開始使用私有模式

Setup and administration

NetApp
April 26, 2024

目錄

開始使用私有模式

入門工作流程（私有模式）

準備您的環境並部署 Connector 、以私有模式開始使用 BlueXP 。

私有模式通常用於沒有網際網路連線的內部環境、以及安全的雲端區域、包括 "AWS Secret Cloud"、 "AWS Top Secret Cloud"和 "Azure IL6."

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. 設定可存取目標網路的網路。
3. 對於雲端部署、請在雲端供應商中設定權限、以便在安裝軟體之後、將這些權限與 Connector 建立關聯。

2 **"部署 Connector"**

1. 在您自己的 Linux 主機上安裝 Connector 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. 對於雲端部署、請提供 BlueXP 先前設定的權限。

準備以私有模式進行部署

在以私有模式部署 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。

> 如果您想在中使用 BlueXP "AWS Secret Cloud" 或 "AWS Top Secret Cloud"然後，您應該按照單獨的說明在這些環境中開始使用。 "瞭解如何在 AWS Secret Cloud 或 Top Secret Cloud 中開始使用 Cloud Volumes ONTAP"

步驟 1 ：瞭解私有模式的運作方式

開始之前、您應該先瞭解 BlueXP 在私有模式下的運作方式。

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。

"瞭解私有模式的運作方式"。

步驟 2 ：檢閱安裝選項

在私有模式中、您可以在內部部署或雲端中手動安裝 Connector 、方法是在您自己的 Linux 主機上安裝 Connector 。

安裝 Connector 的位置決定了使用私有模式時可用的 BlueXP 服務和功能。例如、如果您想要部署和管理 Cloud Volumes ONTAP 、則必須將 Connector 安裝在雲端中。 "深入瞭解私有模式"。

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。

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 ：為 Connector 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。

用於日常作業的端點

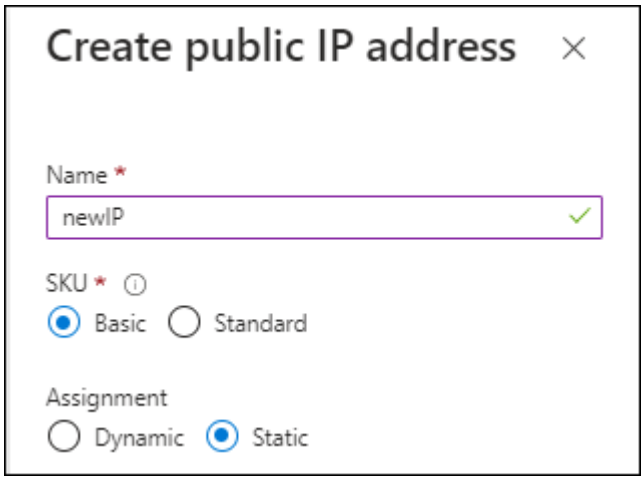
Connector 會聯絡下列端點、以管理公有雲環境中的資源和程序。

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.azure.microsoft.scloud https://login.microsoftonline.microsoft.scloud https://blob.core.microsoft.scloud https://core.microsoft.scloud	管理Azure IL6區域的資源。

端點	目的
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。
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。

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。

+
在私有模式下、 BlueXP 傳送輸出流量的唯一時間是傳送給雲端供應商、以便建立 Cloud Volumes ONTAP 系統。

連接埠

除非您啟動連接器、否則不會有傳入流量進入連接器。

HTTP （ 80 ）和 HTTPS （ 443 ）可讓您存取 BlueXP 主控台。只有在需要連線至主機進行疑難排解時、才需要SSH（22）。

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"

步驟 **5** ：準備雲端權限

如果 Connector 安裝在雲端、而您打算建立 Cloud Volumes ONTAP 系統、則 BlueXP 需要雲端供應商的權限。您需要在雲端供應商中設定權限、然後在安裝之後將這些權限與 Connector 執行個體建立關聯。

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。您需要手動將角色附加至 Connector 的 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. 在您計畫安裝 Connector 的 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 。

