aws

管理員指南

AWS Supply Chain

AWS Supply Chain: 管理員指南

Table of Contents

什麼是 AWS Supply Chain？

AWS Supply Chain是一個基於雲的供應鏈管理應用程序，可與您現有的解決方案配合使用，例如企業資源規劃（ERP）和供應鏈管理系統。您可以使用AWS Supply Chain，將現有 ERP 或供應鏈系統中的庫存、供應和需求相關資料連接並擷取到一個統一的AWS Supply Chain資料模型中。

主題

AWS Supply Chain 支援的瀏覽器

在使用「供AWS應鏈」之前，請使用下表確認您的瀏覽器受支援。

瀏覽器	支援的版本
Google Chrome	最新版本有三個。
Mozilla Firefox ESR	版本支持，直到他們的 Firefox end-of-life日期。有關詳細信息，請參見火狐 ESR 發布日曆。
Mozilla Firefox	最新版本有三個。
微軟邊緣和邊緣鉻	版本 84 及更高版本。
Safari	野生動物園 10 或更高版本在 macOS 上。

支援的語言AWS Supply Chain

AWS Supply Chain 支援以下語言：

- 英文 (美國)
- 英文 (英國)
- 德文
- 西班牙文

- French
- 義大利文
- 葡萄牙人
- 簡體中文
- 繁體中文
- 日文
- 韓文
- 印尼文

設定帳 AWS 戶

使用本節建立 AWS 帳戶並建立 IAM 使用者。如需有關建立 AWS 帳戶的最佳做法的資訊，請參閱建立最佳實務 AWS 環境。

主題

註冊一個 AWS 帳戶

如果您沒有 AWS 帳戶，請完成以下步驟來建立一個。

若要註冊成為 AWS 帳戶

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

   部分註冊程序需接收來電，並在電話鍵盤輸入驗證碼。

   當您註冊時 AWS 帳戶，會建立AWS 帳戶根使用者一個。根使用者有權存取該帳戶中的所有 AWS 服務 和資源。安全性最佳做法是將管理存取權指派給使用者，並僅使用 root 使用者來執行需要 root 使用者存取權的工作。

AWS 註冊過程完成後，會向您發送確認電子郵件。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。

建立具有管理權限的使用者

註冊後，請保護您的 AWS 帳戶 AWS 帳戶根使用者 AWS IAM Identity Center、啟用和建立系統管理使用者，這樣您就不會將 root 使用者用於日常工作。

保護您的 AWS 帳戶根使用者

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

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

2. 若要在您的根使用者帳戶上啟用多重要素驗證 (MFA)。

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

建立具有管理權限的使用者

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 身分中心中，將管理存取權授予使用者。

   若要取得有關使用 IAM Identity Center 目錄 做為身分識別來源的自學課程，請參閱《使用指南》IAM Identity Center 目錄中的「以預設值設定使用AWS IAM Identity Center 者存取」。

以具有管理權限的使用者身分登入

- 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 身分中心使用者登入的說明，請參閱使用AWS 登入 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 身分中心中，建立遵循套用最低權限許可的最佳做法的權限集。

   如需指示，請參閱《AWS IAM Identity Center 使用指南》中的「建立權限集」。

2. 將使用者指派給群組，然後將單一登入存取權指派給群組。

   如需指示，請參閱《AWS IAM Identity Center 使用指南》中的「新增群組」。

關閉帳 AWS 戶

如需關閉 AWS 帳戶的詳細資訊，請參閱關閉帳戶。

開始使用 AWS Supply Chain

在本節中，您可以學習如何建立 AWS Supply Chain 執行個體、授與使用者權限角色、登入 AWS Supply Chain Web 應用程式，以及建立自訂使用者權限角色。一個最多 AWS 帳戶 可以有 10 個 AWS Supply Chain 處於使用中或初始化狀態的執行個體。

主題

必要條件

建立 AWS Supply Chain 執行個體之前，請確定您已完成下列步驟：

- 您已經建立了 AWS 帳戶. 如需詳細資訊，請參閱 設定帳 AWS 戶。

> **Note**
>
> 如果尚未啟用 AWS IAM Identity Center，請建立 AWS 組織並啟用 IAM 身分中心。如需有關建立 AWS 組織的詳細資訊，請參閱建立組織。

- 在您想要建立 AWS Supply Chain 執行個體的相同 AWS 區域 位置開啟 IAM 身分識別中心。 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) 和歐洲 (愛爾蘭) 區域提供支援。如需詳細資訊，請參閱 啟用 IAM 身分識別中心 。

> **Note**
>
> AWS Supply Chain 「歐洲 (愛爾蘭)」區域不支援「需求計劃」與「供給計劃」。

> **Note**
>
> 如果您尚未在此處列出的區域以外的區域啟用 IAM 身分中心，則無法建立 AWS Supply Chain 執行個體。

- 您可以從 AWS Identity and Access Management (IAM) 主控台建立 IAM 使用者。如需詳細資訊，請參閱 設定帳 AWS 戶。
- 新增需要存取 IAM 身分中心的使用者。 AWS Supply Chain 如需詳細資訊，請參閱 在 IAM 身分中心新增使用者。您也可以將作用中目錄連線至 IAM 身分中心。如需詳細資訊，請參閱AWS IAM Identity Center 使用者指南中的 Connect 到 Microsoft AD 目錄。
- 使用 Microsoft 活動目錄時，請確保啟用活動目錄同步。
- 你需要 AWS Key Management Service （ AWS KMS ）來創建一個實例。 AWS Supply Chain 使用它 AWS KMS key 來加密進入的所有數據 AWS Supply Chain。

使用 AWS Supply Chain 主控台

> **Note**
>
> 如果您的 AWS 帳戶是 AWS 組織的成員帳戶，並且包含服務控制原則 (SCP)，請確定組織的 SCP 將下列權限授與成員帳戶。如果組織的 SCP 原則中未包含下列權限，則 AWS Supply Chain 執行個體建立將會失敗。

若要存取 AWS Supply Chain 主控台，您必須擁有最少一組權限。這些權限必須允許您列出和檢視有關 AWS 帳戶. AWS Supply Chain 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。

您不需要為僅對 AWS CLI 或 AWS API 進行呼叫的使用者允許最低主控台權限。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。

若要確保使用者和角色仍可使用 AWS Supply Chain 主控台，請同時將 AWS Supply Chain ConsoleAccess或受ReadOnly AWS 管理的原則附加至實體。如需詳細資訊，請參閱《IAM 使用者指南》中的新增許可到使用者。

Console 管理員需要下列權限才能成功建立和更新 AWS Supply Chain 執行個體。

```
        {
"Version": "2012-10-17",
"Statement": [
    {
        "Action": "scn:*",
        "Resource": "*",
        "Effect": "Allow"
    },
    {
        "Action": [
            "s3:GetObject",
            "s3:PutObject",
            "s3:ListBucket",
            "s3:CreateBucket",
            "s3:PutBucketVersioning",
            "s3:PutBucketObjectLockConfiguration",
            "s3:PutEncryptionConfiguration",
            "s3:PutBucketPolicy",
            "s3:PutLifecycleConfiguration",
            "s3:PutBucketPublicAccessBlock",
            "s3:DeleteObject",
            "s3:ListAllMyBuckets",
            "s3:PutBucketOwnershipControls",
            "s3:PutBucketNotification",
            "s3:PutAccountPublicAccessBlock",
            "s3:PutBucketLogging",
            "s3:PutBucketTagging"
        ],
        "Resource": "arn:aws:s3:::aws-supply-chain-*",
        "Effect": "Allow"
    },
    {
        "Action": [
            "cloudtrail:CreateTrail",
            "cloudtrail:PutEventSelectors",
            "cloudtrail:GetEventSelectors",
```

```
                "cloudtrail:StartLogging"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "events:DescribeRule",
                "events:PutRule",
                "events:PutTargets"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "chime:CreateAppInstance",
                "chime:DeleteAppInstance",
                "chime:PutAppInstanceRetentionSettings",
                "chime:TagResource"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "cloudwatch:PutMetricData",
                "cloudwatch:Describe*",
                "cloudwatch:Get*",
                "cloudwatch:List*"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "organizations:DescribeOrganization",
                "organizations:CreateOrganization",
                "organizations:EnableAWSServiceAccess"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
```

```
            "Action": [
                "kms:CreateGrant",
                "kms:RetireGrant",
                "kms:DescribeKey",
                "kms:ListAliases"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "iam:CreateRole",
                "iam:CreatePolicy",
                "iam:GetRole",
                "iam:PutRolePolicy",
                "iam:AttachRolePolicy",
                "iam:CreateServiceLinkedRole"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "sso:StartPeregrine",
                "sso:DescribeRegisteredRegions",
                "sso:ListDirectoryAssociations",
                "sso:GetPeregrineStatus",
                "sso:GetSSOStatus",
                "sso:ListProfiles",
                "sso:GetProfile",
                "sso:AssociateProfile",
                "sso:AssociateDirectory",
                "sso:RegisterRegion",
                "sso:StartSSO",
                "sso:CreateManagedApplicationInstance",
                "sso:DeleteManagedApplicationInstance",
                "sso:GetManagedApplicationInstance",
                "sso-directory:SearchUsers"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }
    ]
}
```

