



# 开始使用私有模式

## Setup and administration

NetApp  
April 26, 2024

# 目录

- 开始使用私有模式..... 1
  - 入门工作流(私有模式) ..... 1
  - 准备在专用模式下部署..... 1
  - 在专用模式下部署连接器 ..... 14
  - 接下来可以执行的操作(专用模式) ..... 19

# 开始使用私有模式

## 入门工作流(私有模式)

通过准备您的环境并部署Connector、在私有模式下开始使用BlueXP。

私有模式通常用于无Internet连接的内部环境和安全云区域、其中包括 ["AWS机密云"](#)，["AWS云的绝密"](#)，和 ["Azure IL6"](#)

开始之前、您应了解 ["BlueXP帐户"](#)，["连接器"](#)，和 ["部署模式"](#)。

1

### "准备部署"

1. 准备一个满足CPU、RAM、磁盘空间、Docker引擎等要求的专用Linux主机。
2. 设置网络以访问目标网络。
3. 对于云部署、请在云提供商中设置权限、以便您可以在安装软件后将这些权限与Connector相关联。

2

### "部署连接器"

1. 在您自己的Linux主机上安装Connector软件。
2. 打开Web浏览器并输入Linux主机的IP地址、以设置BlueXP。
3. 对于云部署、为BlueXP提供您先前设置的权限。

## 准备在专用模式下部署

在私有模式下部署BlueXP之前、请准备好您的环境。例如、您需要查看主机要求、准备网络连接、设置权限等。



如果要在中使用BlueXP ["AWS机密云"](#) 或 ["AWS云的绝密"](#)然后，您应按照单独的说明开始使用这些环境。 ["了解如何在AWS机密云或Top SecretCloud中开始使用Cloud Volumes ONTAP"](#)

### 第1步：了解私有模式的工作原理

开始之前、您应了解BlueXP在专用模式下的工作原理。

例如、您应了解需要使用基于浏览器的界面、该界面可从需要安装的BlueXP Connector本地访问。您无法从通过SaaS层提供的基于Web的控制台访问BlueXP。

此外、并非所有BlueXP服务都可用。

["了解私有模式的工作原理"](#)。

## 第2步：查看安装选项

在私有模式下、您可以通过在自己的Linux主机上手动安装Connector在内部或云中安装Connector。

连接器的安装位置决定了在使用私有模式时哪些BlueXP服务和功能可用。例如、如果要部署和管理Cloud Volumes ONTAP、必须将连接器安装在云中。 ["了解有关私有模式的更多信息"](#)。

## 第3步：查看主机要求

连接器软件必须在满足特定操作系统要求， RAM 要求，端口要求等要求的主机上运行。

### 专用主机

与其他应用程序共享的主机不支持此连接器。主机必须是专用主机。

### 支持的操作系统

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

主机必须已注册到Red Hat订阅管理。如果未注册、则主机无法在安装Connector期间访问存储库以更新所需的第三方软件。

这些操作系统的英语版本支持 Connector 。

### 虚拟机管理程序

需要一个经过认证可运行Ubuntu、CentOS或Red Hat Enterprise Linux的裸机或托管虚拟机管理程序。

["Red Hat 解决方案：哪些虚拟机管理程序已通过认证，可以运行 Red Hat Enterprise Linux ? "](#)

### CPU

4 个核心或 4 个 vCPU

### RAM

14 GB

### AWS EC2 实例类型

满足上述 CPU 和 RAM 要求的实例类型。我们建议使用 T3.xlarge 。

### Azure 虚拟机大小

满足上述 CPU 和 RAM 要求的实例类型。我们建议使用 DS3 v2 。

### Google Cloud 计算机类型

满足上述 CPU 和 RAM 要求的实例类型。建议使用n2-standard-4。

在具有支持的操作系统的VM实例上、Google Cloud支持Connector ["屏蔽VM功能"](#)

### /opt 中的磁盘空间

必须有 100 GiB 的可用空间

**/var 中的磁盘空间**

必须有20 GiB的可用空间

**Docker 引擎**

在安装Connector之前、主机上需要Docker引擎。

- 支持的最低版本为9.3.1。
- 支持的最大版本为25.0.5。

["查看安装说明"](#)

**第4步：为连接器准备网络连接**

设置您的网络，以便 Connector 可以管理公有云环境中的资源和流程。除了为Connector提供虚拟网络和子网之外、您还需要确保满足以下要求。

**连接到目标网络**

Connector必须与您计划管理存储的位置建立网络连接。例如、您计划部署Cloud Volumes ONTAP 的VPC 或vNet、或者您的内部ONTAP 集群所在的数据中心。

