Azure

Setup and administration

NetApp
April 26, 2024

目錄

Azure

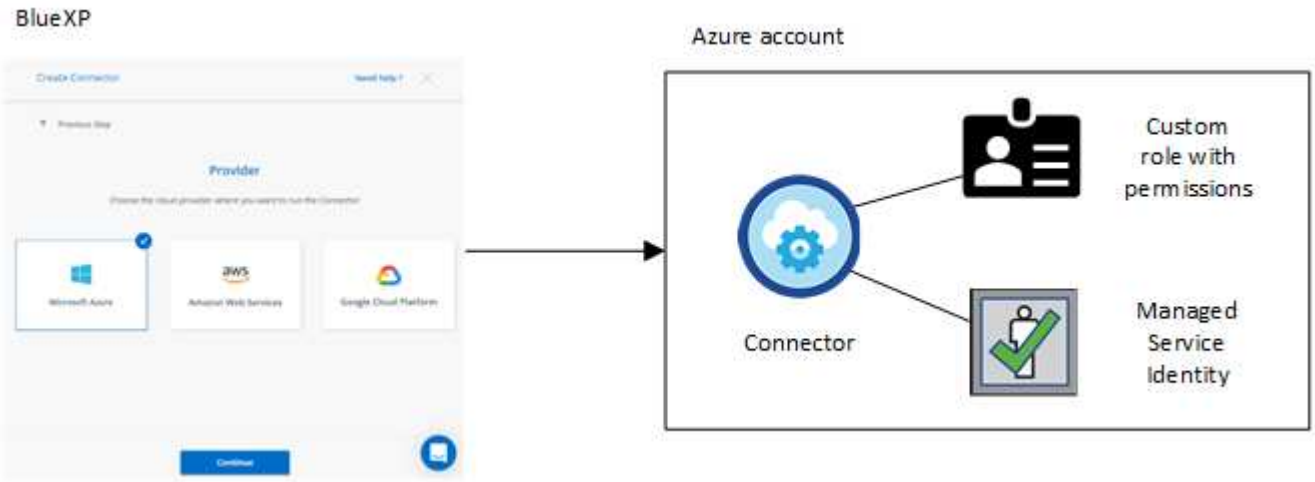
瞭解Azure認證與權限

瞭解 BlueXP 如何使用 Azure 認證來代表您執行動作、以及這些認證如何與市場訂閱相關聯。瞭解這些詳細資料有助於您管理一或多個 Azure 訂閱的認證。例如、您可能想要瞭解何時將額外的 Azure 認證新增至 BlueXP 。

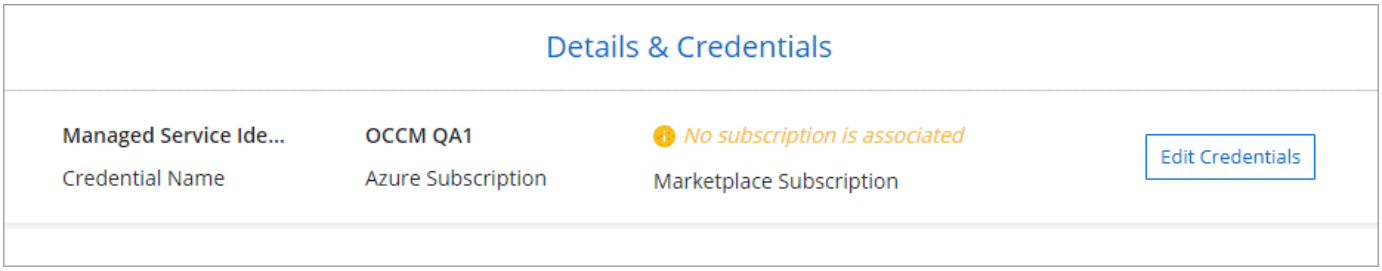
Azure 初始認證

從BlueXP部署Connector時、您需要使用具備部署Connector虛擬機器權限的Azure帳戶或服務主體。所需權限列於 "Azure 的連接器部署原則"。

當BlueXP在Azure中部署Connector虛擬機器時、它會啟用 "系統指派的託管身分識別" 在虛擬機器上建立自訂角色、然後將其指派給虛擬機器。此角色可為BlueXP提供所需的權限、以管理該Azure訂閱中的資源和程序。 "檢閱BlueXP如何使用權限"。



