在本地安装代理

NetApp Console setup and administration

NetApp
February 11, 2026

目录

在本地安装代理

在本地手动安装控制台代理

在本地安装控制台代理，然后登录并设置它以与您的控制台组织协同工作。

如果您是 VMWare 用户，您可以使用 OVA 在您的 VCenter 中安装控制台代理。"了解有关在 VCenter 中安装代理的更多信息。"

在安装之前，您需要确保您的主机（VM 或 Linux 主机）满足要求，并确保控制台代理可以访问互联网以及目标网络。如果您计划使用NetApp数据服务或云存储选项（例如Cloud Volumes ONTAP），则需要在云提供商中创建凭据以添加到控制台，以便控制台代理可以代表您在云中执行操作。

准备安装控制台代理

在安装控制台代理之前，您应该确保您拥有一台满足安装要求的主机。您还需要与网络管理员合作，以确保控制台代理具有对所需端点的出站访问权限以及与目标网络的连接。

查看控制台代理主机要求

在满足操作系统、RAM 和端口要求的 x86 主机上运行控制台代理。在安装控制台代理之前，请确保您的主机满足这些要求。

控制台代理保留 19000 到 19200 的 UID 和 GID 范围。这个范围是固定的，不能修改。如果主机上的任何第三方软件使用此范围内的 UID 或 GID，则代理安装将失败。 NetApp建议使用没有第三方软件的主机以避免冲突。

专用主机

控制台代理需要专用主机。只要满足以下尺寸要求，任何架构都受支持：

- CPU：8 核或 8 个 vCPU
- 内存：32 GB
- 磁盘空间：建议主机预留165GB空间，分区要求如下：
  - `/opt`：必须有 120 GiB 可用空间

    代理使用 `/opt`安装 `/opt/application/netapp`目录及其内容。

  - `/var`：必须有 40 GiB 可用空间

    控制台代理需要此空间 `/var`因为 Podman 或 Docker 的设计初衷就是在这个目录下创建容器。具体来说，他们将在以下位置创建容器： `/var/lib/containers/storage`目录和 `/var/lib/docker`用于 Docker。外部安装或符号链接不适用于此空间。

虚拟机管理程序

需要经过认证可运行受支持的操作系统的裸机或托管虚拟机管理程序。

操作系统和容器要求

在标准模式或受限模式下使用控制台时，控制台代理支持以下操作系统。安装代理之前需要一个容器编排工具。

操作系统	支持的操作系统版本	支持的代理版本	所需的容器工具	SELinux
Red Hat Enterprise Linux		9.6 • 仅限英语版本。 • 主机必须在 Red Hat 订阅管理中注册。如果未注册，主机将无法在代理安装期间访问存储库来更新所需的第三方软件。	4.0.0 或更高版本，控制台处于标准模式或受限模式	Podman 版本 5.4.0，podman-compose 版本 1.5.0。 查看 Podman 配置要求 。
在强制模式或宽容模式下受支持		9.1 至 9.4 • 仅限英语版本。 • 主机必须在 Red Hat 订阅管理中注册。如果未注册，主机将无法在代理安装期间访问存储库来更新所需的第三方软件。	3.9.50 或更高版本，控制台处于标准模式或受限模式	Podman 版本 4.9.4，podman-compose 版本 1.5.0。 查看 Podman 配置要求 。
在强制模式或宽容模式下受支持		8.6 至 8.10 • 仅限英语版本。 • 主机必须在 Red Hat 订阅管理中注册。如果未注册，主机将无法在代理安装期间访问存储库来更新所需的第三方软件。	3.9.50 或更高版本，控制台处于标准模式或受限模式	Podman 版本 4.6.1 或 4.9.4，搭配 podman-compose 1.0.6。 查看 Podman 配置要求 。
在强制模式或宽容模式下受支持	Ubuntu		24.04 LTS	3.9.45 或更高版本，NetApp Console处于标准模式或受限模式
Docker Engine 23.06 至 28.0.0。	不支持		22.04 LTS	3.9.50 或更高版本

为控制台代理设置网络访问

设置网络访问以确保控制台代理可以管理资源。它需要连接到目标网络并访问特定端点的出站互联网。

连接到目标网络

控制台代理需要与您计划创建和管理系统的位置建立网络连接。例如，您计划在本地环境中创建Cloud Volumes ONTAP系统或存储系统的网络。

出站互联网访问

部署控制台代理的网络位置必须具有出站互联网连接才能联系特定端点。

使用基于 **Web** 的**NetApp Console**时从计算机联系的端点

从 Web 浏览器访问控制台的计算机必须能够联系多个端点。您需要使用控制台来设置控制台代理并进行控制台的日常使用。

"为NetApp控制台准备网络" 。

从控制台代理联系的端点

控制台代理需要出站互联网访问来联系以下端点，以管理公共云环境中的资源和流程以进行日常操作。

下面列出的端点都是 CNAME 条目。

安装在您场所的控制台代理无法管理 Google Cloud 中的资源。如果您想管理 Google Cloud 资源，则需要在 Google Cloud 中安装代理。

AWS

当控制台代理安装在本地时，它需要对以下 AWS 端点进行网络访问，以便管理部署在 AWS 中的NetApp 系统（例如Cloud Volumes ONTAP）。

从控制台代理联系的端点

控制台代理需要出站互联网访问来联系以下端点，以管理公共云环境中的资源和流程以进行日常操作。

下面列出的端点都是 CNAME 条目。

端点	目的
AWS 服务（amazonaws.com）： • 云形成 • 弹性计算云（EC2） • 身份和访问管理 (IAM) • 密钥管理服务（KMS） • 安全令牌服务 (STS) • 简单存储服务（S3）	管理 AWS 资源。端点取决于您的 AWS 区域。 "有关详细信息，请参阅 AWS 文档"
Amazon FsX for NetApp ONTAP： • api.workloads.netapp.com	基于 Web 的控制台通过与 Workload Factory API 交互来管理和操作基于ONTAP 的FSx 工作负载。
\ https://mysupport.netapp.com	获取许可信息并向NetApp支持发送AutoSupport消息。
\ https://signin.b2c.netapp.com	更新NetApp支持站点 (NSS) 凭据或将新的 NSS 凭据添加到NetApp Console。
\ https://support.netapp.com	获取许可信息并向NetApp支持发送AutoSupport消息以及接收Cloud Volumes ONTAP的软件更新。
\ https://api.bluexp.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com \ https://console.netapp.com \ https://components.console.bluexp.netapp.com \ https://cdn.auth0.com	在NetApp Console中提供功能和服务。

端点	目的
\ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://bluexpinfraprod.azurecr.io	获取控制台代理升级的图像。 • 当您部署新代理时，验证检查会测试与当前端点的连接。如果你使用"先前的端点"，验证检查失败。为了避免此失败，请跳过验证检查。 尽管以前的端点仍然受支持，但NetApp建议尽快将防火墙规则更新到当前端点。"了解如何更新终端节点列表" 。 • 当您更新到防火墙中的当前端点时，您现有的代理将继续工作。

Azure

当控制台代理安装在本地时，它需要对以下 Azure 端点进行网络访问，以便管理部署在 Azure 中的NetApp系统（例如Cloud Volumes ONTAP）。

端点	目的
\ https://management.azure.com \ https://login.microsoftonline.com \ https://blob.core.windows.net \ https://core.windows.net	管理 Azure 公共区域中的资源。
\ https://management.chinacloudapi.cn \ https://login.chinacloudapi.cn \ https://blob.core.chinacloudapi.cn \ https://core.chinacloudapi.cn	管理 Azure 中国区域的资源。
\ https://mysupport.netapp.com	获取许可信息并向NetApp支持发送AutoSupport消息。
\ https://signin.b2c.netapp.com	更新NetApp支持站点 (NSS) 凭据或将新的 NSS 凭据添加到NetApp Console。
\ https://support.netapp.com	获取许可信息并向NetApp支持发送AutoSupport消息以及接收Cloud Volumes ONTAP的软件更新。
\ https://api.bluexp.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com \ https://console.netapp.com \ https://components.console.bluexp.netapp.com \ https://cdn.auth0.com	在NetApp Console中提供功能和服务。

端点	目的
\ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://bluexpinfraprod.azurecr.io	获取控制台代理升级的图像。 • 当您部署新代理时，验证检查会测试与当前端点的连接。如果你使用"先前的端点"，验证检查失败。为了避免此失败，请跳过验证检查。 尽管以前的端点仍然受支持，但NetApp建议尽快将防火墙规则更新到当前端点。"了解如何更新终端节点列表" 。 • 当您更新到防火墙中的当前端点时，您现有的代理将继续工作。

代理服务器

NetApp支持显式和透明代理配置。如果您使用透明代理，则只需要提供代理服务器的证书。如果您使用显式代理，您还需要 IP 地址和凭据。

- IP 地址
- 凭据
- HTTPS 证书

端口

除非您启动它或将其用作代理将AutoSupport消息从Cloud Volumes ONTAP发送到NetApp支持，否则控制台代理不会有传入流量。

- HTTP（80）和 HTTPS（443）提供对本地 UI 的访问，您会在极少数情况下使用它们。
- 仅当需要连接到主机进行故障排除时才需要 SSH（22）。
- 如果您在没有出站互联网连接的子网中部署Cloud Volumes ONTAP系统，则需要通过端口 3128 建立入站连接。