建立執行個體

> **Note**
>
> 您可以在一個中建立最多 10 個執行個體 AWS 帳戶。這 10 個執行個體包括作用中和初始化執行個體。如果您已啟用 IAM 身分中心 (AWS 單一登入的繼任者)，則必須在啟用 IAM 身分中心的相同 AWS 區域 位置建立 AWS Supply Chain 執行個體。 AWS Supply Chain 不支援跨區域的 IAM 身分中心呼叫。

若要建立 AWS Supply Chain 執行個體，請依照下列步驟執行。

> **Note**
>
> 只有 AWS Management Console 管理員可以建立執行個體。建立 AWS Supply Chain 執行個體的 AWS Management Console 管理員應具有下列出的所有權限使用 AWS Supply Chain 主控台。此管理員應邀請 IAM 使用者以系統管理 AWS Supply Chain 員身分進行管理 AWS Supply Chain。

1. 在開啟 AWS Supply Chain 主控台https://console.aws.amazon.com/scn/home。
2. 如有需要，請變更 AWS 區域。在主控台視窗頂端的列中，開啟 [選取地區] 清單，然後選擇 [區域]。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。另請參閱中的區域和端點Amazon Web Services 一般參考。

   > **Note**
   >
   > 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) 區域提供支援。
   > AWS Supply Chain 「歐洲 (愛爾蘭)」區域不支援「需求計劃」與「供給計劃」。

3. 在 AWS Supply Chain 儀表板上，選擇 [建立執行個體]。

4. 在 [執行個體屬性] 頁面上，輸入下列資訊：

   - AWS 區域 — 選擇您已啟用 IAM 身分中心的區域。若要變更「地區」，請從右上角的下拉式選單中選擇「選取地區」。建立執行個體之後，就無法變更「區域」。
   - 名稱 — 輸入執行個體名稱。
   - (選擇性) 說明 — 輸入執行個體的說明。

5. 在 AWS KMS 金鑰下，輸入您的 KMS 金鑰，並使用下列項目更新您的 KMS 金鑰原則：

> **Note**
>
> 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. 您可以管理新增或移除使用者的使用者權限。如需使用者權限的詳細資訊，請參閱使用者權限角色。

> **Note**
>
> *YourKmsKeyArn*使用您的*##YourAccountNumber*、 AWS Supply Chain 執行個體 *YourInstanceID* 和 AWS KMS 金鑰取代 AWS 帳戶、 AWS 地區、ID 和。

```
   {
   "Version": "2012-10-17",
   "Statement": [{
           "Sid": "Enable IAM User Permissions",
           "Effect": "Allow",
           "Principal": {
               "AWS": "arn:aws:iam::YourAccountNumber: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.Region.amazonaws.com",
                    "kms:CallerAccount": "YourAccountNumber"
                }

            }
        }
    ]
}
```

如果您沒有 KMS 金鑰，請選擇 [建立] 移至 AWS KMS 主控台，您可以在其中建立此金鑰。使用先前的 KMS 金鑰原則。如需如何建立 KMS 金鑰的詳細資訊，請參閱AWS Key Management Service 開發人員指南中的建立金鑰。

如果您打算使用 S/4 Hana 資料連線，請確定您提供的 KMS 金鑰具有相關聯值為 true 的aws-supply-chain-access標籤。

6. (選擇性) 在 [執行個體標籤] 下，選擇 [新增標籤]，為您的執行個體指派標籤。您可以使用這些標籤來識別您的執行個體。如需有關標籤的資訊，請參閱建立標籤。
7. 選擇 建立執行個體。

   建立 AWS Supply Chain 執行個體大約需要 2 到 3 分鐘。建立執行個體之後， AWS Supply Chain 儀表板上的 [狀態] 欄位會顯示為 [使用中]。
8. 建立 AWS Supply Chain 執行個體後，請更新您的 KMS 政策 AWS Supply Chain 以允許存取金 AWS KMS 鑰。

> **Note**
>
> 將 *YourInstanceID* 取代為您的 AWS Supply Chain 執行個體 ID。您可以在 AWS Supply Chain 主控台儀表板上找到您的執行個體 ID。

```
        {
    "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": "*"
},
{
    "Sid": "Enable ASC to backfill KMS permissions",
    "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":"YourKmsKeyArn"
}
```

啟用 IAM 身分識別中心

開始使用之前 AWS Supply Chain，您必須連線至身分識別來源。如需詳細資訊，請參閱 IAM 使用者指南中的開始使用 IAM。

在 IAM 身分中心新增使用者

您可以管理 AWS Supply Chain 使用 IAM 身分中心服務的使用者。IAM 身分中心是雲端型 IAM 身分中心服務，可讓您輕鬆地集中管理 IAM 身分中心存取所有 AWS 帳戶 和雲端應用程式。若要新增 IAM 使用者，請參閱 IAM 使用者指南中的在 AWS 帳戶中建立 IAM 使用者。

如需建立 IAM 使用者群組的詳細資訊，請參閱 IAM 使用者指南中的建立 IAM 使用者群組。

> **Note**
>
> 若要將使用者新增至 AWS Supply Chain，使用者必須是 IAM 身分中心群組的一員。

選擇 AWS Supply Chain 應用程式擁有者

> **Note**
>
> 身為 AWS 主控台管理員，您正在選擇 AWS Supply Chain 應用程式擁有者來管理 AWS Supply Chain Web 應用程式存取權。 AWS Supply Chain 應用程式擁有者可以新增或移除 AWS Supply Chain Web 應用程式的使用者權限角色。

建立執行個體並連線身分識別來源之後，請依照下列步驟選擇 AWS Supply Chain 應用程式擁有者。

1. 在 AWS Supply Chain 主控台儀表板的應用程式擁有者下，選擇指派應用程式擁有者。
2. 在選取應用程式擁有者下，選取將作為應用 AWS Supply Chain 程式擁有者的使用者。您只能搜尋使用者名稱，而且會顯示符合搜尋條件的使用者。

   若要新增更多使用者，請選擇 [前往 IAM 身分中心]。如需有關新增使用者的詳細資訊，請參閱在 IAM 身分中心新增使用者和如需使用者權限角色的詳細資訊，請參閱使用者權限角色。

> **Note**
>
> 您一次只能從 AWS Supply Chain 主控台新增一個使用者。您無法在中新增群組做為應用程式擁有者 AWS Supply Chain。

3. 選擇「傳送邀請」。

   在 AWS Supply Chain 控制台儀表板上，您將看到應用程序所有者下列出的用戶。

4. 選擇「管理於」 AWS Supply Chain以在 AWS Supply Chain Web 應用程式中新增和移除使用者。

指派群組

身為應用程式擁有者或 AWS Supply Chain 管理員，您只能將屬於 IAM 身分中心群組的使用者新增到 AWS Supply Chain。

1. 在 AWS Supply Chain 主控台儀表板的 [群組] 下，選擇 [指派群組]。

   便會顯示「群組」頁面。

2. 在群組名稱下，選取具有可存取 AWS Supply Chain 之使用者的群組，然後選擇指派。

   您將在 AWS Supply Chain 儀表板中的「群組」下看到列出的群組。

3. 您可以選擇「管理群組」，在 IAM 身分中心新增群組。將群組新增至 IAM 身分中心後，該群組就會列在中的群組名稱下 AWS Supply Chain。

登入 AWS 供應鏈 Web 應用程式

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

1. 您可以選擇電子郵件中的連結，或在 AWS Supply Chain 主控台儀表板的子網域下選擇 Web URL。

   AWS Supply ChainWeb 應用程式登入頁面隨即出現。

2. 輸入 AWS IAM 身分中心使用者登入資料，然後選擇 [登入]。

第一 AWS Supply Chain 次登入

> **Note**
>
> 只有在您第一次登入時，系統才會要求您完成帳戶和組織的個人檔案。

以 AWS Supply Chain 系統管理員身分登入 AWS Supply Chain Web 應用程式之後，請依照下列步驟完成設定。

1. 在 [完成您的個人檔案] 頁面上，輸入您的 Job 稱和時區。選擇下一步。
2. 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。
3. 在 [設定您的團隊成員在] AWS Supply Chain頁面上，選取您想要存取 AWS Supply Chain Web 應用程式的使用者。選擇 Invite Users (邀請使用者)。如需如何將使用者新增至 IAM 身分中心的相關資訊，請參閱在 IAM 身分中心新增使用者。如需 AWS Supply Chain 使用者權限角色的資訊，請參閱使用者權限角色。
4. 如果您想稍後新增使用者，可以選擇 [立即略過]。