如果您為 Cloud Volumes ONTAP 建立新的工作環境、 BlueXP 預設會選取以下 Azure 認證：



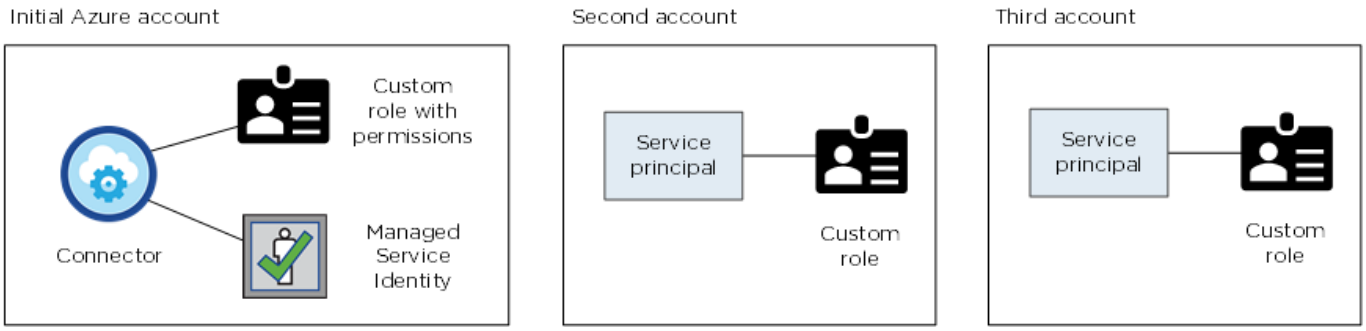
您可以 Cloud Volumes ONTAP 使用初始 Azure 認證來部署所有的整套系統、也可以新增其他認證資料。

額外的 Azure 訂閱、提供託管身分識別

指派給 Connector VM 的系統指派託管身分識別與您啟動 Connector 的訂閱相關聯。如果您想要選擇不同的 Azure 訂閱、則需要 "將託管身分識別與這些訂閱建立關聯"。

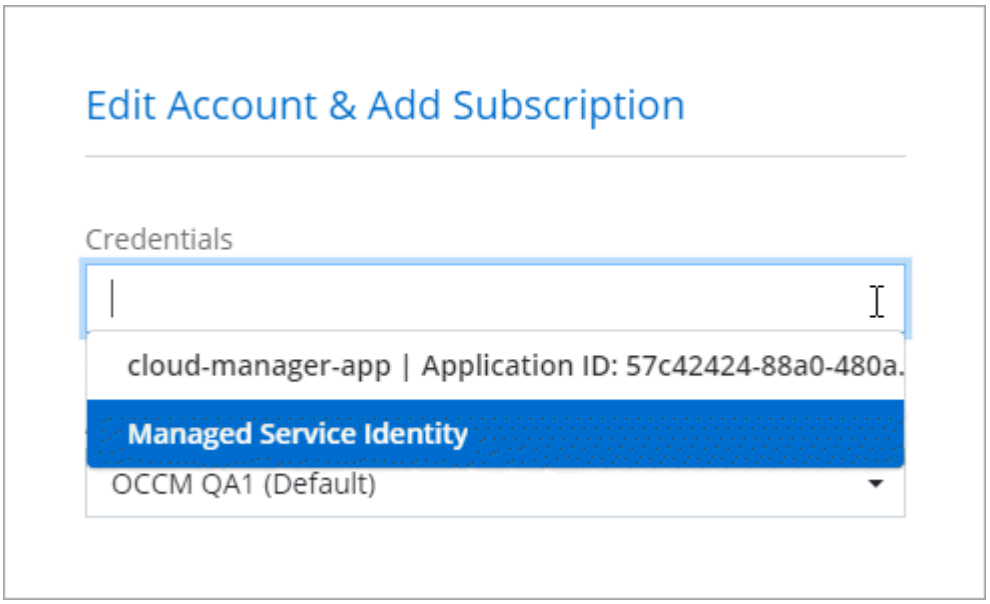
其他 Azure 認證資料

如果您想要將不同的 Azure 認證搭配 BlueXP 使用、則必須將必要的權限授予 "在 Microsoft Entra ID 中建立及設定服務主體" 針對每個 Azure 帳戶。下圖顯示兩個額外的帳戶、每個帳戶都設有提供權限的服務主體和自訂角色：



您可以 "將帳戶認證新增至BlueXP" 提供 AD 服務主體的詳細資料。

例如、您可以在建立新的 Cloud Volumes ONTAP 工作環境時、在認證之間切換：



認證與市場訂閱

您新增至 Connector 的認證必須與 Azure Marketplace 訂閱相關聯、才能以每小時費率（PAYGO）或每年合約支付 Cloud Volumes ONTAP 費用、以及使用其他 BlueXP 服務。

"瞭解如何建立Azure訂閱的關聯"。

請注意以下關於 Azure 認證與市場訂閱的資訊：

- 您只能將一項 Azure Marketplace 訂閱與一組 Azure 認證建立關聯
- 您可以使用新訂閱來取代現有的市場訂閱

常見問題集

下列問題與認證和訂閱有關。

我可以變更適用於 **Cloud Volumes ONTAP** 工作環境的 **Azure Marketplace** 訂閱嗎？

是的、您可以。當您變更與一組 Azure 認證相關聯的 Azure Marketplace 訂閱時、所有現有和新的 Cloud Volumes ONTAP 工作環境都將從新訂閱中扣除費用。

"瞭解如何建立Azure訂閱的關聯"。

我是否可以新增多個 **Azure** 認證、每個認證都有不同的市場訂閱？

屬於同一 Azure 訂閱的所有 Azure 認證資料將與同一 Azure Marketplace 訂閱相關聯。

如果您有多個 Azure 認證屬於不同的 Azure 訂閱、則這些認證可以與相同的 Azure Marketplace 訂閱或不同的市場訂閱相關聯。

我可以將現有的 **Cloud Volumes ONTAP** 工作環境移轉至不同的 **Azure** 訂閱嗎？

否、您無法將與 Cloud Volumes ONTAP 工作環境相關的 Azure 資源移轉至不同的 Azure 訂閱。

認證如何適用於市場部署和內部部署？

以上各節說明建議的連接器部署方法、該方法來自於BlueXP。您也可以從 Azure Marketplace 在 Azure 中部署 Connector 、也可以在自己的 Linux 主機上安裝 Connector 軟體。