  如果Cloud Volumes ONTAP系统没有出站互联网连接来发送AutoSupport消息，控制台会自动配置这些系统以使用控制台代理附带的代理服务器。唯一的要求是确保控制台代理的安全组允许通过端口 3128 进行入站连接。部署控制台代理后，您需要打开此端口。

启用 **NTP**

如果您计划使用NetApp Data Classification来扫描公司数据源，则应在控制台代理和NetApp Data Classification系统上启用网络时间协议 (NTP) 服务，以便系统之间的时间同步。 "了解有关NetApp数据分类的更多信息"

为 **AWS** 或 **Azure** 创建控制台代理云权限

如果您想通过本地控制台代理使用 AWS 或 Azure 中的NetApp数据服务，则需要在云提供商中设置权限，然后

在安装控制台代理后将凭据添加到控制台代理。

您必须在 Google Cloud 中安装控制台代理来管理驻留在那里的任何资源。

AWS

当控制台代理安装在本地时，您需要通过为具有所需权限的 IAM 用户添加访问密钥来为控制台提供 AWS 权限。

如果控制台代理安装在本地，则必须使用此身份验证方法。您不能使用 IAM 角色。

步骤

1. 登录 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** 并复制并粘贴内容"控制台代理的 IAM 策略"。

    c. 完成剩余步骤以创建策略。

    根据您计划使用的NetApp数据服务，您可能需要创建第二个策略。

    对于标准区域，权限分布在两个策略中。由于 AWS 中托管策略的最大字符大小限制，因此需要两个策略。"了解有关控制台代理的 IAM 策略的更多信息" 。

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. 确保用户拥有访问密钥，您可以在安装控制台代理后将其添加到NetApp Console。

结果

您现在应该拥有具有所需权限的 IAM 用户的访问密钥。安装控制台代理后，从控制台将这些凭据与控制台代理关联。

Azure

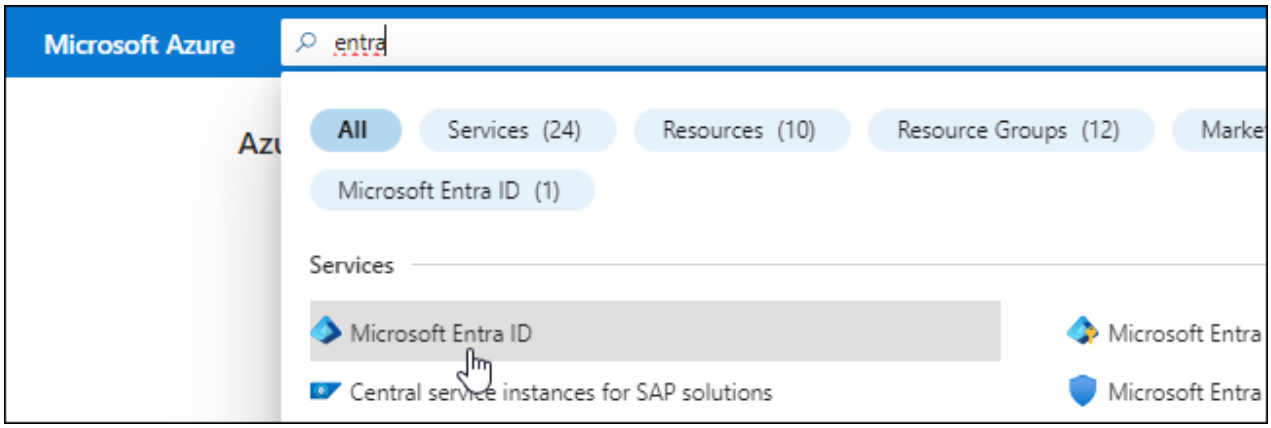
当控制台代理安装在本地时，您需要通过在 Microsoft Entra ID 中设置服务主体并获取控制台代理所需的 Azure 凭据来为控制台代理提供 Azure 权限。

创建用于基于角色的访问控制的 **Microsoft Entra** 应用程序

1. 确保您在 Azure 中拥有创建 Active Directory 应用程序并将该应用程序分配给角色的权限。

    有关详细信息，请参阅 "Microsoft Azure 文档：所需权限"

2. 从 Azure 门户打开 **Microsoft Entra ID** 服务。



3. 在菜单中，选择*应用程序注册*。
4. 选择*新注册*。
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（任何类型都可以与NetApp Console一起使用）。
   - 重定向 **URI**：您可以将此字段留空。
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 CLI 或 REST API 创建 Azure 自定义角色。以下步骤展示如何使用 Azure CLI 创建角色。如果您希望使用其他方法，请参阅 "Azure 文档"

   a. 复制"控制台代理的自定义角色权限"并将它们保存在 JSON 文件中。

   b. 通过将 Azure 订阅 ID 添加到可分配范围来修改 JSON 文件。

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

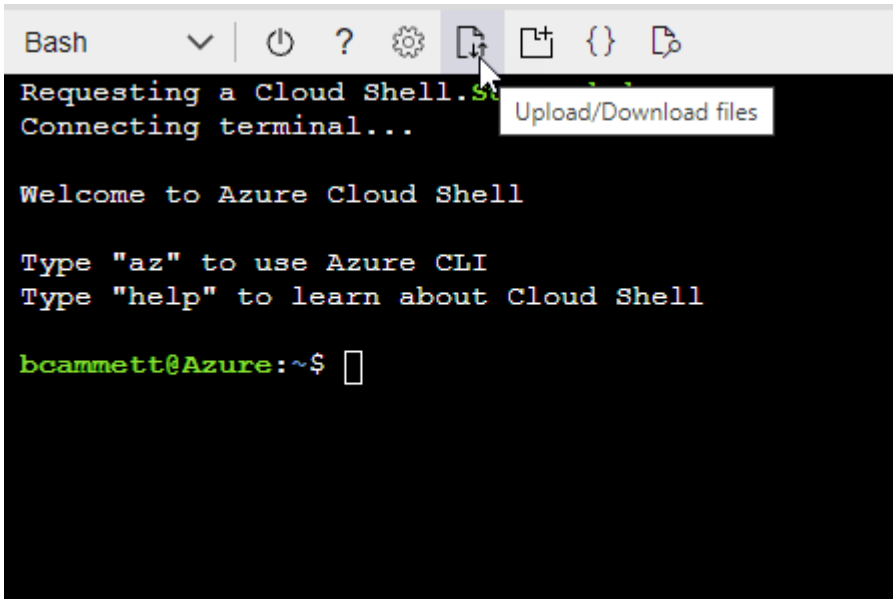
      例子

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

   c. 使用 JSON 文件在 Azure 中创建自定义角色。

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

- 开始 "Azure 云外壳"并选择 Bash 环境。
- 上传 JSON 文件。



- 使用 Azure CLI 创建自定义角色：

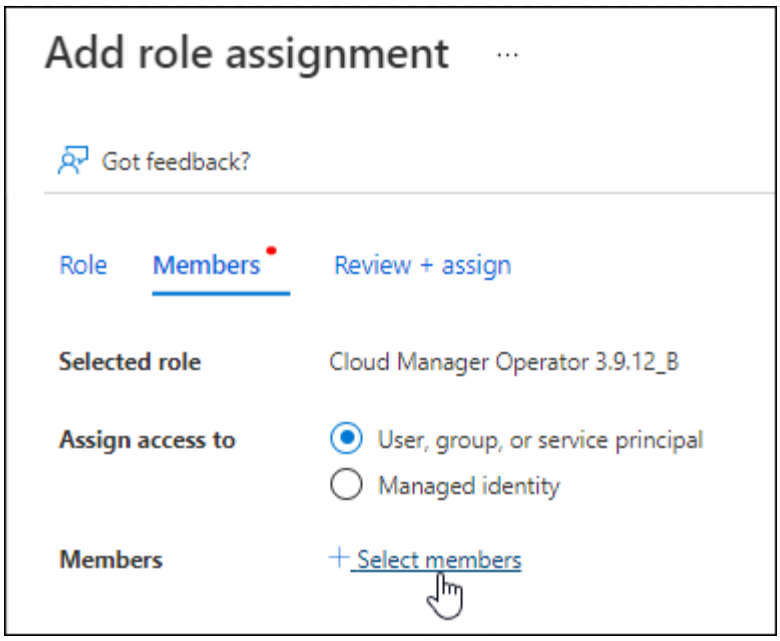
```
az role definition create --role-definition agent_Policy.json
```

