開始使用受限模式

Setup and administration

NetApp
April 26, 2024

目錄

開始使用受限模式

入門工作流程（受限模式）

準備您的環境、部署 Connector 及訂閱 BlueXP 、以受限模式開始使用 BlueXP 。

受限模式通常由州政府和地方政府及受管制公司使用、包括在 AWS GovCloud 和 Azure 政府地區部署。開始之前、您應該先瞭解 "BlueXP 帳戶"、 "連接器"和 "部署模式"。

1 **"準備部署"**

1. 準備符合 CPU 、 RAM 、磁碟空間、 Docker Engine 等需求的專用 Linux 主機。
2. 設定網路以提供目標網路的存取、手動安裝的輸出網際網路存取、以及用於日常存取的輸出網際網路。
3. 在雲端供應商中設定權限、以便在部署這些權限之後、將其與 Connector 執行個體建立關聯。

2 **"部署 Connector"**

1. 從雲端供應商的市場安裝 Connector 、或是在您自己的 Linux 主機上手動安裝軟體。
2. 開啟網頁瀏覽器並輸入 Linux 主機的 IP 位址、即可設定 BlueXP 。
3. 提供 BlueXP 先前設定的權限。

3 **"訂閱 BlueXP"**

從雲端供應商的市場訂閱 BlueXP 、即可按每小時費率（ PAYGO ）或透過年度合約支付 BlueXP 服務費用。

準備以受限模式進行部署

在受限模式下部署 BlueXP 之前、請先準備好您的環境。例如、您需要檢閱主機需求、準備網路、設定權限等。

步驟 1 ：瞭解受限模式的運作方式

開始之前、您應該先瞭解 BlueXP 在受限模式下的運作方式。

例如、您應該瞭解、您必須使用本機可從 BlueXP Connector 取得的瀏覽器型介面來安裝。您無法從透過 SaaS 層提供的網路型主控台存取 BlueXP 。

此外、並非所有 BlueXP 服務都可用。

"瞭解受限模式的運作方式"。

步驟 2 ：檢閱安裝選項

在受限模式中、您只能在雲端安裝 Connector 。提供下列安裝選項：

- 從 AWS Marketplace 取得
- 來自 Azure Marketplace
- 在您自己的 Linux 主機上手動安裝 Connector 、該主機在 AWS 、 Azure 或 Google Cloud 中執行

步驟 3 ：檢閱主機需求

Connector 軟體必須在符合特定作業系統需求、 RAM 需求、連接埠需求等的主機上執行。

當您從 AWS 或 Azure Marketplace 部署 Connector 時、映像會包含所需的作業系統和軟體元件。您只需選擇符合 CPU 和 RAM 需求的執行個體類型即可。

專用主機

與其他應用程式共用的主機不支援 Connector 。主機必須是專屬主機。

支援的作業系統

- Ubuntu 22.04 LTS
- CentOS 7.6、7.7、7.8及7.9
- Red Hat Enterprise Linux 7.6 、 7.7 、 7.8 和 7.9

  主機必須向 Red Hat Subscription Management 登錄。如果主機尚未登錄、則無法在 Connector 安裝期間存取儲存庫來更新所需的協力廠商軟體。

  這些作業系統的英文版本支援 Connector 。

Hypervisor

需要經認證可執行 Ubuntu 、 CentOS 或 Red Hat Enterprise Linux 的裸機或託管 Hypervisor 。

"Red Hat 解決方案：哪些 Hypervisor 已通過認證、可執行 Red Hat Enterprise Linux ？"

CPU

4 個核心或 4 個 vCPU

RAM

14 GB

AWS EC2 執行個體類型

符合上述 CPU 和 RAM 需求的執行個體類型。建議使用T3.xLarge。

Azure VM 大小

符合上述 CPU 和 RAM 需求的執行個體類型。我們建議使用 DS3 v2 。

Google Cloud 機器類型

符合上述 CPU 和 RAM 需求的執行個體類型。我們建議使用 n2 標準 4 。

Google Cloud支援Connector的VM執行個體、其作業系統可支援此連接器 "防護VM功能"

/opt 中的磁碟空間

必須有100 GiB的可用空間

/var.中的磁碟空間

必須提供20 GiB的空間

Docker引擎

安裝 Connector 之前、主機上需要 Docker Engine 。

- 支援的最低版本為 19.3.1 。
- 支援的最大版本為 25.0.0 。

"檢視安裝指示"

步驟 **4** ：準備網路

設定您的網路、讓 Connector 能夠管理公有雲環境中的資源和程序。除了連接器的虛擬網路和子網路之外、您還需要確保符合下列需求。

連線至目標網路

Connector 必須與您計畫管理儲存設備的位置建立網路連線。例如、您計畫部署 Cloud Volumes ONTAP 的 VPC 或 vnet 、或內部部署 ONTAP 叢集所在的資料中心。

準備網路以供使用者存取 **BlueXP** 主控台

在受限模式下、可從 Connector 存取 BlueXP 使用者介面。當您使用 BlueXP 使用者介面時、它會聯絡幾個端點來完成資料管理工作。從 BlueXP 主控台完成特定動作時、會從使用者的電腦聯絡這些端點。

端點	目的
https://signin.b2c.netapp.com	需要更新NetApp 支援網站 驗證（NSS）認證或新增新的NSS認證至BlueXP。
https://netapp-cloud-account.auth0.com https://cdn.auth0.com https://services.cloud.netapp.com	您的網頁瀏覽器會連線至這些端點、以便透過BlueXP進行集中式使用者驗證。
https://widget.intercom.io	產品內對談可讓您與 NetApp 雲端專家交談。

手動安裝期間聯絡的端點

當您在自己的 Linux 主機上手動安裝 Connector 時、 Connector 的安裝程式需要在安裝過程中存取下列 URL ：

- https://support.netapp.com
- https://mysupport.netapp.com
- https://cloudmanager.cloud.netapp.com/tenancy
- https://stream.cloudmanager.cloud.netapp.com
- https://production-artifacts.cloudmanager.cloud.netapp.com

- https://*.blob.core.windows.net
- https://cloudmanagerinfraprod.azurecr.io

  Azure 政府地區不需要此端點。

- https://occmclientinfragov.azurecr.us

  此端點僅在 Azure 政府地區需要使用。

主機可能會在安裝期間嘗試更新作業系統套件。主機可聯絡不同的鏡射站台、以取得這些 OS 套件。

用於日常營運的外傳網際網路存取

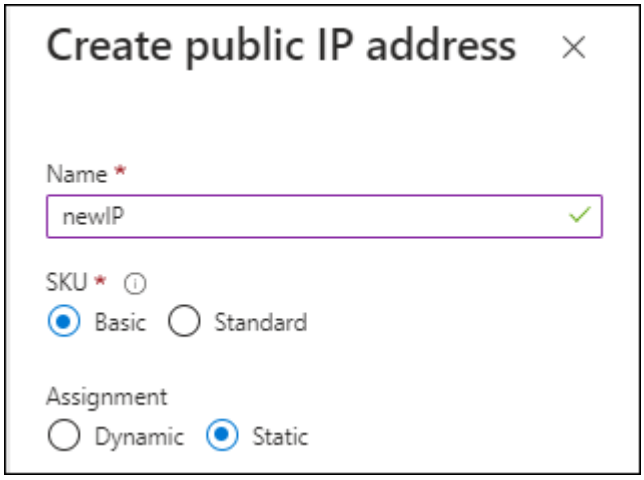
您部署Connector的網路位置必須具有傳出網際網路連線。連接器需要存取傳出網際網路、才能連絡下列端點、以便管理公有雲環境中的資源和程序。

端點	目的
AWS 服務（amazonaws.com): • CloudForation • 彈性運算雲端（EC2） • 身分識別與存取管理（IAM） • 金鑰管理服務（KMS） • 安全性權杖服務（STOS） • 簡易儲存服務（S3）	管理AWS中的資源。確切的端點取決於您使用的 AWS 區域。 "如需詳細資料、請參閱AWS文件"
https://management.azure.com https://login.microsoftonline.com https://blob.core.windows.net https://core.windows.net	管理Azure公共區域的資源。
https://management.usgovcloudapi.net https://login.microsoftonline.us https://blob.core.usgovcloudapi.net https://core.usgovcloudapi.net	管理Azure政府區域的資源。
https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn	管理Azure中國地區的資源。

端點	目的
https://www.googleapis.com/compute/v1/ https://compute.googleapis.com/compute/v1 https://cloudresourcemanager.googleapis.com/v1/projects https://www.googleapis.com/compute/beta https://storage.googleapis.com/storage/v1 https://www.googleapis.com/storage/v1 https://iam.googleapis.com/v1 https://cloudkms.googleapis.com/v1 https://www.googleapis.com/deploymentmanager/v2/projects	管理Google Cloud中的資源。
https://support.netapp.com https://mysupport.netapp.com	以取得授權資訊、並將AutoSupport 資訊傳送給NetApp支援部門。
https://*.api.bluexp.netapp.com https://api.bluexp.netapp.com https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com https://netapp-cloud-account.auth0.com	在BlueXP中提供SaaS功能與服務。 請注意、 Connector 目前正在聯絡「cloudmanager.cloud.netapp.com"」、但在即將推出的版本中、會開始聯絡「 api.bluexp.netapp.com"」。
https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io Azure 政府地區不需要此端點。 https://occmclientinfragov.azurecr.us 此端點僅在 Azure 政府地區需要使用。	升級Connector及其Docker元件。

Azure 中的公有 **IP** 位址

如果您想在 Azure 中的 Connector VM 使用公有 IP 位址、則 IP 位址必須使用基本 SKU 、以確保 BlueXP 使用此公有 IP 位址。



如果您改用標準 SKU IP 位址、則 BlueXP 會使用 Connector 的 _private IP 位址、而非公有 IP 。如果您用來存取 BlueXP 主控台的機器無法存取該私有 IP 位址、則 BlueXP 主控台的動作將會失敗。

"Azure 文件：公有 IP SKU"

Proxy伺服器

如果您的組織需要為所有傳出的網際網路流量部署 Proxy 伺服器、請取得下列關於 HTTP 或 HTTPS Proxy 的資訊。您必須在安裝期間提供此資訊。

- IP 位址
- 認證資料
- HTTPS憑證

請注意、 BlueXP 不支援透明 Proxy 伺服器。

連接埠

除非您啟動連接器、或使用連接器做為 Proxy 、將 AutoSupport 訊息從 Cloud Volumes ONTAP 傳送至 NetApp 支援、否則不會有傳入的流量傳入連接器。