如果您使用 Marketplace 、您可以將自訂角色指派給 Connector VM 和系統指派的託管身分識別、以提供權限、或是使用 Microsoft Entra 服務主體。

對於內部部署、您無法設定 Connector 的託管身分識別、但可以使用服務主體來提供權限。

若要瞭解如何設定權限、請參閱下列頁面：

- 標準模式
  - "設定 Azure Marketplace 部署的權限"
  - "設定內部部署的權限"
- "設定受限模式的權限"
- "設定私有模式的權限"

管理 **BlueXP** 的 **Azure** 認證和市場訂閱

新增及管理 Azure 認證、讓 BlueXP 擁有在 Azure 訂閱中部署及管理雲端資源所需的權限。如果您管理多個 Azure Marketplace 訂閱、您可以從「認證」頁面將每個訂閱指派給不同的 Azure 認證。

如果您需要使用多個Azure認證或多個Azure Marketplace訂閱Cloud Volumes ONTAP 以供使用、請依照本頁的步驟進行。

總覽

在BlueXP中新增額外Azure訂閱和認證的方法有兩種。

1. 將額外的Azure訂閱與Azure託管身分識別建立關聯。
2. 如果您要使用Cloud Volumes ONTAP 不同的Azure認證資料來部署功能、請使用服務主體來授予Azure權限、並將其認證資料新增至藍圖XP。

將額外的 **Azure** 訂閱與託管身分識別建立關聯

BlueXP可讓您選擇要部署Cloud Volumes ONTAP 的Azure認證和Azure訂閱。除非您建立關聯、否則您無法為託管身分識別設定檔選取不同的 Azure 訂閱 "託管身分識別" 這些訂閱。

關於這項工作

託管身分識別是 "初始 Azure 帳戶" 當您從BlueXP部署連接器時。部署Connector時、BlueXP會建立BlueXP運算子角色、並將其指派給Connector虛擬機器。

步驟

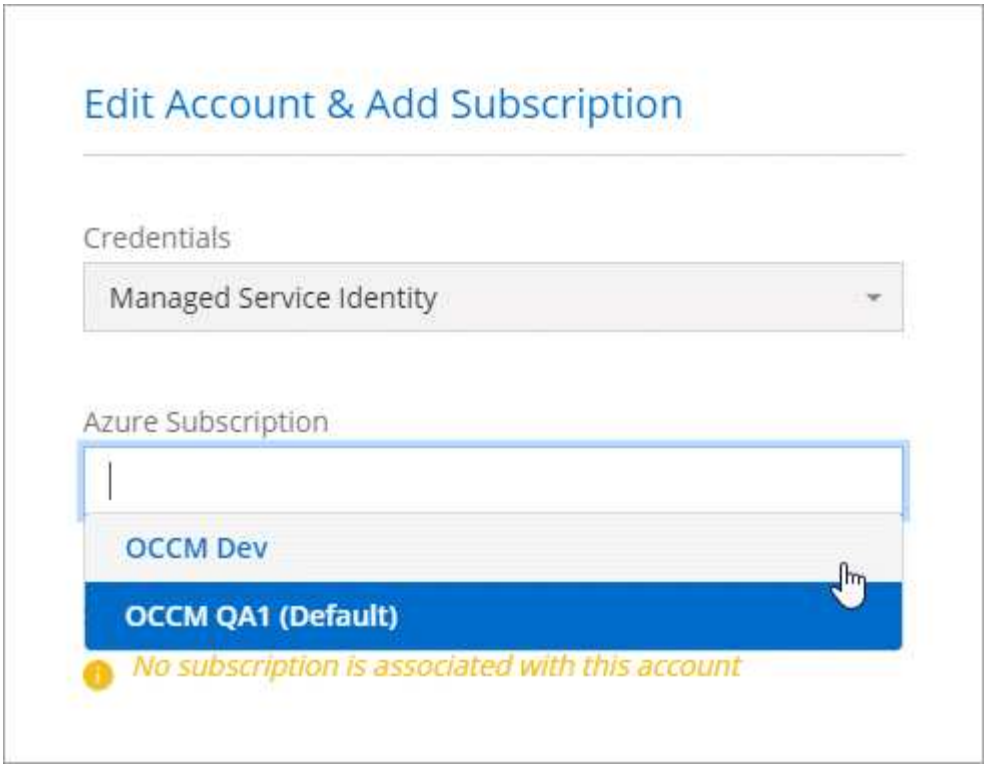
1. 登入 Azure 入口網站。
2. 開啟 * 訂閱 * 服務、然後選取您要部署 Cloud Volumes ONTAP 的訂閱內容。
3. 選取 * 存取控制（IAM） * 。
   a. 選取 * 新增 * > * 新增角色指派 * 、然後新增權限：
      - 選取*藍圖操作員*角色。