现在您应该有一个名为“控制台操作员”的自定义角色，可以将其分配给控制台代理虚拟机。

2. 将应用程序分配给角色：

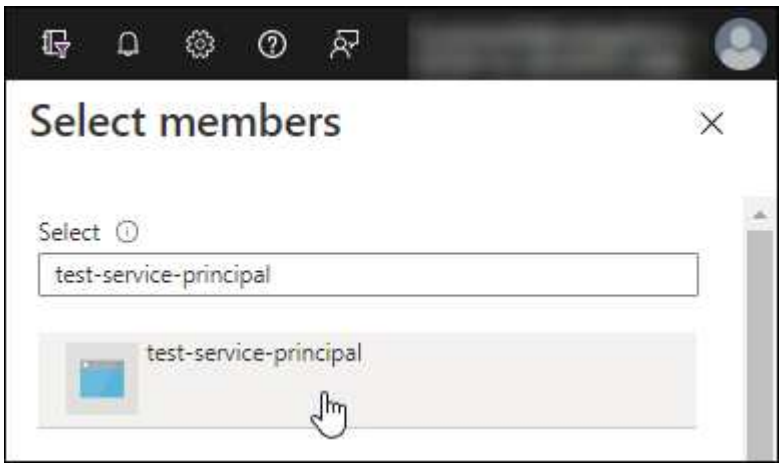
a. 从 Azure 门户打开 **Subscriptions** 服务。
b. 选择订阅。
c. 选择“访问控制 (IAM)”>“添加”>“添加角色分配”。
d. 在*角色*选项卡中，选择*控制台操作员*角色并选择*下一步*。
e. 在“成员”选项卡中，完成以下步骤：

- 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。

  以下是一个例子：



- 选择应用程序并选择*选择*。
- 选择“下一步”。

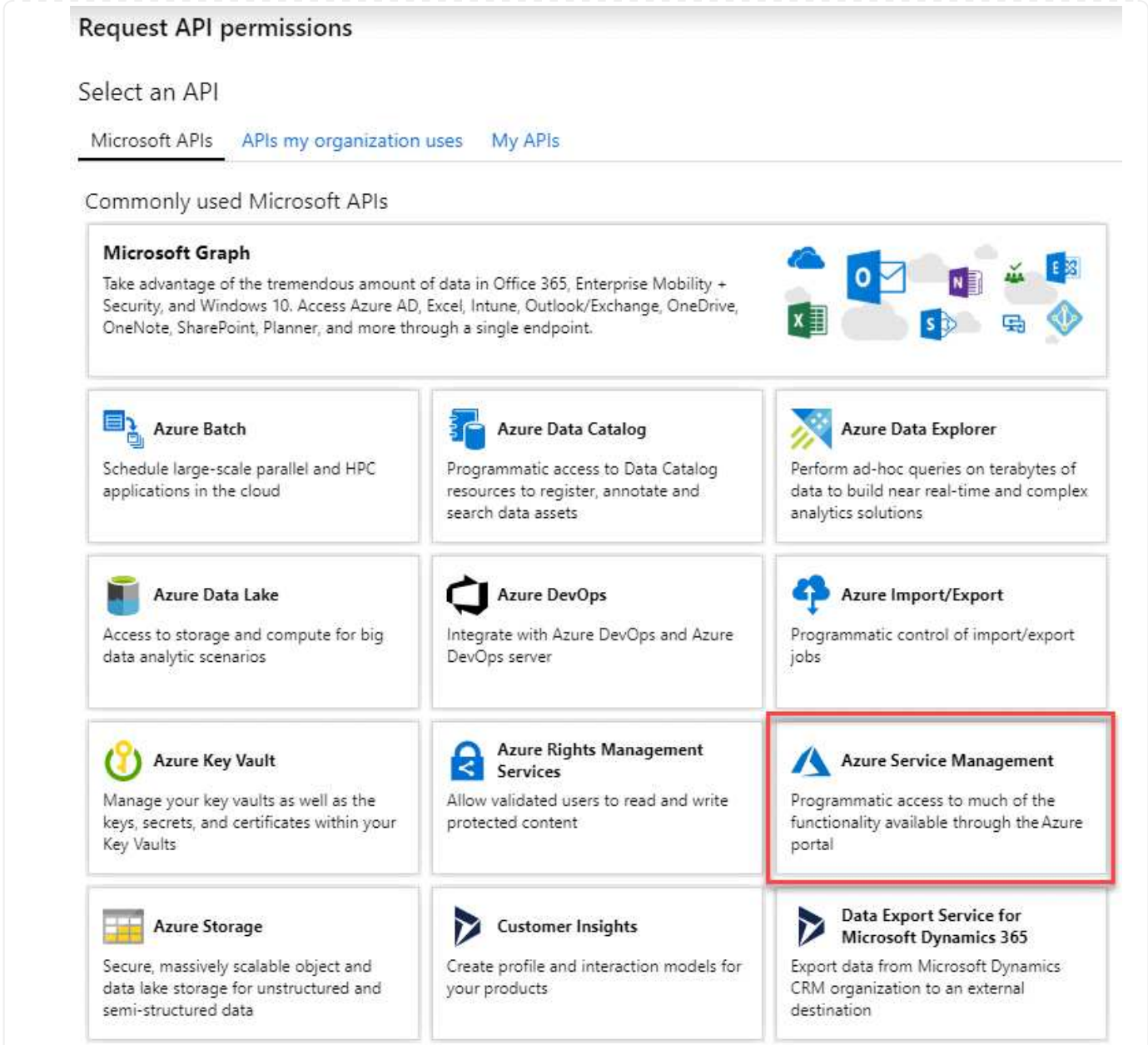
f. 选择*审阅+分配*。

服务主体现在具有部署控制台代理所需的 Azure 权限。

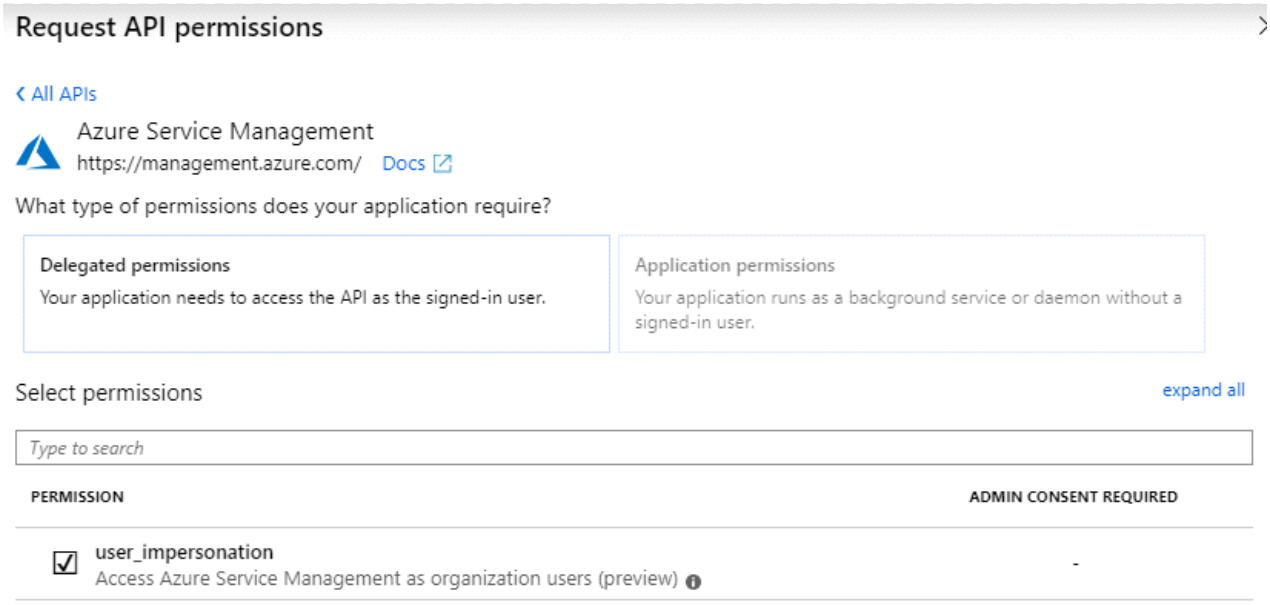
如果您想从多个 Azure 订阅部署Cloud Volumes ONTAP ，则必须将服务主体绑定到每个订阅。在NetApp Console中，您可以选择部署Cloud Volumes ONTAP时要使用的订阅。