**用于日常操作的端点**

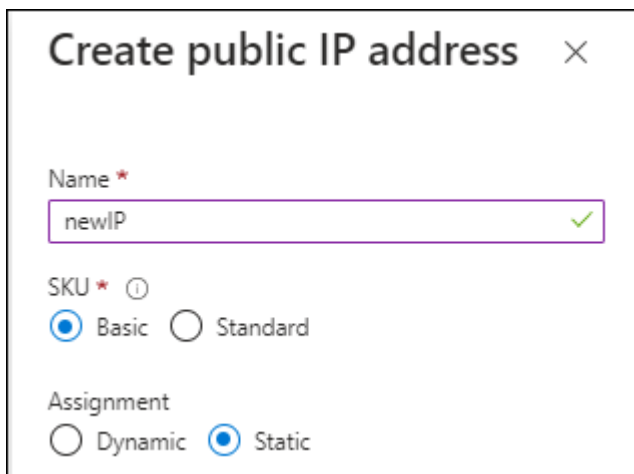
Connector会与以下端点联系、以管理公有云环境中的资源和流程。

端点	目的
<p>AWS 服务（ AmazonAWS.com ）：</p> <ul style="list-style-type: none"><li>• 云形成</li><li>• 弹性计算云（ EC2 ）</li><li>• 身份和访问管理(IAM)</li><li>• 密钥管理服务（ KMS ）</li><li>• 安全令牌服务（ STS ）</li><li>• 简单存储服务 (S3)</li></ul>	管理AWS中的资源。确切的端点取决于您使用的AWS区域。 <a href="#">"有关详细信息、请参见AWS文档"</a>
<p>https://management.azure.com https://login.microsoftonline.com https://blob.core.windows.net https://core.windows.net</p>	管理Azure公共区域中的资源。
<p>https://management.azure.microsoft.scloud https://login.microsoftonline.microsoft.scloud https://blob.core.microsoft.scloud https://core.microsoft.scloud</p>	管理Azure IL6区域中的资源。

端点	目的
<a href="https://management.chinacloudapi.cn">https://management.chinacloudapi.cn</a> <a href="https://login.chinacloudapi.cn">https://login.chinacloudapi.cn</a> <a href="https://blob.core.chinacloudapi.cn">https://blob.core.chinacloudapi.cn</a> <a href="https://core.chinacloudapi.cn">https://core.chinacloudapi.cn</a>	管理Azure中国地区的资源。
<a href="https://www.googleapis.com/compute/v1/">https://www.googleapis.com/compute/v1/</a> <a href="https://compute.googleapis.com/compute/v1">https://compute.googleapis.com/compute/v1</a> <a href="https://cloudresourcemanager.googleapis.com/v1/projects">https://cloudresourcemanager.googleapis.com/v1/projects</a> <a href="https://www.googleapis.com/compute/beta">https://www.googleapis.com/compute/beta</a> <a href="https://storage.googleapis.com/storage/v1">https://storage.googleapis.com/storage/v1</a> <a href="https://www.googleapis.com/storage/v1">https://www.googleapis.com/storage/v1</a> <a href="https://iam.googleapis.com/v1">https://iam.googleapis.com/v1</a> <a href="https://cloudkms.googleapis.com/v1">https://cloudkms.googleapis.com/v1</a> <a href="https://www.googleapis.com/deploymentmanager/v2/projects">https://www.googleapis.com/deploymentmanager/v2/projects</a>	在Google Cloud中管理资源。

### Azure中的公共IP地址

如果要对Azure中的Connector VM使用公共IP地址、则此IP地址必须使用基本SKU以确保BlueXP使用此公共IP地址。



**Create public IP address** ✕

Name \*  
 ✓

SKU \* ⓘ  
☒ Basic ☐ Standard

Assignment  
☐ Dynamic ☒ Static

如果改用标准SKU IP地址、则BlueXP将使用Connector的\_private\_ IP地址、而不是公共IP。如果用于访问BlueXP控制台的计算机无法访问该专用IP地址、则BlueXP控制台的操作将失败。

["Azure文档：公共IP SKU"](#)

### 代理服务器

如果您的组织需要为所有传出Internet流量部署代理服务器、请获取有关HTTP或HTTPS代理的以下信息。您需要在安装期间提供此信息。

- IP 地址
- 凭据
- HTTPS证书

请注意、BlueXP不支持透明代理服务器。

+

在私有模式下、BlueXP只会向云提供商发送出站流量、以便创建Cloud Volumes ONTAP 系统。

## 端口

除非您启动 Connector ，否则不会向其传入流量。

通过HTTP (80)和HTTPS (443)可以访问BlueXP控制台。只有在需要连接到主机进行故障排除时，才需要使用 SSH （ 22 ）。

## 启用NTP

如果您计划使用BlueXP分类来扫描公司数据源、则应在BlueXP Connector系统和BlueXP分类系统上启用网络时间协议(Network Time Protocol、NTP)服务、以便在系统之间同步时间。 ["了解有关BlueXP分类的更多信息"](#)