   便會顯示「上線完成」頁面。
5. 您新增的每位使用者都會收到一封電子郵件訊息，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。
6. 選擇「繼續前往首頁」以檢視 AWS Supply Chain 儀表板。

更新您的帳戶設定檔

您可以隨時在 AWS Supply Chain 網上應用程式上更新您的帳戶資料。請按照以下步驟更新帳戶。

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。

   會出現「帳戶設定檔」頁面。
3. 更新帳戶資訊，然後選擇 [儲存]。

更新您的組織設定檔

您可以隨時在 AWS Supply Chain Web 應用程式上更新組織設定檔。請遵循下列步驟來更新組織設定檔。

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」。

   會出現「組織設定檔」頁面。
3. 更新組織「圖誌」或「總部」位置，然後選擇「儲存」。

使用者權限角色

AWS Supply Chain 身為系統管理員，您可以使用預設的使用者權限角色或建立自訂權限角色。 AWS Supply Chain 具有下列預設使用者權限角色：

- 管理員 — 建立、檢視和管理所有資料和使用者權限的存取權。
- 數據分析師 — 創建，查看和管理所有數據連接的訪問權限。
- 庫存管理器 — 創建，查看和管理見解的訪問權限。
- 供需規劃員 — 建立、檢視及管理預測、修訂及公佈需求計劃的存取權。
- 合作夥伴資料管理員 — 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的存取權。
- 供給供需規劃員 — 管理與檢視供給計劃的存取權。

> **Note**
>
> AWS Supply Chain 身為管理員，在您新增使用者之前，請注意下列事項：
>
> - 每個預設使用者權限角色均使用一組權限定義。您可以將使用者新增至預設使用者權限角色，或建立自訂權限角色。
> - 一位使用者只能指派給一個使用者權限角色。
> - 您無法編輯或刪除預設的使用者權限角色。
> - 當您編輯您建立的自訂權限角色時，自訂權限角色下所有使用者的權限都會更新。
> - 當您刪除您建立的自訂權限角色時，自訂權限角色下的所有使用者都將失去存取權 AWS Supply Chain。

- 中不支援新增群組 AWS Supply Chain。

主題

新增使用者

> **Note**
>
> 在新增使用者之前，請確定該使用者屬於 IAM 身分中心群組，且群組已指派給該群組 AWS Supply Chain。

AWS Supply Chain 身為管理員，您可以新增使用者以存取 AWS Supply Chain Web 應用程式。請依照下列步驟新增使用者。

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 [權限]，然後選擇 [使用者]。

   便會顯示「管理使用者」頁。
3. 選擇「新增使用者」。

   便會顯示「新增使用者」頁。
4. 在 [新增使用者] 下拉式功能表中，選取使用者，然後在 [選取角色] 下選取使用者的角色。
5. 選擇新增。

更新使用者權限

您可以更新目前使用者的使 AWS Supply Chain 用者權限角色。請依照下列步驟更新使用者權限角色。

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 [權限]，然後選擇 [使用者]。

   便會顯示「管理使用者」頁。

3. 在 [管理使用者] 頁面上，選取您要更新其使用者權限角色的使用者或群組，然後從 [權限角色] 下拉式功能表中，選取下列其中一個權限角色：

   > **Note**
   >
   > AWS Supply Chain 儀表板會根據您指派的角色權限自訂。如需詳細資訊，請參閱 建立自訂使用者權限角色。

   - 管理員 — 建立、檢視和管理所有資料和使用者權限的存取權。
   - 數據分析師 — 創建，查看和管理所有數據連接的訪問權限。
   - 庫存管理器 — 創建，查看和管理見解的訪問權限。
   - 供需規劃員 — 建立、檢視及管理預測、修訂及公佈需求計劃的存取權。

4. 選擇儲存。

刪除使用者

AWS Supply Chain 身為管理員，您可以從 AWS Supply Chain Web 應用程式中刪除使用者。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 [權限]，然後選擇 [使用者]。

   便會顯示「管理使用者」頁。

3. 在「管理使用者」頁面上，選取要刪除的使用者，然後選擇「刪除」圖示。

建立自訂使用者權限角色

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

> **Note**
>
> 如果您的執行個體已連線至資料來源，則只能在「位置存取」和「產品存取」下選擇產品和地點。例如，您可以建立自訂管理員使用者，只是為了管理位於西雅圖位置的鱷梨，或建立 Insight 使用者只是為了管理西雅圖位置的鱷梨洞察。

1. 在 AWS Supply Chain 儀表板的左側導覽窗格中，選擇 [設定] 圖示。選擇 [權限]，然後選擇 [權限角色]。

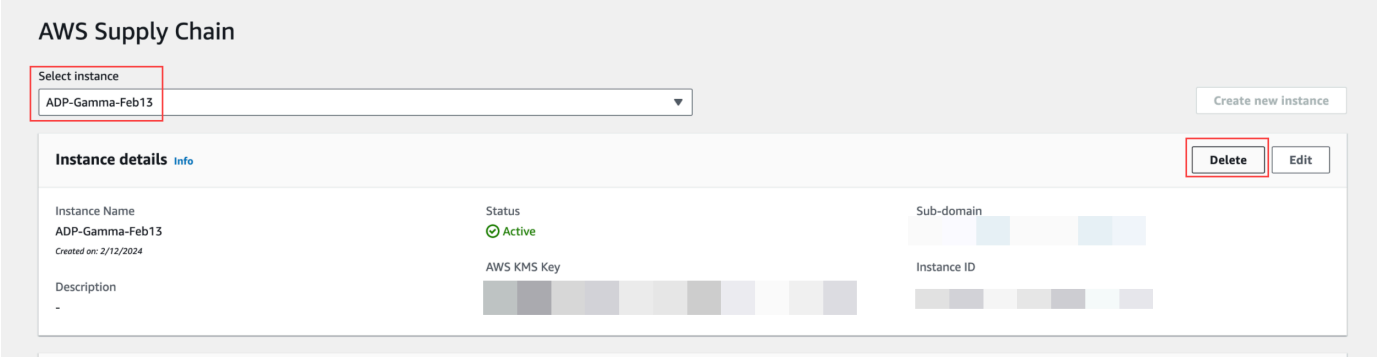
   [權限角色] 頁面隨即出現。
2. 選擇 Create New Role (建立新角色)。
3. 在 [管理權限角色] 頁面的 [角色名稱] 下，輸入名稱。
4. 移動滑桿以選取使用者權限角色。
   - 管理 — 指派具有管理權限的使用者可以新增、編輯和管理資訊。
   - 檢視 — 指派具有檢視權限的使用者只能檢視目前的資訊。
5. 在「位置存取」下，在搜尋列中鍵入時搜尋「區域」，然後選取「區域」。
6. 在「產品存取」下，在搜尋列中鍵入時搜尋產品，然後選取產品。
7. 選擇儲存。

刪除執行個體

若要刪除執行個體，請使用下列步驟。

> **Note**
>
> 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。
2. 在 AWS Supply Chain 主控台儀表板中，從下拉式清單中選取您要刪除的執行個體。



3. 選擇刪除。
4. 在 [刪除 AWS Supply Chain 執行個體] 頁面的 [確認] 底下，輸入**delete**確認您要刪除執行個體。
5. 選擇刪除。執行個體刪除開始，一旦執行個體被刪除，您將看到一則確認訊息。