- HTTP（80）和HTTPS（443）可存取本機UI、在極少數情況下使用。
- 只有在需要連線至主機進行疑難排解時、才需要SSH（22）。
- 如果您在無法使用輸出網際網路連線的子網路中部署 Cloud Volumes ONTAP 系統、則需要透過連接埠 3128 進行輸入連線。

  如果 Cloud Volumes ONTAP 系統沒有輸出網際網路連線來傳送 AutoSupport 訊息、 BlueXP 會自動將這些系統設定為使用 Connector 隨附的 Proxy 伺服器。唯一的需求是確保連接器的安全群組允許透過連接埠3128進行傳入連線。部署Connector之後、您需要開啟此連接埠。

啟用 **NTP**

如果您打算使用 BlueXP 分類來掃描公司資料來源、則應該在 BlueXP Connector 系統和 BlueXP 分類系統上啟用網路時間傳輸協定（ NTP ）服務、以便在系統之間同步時間。 "深入瞭解 BlueXP 分類"

如果您計畫從雲端供應商的市場建立 Connector 、則在建立 Connector 之後、您必須實作這項網路需求。

步驟： 5 準備雲端權限

BlueXP 需要雲端供應商的權限、才能在虛擬網路中部署 Cloud Volumes ONTAP 並使用 BlueXP 資料服務。您需要在雲端供應商中設定權限、然後將這些權限與 Connector 建立關聯。

若要檢視必要步驟、請選取您想要用於雲端供應商的驗證選項。

AWS IAM 角色

使用 IAM 角色為 Connector 提供權限。

如果您是從 AWS Marketplace 建立 Connector 、當您啟動 EC2 執行個體時、系統會提示您選取該 IAM 角色。

如果您是在自己的 Linux 主機上手動安裝 Connector 、則必須將該角色附加至 EC2 執行個體。

步驟

1. 登入 AWS 主控台並瀏覽至 IAM 服務。
2. 建立原則：
   a. 選取 * 原則 > 建立原則 * 。
   b. 選取 * JSON* 、然後複製並貼上的內容 "Connector 的 IAM 原則"。
   c. 完成其餘步驟以建立原則。
3. 建立 IAM 角色：
   a. 選取 * 角色 > 建立角色 * 。
   b. 選取 * AWS 服務 > EC2* 。
   c. 附加您剛建立的原則來新增權限。
   d. 完成剩餘步驟以建立角色。

結果

您現在擁有 Connector EC2 執行個體的 IAM 角色。

AWS 存取金鑰

為 IAM 使用者設定權限和存取金鑰。安裝 Connector 並設定 BlueXP 之後、您需要為 BlueXP 提供 AWS 存取金鑰。

步驟

1. 登入 AWS 主控台並瀏覽至 IAM 服務。
2. 建立原則：
   a. 選取 * 原則 > 建立原則 * 。
   b. 選取 * JSON* 、然後複製並貼上的內容 "Connector 的 IAM 原則"。
   c. 完成其餘步驟以建立原則。

      視您打算使用的 BlueXP 服務而定、您可能需要建立第二個原則。

   對於標準區域、權限分佈在兩個原則之間。由於AWS中受管理原則的字元大小上限、因此需要兩個原則。 "深入瞭解 Connector 的 IAM 原則"。

3. 將原則附加至 IAM 使用者。
   - "AWS 文件：建立 IAM 角色"
   - "AWS 文件：新增和移除 IAM 原則"

4. 請確定使用者擁有存取金鑰、您可以在安裝 Connector 之後新增至 BlueXP 。

結果

帳戶現在擁有必要的權限。

Azure 角色

建立具有必要權限的 Azure 自訂角色。您將會將此角色指派給 Connector VM 。

請注意、您可以使用 Azure 入口網站、 Azure PowerShell 、 Azure CLI 或 REST API 來建立 Azure 自訂角色。下列步驟說明如何使用 Azure CLI 建立角色。如果您想要使用不同的方法、請參閱 "Azure文件"

步驟

1. 如果您打算在自己的主機上手動安裝軟體、請在 VM 上啟用系統指派的託管身分識別、以便透過自訂角色提供必要的 Azure 權限。

   "Microsoft Azure 文件：使用 Azure 入口網站、在 VM 上設定 Azure 資源的託管身分識別"

2. 複製的內容 "Connector的自訂角色權限" 並將它們儲存在Json檔案中。
3. 將 Azure 訂閱 ID 新增至可指派的範圍、以修改 Json 檔案。

   您應該為每個想要搭配 BlueXP 使用的 Azure 訂閱新增 ID 。

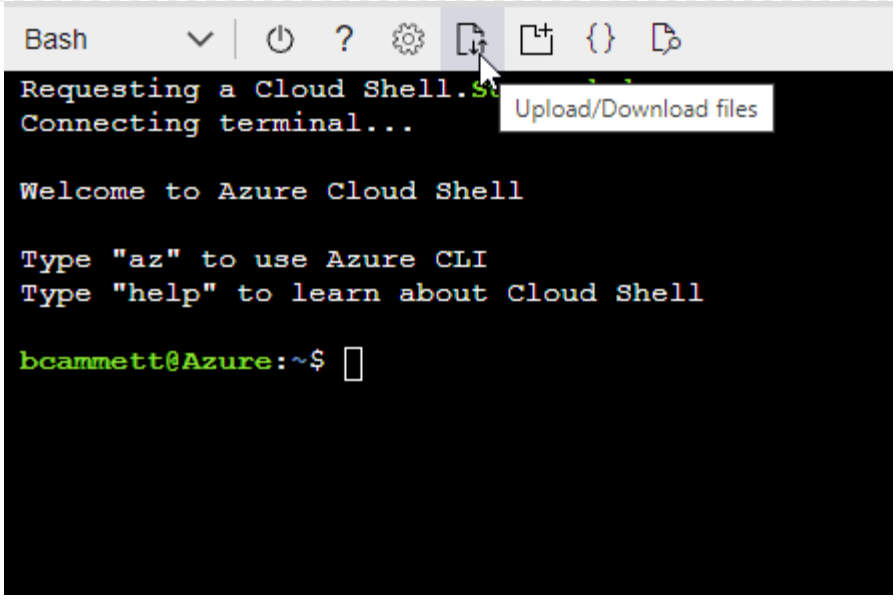
   - 範例 *

```
"AssignableScopes": [
"/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
"/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
"/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
```

4. 使用 Json 檔案在 Azure 中建立自訂角色。

   下列步驟說明如何在Azure Cloud Shell中使用Bash建立角色。

   a. 開始 "Azure Cloud Shell" 並選擇Bash環境。
   b. 上傳Json檔案。



c. 使用Azure CLI建立自訂角色：

```
az role definition create --role-definition Connector_Policy.json
```

結果

現在您應該有一個名為BlueXP運算子的自訂角色、可以指派給連接器虛擬機器。

Azure 服務主體

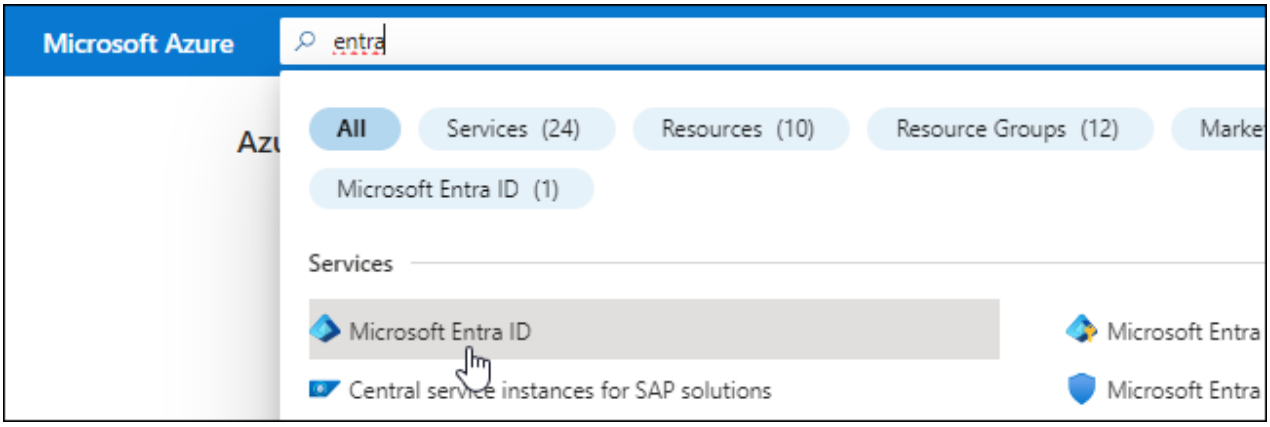
在 Microsoft Entra ID 中建立並設定服務主體、並取得 BlueXP 所需的 Azure 認證。安裝 Connector 並設定 BlueXP 之後、您必須提供 BlueXP 的這些認證。

建立 **Microsoft Entra** 應用程式以進行角色型存取控制

1. 確保您在 Azure 中擁有建立 Active Directory 應用程式及將應用程式指派給角色的權限。

   如需詳細資訊、請參閱 "Microsoft Azure 說明文件：必要權限"

2. 從 Azure 入口網站開啟 * Microsoft Entra ID* 服務。



3. 在功能表中、選取 * 應用程式註冊 * 。

4. 選取 * 新登錄 * 。
5. 指定應用程式的詳細資料：
   - * 名稱 * ：輸入應用程式的名稱。
   - 帳戶類型：選取帳戶類型（任何帳戶類型均可用於BlueXP）。
   - 重新導向**URI**：您可以將此欄位保留空白。
6. 選擇*註冊*。

   您已建立 AD 應用程式和服務主體。

將應用程式指派給角色

1. 建立自訂角色：

   請注意、您可以使用 Azure 入口網站、 Azure PowerShell 、 Azure CLI 或 REST API 來建立 Azure 自訂角色。下列步驟說明如何使用 Azure CLI 建立角色。如果您想要使用不同的方法、請參閱 "Azure文件"

   a. 複製的內容 "Connector的自訂角色權限" 並將它們儲存在Json檔案中。
   b. 將 Azure 訂閱 ID 新增至可指派的範圍、以修改 Json 檔案。

