](#)。

[IAM 群組](#) 會指定 IAM 使用者集合，使管理大量使用者的許可權更加輕鬆。如需詳細資訊，請參閱《IAM 使用者指南》中的 [IAM 使用者的使用案例](#)。

IAM 角色

IAM 角色 https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html 的身分具有特定許可權，其可以提供臨時憑證。您可以透過 [從使用者切換到 IAM 角色（主控台）](#) 或呼叫 AWS CLI 或 AWS API 操作來擔任角色。如需詳細資訊，請參閱《IAM 使用者指南》中的 [擔任角色的方法](#)。

IAM 角色適用於聯合身分使用者存取、臨時 IAM 使用者許可、跨帳戶存取權與跨服務存取，以及在 Amazon EC2 執行的應用程式。如需詳細資訊，請參閱《IAM 使用者指南》中的 [IAM 中的快帳戶資源存取](#)。

使用政策管理存取權

您可以透過建立政策並將其連接到身分或資源 AWS 來控制 AWS 中的存取。政策定義與身分或資源相關聯的許可。當委託人提出請求時 AWS，會評估這些政策。大多數政策會以 JSON 文件 AWS 形式存放在中。如需進一步了解 JSON 政策文件，請參閱《IAM 使用者指南》中的 [JSON 政策概觀](#)。

管理員會使用政策，透過定義哪些主體可在哪些條件下對哪些資源執行動作，以指定可存取的範圍。

預設情況下，使用者和角色沒有許可。IAM 管理員會建立 IAM 政策並將其新增至角色，供使用者後續擔任。IAM 政策定義動作的許可，無論採用何種方式執行。

身分型政策

身分型政策是附加至身分 (使用者、使用者群組或角色) 的 JSON 許可政策文件。這類政策控制身分可對哪些資源執行哪些動作，以及適用的條件。如需了解如何建立身分型政策，請參閱《IAM 使用者指南》中的 [透過客戶管理政策定義自訂 IAM 許可](#)。

身分型政策可分為內嵌政策 (直接內嵌於單一身分) 與受管政策 (可附加至多個身分的獨立政策)。如需了解如何在受管政策及內嵌政策之間做選擇，請參閱《IAM 使用者指南》中的 [在受管政策與內嵌政策之間選擇](#)。

資源型政策

資源型政策是附加到資源的 JSON 政策文件。範例包括 IAM 角色信任政策與 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。您必須在資源型政策中 [指定主體](#)。

資源型政策是位於該服務中的內嵌政策。您無法在以資源為基礎的政策中使用來自 IAM 的 AWS 受管政策。

其他政策類型

AWS 支援其他政策類型，可設定更多常見政策類型授予的最大許可：

- 許可界限 — 設定身分型政策可授與 IAM 實體的最大許可。如需詳細資訊，請參閱《IAM 使用者指南》中的 [IAM 實體許可界限](#)。
- 服務控制政策 (SCP) — 為 AWS Organizations 中的組織或組織單位指定最大許可。如需詳細資訊，請參閱《AWS Organizations 使用者指南》中的 [服務控制政策](#)。
- 資源控制政策 (RCP) — 設定您帳戶中資源可用許可的上限。如需詳細資訊，請參閱《AWS Organizations 使用者指南》中的 [資源控制政策 \(RCP\)](#)。

- 工作階段政策 — 在以程式設計方式為角色或聯合身分使用者建立臨時工作階段時，以參數形式傳遞的進階政策。如需詳細資訊，請參閱《IAM 使用者指南》中的[工作階段政策](#)。

多種政策類型

當多種類型的政策適用於請求時，產生的許可會更複雜而無法理解。若要了解如何 AWS 在涉及多種政策類型時決定是否允許請求，請參閱《IAM 使用者指南》中的[政策評估邏輯](#)。

AWS Supply Chain 如何使用 IAM

在您使用 IAM 管理對的存取之前 AWS Supply Chain，請先了解哪些 IAM 功能可與搭配使用 AWS Supply Chain。

您可以搭配使用的 IAM 功能 AWS Supply Chain

IAM 功能	AWS Supply Chain 支援
身分型政策	是
資源型政策	否
政策動作	是
政策資源	是
政策條件索引鍵	是
臨時憑證	是
轉送存取工作階段 (FAS)	是
服務角色	是
服務連結角色	否

若要全面了解 AWS Supply Chain 和其他 AWS 服務如何與大多數 IAM 功能搭配使用，請參閱《[AWS IAM 使用者指南](#)》中的與 IAM 搭配使用的服務。

的身分型政策 AWS Supply Chain

支援身分型政策：是

身分型政策是可以附加到身分 (例如 IAM 使用者、使用者群組或角色) 的 JSON 許可政策文件。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。如需了解如何建立身分型政策，請參閱《IAM 使用者指南》中的[透過客戶管理政策定義自訂 IAM 許可](#)。

使用 IAM 身分型政策，您可以指定允許或拒絕的動作和資源，以及在何種條件下允許或拒絕動作。如要了解您在 JSON 政策中使用的所有元素，請參閱《IAM 使用者指南》中的[IAM JSON 政策元素參考](#)。

的身分型政策範例 AWS Supply Chain

若要檢視 AWS Supply Chain 身分型政策的範例，請參閱[的身分型政策範例 AWS Supply Chain](#)。

中的資源型政策 AWS Supply Chain

支援資源型政策：否

資源型政策是附加到資源的 JSON 政策文件。資源型政策的最常見範例是 IAM 角色信任政策和 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下執行的動作。您必須在資源型政策中[指定主體](#)。委託人可以包含帳戶、使用者、角色、聯合身分使用者或 AWS 服務。

如需啟用跨帳戶存取權，您可以在其他帳戶內指定所有帳戶或 IAM 實體作為資源型政策的主體。如需詳細資訊，請參閱《IAM 使用者指南》中的[IAM 中的快帳戶資源存取](#)。

的政策動作 AWS Supply Chain

支援政策動作：是

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

JSON 政策的 Action 元素描述您可以用來允許或拒絕政策中存取的動作。政策會使用動作來授予執行相關聯動作的許可。

中的政策動作在動作之前 AWS Supply Chain 使用以下字首：

```
scn
```

若要在單一陳述式中指定多個動作，請用逗號分隔。

```
"Action": [  
  "scn:action1",  
  "scn:action2"  
]
```