        BlueXP運算子是Connector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。

      - 指派 * 虛擬機器 * 的存取權。
      - 選取建立 Connector 虛擬機器的訂閱。
      - 選取 Connector 虛擬機器。
      - 選擇*保存*。
4. 請重複這些步驟以取得額外訂閱內容。

結果

當您建立新的工作環境時、現在應該能夠從多個 Azure 訂閱中選取託管身分識別設定檔。



將額外的 **Azure** 認證新增至 **BlueXP**

從BlueXP部署Connector時、BlueXP會在擁有必要權限的虛擬機器上啟用系統指派的託管身分識別。當您建立Cloud Volumes ONTAP 全新的作業系統環境時、BlueXP會預設選取這些Azure認證資料。

> 如果您在現有系統上手動安裝Connector軟體、則不會新增一組初始認證資料。 "瞭解Azure認證與權限"。

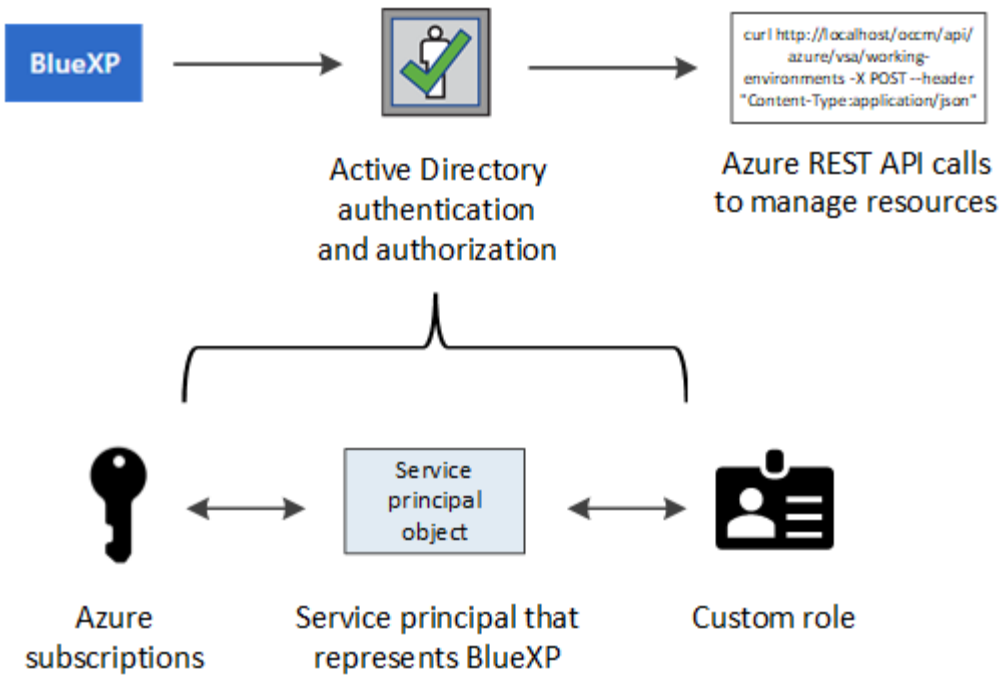
如果您想要使用 _different 的 Azure 認證來部署 Cloud Volumes ONTAP 、則必須在每個 Azure 帳戶的 Microsoft Entra ID 中建立及設定服務主體、以授予必要的權限。然後您可以將新認證新增至藍圖XP。

使用服務主體授與 **Azure** 權限

BlueXP需要權限才能在Azure中執行動作。您可以在 Microsoft Entra ID 中建立及設定服務主體、並取得 BlueXP 所需的 Azure 認證、將必要權限授予 Azure 帳戶。

關於這項工作

下圖說明BlueXP如何取得權限在Azure中執行作業。服務主體物件與一或多個 Azure 訂閱相關、代表 Microsoft Entra ID 中的 BlueXP 、並指派給允許必要權限的自訂角色。



步驟

1. 建立 Microsoft Entra 應用程式。
2. [將應用程式指派給角色]。
3. 新增 Windows Azure Service Management API 權限。
4. 取得應用程式 ID 和目錄 ID。
5. [建立用戶端機密]。