## 第5步：准备云权限

如果Connector安装在云中、而您计划创建Cloud Volumes ONTAP系统、则BlueXP需要云提供商的权限。您需要在云提供商中设置权限、然后在安装Connector实例后将这些权限与之关联。

要查看所需步骤、请选择要用于云提供商的身份验证选项。

## AWS IAM角色

使用IAM角色为Connector提供权限。您需要手动将角色附加到Connector的EC2实例。

### 步骤

1. 登录到AWS控制台并导航到IAM服务。
2. 创建策略：
  - a. 选择\*策略>创建策略\*。
  - b. 选择\*。JSON\*、然后复制并粘贴的内容 "[Connector的IAM策略](#)"。
  - c. 完成其余步骤以创建策略。
3. 创建IAM角色：
  - a. 选择\*角色>创建角色\*。
  - b. 选择\* AWS服务> EC2\*。
  - c. 通过附加刚刚创建的策略来添加权限。
  - d. 完成其余步骤以创建角色。

### 结果

现在、Connector EC2实例具有IAM角色。

## AWS访问密钥

为IAM用户设置权限和访问密钥。安装Connector并设置BlueXP后、您需要为BlueXP提供AWS访问密钥。

### 步骤

1. 登录到AWS控制台并导航到IAM服务。
2. 创建策略：
  - a. 选择\*策略>创建策略\*。
  - b. 选择\*。JSON\*、然后复制并粘贴的内容 "[Connector的IAM策略](#)"。
  - c. 完成其余步骤以创建策略。

根据您计划使用的BlueXP服务、您可能需要创建第二个策略。

对于标准区域、权限会分布在两个策略中。由于AWS中受管策略的字符大小上限、因此需要使用两个策略。 "[详细了解Connector的IAM策略](#)"。

3. 将策略附加到IAM用户。
  - "[AWS 文档：创建 IAM 角色](#)"
  - "[AWS 文档：添加和删除 IAM 策略](#)"
4. 确保用户具有可在安装Connector后添加到BlueXP的访问密钥。

### 结果

现在，此帐户具有所需权限。



## Azure角色

使用所需权限创建Azure自定义角色。您将为Connector VM分配此角色。

请注意、您可以使用Azure门户、Azure PowerShell、Azure命令行界面或REST API创建Azure自定义角色。以下步骤显示了如何使用Azure命令行界面创建角色。如果您希望使用其他方法、请参见 ["Azure 文档"](#)

### 步骤

1. 在计划安装Connector的虚拟机上启用系统分配的托管身份、以便您可以通过自定义角色提供所需的Azure权限。

["Microsoft Azure文档：使用Azure门户为虚拟机上的Azure资源配置托管身份"](#)

2. 复制的内容 ["Connector的自定义角色权限"](#) 并将其保存在JSON文件中。
3. 通过将 Azure 订阅 ID 添加到可分配范围来修改 JSON 文件。