中的安全性 AWS Supply Chain

雲安全 AWS 是最高的優先級。身為 AWS 客戶，您可以從資料中心和網路架構中獲益，這些架 AWS 構是為了滿足對安全性最敏感的組織的需求而建置的。

安全是您和您之間的共同責任 AWS。共同責任模型將其描述為雲端的安全性和雲端中的安全性：

- 雲端的安全性 — AWS 負責保護 AWS 服務 中執行的基礎架構 AWS 雲端。 AWS 還為您提供可以安全使用的服務。在 AWS 合規計劃中，第三方稽核員會定期測試並驗證我們的安全功效。若要深入瞭解適用於的規範遵循計劃 AWS Supply Chain，請參閱合規計劃的AWS 服務範圍範圍)。
- 雲端中的安全性 — 您使用的決定了 AWS 服務 您的責任。您還需要對其他因素負責。包括數據的敏感性，您的要求以及適用的法律和法規。

本文件可協助您瞭解如何在使用時套用共同責任模型 AWS Supply Chain。下列主題說明如何設定 AWS Supply Chain 以符合安全性與合規性目標。您還將學習如何使用其 AWS 服務 他幫助您監控和保護 AWS Supply Chain 資源的其他方法。

主題

- 資料保護 AWS Supply Chain
- 使 AWS Supply Chain 用介面端點存取 (AWS PrivateLink)
- 適用於 IAM 的 AWS Supply Chain
- AWS Supply Chain 的 AWS 受管政策
- AWS Supply Chain 的合規驗證
- AWS Supply Chain 中的恢復能力
- 記錄和監控 AWS Supply Chain

資料保護 AWS Supply Chain

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

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

- 每個帳戶均要使用多重要素驗證 (MFA)。
- 使用 SSL/TLS 與 AWS 資源進行通訊。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 使用設定 API 和使用者活動記錄 AWS CloudTrail。
- 使用 AWS 加密解決方案以及其中的所有默認安全控制 AWS 服務。
- 使用進階的受管安全服務 (例如 Amazon Macie)，協助探索和保護儲存在 Amazon S3 的敏感資料。
- 如果您在透過命令列介面或 API 存取時需要經 AWS 過 FIPS 140-2 驗證的加密模組，請使用 FIPS 端點。如需有關 FIPS 和 FIPS 端點的更多相關資訊，請參閱聯邦資訊處理標準 (FIPS) 140-2 概觀。

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

AWS Supply Chain處理的資料

為了限制特定 AWS 供應鏈執行環境的授權使用者可存取的資料，供應 AWS 鏈中持有的資料會由您的 AWS 帳戶識別碼與 AWS 供應鏈執行環境 ID 隔離。

AWS Supply Chain 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，以及存貨詳細資訊。

退出偏好

我們可能會使用和存放由 AWS Supply ChainAWS 服務條款中所述處理的「您的內容」。如果您想要選擇退出 AWS Supply Chain 以使用或存放您的內容，可以在 AWS Organizations 中建立退出政策。如需建立退出原則的詳細資訊，請參閱 AI 服務退出原則語法和範例。

靜態加密

分類為 PII 的聯絡人資料或代表儲存客戶內容的資料 AWS Supply Chain，會使用具有時間限制且專屬於執行個體的金鑰，在靜態時 (亦即在儲存、儲存或儲存至磁碟之前) 加密。 AWS Supply Chain

Amazon S3 伺服器端加密可使用每個客戶帳戶獨有的資 AWS Key Management Service 料金鑰來加密所有主控台和 Web 應用程式資料。如需相關資訊 AWS KMS keys，請參閱什麼是 AWS Key Management Service？ 在 AWS Key Management Service 開發人員指南中。

> **Note**
>
> AWS Supply Chain 功能「供應計劃」和「N 層能見度」不支援 data-at-rest 使用提供的 KMS-CMK 進行加密。

傳輸中加密

與 AWS 供應鏈交換的資料會在使用者的網頁瀏覽器與 AWS 供應鏈之間的傳輸過程中，使用業界標準的 TLS 加密保護。

金鑰管理

AWS Supply Chain 部分支持 KMS-CMK。

如需在中更新 AWS KMS 金鑰的相關資訊 AWS Supply Chain，請參閱建立執行個體。

網際網路流量隱私權

> **Note**
>
> AWS Supply Chain 不支持 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 會將請求路由傳送至 VPC， AWS Supply Chain 並將回應路由傳回至 VPC。如需詳細資訊，請參閱 VPC 使用手冊中的 VPC 端點。

如何 AWS Supply Chain 使用補助金 AWS KMS

AWS Supply Chain 需要授權才能使用您的客戶管理金鑰。

AWS Supply Chain 會使用CreateInstance作業期間傳遞的 AWS KMS 金鑰建立數個授權。 AWS Supply Chain 透過將CreateGrant請求傳送至，以代表您建立授權 AWS KMS。中的授 AWS Supply Chain 權 AWS KMS 用於授予客戶帳戶中 AWS KMS 金鑰的存取權。

> **Note**
>
> AWS Supply Chain 使用它自己的授權機制。將使用者新增至之後 AWS Supply Chain，您無法拒絕使用該 AWS KMS 策略列出相同的使用者。

AWS Supply Chain 將授權用於以下項目：

- 傳送要GenerateDataKey求以 AWS KMS 加密執行個體中儲存的資料。
- 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、和RetireGrant許可 CreateGrant，以便在將資料傳送到 Amazon Forecast 等其他 AWS 服務時確保資料安全。

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。如果這樣做，將 AWS Supply Chain 無法存取由客戶管理金鑰加密的任何資料，這會影響依賴該資料的作業。

監控您的加密 AWS Supply Chain

下列範例是針對EncryptGenerateDataKey、和監控呼叫Decrypt的 KMS 作業以存取由 AWS Supply Chain 客戶管理金鑰加密之資料的 AWS CloudTrail 事件：