建立 **Microsoft Entra** 應用程式

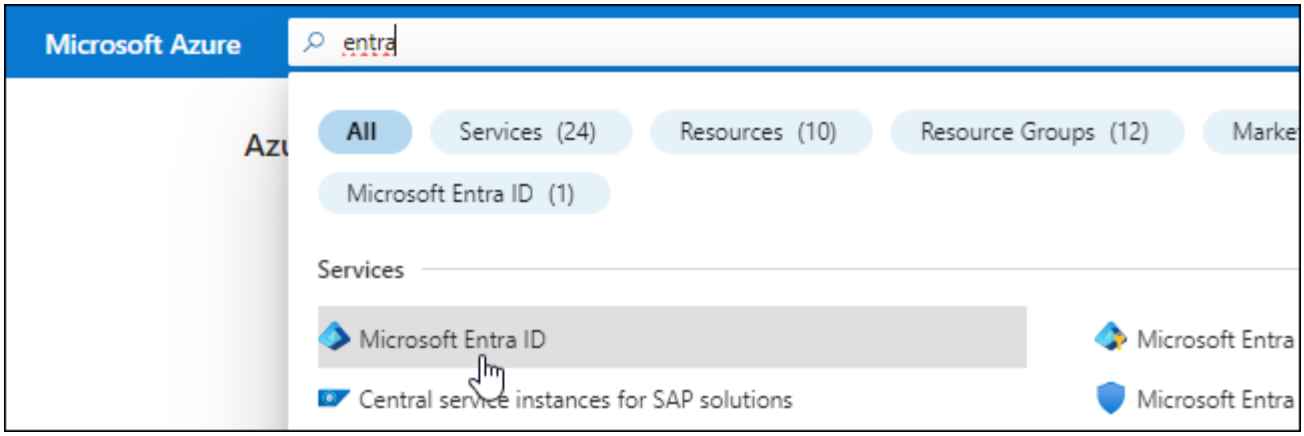
建立 Microsoft Entra 應用程式和服務主體、讓 BlueXP 用於角色型存取控制。

