



開始使用標準模式

Setup and administration

NetApp
April 26, 2024

目錄

開始使用標準模式.....	1
入門工作流程（標準模式）.....	1
準備使用 BlueXP 主控台的網路連線.....	2
註冊BlueXP.....	3
建立連接器.....	4
訂閱 BlueXP（標準模式）.....	99
下一步操作（標準模式）.....	105

開始使用標準模式

入門工作流程（標準模式）

準備 BlueXP 主控台的網路、註冊並建立帳戶、選擇性建立 Connector、以及訂閱 BlueXP、以標準模式開始使用 BlueXP。

在標準模式中、使用者可從網路型主控台以雲端服務的形式存取 BlueXP。開始之前、您應該先瞭解 ["BlueXP 帳戶"](#)、["連接器"](#)和 ["部署模式"](#)。

1

"準備使用 BlueXP 主控台的網路連線"

存取 BlueXP 主控台的電腦應連線至特定端點、以完成一些管理工作。如果您的網路限制了傳出存取、您應該確定允許這些端點。

2

"註冊並建立帳戶"

前往 ["BlueXP 主控台"](#) 並註冊。系統會提供您建立帳戶的選項、但如果您被邀請加入現有帳戶、則可以跳過該步驟。

此時、您已登入、可以開始使用數位顧問、Amazon FSX for ONTAP、Azure NetApp Files 等多項 BlueXP 服務。["瞭解如何在沒有 Connector 的情況下執行"](#)。

3

建立連接器

您不需要 Connector 即可開始使用 BlueXP、但您可以建立 Connector 來解除鎖定所有 BlueXP 功能和服務。Connector 是 NetApp 軟體、可讓 BlueXP 在混合雲環境中管理資源和程序。

BlueXP 帳戶管理員可以在雲端或內部部署網路中建立 Connector。

- ["深入瞭解何時需要連接器及其運作方式"](#)
- ["瞭解如何在 AWS 中建立 Connector"](#)
- ["瞭解如何在 Azure 中建立 Connector"](#)
- ["瞭解如何在 Google Cloud 中建立 Connector"](#)
- ["瞭解如何在內部部署上建立 Connector"](#)

請注意、如果您想要使用 BlueXP 服務來管理 Google Cloud 中的儲存和資料、則 Connector 必須在 Google Cloud 中執行。

4

"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。

準備使用 BlueXP 主控台的網路連線

當您使用透過 SaaS 層提供的 BlueXP 網路型主控台時、它會在完成一些管理工作時與多個端點連絡。存取 BlueXP 主控台的電腦應與這些端點建立連線。

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。您也應該參閱 Connector 的網路需求、以及特定的 BlueXP 服務。如需詳細資訊、請參閱本頁結尾的相關連結。

端點	目的
https://console.bluexp.netapp.com https://*.console.bluexp.netapp.com	當您使用 BlueXP 網路型主控台時、您的網路瀏覽器會連絡這些 URL。
https://aiq.netapp.com	需要存取 BlueXP 數位顧問。
AWS 服務 (amazonaws.com): <ul style="list-style-type: none">• CloudFormation• 彈性運算雲端 (EC2)• 金鑰管理服務 (KMS)• 安全性權杖服務 (STOS)• 簡易儲存服務 (S3)	需要在AWS中部署從BlueXP部署連接器。確切的端點取決於部署Connector的區域。" 如需詳細資料、請參閱 AWS 文件。 "
https://management.azure.com https://login.microsoftonline.com	在大多數Azure地區中部署來自BlueXP的Connector。
https://management.microsoftazure.de https://login.microsoftonline.de	需要在Azure Germany地區部署來自BlueXP的Connector。
https://management.usgovcloudapi.net https://login.microsoftonline.com	需要在Azure US Gov地區部署來自BlueXP的Connector。
https://www.googleapis.com	需要在Google Cloud中部署來自BlueXP的Connector。
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。

除了這些端點之外、您還需要確保 Connector 具備對外網際網路存取權、以便聯絡特定端點、以進行日常作業。您可以依照下一節中的連結、找到這些端點的清單。

相關連結

- 準備連接器的網路連線
 - ["設定 AWS 網路"](#)
 - ["設定 Azure 網路"](#)
 - ["設定 Google Cloud 網路"](#)
 - ["設定內部網路"](#)
- 為 BlueXP 服務做好網路準備

請參閱每項 BlueXP 服務的文件。

["BlueXP文件"](#)

註冊BlueXP

BlueXP 可從網路型主控台存取。當您開始使用 BlueXP 時、您的第一步是使用現有的 NetApp 支援網站 認證或建立 NetApp 雲端登入。

關於這項工作

您可以使用下列其中一個選項註冊至BlueXP：

- 您現有NetApp 支援網站 的功能驗證（NSS）認證
- 指定您的電子郵件地址和密碼、即可登入NetApp雲端

這兩種選項都支援聯盟連線、可讓您使用公司目錄（聯盟身分識別）的認證單一登入。您可以在註冊之後設定聯盟連線。 ["瞭解如何將身分識別聯盟與BlueXP搭配使用"](#)。

步驟

1. 開啟網頁瀏覽器、前往 ["BlueXP主控台"](#)
2. 如果您有 NetApp 支援網站 帳戶、請在 * 登入 * 頁面上直接輸入與您的 NSS 帳戶相關的電子郵件地址。

如果您有 NSS 帳戶、可以跳過註冊頁面。在此初次登入時、BlueXP會為您註冊。

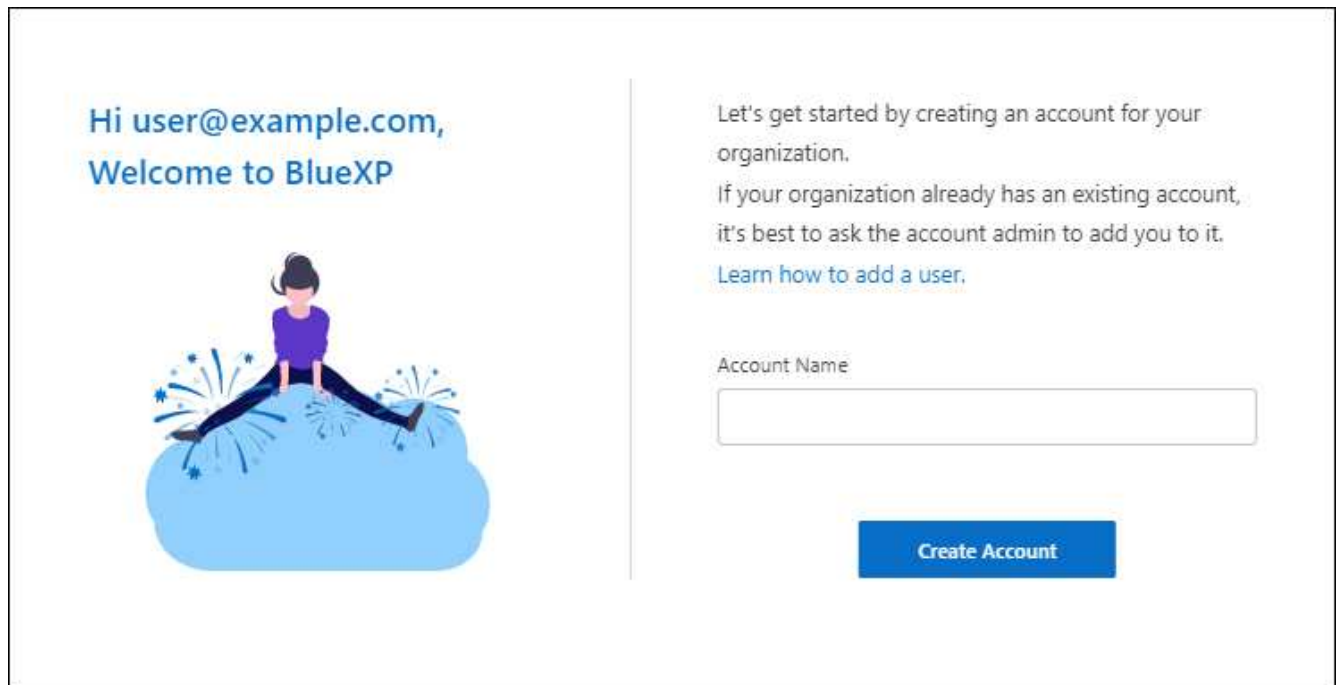
3. 如果您沒有 NSS 帳戶、但想要建立 NetApp 雲端登入來註冊、請選取 * 註冊 * 。
4. 在 * 註冊 * 頁面上、輸入建立 NetApp 雲端登入所需的資訊。

請注意、註冊表單中只允許英文字元。

5. 出現提示時、請檢閱終端使用者授權合約並接受條款。
6. 在*歡迎*頁面上、輸入您帳戶的名稱。

如果您的企業已經有帳戶、而您想要加入帳戶、則應關閉BlueXP、並請擁有者將您與帳戶建立關聯。擁有者新增您之後、您就可以登入、而且您可以存取該帳戶。 ["瞭解如何將成員新增至現有帳戶"](#)。

帳戶是NetApp身分識別平台的最上層元素。它可讓您新增及管理使用者、角色、權限及工作環境。



7. 選擇*建立帳戶*。

結果

您現在有一個BlueXP登入帳戶。在大多數情況下、下一步是建立連接器、將BlueXP的服務連接至混合雲環境。

建立連接器

AWS

AWS 中的連接器安裝選項

在 AWS 中建立 Connector 有幾種不同的方法。直接從 BlueXP 開始是最常見的方法。

提供下列安裝選項：

- "直接從 BlueXP 建立 Connector"（這是標準選項）

此動作會在您選擇的 VPC 中啟動執行 Linux 的 EC2 執行個體和 Connector 軟體。

- "從AWS Marketplace建立連接器"

此動作也會啟動執行 Linux 和 Connector 軟體的 EC2 執行個體、但部署會直接從 AWS Marketplace 啟動、而非從 BlueXP 啟動。

- "在您自己的 Linux 主機上下載並手動安裝軟體"

您選擇的安裝選項會影響您準備安裝的方式。其中包括如何為 BlueXP 提供必要的權限、讓它能夠在 AWS 中驗證和管理資源。

在AWS中從BlueXP建立連接器

若要從 BlueXP 在 AWS 中建立 Connector、您需要設定網路、準備 AWS 權限、然後建立 Connector。

開始之前

您應該檢閱 ["連接器限制"](#)。

步驟 1：設定網路

請確定您計畫安裝 Connector 的網路位置支援下列需求。滿足這些需求後、Connector 便能在混合雲環境中管理資源和程序。

VPC 和子網路

當您建立 Connector 時、您需要指定 Connector 所在的 VPC 和子網路。

連線至目標網路

Connector 需要網路連線、才能連線到您計畫建立和管理工作環境的位置。例如、您計畫在內部部署環境中建立 Cloud Volumes ONTAP 系統或儲存系統的網路。

傳出網際網路存取

您部署 Connector 的網路位置必須具有傳出網際網路連線、才能連絡特定端點。

已從 Connector 聯絡的端點

Connector 需要外傳網際網路存取才能連絡下列端點、以便管理公有雲環境中的資源和程序、以進行日常營運。

請注意、下列端點均為所有的 CNAME 項目。

端點	目的
AWS 服務 (amazonaws.com): <ul style="list-style-type: none">• CloudFormation• 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://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。

端點	目的
https://*.api.bluexp.netapp.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://api.bluexp.netapp.com	
https://*.cloudmanager.cloud.netapp.com	
https://cloudmanager.cloud.netapp.com	
https://netapp-cloud-account.auth0.com	
https://*.blob.core.windows.net	升級Connector及其Docker元件。
https://cloudmanagerinfraprod.azurecr.io	

從 BlueXP 主控台連絡的端點

當您使用透過 SaaS 層提供的 BlueXP 網路型主控台時、它會與多個端點聯絡、以完成資料管理工作。這包括透過 BlueXP 主控台聯絡以部署 Connector 的端點。

"檢視從 BlueXP 主控台連絡的端點清單"。

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"

建立 Connector 之後、您必須實作此網路需求。

步驟 2：設定 AWS 權限

在您的VPC中部署Connector執行個體之前、BlueXP必須先與AWS進行驗證。您可以選擇下列其中一種驗證方法：

- 讓BlueXP承擔具有所需權限的IAM角色
- 為具有所需權限的IAM使用者提供AWS存取金鑰和秘密金鑰

無論使用哪一種選項、第一步都是建立 IAM 原則。此原則僅包含從BlueXP啟動AWS中Connector執行個體所需的權限。

如有需要、您可以使用IAM來限制IAM原則 Condition 元素。"[AWS文件：條件元素](#)"



當 BlueXP 建立 Connector 時、它會將一組新的權限套用至 Connector 執行個體、讓 Connector 能夠管理 AWS 資源。

步驟

1. 前往AWS IAM主控台。
2. 選取 * 原則 > 建立原則 *。
3. 選取 * JSON*。
4. 複製並貼上下列原則：

提醒您、此原則僅包含從 BlueXP 在 AWS 中啟動 Connector 執行個體所需的權限。"[檢視 Connector 執行個體本身所需的權限](#)"。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iam:CreateRole",
        "iam>DeleteRole",
        "iam:PutRolePolicy",
        "iam>CreateInstanceProfile",
        "iam>DeleteRolePolicy",
        "iam:AddRoleToInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam>DeleteInstanceProfile",
        "iam:PassRole",
        "iam:ListRoles",
        "ec2:DescribeInstanceStatus",
        "ec2:RunInstances",
        "ec2:ModifyInstanceAttribute",
```

```

    "ec2:CreateSecurityGroup",
    "ec2:DeleteSecurityGroup",
    "ec2:DescribeSecurityGroups",
    "ec2:RevokeSecurityGroupEgress",
    "ec2:AuthorizeSecurityGroupEgress",
    "ec2:AuthorizeSecurityGroupIngress",
    "ec2:RevokeSecurityGroupIngress",
    "ec2:CreateNetworkInterface",
    "ec2:DescribeNetworkInterfaces",
    "ec2:DeleteNetworkInterface",
    "ec2:ModifyNetworkInterfaceAttribute",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcs",
    "ec2:DescribeDhcpOptions",
    "ec2:DescribeKeyPairs",
    "ec2:DescribeRegions",
    "ec2:DescribeInstances",
    "ec2:CreateTags",
    "ec2:DescribeImages",
    "ec2:DescribeAvailabilityZones",
    "ec2:DescribeLaunchTemplates",
    "ec2:CreateLaunchTemplate",
    "cloudformation:CreateStack",
    "cloudformation:DeleteStack",
    "cloudformation:DescribeStacks",
    "cloudformation:DescribeStackEvents",
    "cloudformation:ValidateTemplate",
    "ec2:AssociateIamInstanceProfile",
    "ec2:DescribeIamInstanceProfileAssociations",
    "ec2:DisassociateIamInstanceProfile",
    "iam:GetRole",
    "iam:TagRole",
    "kms:ListAliases",
    "cloudformation:ListStacks"
  ],
  "Resource": "*"
},
{
  "Effect": "Allow",
  "Action": [
    "ec2:TerminateInstances"
  ],
  "Condition": {
    "StringLike": {
      "ec2:ResourceTag/OCCMInstance": "*"
    }
  }
}

```