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"
}
```

使 AWS Supply Chain 用介面端點存取 (AWS PrivateLink)

您可以使 AWS PrivateLink 用在 VPC 和 AWS Supply Chain. 之間建立私人連線。您可以 AWS Supply Chain 像在 VPC 中一樣進行存取，而無需使用網際網路閘道、NAT 裝置、VPN 連線或 AWS Direct Connect 連線。VPC 中的執行個體不需要公用 IP 位址即可存取 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 AWS PrivateLink中的 AWS 服務 透過存取。

的注意事項 AWS Supply Chain

設定的介面端點之前 AWS Supply Chain，請先檢閱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

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

建立 AWS Supply Chain 使用下列服務名稱的介面端點：

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

如果您為介面端點啟用私有 DNS，您可以 AWS Supply Chain 使用其預設的區域 DNS 名稱向 API 要求。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。預設端點策略允許 AWS Supply Chain 透過介面端點進行完整存取。若要控制允許 AWS Supply Chain 從您的 VPC 存取，請將自訂端點原則附加到介面端點。

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
- 可在其上執行動作的資源

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：用於動作的 VPC 端點原則 AWS Supply Chain

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 IAM 的 AWS Supply Chain

AWS Identity and Access Management (IAM) 可協助管理員安全地控制 AWS 資源存取權。 AWS 服務 IAM 管理員控制哪些人可以驗證 (登入) 和授權 (具有權限) 以使用 AWS Supply Chain 資源。您可以使用 IAM AWS 服務 ，無需額外付費。

主題

- 物件
- 使用身分驗證
- 使用政策管理存取權
- 如何與 IAM AWS Supply Chain 搭配使用
- AWS Supply Chain的身分型政策範例
- 疑難排解 AWS Supply Chain 身分和存取

物件

您使用 AWS Identity and Access Management (IAM) 的方式會有所不同，具體取決於您在進行的工作 AWS Supply Chain。

服務使用者 — 如果您使用 AWS Supply Chain 服務執行工作，則管理員會為您提供所需的認證和權限。當您使用更多 AWS Supply Chain 功能來完成工作時，您可能需要其他權限。了解存取的管理方式可協助您向管理員請求正確的許可。若您無法存取 AWS Supply Chain中的某項功能，請參閱 疑難排解 AWS Supply Chain 身分和存取。

服務管理員 — 如果您負責公司的 AWS Supply Chain 資源，您可能擁有完整的存取權 AWS Supply Chain。決定您的服務使用者應該存取哪些 AWS Supply Chain 功能和資源是您的工作。接著，您必須將請求提交給您的 IAM 管理員，來變更您服務使用者的許可。檢閱此頁面上的資訊，了解 IAM 的基本概念。若要進一步瞭解貴公司如何搭配使用 IAM AWS Supply Chain，請參閱如何與 IAM AWS Supply Chain 搭配使用。

IAM 管理員：如果您是 IAM 管理員，建議您掌握如何撰寫政策以管理 AWS Supply Chain存取權的詳細資訊。若要檢視可在 IAM 中使用的 AWS Supply Chain 基於身分的政策範例，請參閱。AWS Supply Chain的身分型政策範例

使用身分驗證

驗證是您 AWS 使用身分認證登入的方式。您必須以 IAM 使用者身分或假設 IAM 角色進行驗證 (登入 AWS)。 AWS 帳戶根使用者

您可以使用透過 AWS 身分識別來源提供的認證，以聯合身分識別身分登入。 AWS IAM Identity Center (IAM 身分中心) 使用者、貴公司的單一登入身分驗證，以及您的 Google 或 Facebook 登入資料都是聯合身分識別的範例。您以聯合身分登入時，您的管理員先前已設定使用 IAM 角色的聯合身分。當您使 AWS 用同盟存取時，您會間接擔任角色。

根據您的使用者類型，您可以登入 AWS Management Console 或 AWS 存取入口網站。如需有關登入的詳細資訊 AWS，請參閱《AWS 登入 使用指南》 AWS 帳戶中的如何登入您的。

如果您 AWS 以程式設計方式存取，請 AWS 提供軟體開發套件 (SDK) 和命令列介面 (CLI)，以使用您的認證以加密方式簽署要求。如果您不使用 AWS 工具，則必須自行簽署要求。如需使用建議的方法自行簽署請求的詳細資訊，請參閱 IAM 使用者指南中的簽署 AWS API 請求。

無論您使用何種身分驗證方法，您可能都需要提供額外的安全性資訊。例如， AWS 建議您使用多重要素驗證 (MFA) 來增加帳戶的安全性。如需更多資訊，請參閱 AWS IAM Identity Center 使用者指南中的多重要素驗證和 IAM 使用者指南中的在 AWS中使用多重要素驗證 (MFA)。

AWS 帳戶 根使用者

當您建立時 AWS 帳戶，您會從一個登入身分開始，該身分可完整存取該帳戶中的所有資源 AWS 服務和資源。此身分稱為 AWS 帳戶 root 使用者，可透過使用您用來建立帳戶的電子郵件地址和密碼登入來存取。強烈建議您不要以根使用者處理日常任務。保護您的根使用者憑證，並將其用來執行只能由根使用者執行的任務。如需這些任務的完整清單，了解需以根使用者登入的任務，請參閱 IAM 使用者指南中的需要根使用者憑證的任務。

聯合身分

最佳作法是要求人類使用者 (包括需要系統管理員存取權的使用者) 使用與身分識別提供者的同盟，才能使用臨時認證 AWS 服務 來存取。

聯合身分識別是來自企業使用者目錄的使用者、Web 身分識別提供者、Identi ty Center 目錄，或使用透過身分識別來源提供的認證進行存取 AWS 服務 的任何使用者。 AWS Directory Service同盟身分存取時 AWS 帳戶，他們會假設角色，而角色則提供臨時認證。

對於集中式存取權管理，我們建議您使用 AWS IAM Identity Center。您可以在 IAM Identity Center 中建立使用者和群組，也可以連線並同步到自己身分識別來源中的一組使用者和群組，以便在所有應用

程式 AWS 帳戶 和應用程式中使用。如需 IAM Identity Center 的詳細資訊，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 使用者是您內部的身分，具 AWS 帳戶 有單一人員或應用程式的特定許可。建議您盡可能依賴暫時憑證，而不是擁有建立長期憑證 (例如密碼和存取金鑰) 的 IAM 使用者。但是如果特定使用案例需要擁有長期憑證的 IAM 使用者，建議您輪換存取金鑰。如需更多資訊，請參閱 IAM 使用者指南中的為需要長期憑證的使用案例定期輪換存取金鑰。

IAM 群組是一種指定 IAM 使用者集合的身分。您無法以群組身分簽署。您可以使用群組來一次為多名使用者指定許可。群組可讓管理大量使用者許可的程序變得更為容易。例如，您可以擁有一個名為 IAMAdmins 的群組，並給予該群組管理 IAM 資源的許可。

使用者與角色不同。使用者只會與單一人員或應用程式建立關聯，但角色的目的是在由任何需要它的人員取得。使用者擁有永久的長期憑證，但角色僅提供暫時憑證。如需進一步了解，請參閱IAM 使用者指南中的建立 IAM 使用者 (而非角色) 的時機。

IAM 角色

IAM 角色是您 AWS 帳戶 內部具有特定許可的身分。它類似 IAM 使用者，但不與特定的人員相關聯。您可以切換角色，在中暫時擔任 IAM 角色。 AWS Management Console 您可以透過呼叫 AWS CLI 或 AWS API 作業或使用自訂 URL 來擔任角色。如需使用角色的方法詳細資訊，請參閱 IAM 使用者指南中的使用 IAM 角色。

使用暫時憑證的 IAM 角色在下列情況中非常有用：

- 聯合身分使用者存取 — 如需向聯合身分指派許可，請建立角色，並為角色定義許可。當聯合身分進行身分驗證時，該身分會與角色建立關聯，並獲授予由角色定義的許可。如需有關聯合角色的相關資訊，請參閱 IAM 使用者指南中的為第三方身分提供者建立角色。如果您使用 IAM Identity Center，則需要設定許可集。為控制身分驗證後可以存取的內容，IAM Identity Center 將許可集與 IAM 中的角色相關聯。如需有關許可集的資訊，請參閱 AWS IAM Identity Center 使用者指南中的許可集。
- 暫時 IAM 使用者許可 – IAM 使用者或角色可以擔任 IAM 角色來暫時針對特定任務採用不同的許可。
- 跨帳戶存取權：您可以使用 IAM 角色，允許不同帳戶中的某人 (信任的主體) 存取您帳戶的資源。角色是授予跨帳戶存取權的主要方式。但是，對於某些策略 AWS 服務，您可以將策略直接附加到資源（而不是使用角色作為代理）。若要了解跨帳戶存取角色和以資源為基礎的政策之間的差異，請參閱 IAM 使用者指南中的 IAM 中的跨帳戶資源存取。