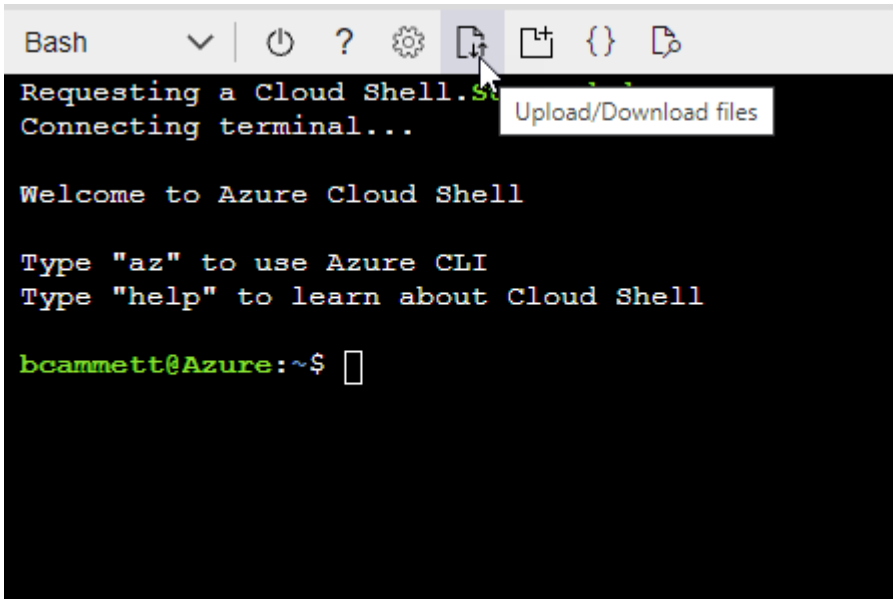
   - 範例 *

```
"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

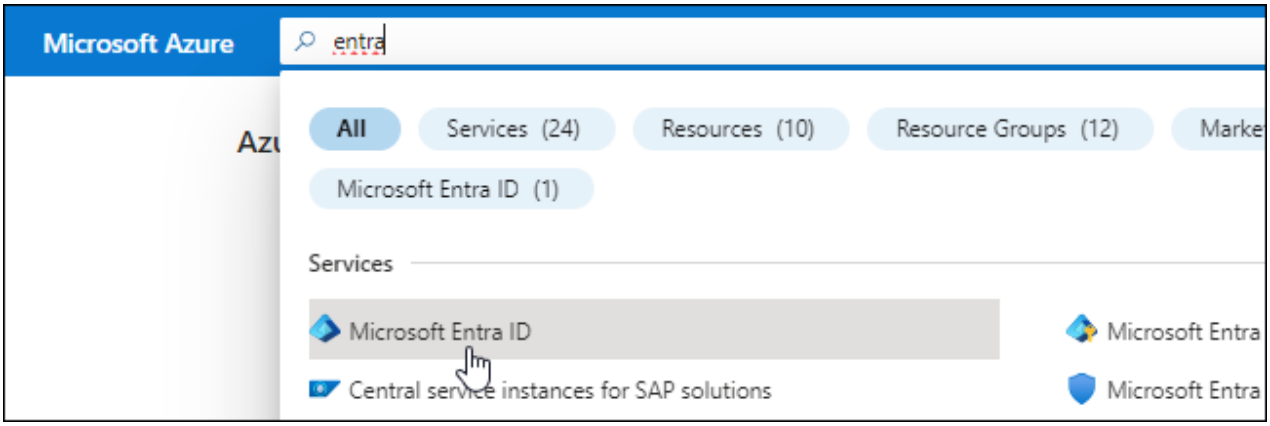
在 Microsoft Entra ID 中建立並設定服務主體、並取得 BlueXP 所需的 Azure 認證。安裝 Connector 並設定 BlueXP 之後、您必須提供 BlueXP 的這些認證。

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 。

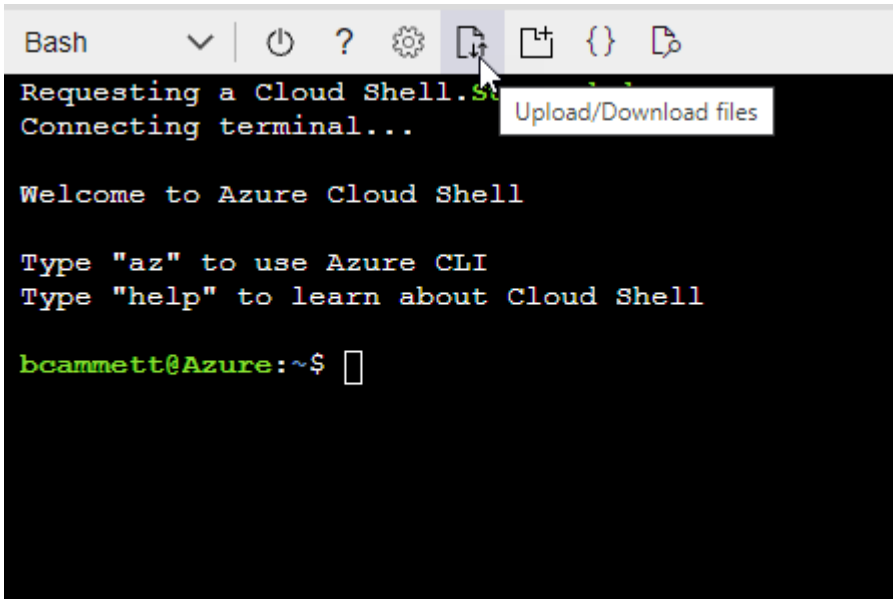
   - 範例 *