步驟

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。

結果

您已建立 AD 應用程式和服務主體。

將應用程式指派給角色

您必須將服務主體繫結至一或多個Azure訂閱、並指派自訂的「BlueXP運算子」角色給它、以便BlueXP在Azure中擁有權限。

步驟

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 。

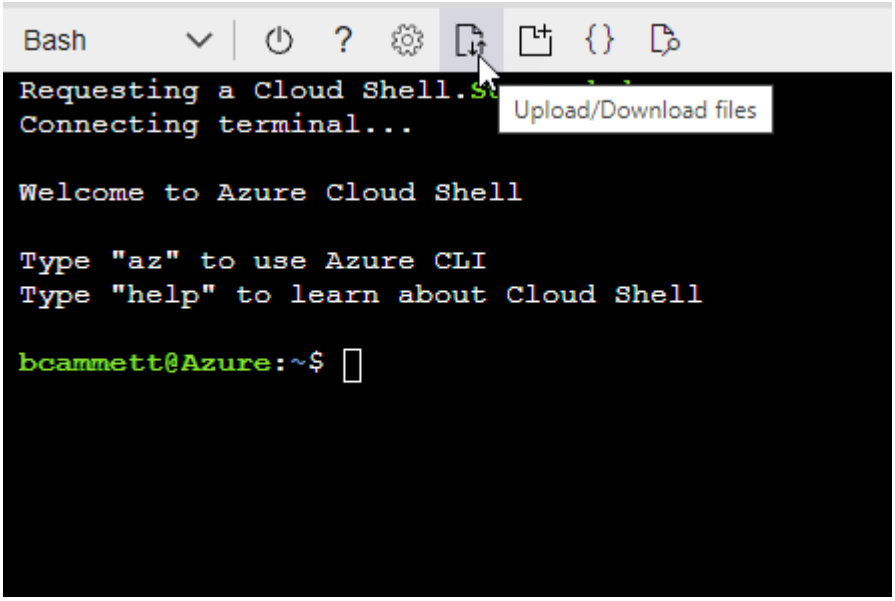
      - 範例 *

```
"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。

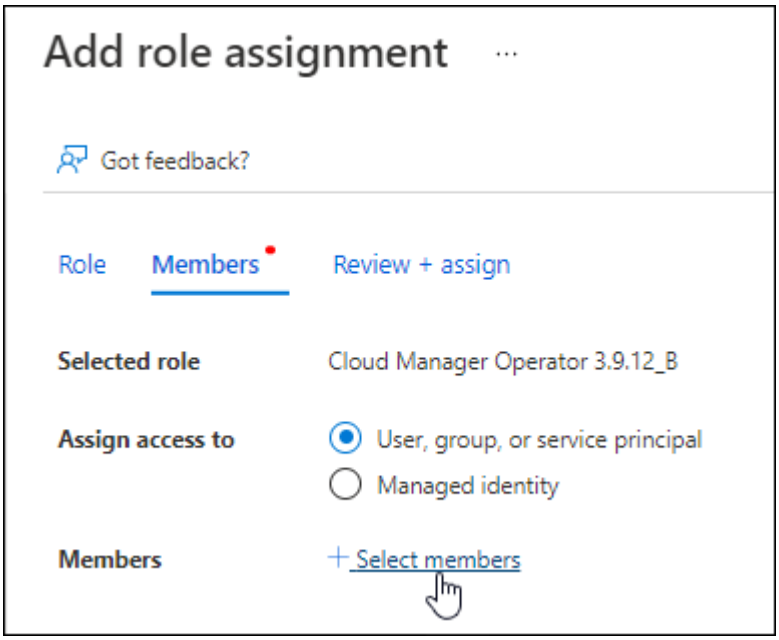
b. 選取訂閱。

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 * 。

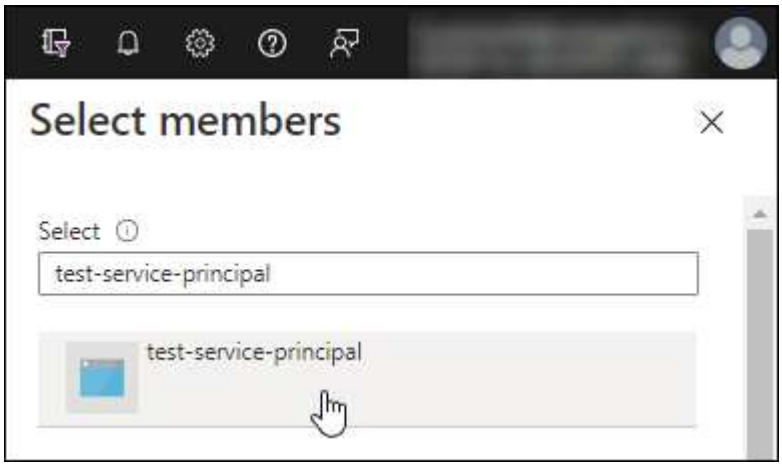
e. 在「成員」索引標籤中、完成下列步驟：

- 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。

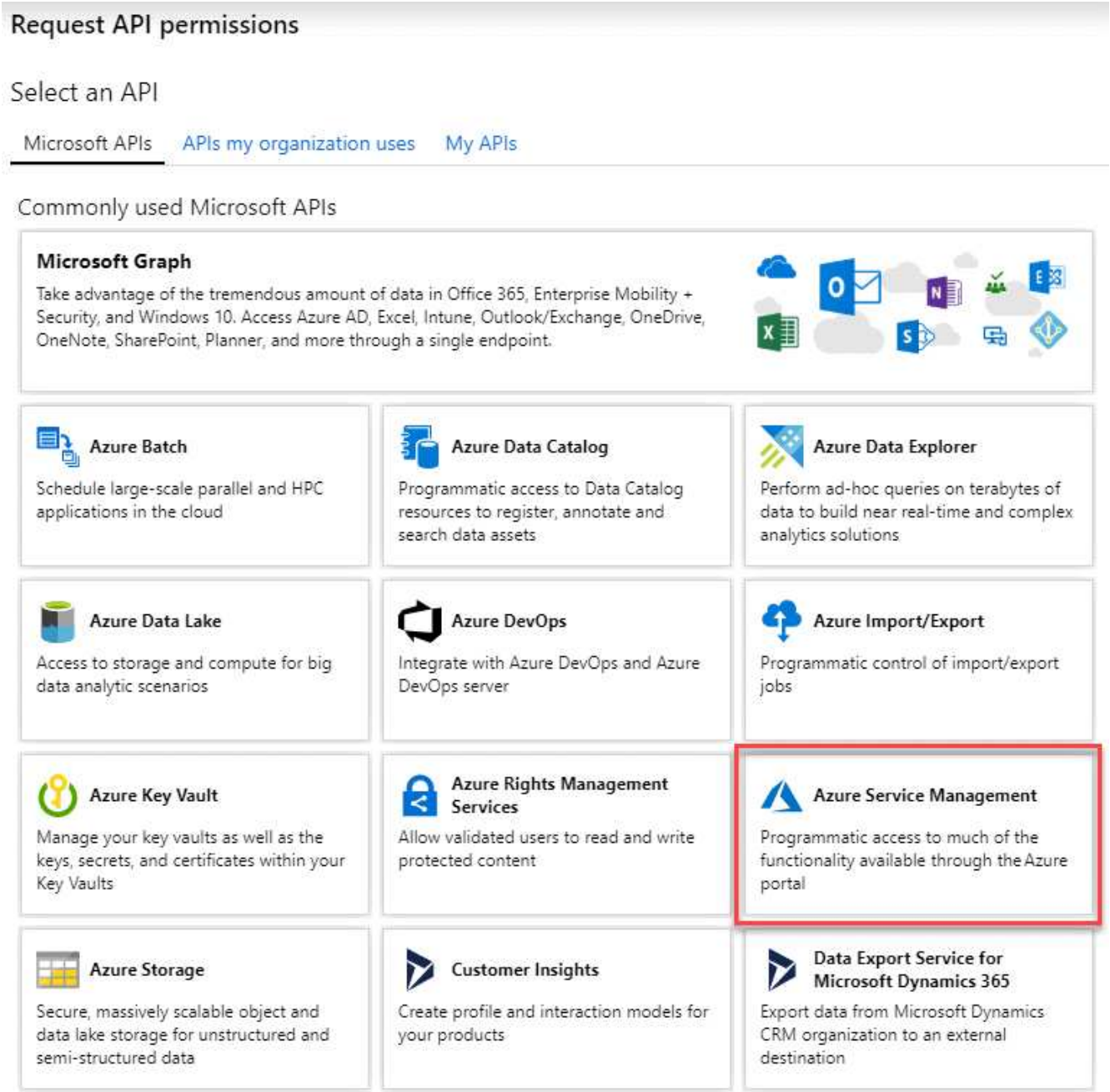
如果您想要從 Cloud Volumes ONTAP 多個 Azure 訂閱中部署支援功能、則必須將服務授權對象繫結至每個訂閱項目。BlueXP可讓您選擇部署Cloud Volumes ONTAP 時要使用的訂閱內容。

新增 **Windows Azure Service Management API** 權限

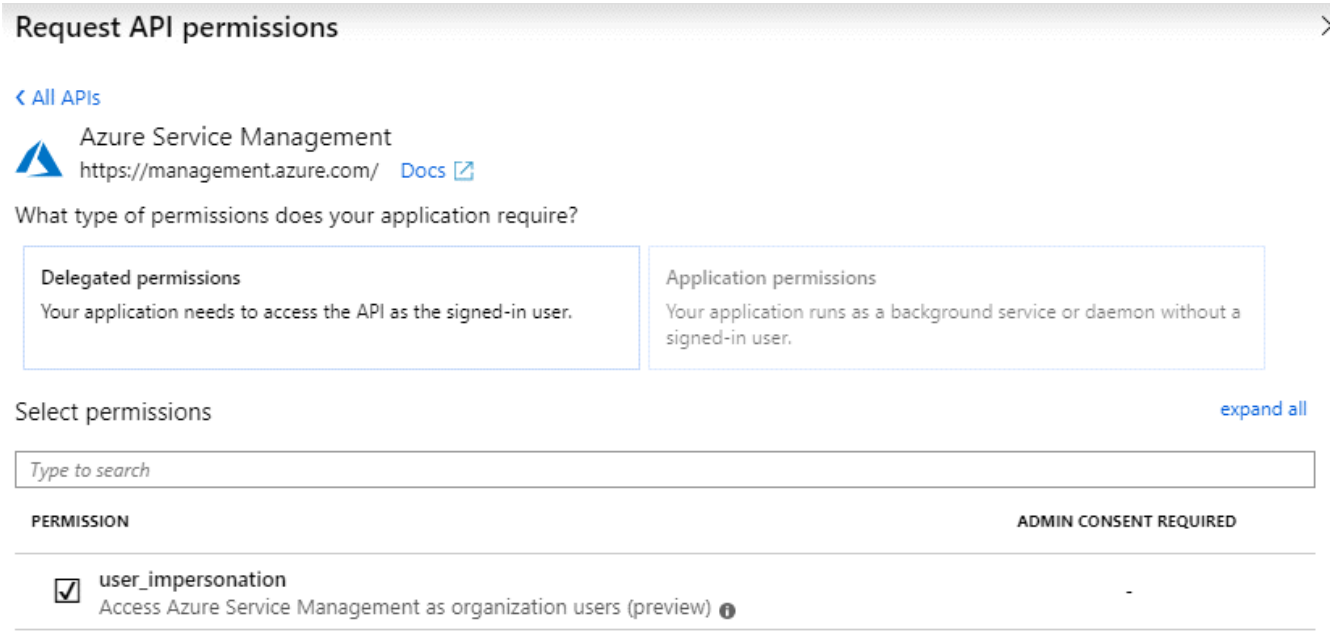
服務主體必須具有「 Windows Azure Service Management API 」權限。