若要檢視 AWS Supply Chain 身分型政策的範例，請參閱 [的身分型政策範例 AWS Supply Chain](#)。

的政策資源 AWS Supply Chain

支援政策資源：是

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

Resource JSON 政策元素可指定要套用動作的物件。最佳實務是使用其 [Amazon Resource Name \(ARN\)](#) 來指定資源。若動作不支援資源層級許可，使用萬用字元 (*) 表示該陳述式適用於所有資源。

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

若要檢視 AWS Supply Chain 身分型政策的範例，請參閱 [的身分型政策範例 AWS Supply Chain](#)。

的政策條件索引鍵 AWS Supply Chain

支援服務特定政策條件金鑰：是

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

Condition 元素會根據定義的條件，指定陳述式的執行時機。您可以建立使用 [條件運算子](#) 的條件運算式 (例如等於或小於)，來比對政策中的條件和請求中的值。若要查看所有 AWS 全域條件索引鍵，請參閱《IAM 使用者指南》中的 [AWS 全域條件內容索引鍵](#)。

若要檢視 AWS Supply Chain 身分型政策的範例，請參閱 [的身分型政策範例 AWS Supply Chain](#)。

搭配 使用臨時登入資料 AWS Supply Chain

支援臨時憑證：是

臨時登入資料提供 AWS 資源的短期存取權，並在您使用聯合或切換角色時自動建立。AWS 建議您動態產生臨時登入資料，而不是使用長期存取金鑰。如需詳細資訊，請參閱《IAM 使用者指南》中的 [IAM 中的臨時安全憑證與可與 IAM 搭配運作的AWS 服務](#)。

轉送 的存取工作階段 AWS Supply Chain

支援轉寄存取工作階段 (FAS)：是

轉送存取工作階段 (FAS) 使用呼叫的委託人許可 AWS 服務，並結合 AWS 服務請求向下游服務提出請求。如需提出 FAS 請求時的政策詳細資訊，請參閱 [轉發存取工作階段](#)。

的服務角色 AWS Supply Chain

支援服務角色：是

服務角色是服務擔任的 [IAM 角色](#)，可代您執行動作。IAM 管理員可以從 IAM 內建立、修改和刪除服務角色。如需詳細資訊，請參閱《IAM 使用者指南》中的 [建立角色以委派許可給 AWS 服務](#)。

Warning

變更服務角色的許可可能會中斷 AWS Supply Chain 功能。只有在 AWS Supply Chain 提供指引時，才能編輯服務角色。

的服務連結角色 AWS Supply Chain

支援服務連結角色：否

服務連結角色是連結至的一種服務角色 AWS 服務。服務可以擔任代表您執行動作的角色。服務連結角色會出現在您的 [AWS 帳戶](#)，並由服務擁有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。

如需建立或管理服务連結角色的詳細資訊，請參閱《[可與 IAM 搭配運作的AWS 服務](#)》。在資料表中尋找服務，其中包含服務連結角色欄中的 Yes。選擇是連結，以檢視該服務的服務連結角色文件。

的身分型政策範例 AWS Supply Chain

根據預設，使用者和角色沒有建立或修改 AWS Supply Chain 資源的許可。他們也無法使用 AWS 管理主控台、AWS Command Line Interface (AWS CLI) 或 AWS API 來執行任務。若要授予使用者對其所需資源執行動作的許可，IAM 管理員可以建立 IAM 政策。然後，管理員可以將 IAM 政策新增至角色，使用者便能擔任這些角色。

若要了解如何使用這些範例 JSON 政策文件建立 IAM 身分型政策，請參閱 [《IAM 使用者指南》中的建立 IAM 政策](#)。

主題

- [政策最佳實務](#)

政策最佳實務

身分型政策會判斷您帳戶中的某個人員是否可以建立、存取或刪除 AWS Supply Chain 資源。這些動作可能會讓您的 AWS 帳戶產生費用。當您建立或編輯身分型政策時，請遵循下列準則及建議事項：

- 開始使用 AWS 受管政策並邁向最低權限許可 – 若要開始將許可授予您的使用者和工作負載，請使用將許可授予許多常見使用案例的 AWS 受管政策。它們可在您的 中使用 AWS 帳戶。我們建議您定義特定於使用案例 AWS 的客戶受管政策，進一步減少許可。如需更多資訊，請參閱《IAM 使用者指南》中的 [AWS 受管政策](#) 或 [任務職能的 AWS 受管政策](#)。
- 套用最低權限許可 – 設定 IAM 政策的許可時，請僅授予執行任務所需的許可。為實現此目的，您可以定義在特定條件下可以對特定資源採取的動作，這也稱為最低權限許可。如需使用 IAM 套用許可的更多相關資訊，請參閱《IAM 使用者指南》中的 [IAM 中的政策和許可](#)。
- 使用 IAM 政策中的條件進一步限制存取權 – 您可以將條件新增至政策，以限制動作和資源的存取。例如，您可以撰寫政策條件，指定必須使用 SSL 傳送所有請求。如果透過特定 例如 使用服務動作 AWS 服務，您也可以使用條件來授予其存取權 CloudFormation。如需詳細資訊，請參閱《IAM 使用者指南》中的 [IAM JSON 政策元素：條件](#)。
- 使用 IAM Access Analyzer 驗證 IAM 政策，確保許可安全且可正常運作 – IAM Access Analyzer 驗證新政策和現有政策，確保這些政策遵從 IAM 政策語言 (JSON) 和 IAM 最佳實務。IAM Access Analyzer 提供 100 多項政策檢查及切實可行的建議，可協助您撰寫安全且實用的政策。如需詳細資訊，請參閱《IAM 使用者指南》中的 [使用 IAM Access Analyzer 驗證政策](#)。
- 需要多重要素驗證 (MFA) – 如果您的案例需要 IAM 使用者或 中的根使用者 AWS 帳戶，請開啟 MFA 以提高安全性。如需在呼叫 API 操作時請求 MFA，請將 MFA 條件新增至您的政策。如需詳細資訊，請參閱《IAM 使用者指南》中的 [透過 MFA 的安全 API 存取](#)。