      您應該為使用者建立 Cloud Volumes ONTAP 的各個 Azure 訂閱新增 ID 。

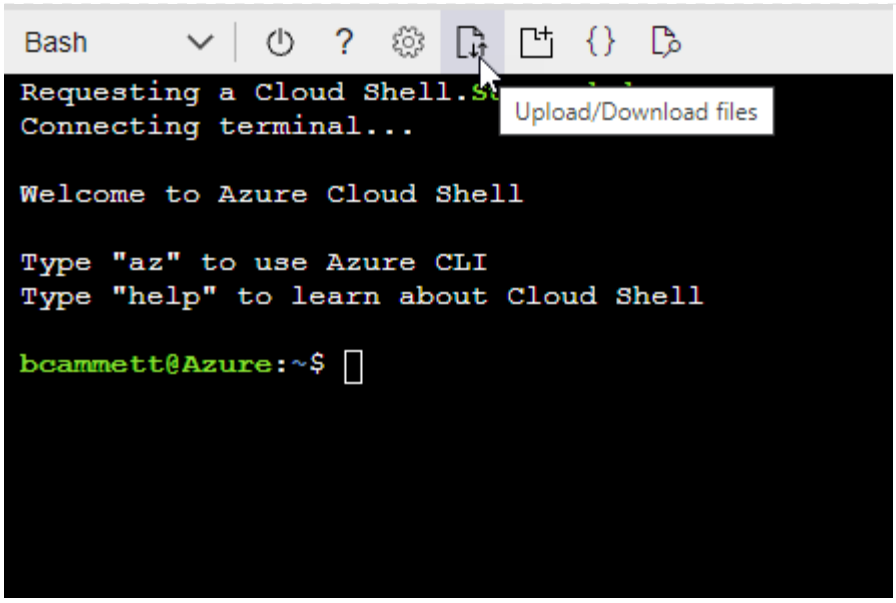
      - 範例 *

      ```
      "AssignableScopes": [
      "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
      "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
      "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
      ```

   c. 使用 Json 檔案在 Azure 中建立自訂角色。

      下列步驟說明如何在Azure Cloud Shell中使用Bash建立角色。

      - 開始 "Azure Cloud Shell" 並選擇Bash環境。
      - 上傳Json檔案。



- 使用Azure CLI建立自訂角色：

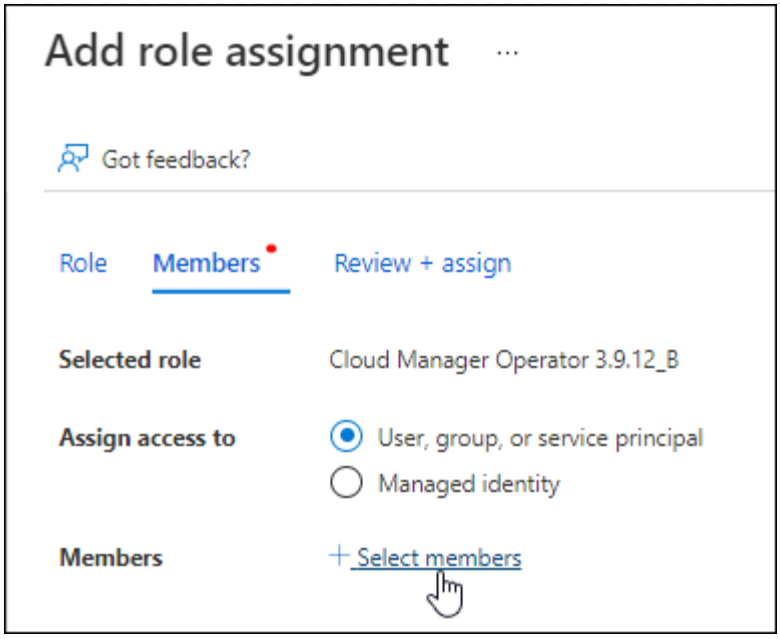
```
az role definition create --role-definition
Connector_Policy.json
```

現在您應該有一個名為BlueXP運算子的自訂角色、可以指派給連接器虛擬機器。

2. 將應用程式指派給角色：

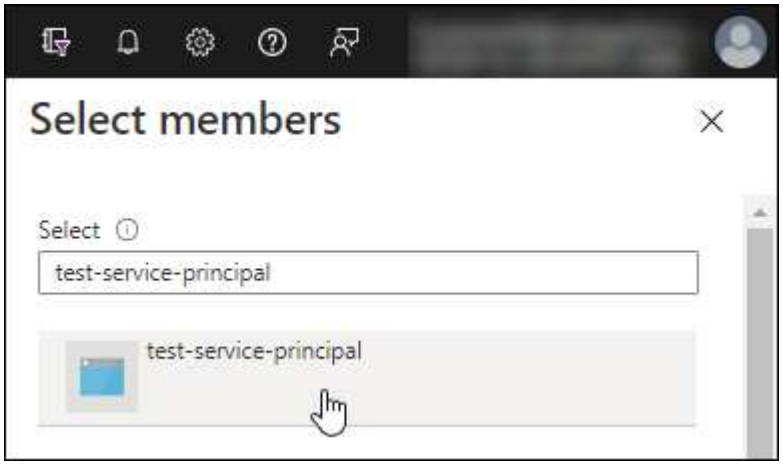
   a. 從 Azure 入口網站開啟 * 訂閱 * 服務。
   b. 選取訂閱。
   c. 選取 * 存取控制（IAM） > 新增 > 新增角色指派 * 。
   d. 在 * 角色 * 索引標籤中、選取 * BlueXP 操作員 * 角色、然後選取 * 下一步 * 。
   e. 在「成員」索引標籤中、完成下列步驟：

      - 保留*選取「使用者」、「群組」或「服務主體」*。
      - 選取 * 選取成員 * 。



- 搜尋應用程式名稱。

  範例如下：



- 選取應用程式、然後選取 * 選取 * 。
- 選擇*下一步*。

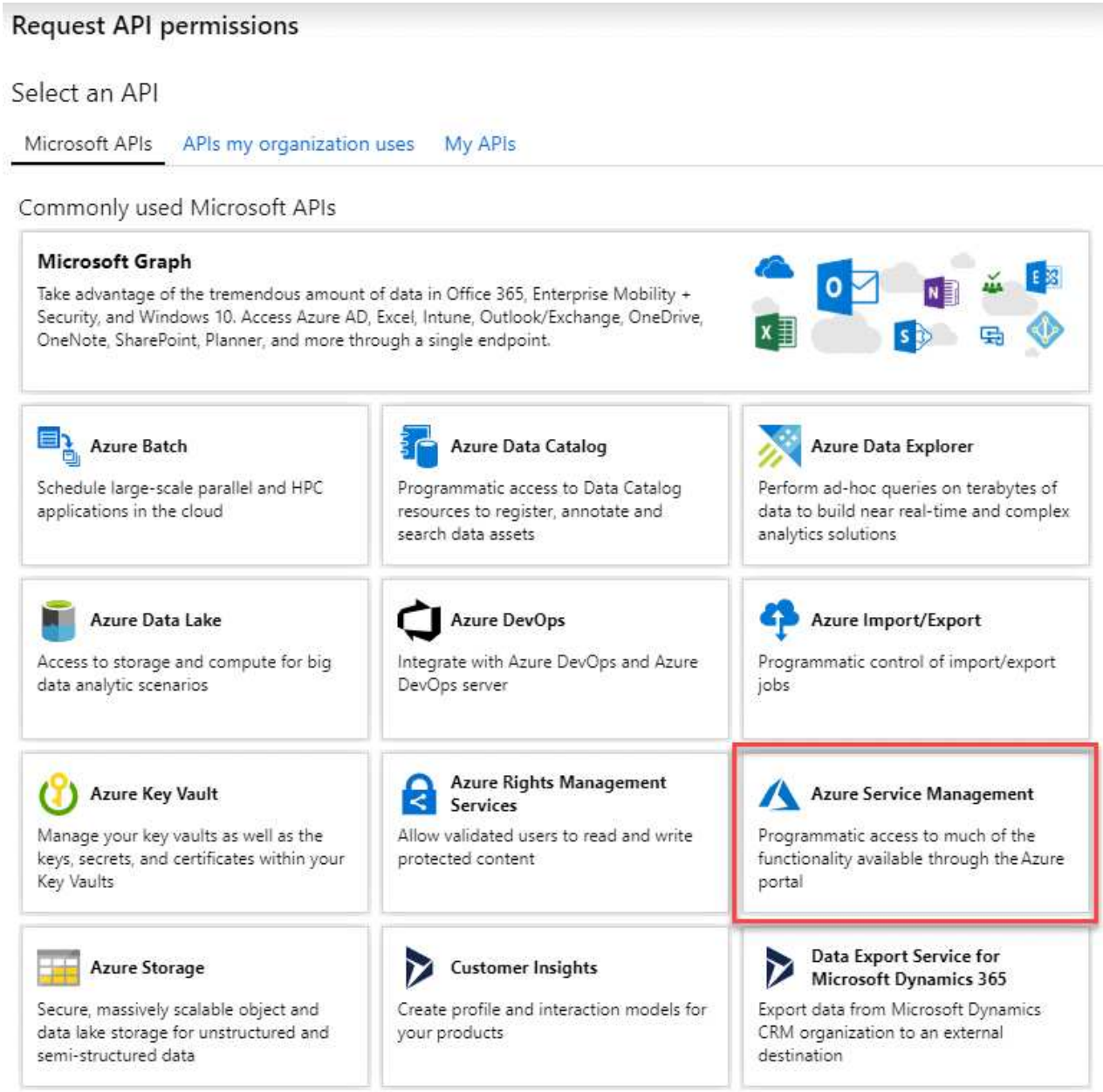
f. 選取 * 檢閱 + 指派 * 。

服務主體現在擁有部署Connector所需的Azure權限。

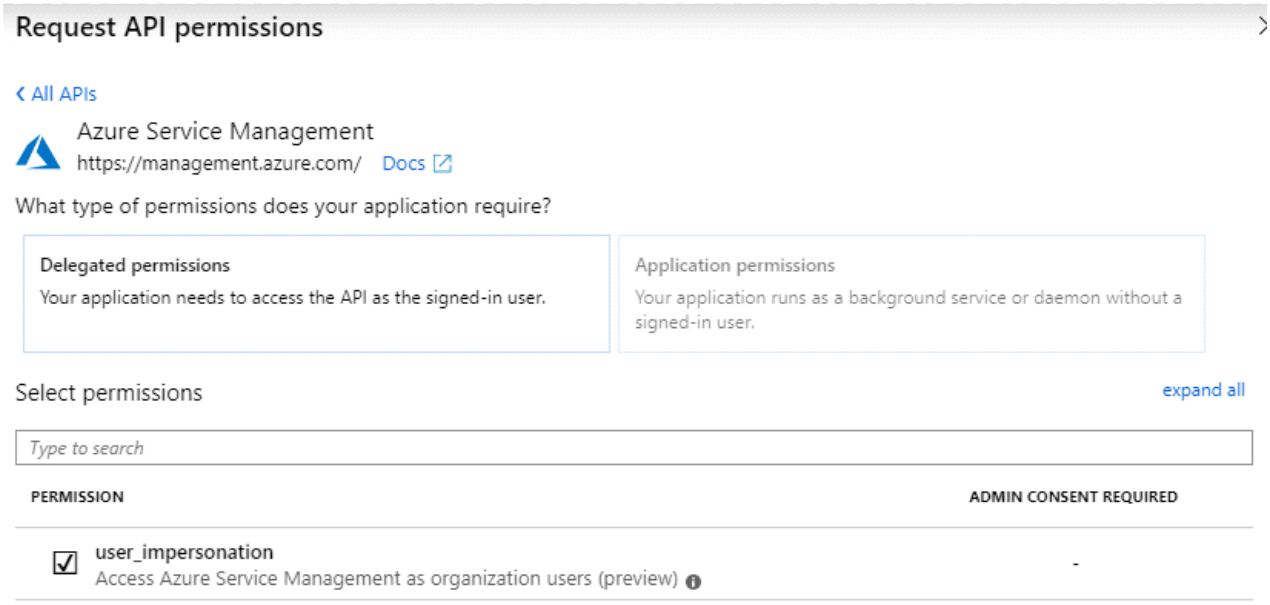
如果您想要從 Cloud Volumes ONTAP 多個 Azure 訂閱中部署支援功能、則必須將服務授權對象繫結至每個訂閱項目。BlueXP可讓您選擇部署Cloud Volumes ONTAP 時要使用的訂閱內容。