- 跨服務訪問 — 有些 AWS 服務 使用其他 AWS 服務功能。例如，當您在服務中進行呼叫時，該服務通常會在 Amazon EC2 中執行應用程式或將物件儲存在 Amazon Simple Storage Service (Amazon S3) 中。服務可能會使用呼叫主體的許可、使用服務角色或使用服務連結角色來執行此作業。
  - 轉寄存取工作階段 (FAS) — 當您使用 IAM 使用者或角色在中執行動作時 AWS，您會被視為主體。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS 會使用主體呼叫的權限 AWS 服務，並結合要求 AWS 服務 向下游服務發出要求。只有當服務收到需要與其 AWS 服務 他資源互動才能完成的請求時，才會發出 FAS 請求。在此情況下，您必須具有執行這兩個動作的許可。如需提出 FAS 請求時的政策詳細資訊，請參閱《轉發存取工作階段》。
  - 服務角色 – 服務角色是服務擔任的 IAM 角色，可代表您執行動作。IAM 管理員可以從 IAM 內建立、修改和刪除服務角色。如需詳細資訊，請參閱 IAM 使用者指南中的建立角色以委派許可給 AWS 服務服務。
  - 服務連結角色 — 服務連結角色是連結至. AWS 服務服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的中， AWS 帳戶 且屬於服務所有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。
- 在 Amazon EC2 上執行的應用程式 — 您可以使用 IAM 角色來管理在 EC2 執行個體上執行的應用程式以及發出 AWS CLI 或 AWS API 請求的臨時登入資料。這是在 EC2 執行個體內儲存存取金鑰的較好方式。若要將 AWS 角色指派給 EC2 執行個體並提供給其所有應用程式，請建立連接至執行個體的執行個體設定檔。執行個體設定檔包含該角色，並且可讓 EC2 執行個體上執行的程式取得暫時憑證。如需詳細資訊，請參閱 IAM 使用者指南中的利用 IAM 角色來授予許可給 Amazon EC2 執行個體上執行的應用程式。

如需了解是否要使用 IAM 角色或 IAM 使用者，請參閱 IAM 使用者指南中的建立 IAM 角色 (而非使用者) 的時機。

使用政策管理存取權

您可以透 AWS 過建立原則並將其附加至 AWS 身分識別或資源來控制中的存取。原則是一個物件 AWS ，當與身分識別或資源相關聯時，會定義其權限。 AWS 當主參與者 (使用者、root 使用者或角色工作階段) 提出要求時，評估這些原則。政策中的許可決定是否允許或拒絕請求。大多數原則會 AWS 以 JSON 文件的形式儲存在中。如需 JSON 政策文件結構和內容的詳細資訊，請參閱 IAM 使用者指南中的 JSON 政策概觀。

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

預設情況下，使用者和角色沒有許可。若要授予使用者對其所需資源執行動作的許可，IAM 管理員可以建立 IAM 政策。然後，管理員可以將 IAM 政策新增至角色，使用者便能擔任這些角色。

IAM 政策定義該動作的許可，無論您使用何種方法來執行操作。例如，假設您有一個允許 `iam:GetRole` 動作的政策。具有該原則的使用者可以從 AWS Management Console AWS CLI、或 AWS API 取得角色資訊。

身分型政策

身分型政策是可以附加到身分 (例如 IAM 使用者、使用者群組或角色) 的 JSON 許可政策文件。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。若要了解如何建立身分類型政策，請參閱 IAM 使用者指南中的建立 IAM 政策。

身分型政策可進一步分類成內嵌政策或受管政策。內嵌政策會直接內嵌到單一使用者、群組或角色。受管理的策略是獨立策略，您可以將其附加到您的 AWS 帳戶. 受管政策包括 AWS 受管政策和客戶管理的策略。如需了解如何在受管政策及內嵌政策間選擇，請參閱 IAM 使用者指南中的在受管政策和內嵌政策間選擇。

資源型政策

資源型政策是連接到資源的 JSON 政策文件。資源型政策的最常見範例是 IAM 角色信任政策和 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下執行的動作。您必須在資源型政策中指定主體。主參與者可以包括帳戶、使用者、角色、同盟使用者或。 AWS 服務

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

存取控制清單 (ACL)

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

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

其他政策類型

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

- 許可界限 – 許可範圍是一種進階功能，可供您設定身分型政策能授予 IAM 實體 (IAM 使用者或角色) 的最大許可。您可以為實體設定許可界限。所產生的許可會是實體的身分型政策和其許可界限的交集。會在 `Principal` 欄位中指定使用者或角色的資源型政策則不會受到許可界限限制。所有這類政

策中的明確拒絕都會覆寫該允許。如需許可界限的詳細資訊，請參閱 IAM 使用者指南中的 IAM 實體許可界限。

- 服務控制策略（SCP）— SCP 是 JSON 策略，用於指定中組織或組織單位（OU）的最大權限。AWS Organizations AWS Organizations 是一種用於分組和集中管理您企業擁 AWS 帳戶 有的多個服務。若您啟用組織中的所有功能，您可以將服務控制政策 (SCP) 套用到任何或所有帳戶。SCP 限制成員帳戶中實體的權限，包括每個 AWS 帳戶根使用者帳戶。如需 Organizations 和 SCP 的詳細資訊，請參閱 AWS Organizations 使用者指南中的 SCP 運作方式。
- 工作階段政策 – 工作階段政策是一種進階政策，您可以在透過編寫程式的方式建立角色或聯合使用者的暫時工作階段時，作為參數傳遞。所產生工作階段的許可會是使用者或角色的身分型政策和工作階段政策的交集。許可也可以來自資源型政策。所有這類政策中的明確拒絕都會覆寫該允許。如需詳細資訊，請參閱 IAM 使用者指南中的工作階段政策。

多種政策類型

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

如何與 IAM AWS Supply Chain 搭配使用

在您使用 IAM 管理存取權限之前 AWS Supply Chain，請先了解哪些 IAM 功能可搭配使用 AWS Supply Chain。

您可以搭配使用的 IAM 功能 AWS Supply Chain

IAM 功能	AWS Supply Chain 支持
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

IAM 功能	AWS Supply Chain 支持
轉送存取工作階段 (FAS)	是
服務角色	是
服務連結角色	否

若要深入瞭解如何以 AWS Supply Chain 及其他 AWS 服務如何使用大多數 IAM 功能，請參閱 IAM 使用者指南中的搭配 IAM 使用的AWS 服務。

以身分識別為基礎的原則 AWS Supply Chain

支援身分型政策	是

身分型政策是可以連接到身分 (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。若要了解如何建立身分類型政策，請參閱《IAM 使用者指南》中的建立 IAM 政策。

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。您無法在身分型政策中指定主體，因為這會套用至連接的使用者或角色。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。

以身分識別為基礎的原則範例 AWS Supply Chain

若要檢視以 AWS Supply Chain 身分為基礎的原則範例，請參閱。AWS Supply Chain的身分型政策範例

以資源為基礎的政策 AWS Supply Chain

支援以資源基礎的政策	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。主參與者可以包括帳戶、使用者、角色、同盟使用者或。 AWS 服務

如需啟用跨帳戶存取權，您可以指定在其他帳戶內的所有帳戶或 IAM 實體，作為資源型政策的主體。新增跨帳戶主體至資源型政策，只是建立信任關係的一半。當主體和資源位於不同時 AWS 帳戶，受信任帳戶中的 IAM 管理員也必須授與主體實體 (使用者或角色) 權限，才能存取資源。其透過將身分型政策連接到實體來授與許可。不過，如果資源型政策會為相同帳戶中的主體授予存取，這時就不需要額外的身分型政策。如需詳細資訊，請參閱 IAM 使用者指南中的 IAM 中的跨帳戶資源存取。

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哪些內容。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。原則動作通常與關聯的 AWS API 作業具有相同的名稱。有一些例外狀況，例如沒有相符的 API 操作的僅限許可動作。也有一些作業需要政策中的多個動作。這些額外的動作稱為相依動作。

政策會使用動作來授予執行相關聯動作的許可。

中的策略動作在動作之前 AWS Supply Chain 使用下列前置詞：

