创建控制台代理

NetApp Console setup and administration

NetApp
December 12, 2025

目录

创建控制台代理

AWS

AWS 中的控制台代理安装选项

有几种不同的方法可以在 AWS 中创建控制台代理。直接从NetApp Console是最常见的方式。

有以下安装选项可用：

- "直接从控制台创建控制台代理"（这是标准选项）

  此操作将在您选择的 VPC 中启动运行 Linux 和控制台代理软件的 EC2 实例。

- "从 AWS Marketplace 创建控制台代理"

  此操作还会启动运行 Linux 和控制台代理软件的 EC2 实例，但部署直接从 AWS Marketplace 启动，而不是从控制台启动。

- "在您自己的Linux主机上下载并手动安装软件"

您选择的安装选项会影响您如何准备安装。这包括如何向控制台提供验证和管理 AWS 中的资源所需的权限。

通过NetApp Console在 AWS 中创建控制台代理

您可以直接从NetApp Console在 AWS 中创建控制台代理。在从控制台创建 AWS 中的控制台代理之前，您需要设置网络并准备 AWS 权限。

开始之前

- 你应该有一个"了解控制台代理"。
- 你应该回顾一下"控制台代理限制"。

步骤 1：设置网络以在 AWS 中部署控制台代理

确保您计划安装控制台代理的网络位置支持以下要求。这些要求使控制台代理能够管理混合云中的资源和流程。

VPC 和子网
: 创建控制台代理时，您需要指定它所在的 VPC 和子网。

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。

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。

从**NetApp**控制台联系的端点

当您使用通过 SaaS 层提供的基于 Web 的NetApp Console时，它会联系多个端点来完成数据管理任务。这包括从控制台联系以部署控制台代理的端点。

"查看从NetApp控制台联系的端点列表" 。

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"

创建控制台代理后，您需要实现此网络要求。

步骤 **2**：为控制台代理设置 **AWS** 权限

控制台需要通过 AWS 进行身份验证，然后才能在您的 VPC 中部署控制台代理。您可以选择以下身份验证方法之一：

- 让控制台承担具有所需权限的 IAM 角色
- 为具有所需权限的 IAM 用户提供 AWS 访问密钥和密钥

无论选择哪种方式，第一步都是创建 IAM 策略。此策略仅包含从控制台启动 AWS 中的控制台代理所需的权限。

如果需要，您可以使用 IAM 限制 IAM 策略 `Condition`元素。 "AWS 文档：条件元素"