您应添加要用于BlueXP的每个Azure订阅的ID。

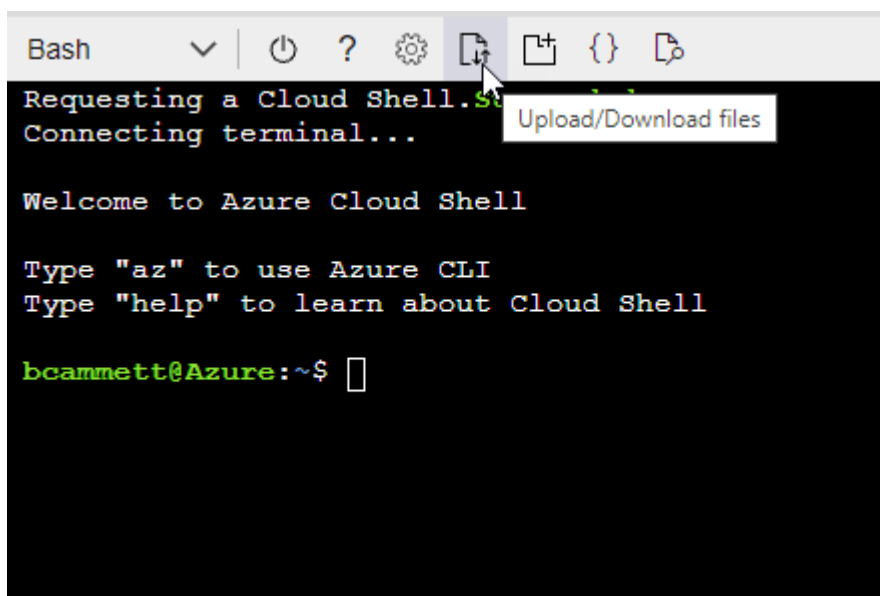
◦ 示例 \*

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

4. 使用 JSON 文件在 Azure 中创建自定义角色。

以下步骤介绍如何在 Azure Cloud Shell 中使用 Bash 创建角色。

- a. start ["Azure Cloud Shell"](#) 并选择 Bash 环境。
- b. 上传 JSON 文件。



c. 使用Azure命令行界面创建自定义角色：

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

结果

现在、您应该拥有一个名为BlueXP操作员的自定义角色、可以将该角色分配给Connector虚拟机。

**Azure服务主体**

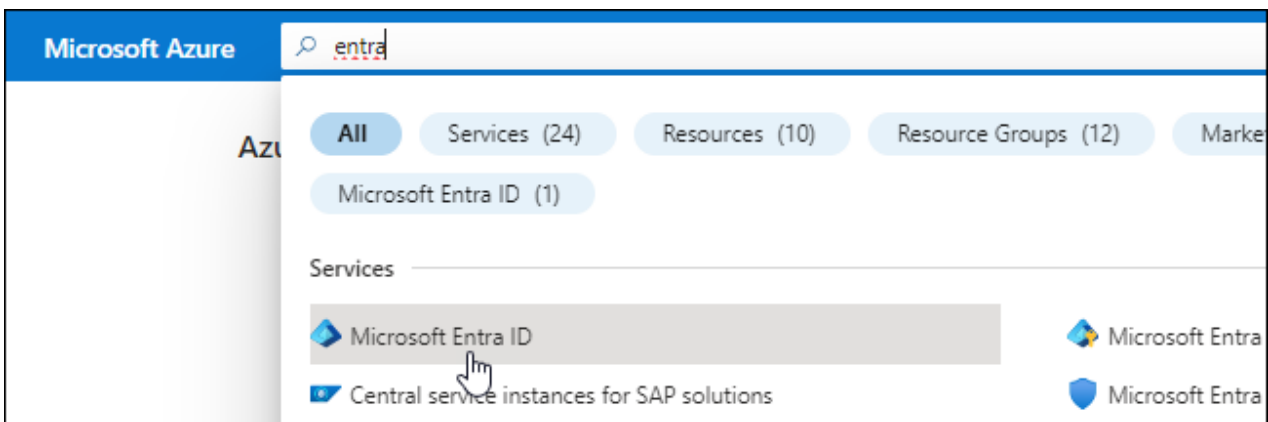
在Microsoft Entra ID中创建和设置服务主体、并获取BlueXP所需的Azure凭据。安装Connector并设置BlueXP后、您需要为BlueXP提供这些凭据。

创建**Microsoft Entra**应用程序以实现基于角色的访问控制

1. 确保您在Azure中拥有创建Active Directory应用程序和将应用程序分配给角色的权限。

有关详细信息，请参见 "[Microsoft Azure 文档：所需权限](#)"

2. 从Azure门户中，打开\*Microsoft Entra ID\*服务。



3. 在菜单中、选择\*应用程序注册\*。
4. 选择\*新建注册\*。
5. 指定有关应用程序的详细信息：
  - \* 名称 \*：输入应用程序的名称。
  - 帐户类型：选择帐户类型(任何将适用于BlueXP)。
  - \* 重定向 URI\*：可以将此字段留空。
6. 选择 \* 注册 \*。

您已创建 AD 应用程序和服务主体。

将应用程序分配给角色

1. 创建自定义角色：

请注意、您可以使用Azure门户、Azure PowerShell、Azure命令行界面或REST API创建Azure自定义角色。以下步骤显示了如何使用Azure命令行界面创建角色。如果您希望使用其他方法、请参见 "[Azure](#)

## 文档"

- 复制的内容 "[Connector的自定义角色权限](#)" 并将其保存在JSON文件中。
- 通过将 Azure 订阅 ID 添加到可分配范围来修改 JSON 文件。