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 API”下，选择“Azure 服务管理”。

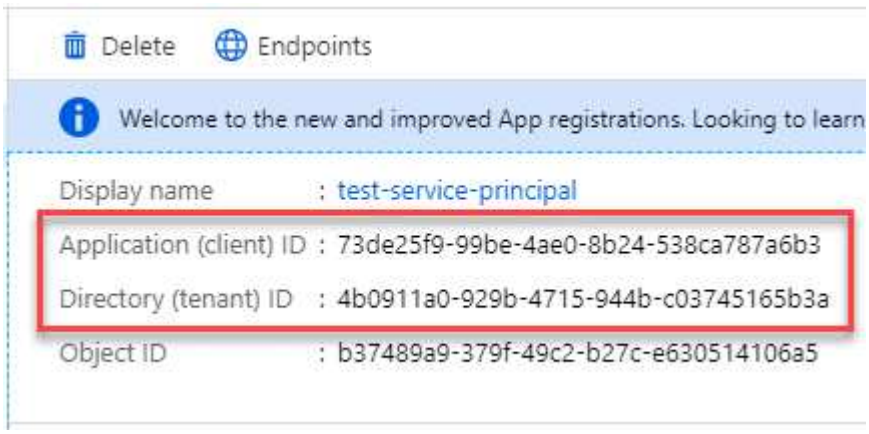


4. 选择*以组织用户身份访问 Azure 服务管理*，然后选择*添加权限*。



获取应用程序的应用程序**ID**和目录**ID**

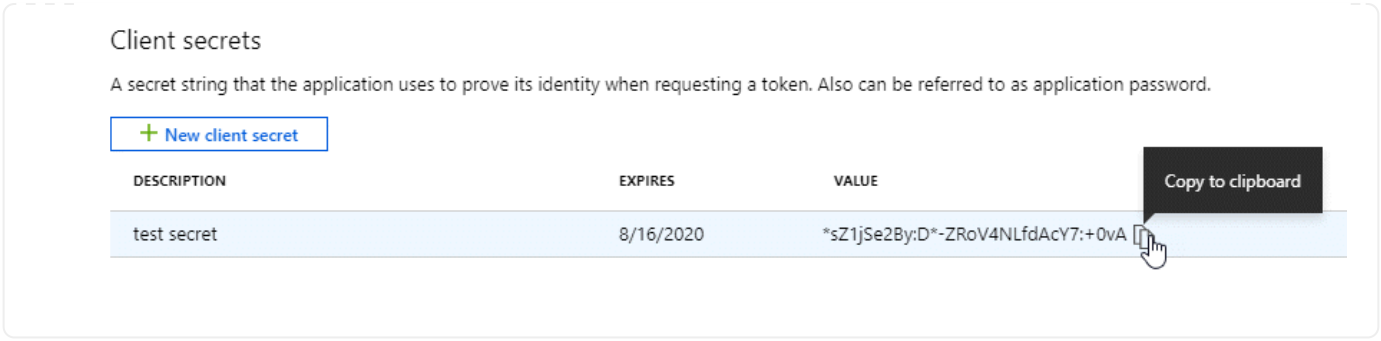
1. 在*Microsoft Entra ID*服务中，选择*App Registrations*并选择应用程序。
2. 复制*应用程序（客户端）ID*和*目录（租户）ID*。



将 Azure 帐户添加到控制台时，您需要提供应用程序（客户端）ID 和应用程序的目录（租户）ID。控制台使用 ID 以编程方式登录。

创建客户端机密

1. 开启*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. 提供秘密的描述和持续时间。
5. 选择“添加”。
6. 复制客户端机密的值。



手动安装控制台代理

当您手动安装控制台代理时，您需要准备您的机器环境以使其满足要求。您需要一台 Linux 机器，并且需要安装 Podman 或 Docker，具体取决于您的 Linux 操作系统。

安装 **Podman** 或 **Docker Engine**

根据您的操作系统，安装代理之前需要 Podman 或 Docker Engine。

- Red Hat Enterprise Linux 8 和 9 需要 Podman。

  查看支持的 Podman 版本 。

- Ubuntu 需要 Docker 引擎。

  查看支持的 Docker Engine 版本 。

示例 **1.** 步骤

Podman

按照以下步骤安装和配置 Podman：

- 启用并启动 podman.socket 服务
- 安装python3
- 安装 podman-compose 包版本 1.0.6
- 将 podman-compose 添加到 PATH 环境变量
- 如果使用 Red Hat Enterprise Linux，请验证您的 Podman 版本使用的是 Netavark Aardvark DNS 而不是 CNI

> 安装代理后调整 aardvark-dns 端口（默认值：53），以避免 DNS 端口冲突。按照说明配置端口。

步骤

1. 如果主机上安装了 podman-docker 包，请将其删除。

```
dnf remove podman-docker
rm /var/run/docker.sock
```

2. 安装 Podman。

   您可以从官方 Red Hat Enterprise Linux 存储库获取 Podman。

   a. 对于 Red Hat Enterprise Linux 9.6：

   ```
   sudo dnf install podman-5:<version>
   ```

   其中 <version> 是您正在安装的 Podman 支持的版本。查看支持的 Podman 版本 。

   b. 适用于 Red Hat Enterprise Linux 9.1 至 9.4：

   ```
   sudo dnf install podman-4:<version>
   ```

   其中 <version> 是您正在安装的 Podman 支持的版本。查看支持的 Podman 版本 。

   c. 对于 Red Hat Enterprise Linux 8：

   ```
   sudo dnf install podman-4:<version>
   ```

   其中 <version> 是您正在安装的 Podman 支持的版本。查看支持的 Podman 版本 。

3. 启用并启动 podman.socket 服务。

```
sudo systemctl enable --now podman.socket
```

4. 安装 python3。

```
sudo dnf install python3
```

5. 如果您的系统上还没有 EPEL 存储库包，请安装它。

   此步骤是必需的，因为 podman-compose 可从 Extra Packages for Enterprise Linux (EPEL) 存储库中获得。

6. 如果使用 Red Hat Enterprise 9：

   a. 安装EPEL存储库软件包。

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
```

   +

   a. 安装 podman-compose 包 1.5.0。

```
sudo dnf install podman-compose-1.5.0
```

7. 如果使用的是 Red Hat Enterprise Linux 8：

   a. 安装EPEL存储库软件包。

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

   b. 安装 podman-compose 包 1.0.6。

```
sudo dnf install podman-compose-1.0.6
```

   使用 `dnf install`命令满足将 podman-compose 添加到 PATH 环境变量的要求。安装命令将 podman-compose 添加到 /usr/bin，它已经包含在 `secure_path`主机上的选项。

   c. 如果使用 Red Hat Enterprise Linux 8，请验证您的 Podman 版本是否使用带有 Aardvark DNS 的 NetAvark 而不是 CNI。

i. 通过运行以下命令检查您的 networkBackend 是否设置为 CNI：

```
podman info | grep networkBackend
```

ii. 如果 networkBackend 设置为 `CNI`，你需要将其更改为 `netavark`。

iii. 安装 `netavark`和 `aardvark-dns`使用以下命令：

```
dnf install aardvark-dns netavark
```

iv. 打开 `/etc/containers/containers.conf`文件并修改 network_backend 选项以使用“netavark”而不是“cni”。

如果 `/etc/containers/containers.conf`不存在，请将配置更改为 `/usr/share/containers/containers.conf`。

v. 重新启动 podman。

```
systemctl restart podman
```

vi. 使用以下命令确认 networkBackend 现在已更改为“netavark”：

```
podman info | grep networkBackend
```

Docker 引擎

按照 Docker 的文档安装 Docker Engine。

步骤

1. "查看 Docker 的安装说明"

   按照步骤安装受支持的 Docker Engine 版本。请勿安装最新版本，因为控制台不支持它。

2. 验证 Docker 是否已启用并正在运行。

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

手动安装控制台代理

在本地现有 Linux 主机上下载并安装控制台代理软件。

开始之前

您应该具有以下内容：

- 安装控制台代理的 root 权限。
- 如果控制台代理需要代理才能访问互联网，则提供有关代理服务器的详细信息。

  您可以选择在安装后配置代理服务器，但这样做需要重新启动控制台代理。

- 如果代理服务器使用 HTTPS 或代理是拦截代理，则需要 CA 签名的证书。

手动安装控制台代理时，无法为透明代理服务器设置证书。如果需要为透明代理服务器设置证书，则必须在安装后使用维护控制台。详细了解"代理维护控制台"。

关于此任务

安装后，如果有新版本可用，控制台代理会自动更新。

步骤

1. 如果主机上设置了 *http_proxy* 或 *https_proxy* 系统变量，请将其删除：

   ```
   unset http_proxy
   unset https_proxy
   ```

   如果不删除这些系统变量，安装将失败。

2. 下载控制台代理软件，然后将其复制到 Linux 主机。您可以从NetApp Console或NetApp支持网站下载。
   - NetApp Console：转到*代理 > 管理 > 部署代理 > 本地部署 > 手动安装*。

     选择下载代理安装程序文件或文件的 URL。

   - NetApp支持网站（如果您还没有访问控制台的权限，则需要此网站） "NetApp 支持站点" ，
3. 分配运行脚本的权限。

   ```
   chmod +x NetApp_Console_Agent_Cloud_<version>
   ```

   其中 <version> 是您下载的控制台代理的版本。

4. 如果在政府云环境中安装，请禁用配置检查。"了解如何禁用手动安装的配置检查。"
5. 运行安装脚本。

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

   如果您的网络需要代理才能访问互联网，则需要添加代理信息。您可以在安装过程中添加显式代理。 `--proxy` 和 `--cacert` 参数是可选的，系统不会提示您添加它们。如果您有显式代理服务器，则需要输入如图所示的参数。

如果要配置透明代理，可以在安装完成后进行配置。 "了解代理维护控制台"

+

以下是使用 CA 签名证书配置显式代理服务器的示例：