新增 **Windows Azure Service Management API** 權限

1. 在 * Microsoft Entra ID* 服務中、選取 * 應用程式登錄 * 、然後選取應用程式。
2. 選取 * API 權限 > 新增權限 * 。
3. 在「 * Microsoft API* 」下、選取「 * Azure 服務管理 * 」。

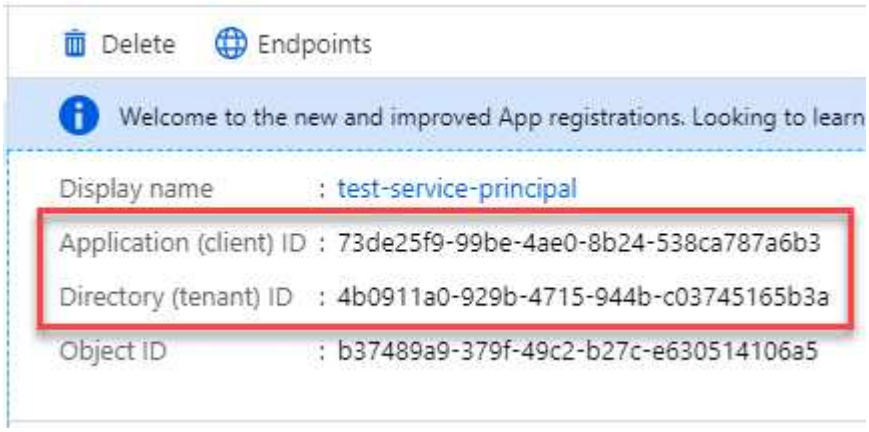


4. 選取 * 以組織使用者身分存取 Azure 服務管理 * 、然後選取 * 新增權限 * 。



取得應用程式的應用程式 **ID** 和目錄 **ID**

1. 在 * Microsoft Entra ID* 服務中、選取 * 應用程式登錄 * 、然後選取應用程式。
2. 複製 * 應用程式（用戶端） ID* 和 * 目錄（租戶） ID* 。



將Azure帳戶新增至BlueXP時、您必須提供應用程式的應用程式（用戶端）ID和目錄（租戶）ID。BlueXP使用ID以程式設計方式登入。

建立用戶端機密

1. 開啟 * Microsoft Entra ID* 服務。
2. 選取 * 應用程式註冊 * 、然後選取您的應用程式。
3. 選取 * 「憑證與機密」 > 「新用戶端機密」 * 。
4. 提供機密與持續時間的說明。
5. 選取*「Add*」 。
6. 複製用戶端機密的值。

您現在擁有一個客戶機密、 BlueXP 可以使用它來驗證 Microsoft Entra ID 。

結果

您的服務主體現在已設定完成、您應該已經複製應用程式（用戶端） ID 、目錄（租戶） ID 、以及用戶端機密的值。新增Azure帳戶時、您必須在BlueXP中輸入此資訊。

Google Cloud 服務帳戶

建立角色、並將其套用至將用於 Connector VM 執行個體的服務帳戶。

步驟

1. 在 Google Cloud 中建立自訂角色：

   a. 建立包含中定義權限的 YAML 檔案 "Google Cloud 的 Connector 原則"。

   b. 從 Google Cloud 啟動 Cloud Shell 。

   c. 上傳包含 Connector 必要權限的 YAML 檔案。

   d. 使用建立自訂角色 `gcloud iam roles create` 命令。

      以下範例在專案層級建立名為「 Connector 」的角色：

```
gcloud iam roles create connector --project=myproject
--file=connector.yaml
```

   +
   "Google Cloud 文件：建立及管理自訂角色"

2. 在 Google Cloud 中建立服務帳戶：

   a. 從 IAM & Admin 服務中、選取 * 服務帳戶 > 建立服務帳戶 * 。

   b. 輸入服務帳戶詳細資料、然後選取 * 建立並繼續 * 。

   c. 選取您剛建立的角色。

   d. 完成剩餘步驟以建立角色。

      "Google Cloud 文件：建立服務帳戶"

結果

現在您有一個服務帳戶、可以指派給 Connector VM 執行個體。

步驟 6 ：啟用 Google Cloud API

在 Google Cloud 中部署 Cloud Volumes ONTAP 需要幾個 API 。

步驟

1. "在專案中啟用下列 Google Cloud API"
    - Cloud Deployment Manager V2 API
    - 雲端記錄 API
    - Cloud Resource Manager API
    - 運算引擎 API
    - 身分識別與存取管理（ IAM ） API
    - 雲端金鑰管理服務（ KMS ） API

      （僅當您打算使用 BlueXP 備份與還原搭配客戶管理的加密金鑰（ CMEK ）時才需要）

以受限模式部署 Connector

在受限模式下部署 Connector 、以便在與 BlueXP SaaS 層的輸出連線有限的情況下使用 BlueXP 。若要開始使用、請安裝 Connector 、存取 Connector 上執行的使用者介面來設定 BlueXP 、然後提供您先前設定的雲端權限。

步驟 1 ：安裝 Connector

從雲端供應商的市場安裝 Connector 、或是在您自己的 Linux 主機上手動安裝軟體。

AWS 商業市場

開始之前

您應該擁有下列項目：

- 符合網路需求的 VPC 和子網路。

  "深入瞭解網路需求"

- 具有附加原則的 IAM 角色、其中包含 Connector 所需的權限。

  "瞭解如何設定 AWS 權限"

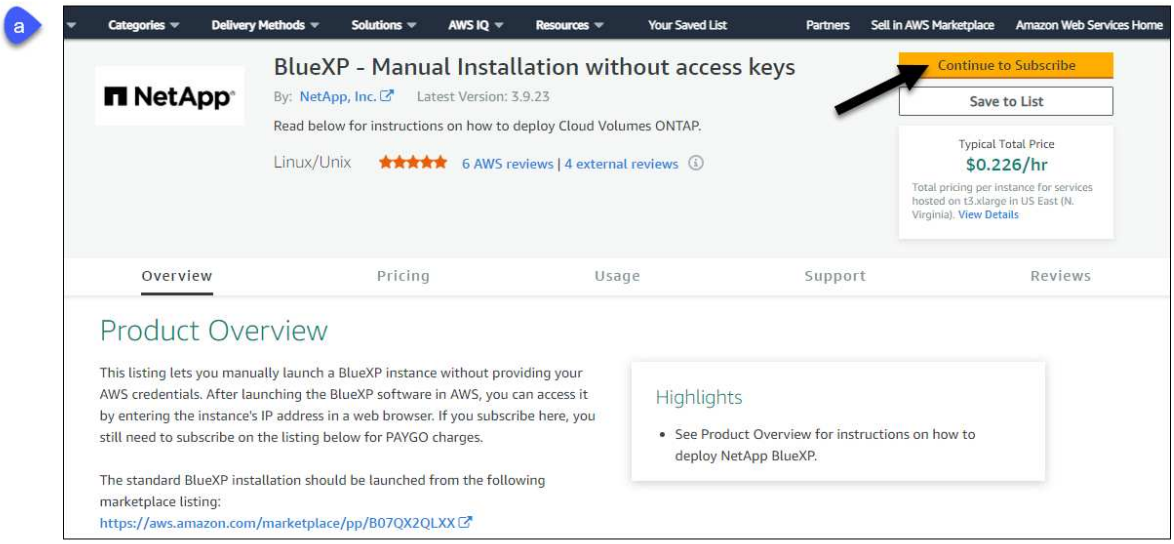
- 為您的 IAM 使用者訂閱及取消訂閱 AWS Marketplace 的權限。
- 瞭解執行個體的 CPU 和 RAM 需求。

  "檢閱執行個體需求"。

- EC2 執行個體的金鑰配對。

步驟

1. 前往 "AWS Marketplace上的BlueXP頁面"
2. 在 Marketplace 頁面上，選擇 * 繼續訂閱 * ，然後選擇 * 繼續至組態 * 。



3. 變更任何預設選項、然後選取 * 繼續啟動 * 。
4. 在「 * 選擇行動 * 」下、選取 * 透過 EC2* 啟動、然後選取 * 啟動 * 。

   這些步驟說明如何從EC2主控台啟動執行個體、因為主控台可讓您將IAM角色附加至連接器執行個體。這無法使用 * 從網站啟動 * 動作。

5. 依照提示設定及部署執行個體：
   - 名稱和標記：輸入執行個體的名稱和標記。
   - 應用程式與作業系統映像：跳過本節。已選取連接器AMI。
   - * 執行個體類型 * ：根據區域可用度、選擇符合 RAM 和 CPU 需求的執行個體類型（建議使用 T3.x 大型）。
   - 金鑰配對（登入）：選取您要用來安全連線至執行個體的金鑰配對。
   - 網路設定：視需要編輯網路設定：
     - 選擇所需的VPC和子網路。
     - 指定執行個體是否應有公有IP位址。
     - 指定防火牆設定、以啟用Connector執行個體所需的連線方法：SSH、HTTP和HTTPS。