您应该为每个 Azure 订阅添加 ID、用户将从中创建 Cloud Volumes ONTAP 系统。

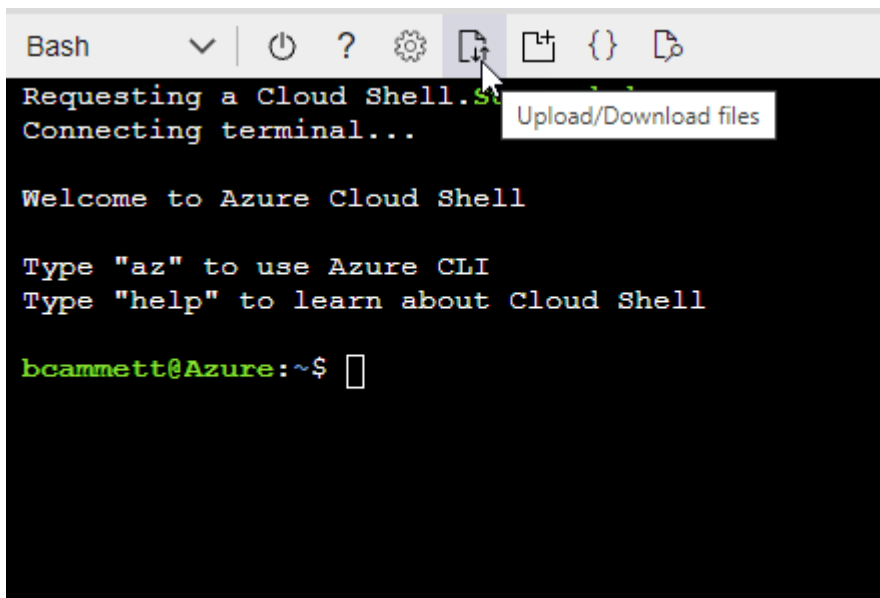
### ▪ 示例 \*

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

- 使用 JSON 文件在 Azure 中创建自定义角色。

以下步骤介绍如何在 Azure Cloud Shell 中使用 Bash 创建角色。

- start "[Azure Cloud Shell](#)" 并选择 Bash 环境。
- 上传 JSON 文件。



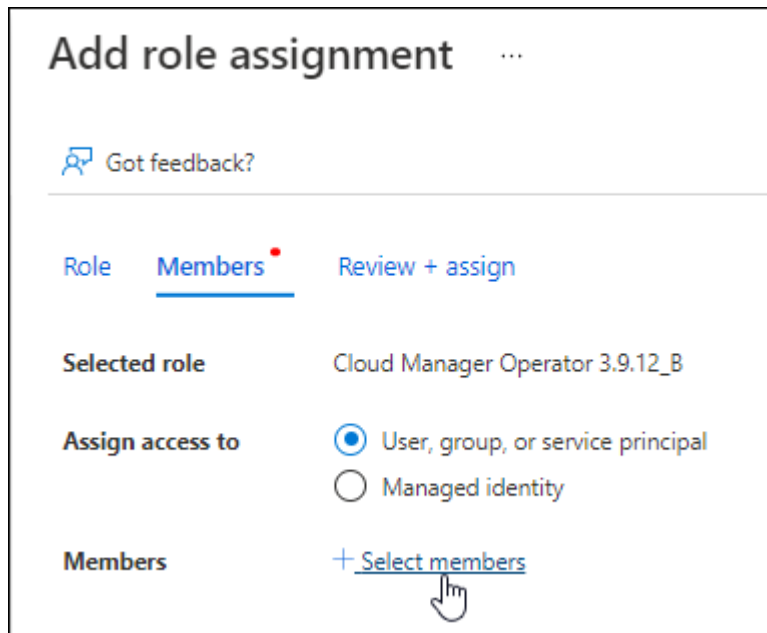
- 使用Azure命令行界面创建自定义角色：

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

现在、您应该拥有一个名为BlueXP操作员的自定义角色、可以将该角色分配给Connector虚拟机。

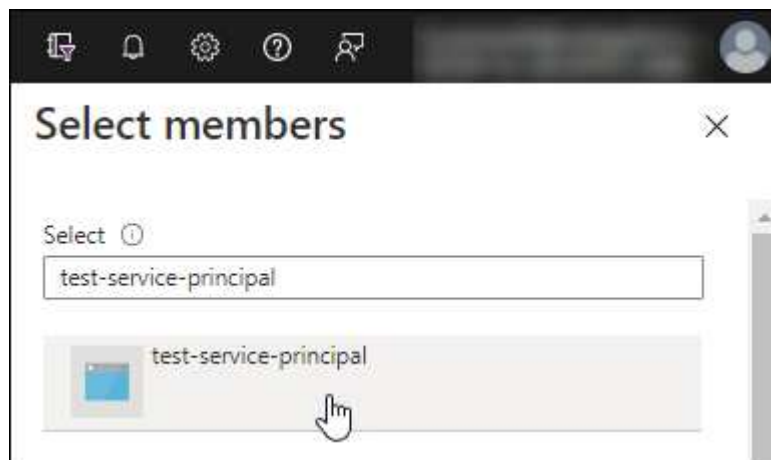
## 2. 将应用程序分配给角色：

- a. 从 Azure 门户中，打开 \* 订阅 \* 服务。
- b. 选择订阅。
- c. 选择\*访问控制(IAM)>添加>添加角色分配\*。
- d. 在\*角色\*选项卡中、选择\* BlueXP操作员\*角色、然后选择\*下一步\*。
- e. 在 \* 成员 \* 选项卡中，完成以下步骤：
  - 保持选中 \* 用户，组或服务主体 \*。
  - 选择\*选择成员\*。



- 搜索应用程序的名称。

以下是一个示例：



- 选择应用程序并选择\*选择\*。
  - 选择 \* 下一步 \*。
- f. 选择\*审核+分配\*。

现在，服务主体具有部署 Connector 所需的 Azure 权限。

如果要从多个 Azure 订阅部署 Cloud Volumes ONTAP，则必须将服务主体绑定到每个订阅。通过 BlueXP，您可以选择要在部署 Cloud Volumes ONTAP 时使用的订阅。