+

```
./NetApp_Console_Agent_Cloud_v4.0.0--proxy
https://user:password@10.0.0.30:8080/ --cacert /tmp/cacert/certificate.cer
```

+
`--proxy` 使用以下格式之一将 Console 代理配置为使用 HTTP 或 HTTPS 代理服务器：

+ * 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

+ 注意以下事项：

+ 用户可以是本地用户或域用户。 对于域用户，您必须使用 \ 的 ASCII 码，如上所示。 **Console** 代理不支持包含 **@** 字符的用户名或密码。 如果密码包含以下任何特殊字符，则必须使用反斜杠前缀来转义该特殊字符：& 或 !

+ 例如：

+ http://bxpproxyuser:netapp1\!@address:3128

1. 如果您使用 Podman，则需要调整 aardvark-dns 端口。

   a. 通过 SSH 连接到控制台代理虚拟机。

   b. 打开 podman */usr/share/containers/containers.conf* 文件并修改 Aardvark DNS 服务的选定端口。例如，将其更改为54。

      ```
      vi /usr/share/containers/containers.conf
      ```

      例如：

      ```
      # Port to use for dns forwarding daemon with netavark in rootful bridge
      # mode and dns enabled.
      # Using an alternate port might be useful if other DNS services should
      # run on the machine.
      #
      dns_bind_port = 54
      ```

   a. 重新启动控制台代理虚拟机。

下一步是什么?

您需要在NetApp Console中注册控制台代理。

使用NetApp Console注册控制台代理

登录控制台并将控制台代理与您的组织关联。登录方式取决于您使用控制台的模式。如果您在标准模式下使用控制台，则可以通过 SaaS 网站登录。如果您在受限模式下使用控制台，则可以从控制台代理主机本地登录。

步骤

1. 打开 Web 浏览器并输入控制台代理主机 URL：

   控制台主机 URL 可以是本地主机、私有 IP 地址或公共 IP 地址，具体取决于主机的配置。例如，如果控制台代理位于没有公共 IP 地址的公共云中，则必须输入与控制台代理主机有连接的主机的私有 IP 地址。

2. 注册或登录。
3. 登录后，设置控制台：
   a. 指定与控制台代理关联的控制台组织。
   b. 输入系统的名称。
   c. 在*您是否在安全环境中运行？*下保持限制模式处于禁用状态。

      当控制台代理安装在本地时，不支持限制模式。

   d. 选择*让我们开始吧*。

向NetApp Console提供云提供商凭据

安装并设置控制台代理后，添加您的云凭据，以便控制台代理具有在 AWS 或 Azure 中执行操作所需的权限。

AWS

开始之前

如果您刚刚创建了这些 AWS 凭证，它们可能需要几分钟才能生效。等待几分钟，然后将凭据添加到控制台。

步骤

1. 选择“管理 > 凭证”。
2. 选择*组织凭证*。
3. 选择“添加凭据”并按照向导中的步骤操作。
   a. 凭证位置：选择*Amazon Web Services > 代理。
   b. 定义凭证：输入 AWS 访问密钥和密钥。
   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证关联。
   d. 审核：确认有关新凭证的详细信息并选择*添加*。

您现在可以前往 "NetApp Console"开始使用控制台代理。

Azure

开始之前

如果您刚刚创建了这些 Azure 凭据，它们可能需要几分钟才能使用。等待几分钟，然后再添加控制台代理的凭据。

步骤

1. 选择“管理 > 凭证”。
2. 选择“添加凭据”并按照向导中的步骤操作。
   a. 凭证位置：选择*Microsoft Azure > 代理*。
   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证关联。
   d. 审核：确认有关新凭证的详细信息并选择*添加*。

结果

控制台代理现在具有代表您在 Azure 中执行操作所需的权限。您现在可以前往 "NetApp Console"开始使用控制台代理。

使用 VCenter 在本地安装控制台代理

如果您是 VMWare 用户，您可以使用 OVA 在您的 VCenter 中安装控制台代理。可通过NetApp Console获取 OVA 下载或 URL。

当您使用 VCenter 工具安装控制台代理时，您可以使用 VM Web 控制台执行维护任务。"了解有关代理的 VM 控制台的更多信息。"

准备安装控制台代理

安装之前，请确保您的 VM 主机满足要求并且控制台代理可以访问互联网和目标网络。要使用NetApp数据服务或Cloud Volumes ONTAP，请为控制台代理创建云提供商凭据以代表您执行操作。

查看控制台代理主机要求

在安装控制台代理之前，请确保您的主机满足安装要求。

- CPU：8 核或 8 个 vCPU
- 内存：32 GB
- 磁盘空间：165 GB（厚置备）
- vSphere 7.0 或更高版本
- ESXi 主机 7.03 或更高版本

在 vCenter 环境中安装代理，而不是直接在 ESXi 主机上安装。

为控制台代理设置网络访问

与您的网络管理员合作，确保控制台代理具有对所需端点的出站访问权限以及与目标网络的连接。

连接到目标网络

控制台代理需要与您计划创建和管理系统的位置建立网络连接。例如，您计划在本地环境中创建Cloud Volumes ONTAP系统或存储系统的网络。

出站互联网访问

部署控制台代理的网络位置必须具有出站互联网连接才能联系特定端点。

使用基于 **Web** 的**NetApp Console**时从计算机联系的端点

从 Web 浏览器访问控制台的计算机必须能够联系多个端点。您需要使用控制台来设置控制台代理并进行控制台的日常使用。

"为NetApp控制台准备网络" 。

从控制台代理联系的端点

控制台代理需要出站互联网访问来联系以下端点，以管理公共云环境中的资源和流程以进行日常操作。

下面列出的端点都是 CNAME 条目。