```
"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。



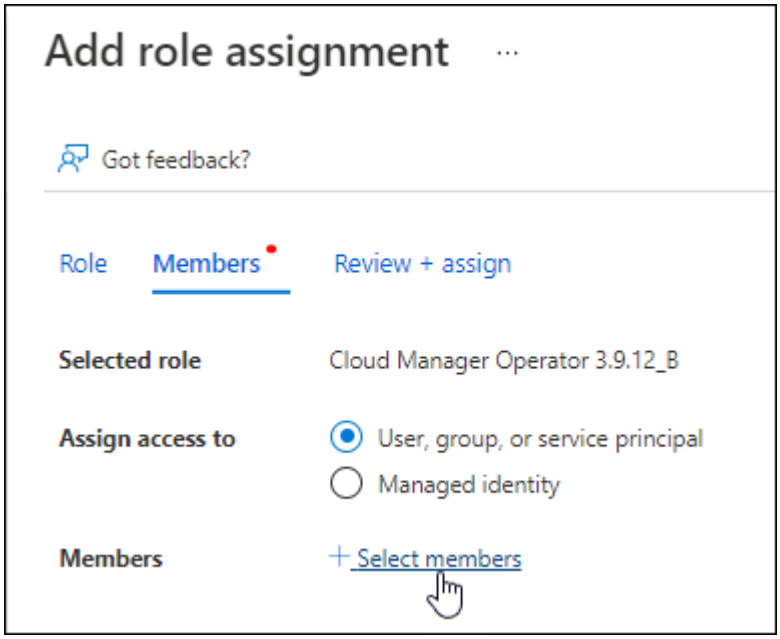
   - 使用Azure CLI建立自訂角色：

```
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。

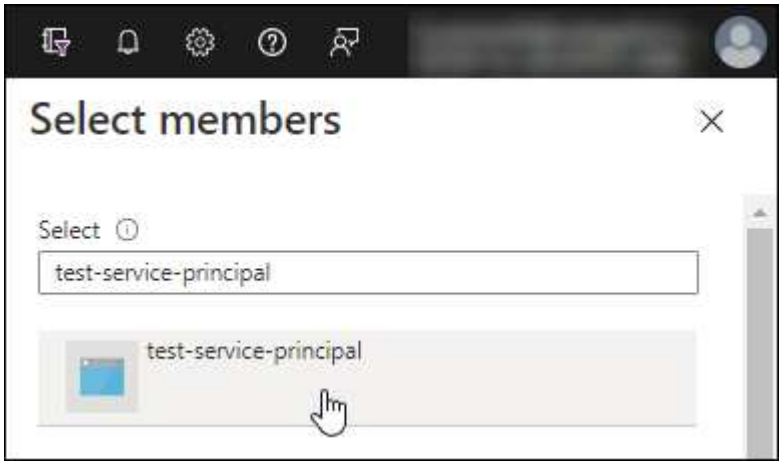
2. 將應用程式指派給角色：

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：



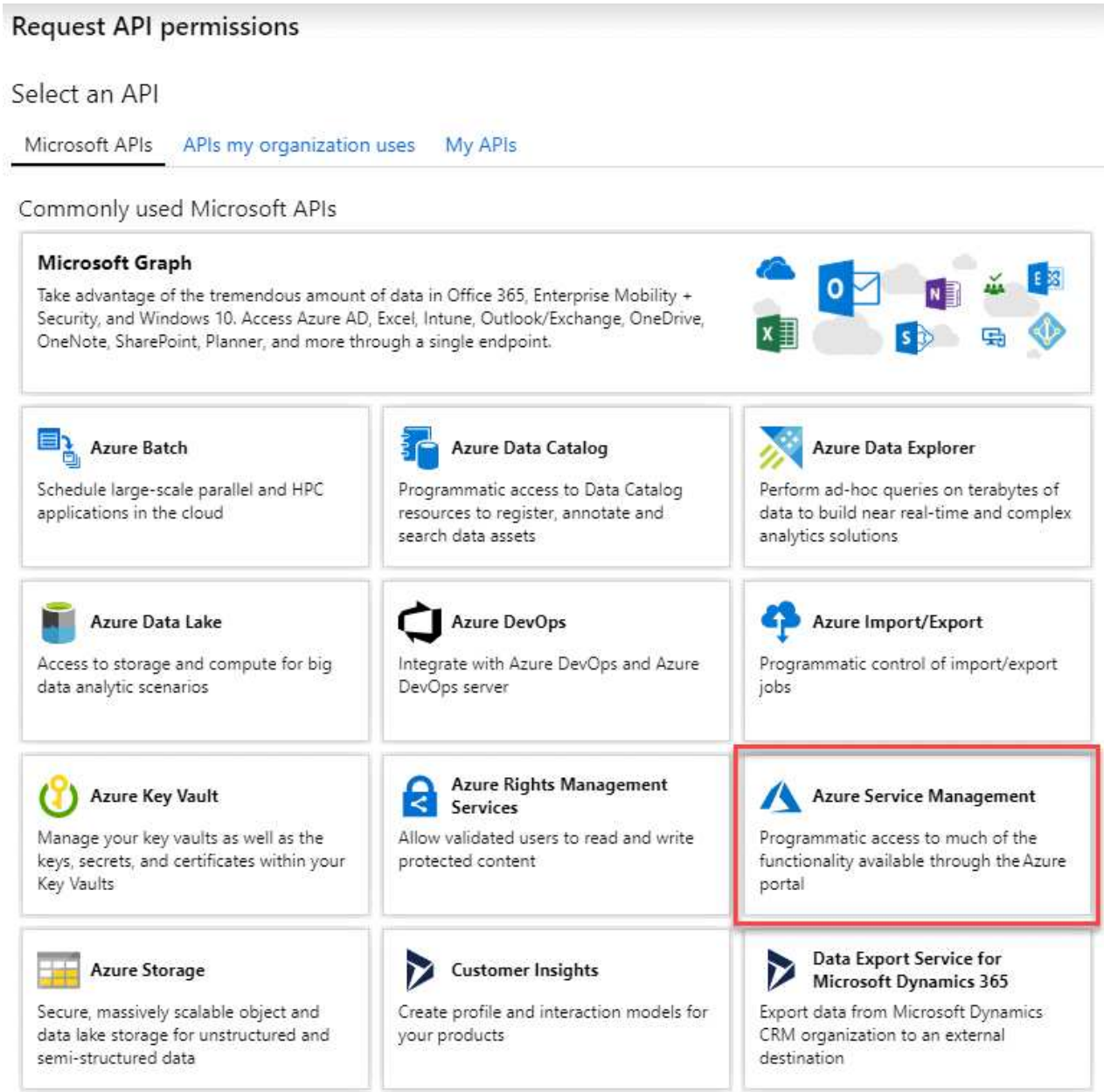
    - 選取應用程式、然後選取 * 選取 * 。
    - 選擇*下一步*。
f. 選取 * 檢閱 + 指派 * 。

服務主體現在擁有部署Connector所需的Azure權限。