       特定組態還需要一些規則。

"檢視 AWS 的安全性群組規則"。

- * 設定儲存設備 * ：保留根磁碟區的預設大小和磁碟類型。

  如果您要在根磁碟區上啟用 Amazon EBS 加密、請選取 * 進階 * 、展開 * Volume 1* 、選取 * 加密 * 、然後選擇 KMS 金鑰。

- * 進階詳細資料 * ：在 * IAM 執行個體設定檔 * 下、選擇包含 Connector 所需權限的 IAM 角色。
- * 摘要 * ：檢閱摘要並選取 * 啟動執行個體 * 。

結果

AWS 會以指定的設定啟動軟體。Connector 執行個體和軟體應在大約五分鐘內執行。

接下來呢？

設定 BlueXP 。

AWS Gov Marketplace

開始之前

您應該擁有下列項目：

- 符合網路需求的 VPC 和子網路。

  "深入瞭解網路需求"

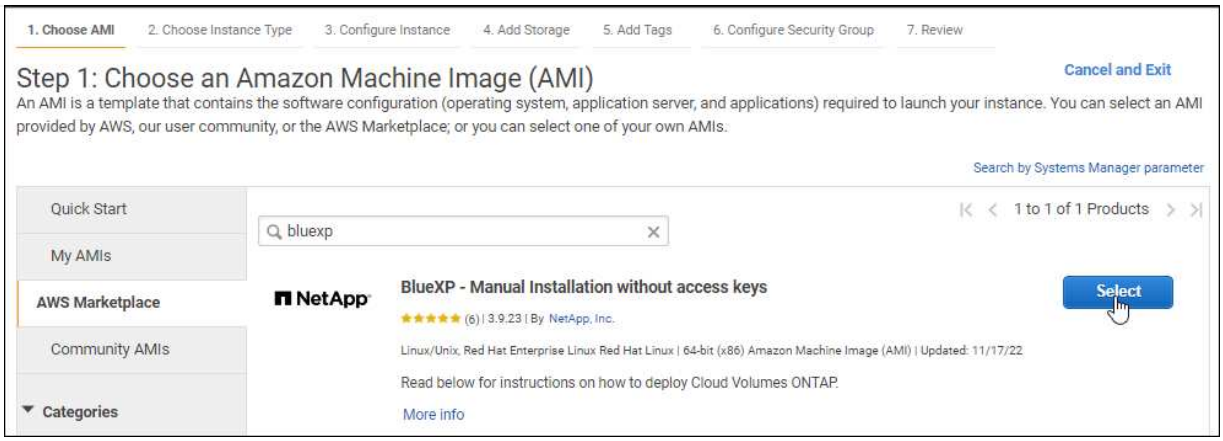
- 具有附加原則的 IAM 角色、其中包含 Connector 所需的權限。

  "瞭解如何設定 AWS 權限"

- 為您的 IAM 使用者訂閱及取消訂閱 AWS Marketplace 的權限。
- EC2 執行個體的金鑰配對。

步驟

1. 前往AWS Marketplace的BlueXP產品。
   a. 開啟EC2服務、然後選取* Launch instance*。
   b. 選擇* AWS Marketplace *。
   c. 搜尋BlueXP並選取產品項目。



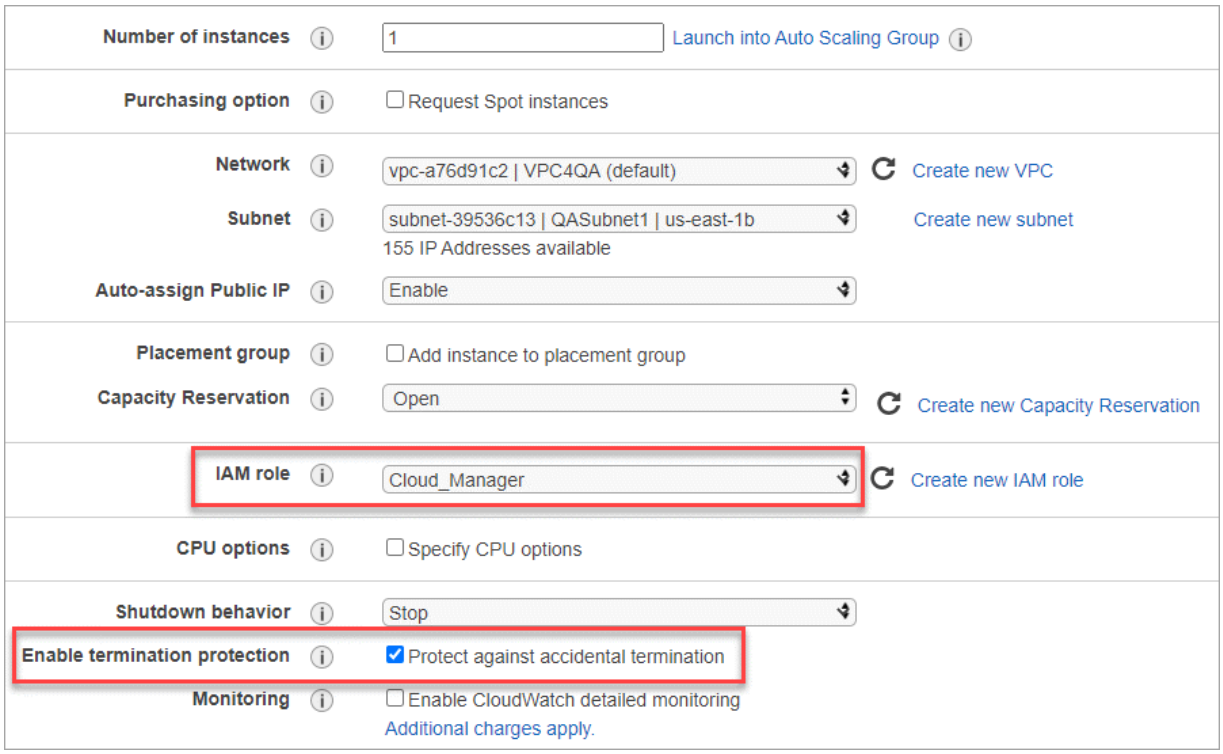
d. 選擇*繼續*。

2. 依照提示設定及部署執行個體：

   - 選擇執行個體類型：視區域可用度而定、請選擇其中一種支援的執行個體類型（建議使用T3.xlge）。

     "檢閱執行個體需求"。

   - 設定執行個體詳細資料：選取VPC和子網路、選擇您在步驟1中建立的IAM角色、啟用終止保護（建議）、並選擇符合您需求的任何其他組態選項。



   - * 新增儲存設備 * ：保留預設的儲存選項。
   - * 新增標記 * ：視需要輸入執行個體的標記。
   - * 設定安全性群組 * ：指定連接器執行個體所需的連線方法： SSH 、 HTTP 和 HTTPS 。
   - * 審查 * ：檢閱您的選擇並選擇 * 發表 * 。

結果

AWS 會以指定的設定啟動軟體。Connector 執行個體和軟體應在大約五分鐘內執行。

接下來呢？

設定 BlueXP 。

Azure Marketplace

開始之前

您應該擁有下列項目：

- 符合網路需求的 vnet 和子網路。

  "深入瞭解網路需求"

- Azure 自訂角色、包含 Connector 所需的權限。

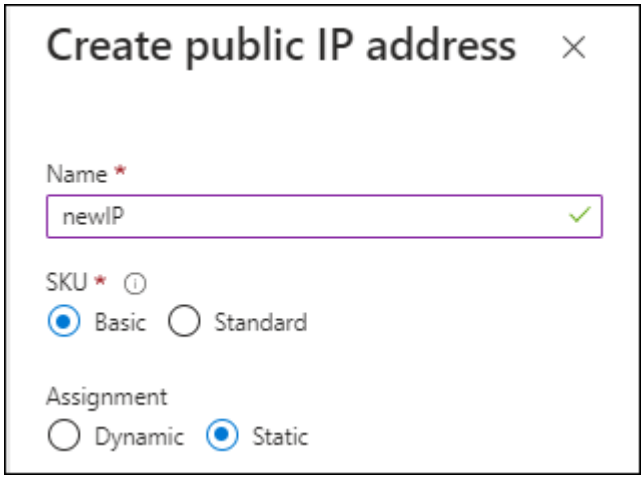
  "瞭解如何設定 Azure 權限"

步驟

1. 前往Azure Marketplace的NetApp Connector VM頁面。
   - "適用於商業區域的Azure Marketplace頁面"
   - "Azure政府區域的Azure Marketplace頁面"
2. 選擇 * 立即取得 * 、然後選擇 * 繼續 * 。
3. 從 Azure 入口網站選取 * Create * 、然後依照步驟設定虛擬機器。

   設定 VM 時請注意下列事項：

   - * VM 大小 * ：選擇符合 CPU 和 RAM 需求的 VM 大小。我們建議使用 DS3 v2 。
   - * 磁碟 * ：連接器可在 HDD 或 SSD 磁碟上以最佳方式執行。
   - * 公有 IP* ：如果您想將公有 IP 位址與 Connector VM 搭配使用、則 IP 位址必須使用基本 SKU 、以確保 BlueXP 使用此公有 IP 位址。



   如果您改用標準 SKU IP 位址、則 BlueXP 會使用 Connector 的 _private IP 位址、而非公有 IP 。

如果您用來存取 BlueXP 主控台的機器無法存取該私有 IP 位址、則 BlueXP 主控台的動作將會失敗。

"Azure 文件：公有 IP SKU"

- * 網路安全群組 * ： Connector 需要使用 SSH 、 HTTP 和 HTTPS 的傳入連線。

  "檢視 Azure 的安全性群組規則"。

- * 識別 * ：在 * 管理 * 下、選取 * 啟用系統指派的託管識別 * 。

  此設定很重要、因為託管身分識別可讓 Connector 虛擬機器在 Microsoft Entra ID 中識別自己、而無需提供任何認證。 "深入瞭解 Azure 資源的託管身分識別"。

4. 在 **Review + create** 頁面上、檢閱您的選擇、然後選取 * Create* 開始部署。

結果

Azure 以指定的設定部署虛擬機器。虛擬機器和 Connector 軟體應在大約五分鐘內執行。

接下來呢？

設定 BlueXP 。

手動安裝

開始之前

您應該擁有下列項目：

- 安裝Connector的root權限。
- Proxy伺服器的詳細資料、如果需要Proxy才能從Connector存取網際網路。

  您可以選擇在安裝後設定Proxy伺服器、但需要重新啟動Connector。

  請注意、 BlueXP 不支援透明 Proxy 伺服器。

- CA 簽署的憑證（如果 Proxy 伺服器使用 HTTPS 或 Proxy 是攔截 Proxy ）。

關於這項工作

NetApp 支援網站上提供的安裝程式可能是舊版。安裝後、如果有新版本可用、 Connector 會自動自行更新。

步驟

1. 確認已啟用並執行Docker。

```
sudo systemctl enable docker && sudo systemctl start docker
```