```
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"
         ]
```

若要檢視以 AWS Supply Chain 身分為基礎的原則範例，請參閱。AWS Supply Chain的身分型政策範例

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哪些內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

Resource JSON 政策元素可指定要套用動作的物件。陳述式必須包含 Resource 或 NotResource 元素。最佳實務是使用其 Amazon Resource Name (ARN) 來指定資源。您可以針對支援特定資源類型的動作 (稱為資源層級許可) 來這麼做。

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

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

若要檢視以 AWS Supply Chain 身分為基礎的原則範例，請參閱。AWS Supply Chain的身分型政策範例

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哪些內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

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

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

您也可以在指定條件時使用預留位置變數。例如，您可以只在使用者使用其 IAM 使用者名稱標記時，將存取資源的許可授予該 IAM 使用者。如需更多資訊，請參閱 IAM 使用者指南中的 IAM 政策元素：變數和標籤。

AWS 支援全域條件金鑰和服務特定條件金鑰。若要查看所有 AWS 全域條件金鑰，請參閱《IAM 使用者指南》中的AWS 全域條件內容金鑰。

若要檢視以 AWS Supply Chain 身分為基礎的原則範例，請參閱。AWS Supply Chain的身分型政策範例

使用臨時登入資料 AWS Supply Chain

支援臨時憑證	是

當您使用臨時憑據登錄時，某些 AWS 服務 不起作用。如需其他資訊，包括哪些 AWS 服務 與臨時登入資料搭配AWS 服務 使用，請參閱 IAM 使用者指南中的 IAM。

如果您使用除了使用者名稱和密碼以外的任何方法登入，則您正在 AWS Management Console 使用臨時認證。例如，當您 AWS 使用公司的單一登入 (SSO) 連結存取時，該程序會自動建立暫時認證。當您以使用者身分登入主控台，然後切換角色時，也會自動建立臨時憑證。如需切換角色的詳細資訊，請參閱 IAM 使用者指南中的切換至角色 (主控台)。

您可以使用 AWS CLI 或 AWS API 手動建立臨時登入資料。然後，您可以使用這些臨時登入資料來存取 AWS。 AWS 建議您動態產生臨時登入資料，而非使用長期存取金鑰。如需詳細資訊，請參閱 IAM 中的暫時性安全憑證。

轉寄存取工作階段 AWS Supply Chain

支援轉寄存取工作階段 (FAS)	是

當您使用 IAM 使用者或角色在中執行動作時 AWS，您會被視為主體。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS 會使用主體呼叫的權限 AWS 服務，並結合要求 AWS 服務 向下游服務發出要求。只有當服務收到需要與其 AWS 服務 他資源互動才能完成的請求時，才會發出 FAS 請求。在此情況下，您必須具有執行這兩個動作的許可。如需提出 FAS 請求時的政策詳細資訊，請參閱《轉發存取工作階段》。

AWS Supply Chain的服務角色

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 服務服務。

> **Warning**
>
> 變更服務角色的權限可能會中斷 AWS Supply Chain 功能。只有在 AWS Supply Chain 提供指引時才編輯服務角色。

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. AWS 服務服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的中， AWS 帳戶 且屬於服務所有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。

如需建立或管理服務連結角色的詳細資訊 AWS 服務 ，請參閱使用 IAM。在表格中尋找服務，其中包含服務連結角色欄中的 Yes。選擇 Yes (是) 連結，以檢視該服務的服務連結角色文件。

AWS Supply Chain的身分型政策範例

依預設，使用者和角色沒有建立或修改 AWS Supply Chain 資源的權限。他們也無法使用 AWS 管理主控台、AWS Command Line Interface (AWS CLI) (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 JSON 政策文件範例建立 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

以身分識別為基礎的政策會決定某人是否可以建立、存取或刪除您帳戶中的 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 受管原則並邁向最低權限權限 — 若要開始將權限授與使用者和工作負載，請使用可授與許多常見使用案例權限的AWS 受管理原則。它們在您的 AWS 帳戶. 建議您透過定義特定於您使用案例的 AWS 客戶管理政策，進一步降低使用權限。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。您也可以使用條件來授與對服務動作的存取權 (如透過特定 AWS 服務) 使用 AWS CloudFormation。如需詳細資訊，請參閱 IAM 使用者指南中的 IAM JSON 政策元素：條件。
- 使用 IAM Access Analyzer 驗證 IAM 政策，確保許可安全且可正常運作 – IAM Access Analyzer 驗證新政策和現有政策，確保這些政策遵從 IAM 政策語言 (JSON) 和 IAM 最佳實務。IAM Access Analyzer 提供 100 多項政策檢查及切實可行的建議，可協助您編寫安全且實用的政策。如需更多資訊，請參閱 IAM 使用者指南中的 IAM Access Analyzer 政策驗證。
- 需要多因素身份驗證 (MFA) — 如果您的案例需要 IAM 使用者或根使用者 AWS 帳戶，請開啟 MFA 以獲得額外的安全性。如需在呼叫 API 操作時請求 MFA，請將 MFA 條件新增至您的政策。如需更多資訊，請參閱 IAM 使用者指南中的設定 MFA 保護的 API 存取。

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。

疑難排解 AWS Supply Chain 身分和存取

使用下列資訊可協助您診斷和修正使用和 IAM 時可能會遇到的 AWS Supply Chain 常見問題。

主題

- 我沒有執行動作的授權 AWS Supply Chain
- 我沒有授權執行 iam：PassRole
- 我想允許我以外的人訪 AWS 帳戶 問我的 AWS Supply Chain 資源

我沒有執行動作的授權 AWS Supply Chain

如果您 AWS Management Console 未獲授權執行操作，則必須聯繫管理員以尋求幫助。您的管理員是提供您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。

我沒有授權執行 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 允許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 沒有將角色傳遞至該服務的許可。

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

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

如果您需要協助，請聯絡您的 AWS 管理員。您的管理員提供您的簽署憑證。

我想允許我以外的人訪 AWS 帳戶 問我的 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：

- 若要瞭解是否 AWS Supply Chain 支援這些功能，請參閱如何與 IAM AWS Supply Chain 搭配使用。
- 若要了解如何提供對您所擁有資源 AWS 帳戶 的存取權，請參閱 IAM 使用者指南中您擁有的另一 AWS 帳戶 個 IAM 使用者提供存取權限。

- 若要了解如何將資源存取權提供給第三方 AWS 帳戶，請參閱 IAM 使用者指南中的提供第三方 AWS 帳戶 擁有的存取權。
- 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)。
- 若要了解跨帳戶存取使用角色和以資源為基礎的政策之間的差異，請參閱 IAM 使用者指南中的 IAM 中的跨帳戶資源存取。

AWS Supply Chain 的 AWS 受管政策

AWS 管理的政策是由 AWS 建立和管理的獨立政策。AWS 管理的政策的設計在於為許多常見使用案例提供許可，如此您就可以開始將許可指派給使用者、群組和角色。

請謹記，AWS 管理的政策可能不會授予您特定使用案例的最低權限許可，因為它們可供所有 AWS 客戶使用。我們建議您定義使用案例專屬的客戶管理政策，以便進一步減少許可。

您無法更改 AWS 管理的政策中定義的許可。如果 AWS 更新 AWS 管理的政策中定義的許可，更新會影響政策連接的所有主體身分 (使用者、群組和角色)。在推出新的 AWS 服務 或有新的 API 操作可供現有服務使用時，AWS 很可能會更新 AWS 管理的政策。

如需詳細資訊，請參閱《IAM 使用者指南》中的 AWS 受管政策。

AWS受管理策略： AWSSupplyChainFederationAdminAccess

AWSSupplyChainFederationAdminAccess 提供AWS Supply Chain聯合身分使用者對AWS Supply Chain應用程式的存取權，包括在AWS Supply Chain應用程式內執行動作所需的權限。該政策提供 IAM 身分中心使用者和群組的管理許可，並附加至由您建立AWS Supply Chain的角色。您不應將該 AWSSupplyChainFederationAdminAccess 政策附加到任何其他 IAM 實體。

雖然此原則可AWS Supply Chain透過 scn: * 權限提供所有存取權，但AWS Supply Chain角色會決定您的權限。該AWS Supply Chain角色僅包含必要的權限，並且沒有管理 API 的權限。

許可詳細資訊

此政策包含以下許可：

- Chime— 提供在 Amazon Chime 下建立或刪除使用者的存取權 AppInstance；提供管理頻道、頻道成員和仲裁者的存取權；提供將訊息傳送至頻道的存取權。Chime 作業的範圍是標記為「SCN」的應用程式執行個體。InstanceId
- AWS IAM Identity Center (AWS SSO)— 提供關聯和取消關聯使用者設定檔所需的許可，並列出與 IAM Identity Center 應用程式執行個體相關聯的設定
- 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；提供對流程標記和取消標記的存取，以及描述流程記錄。
- Amazon S3— 提供列出所有值區的存取權。使用資源 arn ARN: aw:s3:::-* 提 GetBucketLocation供 GetObject、、和 ListBucket 存取值區。 GetBucketPolicy PutObject aws-supply-chain-data
- SecretsManager— 提供建立密碼和更新密碼原則的存取權。
- KMS— 為 Amazon AppFlow 服務提供對列表密鑰和密鑰別名的訪問權限。提供 DescribeKey以索引鍵值標記的 KMS 金鑰 CreateGrant 和 ListGrants 權限 aws-suply-chain-access ：true；提供建立密碼和更新密碼原則的存取權。

  權限（公里：ListKeys，公里：ListAliases，公里：和 KMS：解密）不限於 Amazon GenerateDataKey AppFlow ，這些許可可可可可以授予您帳戶中的任何密AWS KMS鑰。

若要檢視此原則的權限，請參閱AWSSupplyChainFederationAdminAccess中的AWS Management Console。

AWS 管理的政策的 AWS Supply Chain 更新項目

下表列出AWS Supply Chain自此服務開始追蹤這些變更之後，AWS受管理策略的更新詳細資訊。如需有關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	日期
AWSSupplyChainFederationAdminAccess-更新的政策	AWS Supply Chain已更新受管政策，允許聯合身分使用者存取 IAM 身分中心中的 ListProfileAssociations 作業。	2023年11月01 日

變更	描述	日期
AWSSupplyChainFederationAdminAccess-更新的政策	AWS Supply Chain已更新受管政策，允許聯合身分使用者使用資源 arn arn: awn: s3:: aws-供應鏈資料 * 存取專用 S3 儲存貯體上的 PutObject 和 GetObject 操作。	2023 年 9 月 21 日
AWSSupplyChainFederationAdminAccess – 新政策	AWS Supply Chain已新增新原則，以允許同盟使用者存取應用AWS Supply Chain程式。這包括在應用程式中執行動作所需的AWS Supply Chain權限。	2023年3月01 日
AWS Supply Chain 已開始追蹤變更	AWS Supply Chain 已開始追蹤其 AWS 管理的政策的變更。	2023年3月01 日

AWS Supply Chain 的合規驗證

在多個 AWS 合規計劃中，第三方稽核人員會評估 AWS Supply Chain 的安全與合規。這些計劃包括 SOC、PCI、FedRAMP、HIPAA 等等。

如需定合規計AWS畫範圍範圍的AWS服務範圍範圍範圍範圍範圍。AWS 服務如需一般資訊，請參閱 AWS 合規計畫。

您可使用下載第三方稽核報告AWS Artifact。如需詳細資訊，請參閱 AWS Artifact 中的下載報告。

您公司的合規目標及適用AWS Supply Chain法律和法規目標及適用法律和法規計畫的機密性、您公司的合規目標及適用法律和法規。 AWS提供下列資源，以協助合規：

- 安全與合規快速入門指南 指南 — 這些部署指南討論架構考量，並提供在部署以安全性及合規為重心之基準AWS環境的步驟。
- HIPAA 安全與合規架構白皮書：本白皮書說明公司可如何運用 AWS 來建立 HIPAA 合規的應用程式。
- AWS 合規資源：這組手冊和指南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狀態評估資源 — 本指南評估資源組態對於內部實務、業界界界界界定實務、業界界界界界界定合規的合規狀態
- AWS Security Hub— 這AWS 服務可助您檢查是否符合安全產業界標準和最佳實務。AWS

AWS Supply Chain 中的恢復能力

AWS全球基礎設施是以可用區域為中心建置的。AWS 區域 AWS 區域提供多個實體分離和隔離的可用區域。它們以低延遲、高輸送量和高度備援聯網功能相互連結。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 與可用區域的詳細資訊，請參閱AWS全球基礎架構。

除了 AWS 全球基礎設施，AWS Supply Chain 還提供數種功能，可協助支援資料的彈性和備份需求。

記錄和監控 AWS Supply Chain

記錄和監控是維護 AWS 供應鏈及其他 AWS 解決方案的可靠性、可用性和效能的重要組成部分。AWS 提供 AWS CloudTrail 監控工具來監視 AWS 供應鏈、在發生錯誤時報告，並在適當時自動採取行動。

> **Note**
>
> 只從 AWS Supply Chain 主控台呼叫的 API 會在中擷取 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 地址，以及呼叫的發生時間。您可以在下面查看 AWS 供應鏈事件。如需詳細資訊，請參閱 AWS CloudTrail 使用者指南。

> **Note**
>
> 請注意以下內容 AWS Supply Chain：
>
> - 當您邀請無權存取的使用者時 AWS Supply Chain，這些使用者不會在他們從 Web 應用程式收到的通知中收到資訊。受邀的使用者會收到含有 Web 應用程式連結的電子郵件通知。如果他們具有必要的使用者權限，他們才能登入並檢視通知中的內容。

- 所有具有或沒有特定 Insight 使用者權限的使用者都可以檢視見解聊天訊息。
- 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. 您可以管理新增或移除使用者的使用者權限。如需使用者權限的詳細資訊，請參閱使用者權限角色。

AWS Supply Chain 資料事件 CloudTrail

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。依預設， CloudTrail 不會記錄資料事件。 CloudTrail 事件歷史記錄不會記錄數據事件。

資料事件需支付額外的費用。如需有關 CloudTrail 定價的詳細資訊，請參閱AWS CloudTrail 定價。

您可以使用 CloudTrail 主控台或 CloudTrail API 作業記錄 AWS Supply Chain 資源類型的資料事件。AWS CLI

- 若要使用 CloudTrail 主控台記錄資料事件，請建立追蹤或事件資料存放區以記錄資料事件，或更新現有追蹤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，選擇您要記錄其資料事件的資源類型。
  3. 選擇您要使用的記錄選取器範本。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，或建立自訂記錄選取器範本以篩選`readOnly`、`eventName`、和`resources.ARN`欄位。
- 若要使用記錄資料事件 AWS CLI，請配置`--advanced-event-selectors`參數以將`eventCategory`欄位設定為等於，`Data`且`resources.type`欄位等於資源類型值。您可以加入條件以篩選`readOnly`、`eventName`、和`resources.ARN`欄位的值。
  - 若要設定追蹤以記錄資料事件，請執行put-event-selectors命令。如需詳細資訊，請參閱使用 AWS CLI.
  - 若要規劃事件資料倉庫以記錄資料事件，請執行create-event-data-store指令以建立新的事件資料倉庫以記錄資料事件，或執行update-event-data-store指令來更新現有的事件資料倉庫。如需詳細資訊，請參閱使用 AWS CLI.

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

AWS Supply Chain 管理事件 CloudTrail

管理事件提供有關對您 AWS 帳戶中資源執行之管理作業的相關資訊。這些也稱為控制平面操作。依預設，會 CloudTrail 記錄管理事件。

AWS 供應鏈將所有控制平面操作記錄 CloudTrail 為管理事件。

AWS Supply Chain 網頁應用程式 API

本節中列出的 API 由 AWS Supply Chain 應用程式代表聯合身分使用者呼叫。這些 API 在 CloudTrail 日誌中不可見，並且不會在服務授權參考文檔中捕獲，請參閱AWS Supply Chain。這些 API 的存取權由 AWS Supply Chain 應用程式根據聯合使用者角色權限來控制。您不應該嘗試控制對這些 API 的訪問以防止解釋應用程序 AWS Supply Chain 。

使用者角色

下列 API 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 API 用於建立和管理資料湖中的資料流程和連線。