您无法使用安装在本地的控制台代理来管理 Google Cloud 中的资源。要管理 Google Cloud 资源，请在 Google Cloud 中安装代理。

AWS

当控制台代理安装在本地时，它需要对以下 AWS 端点进行网络访问，以便管理部署在 AWS 中的NetApp 系统（例如Cloud Volumes ONTAP）。

从控制台代理联系的端点

控制台代理需要出站互联网访问来联系以下端点，以管理公共云环境中的资源和流程以进行日常操作。

下面列出的端点都是 CNAME 条目。

端点	目的
AWS 服务（amazonaws.com）： • 云形成 • 弹性计算云（EC2） • 身份和访问管理 (IAM) • 密钥管理服务（KMS） • 安全令牌服务 (STS) • 简单存储服务（S3）	管理 AWS 资源。端点取决于您的 AWS 区域。 "有关详细信息，请参阅 AWS 文档"
Amazon FsX for NetApp ONTAP： • api.workloads.netapp.com	基于 Web 的控制台通过与 Workload Factory API 交互来管理和操作基于ONTAP 的FSx 工作负载。
\ https://mysupport.netapp.com	获取许可信息并向NetApp支持发送AutoSupport消息。
\ https://signin.b2c.netapp.com	更新NetApp支持站点 (NSS) 凭据或将新的 NSS 凭据添加到NetApp Console。
\ https://support.netapp.com	获取许可信息并向NetApp支持发送AutoSupport消息以及接收Cloud Volumes ONTAP的软件更新。
\ https://api.bluexp.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com \ https://console.netapp.com \ https://components.console.bluexp.netapp.com \ https://cdn.auth0.com	在NetApp Console中提供功能和服务。

端点	目的
\ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://bluexpinfraprod.azurecr.io	获取控制台代理升级的图像。 • 当您部署新代理时，验证检查会测试与当前端点的连接。如果你使用"先前的端点"，验证检查失败。为了避免此失败，请跳过验证检查。 尽管以前的端点仍然受支持，但NetApp建议尽快将防火墙规则更新到当前端点。"了解如何更新终端节点列表" 。 • 当您更新到防火墙中的当前端点时，您现有的代理将继续工作。

Azure

当控制台代理安装在本地时，它需要对以下 Azure 端点进行网络访问，以便管理部署在 Azure 中的NetApp系统（例如Cloud Volumes ONTAP）。

端点	目的
\ https://management.azure.com \ https://login.microsoftonline.com \ https://blob.core.windows.net \ https://core.windows.net	管理 Azure 公共区域中的资源。
\ https://management.chinacloudapi.cn \ https://login.chinacloudapi.cn \ https://blob.core.chinacloudapi.cn \ https://core.chinacloudapi.cn	管理 Azure 中国区域的资源。
\ https://mysupport.netapp.com	获取许可信息并向NetApp支持发送AutoSupport消息。
\ https://signin.b2c.netapp.com	更新NetApp支持站点 (NSS) 凭据或将新的 NSS 凭据添加到NetApp Console。
\ https://support.netapp.com	获取许可信息并向NetApp支持发送AutoSupport消息以及接收Cloud Volumes ONTAP的软件更新。
\ https://api.bluexp.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com \ https://console.netapp.com \ https://components.console.bluexp.netapp.com \ https://cdn.auth0.com	在NetApp Console中提供功能和服务。

端点	目的
\ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://bluexpinfraprod.azurecr.io	获取控制台代理升级的图像。 • 当您部署新代理时，验证检查会测试与当前端点的连接。如果你使用"先前的端点"，验证检查失败。为了避免此失败，请跳过验证检查。 尽管以前的端点仍然受支持，但NetApp建议尽快将防火墙规则更新到当前端点。"了解如何更新终端节点列表" 。 • 当您更新到防火墙中的当前端点时，您现有的代理将继续工作。

代理服务器

NetApp支持显式和透明代理配置。如果您使用透明代理，则只需要提供代理服务器的证书。如果您使用显式代理，您还需要 IP 地址和凭据。

- IP 地址
- 凭据
- HTTPS 证书

端口

除非您启动它或将其用作代理将AutoSupport消息从Cloud Volumes ONTAP发送到NetApp支持，否则控制台代理不会有传入流量。

- HTTP（80）和 HTTPS（443）提供对本地 UI 的访问，您会在极少数情况下使用它们。
- 仅当需要连接到主机进行故障排除时才需要 SSH（22）。
- 如果您在没有出站互联网连接的子网中部署Cloud Volumes ONTAP系统，则需要通过端口 3128 建立入站连接。

  如果Cloud Volumes ONTAP系统没有出站互联网连接来发送AutoSupport消息，控制台会自动配置这些系统以使用控制台代理附带的代理服务器。唯一的要求是确保控制台代理的安全组允许通过端口 3128 进行入站连接。部署控制台代理后，您需要打开此端口。

启用 **NTP**

如果您计划使用NetApp Data Classification来扫描公司数据源，则应在控制台代理和NetApp Data Classification系统上启用网络时间协议 (NTP) 服务，以便系统之间的时间同步。 "了解有关NetApp数据分类的更多信息"

为 **AWS** 或 **Azure** 创建控制台代理云权限