```

    },
    "Resource": [
        "arn:aws:ec2:*:*:instance/*"
    ]
}
]
}

```

5. 選擇 * 下一步 * 並視需要新增標記。
6. 選擇 * 下一步 * 並輸入名稱和說明。
7. 選取 * 建立原則 *。
8. 將原則附加至 BlueXP 可以承擔的 IAM 角色、或附加至 IAM 使用者、以便提供 BlueXP 存取金鑰：
 - (選項 1) 設定 BlueXP 可承擔的 IAM 角色：
 - i. 前往目標帳戶中的AWS IAM主控台。
 - ii. 在「存取管理」下、選取 * 角色 > 建立角色 *、然後依照步驟建立角色。
 - iii. 在*信任的實體類型*下、選取* AWS帳戶*。
 - iv. 選取*其他AWS帳戶*、然後輸入BlueXP SaaS帳戶的ID：95201331444
 - v. 選取您在上一節中建立的原則。
 - vi. 建立角色之後、請複製角色ARN、以便在建立Connector時將其貼到BlueXP中。
 - (選項 2) 設定 IAM 使用者的權限、以便提供 BlueXP 存取金鑰：
 - i. 從 AWS IAM 主控台選取 * 使用者 *、然後選取使用者名稱。
 - ii. 選取 * 新增權限 > 直接附加現有原則 *。
 - iii. 選取您建立的原則。
 - iv. 選取 * 下一步 *、然後選取 * 新增權限 *。
 - v. 確保您擁有 IAM 使用者的存取金鑰和秘密金鑰。

結果

您現在應該擁有具有所需權限的 IAM 角色、或是擁有所需權限的 IAM 使用者。從 BlueXP 建立 Connector 時、您可以提供角色或存取金鑰的相關資訊。

步驟 3：建立 Connector

直接從 BlueXP 網路型主控台建立 Connector。

關於這項工作

從 BlueXP 建立 Connector 會使用預設組態、在 AWS 中部署 EC2 執行個體。建立 Connector 之後、不應變更為 CPU 或 RAM 較少的較小 EC2 執行個體類型。"瞭解連接器的預設組態"。

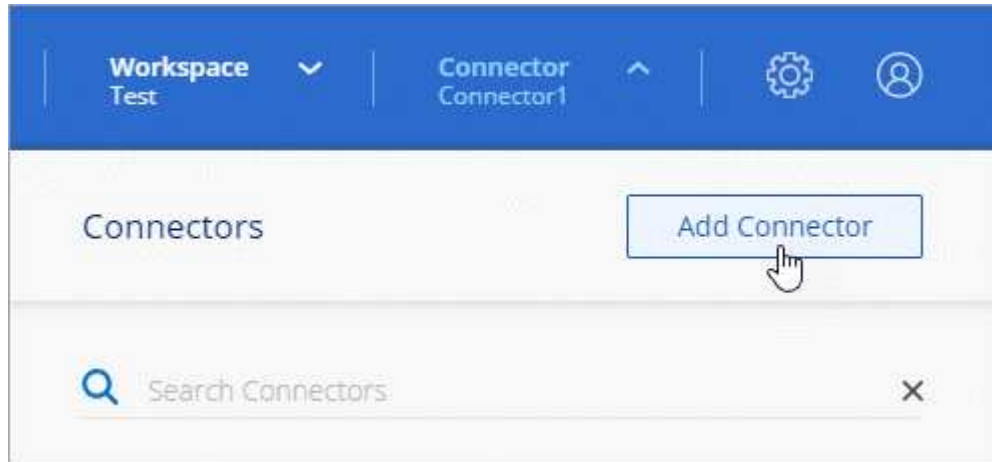
開始之前

您應該擁有下列項目：

- AWS 驗證方法：為具有必要權限的 IAM 使用者提供 IAM 角色或存取金鑰。
- 符合網路需求的 VPC 和子網路。
- EC2 執行個體的金鑰配對。
- Proxy 伺服器的詳細資料、如果需要 Proxy 才能從 Connector 存取網際網路。

步驟

1. 選取 * Connector * 下拉式清單、然後選取 * 新增 Connector * 。



2. 選擇 * Amazon Web Services * 作為您的雲端供應商、然後選擇 * 繼續 * 。
3. 在「部署連接器」頁面上、檢閱您需要的詳細資料。您有兩種選擇：
 - a. 選擇 * 繼續 * 、使用產品內建指南準備部署。產品內建指南中的每個步驟都包含文件本頁所含的資訊。
 - b. 如果您已按照本頁的步驟做好準備、請選取 * 跳至部署 * 。
4. 依照精靈中的步驟建立連接器：
 - 準備好：檢視您需要的內容。
 - * AWS 認證資料*：指定您的AWS區域、然後選擇驗證方法、這是BlueXP可以承擔的IAM角色、或是AWS存取金鑰和秘密金鑰。



如果選擇*假定角色*、您可以從連接器部署精靈建立第一組認證。必須從「認證資料」頁面建立任何其他一組認證資料。然後、精靈會在下拉式清單中提供這些工具。 ["瞭解如何新增其他認證資料"](#)。

- 詳細資料：提供連接器的詳細資料。
 - 輸入執行個體的名稱。
 - 新增自訂標記（中繼資料）至執行個體。
 - 選擇是否要讓BlueXP建立具有所需權限的新角色、或是要選取您所設定的現有角色 ["必要的權限"](#)。
 - 選擇是否要加密Connector的EBS磁碟。您可以選擇使用預設加密金鑰或使用自訂金鑰。
- 網路：指定執行個體的VPC、子網路和金鑰配對、選擇是否啟用公用IP位址、以及選擇性地指定Proxy組態。

請確定您的金鑰配對正確、可與連接器搭配使用。如果沒有金鑰配對、您將無法存取Connector虛擬機器。

- * 安全性群組 *：選擇是否要建立新的安全性群組、或是選擇允許所需輸入和輸出規則的現有安全性群組。

["檢視 AWS 的安全性群組規則"](#)。

- 審查：請檢閱您的選擇、確認您的設定正確無誤。

5. 選取*「Add*」。

執行個體應在 7 分鐘內就緒。您應該留在頁面上、直到程序完成為止。

結果

程序完成後、即可從 BlueXP 使用 Connector。

如果您在建立 Connector 的同一個 AWS 帳戶中有 Amazon S3 工作區、則 BlueXP 畫布上會自動出現 Amazon S3 工作環境。["瞭解如何從 BlueXP 管理 S3 儲存區"](#)

從AWS Marketplace建立連接器

若要從 AWS Marketplace 建立 Connector、您需要設定網路、準備 AWS 權限、檢閱執行個體需求、然後建立 Connector。

開始之前

您應該檢閱 ["連接器限制"](#)。

步驟 1：設定網路

請確定您計畫安裝 Connector 的網路位置支援下列需求。滿足這些需求後、Connector 便能在混合雲環境中管理資源和程序。

VPC 和子網路

當您建立 Connector 時、您需要指定 Connector 所在的 VPC 和子網路。

連線至目標網路

Connector 需要網路連線、才能連線到您計畫建立和管理工作環境的位置。例如、您計畫在內部部署環境中建立 Cloud Volumes ONTAP 系統或儲存系統的網路。

傳出網際網路存取

您部署 Connector 的網路位置必須具有傳出網際網路連線、才能連絡特定端點。

已從 Connector 聯絡的端點

Connector 需要外傳網際網路存取才能連絡下列端點、以便管理公有雲環境中的資源和程序、以進行日常營運。

請注意、下列端點均為所有的 CNAME 項目。

端點	目的
AWS 服務 (amazonaws.com): <ul style="list-style-type: none"> • CloudFormation • 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://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.blueexp.netapp.com https://api.blueexp.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.blueexp.netapp.com」。
https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	升級Connector及其Docker元件。

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](#)"

建立 Connector 之後、您必須實作此網路需求。

步驟 2：設定 AWS 權限

若要準備進行市場部署、請在 AWS 中建立 IAM 原則、並將其附加至 IAM 角色。當您從 AWS Marketplace 建立 Connector 時、系統會提示您選取該 IAM 角色。

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. 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 IAM 角色、可在 AWS Marketplace 部署期間與 EC2 執行個體建立關聯。

步驟 3：審查執行個體需求

建立 Connector 時、您需要選擇符合下列需求的 EC2 執行個體類型。

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。

步驟 4：建立 Connector

直接從 AWS Marketplace 建立 Connector。

關於這項工作

從 AWS Marketplace 建立 Connector 會使用預設組態、在 AWS 中部署 EC2 執行個體。"瞭解連接器的預設組態"。

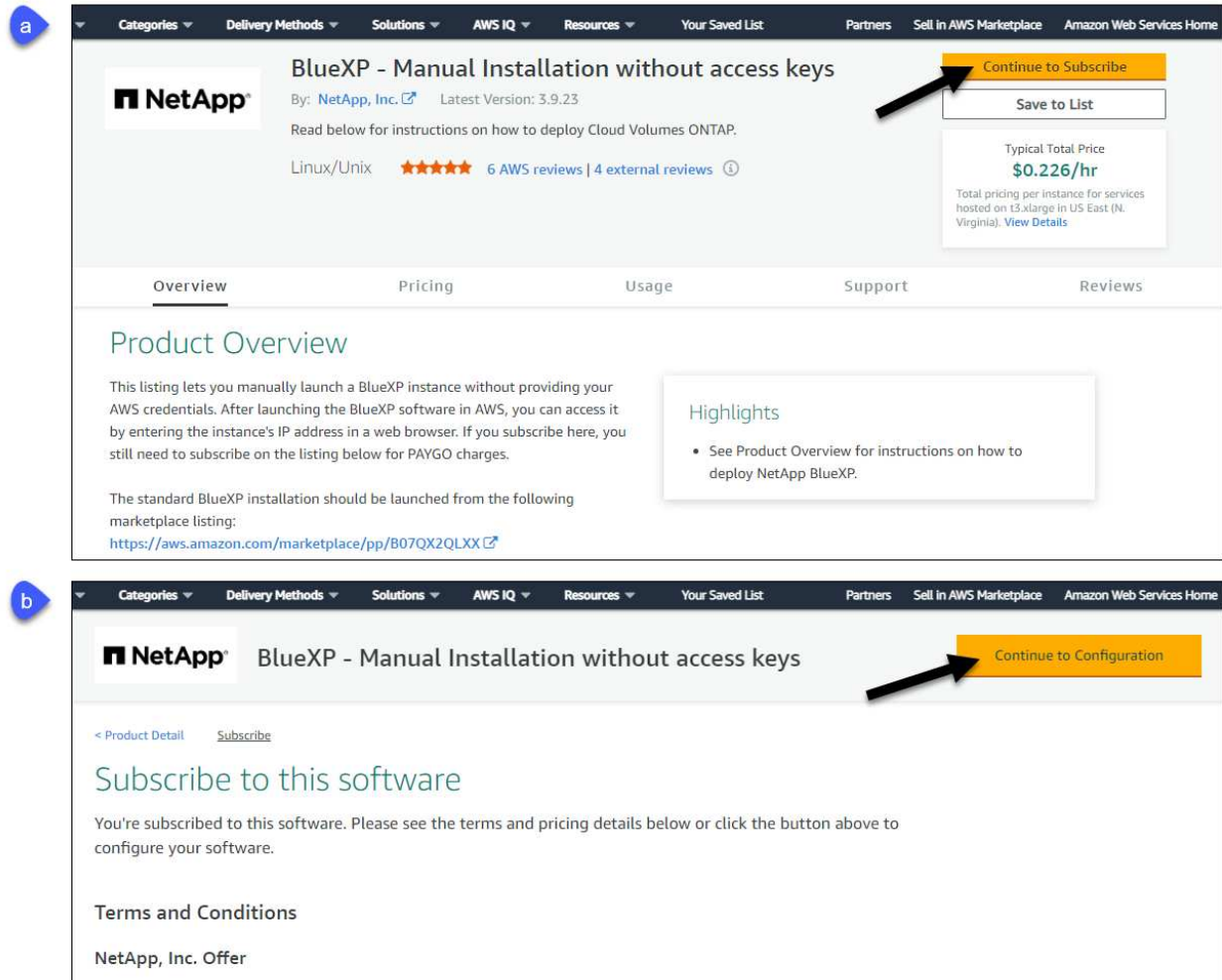
開始之前

您應該擁有下列項目：

- 符合網路需求的 VPC 和子網路。
- 具有附加原則的 IAM 角色、其中包含 Connector 所需的權限。
- 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。
- 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 *。

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。

6. 從連線至 Connector 虛擬機器的主機開啟網頁瀏覽器、然後輸入下列 URL：

`https://ipaddress`

7. 登入後、設定 Connector：

- a. 指定與 Connector 相關聯的 BlueXP 帳戶。
- b. 輸入系統名稱。
- c. 在 * 您是在安全的環境中執行？ * 保持停用限制模式。

您應該保持停用受限模式、因為這些步驟說明如何在標準模式中使用 BlueXP。只有當您擁有安全的環境、而且想要中斷此帳戶與 BlueXP 後端服務的連線時、才應啟用受限模式。如果是這樣、["請依照步驟、以受限模式開始使用 BlueXP"](#)。

- d. 選取 * 開始 *。

結果

Connector 現在已安裝、並使用您的 BlueXP 帳戶進行設定。

開啟網頁瀏覽器、前往 ["BlueXP 主控台"](#) 開始使用 Connector with BlueXP。

如果您在建立 Connector 的同一個 AWS 帳戶中有 Amazon S3 工作區、則 BlueXP 畫布上會自動出現 Amazon S3 工作環境。["瞭解如何從 BlueXP 管理 S3 儲存區"](#)

在 AWS 中手動安裝 Connector

若要在您自己的 Linux 主機上手動安裝 Connector、您必須檢閱主機需求、設定網路、準備 AWS 權限、安裝 Connector、然後提供您準備的權限。

開始之前

您應該檢閱 ["連接器限制"](#)。

步驟 1：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。

金鑰配對

建立 Connector 時、您需要選取 EC2 金鑰配對以搭配執行個體使用。

/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 2：設定網路

請確定您計畫安裝 Connector 的網路位置支援下列需求。滿足這些需求後、Connector 便能在混合雲環境中管理資源和程序。

連線至目標網路

Connector 需要網路連線、才能連線到您計畫建立和管理工作環境的位置。例如、您計畫在內部部署環境中建立 Cloud Volumes ONTAP 系統或儲存系統的網路。

傳出網際網路存取

您部署 Connector 的網路位置必須具有傳出網際網路連線、才能連絡特定端點。

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>

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。

已從 Connector 聯絡的端點

Connector 需要外傳網際網路存取才能連絡下列端點、以便管理公有雲環境中的資源和程序、以進行日常營運。

請注意、下列端點均為所有的 CNAME 項目。

端點	目的
AWS 服務 (amazonaws.com): <ul style="list-style-type: none">• CloudFormation• 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://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。

端點	目的
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	升級Connector及其Docker元件。

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"](#)

步驟 3：設定權限

您需要使用下列其中一個選項、提供 AWS 對 BlueXP 的權限：

- 選項 1：建立 IAM 原則、並將原則附加至您可以與 EC2 執行個體建立關聯的 IAM 角色。

- 選項 2：為具有必要權限的 IAM 使用者提供 BlueXP AWS 存取金鑰。

請依照步驟準備 BlueXP 的權限。

IAM 角色

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. 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

現在您有一個 IAM 角色、可以在安裝 Connector 之後與 EC2 執行個體建立關聯。

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

您現在擁有一個 IAM 使用者、該使用者擁有必要的權限、以及您可以提供給 BlueXP 的存取金鑰。

步驟 4：安裝 Connector

完成先決條件後、您可以在自己的 Linux 主機上手動安裝軟體。

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。

6. 等待安裝完成。

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。

7. 從連線至 Connector 虛擬機器的主機開啟網頁瀏覽器、然後輸入下列 URL：

https://ipaddress

8. 登入後、設定 Connector：

- a. 指定與 Connector 相關聯的 BlueXP 帳戶。
- b. 輸入系統名稱。
- c. 在 * 您是在安全的環境中執行？ * 保持停用限制模式。

您應該保持停用受限模式、因為這些步驟說明如何在標準模式中使用 BlueXP。只有當您擁有安全的環境、而且想要中斷此帳戶與 BlueXP 後端服務的連線時、才應啟用受限模式。如果是這樣、[請依照步](#)

驟、以受限模式開始使用 BlueXP"。

d. 選取 * 開始 * 。

結果

Connector 現已安裝、並已使用您的 BlueXP 帳戶進行設定。

如果您在建立 Connector 的同一個 AWS 帳戶中有 Amazon S3 工作區、則 BlueXP 畫布上會自動出現 Amazon S3 工作環境。"[瞭解如何從 BlueXP 管理 S3 儲存區](#)"

步驟 5：提供 **BlueXP** 的權限

安裝 Connector 之後、您必須提供 BlueXP 先前設定的 AWS 權限。提供權限可讓 BlueXP 在 AWS 中管理您的資料和儲存基礎架構。

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。

前往 "[BlueXP主控台](#)" 開始使用Connector with BlueXP。

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. 確定目前在BlueXP中選取正確的連接器。
2. 在 BlueXP 主控台的右上角、選取「設定」圖示、然後選取 * 認證 *。



3. 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。

前往 "[BlueXP主控台](#)" 開始使用Connector with BlueXP。

Azure

Azure 中的連接器安裝選項

在 Azure 中建立 Connector 有幾種不同的方法。直接從 BlueXP 開始是最常見的方法。

提供下列安裝選項：

- ["直接從 BlueXP 建立 Connector"](#)（這是標準選項）

此動作會在您選擇的 vnet 中啟動執行 Linux 的 VM 和 Connector 軟體。

- ["從 Azure Marketplace 建立連接器"](#)

此動作也會啟動執行 Linux 和 Connector 軟體的 VM、但部署是直接從 Azure Marketplace 啟動、而非從 BlueXP 啟動。

- ["在您自己的 Linux 主機上下載並手動安裝軟體"](#)

您選擇的安裝選項會影響您準備安裝的方式。其中包括如何為 BlueXP 提供驗證和管理 Azure 資源所需的必要權限。

從 BlueXP 在 Azure 中建立連接器

若要從 BlueXP 在 Azure 中建立 Connector、您必須設定網路、準備 Azure 權限、然後建立 Connector。

開始之前

您應該檢閱 ["連接器限制"](#)。

步驟 1：設定網路

請確定您計畫安裝 Connector 的網路位置支援下列需求。滿足這些需求後、Connector 便能在混合雲環境中管理資源和程序。

Azure 地區

如果您使用 Cloud Volumes ONTAP、Connector 應部署在與其管理的 Cloud Volumes ONTAP 系統所在的同一個 Azure 區域、或部署在中 ["Azure 區域配對"](#) 適用於整個系統。Cloud Volumes ONTAP 這項需求可確保 Cloud Volumes ONTAP Azure Private Link 連線可用於連接至相關的儲存帳戶。

["瞭解 Cloud Volumes ONTAP 解如何使用 Azure Private Link"](#)

vnet 和子網路

建立 Connector 時、您需要指定 Connector 應位於的 vnet 和子網路。

連線至目標網路

Connector 需要網路連線、才能連線到您計畫建立和管理工作環境的位置。例如、您計畫在內部部署環境中建立 Cloud Volumes ONTAP 系統或儲存系統的網路。

傳出網際網路存取

您部署 Connector 的網路位置必須具有傳出網際網路連線、才能連絡特定端點。

已從 Connector 聯絡的端點

Connector 需要外傳網際網路存取才能連絡下列端點、以便管理公有雲環境中的資源和程序、以進行日常營運。

請注意、下列端點均為所有的 CNAME 項目。

端點	目的
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.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://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.blueexp.netapp.com https://api.blueexp.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.blueexp.netapp.com" 」。
https://*.blob.core.windows.net https://cloudmanagerinfraproduct.azurecr.io	升級Connector及其Docker元件。

從 BlueXP 主控台連絡的端點

當您使用透過 SaaS 層提供的 BlueXP 網路型主控台時、它會與多個端點聯絡、以完成資料管理工作。這包括透過 BlueXP 主控台聯絡以部署 Connector 的端點。

"檢視從 BlueXP 主控台連絡的端點清單"。

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"](#)

建立 Connector 之後、您必須實作此網路需求。

步驟 2：建立自訂角色

建立可指派給 Azure 帳戶或 Microsoft Entra 服務主體的 Azure 自訂角色。BlueXP 會驗證 Azure 、並使用這些權限代表您建立 Connector 執行個體。

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. 複製Azure中新自訂角色所需的權限、並將其儲存在Json檔案中。



此自訂角色僅包含從 BlueXP 在 Azure 中啟動 Connector VM 所需的權限。請勿在其他情況下使用此原則。當BlueXP建立Connector時、它會套用一組新的權限至Connector VM、讓Connector能夠管理公有雲環境中的資源。