```
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
```

深入分析

Insights 應用程式會使用下列 API 來管理篩選器、監看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
```

需求計劃

中使用下列 API AWS Supply Chain 來建立和管理預測、需求計劃或工作簿。

```
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
```

供應計劃

在中使用下列 API AWS Supply Chain 來建立與管理供給計劃。

```
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
```

的配額 AWS Supply Chain

您的每個配額都 AWS 帳戶 有預設配額 (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。您可以要求增加設定為您帳戶層級的資源配額。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，請使用提高限制表單。

您 AWS 帳戶 有下列相關配額 AWS Supply Chain。

資源	預設	可調整
執行個體的數目 **Note** 您最多可以在一個 AWS 帳戶中建立 10 個執行個體。	10	否
Amazon S3 存儲桶的數量	100	否
AWS 帳戶內有效和待處理的邀請	30	是
AWS 帳戶內的資料請求	4,000	是
洞察每個監視清單的明細項目	1,000	否
帳戶 AWS 內每個執行個體的見解監視清單	1,000	是
帳戶內每位使用者的 AWS 深入分析監視清單	100	是

取得 AWS Supply Chain 的管理支援

如果您是管理員，且需要聯絡 AWS Supply Chain 支援部門，請選擇以下其中一個選項：

- 如果您有AWS Support帳戶，請轉到 Sup port 中心並提交票證。
- 開啟AWS Management Console並選擇「AWS供應鏈」、「Sup port」、「建立案例」。

提供下列資訊會很有幫助：

- 您的AWS供應鏈執行環境 ID/ARN。
- 您所在的AWS地區。
- 問題的詳細說明。

AWS Supply Chain 管理員指南的文件歷史記錄

下表說明的文件版本 AWS Supply Chain。

變更	描述	日期
KMS 政策更新	更新 KMS 政策以允許存 AWS Supply Chain 取您的金 AWS KMS 鑰。	2024年3月18日
PrivateLink 支持	您可以使 AWS Supply Chain 用界面端點 (AWS PrivateLink) 存取。	2024年2月26日
新增群組	使用者必須是 IAM 身分中心群組的一員才能存取 AWS Supply Chain。	2023 年 11 月 14 日
更新的 AWS 受管政策	AWS Supply Chain 已更新受管政策，允許聯合身分使用者存取 IAM 身分中心中的 ListProfileAssociations 作業。	2023 年 11 月 1 日
更新的 AWS 受管政策	AWS Supply Chain 更新受管政策，允許聯合身分使用者使用資源 arn arn: awn: s3:: aws 供應鏈資料 * 存取專用 Amazon S3 儲存貯體上的 PutObject 和 GetObject 操作。	2023 年 9 月 21 日
區域支援的更新資訊	AWS Supply Chain 亞太區域 (雪梨) 區域現在也支援「需求計劃」。	2023 年 9 月 12 日
使用 AWS 主控台選擇加入和選擇退出 AWS Supply Chain	AWS Supply Chain 使用者現在可以使用 AWS 主控台選擇加入和選擇退出，以 AWS Supply Chain 便在 AWS	2023 年 9 月 7 日

	Organizations 上使用或存放您的內容。	
區域支援的更新資訊	AWS Supply Chain 現在也支援亞太區域 (雪梨) 區域和歐洲 (愛爾蘭) 區域。	2023 年 7 月 19 日
更新有關如何聯絡 AWS Support 和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 受管理政策	AWS 「供應鏈」新增政策，允許聯合使用者存取「 AWS 供應鏈」應用模組，包括在「供應鏈」 AWS 應用模組中執行作業所需的權限。	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。