如需 IAM 中最佳實務的相關資訊，請參閱《IAM 使用者指南》中的 [IAM 安全最佳實務](#)。

對 AWS Supply Chain 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 Supply Chain 和 IAM 時可能遇到的常見問題。

主題

- [我未獲授權在 中執行動作 AWS Supply Chain](#)
- [我未獲授權執行 iam:PassRole](#)
- [我想要允許 以外的人員 AWS 帳戶 存取我的 AWS Supply Chain 資源](#)

我未獲授權在 中執行動作 AWS Supply Chain

如果您未獲授權執行動作的 AWS 管理主控台，則必須聯絡管理員尋求協助。您的管理員是為您提供使用者名稱和密碼的人員。

下列範例錯誤會在mateojackson IAM 使用者嘗試使用主控台檢視一個虛構 *my-example-widget* 資源的詳細資訊，但卻無虛構 `scn:GetWidget` 許可時發生。

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

我未獲授權執行 iam:PassRole

如果您收到錯誤，告知您未獲授權執行 `iam:PassRole` 動作，您的政策必須更新，允許您將角色傳遞給 AWS Supply Chain。

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。

名為 marymajor 的 IAM 使用者嘗試使用主控台在 AWS Supply Chain 中執行動作時，發生下列範例錯誤。但是，動作要求服務具備服務角色授予的許可。Mary 沒有將角色傳遞給服務的許可。

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

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

如果您需要協助，請聯絡您的 AWS 管理員。您的管理員提供您的簽署憑證。

我想要允許以外的人員 AWS 帳戶 存取我的 AWS Supply Chain 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 Supply Chain 支援這些功能，請參閱 [AWS Supply Chain 如何使用 IAM](#)。
- 若要了解如何提供您擁有 AWS 帳戶 的資源存取權，請參閱 [《IAM 使用者指南》中的在您擁有 AWS 帳戶 的另一個 IAM 使用者中提供存取權](#)。
- 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 AWS 帳戶 擁有](#)。
- 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 \(聯合身分\)](#)。
- 如需了解使用角色和資源型政策進行跨帳戶存取之間的差異，請參閱 [《IAM 使用者指南》中的 IAM 中的跨帳戶資源存取](#)。

AWS 的 受管政策 AWS Supply Chain

AWS 受管政策是由 AWS 受管政策建立和管理的獨立政策旨在為許多常用案例提供許可，以便您可以開始將許可指派給使用者、群組和角色。

請記住，AWS 受管政策可能不會授予特定使用案例的最低權限許可，因為這些許可可供所有 AWS 客戶使用。我們建議您定義特定於使用案例的 [客戶管理政策](#)，以便進一步減少許可。

您無法變更 AWS 受管政策中定義的許可。如果 AWS 更新受管政策中定義的許可，則更新會影響政策連接的所有委託人身分（使用者、群組和角色）。當新的 AWS 服務 啟動或新的 API 操作可用於現有服務時，AWS 最有可能更新 AWS 受管政策。

如需詳細資訊，請參閱 IAM 使用者指南中的 [AWS 受管政策](#)。

AWS 受管政策：AWSSupplyChainFederationAdminAccess

AWSSupplyChainFederationAdminAccess AWS Supply Chain 可讓聯合身分使用者存取 AWS Supply Chain 應用程式，包括在 AWS Supply Chain 應用程式中執行動作所需的許可。此政策透過 IAM Identity Center 使用者和群組提供管理許可，並連接到 AWS Supply Chain 為您建立的角色。您不應將 AWSSupplyChainFederationAdminAccess 政策連接至任何其他 IAM 實體。

雖然此政策 AWS Supply Chain 透過 `scn:*` 許可提供的所有存取權，但 AWS Supply Chain 角色會決定您的許可。AWS Supply Chain 角色僅包含必要的許可，而且沒有管理員 APIs 許可。

許可詳細資訊

此政策包含以下許可：

- Chime – 提供在 Amazon Chime AppInstance 下建立或刪除使用者的存取權；提供管理頻道、頻道成員和主持人的存取權；提供傳送訊息至頻道的存取權。Chime 操作的範圍是標記為 "SCNInstanceID" 的應用程式執行個體。
- AWS IAM Identity Center (AWS SSO) – 提供在 IAM Identity Center 中關聯和取消關聯使用者設定檔、列出設定檔關聯、列出應用程式指派、描述應用程式、描述執行個體和取得應用程式指派組態所需的許可。
- AppFlow – 提供建立、更新和刪除連線設定檔的存取權；提供建立、更新、刪除、啟動和停止流程的存取權；提供標記和取消標記流程的存取權，以及描述流程記錄。
- Amazon S3 – 提供列出所有儲存貯體的存取權。提供 GetBucketLocation、GetBucketPolicy、PutObject、GetObject 和 ListBucket 存取具有 `arn:aws:s3:::aws-supply-chain-data-*` 資源的儲存貯體。
- SecretsManager – 提供建立秘密和更新秘密政策的存取權。
- KMS – 為 Amazon AppFlow 服務提供列出金鑰和金鑰別名的存取權。提供 DescribeKey、CreateGrant 和 ListGrants 許可給標記為 `key-value aws-supply-chain-access` 的 KMS 金鑰：`true`；提供建立秘密和更新秘密政策的存取權。

許可 (`kms:ListKeys`、`kms:ListAliases`、`kms:GenerateDataKey` 和 `kms:Decrypt`) 不限於 Amazon AppFlow，而且這些許可可以授予您帳戶中的任何 AWS KMS 金鑰。

若要檢視此政策的許可，請參閱《》中的 [AWSSupplyChainFederationAdminAccess](#) AWS 管理主控台。

AWS Supply Chain AWS 受管政策的更新

下表列出自此服務開始追蹤這些變更以來，AWS Supply Chain 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 AWS Supply Chain 文件歷史記錄頁面上的 RSS 摘要。