如果您想将 AWS 或 Azure 中的NetApp数据服务与本地控制台代理一起使用，则需要在云提供商中设置权限，

以便在安装控制台代理后将凭据添加到控制台代理。

您无法使用安装在本地的控制台代理来管理 Google Cloud 中的资源。如果您想管理 Google Cloud 资源，则需要在 Google Cloud 中安装代理。

AWS

对于本地控制台代理，通过添加 IAM 用户访问密钥提供 AWS 权限。

对本地控制台代理使用 IAM 用户访问密钥；本地控制台代理不支持 IAM 角色。

步骤

1. 登录 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** 并复制并粘贴内容"控制台代理的 IAM 策略"。

    c. 完成剩余步骤以创建策略。

    根据您计划使用的NetApp数据服务，您可能需要创建第二个策略。

    对于标准区域，权限分布在两个策略中。由于 AWS 中托管策略的最大字符大小限制，因此需要两个策略。"了解有关控制台代理的 IAM 策略的更多信息" 。

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. 确保用户拥有访问密钥，您可以在安装控制台代理后将其添加到NetApp Console。

结果

您现在应该拥有具有所需权限的 IAM 用户访问密钥。安装控制台代理后，从控制台将这些凭证与控制台代理关联。

Azure

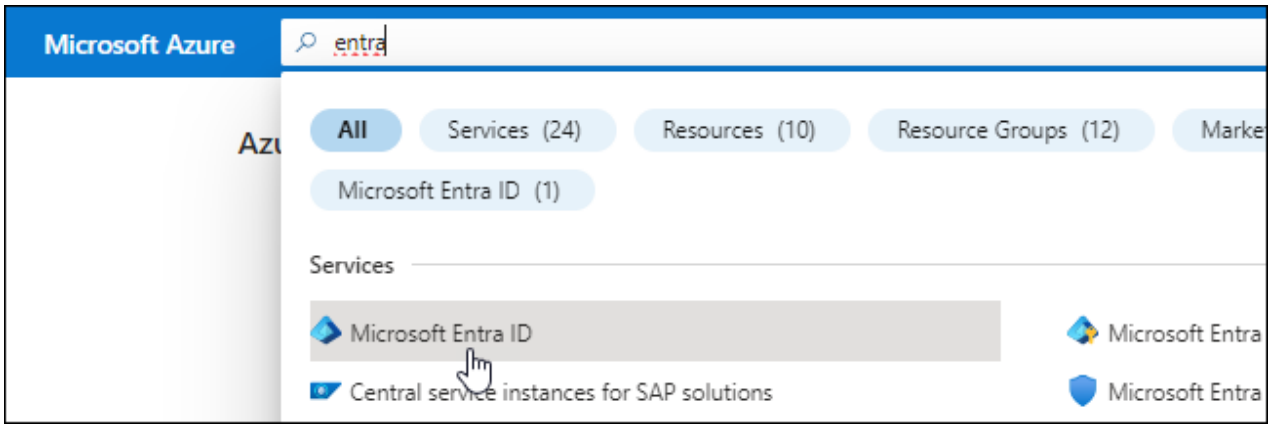
当控制台代理安装在本地时，您需要通过在 Microsoft Entra ID 中设置服务主体并获取控制台代理所需的 Azure 凭据来授予控制台代理 Azure 权限。

创建用于基于角色的访问控制的 **Microsoft Entra** 应用程序

1. 确保您在 Azure 中拥有创建 Active Directory 应用程序并将该应用程序分配给角色的权限。

    有关详细信息，请参阅 "Microsoft Azure 文档：所需权限"

2. 从 Azure 门户打开 **Microsoft Entra ID** 服务。



3. 在菜单中，选择*应用程序注册*。
4. 选择*新注册*。
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（任何类型都可以与NetApp Console一起使用）。
   - 重定向 **URI**：您可以将此字段留空。
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 CLI 或 REST API 创建 Azure 自定义角色。以下步骤展示如何使用 Azure CLI 创建角色。如果您希望使用其他方法，请参阅 "Azure 文档"

   a. 复制"控制台代理的自定义角色权限"并将它们保存在 JSON 文件中。
   b. 通过将 Azure 订阅 ID 添加到可分配范围来修改 JSON 文件。

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

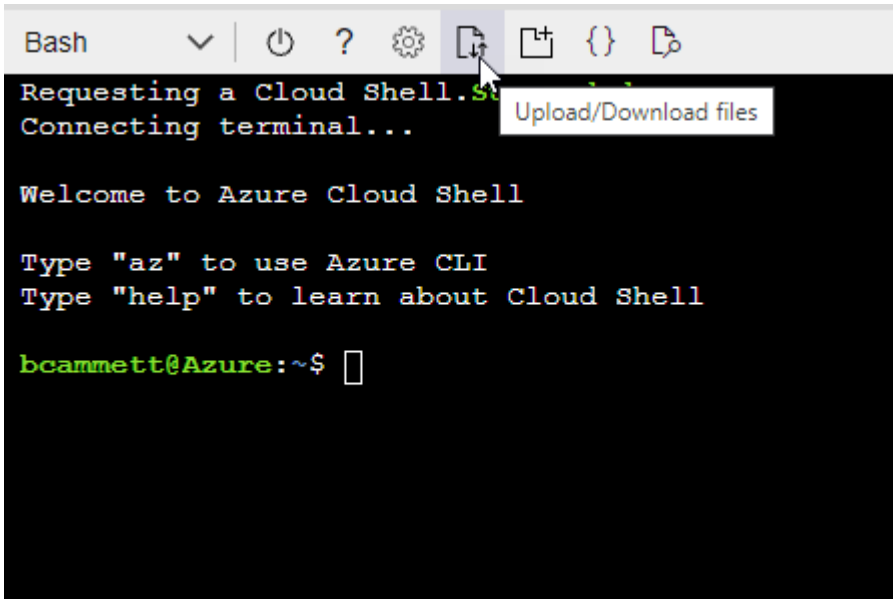
      例子

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

   c. 使用 JSON 文件在 Azure 中创建自定义角色。

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

- 开始 "Azure 云外壳"并选择 Bash 环境。
- 上传 JSON 文件。



- 使用 Azure CLI 创建自定义角色：

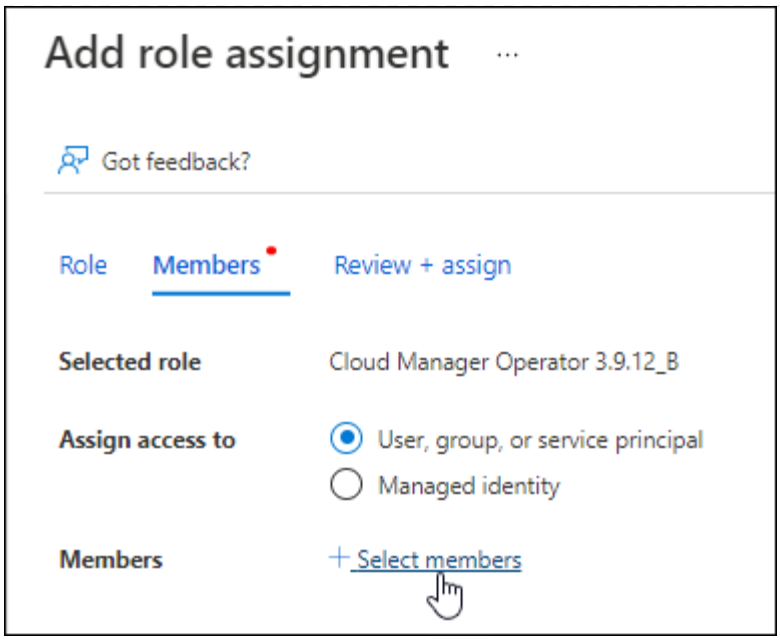
```
az role definition create --role-definition agent_Policy.json
```

现在您应该有一个名为“控制台操作员”的自定义角色，可以将其分配给控制台代理虚拟机。

2. 将应用程序分配给角色：

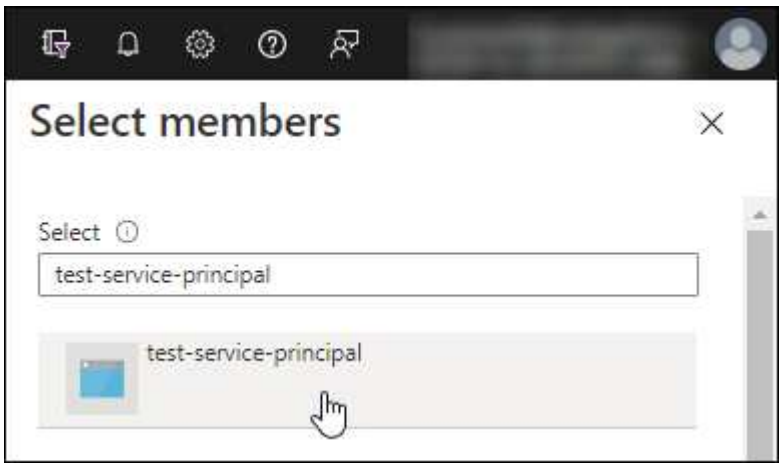
a. 从 Azure 门户打开 **Subscriptions** 服务。
b. 选择订阅。
c. 选择“访问控制 (IAM)”>“添加”>“添加角色分配”。
d. 在*角色*选项卡中，选择*控制台操作员*角色并选择*下一步*。
e. 在“成员”选项卡中，完成以下步骤：

- 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。

  以下是一个例子：



- 选择应用程序并选择*选择*。
- 选择“下一步”。

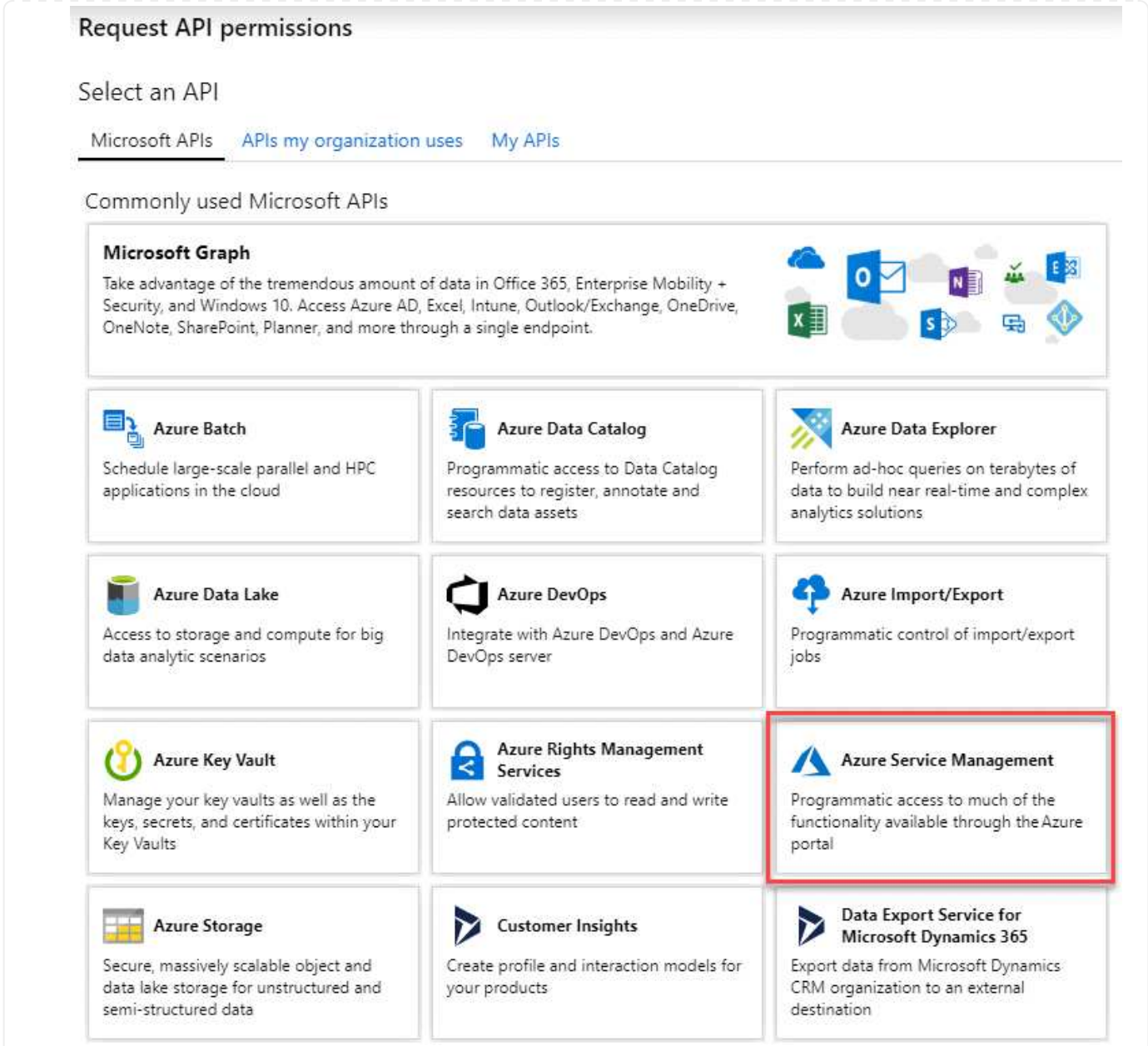
f. 选择*审阅+分配*。

服务主体现在具有部署控制台代理所需的 Azure 权限。

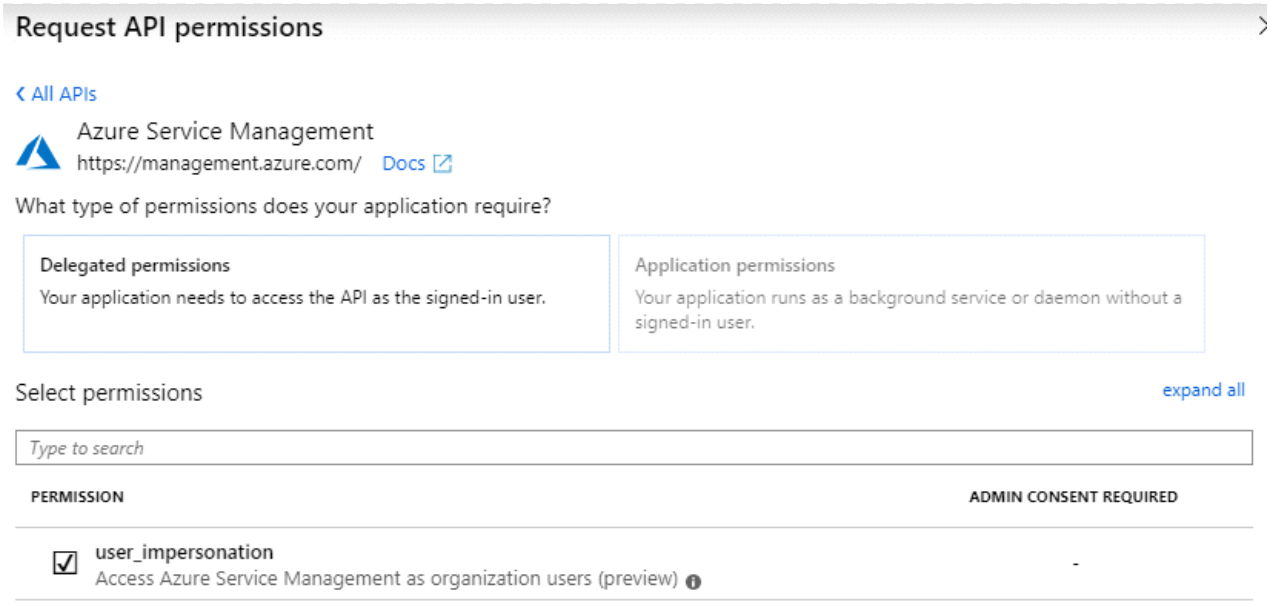
如果您想从多个 Azure 订阅部署Cloud Volumes ONTAP ，则必须将服务主体绑定到每个订阅。在NetApp Console中，您可以选择部署Cloud Volumes ONTAP时要使用的订阅。

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 API”下，选择“Azure 服务管理”。

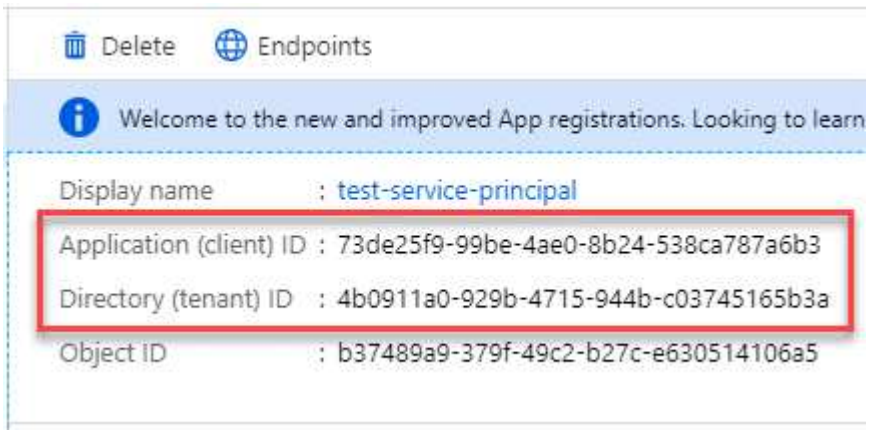


4. 选择*以组织用户身份访问 Azure 服务管理*，然后选择*添加权限*。



获取应用程序的应用程序**ID**和目录**ID**

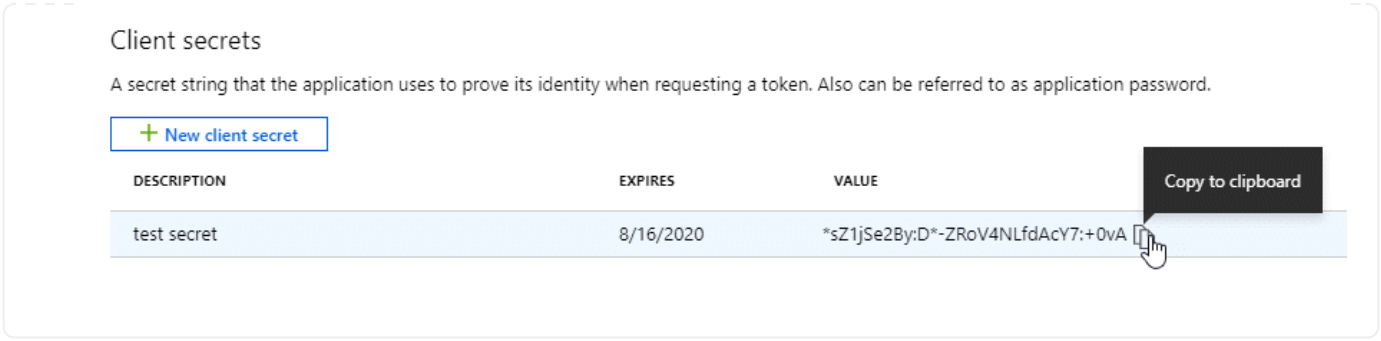
1. 在*Microsoft Entra ID*服务中，选择*App Registrations*并选择应用程序。
2. 复制*应用程序（客户端）ID*和*目录（租户）ID*。



将 Azure 帐户添加到控制台时，您需要提供应用程序（客户端）ID 和应用程序的目录（租户）ID。控制台使用 ID 以编程方式登录。

创建客户端机密

1. 开启*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. 提供秘密的描述和持续时间。
5. 选择“添加”。
6. 复制客户端机密的值。



在 **VCenter** 环境中安装控制台代理

NetApp支持在您的 VCenter 环境中安装控制台代理。 OVA 文件包含一个预配置的 VM 映像，您可以在 VMware 环境中部署该映像。可直接从NetApp Console下载文件或部署 URL。它包括控制台代理软件和自签名证书。