步驟

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 * 。

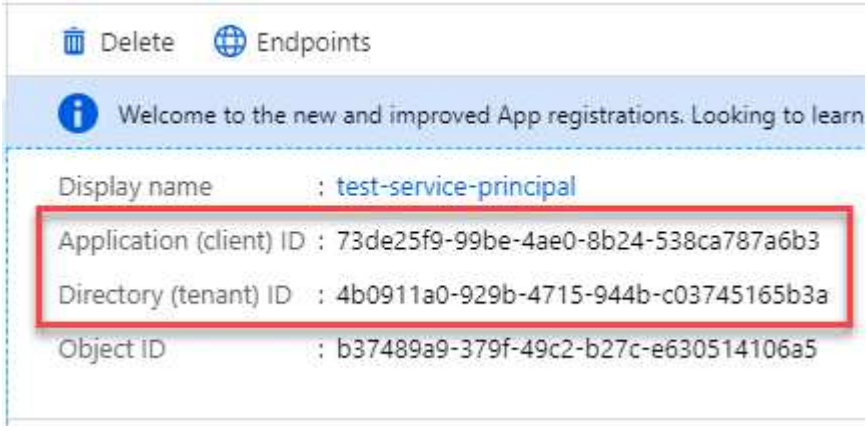


取得應用程式 **ID** 和目錄 **ID**

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。

步驟

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

您需要建立用戶端機密、然後提供 BlueXP 的機密值、以便 BlueXP 使用它來驗證 Microsoft Entra ID 。

步驟

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。

將認證資料新增至藍圖**XP**

在您提供Azure帳戶所需的權限之後、即可將該帳戶的認證資料新增至BlueXP。完成此步驟可讓您Cloud Volumes ONTAP 使用不同的Azure認證資料來啟動功能。

開始之前

如果您剛在雲端供應商中建立這些認證資料、可能需要幾分鐘的時間才能使用。請稍候幾分鐘、再將認證資料新增至BlueXP。

開始之前

您必須先建立連接器、才能變更BlueXP設定。 "瞭解如何建立連接器"。

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

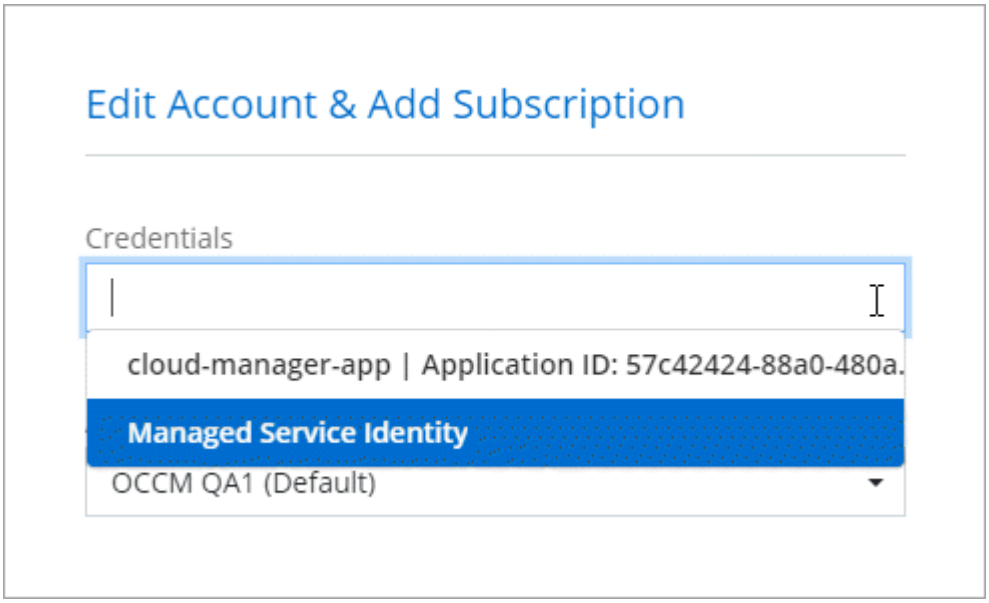
- 用戶端機密

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

您現在可以從「詳細資料與認證」頁面切換至不同的認證集合 "在建立新的工作環境時"



管理現有認證資料

透過建立Marketplace訂閱、編輯認證及刪除認證、來管理您已新增至BlueXP的Azure認證資料。