變更	描述	Date
AWSSupplyChainFederationAdminAccess – 更新的政策	AWS Supply Chain 已更新 受管政策，以允許聯合身分使用者存取使用客戶受管 KMS 金鑰 (CMKs) 加密的 IAM Identity Center 中的資料。	2025 年 10 月 30 日
AWSSupplyChainFederationAdminAccess – 更新的政策	AWS Supply Chain 已更新 受管政策，以允許聯合身分使用者存取 IAM Identity Center 中的 ListApplicationAssignments、DescribeInstance、DescribeApplication 和 GetApplicationAssignmentConfiguration 操作。	2024 年 12 月 10 日
AWSSupplyChainFederationAdminAccess – 更新的政策	AWS Supply Chain 已更新 受管政策，以允許聯合身分使用者存取 IAM Identity Center 中的 ListProfileAssociations 操作。	2023 年 11 月 1 日
AWSSupplyChainFederationAdminAccess – 更新的政策	AWS Supply Chain 已更新 受管政策，以允許聯合身分使用者存取專用 S3 儲存貯體上	2023 年 9 月 21 日

變更	描述	Date
	的 PutObject 和 GetObject 操作，其中資源 arn arn : aws : s3 : : aws-Provide- chain-dat a-*。	
AWSSupplyChainFederationAdminAccess – 新政策	AWS Supply Chain 新增了新的政策，以允許聯合身分使用者存取 AWS Supply Chain 應用程式。這包括在 AWS Supply Chain 應用程式中執行動作所需的許可。	2023 年 3 月 1 日
AWS Supply Chain 開始追蹤變更	AWS Supply Chain 已開始追蹤其 AWS 受管政策的變更。	2023 年 3 月 1 日

的合規驗證 AWS Supply Chain

第三方稽核人員 AWS Supply Chain 會在多個合規計畫中評估的安全性和 AWS 合規性。這些計畫包括 SOC、PCI、FedRAMP、HIPAA 等等。

如需 AWS 服務屬於特定合規計畫範圍內的清單，請參閱[AWS 合規計畫範圍內的服務](#)。如需一般資訊，請參閱 [AWS Compliance Programs](#)。

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

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

- [安全與合規快速入門指南](#) – 這些部署指南討論架構考量，並提供部署以安全為中心和以合規為中心的基準 AWS 環境時應採取的步驟。
- [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](#) – 此工作手冊和指南的集合可能適用於您的產業和位置。
- AWS Config 開發人員指南中的 [使用規則評估資源](#) – 本指南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](#) – 這 AWS 服務 可讓您全面檢視 的安全狀態 AWS ，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 Supply Chain

AWS 全域基礎設施是以 AWS 區域 和 可用區域為基礎建置。AWS 區域 提供多個實體分隔和隔離的可用區域。這些都與低延遲、高輸送量和高備援聯網連線。透過可用區域，您可以設計與操作的應用程式和資料庫，在可用區域之間自動容錯移轉而不會發生中斷。可用區域的可用性、容錯能力和擴展能力，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 Supply Chain 還提供多種功能，以協助支援您的資料彈性和備份需求。

記錄和監控 AWS Supply Chain

記錄和監控是維護 AWS Supply Chain 和其他 AWS 解決方案的可靠性、可用性和效能的重要部分。AWS 提供 AWS CloudTrail 監控工具來監看 AWS Supply Chain、在發生錯誤時回報，以及適時採取自動動作。

Note

只會擷取從 AWS Supply Chain 主控台呼叫的 APIs AWS CloudTrail。

AWS CloudTrail 擷取您 AWS 帳戶 發出或代表發出的 API 呼叫和相關事件，並傳送日誌檔案至您指定的 Amazon S3 儲存貯體。您可以找出哪些使用者和帳戶呼叫 AWS、發出呼叫的來源 IP 位址，以及呼叫的發生時間。您可以在 <https://scn.amazonaws.com> 下檢視 AWS 供應鏈事件。如需詳細資訊，請參閱「[AWS CloudTrail 使用者指南](#)」。

Note

請注意下列事項 AWS Supply Chain：

- 當您邀請無法存取的使用者時 AWS Supply Chain，這些使用者不會在從 Web 應用程式收到的通知中收到資訊。受邀使用者會收到包含 Web 應用程式連結的電子郵件通知。他們只有在擁有必要的使用者許可時，才能登入和檢視通知中的內容。

- 具有或沒有特定 Insight 使用者許可的所有使用者都可以檢視 Insights 聊天訊息。
- 身為應用程式管理員，當您將使用者新增至 AWS Supply Chain 執行個體時，他們可以存取 AWS KMS key。您可以管理使用者許可來新增或移除使用者。如需使用者許可的詳細資訊，請參閱 [管理使用者許可角色](#)。

AWS Supply Chain CloudTrail 中的資料事件

Note

下列出的 Web 應用程式 APIs [AWS Supply Chain Web 應用程式 APIs](#) 會列在 CloudTrail 的資料事件中。

[資料事件](#) 提供在資源上或在資源中執行的資源操作的相關資訊 (例如，讀取或寫入 Amazon S3 物件)。這些也稱為資料平面操作。資料事件通常是大量資料的活動。根據預設，CloudTrail 不會記錄資料事件。CloudTrail 事件歷史記錄不會記錄資料事件。

資料事件需支付額外的費用。如需 CloudTrail 定價的詳細資訊，請參閱 [AWS CloudTrail 定價](#)。

您可以使用 CloudTrail 主控台 AWS CLI 或 CloudTrail API 操作來記錄 AWS Supply Chain 資源類型的資料事件。

- 若要使用 CloudTrail 主控台記錄資料事件，請建立 [線索](#) 或 [事件資料存放區](#) 以記錄資料事件，或 [更新現有的線索或事件資料存放區](#) 以記錄資料事件。
 1. 選擇資料事件以記錄資料事件。
 2. 從資料事件類型清單中，選擇您要記錄資料事件的資源類型。
 3. 選擇您要使用的日誌選取器範本。您可以記錄資源類型的所有資料事件、記錄所有 readOnly 事件、記錄所有 writeOnly 事件，或建立自訂日誌選取器範本來篩選 readOnly、eventName 和 resources.ARN 欄位。
- 若要使用 記錄資料事件 AWS CLI，請設定 --advanced-event-selectors 參數以將 eventCategory 欄位設定為 `Data` 並將 resources.type 欄位設定為 資源類型值。您可以新增條件來篩選 readOnly、eventName 和 resources.ARN 欄位的值。
 - 若要設定追蹤記錄資料事件，請執行 [put-event-selectors](#) 命令。如需詳細資訊，請參閱 [使用 記錄線索的資料事件 AWS CLI](#)。