步骤

1. 转到 AWS IAM 控制台。
2. 选择“策略”>“创建策略”。
3. 选择 **JSON**。
4. 复制并粘贴以下策略：

   此策略仅包含从控制台启动 AWS 中的控制台代理所需的权限。当控制台创建控制台代理时，它会将一组新权限应用于控制台代理，使控制台代理能够管理 AWS 资源。"查看控制台代理本身所需的权限"。

```
{
  "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. 选择*下一步*并添加标签（如果需要）。
6. 选择*下一步*并输入名称和描述。
7. 选择*创建策略*。
8. 将策略附加到控制台可以承担的 IAM 角色或 IAM 用户，以便您可以为控制台提供访问密钥：
   - （选项 1）设置控制台可以承担的 IAM 角色：
     i. 转到目标账户中的 AWS IAM 控制台。
     ii. 在访问管理下，选择*角色>创建角色*并按照步骤创建角色。
     iii. 在 受信任实体类型 下，选择 **AWS** 账户。
     iv. 选择*另一个 AWS 账户*并输入控制台 SaaS 账户的 ID：952013314444
     v. 选择您在上一节中创建的策略。
     vi. 创建角色后，复制角色 ARN，以便在创建控制台代理时将其粘贴到控制台中。
   - （选项 2）为 IAM 用户设置权限，以便您可以向控制台提供访问密钥：
     i. 从 AWS IAM 控制台中，选择 用户，然后选择用户名。
     ii. 选择*添加权限>直接附加现有策略*。
     iii. 选择您创建的策略。
     iv. 选择*下一步*，然后选择*添加权限*。
     v. 确保您拥有 IAM 用户的访问密钥和密钥。

结果

您现在应该拥有一个具有所需权限的 IAM 角色或一个具有所需权限的 IAM 用户。从控制台创建控制台代理时，您可以提供有关角色或访问密钥的信息。

步骤 **3**：创建控制台代理

直接从基于 Web 的控制台创建控制台代理。

关于此任务

- 从控制台创建控制台代理使用默认配置在 AWS 中部署 EC2 实例。创建控制台代理后，请勿切换到具有较少 CPU 或较少 RAM 的较小 EC2 实例。"了解控制台代理的默认配置" 。
- 当控制台创建控制台代理时，它会为代理创建一个 IAM 角色和一个配置文件。此角色包括使控制台代理能够管理 AWS 资源的权限。确保在未来版本中添加新权限时更新角色。"了解有关控制台代理的 IAM 策略的更多信息"。

开始之前

您应该具有以下内容：

- AWS 身份验证方法：具有所需权限的 IAM 角色或 IAM 用户的访问密钥。
- 满足组网需求的VPC及子网。
- EC2 实例的密钥对。
- 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。
- 设置"网络要求"。
- 设置"AWS 权限"。

步骤

1. 选择“管理 > 代理”。
2. 在“概览”页面上，选择“部署代理”>“AWS”
3. 按照向导中的步骤创建控制台代理：
4. 在“简介”页面上提供了该过程的概述
5. 在 **AWS Credentials** 页面上，指定您的 AWS 区域，然后选择一种身份验证方法，该方法可以是控制台可以承担的 IAM 角色，也可以是 AWS 访问密钥和密钥。

   如果您选择*承担角色*，您可以从控制台代理部署向导创建第一组凭据。任何附加凭证集都必须从凭证页面创建。然后，它们将从向导的下拉列表中提供。"了解如何添加其他凭证" 。

6. 在“详细信息”页面上，提供有关控制台代理的详细信息。
   - 输入名称。
   - 添加自定义标签（元数据）。
   - 选择是否希望控制台创建具有所需权限的新角色，或者是否要选择您设置的现有角色"所需的权限"。
   - 选择是否要加密控制台代理的 EBS 磁盘。您可以选择使用默认加密密钥或使用自定义密钥。
7. 在*网络*页面上，为代理指定 VPC、子网和密钥对，选择是否启用公共 IP 地址，并选择性地指定代理配置。

   确保您拥有正确的密钥对来访问控制台代理虚拟机。如果没有密钥对，您就无法访问它。

8. 在“安全组”页面上，选择是否创建新的安全组或是否选择允许所需入站和出站规则的现有安全组。

   "查看 AWS 的安全组规则" 。

9. 检查您的选择以验证您的设置是否正确。

   a. 默认情况下，*验证代理配置*复选框处于选中状态，以便控制台在您部署时验证网络连接要求。如果控制台无法部署代理，它会提供一份报告来帮助您排除故障。如果部署成功，则不会提供报告。

   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，请取消选中复选框以跳过验证检查。

10. 选择“添加”。

    控制台大约需要 10 分钟即可部署代理。停留在该页面上直到该过程完成。

结果

该过程完成后，即可从控制台使用控制台代理。

如果部署失败，您可以从控制台下载报告和日志来帮助您解决问题。"了解如何解决安装问题。"

如果您在创建控制台代理的同一 AWS 账户中拥有 Amazon S3 存储桶，您将看到 Amazon S3 工作环境自动出现在 系统 页面上。 "了解如何从NetApp Console管理 S3 存储桶"

从 **AWS Marketplace** 创建控制台代理

您可以直接从 AWS Marketplace 在 AWS 中创建控制台代理。要从 AWS Marketplace 创建控制台代理，您需要设置网络、准备 AWS 权限、查看实例要求，然后创建控制台代理。

开始之前

- 你应该有一个"了解控制台代理"。
- 你应该回顾一下"控制台代理限制"。

步骤 **1**：设置网络

确保控制台代理的网络位置满足以下要求以管理混合云资源。

VPC 和子网

创建控制台代理时，您需要指定它所在的 VPC 和子网。

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。

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。

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"

创建控制台代理后实现此网络访问。

步骤 2：设置 AWS 权限