#### 添加 Windows Azure 服务管理 API 权限

1. 在 \*Microsoft Entra ID\* 服务中，选择 \*App Registrations\* 并选择应用程序。
2. 选择 \*API 权限 > 添加权限\*。
3. 在 \*Microsoft APIs\* 下，选择 \*Azure Service Management\*。













### 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.

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

4. 选择 \*以组织用户身份访问 Azure 服务管理\*，然后选择 \*添加权限\*。

## 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

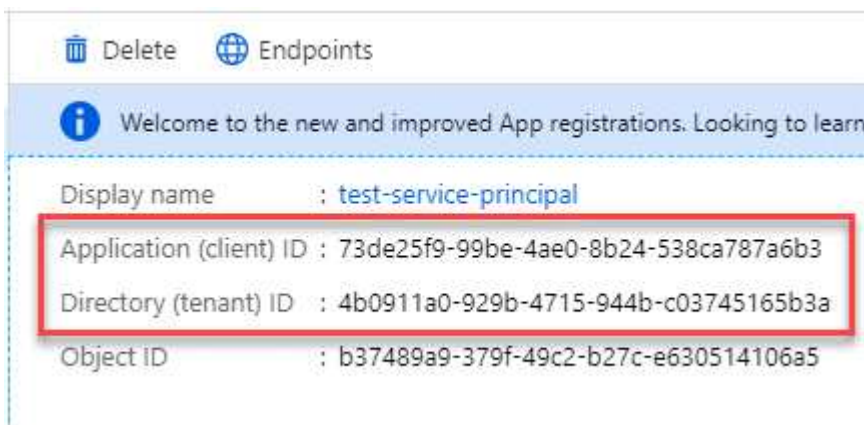


user\_impersonation

Access Azure Service Management as organization users (preview)

获取应用程序的应用程序ID和目录ID

1. 在\*Microsoft Entra ID\*服务中，选择\*App Registrations\*并选择应用程序。
2. 复制 \* 应用程序（客户端） ID\* 和 \* 目录（租户） ID\*。



将Azure帐户添加到BlueXP时、您需要提供应用程序(客户端) ID和目录(租户) ID。BlueXP使用ID以编程方式登录。

创建客户端密钥

1. 打开\*Microsoft Entra ID\*服务。
2. 选择\*应用程序注册\*并选择您的应用程序。
3. 选择\*证书和机密>新客户端机密\*。
4. 提供密钥和持续时间的问题描述。
5. 选择 \* 添加 \*。
6. 复制客户端密钥的值。

## 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.

<a href="#">+ New client secret</a>		
DESCRIPTION	EXPIRES	VALUE
test secret	8/16/2020	*sZ1jSe2By:D*-ZRoV4NLfdAcY7:+0vA

Copy to clipboard

现在、您有了一个客户端密钥、BlueXP可以使用它通过Microsoft Entra ID进行身份验证。

## 结果

此时，您的服务主体已设置完毕，您应已复制应用程序（客户端）ID，目录（租户）ID 和客户端密钥值。添加Azure帐户时、您需要在BlueXP中输入此信息。

## Google Cloud服务帐户

创建一个角色并将其应用于要用于Connector VM实例的服务帐户。

## 步骤

1. 在Google Cloud中创建自定义角色：
  - a. 创建包含中定义的权限的YAML文件 ["适用于Google Cloud的连接策略"](#)。
  - b. 从Google Cloud激活Cloud Shell。
  - c. 上传包含Connector所需权限的YAML文件。
  - d. 使用创建自定义角色 `gcloud iam roles create` 命令：

以下示例将在项目级别创建一个名为"connector"的角色：

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

+

["Google Cloud文档：创建和管理自定义角色"](#)

2. 在Google Cloud中创建服务帐户：
  - a. 从IAM和Admin服务中，选择\*服务帐户>创建服务帐户\*。
  - b. 输入服务帐户详细信息，然后选择\*创建并继续\*。
  - c. 选择刚刚创建的角色。
  - d. 完成其余步骤以创建角色。

["Google Cloud文档：创建服务帐户"](#)

## 结果

现在、您可以为Connector VM实例分配一个服务帐户。

## 第6步：启用Google Cloud API

要在Google Cloud中部署Cloud Volumes ONTAP、需要使用多个API。

### 步骤

#### 1. "在项目中启用以下 Google Cloud API"

- Cloud Deployment Manager V2 API
- 云日志记录 API
- Cloud Resource Manager API
- 计算引擎 API
- 身份和访问管理（IAM）API
- 云密钥管理服务(KMS) API

(仅当您计划将BlueXP备份和恢复与客户管理的加密密钥(CMDK)结合使用时才需要)

## 在专用模式下部署连接器

在私有模式下部署Connector、以便在使用BlueXP时无需与BlueXP SaaS层建立出站连接。要开始使用、请安装Connector、通过访问Connector上运行的用户界面来设置BlueXP、然后提供您先前设置的云权限。