- 若要設定事件資料存放區來記錄資料事件，請執行 [create-event-data-store](#) 命令來建立新的事件資料存放區來記錄資料事件，或執行 [update-event-data-store](#) 命令來更新現有的事件資料存放區。如需詳細資訊，請參閱 [使用 記錄事件資料存放區的資料事件 AWS CLI](#)。

*您可以設定進階事件選取器來篩選 `eventName`、和 `resources.ARN` 欄位 `readOnly`，以僅記錄對您重要的事件。如需有關這些欄位的詳細資訊，請參閱 [AdvancedFieldSelector](#)。

AWS Supply Chain CloudTrail 中的 管理事件

[管理事件](#) 提供對 AWS 帳戶中資源執行的管理操作的相關資訊。這些也稱為控制平面操作。根據預設，CloudTrail 記錄管理事件。

AWS Supply Chain 會將 CloudTrail 的所有控制平面操作記錄為管理事件。

AWS Supply Chain Web 應用程式 APIs

本節中列出的 APIs 由 AWS Supply Chain 應用程式代表聯合身分使用者呼叫。這些 APIs 不會顯示在 CloudTrail 日誌中，也不會擷取在服務授權參考文件中，請參閱 [AWS Supply Chain](#)。這些 APIs 存取是由 AWS Supply Chain 應用程式根據聯合身分使用者角色許可來控制。您不應該嘗試控制對這些 APIs 存取，以防止破壞 AWS Supply Chain 應用程式。

使用者角色

下列 APIs 用於管理 中的使用者、使用者角色、使用者通知和聊天訊息 AWS Supply Chain。

```
scn:AddMembersToResourceBasedChat
scn:AssignGalaxyRoleToUser
scn:AssociateUser
scn:BatchGetUsers
scn:BatchMarkNotificationAsDelivered
scn:CreateRole
scn>DeleteRole
scn:DescribeChatForUser
scn:GetAccessDetailConfig
scn:GetChatPreferencesForUser
scn:GetMessagingSessionConnectionDetails
scn:GetNotificationsPreference
scn:GetOrCreateChimeUser
scn:GetOrCreateResourceBasedChat
```

```
scn:GetOrCreateUserBasedChat
scn:GetOrganizationInfo
scn:GetResourceBasedChatArn
scn:GetUserDetails
scn:ListChatMembers
scn:ListChatMessages
scn:ListChatModerators
scn:ListChats
scn:ListRoles
scn:ListUserNotifications
scn:ListUsersWithRole
scn:MarkNotificationAsDelivered
scn:MarkNotificationAsRead
scn:RemoveMemberFromResourceBasedChat
scn:RemoveUser
scn:SearchChimeUsers
scn:SearchUsers
scn:SendChatMessage
scn:SetNotificationsPreference
scn:UpdateChatPreferencesForUser
scn:UpdateChatReadMarker
scn:UpdateOrganizationInfo
scn:UpdateRole
scn:UpdateUser
```

資料湖

下列 APIs 用於在資料湖中建立和管理資料流程和連線。

```
scn:CreateConnection
scn:CreateDataflow
scn:CreateDeleteDataByPartitionJob
scn:CreateExtractFlows
scn:CreatePresignedUrl
scn:CreateSampleParsingJob
scn:CreateSapODataConnection
scn:CreateUpdateDatasetSchemaJob
scn>DeleteConnection
scn>DeleteDataflow
```

```
scn:DeleteExtractFlows
scn:DeleteSapODataConnection
scn:describeDatasetGroup
scn:DescribeDataset
scn:DescribeJob
scn:GetConnection
scn:GetCreateExtractFlowsStatus
scn:GetDataflow
scn:ListConnections
scn:ListCustomerFiles
scn:ListDataflows
scn:ListDataflowStats
scn:ListDatasets
scn:UpdateConnection
scn:UpdateDataflow
scn:UpdateExtractFlow
```

洞見

Insights 應用程式會使用下列 APIs 來管理篩選條件、監視清單和檢視庫存變更。

```
scn:AddModeratorToResourceBasedChat
scn:ComputePostRebalancedQuantities
scn:ComputePostRebalancedQuantitiesV1
scn:CreateInsightFilter
scn:CreateInsightSubscription
scn>DeleteInsightFilter
scn>DeleteInsightSubscription
scn:GetInsightLineItem
scn:GetInsightSubscription
scn:GetInstanceAttribute
scn:GetInstanceRequiredDatasetAvailabilityStatus
scn:GetKpiData
scn:GetModelEndpointStatus
scn:GetPIVForProduct
scn:GetPIVForSite
scn:GetPIVForSiteAndProduct
scn:GetPIVForSitesAndProducts
scn:GetProducts
```

```
scn:GetProductSummaryAggregates
scn:GetSites
scn:GetSiteSummaryAggregates
scn:IsUserAuthorizedForInsightLineItem
scn:ListCustomAttributeValues
scn:ListGeographiesAsGalaxyAdmin
scn:ListInsightFilters
scn:ListInsightLineItems
scn:ListInsightSubscriptions
scn:ListInventoryQuantityAggregates
scn:ListInventoryRisksBySiteAndProduct
scn:ListInventorySummariesBySite
scn:ListPIVProductsBySite
scn:ListProductHierarchiesAsGalaxyAdmin
scn:ListProducts
scn:ListProductsAsGalaxyAdmin
scn:ListSites
scn:ListUsers
scn:PotentiallyComputeThenListRebalancingOptionsForInsightLineItem
scn:RegisterInstanceAttribute
scn:UpdateInsightFilter
scn:UpdateInsightLineItemStatus
scn:UpdateInsightSubscription
scn:UpdateRebalancingOptionStatus
scn:UpdateRebalancingOptionStatusV1
```