```
{
  "Name": "Azure SetupAsService",
  "Actions": [
    "Microsoft.Compute/disks/delete",
    "Microsoft.Compute/disks/read",
    "Microsoft.Compute/disks/write",
    "Microsoft.Compute/locations/operations/read",
    "Microsoft.Compute/operations/read",
    "Microsoft.Compute/virtualMachines/instanceView/read",
    "Microsoft.Compute/virtualMachines/read",
    "Microsoft.Compute/virtualMachines/write",
    "Microsoft.Compute/virtualMachines/delete",
    "Microsoft.Compute/virtualMachines/extensions/write",
    "Microsoft.Compute/virtualMachines/extensions/read",
    "Microsoft.Compute/availabilitySets/read",
    "Microsoft.Network/locations/operationResults/read",
    "Microsoft.Network/locations/operations/read",
```

```

"Microsoft.Network/networkInterfaces/join/action",
"Microsoft.Network/networkInterfaces/read",
"Microsoft.Network/networkInterfaces/write",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkSecurityGroups/join/action",
"Microsoft.Network/networkSecurityGroups/read",
"Microsoft.Network/networkSecurityGroups/write",

"Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read",
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/virtualNetworks/subnets/join/action",
"Microsoft.Network/virtualNetworks/subnets/read",

"Microsoft.Network/virtualNetworks/subnets/virtualMachines/read",
"Microsoft.Network/virtualNetworks/virtualMachines/read",
"Microsoft.Network/publicIPAddresses/write",
"Microsoft.Network/publicIPAddresses/read",
"Microsoft.Network/publicIPAddresses/delete",
"Microsoft.Network/networkSecurityGroups/securityRules/read",
"Microsoft.Network/networkSecurityGroups/securityRules/write",
"Microsoft.Network/networkSecurityGroups/securityRules/delete",
"Microsoft.Network/publicIPAddresses/join/action",

"Microsoft.Network/locations/virtualNetworkAvailableEndpointServices/read",
"Microsoft.Network/networkInterfaces/ipConfigurations/read",
"Microsoft.Resources/deployments/operations/read",
"Microsoft.Resources/deployments/read",
"Microsoft.Resources/deployments/delete",
"Microsoft.Resources/deployments/cancel/action",
"Microsoft.Resources/deployments/validate/action",
"Microsoft.Resources/resources/read",
"Microsoft.Resources/subscriptions/operationresults/read",
"Microsoft.Resources/subscriptions/resourceGroups/delete",
"Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Resources/subscriptions/resourcegroups/resources/read",
"Microsoft.Resources/subscriptions/resourceGroups/write",
"Microsoft.Authorization/roleDefinitions/write",
"Microsoft.Authorization/roleAssignments/write",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/read",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/write",

```

```

    "Microsoft.Network/networkSecurityGroups/delete",
    "Microsoft.Storage/storageAccounts/delete",
    "Microsoft.Storage/storageAccounts/write",
    "Microsoft.Resources/deployments/write",
    "Microsoft.Resources/deployments/operationStatuses/read",
    "Microsoft.Authorization/roleAssignments/read"
  ],
  "NotActions": [],
  "AssignableScopes": [],
  "Description": "Azure SetupAsService",
  "IsCustom": "true"
}

```

2. 將您的Azure訂閱ID新增至可指派的範圍、以修改Json。

◦ 範例 *

```

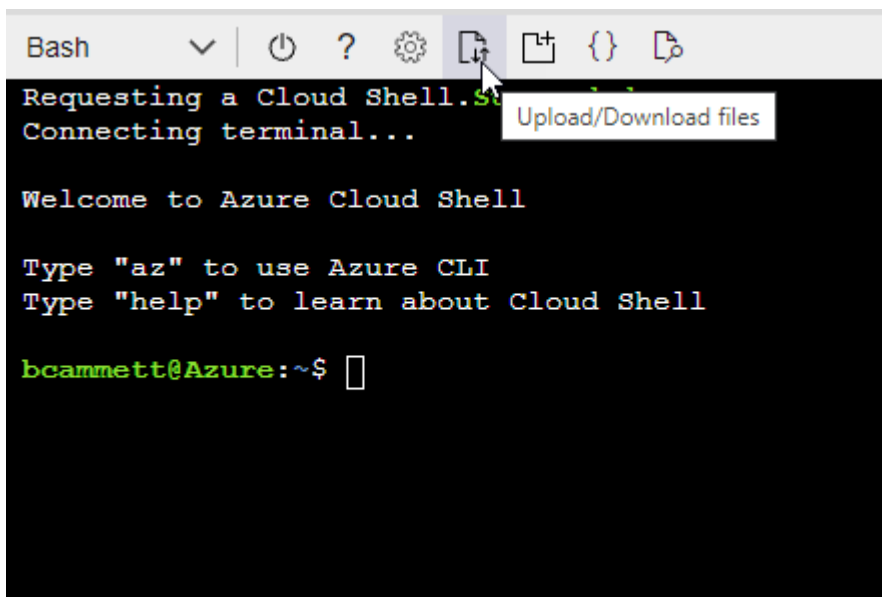
"AssignableScopes": [
  "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz"
],

```

3. 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. 輸入下列Azure CLI命令：


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

您現在應該擁有名為 *Azure Setup AsService* 的自訂角色。您現在可以將此自訂角色套用至您的使用者帳戶或服務主體。

步驟 3：設定驗證

從 BlueXP 建立 Connector 時、您需要提供登入資訊、讓 BlueXP 能夠與 Azure 驗證並部署 VM。您有兩種選擇：

1. 收到提示時、請使用 Azure 帳戶登入。此帳戶必須具有特定的 Azure 權限。這是預設選項。
2. 提供 Microsoft Entra 服務主體的詳細資料。此服務主體也需要特定權限。

請依照下列步驟準備其中一種驗證方法、以搭配 BlueXP 使用。

Azure 帳戶

將自訂角色指派給將從 BlueXP 部署 Connector 的使用者。

步驟

1. 在 Azure 入口網站中、開啟 * 訂閱 * 服務、然後選取使用者的訂閱。
2. 按一下 * 存取控制 (IAM) *。
3. 按一下「* 新增 * > * 新增角色指派 *」、然後新增權限：
 - a. 選取「* Azure Setup AsService*」角色、然後按一下「* Next*」。



Azure Setup AsService是Azure的Connector部署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。

- b. 保留*選取「使用者」、「群組」或「服務主體」*。
- c. 按一下*選取成員*、選擇您的使用者帳戶、然後按一下*選取*。
- d. 單擊 * 下一步 *。
- e. 按一下「檢閱+指派」。

結果

Azure使用者現在擁有從BlueXP部署Connector所需的權限。

服務主體

您可以為 BlueXP 提供具有必要權限的 Azure 服務主體認證、而非使用 Azure 帳戶登入。

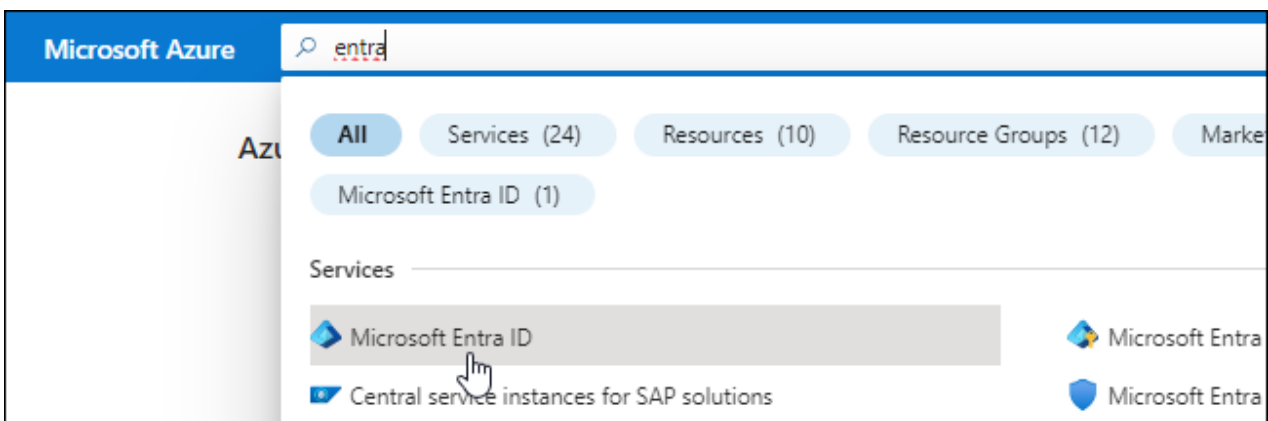
在 Microsoft Entra ID 中建立並設定服務主體、並取得 BlueXP 所需的 Azure 認證。

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。



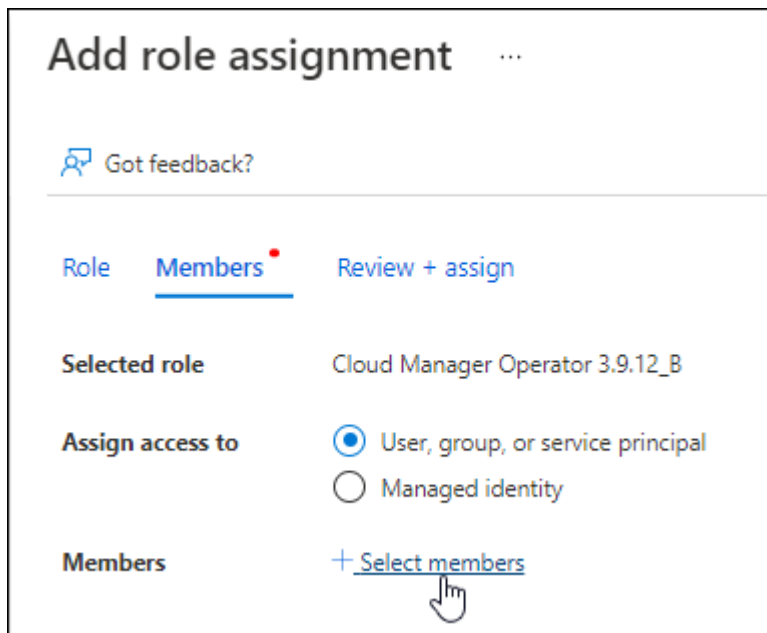
3. 在功能表中、選取 * 應用程式註冊 *。

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。

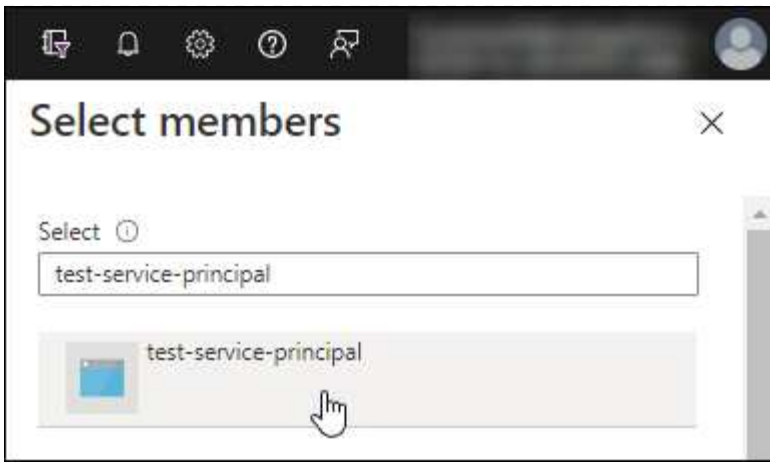
將自訂角色指派給應用程式

1. 從 Azure 入口網站開啟 * 訂閱 * 服務。
2. 選取訂閱。
3. 按一下 * 存取控制（IAM） > 新增 > 新增角色指派 *。
4. 在「角色」索引標籤中、選取「藍圖XP操作員」角色、然後按一下「下一步」。
5. 在「成員」索引標籤中、完成下列步驟：
 - a. 保留*選取「使用者」、「群組」或「服務主體」*。
 - b. 按一下*選取成員*。



- c. 搜尋應用程式名稱。

範例如下：



- a. 選取應用程式、然後按一下*選取*。
 - b. 單擊 * 下一步 * 。
6. 按一下「檢閱+指派」。

服務主體現在擁有部署Connector所需的Azure權限。

如果您想要在多個 Azure 訂閱中管理資源、則必須將服務主體繫結至每個訂閱。例如、BlueXP 可讓您選取部署 Cloud Volumes ONTAP 時要使用的訂閱。

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 *」。

Request API permissions

Select an API

Microsoft APIs [APIs my organization uses](#) [My APIs](#)

Commonly used Microsoft APIs

Microsoft Graph

Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.



Azure Batch

Schedule large-scale parallel and HPC applications in the cloud

Azure Data Catalog

Programmatic access to Data Catalog resources to register, annotate and search data assets

Azure Data Explorer

Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions

Azure Data Lake

Access to storage and compute for big data analytic scenarios

Azure DevOps

Integrate with Azure DevOps and Azure DevOps server

Azure Import/Export

Programmatic control of import/export jobs

Azure Key Vault

Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults

Azure Rights Management Services

Allow validated users to read and write protected content

Azure Service Management

Programmatic access to much of the functionality available through the Azure portal

Azure Storage

Secure, massively scalable object and data lake storage for unstructured and semi-structured data

Customer Insights

Create profile and interaction models for your products

Data Export Service for Microsoft Dynamics 365

Export data from Microsoft Dynamics CRM organization to an external destination

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 * 。

Request API permissions

[← All APIs](#)



Azure Service Management

<https://management.azure.com/> [Docs](#)

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

Select permissions

[expand all](#)

Type to search

PERMISSION

ADMIN CONSENT REQUIRED

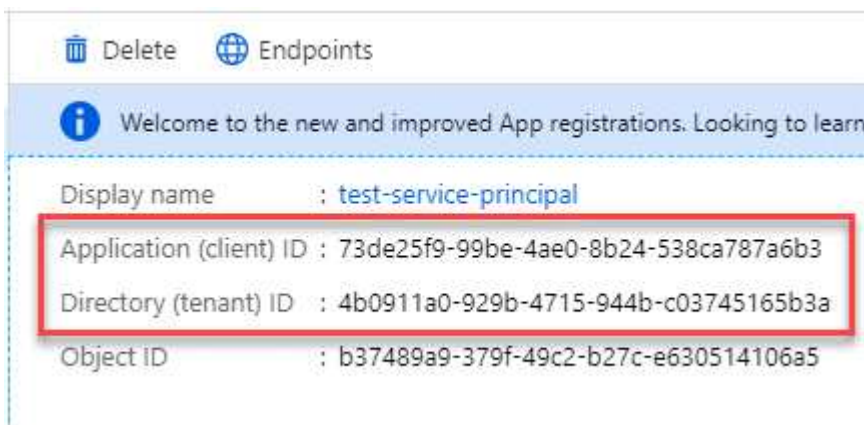


user_impersonation

Access Azure Service Management as organization users (preview)

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。

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret		
DESCRIPTION	EXPIRES	VALUE
test secret	8/16/2020	*sZ1jSe2By:D*-ZRoV4NLfdAcY7:+0vA

Copy to clipboard

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。建立Connector時、您必須在BlueXP中輸入此資訊。

步驟 4：建立 Connector

直接從 BlueXP 網路型主控台建立 Connector。

關於這項工作

從 BlueXP 建立 Connector 會使用預設組態、在 Azure 中部署虛擬機器。建立 Connector 之後、不應變更為 CPU 或 RAM 較少的較小 VM 類型。["瞭解連接器的預設組態"](#)。

開始之前

您應該擁有下列項目：

- Azure 訂閱。
- 您所選擇的 Azure 區域中的 Vnet 和子網路。
- 若貴組織需要代理處理所有傳出的網際網路流量、請參閱Proxy伺服器的詳細資料：
 - IP 位址
 - 認證資料
 - HTTPS憑證
- SSH 公開金鑰、如果您想要將該驗證方法用於 Connector 虛擬機器。驗證方法的另一個選項是使用密碼。

["瞭解如何在 Azure 中連線至 Linux VM"](#)

- 如果您不想讓BlueXP自動為Connector建立Azure角色、則需要自行建立 ["使用此頁面上的原則"](#)。

這些權限適用於Connector執行個體本身。這是一組不同於您先前設定的權限、可用來部署 Connector VM。

步驟

1. 選取 * Connector * 下拉式清單、然後選取 * 新增 Connector *。



2. 選擇 * Microsoft Azure * 作為雲端供應商。

3. 在*部署連接器*頁面上：

a. 在 * 驗證 * 下、選取符合您設定 Azure 權限方式的驗證選項：

- 選取 * Azure 使用者帳戶 * 以登入您的 Microsoft 帳戶、該帳戶應具有必要的權限。

此表單由 Microsoft 擁有及託管。您的認證資料不會提供給 NetApp。



如果您已經登入 Azure 帳戶、則 BlueXP 會自動使用該帳戶。如果您有多個帳戶、則可能需要先登出、以確保您使用的是正確的帳戶。

- 選取 * Active Directory 服務主體 * 以輸入 Microsoft Entra 服務主體的相關資訊、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

[瞭解如何取得服務主體的這些值。](#)

4. 依照精靈中的步驟建立連接器：

- * VM 驗證 *：選擇 Azure 訂閱、位置、新資源群組或現有資源群組、然後為您正在建立的 Connector 虛擬機器選擇驗證方法。

虛擬機器的驗證方法可以是密碼或 SSH 公開金鑰。

["瞭解如何在 Azure 中連線至 Linux VM"](#)

- 詳細資料：輸入執行個體的名稱、指定標記、然後選擇是否要 BlueXP 建立具有所需權限的新角色、或是要選取所設定的現有角色 **"必要的權限"**。

請注意、您可以選擇與此角色相關的 Azure 訂閱。您選擇的每個訂閱都會提供 Connector 權限、以管理該訂閱中的資源（例如 Cloud Volumes ONTAP）。

- * 網路 *：選擇 Vnet 和子網路、是否啟用公用 IP 位址、以及是否指定 Proxy 組態（選用）。

- * 安全性群組 *：選擇是否要建立新的安全性群組、或是選擇允許所需輸入和輸出規則的現有安全性群組。

["檢視 Azure 的安全性群組規則"](#)。

- 審查：請檢閱您的選擇、確認您的設定正確無誤。

5. 按一下「* 新增 *」。

虛擬機器應在約 7 分鐘內就緒。您應該留在頁面上、直到程序完成為止。

結果

程序完成後、即可從 BlueXP 使用 Connector。

如果您在建立 Connector 的同一個 Azure 訂閱中擁有 Azure Blob 儲存設備、則會在 BlueXP 畫布上自動顯示 Azure Blob 儲存設備工作環境。["瞭解如何從 BlueXP 管理 Azure Blob 儲存設備"](#)

從 Azure Marketplace 建立連接器

若要從 Azure Marketplace 建立 Connector、您必須設定網路、準備 Azure 權限、檢閱執行個體需求、然後建立 Connector。

開始之前

您應該檢閱 ["連接器限制"](#)。

步驟 1：設定網路

請確定您計畫安裝 Connector 的網路位置支援下列需求。滿足這些需求後、Connector 便能在混合雲環境中管理資源和程序。

Azure 地區

如果您使用 Cloud Volumes ONTAP、Connector 應部署在與其管理的 Cloud Volumes ONTAP 系統所在的同一個 Azure 區域、或部署在中 ["Azure 區域配對"](#) 適用於整個系統。Cloud Volumes ONTAP 這項需求可確保 Cloud Volumes ONTAP Azure Private Link 連線可用於連接至相關的儲存帳戶。

["瞭Cloud Volumes ONTAP 解如何使用Azure Private Link"](#)

vnet 和子網路

建立 Connector 時、您需要指定 Connector 應位於的 vnet 和子網路。

連線至目標網路

Connector 需要網路連線、才能連線到您計畫建立和管理工作環境的位置。例如、您計畫在內部部署環境中建立 Cloud Volumes ONTAP 系統或儲存系統的網路。

傳出網際網路存取

您部署 Connector 的網路位置必須具有傳出網際網路連線、才能連絡特定端點。

已從 Connector 聯絡的端點

Connector 需要外傳網際網路存取才能連絡下列端點、以便管理公有雲環境中的資源和程序、以進行日常營運。

請注意、下列端點均為所有的 CNAME 項目。

端點	目的
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.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://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.blueexp.netapp.com https://api.blueexp.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.blueexp.netapp.com" 」。
https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	升級Connector及其Docker元件。

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"](#)

建立 Connector 之後、您必須實作此網路需求。

步驟 2：檢閱 VM 需求

建立 Connector 時、您需要選擇符合下列需求的虛擬機器類型。

CPU

4 個核心或 4 個 vCPU

RAM

14 GB

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。

步驟 3：設定權限

您可以使用下列方式提供權限：

- 選項 1：使用系統指派的託管身分識別、將自訂角色指派給 Azure VM。
- 選項 2：為 BlueXP 提供具有必要權限的 Azure 服務主體認證。

請依照下列步驟設定 BlueXP 的權限。

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"](#)

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。

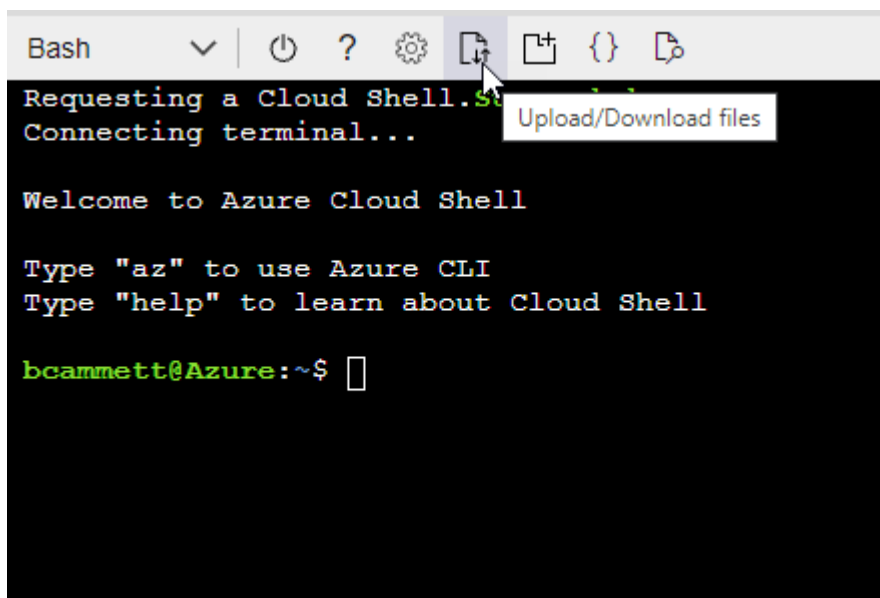
◦ 範例 *