为了准备市场部署，请在 AWS 中创建 IAM 策略并将其附加到 IAM 角色。当您从 AWS Marketplace 创建控制台代理时，系统会提示您选择该 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。

      您可能需要根据计划使用的NetApp数据服务创建第二个策略。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. 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. 完成剩余步骤以创建角色。

结果

现在，您拥有一个 IAM 角色，可以在从 AWS Marketplace 部署期间将其与 EC2 实例关联。

步骤 3：查看实例要求

创建控制台代理时，您需要选择满足以下要求的 EC2 实例类型。

CPU

8 个核心或 8 个 vCPU

RAM

32 GB

AWS EC2 实例类型

满足 CPU 和 RAM 要求的实例类型。 NetApp推荐使用 t3.2xlarge。

步骤 4：创建控制台代理

直接从 AWS Marketplace 创建控制台代理。

关于此任务

从 AWS Marketplace 创建控制台代理会使用默认配置在 AWS 中部署 EC2 实例。"了解控制台代理的默认配置" 。

开始之前

您应该具有以下内容：

- 满足组网需求的VPC及子网。
- 具有附加策略的 IAM 角色，其中包含控制台代理所需的权限。
- 您的 IAM 用户订阅和取消订阅 AWS Marketplace 的权限。
- 了解实例的 CPU 和 RAM 要求。
- EC2 实例的密钥对。

步骤

1. 前往 "AWS Marketplace 上的NetApp Console代理列表"
2. 在市场页面上，选择*继续订阅*。
3. 要订阅该软件，请选择*接受条款*。

   订阅过程可能需要几分钟。

4. 订阅过程完成后，选择*继续配置*。
5. 在*配置此软件*页面上，确保您选择了正确的区域，然后选择*继续启动*。
6. 在*启动此软件*页面的*选择操作*下，选择*通过 EC2 启动*，然后选择*启动*。

   使用 EC2 控制台启动实例并附加 IAM 角色。使用“从网站启动”操作无法实现这一点。

7. 按照提示配置并部署实例：

   - 名称和标签：输入实例的名称和标签。
   - 应用程序和操作系统映像：跳过此部分。控制台代理 AMI 已被选中。
   - 实例类型：根据区域可用性，选择满足 RAM 和 CPU 要求的实例类型（预先选择并推荐 t3.2xlarge）。
   - 密钥对（登录）：选择您想要用来安全连接到实例的密钥对。
   - 网络设置：根据需要编辑网络设置：
     - 选择所需的 VPC 和子网。
     - 指定实例是否应具有公共 IP 地址。
     - 指定安全组设置，为控制台代理实例启用所需的连接方法：SSH、HTTP 和 HTTPS。

       "查看 AWS 的安全组规则" 。
   - 配置存储：保留根卷的默认大小和磁盘类型。

     如果要在根卷上启用 Amazon EBS 加密，请选择 高级，展开 卷 **1**，选择 加密，然后选择一个 KMS 密钥。
   - 高级详细信息：在 **IAM** 实例配置文件 下，选择包含控制台代理所需权限的 IAM 角色。
   - 摘要：查看摘要并选择*启动实例*。

     AWS 使用指定的设置启动控制台代理，控制台代理将在大约十分钟内运行。

如果安装失败，您可以查看日志和报告来帮助您排除故障。"了解如何解决安装问题。"

8. 从连接到控制台代理虚拟机并具有控制台代理 URL 的主机打开 Web 浏览器。
9. 登录后，设置控制台代理：
   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。

      保持限制模式处于禁用状态以便在标准模式下使用控制台。仅当您拥有安全的环境并希望断开此帐户与控制台后端服务的连接时，才应启用受限模式。如果真是这样的话，"按照步骤在受限模式下开始使用NetApp Console" 。

   d. 选择*让我们开始吧*。

结果

控制台代理现已安装并设置到您的控制台组织。

打开 Web 浏览器并转到 "NetApp Console"开始将控制台代理与控制台一起使用。

如果您在创建控制台代理的同一 AWS 账户中拥有 Amazon S3 存储桶，您将看到 Amazon S3 工作环境自动出现在 系统 页面上。 "了解如何从NetApp Console管理 S3 存储桶"

在 AWS 中手动安装控制台代理

您可以在 AWS 中运行的 Linux 主机上手动安装控制台代理。要在您自己的 Linux 主机上手动安装控制台代理，您需要查看主机要求、设置网络、准备 AWS 权限、安装控制台代理，然后提供您准备好的权限。

开始之前

- 你应该有一个"了解控制台代理"。
- 你应该回顾一下"控制台代理限制"。

步骤 1：查看主机要求

确保运行控制台代理软件的主机满足操作系统、内存和端口要求。

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。

AWS EC2 实例类型

满足 CPU 和 RAM 要求的实例类型。 NetApp推荐使用 t3.2xlarge。

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 。

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**
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

密钥对

创建控制台代理时，您需要选择一个 EC2 密钥对来与实例一起使用。

使用 **IMDSv2** 时的 **PUT** 响应跳数限制

如果启用了 IMDSv2（新 EC2 实例的默认设置），请将 PUT 响应跳数限制设置为 3。否则，系统会在代理设置期间显示 UI 初始化错误。

- "要求在 Amazon EC2 实例上使用 IMDSv2"
- "AWS 文档：更改 PUT 响应跳数限制"

步骤 2：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
```