需求規劃

下列 APIs 用於 AWS Supply Chain 建立和管理預測、需求計劃或工作手冊。

```
scn:AssociateDatasetWithWorkbook
scn:CreateBaselineForecast
scn:CreateDemandPlan
scn:CreateDemandPlanningCycle
scn:CreateDemandPlanningDatasetExportJob
scn:CreateDerivedForecast
scn:CreateWorkbook
scn>DeleteDemandForecastConfig
scn>DeleteDemandPlanningCycle
```

```
scn:DeleteDerivedForecast
scn:DeleteWorkbook
scn:DescribeBaselineForecast
scn:DescribeDemandPlanningCycleAccuracyJob
scn:DescribeDerivedForecast
scn:DescribePlanningCycle
scn:DescribeWorkbook
scn:DisassociatePlanningCycle
scn:GetDemandForecastConfig
scn:GetDemandPlan
scn:GetDemandPlanningCycle
scn:GetDemandPlanningCycleAccuracy
scn:GetDemandPlanningDatasetJob
scn:ListDemandPlans
scn:ListDerivedForecasts
scn:ListForecastingJobs
scn:ListPlanningCycles
scn:ListWorkbooks
scn:PublishDemandPlan
scn:PutDemandForecastConfig
scn:StartDemandPlanningCycleAccuracyJob
scn:StartForecastingJob
scn:UpdateDemandPlan
scn:UpdateDemandPlanningCycleMetadata
scn:UpdateWorkbook
```

供應規劃

下列 APIs 用於 AWS Supply Chain 建立和管理供應計劃。

```
scn:CreateReplenishmentPipeline
scn:GetReplenishmentPipeline
scn:UpdateReplenishmentPipeline
scn:ListReplenishmentPipelinesByInstance
scn:GetInstanceReplenishmentConfig
scn:CreateBacktest
scn:CreateReplenishmentReviewInstanceConfig
scn:GetReplenishmentReviewInstanceConfig
scn:ListReplenishmentVendors
```

```
scn:GetExceptionsSupplyInsightsStatistics
scn:GetPorSupplyInsightsStatistics
scn:GetPlanToPOConversionAnalytics
scn:GetPurchasePlanStatistics
scn:ListPlanExceptions
scn:ListPurchaseOrderRequestLines
scn:UpdatePurchaseOrderRequestLines
scn:ListBomPurchasePlans
scn:ListBomProductionPlans
scn:ListBomTransferPlans
scn:ListBomInsights
scn:ListBomProcesses
scn:ExportBomPlans
scn:GetBomPlanSummary
scn:GetDashboardAnalytics
scn:GetPurchaseOrderRequestExplanation
scn:ListBomSupplyPlan
scn:GetBomPlanRecordDetails
scn:GetBomPlanSummaryAnalytics
scn:ListBomPurchaseOrders
scn:ListBomTransferOrders
scn:ListBomProductionOrders
scn:ExportAllExplodedBoms
scn:ExportBillOfMaterials
scn:ExportInventoryPolicy
scn:ExportProductionProcess
scn:ExportSourcingRule
scn:ExportTransportationLane
scn:ExportVendorLeadTime
scn:ImportBillOfMaterials
scn:ImportInventoryPolicy
scn:ImportProductionProcess
scn:ImportSourcingRule
scn:ImportTransportationLane
scn:ImportVendorLeadTime
```

中的 Amazon Q AWS Supply Chain

Amazon Q in 中會使用下列 APIs AWS Supply Chain。

```

scn:GetQMessage
scn:ListQMessages
scn:PutQMessageFeedback
scn:SendMessage
scn:GetQEnablementStatus
scn:UpdateQEnablementStatus

```

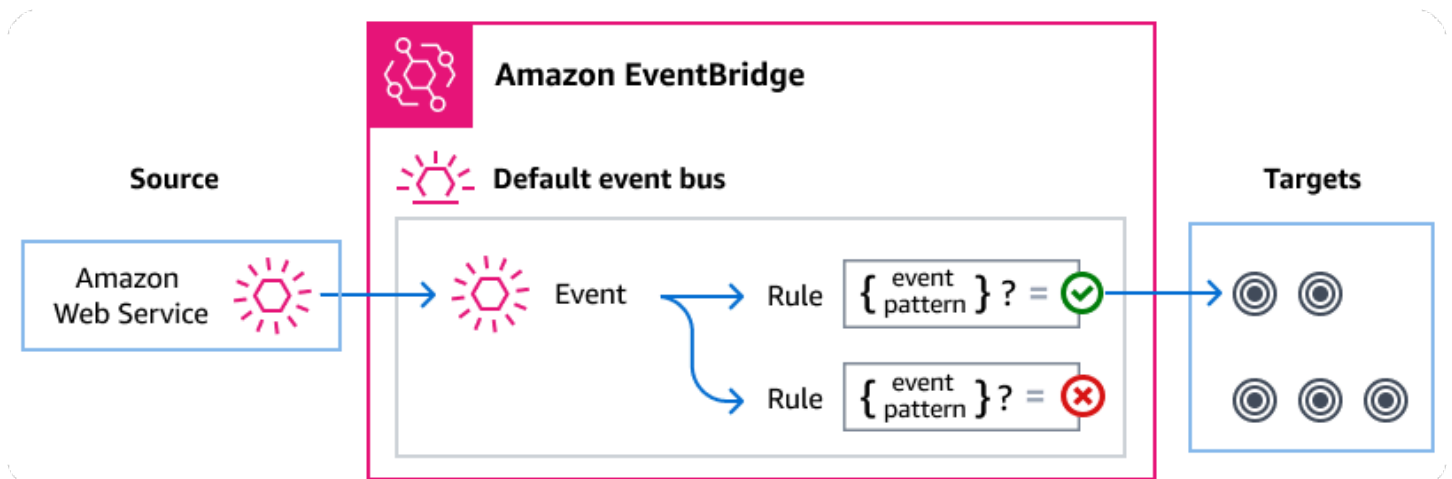
使用 管理 AWS Supply Chain 事件 Amazon EventBridge