```
"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。

服務主體

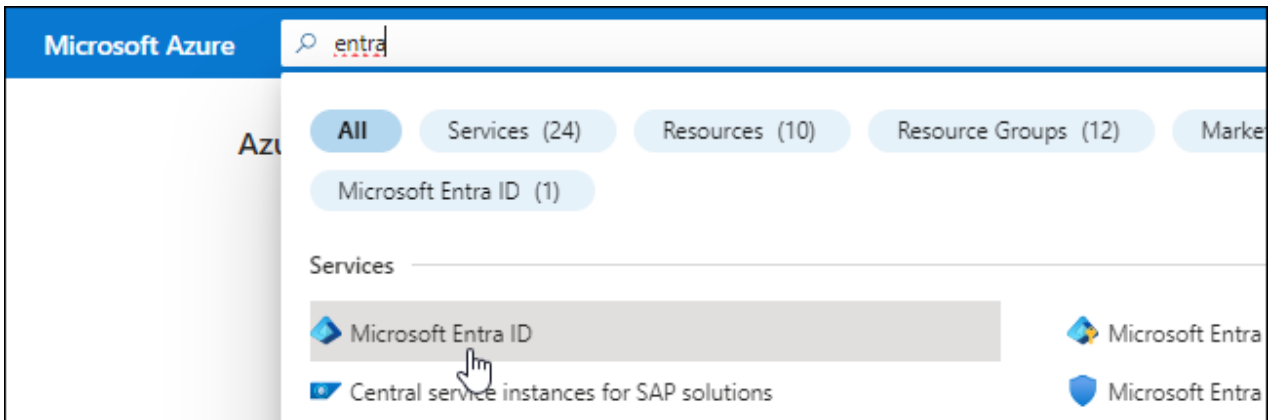
在 Microsoft Entra ID 中建立並設定服務主體、並取得 BlueXP 所需的 Azure 認證。