下载 **OVA** 或复制 **URL**

直接从NetApp Console下载 OVA 或复制 OVA URL。

1. 选择“管理 **>** 代理”。
2. 在“概览”页面上，选择“部署代理**>**本地”。
3. 选择*使用 OVA*。
4. 选择下载 OVA 或复制 URL 以在 VCenter 中使用。

在您的 **VCenter** 中部署代理

登录您的 VCenter 环境以部署代理。

步骤

1. 如果您的环境需要，请将自签名证书上传到您的受信任证书。安装后，您可以替换此证书。"了解如何替换自签名证书。"
2. 从内容库或本地系统部署 OVA。

从本地系统	来自内容库
a. 右键单击并选择 部署 **OVF** 模板...。b. 从 URL 中选择 OVA 文件或浏览到其位置，然后选择 下一步。	a. 转到您的内容库并选择控制台代理 OVA。b. 选择“操作”>“从此模板新建虚拟机”

3. 完成部署 OVF 模板向导以部署控制台代理。
4. 为虚拟机选择名称和文件夹，然后选择“下一步”。
5. 选择一个计算资源，然后选择*下一步*。
6. 查看模板的详细信息，然后选择*下一步*。
7. 接受许可协议，然后选择*下一步*。
8. 选择要使用的代理配置类型：显式代理、透明代理或无代理。
9. 选择要部署虚拟机的数据存储，然后选择*下一步*。确保它满足主机要求。

10. 选择您想要连接虚拟机的网络，然后选择*下一步*。确保网络为 IPv4 并且具有对所需端点的出站互联网访问权限。
11. 在*自定义模板*窗口中，填写以下字段：
    - 代理信息
      - 如果选择了显式代理，请输入代理服务器主机名或 IP 地址和端口号，以及用户名和密码。
      - 如果您选择了透明代理，请上传相应的证书。
    - 虚拟机配置
      - 跳过配置检查：默认情况下未选中此复选框，这意味着代理运行配置检查以验证网络访问。
        - NetApp建议不要选中此框，以便安装包含代理的配置检查。配置检查验证代理是否具有对所需端点的网络访问权限。如果由于连接问题导致部署失败，您可以从代理主机访问验证报告和日志。在某些情况下，如果您确信代理具有网络访问权限，则可以选择跳过检查。例如，如果您仍在使用"先前的端点"用于代理升级，验证失败并出现错误。为了避免这种情况，请勾选复选框以在不进行验证检查的情况下进行安装。"了解如何更新终端节点列表" 。
      - 维护密码：设置维护密码 `maint`允许访问代理维护控制台的用户。
      - **NTP** 服务器：指定一个或多个 NTP 服务器进行时间同步。
      - 主机名：设置此虚拟机的主机名。它不能包含搜索域。例如，FQDN console10.searchdomain.company.com 应输入为 console10。
      - 主 **DNS**：指定用于名称解析的主 DNS 服务器。
      - 辅助 **DNS**：指定用于名称解析的辅助 DNS 服务器。
      - 搜索域：指定解析主机名时使用的搜索域名。例如，如果 FQDN 是 console10.searchdomain.company.com，则输入 searchdomain.company.com。
      - **IPv4** 地址：映射到主机名的 IP 地址。
      - **IPv4** 子网掩码：IPv4 地址的子网掩码。
      - **IPv4** 网关地址：IPv4 地址的网关地址。
12. 选择“下一步”。
13. 查看“准备完成”窗口中的详细信息，选择“完成”。

    vSphere 任务栏显示控制台代理部署的进度。
14. 启动此虚拟机。

如果部署失败，您可以从代理主机访问验证报告和日志。"了解如何解决安装问题。"

使用NetApp Console注册控制台代理

登录控制台并将控制台代理与您的组织关联。登录方式取决于您使用控制台的模式。如果您在标准模式下使用控制台，则可以通过 SaaS 网站登录。如果您在受限或私人模式下使用控制台，则可以从控制台代理主机本地登录。

步骤

1. 打开 Web 浏览器并输入控制台代理主机 URL：

控制台主机 URL 可以是本地主机、私有 IP 地址或公共 IP 地址，具体取决于主机的配置。例如，如果控制台代理位于没有公共 IP 地址的公共云中，则必须输入与控制台代理主机有连接的主机的私有 IP 地址。

2. 注册或登录。
3. 登录后，设置控制台：
   a. 指定与控制台代理关联的控制台组织。
   b. 输入系统的名称。
   c. 在*您是否在安全环境中运行？*下保持限制模式处于禁用状态。

      当控制台代理安装在本地时，不支持限制模式。

   d. 选择*让我们开始吧*。

将云提供商凭据添加到控制台

安装并设置控制台代理后，添加您的云凭据，以便控制台代理具有在 AWS 或 Azure 中执行操作所需的权限。

AWS

开始之前

如果您刚刚创建了这些 AWS 凭证，它们可能需要几分钟才能生效。等待几分钟，然后将凭据添加到控制台。

步骤

1. 选择“管理 > 凭证”。
2. 选择*组织凭证*。
3. 选择“添加凭据”并按照向导中的步骤操作。
   a. 凭证位置：选择*Amazon Web Services > 代理。
   b. 定义凭证：输入 AWS 访问密钥和密钥。
   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证关联。
   d. 审核：确认有关新凭证的详细信息并选择*添加*。

您现在可以前往 "NetApp Console"开始使用控制台代理。

Azure

开始之前

如果您刚刚创建了这些 Azure 凭据，它们可能需要几分钟才能使用。等待几分钟，然后再添加控制台代理的凭据。

步骤

1. 选择“管理 > 凭证”。
2. 选择“添加凭据”并按照向导中的步骤操作。
   a. 凭证位置：选择*Microsoft Azure > 代理*。
   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证关联。
   d. 审核：确认有关新凭证的详细信息并选择*添加*。

结果

控制台代理现在具有代表您在 Azure 中执行操作所需的权限。您现在可以前往 "NetApp Console"开始使用控制台代理。

本地控制台代理的端口

当在本地 Linux 主机上手动安装时，控制台代理使用_入站_端口。请参考这些端口以进行规划。

这些入站规则适用于所有NetApp Console部署模式。

协议	端口	目的
HTTP	80	• 提供从客户端 Web 浏览器到本地用户界面的 HTTP 访问 • 在Cloud Volumes ONTAP升级过程中使用
HTTPS	443	提供从客户端 Web 浏览器到本地用户界面的 HTTPS 访问