2. 如果主機上已設定_http或_https或proxy_系統變數、請將其移除：

```
unset http_proxy
unset https_proxy
```

如果您未移除這些系統變數、安裝將會失敗。

3. 從下載Connector軟體 "NetApp 支援網站"，然後將其複製到 Linux 主機。

   您應該下載「線上」 Connector 安裝程式、以供您的網路或雲端使用。Connector 有獨立的「離線」安裝程式、但僅支援私有模式部署。

4. 指派執行指令碼的權限。

```
chmod +x BlueXP-Connector-Cloud-<version>
```

   其中、就是您下載的Connector版本<version> 。

5. 執行安裝指令碼。

```
 ./BlueXP-Connector-Cloud-<version> --proxy <HTTP or HTTPS proxy
server> --cacert <path and file name of a CA-signed certificate>
```

   -Proxy和—cacert參數是可選的。如果您有 Proxy 伺服器、則需要輸入如圖所示的參數。安裝程式不會提示您提供Proxy的相關資訊。

   以下是使用兩個選用參數的命令範例：

```
 ./BlueXP-Connector-Cloud-v3.9.38 --proxy
https://user:password@10.0.0.30:8080/ --cacert
/tmp/cacert/certificate.cer
```

   -Proxy會使用下列其中一種格式、將Connector設定為使用HTTP或HTTPS Proxy伺服器：

   - http://address:port
   - http://user-name:password@address:port
   - http://domain-name%92user-name:password@address:port
   - https://address:port
   - https://user-name:password@address:port
   - https://domain-name%92user-name:password@address:port

     請注意下列事項：

     - 使用者可以是本機使用者或網域使用者。
     - 對於網域使用者、您必須使用上方所示的 \ 的 ASCII 碼。

- BlueXP不支援包含@字元的密碼。

-cacert指定用於連接器與Proxy伺服器之間HTTPS存取的CA簽署憑證。只有當您指定 HTTPS Proxy 伺服器或 Proxy 是攔截 Proxy 時、才需要此參數。

結果

現在已安裝Connector。安裝結束時、如果您指定Proxy伺服器、Connector服務（occm）會重新啟動兩次。

接下來呢？

設定 BlueXP 。

步驟 2 ：設定 BlueXP

當您第一次存取 BlueXP 主控台時、系統會提示您選擇要與 Connector 建立關聯的帳戶、您需要啟用受限模式。

> 如果您已經有帳戶、而且想要建立另一個帳戶、則需要使用 Tenancy API 。 "瞭解如何建立其他 BlueXP 帳戶"。

步驟

1. 從連線至 Connector 執行個體的主機開啟網頁瀏覽器、然後輸入下列 URL ：

   https://ipaddress

2. 註冊或登入 BlueXP 。
3. 登入後、請設定 BlueXP ：

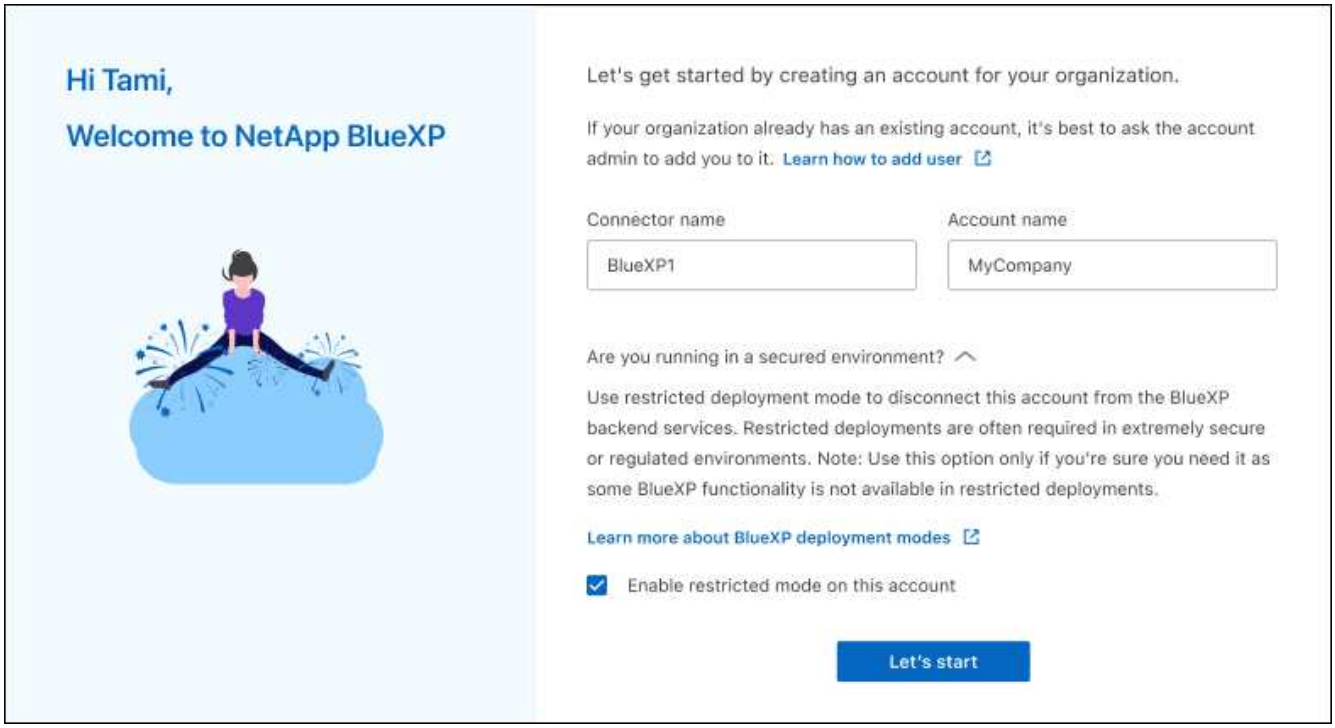
   a. 輸入 Connector 的名稱。
   b. 輸入新 BlueXP 帳戶的名稱、或選取現有帳戶。

      如果您的登入已與 BlueXP 帳戶建立關聯、您可以選取現有帳戶。

   c. 選擇 * 您是否在安全的環境中執行？ *
   d. 選取 * 啟用此帳戶的受限模式 * 。

      請注意、在 BlueXP 建立帳戶之後、您無法變更此設定。您稍後無法啟用受限模式、之後也無法停用。

      如果您在政府區域部署 Connector 、則核取方塊已啟用、無法變更。這是因為受限模式是政府地區唯一支援的模式。



a. 選取 * 開始 * 。

結果

Connector 現在已安裝、並使用您的 BlueXP 帳戶進行設定。所有使用者都需要使用 Connector 執行個體的 IP 位址來存取 BlueXP 。

接下來呢？

提供 BlueXP 先前設定的權限。

步驟 3 ：提供 BlueXP 的權限

如果您是從 Azure Marketplace 部署 Connector 、或是手動安裝 Connector 軟體、則必須提供先前設定的權限、才能使用 BlueXP 服務。

如果您從 AWS Marketplace 部署 Connector 、則這些步驟不適用、因為您在部署期間選擇了所需的 IAM 角色。

"瞭解如何準備雲端權限"。

AWS IAM 角色

將您先前建立的 IAM 角色附加至您安裝 Connector 的 EC2 執行個體。

只有在 AWS 中手動安裝 Connector 時、才適用這些步驟。對於 AWS Marketplace 部署、您已將 Connector 執行個體與包含必要權限的 IAM 角色建立關聯。

步驟

1. 前往 Amazon EC2 主控台。
2. 選取 * 執行個體 * 。
3. 選取 Connector 執行個體。
4. 選取 * 「動作」 > 「安全性」 > 「修改 IAM 角色」 * 。
5. 選取 IAM 角色、然後選取 * 更新 IAM 角色 * 。

結果

BlueXP 現在擁有代表您在 AWS 中執行動作所需的權限。

AWS 存取金鑰

為具有必要權限的 IAM 使用者提供 BlueXP AWS 存取金鑰。

步驟

1. 在 BlueXP 主控台的右上角、選取「設定」圖示、然後選取 * 認證 * 。

2. 選取 * 新增認證 * 、然後依照精靈中的步驟進行。
   a. 認證資料位置：選取* Amazon Web Services > Connector*。
   b. * 定義認證 * ：輸入 AWS 存取金鑰和秘密金鑰。
   c. 市場訂閱：立即訂閱或選取現有的訂閱、以建立Marketplace訂閱與這些認證的關聯。
   d. * 審查 * ：確認新認證的詳細資料、然後選取 * 新增 * 。

結果

BlueXP 現在擁有代表您在 AWS 中執行動作所需的權限。

Azure 角色

前往 Azure 入口網站、將 Azure 自訂角色指派給 Connector 虛擬機器、以進行一或多個訂閱。

步驟

1. 從 Azure Portal 開啟 * Subscriptions * 服務、然後選取您的訂閱。

   請務必從 * 訂閱 * 服務指派角色、因為這會指定訂閱層級的角色指派範圍。*scacity* 定義存取所套用的資源集。如果您在不同層級（例如虛擬機器層級）指定範圍、則從 BlueXP 中完成動作的能力將受到影響。

"Microsoft Azure 文件：瞭解 Azure RBAC 的範圍"

2. 選取 * 存取控制（IAM） * > * 新增 * > * 新增角色指派 * 。
3. 在 * 角色 * 索引標籤中、選取 * BlueXP 操作員 * 角色、然後選取 * 下一步 * 。

> BlueXP運算子是在BlueXP原則中提供的預設名稱。如果您為角色選擇不同的名稱、請改為選取該名稱。

4. 在「成員」索引標籤中、完成下列步驟：
   a. 指派*託管身分識別*的存取權。
   b. 選取 * 選取成員 * 、選取建立 Connector 虛擬機器的訂閱、然後在 * 管理身分識別 * 下選擇 * 虛擬機器 * 、然後選取 Connector 虛擬機器。
   c. 選取 * 選取 * 。
   d. 選擇*下一步*。
   e. 選取 * 檢閱 + 指派 * 。
   f. 如果您想要在其他 Azure 訂閱中管理資源、請切換至該訂閱、然後重複這些步驟。