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。

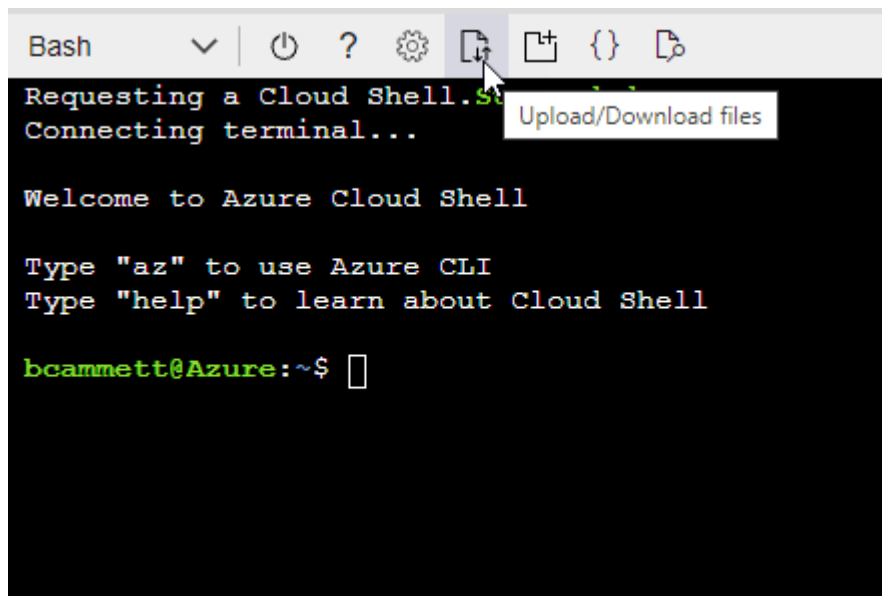
- 範例 *

```
"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：

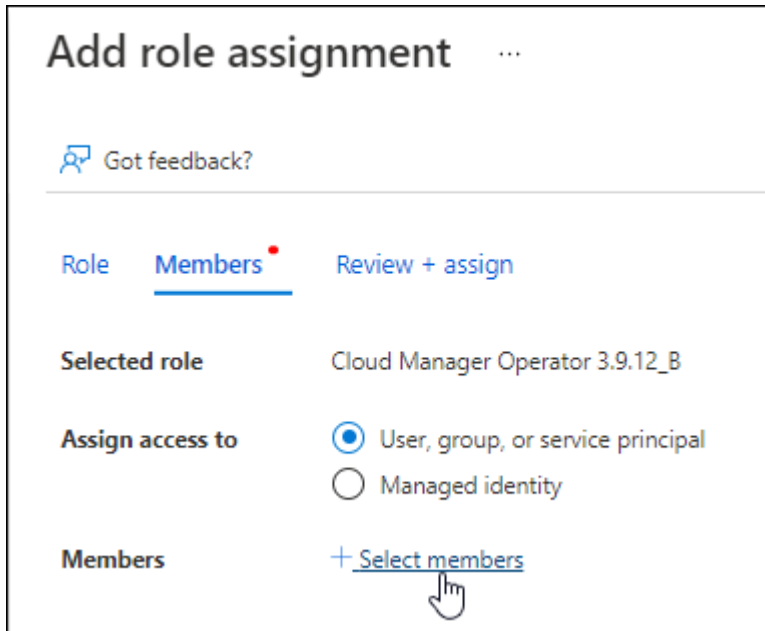
```
az role definition create --role-definition  
Connector_Policy.json
```

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：

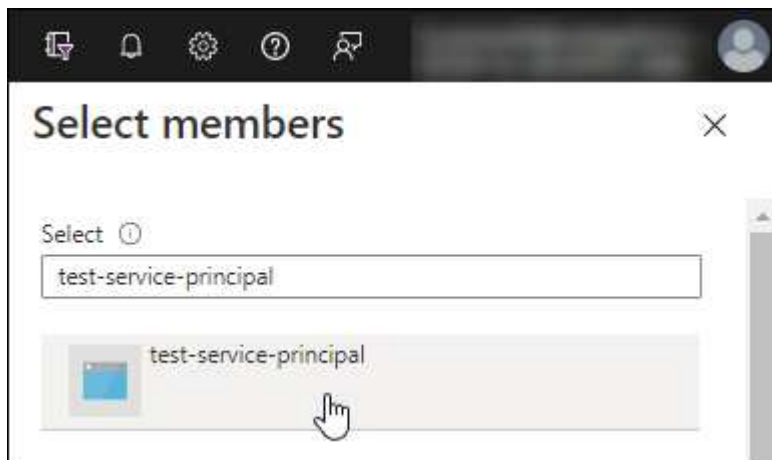
- 從 Azure 入口網站開啟 * 訂閱 * 服務。
- 選取訂閱。
- 選取 * 存取控制 (IAM) > 新增 > 新增角色指派 *。

- 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 * 」。













Request API permissions

Select an API

Microsoft APIs **APIs my organization uses** My APIs

Commonly used Microsoft APIs

Microsoft Graph
Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

 Azure Batch Schedule large-scale parallel and HPC applications in the cloud	 Azure Data Catalog Programmatic access to Data Catalog resources to register, annotate and search data assets	 Azure Data Explorer Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions
 Azure Data Lake Access to storage and compute for big data analytic scenarios	 Azure DevOps Integrate with Azure DevOps and Azure DevOps server	 Azure Import/Export Programmatic control of import/export jobs
 Azure Key Vault Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults	 Azure Rights Management Services Allow validated users to read and write protected content	 Azure Service Management Programmatic access to much of the functionality available through the Azure portal
 Azure Storage Secure, massively scalable object and data lake storage for unstructured and semi-structured data	 Customer Insights Create profile and interaction models for your products	 Data Export Service for Microsoft Dynamics 365 Export data from Microsoft Dynamics CRM organization to an external destination

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 * 。

Request API permissions

[← All APIs](#)



Azure Service Management

<https://management.azure.com/> [Docs](#)

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

Select permissions

[expand all](#)

Type to search

PERMISSION

ADMIN CONSENT REQUIRED

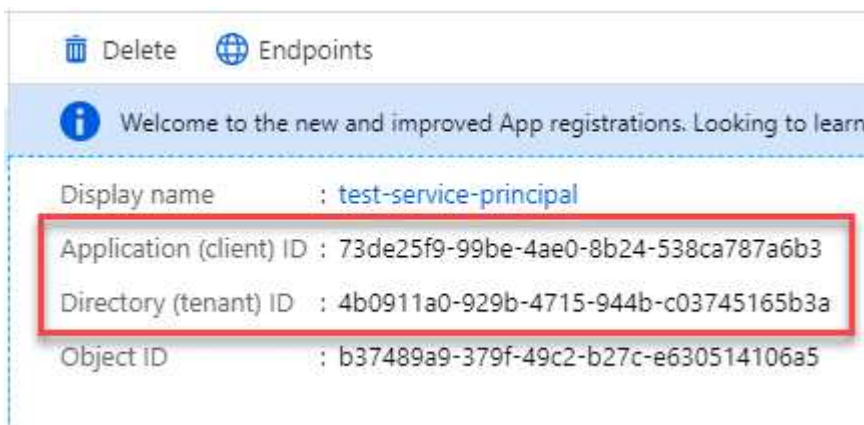


user_impersonation

Access Azure Service Management as organization users (preview)

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。

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

[+ New client secret](#)

DESCRIPTION	EXPIRES	VALUE	Copy to clipboard
test secret	8/16/2020	*sZ1jSe2By:D*-ZRoV4NLfdAcY7:+0vA	

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。

步驟 4：建立 Connector

直接從 Azure Marketplace 啟動 Connector 。

關於這項工作

從 Azure Marketplace 建立 Connector 會使用預設組態、在 Azure 中部署虛擬機器。"[瞭解連接器的預設組態](#)"。

開始之前

您應該擁有下列項目：

- Azure 訂閱。
- 您所選擇的 Azure 區域中的 Vnet 和子網路。
- 若貴組織需要代理處理所有傳出的網際網路流量、請參閱 Proxy 伺服器的詳細資料：
 - IP 位址
 - 認證資料
 - HTTPS 憑證
- SSH 公開金鑰、如果您想要將該驗證方法用於 Connector 虛擬機器。驗證方法的另一個選項是使用密碼。

["瞭解如何在 Azure 中連線至 Linux VM"](#)

- 如果您不想讓 BlueXP 自動為 Connector 建立 Azure 角色、則需要自行建立 "[使用此頁面上的原則](#)"。

這些權限適用於 Connector 執行個體本身。這是一組不同於您先前設定的權限、可用來部署 Connector VM。

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"](#)

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。
- * 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。

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。

5. 從連線至 Connector 虛擬機器的主機開啟網頁瀏覽器、然後輸入下列 URL：

`https://ipaddress`

6. 登入後、設定 Connector：
 - a. 指定與 Connector 相關聯的 BlueXP 帳戶。
 - b. 輸入系統名稱。
 - c. 在 * 您是在安全的環境中執行？ * 保持停用限制模式。

您應該保持停用受限模式、因為這些步驟說明如何在標準模式中使用 BlueXP。只有當您擁有安全的環境、而且想要中斷此帳戶與 BlueXP 後端服務的連線時、才應啟用受限模式。如果是這樣、"請依照步驟、以受限模式開始使用 BlueXP"。

- d. 選取 * 開始 * 。

結果

Connector 現已安裝、並已使用您的 BlueXP 帳戶進行設定。

如果您在建立 Connector 的同一個 Azure 訂閱中擁有 Azure Blob 儲存設備、則會在 BlueXP 畫布上自動顯示 Azure Blob 儲存設備工作環境。"瞭解如何從 BlueXP 管理 Azure Blob 儲存設備"

步驟 5：提供 BlueXP 的權限

建立 Connector 之後、您必須提供 BlueXP 先前設定的權限。提供權限可讓 BlueXP 管理 Azure 中的資料和儲存基礎架構。

自訂角色

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。

接下來呢？

前往 ["BlueXP主控台"](#) 開始使用Connector with BlueXP。

服務主體

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。

在 Azure 中手動安裝 Connector

若要在您自己的 Linux 主機上手動安裝 Connector、您必須檢閱主機需求、設定網路、準備 Azure 權限、安裝 Connector、然後提供您準備的權限。

開始之前

您應該檢閱 ["連接器限制"](#)。

步驟 1：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

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 。

/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 2：設定網路

請確定您計畫安裝 Connector 的網路位置支援下列需求。滿足這些需求後、Connector 便能在混合雲環境中管理資源和程序。

Azure地區

如果您使用 Cloud Volumes ONTAP 、Connector 應部署在與其管理的 Cloud Volumes ONTAP 系統所在的同一個 Azure 區域、或部署在中 ["Azure區域配對"](#) 適用於整個系統。Cloud Volumes ONTAP這項需求可確保Cloud Volumes ONTAP Azure Private Link連線可用於連接至相關的儲存帳戶。

["瞭Cloud Volumes ONTAP 解如何使用Azure Private Link"](#)

連線至目標網路

Connector 需要網路連線、才能連線到您計畫建立和管理工作環境的位置。例如、您計畫在內部部署環境中建立 Cloud Volumes ONTAP 系統或儲存系統的網路。

傳出網際網路存取

您部署 Connector 的網路位置必須具有傳出網際網路連線、才能連絡特定端點。

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>

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。

已從 **Connector** 聯絡的端點

Connector 需要外傳網際網路存取才能連絡下列端點、以便管理公有雲環境中的資源和程序、以進行日常營運。

請注意、下列端點均為所有的 CNAME 項目。

端點	目的
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.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://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.blueexp.netapp.com https://api.blueexp.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.blueexp.netapp.com" 」。
https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	升級Connector及其Docker元件。

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](#)"

步驟 3：設定權限

您必須使用下列其中一個選項、提供 Azure BlueXP 權限：

- 選項 1：使用系統指派的託管身分識別、將自訂角色指派給 Azure VM。
- 選項 2：為 BlueXP 提供具有必要權限的 Azure 服務主體認證。

請依照步驟準備 BlueXP 的權限。

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"](#)

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。

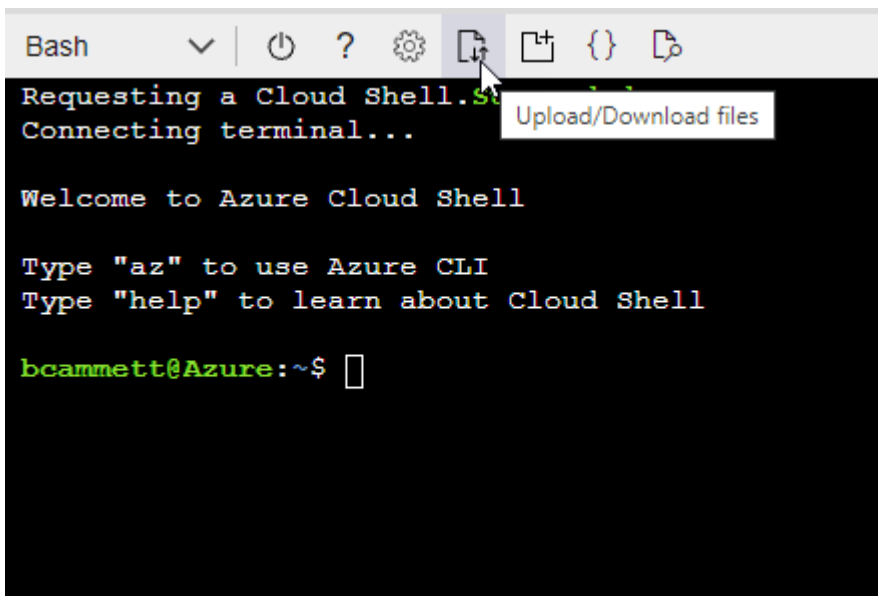
◦ 範例 *

```
"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。

服務主體

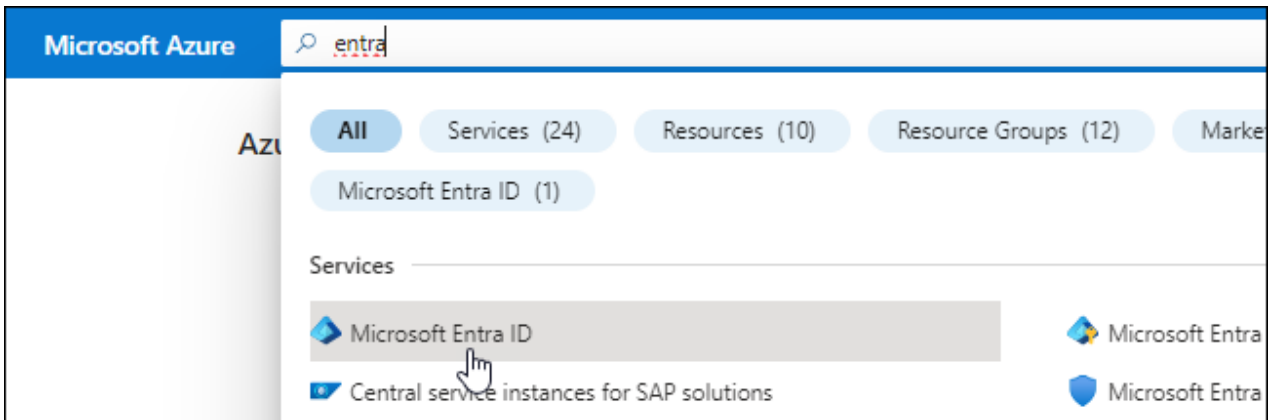
在 Microsoft Entra ID 中建立並設定服務主體、並取得 BlueXP 所需的 Azure 認證。