### 步骤1：安装连接器

从NetApp 支持站点 下载产品安装程序、然后在您自己的Linux主机上手动安装连接器。

如果要在中使用BlueXP "AWS机密云" 或 "AWS云的绝密"然后，您应按照单独的说明开始使用这些环境。 [了解如何在AWS机密云或Top SecretCloud中开始使用Cloud Volumes ONTAP](#)

#### 开始之前

安装连接器需要 root 权限。

#### 步骤

1. 验证 Docker 是否已启用且正在运行。

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

2. 从下载Connector软件 ["NetApp 支持站点"](#)

请务必为无法访问Internet的专用网络下载脱机安装程序。

3. 将安装程序复制到 Linux 主机。
4. 分配运行脚本的权限。



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

其中、<version> 是您下载的连接器版本。

#### 5. 运行安装脚本：

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

其中、<version> 是您下载的连接器版本。

#### 结果

已安装Connector软件。现在、您可以设置BlueXP。

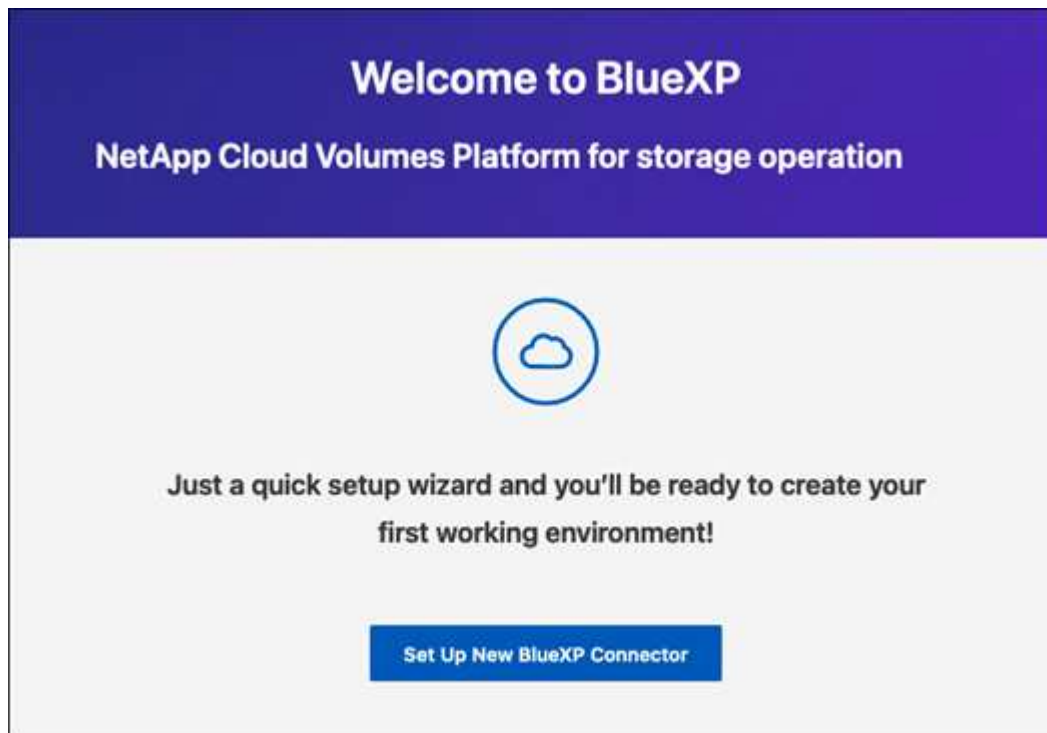
## 第2步：设置BlueXP

首次访问BlueXP控制台时、系统将提示您设置BlueXP。

#### 步骤

1. 打开 Web 浏览器并输入 <https://<em>ipaddress</em>> 其中\_ipaddress\_是安装了连接器的Linux主机的IP地址。

您应看到以下屏幕。



2. 选择\*设置新BlueXP Connector\*并按照提示设置系统。
  - 系统详细信息：输入Connector的名称和公司名称。

1 System Details   2 Create Admin User   3 Review

### System Details

To help us provide better support, enter a name for BlueXP Connector and your company name.