使用 EventBridge，您可以將其他 服務自動化，以回應 Step Functions 標準工作流程的執行狀態變更。

Amazon EventBridge 是一種無伺服器服務，使用事件將應用程式元件連接在一起，讓您更輕鬆地建置可擴展的事件驅動型應用程式。事件驅動架構是一種建置鬆耦合軟體系統的方式，透過發出和回應事件來協作。事件代表資源或環境中的變更。

以下是其運作方式：

如同許多 AWS 服務，AWS Supply Chain 會產生事件並將其傳送至 EventBridge 預設事件匯流排。（預設事件匯流排會自動在每個 AWS 帳戶中佈建。）事件匯流排是接收事件，並將事件傳遞至零個或多個目的地或目標的路由器。為事件匯流排指定的規則會在事件到達時評估事件。每項規則都會檢查事件是否與規則的事件模式相符。如果事件不相符，事件匯流排會將事件傳送至指定的目標。



主題

- [AWS Supply Chain 事件](#)
- [使用 EventBridge 規則交付 AWS Supply Chain 事件](#)

- [AWS Supply Chain 事件詳細資訊參考](#)

AWS Supply Chain 事件

AWS Supply Chain 會自動將下列事件傳送至預設 EventBridge 事件匯流排。符合規則事件模式的事件會根據[基準](#)交付至指定的目標。事件可能無法按順序交付。

如需詳細資訊，請參閱《使用者指南》中的[EventBridge 事件](#)。Amazon EventBridge

事件詳細資訊類型	Description
AWS 供應鏈資料整合狀態變更	顯示每個擷取檔案的狀態 AWS Supply Chain。

使用 EventBridge 規則交付 AWS Supply Chain 事件

若要讓 EventBridge 預設事件匯流排將 AWS Supply Chain 事件傳送至目標，您必須建立規則。每個規則都包含一個事件模式，與事件匯流排上收到的每個事件 EventBridge 相符。如果事件資料符合指定的事件模式，會將該事件 EventBridge 傳遞至規則的目標 (s)。

如需建立事件匯流排規則的完整說明，請參閱 EventBridge 《使用者指南》中的[建立對事件做出反應的規則](#)。

建立符合事件 AWS Supply Chain 的事件模式

每個事件模式都是 JSON 物件，它包含：

- 識別傳送事件之服務的 `source` 屬性。對於 AWS Supply Chain 事件，來源為 `aws.supplychain`。
- (選擇性)：包含要比對之事件類型陣列的 `detail-type` 屬性。
- (選擇性)：包含要比對的任何其他事件資料的 `detail` 屬性。

例如，下列事件模式會比對來自的所有 AWS Supply Chain Data Integration Status Change 事件 AWS Supply Chain：

```
{
  "source": ["aws.supplychain"],
  "detail-type": ["AWS Supply Chain Data Integration Status Change"]
}
```

```
}
```

如需撰寫事件模式的詳細資訊，請參閱EventBridge 《使用者指南》中的[事件模式](#)。

AWS Supply Chain 事件詳細資訊參考

AWS 服務中的所有事件都有一組通用的欄位，其中包含事件的中繼資料，例如事件來源 AWS 的服務、事件產生的時間、事件發生的帳戶和區域，以及其他。如需這些一般欄位的定義，請參閱Amazon EventBridge 《使用者指南》中的[事件結構參考](#)。

此外，每個事件都有一個 detail 欄位，其中包含該特定事件的特定資料。以下參考定義了各種 AWS Supply Chain 事件的詳細資訊欄位。

使用 EventBridge 來選取和管理 AWS Supply Chain 事件時，請謹記下列事項：

- 來自的所有事件的 source 欄位 AWS Supply Chain 都設定為 `aws.supplychain`。
- detail-type 欄位指定事件類型。

例如 AWS Supply Chain Data Integration Status Change。

- detail 欄位包含該特定事件的特定資料。

如需建構事件模式以讓規則符合 AWS Supply Chain 事件的資訊，請參閱Amazon EventBridge 《使用者指南》中的[事件模式](#)。

如需事件及其 EventBridge 處理方式的詳細資訊，請參閱Amazon EventBridge 《使用者指南》中的[Amazon EventBridge 事件](#)。

AWS 供應鏈資料整合狀態變更

以下是AWS Supply Chain Data Integration Status Change event事件的範例。

```
{
  "version": "0",
  "id": "instanceID",
  "detail-type": "AWS Supply Chain Data Integration Status Change",
  "source": "aws.supplychain",
  "account": "accountID",
  "time": "2024-03-30T12:26:13Z",
  "region": "us-east-1",
```

```
"resources": [],
"detail": {
  "version": "1.0",
  "instanceId": "instanceID",
  "flowArn": "arn:aws:scn:region:accountID:instance/instanceID/data-integration-
flows/flowname",
  "flowExecutionId": "flowExecutionId",
  "status": "IN_PROGRESS",
  "startTime": "2024-03-30T12:26:13Z",
  "endTime": "",
  "message": "",
  "sourceType": "S3",
  "sourceInfo": {
    "s3Source": {
      "bucketName": "aws-supply-chain-data-instanceID",
      "key": "flowname"
    }
  }
}
```

endTime 只有在狀態為失敗或成功時才可用。


的配額 AWS Supply Chain

您的 AWS 帳戶 具有每個 的預設配額，先前稱為限制 AWS 服務。除非另有說明，否則每個配額都是區域特定規定。您可以請求增加設定為您帳戶層級之資源的配額。如需帳戶層級配額的詳細資訊，請參閱下表。

若要檢視 的配額 AWS Supply Chain，請開啟 [Service Quotas 主控台](#)。在導覽窗格中，選擇 AWS 服務，然後選取 AWS Supply Chain。

若要請求提升配額，請參閱《[Service Quotas 使用者指南](#)》中的請求提升配額。如果 Service Quotas 中尚未提供配額，請使用[限制增加表單](#)。