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。

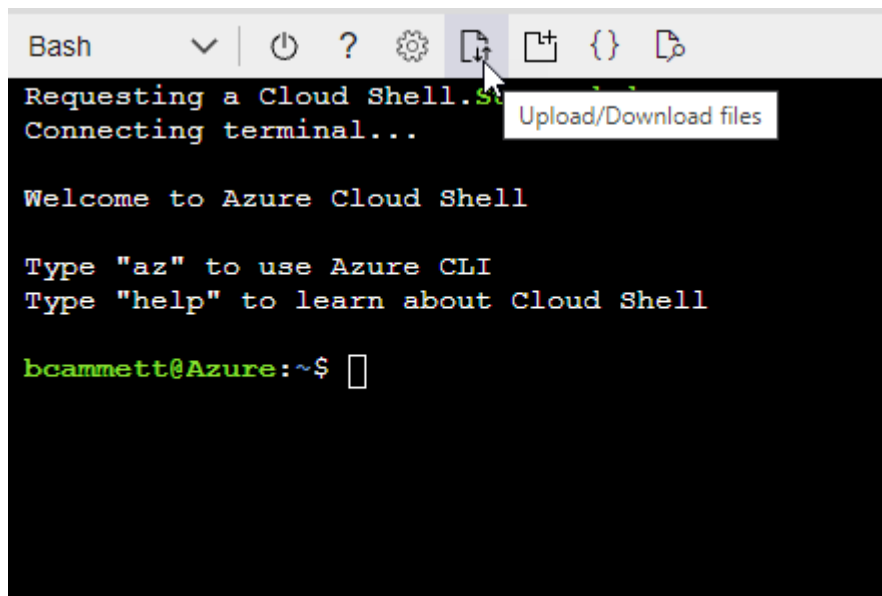
- 範例 *

```
"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：

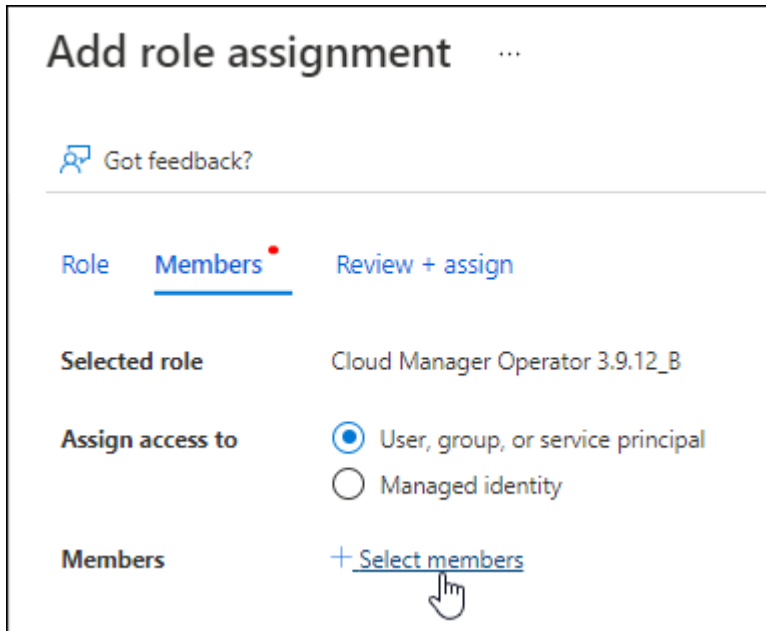
```
az role definition create --role-definition  
Connector_Policy.json
```

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：

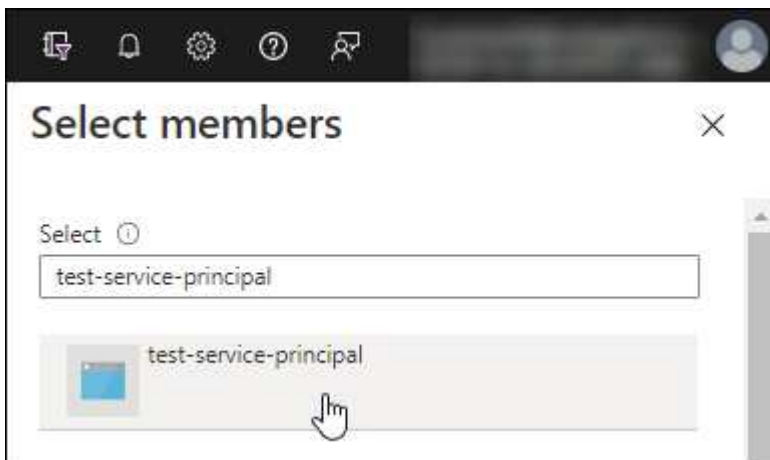
- a. 從 Azure 入口網站開啟 * 訂閱 * 服務。
- b. 選取訂閱。
- c. 選取 * 存取控制 (IAM) > 新增 > 新增角色指派 *。

- 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 * 」。













Request API permissions

Select an API

Microsoft APIs **APIs my organization uses** My APIs

Commonly used Microsoft APIs

Microsoft Graph
Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

 Azure Batch Schedule large-scale parallel and HPC applications in the cloud	 Azure Data Catalog Programmatic access to Data Catalog resources to register, annotate and search data assets	 Azure Data Explorer Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions
 Azure Data Lake Access to storage and compute for big data analytic scenarios	 Azure DevOps Integrate with Azure DevOps and Azure DevOps server	 Azure Import/Export Programmatic control of import/export jobs
 Azure Key Vault Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults	 Azure Rights Management Services Allow validated users to read and write protected content	 Azure Service Management Programmatic access to much of the functionality available through the Azure portal
 Azure Storage Secure, massively scalable object and data lake storage for unstructured and semi-structured data	 Customer Insights Create profile and interaction models for your products	 Data Export Service for Microsoft Dynamics 365 Export data from Microsoft Dynamics CRM organization to an external destination

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 * 。

Request API permissions

[← All APIs](#)



Azure Service Management

<https://management.azure.com/> [Docs](#)

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

Select permissions

[expand all](#)

Type to search

PERMISSION

ADMIN CONSENT REQUIRED

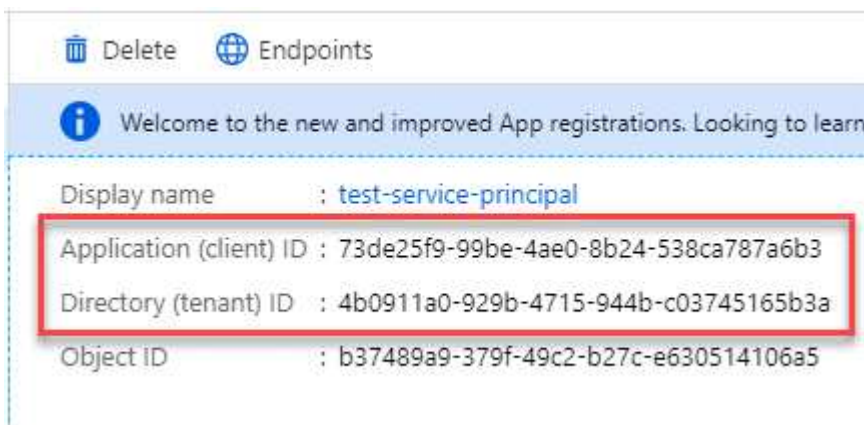


user_impersonation

Access Azure Service Management as organization users (preview)

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。

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

[+ New client secret](#)

DESCRIPTION	EXPIRES	VALUE	Copy to clipboard
test secret	8/16/2020	*sZ1jSe2By:D*-ZRoV4NLfdAcY7:+0vA	

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。

步驟 4：安裝 Connector

完成先決條件後、您可以在自己的 Linux 主機上手動安裝軟體。

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）。
- Azure 中 VM 上啟用的託管身分識別、可讓您透過自訂角色提供所需的 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"](#)

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。

6. 等待安裝完成。

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。

7. 從連線至 Connector 虛擬機器的主機開啟網頁瀏覽器、然後輸入下列 URL：

`https://ipaddress`

8. 登入後、設定 Connector：

- 指定與 Connector 相關聯的 BlueXP 帳戶。
- 輸入系統名稱。
- 在 * 您是在安全的環境中執行？ * 保持停用限制模式。

您應該保持停用受限模式、因為這些步驟說明如何在標準模式中使用 BlueXP。只有當您擁有安全的環境、而且想要中斷此帳戶與 BlueXP 後端服務的連線時、才應啟用受限模式。如果是這樣、["請依照步驟、以受限模式開始使用 BlueXP"](#)。

- 選取 * 開始 *。

結果

Connector 現已安裝、並已使用您的 BlueXP 帳戶進行設定。

如果您在建立 Connector 的同一個 Azure 訂閱中擁有 Azure Blob 儲存設備、則會在 BlueXP 畫布上自動顯示 Azure Blob 儲存設備工作環境。["瞭解如何從 BlueXP 管理 Azure Blob 儲存設備"](#)

步驟 5：提供 BlueXP 的權限

安裝 Connector 之後、您必須提供 BlueXP 先前設定的 Azure 權限。提供權限可讓 BlueXP 管理 Azure 中的資料和儲存基礎架構。

自訂角色

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。

接下來呢？

前往 ["BlueXP主控台"](#) 開始使用Connector with BlueXP。

服務主體

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

Google Cloud 中的 Connector 安裝選項

在 Google Cloud 中建立 Connector 有幾種不同的方法。直接從 BlueXP 開始是最常見的方法。

提供下列安裝選項：

- ["直接從 BlueXP 建立 Connector"](#)（這是標準選項）

此動作會在您選擇的 VPC 中啟動執行 Linux 的 VM 執行個體和 Connector 軟體。

- ["使用 gCloud 建立 Connector"](#)

此動作也會啟動執行 Linux 和 Connector 軟體的 VM 執行個體、但部署是直接從 Google Cloud 啟動、而非從 BlueXP 啟動。

- ["在您自己的 Linux 主機上下載並手動安裝軟體"](#)

您選擇的安裝選項會影響您準備安裝的方式。其中包括如何為 BlueXP 提供必要的權限、讓它能夠在 Google Cloud 中驗證及管理資源。

從 BlueXP 或 gCloud 在 Google Cloud 中建立 Connector

若要從 BlueXP 或使用 gCloud 在 Google Cloud 中建立 Connector、您必須設定網路、準備 Google Cloud 權限、啟用 Google Cloud API、然後建立 Connector。

開始之前

您應該檢閱 ["連接器限制"](#)。

步驟 1：設定網路

設定您的網路、讓 Connector 能夠管理混合雲環境中的資源和程序。例如、您需要確保目標網路可以使用連線、而且可以使用輸出網際網路存取。

VPC 和子網路

當您建立 Connector 時、您需要指定 Connector 所在的 VPC 和子網路。

連線至目標網路

Connector 需要網路連線、才能連線到您計畫建立和管理工作環境的位置。例如、您計畫在內部部署環境中建立 Cloud Volumes ONTAP 系統或儲存系統的網路。

傳出網際網路存取

您部署 Connector 的網路位置必須具有傳出網際網路連線、才能連絡特定端點。

已從 **Connector** 聯絡的端點

Connector 需要外傳網際網路存取才能連絡下列端點、以便管理公有雲環境中的資源和程序、以進行日常營運。

請注意、下列端點均為所有的 CNAME 項目。

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	升級Connector及其Docker元件。

從 **BlueXP** 主控台連絡的端點

當您使用透過 SaaS 層提供的 BlueXP 網路型主控台時、它會與多個端點聯絡、以完成資料管理工作。這包括透過 BlueXP 主控台聯絡以部署 Connector 的端點。

"檢視從 **BlueXP** 主控台連絡的端點清單"。

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](#)"

建立 Connector 之後、您必須實作此網路需求。

步驟 2：設定建立 **Connector** 的權限

您必須先為部署 Connector VM 的 Google Cloud 使用者設定權限、才能從 BlueXP 或使用 gCloud 部署 Connector 。

步驟

1. 在 Google Cloud 中建立自訂角色：
 - a. 建立包含下列權限的 YAML 檔案：

```
title: Connector deployment policy
description: Permissions for the user who deploys the Connector from
BlueXP
stage: GA
includedPermissions:
- compute.disks.create
- compute.disks.get
- compute.disks.list
```

- compute.disks.setLabels
- compute.disks.use
- compute.firewalls.create
- compute.firewalls.delete
- compute.firewalls.get
- compute.firewalls.list
- compute.globalOperations.get
- compute.images.get
- compute.images.getFromFamily
- compute.images.list
- compute.images.useReadOnly
- compute.instances.attachDisk
- compute.instances.create
- compute.instances.get
- compute.instances.list
- compute.instances.setDeletionProtection
- compute.instances.setLabels
- compute.instances.setMachineType
- compute.instances.setMetadata
- compute.instances.setTags
- compute.instances.start
- compute.instances.updateDisplayDevice
- compute.machineTypes.get
- compute.networks.get
- compute.networks.list
- compute.networks.updatePolicy
- compute.projects.get
- compute.regions.get
- compute.regions.list
- compute.subnetworks.get
- compute.subnetworks.list
- compute.zoneOperations.get
- compute.zones.get
- compute.zones.list
- deploymentmanager.compositeTypes.get
- deploymentmanager.compositeTypes.list
- deploymentmanager.deployments.create
- deploymentmanager.deployments.delete
- deploymentmanager.deployments.get
- deploymentmanager.deployments.list
- deploymentmanager.manifests.get
- deploymentmanager.manifests.list
- deploymentmanager.operations.get
- deploymentmanager.operations.list
- deploymentmanager.resources.get
- deploymentmanager.resources.list

```
- deploymentmanager.typeProviders.get
- deploymentmanager.typeProviders.list
- deploymentmanager.types.get
- deploymentmanager.types.list
- resourcemanager.projects.get
- compute.instances.setServiceAccount
- iam.serviceAccounts.list
```

- b. 從 Google Cloud 啟動 Cloud Shell 。
- c. 上傳包含必要權限的 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「connectorDeployment」的角色：

```
gCloud iam 角色會建立 connectorDeployment --project=MyProject --file=connector-deployment.yaml
```

"Google Cloud 文件：建立及管理自訂角色"

2. 將此自訂角色指派給將從 BlueXP 或使用 gCloud 部署 Connector 的使用者。

"Google Cloud 文件：授予單一角色"

結果

Google Cloud 使用者現在擁有建立 Connector 所需的權限。

步驟 3：設定 Connector 的權限

需要 Google Cloud 服務帳戶、才能為 Connector 提供 BlueXP 在 Google Cloud 中管理資源所需的權限。建立 Connector 時、您需要將此服務帳戶與 Connector VM 建立關聯。

步驟

1. 在 Google Cloud 中建立自訂角色：
 - a. 建立包含的內容的 YAML 檔案 "[Connector 的服務帳戶權限](#)"。
 - b. 從 Google Cloud 啟動 Cloud Shell 。
 - c. 上傳包含必要權限的 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、並將角色指派給服務帳戶：
 - 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"

3. 如果您計畫在Cloud Volumes ONTAP Connector所在專案的不同專案中部署支援功能、則需要提供Connector的服務帳戶、以便存取這些專案。

例如、假設Connector在專案1中、您想在Cloud Volumes ONTAP 專案2中建立一套支援系統。您必須在專案2中授予服務帳戶存取權。

- a. 從 IAM & Admin 服務中、選取您要建立 Cloud Volumes ONTAP 系統的 Google Cloud 專案。
- b. 在「* IAM 」頁面上、選取「*授予存取權」、並提供所需的詳細資料。
 - 輸入Connector服務帳戶的電子郵件。
 - 選取Connector的自訂角色。
 - 選擇*保存*。

如需詳細資料、請參閱 "Google Cloud文件"

結果

已設定Connector VM的服務帳戶。

步驟 4：設定共用 VPC 權限

如果您使用共享 VPC 將資源部署到服務專案中、則需要準備權限。

此表供參考、當IAM組態完成時、您的環境應反映權限表。

檢視共享的 VPC 權限

身分識別	建立者	裝載於	服務專案權限	主機專案權限	目的
Google 帳戶以部署 Connector	自訂	服務專案	"Connector 部署原則"	compute.network User	在服務專案中部署Connector
連接器服務帳戶	自訂	服務專案	"Connector 服務帳戶原則"	compute.network User 部署manager.manager	在Cloud Volumes ONTAP 服務專案中部署及維護功能與服務
服務帳戶Cloud Volumes ONTAP	自訂	服務專案	儲存設備管理 成員： serviceAccount.user的BlueXP服務帳戶	不適用	(選用) 用於資料分層和 BlueXP 備份與還原
Google API服務代理程式	Google Cloud	服務專案	(預設) 編輯器	compute.network User	代表部署與Google Cloud API互動。允許BlueXP使用共享網路。
Google Compute Engine預設服務帳戶	Google Cloud	服務專案	(預設) 編輯器	compute.network User	代表部署部署部署部署Google Cloud執行個體和運算基礎架構。允許BlueXP使用共享網路。

附註：

1. 只有當您未將防火牆規則傳遞給部署、並選擇讓BlueXP為您建立時、才需要在主機專案中部署manager.manager。如果未指定任何規則、則BlueXP會在主機專案中建立包含VPC0防火牆規則的部署。
2. 只有當您未將防火牆規則傳遞至部署、並選擇讓BlueXP為您建立防火牆規則時、才需要使用Firewall.create和firewall.delete。這些權限位於BlueXP帳戶.yaml檔案中。如果您使用共用VPC部署HA配對、這些權限將用於建立VPC1、2和3的防火牆規則。對於所有其他部署、這些權限也會用於建立VPC0的規則。
3. 對於資料分層、分層服務帳戶必須在服務帳戶上具有serviceAccount.user角色、而不只是在專案層級。目前、如果您在專案層級指派serviceAccount.user、則當您使用getIAMPolicy查詢服務帳戶時、不會顯示權限。

步驟 5：啟用 Google Cloud API

您必須先啟用數個 Google Cloud API、才能在 Google Cloud 中部署 Connector 和 Cloud Volumes ONTAP。

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）

["Google Cloud 文件：啟用 API"](#)

步驟 6：建立 Connector

直接從 BlueXP 網路型主控台或使用 gCloud 建立 Connector。

關於這項工作

建立 Connector 會使用預設組態、在 Google Cloud 中部署虛擬機器執行個體。建立 Connector 之後、不應變更為 CPU 或 RAM 較少的較小 VM 執行個體。["瞭解連接器的預設組態"](#)。

藍圖

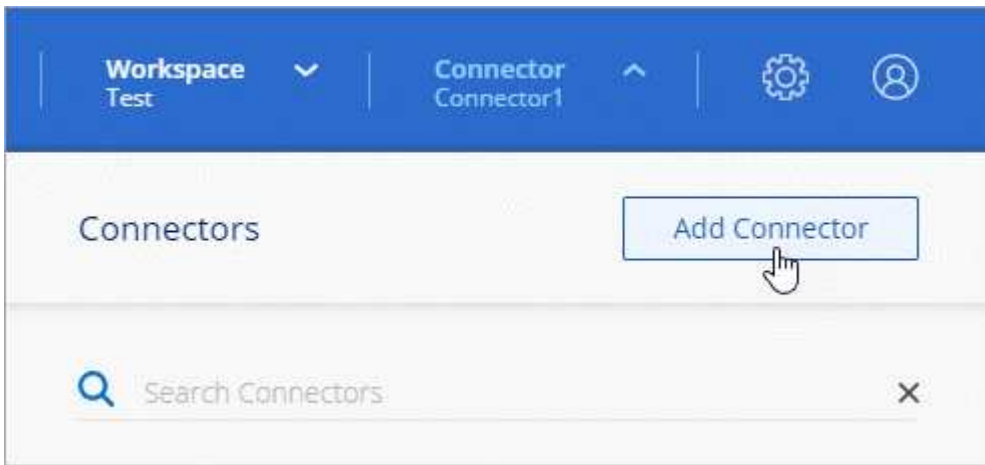
開始之前

您應該擁有下列項目：

- 建立 Connector 和 Connector VM 服務帳戶所需的 Google Cloud 權限。
- 符合網路需求的 VPC 和子網路。
- Proxy 伺服器的詳細資料、如果需要 Proxy 才能從 Connector 存取網際網路。

步驟

1. 選取 * Connector * 下拉式清單、然後選取 * 新增 Connector * 。



2. 選擇 * Google Cloud Platform * 做為雲端供應商。
3. 在「部署連接器」頁面上、檢閱您需要的詳細資料。您有兩種選擇：
 - a. 選擇 * 繼續 * 、使用產品內建指南準備部署。產品內建指南中的每個步驟都包含文件本頁所含的資訊。
 - b. 如果您已按照本頁的步驟做好準備、請選取 * 跳至部署 * 。

4. 依照精靈中的步驟建立連接器：

- 如果出現提示、請登入您的 Google 帳戶、該帳戶應有建立虛擬機器執行個體所需的權限。

這份表單由 Google 擁有及託管。您的認證資料不會提供給 NetApp 。

- 詳細資料：輸入虛擬機器執行個體的名稱、指定標籤、選取專案、然後選取具有必要權限的服務帳戶（詳細資料請參閱上節）。
- * 位置 *：指定執行個體的區域、區域、VPC 和子網路。
- * 網路 *：選擇是否啟用公用 IP 位址、並選擇性地指定 Proxy 組態。
- * 防火牆原則 *：選擇是否要建立新的防火牆原則，或是選擇允許所需輸入和輸出規則的現有防火牆原則。

"Google Cloud 中的防火牆規則"

- 審查：請檢閱您的選擇、確認您的設定正確無誤。

5. 選取*「Add*」。

執行個體應在 7 分鐘內就緒。您應該留在頁面上、直到程序完成為止。

結果

程序完成後、即可從 BlueXP 使用 Connector。

如果您在建立 Connector 的同一個 Google Cloud 帳戶中有 Google Cloud Storage 貯體、則 BlueXP 畫布會自動顯示 Google Cloud Storage 工作環境。["瞭解如何從 BlueXP 管理 Google Cloud Storage"](#)

gCloud

開始之前

您應該擁有下列項目：

- 建立 Connector 和 Connector VM 服務帳戶所需的 Google Cloud 權限。
- 符合網路需求的 VPC 和子網路。
- 瞭解 VM 執行個體需求。
 - * CPU*：4 核心或 4 個 vCPU
 - * RAM*：14 GB
 - * 機器類型*：建議使用 n2-Standard-4。

在支援 Shielded VM 功能的 VM 執行個體上、Google Cloud 支援 Connector。

步驟

1. 使用您偏好的方法登入gCloud SDK。

在我們的範例中、我們會使用已安裝gCloud SDK的本機Shell、但您可以在Google Cloud主控台使用原生Google Cloud Shell。

如需Google Cloud SDK的詳細資訊、請參閱 ["Google Cloud SDK文件頁面"](#)。

2. 請確認您以具有上述區段所定義之必要權限的使用者身分登入：