結果

BlueXP 現在擁有代表您在 Azure 中執行動作所需的權限。

Azure 服務主體

為 BlueXP 提供您先前設定的 Azure 服務主體認證。

步驟

1. 在 BlueXP 主控台的右上角、選取「設定」圖示、然後選取 * 認證 * 。

2. 選取 * 新增認證 * 、然後依照精靈中的步驟進行。
   a. 認證位置：選擇* Microsoft Azure > Connector*。
   b. * 定義認證 * ：輸入 Microsoft Entra 服務授權者的相關資訊、以授予必要的權限：
      - 應用程式（用戶端）ID
      - 目錄（租戶）ID
      - 用戶端機密
   c. 市場訂閱：立即訂閱或選取現有的訂閱、以建立Marketplace訂閱與這些認證的關聯。
   d. * 審查 * ：確認新認證的詳細資料、然後選取 * 新增 * 。

結果

BlueXP 現在擁有代表您在 Azure 中執行動作所需的權限。

Google Cloud 服務帳戶

將服務帳戶與 Connector VM 建立關聯。

步驟

1. 前往 Google Cloud 入口網站、將服務帳戶指派給 Connector VM 執行個體。

   "Google Cloud 文件：變更執行個體的服務帳戶和存取範圍"

2. 如果您想要管理其他專案中的資源、請將具有 BlueXP 角色的服務帳戶新增至該專案、以授予存取權。您必須針對每個專案重複此步驟。

結果

BlueXP 現在擁有代表您在 Google Cloud 中執行動作所需的權限。

訂閱 BlueXP （受限模式）

從雲端供應商的市場訂閱 BlueXP 、即可按每小時費率（PAYGO）或透過年度合約支付 BlueXP 服務費用。如果您向 NetApp （BYOL）購買授權、您也需要訂閱市場方案。您的授權一律會先收費、但如果您超過授權容量或授權期限到期、則會以每小時費率收費。

市場訂閱可在受限模式下為下列 BlueXP 服務收費：

- 備份與還原
- 分類
- Cloud Volumes ONTAP

開始之前

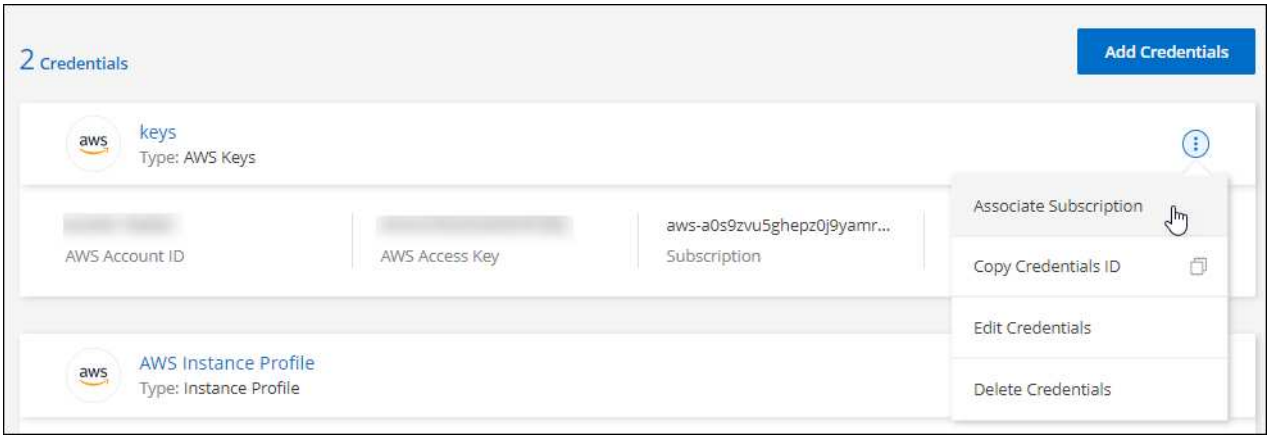
訂閱 BlueXP 涉及將市場訂閱與與 Connector 相關的雲端認證建立關聯。如果您遵循「開始使用受限模式」工作流程、則您應該已經擁有 Connector 。若要深入瞭解、請檢視 "以受限模式快速啟動 BlueXP"。

AWS

步驟

1. 在 BlueXP 主控台的右上角、選取「設定」圖示、然後選取 * 認證 * 。
2. 選取一組認證的動作功能表、然後選取 * 關聯訂閱 * 。

   您必須選取與 Connector 相關聯的認證。您無法將市場訂閱與 BlueXP 相關的認證建立關聯。



3. 若要將認證與現有訂閱建立關聯、請從下拉式清單中選取訂閱、然後選取 * 關聯 * 。
4. 若要將認證與新訂閱建立關聯、請選取 * 新增訂閱 > 繼續 * 、然後依照 AWS Marketplace 中的步驟進行：

   a. 選取 * 檢視購買選項 * 。
   b. 選取 * 訂閱 * 。
   c. 選取 * 設定您的帳戶 * 。

      您將被重新導向至BlueXP網站。

   d. 從*訂閱指派*頁面：

      - 選取您要與此訂閱建立關聯的 BlueXP 帳戶。
      - 在「取代現有訂閱」欄位中、選擇您是否要使用此新訂閱來自動取代現有的單一帳戶訂閱。

        此新訂閱取代現有的帳戶所有認證訂閱。如果一組認證資料從未與訂閱建立關聯、則此新訂閱將不會與這些認證資料建立關聯。

   對於所有其他帳戶、您必須重複這些步驟、手動建立訂閱的關聯。

      - 選擇*保存*。

        下列影片顯示從 AWS Marketplace 訂閱的步驟：

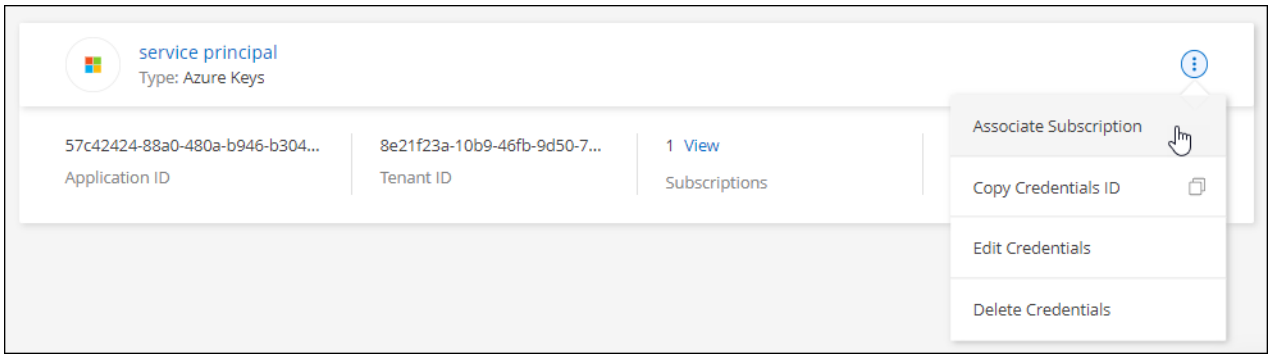
   從 AWS Marketplace 訂閱 BlueXP

Azure

步驟

1. 在 BlueXP 主控台的右上角、選取「設定」圖示、然後選取 * 認證 * 。
2. 選取一組認證的動作功能表、然後選取 * 關聯訂閱 * 。

   您必須選取與 Connector 相關聯的認證。您無法將市場訂閱與 BlueXP 相關的認證建立關聯。



3. 若要將認證與現有訂閱建立關聯、請從下拉式清單中選取訂閱、然後選取 * 關聯 * 。
4. 若要將認證與新訂閱建立關聯、請選取 * 新增訂閱 > 繼續 * 、然後依照 Azure Marketplace 中的步驟進行：

   a. 出現提示時、請登入您的Azure帳戶。
   b. 選取 * 訂閱 * 。
   c. 填寫表單並選擇 * 訂閱 * 。
   d. 訂閱程序完成後、請選取 * 立即設定帳戶 * 。