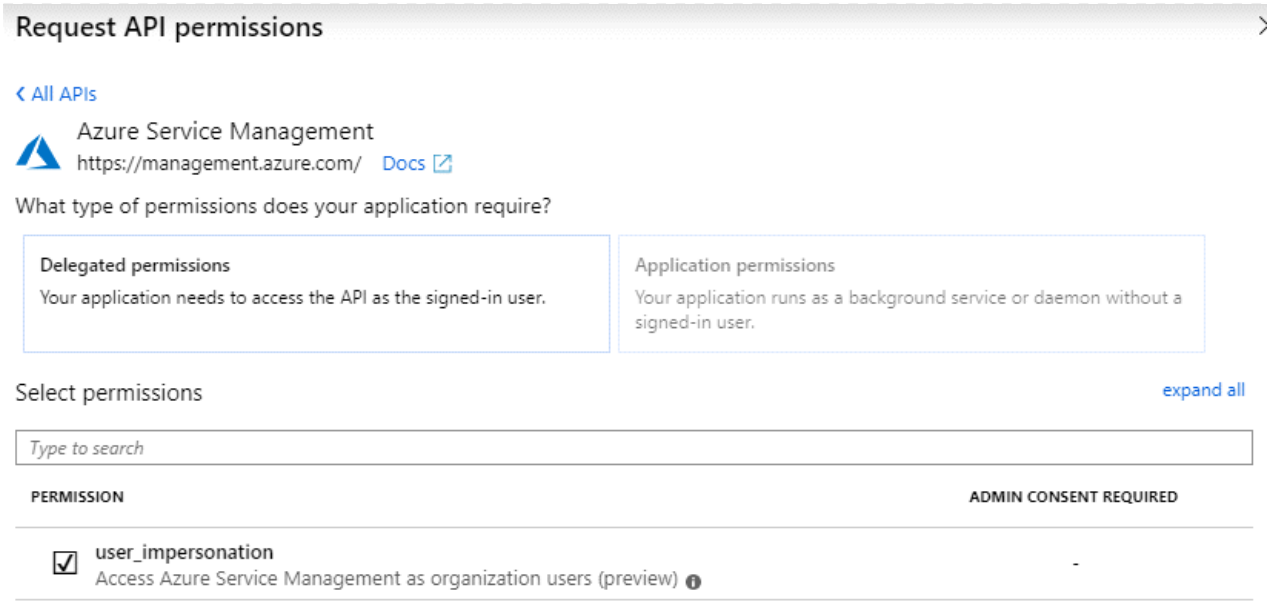
如果您想要從 Cloud Volumes ONTAP 多個 Azure 訂閱中部署支援功能、則必須將服務授權對象繫結至每個訂閱項目。BlueXP可讓您選擇部署Cloud Volumes ONTAP 時要使用的訂閱內容。

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 * 」。

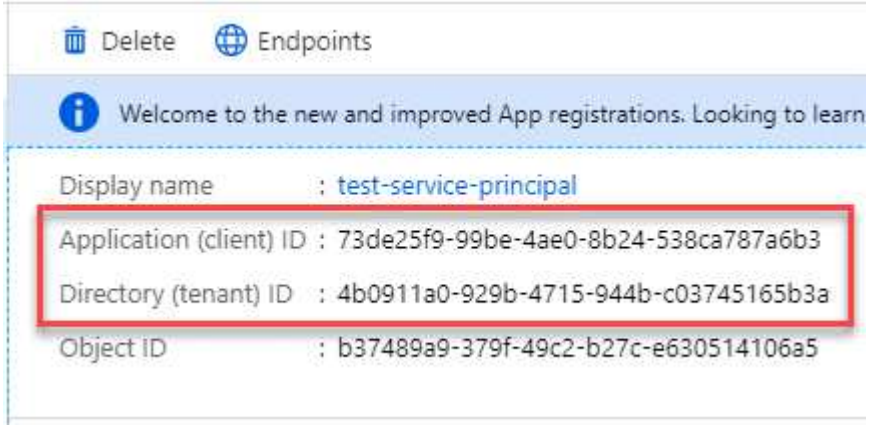


4. 選取 * 以組織使用者身分存取 Azure 服務管理 * 、然後選取 * 新增權限 * 。



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）

以私有模式部署 Connector

以私有模式部署 Connector 、讓您可以使用 BlueXP 、而不需外傳連線至 BlueXP SaaS 層。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 NetApp 支援網站 下載產品安裝程式、然後在您自己的 Linux 主機上手動安裝 Connector 。

如果您想在中使用 BlueXP "AWS Secret Cloud" 或 "AWS Top Secret Cloud"然後，您應該按照單獨的說明在這些環境中開始使用。 "瞭解如何在 AWS Secret Cloud 或 Top Secret Cloud 中開始使用 Cloud Volumes ONTAP"

開始之前

需要root權限才能安裝Connector。

步驟

1. 確認已啟用並執行Docker。

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

2. 從下載Connector軟體 "NetApp 支援網站"

    請務必下載無網際網路存取的私有網路離線安裝程式。

3. 將安裝程式複製到Linux主機。
4. 指派執行指令碼的權限。