```
gcloud auth list
```

輸出應顯示下列項目、其中*使用者帳戶是所需的使用者帳戶、以下列身分登入：

```
Credentialed Accounts
ACTIVE ACCOUNT
    some_user_account@domain.com
*    desired_user_account@domain.com
To set the active account, run:
$ gcloud config set account `ACCOUNT`
Updates are available for some Cloud SDK components. To install
them,
please run:
$ gcloud components update
```

3. 執行 gcloud compute instances create 命令：

```
gcloud compute instances create <instance-name>
  --machine-type=n2-standard-4
  --image-project=netapp-cloudmanager
  --image-family=cloudmanager
  --scopes=cloud-platform
  --project=<project>
  --service-account=<service-account>
  --zone=<zone>
  --no-address
  --tags <network-tag>
  --network <network-path>
  --subnet <subnet-path>
  --boot-disk-kms-key <kms-key-path>
```

執行個體名稱

VM執行個體所需的執行個體名稱。

專案

(選用) 您要部署VM的專案。

服務帳戶

步驟2輸出中指定的服務帳戶。

區域

您要部署VM的區域

無位址

(選用) 不使用外部IP位址 (您需要雲端NAT或Proxy才能將流量路由至公有網際網路)

網路標籤

(選用) 新增網路標記、使用標記將防火牆規則連結至連接器執行個體

網路路徑

(選用) 新增要部署連接器的網路名稱 (若為共享VPC、您需要完整路徑)

子網路路徑

(選用) 新增要部署連接器的子網路名稱 (對於共享VPC、您需要完整路徑)

kms-key-path

(選用) 新增KMS金鑰以加密連接器的磁碟 (也需要套用IAM權限)

如需這些旗標的詳細資訊、請參閱 ["Google Cloud Compute SDK文件"](#)。

+

執行命令會使用NetApp黃金映像部署Connector。Connector 執行個體和軟體應在大約五分鐘內執行。

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. 登入後、設定 Connector：

- a. 指定與 Connector 相關聯的 BlueXP 帳戶。

["瞭解 BlueXP 帳戶"](#)。

- b. 輸入系統名稱。

結果

Connector 現在已安裝、並使用您的 BlueXP 帳戶進行設定。

開啟網頁瀏覽器、前往 ["BlueXP主控台"](#) 開始使用Connector with BlueXP。

在 Google Cloud 中手動安裝 Connector

若要在您自己的 Linux 主機上手動安裝 Connector、您必須檢閱主機需求、設定網路、準備 Google Cloud 權限、啟用 Google Cloud API、安裝 Connector、然後提供您準備的權限。

開始之前

您應該檢閱 ["連接器限制"](#)。

步驟 1：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

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 2：設定網路

設定您的網路、讓 Connector 能夠管理混合雲環境中的資源和程序。例如、您需要確保目標網路可以使用連線、而且可以使用輸出網際網路存取。

連線至目標網路

Connector 需要網路連線、才能連線到您計畫建立和管理工作環境的位置。例如、您計畫在內部部署環境中建立 Cloud Volumes ONTAP 系統或儲存系統的網路。

傳出網際網路存取

您部署 Connector 的網路位置必須具有傳出網際網路連線、才能連絡特定端點。

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>

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。

已從 **Connector** 聯絡的端點

Connector 需要外傳網際網路存取才能連絡下列端點、以便管理公有雲環境中的資源和程序、以進行日常營運。

請注意、下列端點均為所有的 CNAME 項目。

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.bluelxp.netapp.com https://api.bluelxp.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.bluelxp.netapp.com" 」。

端點	目的
https://*.blob.core.windows.net	升級Connector及其Docker元件。
https://cloudmanagerinfraprod.azurecr.io	

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"](#)

步驟 3：設定 Connector 的權限

需要 Google Cloud 服務帳戶、才能為 Connector 提供 BlueXP 在 Google Cloud 中管理資源所需的權限。建立 Connector 時、您需要將此服務帳戶與 Connector VM 建立關聯。

步驟

1. 在 Google Cloud 中建立自訂角色：
 - a. 建立包含的內容的 YAML 檔案 ["Connector 的服務帳戶權限"](#)。
 - b. 從 Google Cloud 啟動 Cloud Shell。
 - c. 上傳包含必要權限的 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、並將角色指派給服務帳戶：
 - 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"

3. 如果您計畫在Cloud Volumes ONTAP Connector所在專案的不同專案中部署支援功能、則需要提供Connector的服務帳戶、以便存取這些專案。

例如、假設Connector在專案1中、您想在Cloud Volumes ONTAP 專案2中建立一套支援系統。您必須在專案2中授予服務帳戶存取權。

- a. 從 IAM & Admin 服務中、選取您要建立 Cloud Volumes ONTAP 系統的 Google Cloud 專案。
- b. 在「* IAM 」頁面上、選取「*授予存取權」、並提供所需的詳細資料。
 - 輸入Connector服務帳戶的電子郵件。
 - 選取Connector的自訂角色。
 - 選擇*保存*。

如需詳細資料、請參閱 ["Google Cloud文件"](#)

結果

已設定Connector VM的服務帳戶。

步驟 4：設定共用 VPC 權限

如果您使用共享 VPC 將資源部署到服務專案中、則需要準備權限。

此表供參考、當IAM組態完成時、您的環境應反映權限表。

檢視共享的 VPC 權限

身分識別	建立者	裝載於	服務專案權限	主機專案權限	目的
Google 帳戶以部署 Connector	自訂	服務專案	"Connector 部署原則"	compute.network User	在服務專案中部署Connector
連接器服務帳戶	自訂	服務專案	"Connector 服務帳戶原則"	compute.network User 部署manager.manager	在Cloud Volumes ONTAP 服務專案中部署及維護功能與服務
服務帳戶Cloud Volumes ONTAP	自訂	服務專案	儲存設備管理 成員 ：serviceAccount.user的BlueXP服務帳戶	不適用	(選用) 用於資料分層和 BlueXP 備份與還原
Google API服務代理程式	Google Cloud	服務專案	(預設) 編輯器	compute.network User	代表部署與Google Cloud API互動。允許BlueXP使用共享網路。
Google Compute Engine預設服務帳戶	Google Cloud	服務專案	(預設) 編輯器	compute.network User	代表部署部署部署部署Google Cloud執行個體和運算基礎架構。允許BlueXP使用共享網路。

附註：

1. 只有當您未將防火牆規則傳遞給部署、並選擇讓BlueXP為您建立時、才需要在主機專案中部署manager.manager。如果未指定任何規則、則BlueXP會在主機專案中建立包含VPC0防火牆規則的部署。
2. 只有當您未將防火牆規則傳遞至部署、並選擇讓BlueXP為您建立防火牆規則時、才需要使用Firewall.create和firewall.delete。這些權限位於BlueXP帳戶.yaml檔案中。如果您使用共用VPC部署HA配對、這些權限將用於建立VPC1、2和3的防火牆規則。對於所有其他部署、這些權限也會用於建立VPC0的規則。
3. 對於資料分層、分層服務帳戶必須在服務帳戶上具有serviceAccount.user角色、而不只是在專案層級。目前、如果您在專案層級指派serviceAccount.user、則當您使用getIAMPolicy查詢服務帳戶時、不會顯示權限。

步驟 5：啟用 Google Cloud API

您必須先啟用數個 Google Cloud API、才能在 Google Cloud 中部署 Cloud Volumes ONTAP 系統。

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）

"Google Cloud 文件：啟用 API"

步驟 6：安裝 Connector

完成先決條件後、您可以在自己的 Linux 主機上手動安裝軟體。

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。

6. 等待安裝完成。

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。

7. 從連線至 Connector 虛擬機器的主機開啟網頁瀏覽器、然後輸入下列 URL：

`https://ipaddress`

8. 登入後、設定 Connector：

- a. 指定與 Connector 相關聯的 BlueXP 帳戶。
- b. 輸入系統名稱。
- c. 在 * 您是在安全的環境中執行？ * 保持停用限制模式。

您應該保持停用受限模式、因為這些步驟說明如何在標準模式中使用 BlueXP。只有當您擁有安全的環境、而且想要中斷此帳戶與 BlueXP 後端服務的連線時、才應啟用受限模式。如果是這樣、["請依照步驟、以受限模式開始使用 BlueXP"](#)。

- d. 選取 * 開始 *。

結果

Connector 現已安裝、並已使用您的 BlueXP 帳戶進行設定。

如果您在建立 Connector 的同一個 Google Cloud 帳戶中有 Google Cloud Storage 貯體、則 BlueXP 畫布會自動顯示 Google Cloud Storage 工作環境。["瞭解如何從 BlueXP 管理 Google Cloud Storage"](#)

步驟 7：提供 BlueXP 的權限

您必須提供 BlueXP 先前設定的 Google Cloud 權限。提供權限可讓 BlueXP 在 Google Cloud 中管理您的資料和儲存基礎架構。

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 Google Cloud 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。

在內部部署安裝並設定 Connector

在內部部署安裝 Connector、然後登入並設定以搭配 BlueXP 帳戶使用。

開始之前

您應該檢閱 ["連接器限制"](#)。

步驟 1：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。安裝 Connector 之前、請先確定您的主機符合這些要求。

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

/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 2：設定網路

設定您的網路、讓 Connector 能夠管理混合雲環境中的資源和程序。例如、您需要確保目標網路可以使用連線、而且可以使用輸出網際網路存取。

連線至目標網路

Connector 需要網路連線、才能連線到您計畫建立和管理工作環境的位置。例如、您計畫在內部部署環境中建立 Cloud Volumes ONTAP 系統或儲存系統的網路。

傳出網際網路存取

您部署 Connector 的網路位置必須具有傳出網際網路連線、才能連絡特定端點。

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>

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。

已從 Connector 聯絡的端點

Connector 需要外傳網際網路存取才能連絡下列端點、以便管理公有雲環境中的資源和程序、以進行日常營運。

請注意、下列端點均為所有的 CNAME 項目。

端點	目的
AWS 服務 (amazonaws.com): <ul style="list-style-type: none">• CloudFormation• 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.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.blueexp.netapp.com https://api.blueexp.netapp.com https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com https://netapp-cloud-account.auth0.com	<p>在BlueXP中提供SaaS功能與服務。</p> <p>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.blueexp.netapp.com」。</p>
https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	升級Connector及其Docker元件。

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](#)"

步驟 3：設定雲端權限

如果您想在 AWS 或 Azure 中搭配內部部署 Connector 使用 BlueXP 服務、則需要在雲端供應商中設定權限、以便在安裝之後將認證新增至 Connector。



為何不選擇 Google Cloud？當 Connector 安裝在您的內部環境中時、就無法在 Google Cloud 中管理您的資源。Connector 必須安裝在 Google Cloud 中、才能管理任何位於該處的資源。

AWS

當 Connector 安裝在內部部署時、您需要為具有必要權限的 IAM 使用者新增存取金鑰、以提供 BlueXP AWS 權限。

如果連接器安裝在內部部署環境中、則必須使用此驗證方法。您無法使用IAM角色。

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

您現在應該擁有具有必要權限的 IAM 使用者存取金鑰。安裝 Connector 之後、您需要將這些認證與 BlueXP 的 Connector 建立關聯。

Azure

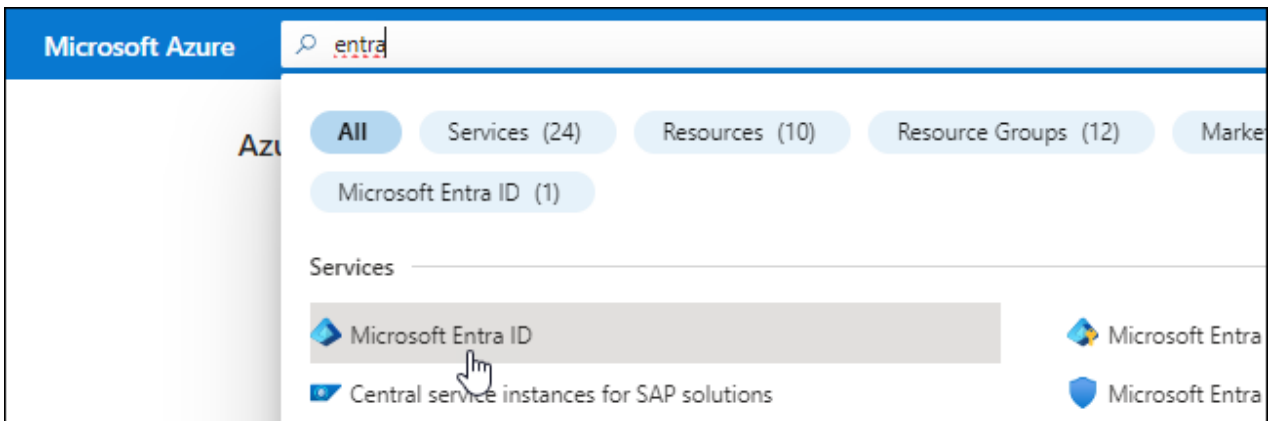
當 Connector 安裝在內部部署時、您需要在 Microsoft Entra ID 中設定服務主體、並取得 BlueXP 所需的 Azure 認證、以提供 BlueXP 的 Azure 權限。

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 *

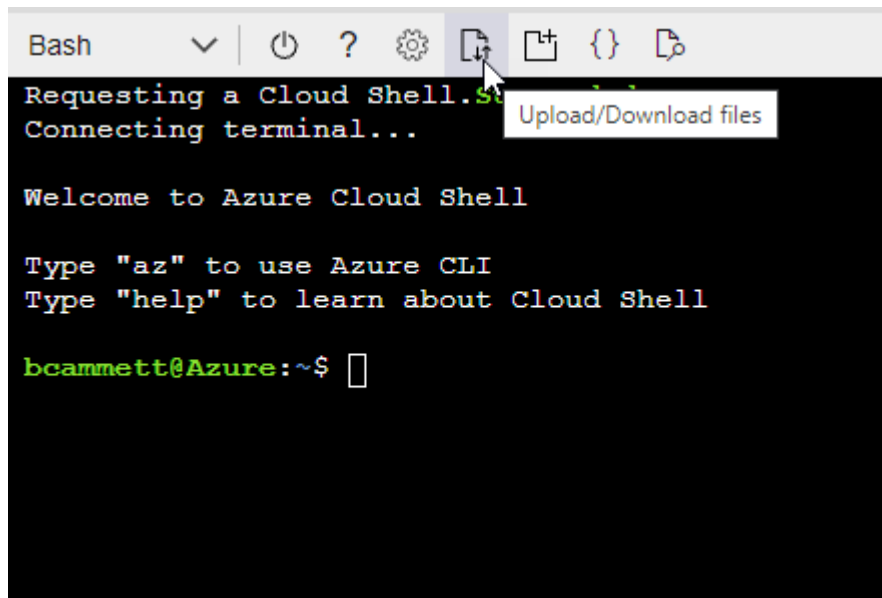
```
"AssignableScopes": [
  "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
  "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
  "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
```

- 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。



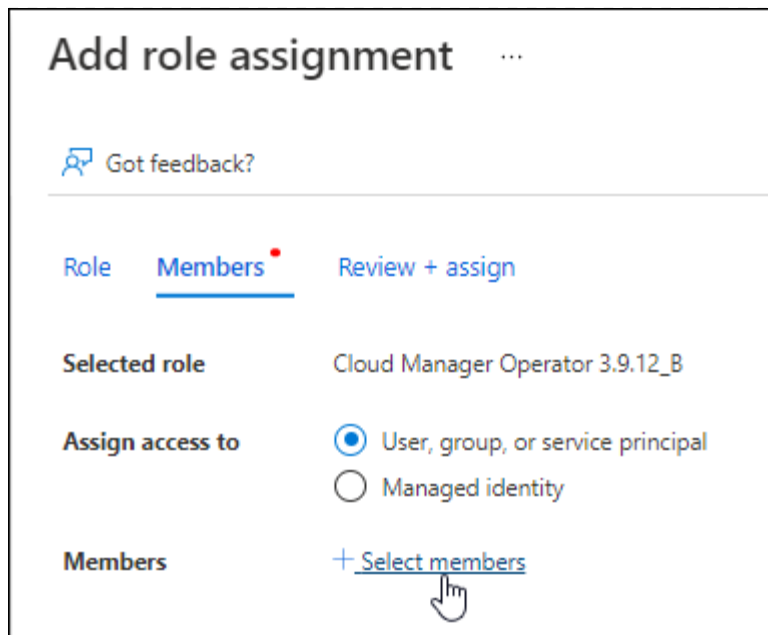
- 使用Azure CLI建立自訂角色：