將 **Azure Marketplace** 訂閱與認證建立關聯

將Azure認證資料新增至BlueXP之後、您就可以將Azure Marketplace訂閱與這些認證資料建立關聯。訂閱可讓您建立隨用隨付的 Cloud Volumes ONTAP 系統、並使用其他 BlueXP 服務。

您可能會在將認證新增至BlueXP之後、在兩種情況下建立Azure Marketplace訂閱的關聯：

- 當您初次將認證新增至BlueXP時、並未建立訂閱關聯。
- 您想要變更與 Azure 認證相關的 Azure Marketplace 訂閱。

  以新訂閱取代目前的市場訂閱、可變更任何現有 Cloud Volumes ONTAP 工作環境和所有新工作環境的市場訂閱。

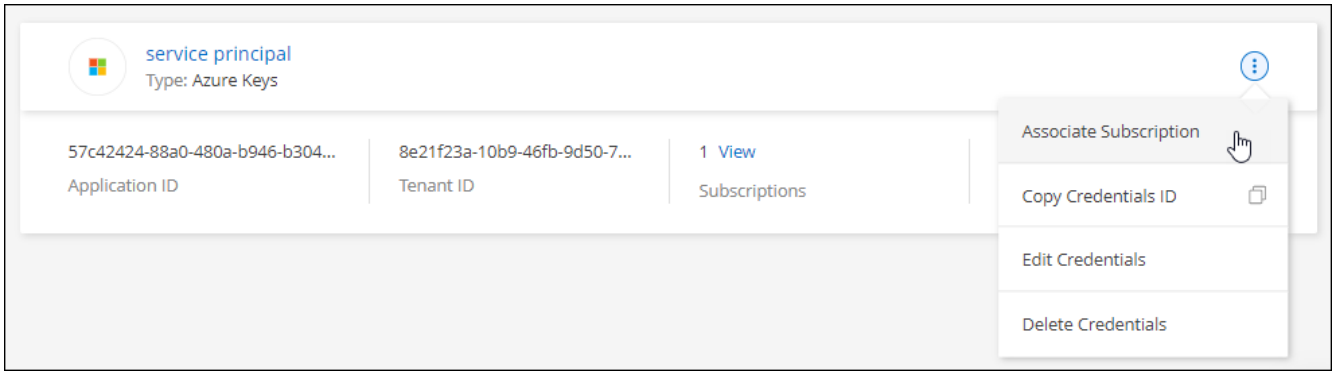
開始之前

您必須先建立連接器、才能變更BlueXP設定。 "瞭解方法"。

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

編輯認證資料

修改Azure服務認證資料的詳細資料、即可在BlueXP中編輯Azure認證資料。例如、如果為服務主體應用程式建立新的密碼、您可能需要更新用戶端密碼。

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. 在 * 帳戶認證 * 頁面上、選取一組認證的動作功能表、然後選取 * 編輯認證 * 。
3. 進行必要的變更、然後選取 * 套用 * 。

刪除認證

如果您不再需要一組認證資料、可以從BlueXP中刪除。您只能刪除與工作環境無關的認證資料。

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. 在 * 帳戶認證 * 頁面上、選取一組認證的動作功能表、然後選取 * 刪除認證 * 。
3. 選擇 * 刪除 * 進行確認。