您的 AWS 帳戶 具有下列與 相關的配額 AWS Supply Chain。

資源	預設	可調整
執行個體的數目	10	否
<div style="border: 1px solid #ccc; border-radius: 10px; padding: 10px; background-color: #e6f2ff;"> <p> Note</p> <p>您可以在 AWS 帳戶中建立最多 10 個執行個體。</p> </div>		
Amazon S3 儲存貯體數量	100	否
AWS 帳戶中的作用中和待定邀請	30	是
AWS 帳戶內的資料請求	4,000	是
每個監視清單的 Insights 明細項目	1,000	否
AWS 帳戶中每個執行個體的 Insights 監視清單	1,000	是
AWS 帳戶中每個使用者的 Insights 監視清單	100	是

資源	預設	可調整
AWS 帳戶內每個執行個體的資料整合流程	100	否
AWS 帳戶中每個執行個體的自訂資料集命名空間	20	是
AWS 帳戶中每個執行個體的每個自訂資料集命名空間的資料集	250	是
AWS 帳戶內每個執行個體的預設資料集命名空間中的資料集	1,000	否

常見問答集 (FAQ)

以下資訊可協助您疑難排解啟用 IAM Identity Center 時的常見問題。

問題	答案
為什麼需要 IAM Identity Center 整合？	IAM Identity Center 是 IAM 中的功能，可管理身分來源的同步。IAM Identity Center 是 AWS Supply Chain 執行個體的身分來源。您需要設定 IAM Identity Center 來設定 AWS 主控台和 AWS Supply Chain Web 應用程式。如需 IAM Identity Center 的詳細資訊，請參閱 AWS IAM Identity Center 《使用者指南》 中的 啟用 AWS IAM Identity Center 。
為什麼要使用 IAM Identity Center 組織執行個體 AWS Supply Chain？	透過建立組織執行個體，您可以跨 AWS 帳戶啟用 IAM Identity Center 存取。例如，如果您的 IAM Identity Center 未在與 AWS Supply Chain 執行個體 AWS 帳戶相同的帳戶中啟用。如需建立組織 IAM Identity Center 執行個體之優勢的詳細資訊，請參閱 AWS IAM Identity Center 《使用者指南》 中的 IAM Identity Center 的組織執行個體 。
為什麼需要委派管理員權限 AWS Supply Chain？	不需要有委派管理員才能使用，AWS Supply Chain 但 AWS 組織設定最佳實務是限制對組織管理帳戶的存取和管理 IAM Identity Center。如需詳細資訊，請參閱 AWS Organizations 的委派管理員 。 建立組織執行個體時，請確定將用於建立 AWS Supply Chain 執行個體的帳戶與 IAM Identity Center 帳戶屬於同一個組織。請確定已啟用建立執行個體所需的許可，而且您可以在與 IAM Identity Center 帳戶相同的區域中建立 AWS Supply Chain 執行個體。如需建立 AWS Supply

問題	答案
	Chain 執行個體所需許可的資訊，請參閱 入門 AWS Supply Chain 。

AWS 支援

如果您是 管理員且需要聯絡 的支援 AWS Supply Chain，請選擇下列其中一個選項：

- 如果您有 支援 帳戶，請前往[支援中心](#)並提交票證。
- 開啟 [AWS 管理主控台](#)，然後選擇AWS 供應鏈、支援、建立案例。

提供下列資訊會很有幫助：

- 您的 AWS Supply Chain 執行個體 ID/ARN。
- 您的 AWS 區域。
- 問題的詳細說明。

AWS Supply Chain 管理員指南的文件歷史記錄

下表說明 文件的發行版本 AWS Supply Chain。

變更	描述	日期
更新 AWS 受管政策	AWS Supply Chain 已更新 受管政策，以允許聯合身分使用者存取使用客戶受管 KMS 金鑰 (CMKs) 加密的 IAM Identity Center 中的資料。	2025 年 10 月 30 日
更新 AWS Supply Chain 配額	已更新與 相關的 AWS 帳戶配額 AWS Supply Chain。	2025 年 5 月 12 日
更新 AWS 受管政策	AWS Supply Chain 已更新 受管政策，以允許聯合身分使用者存取 IAM Identity Center 中的 ListApplicationAssignments、DescribeInstance、DescribeApplication 和 GetApplicationAssignmentConfiguration 操作。	2024 年 12 月 10 日
KMS 政策更新	更新 KMS 政策以允許 AWS Supply Chain 存取您的 AWS KMS 金鑰。	2024 年 3 月 18 日
PrivateLink 支援	您可以使用界面端點 AWS Supply Chain (AWS PrivateLink) 存取。	2024 年 2 月 26 日
新增群組	使用者必須是 IAM Identity Center 群組的一部分才能存取 AWS Supply Chain。	2023 年 11 月 14 日

更新 AWS 受管政策	AWS Supply Chain 已更新 受管政策，以允許聯合身分使用者存取 IAM Identity Center 中的 ListProfileAssociations 操作。	2023 年 11 月 1 日
更新 AWS 受管政策	AWS Supply Chain 已更新 受管政策，以允許聯合身分使用者存取專用 Amazon S3 儲存貯體上的 PutObject 和 GetObject 操作，其中包含資源 arn arn : aws : s3 : : aws-Provide-chain-data-*。	2023 年 9 月 21 日
更新區域支援的相關資訊	AWS Supply Chain 亞太區域（雪梨）區域現在也支援需求規劃。	2023 年 9 月 12 日
使用 AWS 主控台選擇加入和退出 AWS Supply Chain	AWS Supply Chain 使用者現在可以使用 AWS 主控台來選擇加入和退出 AWS Supply Chain，以在 AWS Organizations 上使用或存放您的內容。	2023 年 9 月 7 日
更新區域支援的相關資訊	AWS Supply Chain 亞太區域（雪梨）區域和歐洲（愛爾蘭）區域現在也支援。	2023 年 7 月 19 日
更新如何聯絡 AWS Support 並建立執行個體的資訊	AWS Supply Chain 使用者現在可以聯絡 AWS Support 尋求協助，並更新如何建立執行個體的內容。	2023 年 4 月 3 日

新增 AWS 受管政策

AWS Supply Chain 新增了一項政策，以允許聯合身分使用者存取 AWS Supply Chain 應用程式，包括在 AWS Supply Chain 應用程式中執行動作所需的許可。

2023 年 3 月 1 日

初始版本

AWS Supply Chain 管理員指南的初始版本。

2022 年 11 月 29 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。