```
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。

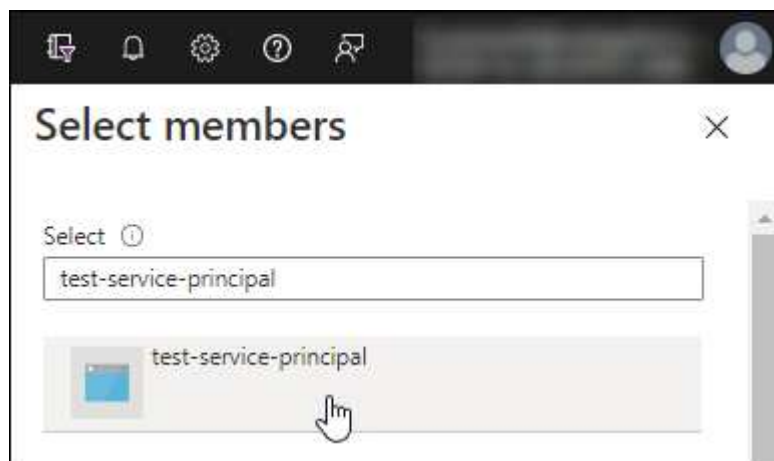
2. 將應用程式指派給角色：

- 從 Azure 入口網站開啟 * 訂閱 * 服務。
- 選取訂閱。
- 選取 * 存取控制（IAM） > 新增 > 新增角色指派 *。
- 在 * 角色 * 索引標籤中、選取 * BlueXP 操作員 * 角色、然後選取 * 下一步 *。
- 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 *」。

Request API permissions

Select an API

Microsoft APIs APIs my organization uses My APIs

Commonly used Microsoft APIs

Microsoft Graph

Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.



Azure Batch

Schedule large-scale parallel and HPC applications in the cloud

Azure Data Catalog

Programmatic access to Data Catalog resources to register, annotate and search data assets

Azure Data Explorer

Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions

Azure Data Lake

Access to storage and compute for big data analytic scenarios

Azure DevOps

Integrate with Azure DevOps and Azure DevOps server

Azure Import/Export

Programmatic control of import/export jobs

Azure Key Vault

Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults

Azure Rights Management Services

Allow validated users to read and write protected content

Azure Service Management

Programmatic access to much of the functionality available through the Azure portal

Azure Storage

Secure, massively scalable object and data lake storage for unstructured and semi-structured data

Customer Insights

Create profile and interaction models for your products

Data Export Service for Microsoft Dynamics 365

Export data from Microsoft Dynamics CRM organization to an external destination

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 * 。

Request API permissions

[← All APIs](#)



Azure Service Management

<https://management.azure.com/> [Docs](#)

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

Select permissions

[expand all](#)

Type to search

PERMISSION

ADMIN CONSENT REQUIRED

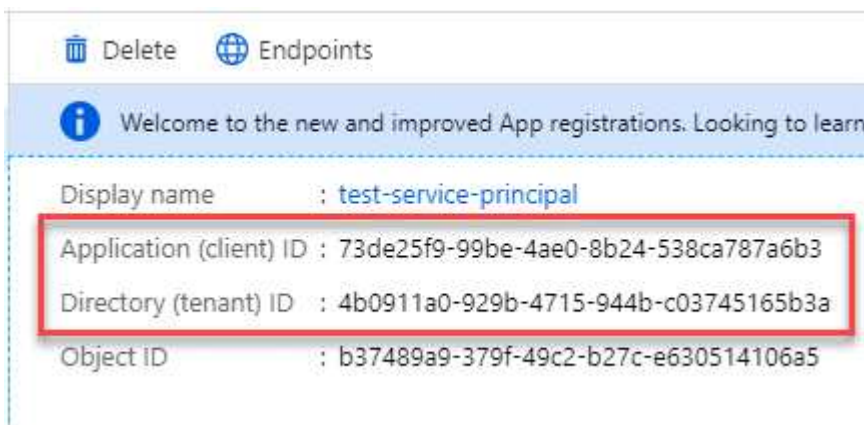


user_impersonation

Access Azure Service Management as organization users (preview)

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。

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

[+ New client secret](#)

DESCRIPTION	EXPIRES	VALUE	Copy to clipboard
test secret	8/16/2020	*sZ1jSe2By:D*-ZRoV4NLfdAcY7:+0vA	

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。安裝 Connector 之後、您需要將這些認證與 BlueXP 的 Connector 建立關聯。

步驟 4：安裝 Connector

在內部部署的現有 Linux 主機上下載並安裝 Connector 軟體。

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。

步驟 5：設定 Connector

註冊或登入、然後設定 Connector 以搭配 BlueXP 帳戶使用。

步驟

1. 開啟網頁瀏覽器並輸入下列 URL：

```
<a href="https://<em>ipaddress</em>" class="bare">https://<em>ipaddress</em></a>
```

ipaddress 可以是 localhost、私有 IP 位址或公有 IP 位址、視主機的組態而定。例如、如果連接器位於沒有公有 IP 位址的公有雲中、您必須輸入連接至連接器主機之主機的私有 IP 位址。

2. 註冊或登入。
3. 登入之後、請設定BlueXP：
 - a. 指定與 Connector 相關聯的 BlueXP 帳戶。
 - b. 輸入系統名稱。
 - c. 在 * 您是在安全的環境中執行？ * 保持停用限制模式。

您應該保持停用受限模式、因為這些步驟說明如何在標準模式中使用 BlueXP。（此外、當 Connector 安裝在內部部署時、不支援受限模式。）

- d. 選取 * 開始 *。

結果

BlueXP 現在已設定好您剛安裝的 Connector。

步驟 6：提供 BlueXP 的權限

安裝並設定 Connector 之後、請新增您的雲端認證、以便 BlueXP 具有必要的權限、可在 AWS 或 Azure 中執行動作。

AWS

開始之前

如果您剛在 AWS 中建立這些認證、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。

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。

您現在可以前往 ["BlueXP主控台"](#) 開始使用Connector with BlueXP。

Azure

開始之前

如果您剛在 Azure 中建立這些認證、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。

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。您現在可以前往 ["BlueXP主控台"](#) 開始使用Connector with BlueXP。

訂閱 BlueXP（標準模式）

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。

市場訂閱可為下列 BlueXP 服務收費：

- 備份與還原
- 分類
- Cloud Volumes ONTAP
- 分層

開始之前

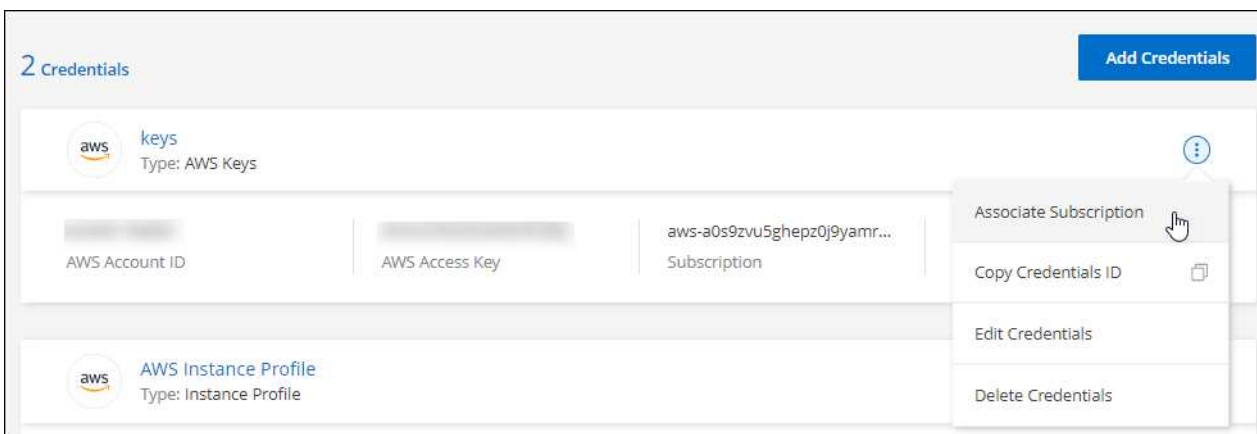
訂閱 BlueXP 涉及將市場訂閱與與 Connector 相關的雲端認證建立關聯。如果您遵循「標準模式入門」工作流程、則應該已經有 Connector。若要深入瞭解、請檢視 ["以標準模式快速啟動 BlueXP"](#)。

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：

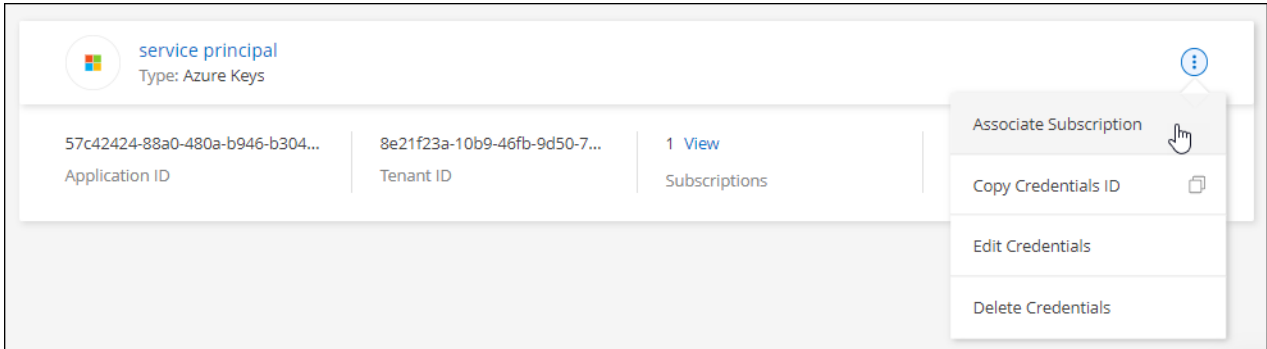
[從 AWS Marketplace 訂閱 BlueXP](#)

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*。

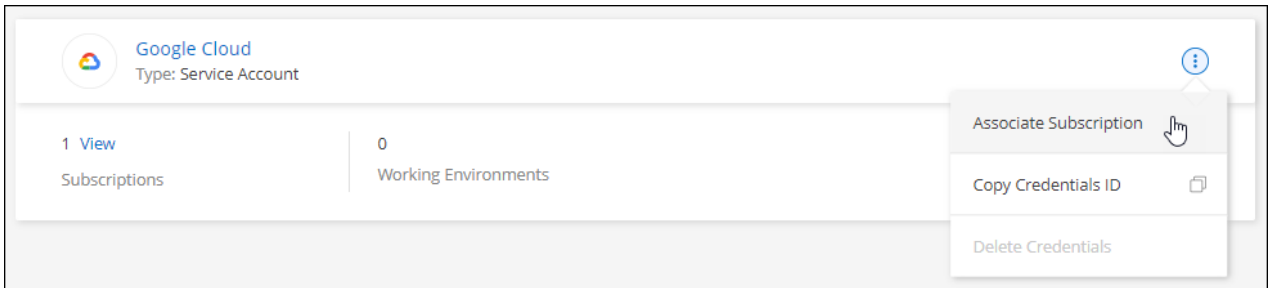
下列影片顯示從Azure Marketplace訂閱的步驟：

[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*。

Google Cloud Project

OCCM-Dev

Subscription

 GCP subscription for staging


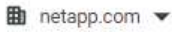
[+ Add Subscription](#)


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。

 Product details



NetApp BlueXP

[NetApp, Inc.](#)

BlueXP lets you build, protect, and govern your hybrid multicloud data estate.

[SUBSCRIBE](#)

[OVERVIEW](#) [PRICING](#) [DOCUMENTATION](#) [SUPPORT](#)

Overview

BlueXP is NetApp's hybrid multicloud storage and data services experience that helps organizations build and operate a centrally controlled data foundation across on-premises, edge, and cloud environments.

BlueXP abstracts the complexity of architecting the underlying Google Cloud infrastructure resources making it easier to deploy and operate NetApp's storage, mobility, protection, and analysis services within your Google Cloud environment.

Additional details

Type: [SaaS & APIs](#)

Last updated: 12/19/22

Category: [Analytics](#), [Developer tools](#), [Storage](#)


- 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。

Your order request has been sent to NetApp, Inc.



Your new subscription to the Cloud Manager 1 month plan for Cloud Manager for Cloud Volumes ONTAP requires your registration with NetApp, Inc.. After NetApp, Inc. approves your request, your subscription will be active and you will begin getting charged. This processing time will depend on the vendor, and you should reach out to NetApp, Inc. directly with any questions related to signup.

[VIEW ORDERS](#) [REGISTER WITH NETAPP, INC.](#)

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。

Google Cloud Project

OCCM-Dev

Subscription

GCP subscription for staging

+ Add Subscription

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（標準模式）

現在您已經以標準模式登入並設定 BlueXP、使用者可以建立和探索工作環境、並使用 BlueXP 資料服務。



如果您在 AWS、Microsoft Azure 或 Google Cloud 中安裝 Connector、則 BlueXP 會自動探索安裝 Connector 所在位置的 Amazon S3 貯體、Azure Blob 儲存設備或 Google Cloud Storage 貯體相關資訊。工作環境會自動新增至 BlueXP 畫布。

如需協助、請前往 ["BlueXP 文件首頁"](#) 檢視所有 BlueXP 服務的文件。

相關連結

["BlueXP 部署模式"](#)

版權資訊

Copyright © 2024 NetApp, Inc. 版權所有。台灣印製。非經版權所有人事先書面同意，不得將本受版權保護文件的任何部分以任何形式或任何方法（圖形、電子或機械）重製，包括影印、錄影、錄音或儲存至電子檢索系統中。

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

此軟體以 NETAPP「原樣」提供，不含任何明示或暗示的擔保，包括但不限於有關適售性或特定目的適用性之擔保，特此聲明。於任何情況下，就任何已造成或基於任何理論上責任之直接性、間接性、附隨性、特殊性、懲罰性或衍生性損害（包括但不限於替代商品或服務之採購；使用、資料或利潤上的損失；或企業營運中斷），無論是在使用此軟體時以任何方式所產生的契約、嚴格責任或侵權行為（包括疏忽或其他）等方面，NetApp 概不負責，即使已被告知有前述損害存在之可能性亦然。

NetApp 保留隨時變本文所述之任何產品的權利，恕不另行通知。NetApp 不承擔因使用本文所述之產品而產生的責任或義務，除非明確經過 NetApp 書面同意。使用或購買此產品並不會在依據任何專利權、商標權或任何其他 NetApp 智慧財產權的情況下轉讓授權。

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

有限權利說明：政府機關的使用、複製或公開揭露須受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中的「技術資料權利 - 非商業項目」條款 (b)(3) 小段所述之限制。

此處所含屬於商業產品和 / 或商業服務（如 FAR 2.101 所定義）的資料均為 NetApp, Inc. 所有。根據本協議提供的所有 NetApp 技術資料和電腦軟體皆屬於商業性質，並且完全由私人出資開發。美國政府對於該資料具有非專屬、非轉讓、非轉授權、全球性、有限且不可撤銷的使用權限，僅限於美國政府為傳輸此資料所訂合約所允許之範圍，並基於履行該合約之目的方可使用。除非本文另有規定，否則未經 NetApp Inc. 事前書面許可，不得逕行使用、揭露、重製、修改、履行或展示該資料。美國政府授予國防部之許可權利，僅適用於 DFARS 條款 252.227-7015(b)（2014 年 2 月）所述權利。

商標資訊

NETAPP、NETAPP 標誌及 <http://www.netapp.com/TM> 所列之標章均為 NetApp, Inc. 的商標。文中所涉及的所有其他公司或產品名稱，均為其各自所有者的商標，不得侵犯。