      您將被重新導向至BlueXP網站。

   e. 從*訂閱指派*頁面：

      - 選取您要與此訂閱建立關聯的 BlueXP 帳戶。
      - 在「取代現有訂閱」欄位中、選擇您是否要使用此新訂閱來自動取代現有的單一帳戶訂閱。

        此新訂閱取代現有的帳戶所有認證訂閱。如果一組認證資料從未與訂閱建立關聯、則此新訂閱將不會與這些認證資料建立關聯。

   對於所有其他帳戶、您必須重複這些步驟、手動建立訂閱的關聯。

      - 選擇*保存*。

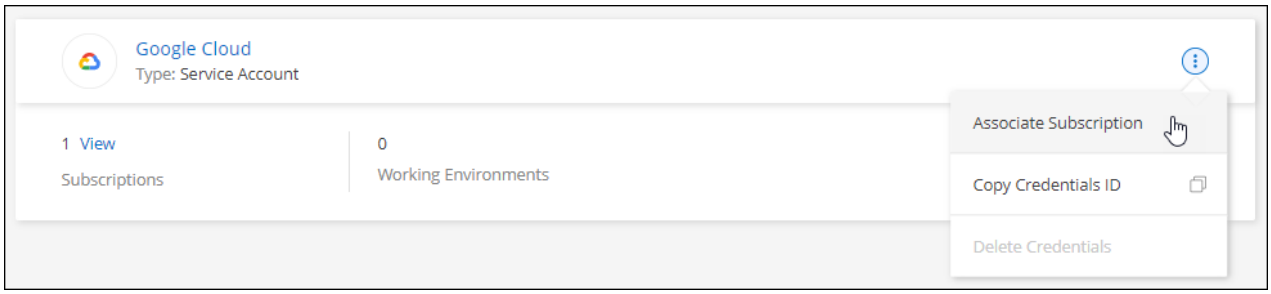
        下列影片顯示從Azure Marketplace訂閱的步驟：

   從 Azure Marketplace 訂閱 BlueXP

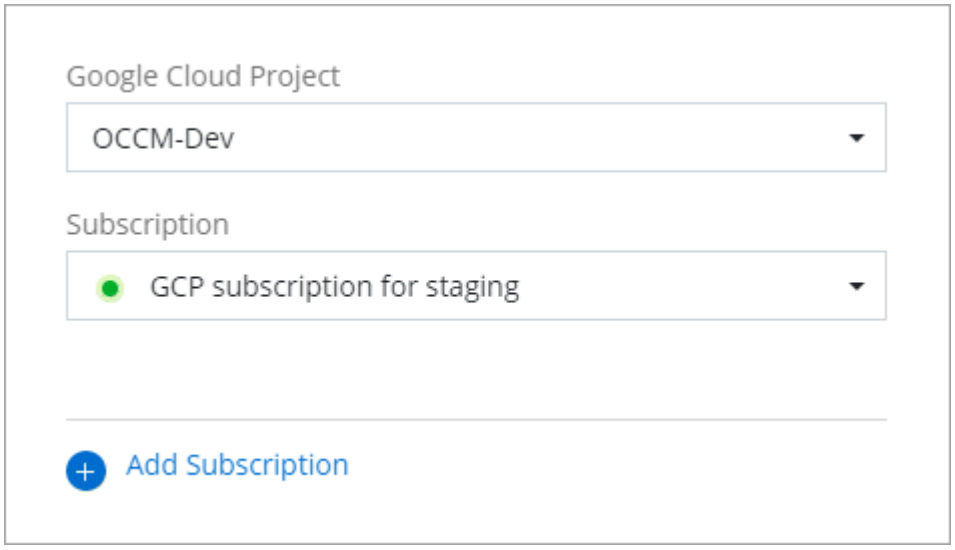
Google Cloud

步驟

1. 在 BlueXP 主控台的右上角、選取「設定」圖示、然後選取 * 認證 * 。
2. 選取一組認證的動作功能表、然後選取 * 關聯訂閱 * 。



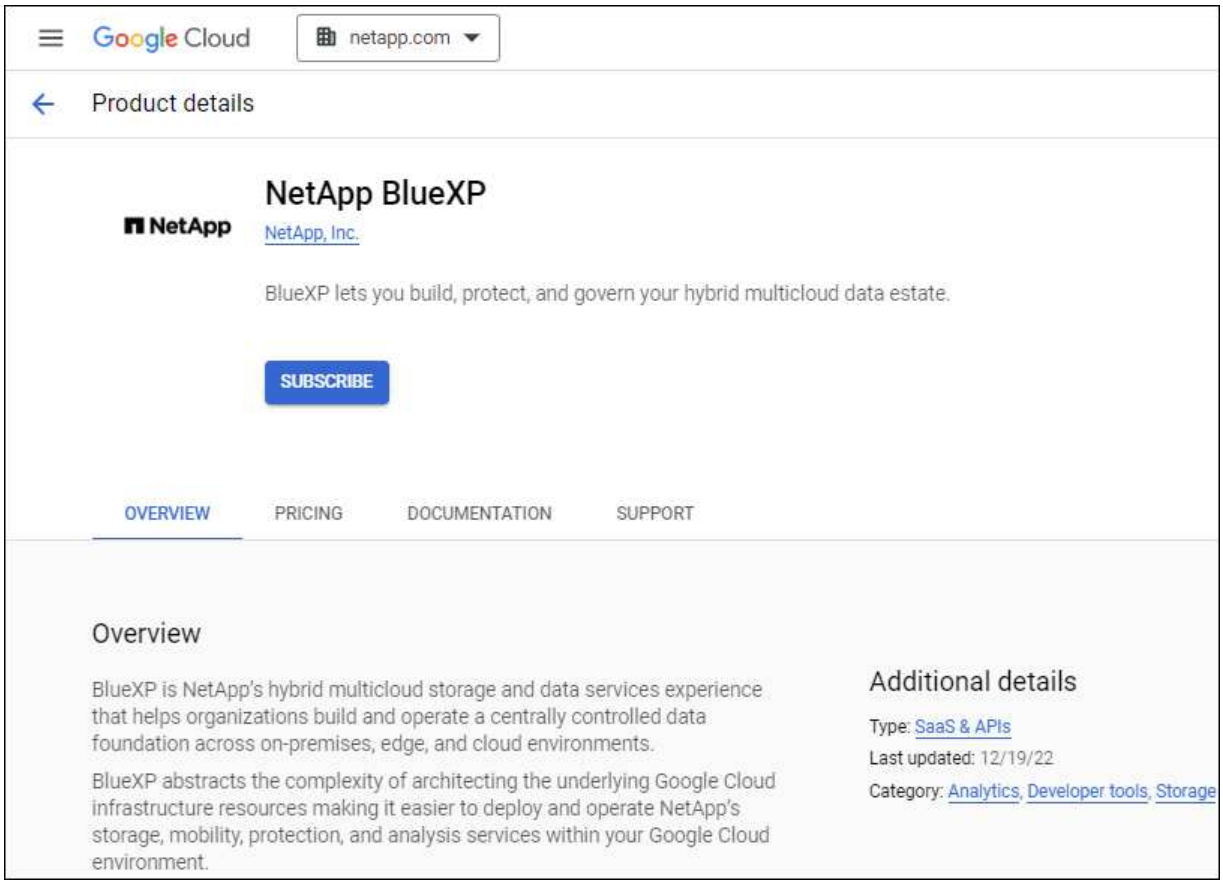
3. 若要將認證與現有訂閱建立關聯、請從下拉式清單中選取 Google Cloud 專案和訂閱、然後選取 * Associate* 。



4. 如果您尚未訂閱、請選取 * 新增訂閱 > 繼續 * 、然後依照 Google Cloud Marketplace 中的步驟進行。

> 在您完成下列步驟之前、請先確認您的Google Cloud帳戶擁有「帳單管理」權限、以及BlueXP登入權限。

a. 重新導向至之後 "Google Cloud Marketplace上的NetApp BlueXP頁面"下、請確定在頂端導覽功能表中選取正確的專案。



b. 選取 * 訂閱 * 。

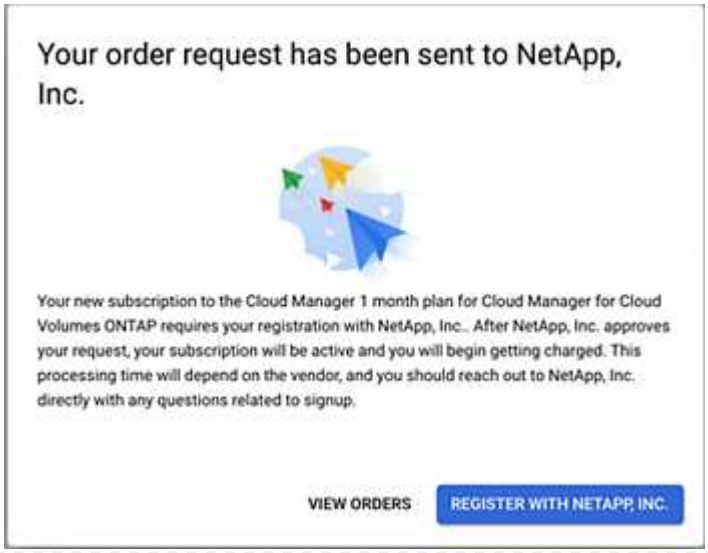
c. 選擇適當的帳單帳戶、並同意條款與條件。

d. 選取 * 訂閱 * 。

此步驟會將您的轉帳要求傳送給NetApp。

e. 在快顯對話方塊中、選取 * 註冊 NetApp 、 Inc.*

您必須完成此步驟、才能將 Google Cloud 訂閱連結至您的 BlueXP 帳戶。連結訂閱的程序要等到您從本頁重新導向、然後登入BluXP之後才會完成。



f. 完成「訂閱指派」頁面上的步驟：

> 如果貴組織的人員已從您的帳單帳戶訂閱NetApp BlueXP訂閱、您將會被重新導向至 "BlueXP網站上的「支持」頁面Cloud Volumes ONTAP" 而是。如果這是意外情況、請聯絡您的NetApp銷售團隊。Google每個Google帳單帳戶只能啟用一次訂閱。

- 選取您要與此訂閱建立關聯的 BlueXP 帳戶。
- 在「取代現有訂閱」欄位中、選擇您是否要使用此新訂閱來自動取代現有的單一帳戶訂閱。

  此新訂閱取代現有的帳戶所有認證訂閱。如果一組認證資料從未與訂閱建立關聯、則此新訂閱將不會與這些認證資料建立關聯。

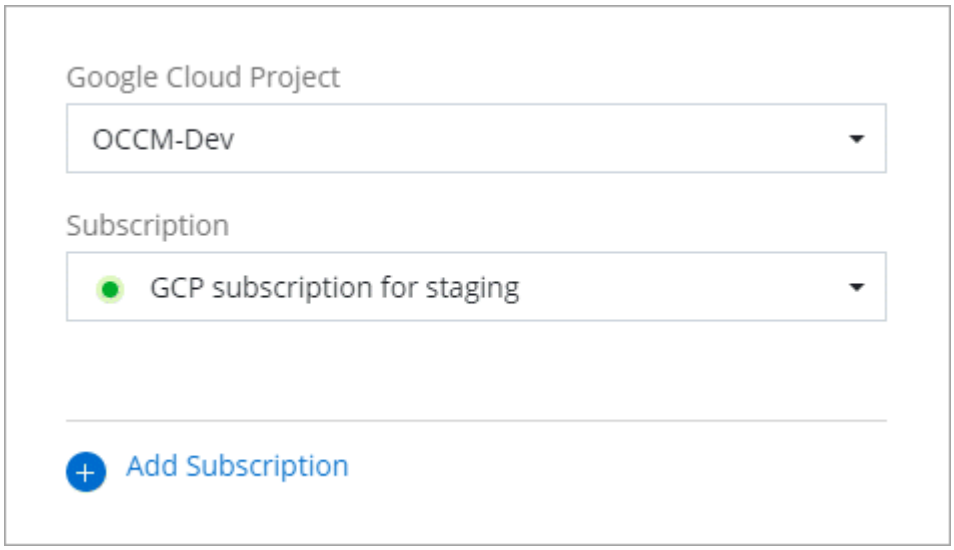
對於所有其他帳戶、您必須重複這些步驟、手動建立訂閱的關聯。

- 選擇*保存*。

  下列影片顯示從Google Cloud Marketplace訂閱的步驟：

從 Google Cloud Marketplace 訂閱 BlueXP

a. 完成此程序後、請瀏覽至BlueXP中的「認證」頁面、然後選取此新的訂閱。



相關連結

- "管理 Cloud Volumes ONTAP 的 BYOL 容量型授權"
- "管理 BlueXP 資料服務的 BYOL 授權"
- "管理適用於BlueXP的AWS認證與訂閱"
- "管理Azure認證資料與BlueXP訂閱"
- "管理 BlueXP 的 Google Cloud 認證和訂閱"

下一步操作（受限模式）

在受限模式下以 BlueXP 啟動並執行之後、您可以開始使用受限模式支援的 BlueXP 服務。

如需協助、請參閱以下服務的文件：

- "Amazon FSX for ONTAP Sfedocs"
- "文件Azure NetApp Files"
- "備份與還原文件"
- "分類文件"
- "文件Cloud Volumes ONTAP"
- "內部部署ONTAP 的叢集文件"
- "複寫文件"

相關連結

"BlueXP 部署模式"