```
chmod +x /path/BlueXP-Connector-offline-<version>
```

其中、就是您下載的Connector版本<version> 。

5. 執行安裝指令碼：

```
sudo /path/BlueXP-Connector-offline-<version>
```

其中、就是您下載的Connector版本<version> 。

結果

已安裝 Connector 軟體。您現在可以設定 BlueXP 。

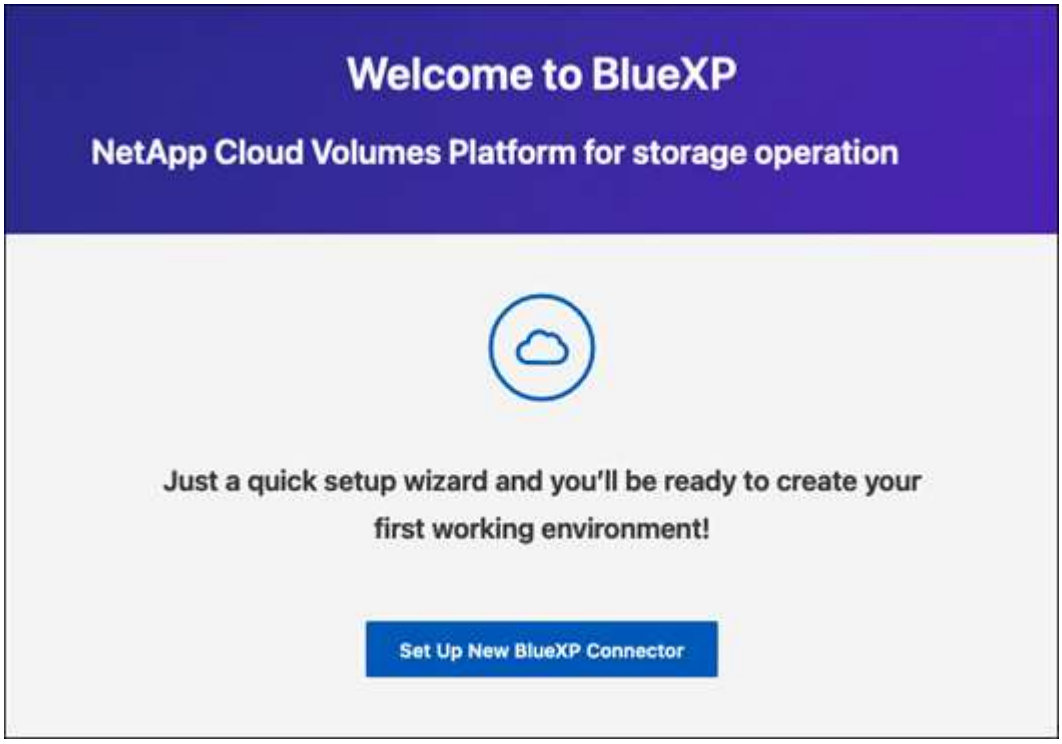
步驟 2 ：設定 BlueXP

第一次存取 BlueXP 主控台時、系統會提示您設定 BlueXP 。

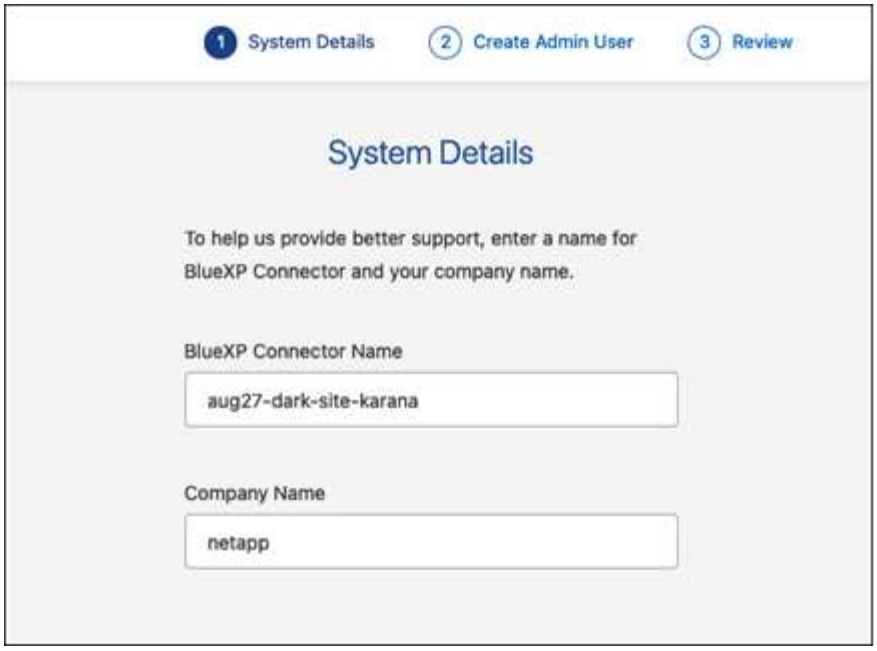
步驟

1. 開啟網頁瀏覽器並輸入 https://ipaddress 其中 ipaddress 是您安裝 Connector 的 Linux 主機的 IP 位址。

   您應該會看到下列畫面。



2. 選取 * 設定新的 BlueXP Connector* 、然後依照提示設定系統。
   - 系統詳細資料：輸入Connector的名稱及您的公司名稱。



- * 建立管理員使用者 * ：為系統建立管理員使用者。

  此使用者帳戶在本機系統上執行。無法透過BlueXP連線至驗證0服務。

- * 審查 * ：檢閱詳細資料、接受授權合約、然後選取 * 設定 * 。

3. 使用您剛建立的管理使用者登入BlueXP。

結果

現在已安裝並設定 Connector 。

當有新版 Connector 軟體推出時，這些軟體都會發佈至 NetApp 支援網站。 "瞭解如何升級Connector"。

接下來呢？

提供 BlueXP 先前設定的權限。

步驟 3 ：提供 BlueXP 的權限

如果您想要建立 Cloud Volumes ONTAP 工作環境、您必須提供 BlueXP 先前設定的雲端權限。

"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 Connector EC2 執行個體。

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。

下一步操作（私有模式）

以私人模式使用 BlueXP 開始運作後、您可以開始使用受私有模式支援的 BlueXP 服務。

如需協助、請參閱下列文件：

- "建立 Cloud Volumes ONTAP 系統"
- "探索內部部署ONTAP 的叢集"
- "複寫資料"
- "使用 BlueXP 分類掃描內部部署 ONTAP Volume 資料"
- "使用 BlueXP 備份與還原、將內部部署的 ONTAP Volume 資料備份至 StorageGRID"

相關連結

"BlueXP 部署模式"