BlueXP Connector Name

Company Name

- 创建管理员用户：创建系统的管理员用户。

此用户帐户在系统本地运行。无法通过BlueXP连接到可用的auth0服务。

- \*Review\*：查看详细信息，接受许可协议，然后选择\*Set Up\*。

3. 使用刚刚创建的管理员用户登录到BlueXP。

结果

现在，已安装并设置 Connector 。

如果有新版本的 Connector 软件可用，则这些软件将发布到 NetApp 支持站点。 ["了解如何升级 Connector"](#)。

下一步是什么？

为BlueXP提供您先前设置的权限。

### 第3步：为BlueXP提供权限

如果要创建Cloud Volumes ONTAP 工作环境、您需要为BlueXP提供先前设置的云权限。

["了解如何准备云权限"](#)。

## AWS IAM角色

将先前创建的IAM角色附加到Connector EC2实例。

### 步骤

1. 转到Amazon EC2控制台。
2. 选择\*实例\*。
3. 选择Connector实例。
4. 选择\*操作>安全性>修改IAM角色\*。
5. 选择IAM角色并选择\*更新IAM角色\*。

### 结果

现在、BlueXP拥有代表您在AWS中执行操作所需的权限。

## AWS访问密钥

为BlueXP提供具有所需权限的IAM用户的AWS访问密钥。

### 步骤

1. 在BlueXP控制台的右上角、选择设置图标、然后选择\*凭据\*。



2. 选择\*添加凭据\*并按照向导中的步骤进行操作。
  - a. \*凭据位置\*：选择 \* Amazon Web Services > Connector\*。
  - b. 定义凭据：输入AWS访问密钥和机密密钥。
  - c. \*市场订阅\*：通过立即订阅或选择现有订阅，将市场订阅与这些凭据相关联。
  - d. 查看：确认有关新凭据的详细信息、然后选择\*添加\*。

### 结果

现在、BlueXP拥有代表您在AWS中执行操作所需的权限。

## Azure角色

转到Azure门户、为一个或多个订阅向Connector虚拟机分配Azure自定义角色。

### 步骤

1. 从Azure门户中、打开\*订阅\*服务并选择您的订阅。

请务必从\*订阅\*服务中分配角色，因为这会指定订阅级别的角色分配范围。范围定义了适用场景访问的一组资源。如果在其他级别(例如、在虚拟机级别)指定范围、则从BlueXP中完成操作的能力将受到影响。

["Microsoft Azure文档：了解Azure RBAC的范围"](#)

2. 选择\*访问控制(IA)>\*添加>\*添加角色指派\*。
3. 在\*角色\*选项卡中、选择\* BlueXP操作员\*角色、然后选择\*下一步\*。



BlueXP操作员是BlueXP策略中提供的默认名称。如果您为角色选择了其他名称，请选择该名称。

4. 在 \* 成员 \* 选项卡中，完成以下步骤：
  - a. 为 \* 受管身份 \* 分配访问权限。
  - b. 选择\*选择成员\*，选择创建连接器虚拟机时使用的订阅，在\*受管身份\*下选择\*虚拟机\*，然后选择连接器虚拟机。
  - c. 选择\*选择\*。
  - d. 选择 \* 下一步 \*。
  - e. 选择\*审核+分配\*。
  - f. 如果要管理其他Azure订阅中的资源、请切换到该订阅、然后重复这些步骤。

#### 结果

现在、BlueXP拥有代表您在Azure中执行操作所需的权限。

#### Azure服务主体

为BlueXP提供您先前设置的Azure服务主体的凭据。

#### 步骤

1. 在BlueXP控制台的右上角、选择设置图标、然后选择\*凭据\*。



2. 选择\*添加凭据\*并按照向导中的步骤进行操作。
  - a. \* 凭据位置 \*：选择 \* Microsoft Azure > Connector\* 。
  - b. 定义凭据：输入有关授予所需权限的Microsoft Entra服务主体的信息：
    - 应用程序(客户端) ID
    - 目录(租户) ID
    - 客户端密钥
  - c. \* 市场订阅 \*：通过立即订阅或选择现有订阅，将市场订阅与这些凭据相关联。
  - d. 查看：确认有关新凭据的详细信息、然后选择\*添加\*。

#### 结果

现在、BlueXP拥有代表您在Azure中执行操作所需的权限。

#### Google Cloud服务帐户

将服务帐户与Connector VM关联。

#### 步骤

1. 转到Google Cloud门户、并将服务帐户分配给Connector VM实例。

["Google Cloud文档：更改实例的服务帐户和访问范围"](#)

2. 如果要管理其他项目中的资源、请通过向该项目添加具有BlueXP角色的服务帐户来授予访问权限。您需要对每个项目重复此步骤。

#### 结果

现在、BlueXP拥有代表您在Google Cloud中执行操作所需的权限。

## 接下来可以执行的操作(专用模式)

在专用模式下启动和运行BlueXP后、您可以开始使用私有模式支持的BlueXP服务。

要获得帮助、请参见以下文档：

- ["创建Cloud Volumes ONTAP 系统"](#)
- ["发现内部ONTAP 集群"](#)
- ["复制数据"](#)
- ["使用BlueXP分类扫描内置ONTAP 卷数据"](#)
- ["使用BlueXP备份和恢复将ONTAP 卷数据备份到StorageGRID"](#)

#### 相关链接

["BlueXP部署模式"](#)

## 版权信息

版权所有 © 2024 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本文档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

## 商标信息

NetApp、NetApp 标识和 <http://www.netapp.com/TM> 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。