步骤 **3**：设置网络

请确保网络位置满足以下要求，以便控制台代理能够管理混合云中的资源。

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。

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。

端点	目的
\ 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。
\ 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"

步骤 **4**：设置控制台的 **AWS** 权限

请使用以下选项之一为NetApp Console提供 AWS 权限：

- 选项 1：创建 IAM 策略并将策略附加到可与 EC2 实例关联的 IAM 角色。
- 选项 2：向控制台提供具有所需权限的 IAM 用户的 AWS 访问密钥。

按照步骤准备控制台的权限。

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. 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. 完成剩余步骤以创建角色。

结果

安装控制台代理后，您现在拥有一个可以与 EC2 实例关联的 IAM 角色。

AWS 访问密钥

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

现在，您拥有一个具有所需权限的 IAM 用户和一个可以提供给控制台的访问密钥。

步骤 **5**：安装控制台代理

完成所有先决条件后，请在您的 Linux 主机上手动安装该软件。

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来访问互联网，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。如果您有明确的代理服务器，则需要按所示方式输入参数。

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控制台代理配置为使用 HTTP 或 HTTPS 代理服务器：

- http://地址:端口
- http://用户名:密码@地址:端口
- http://域名%92用户名:密码@地址:端口
- https://地址:端口
- https://用户名:密码@地址:端口
- https://域名%92用户名:密码@地址:端口

  请注意以下事项：

  - 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 代码，如上所示。
  - 控制台代理不支持包含 @ 字符的用户名或密码。
  - 如果密码包含以下任何特殊字符，则必须在该特殊字符前面加上反斜杠来转义该特殊字符：& 或 !

    例如：

http://bxpproxyuser:netapp1\!@地址:3128

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"

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。

2. 等待安装完成。

安装结束时，如果您指定了代理服务器，控制台代理服务 (occm) 将重新启动两次。

如果安装失败，您可以查看安装报告和日志来帮助您解决问题。"了解如何解决安装问题。"

1. 从连接到控制台代理虚拟机的主机打开 Web 浏览器并输入以下 URL：

https://ipaddress

2. 登录后，设置控制台代理：

a. 指定与控制台代理关联的组织。

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。

您应该保持限制模式处于禁用状态，因为这些步骤描述了如何在标准模式下使用控制台。仅当您拥有安全的环境并希望断开此帐户与后端服务的连接时，才应启用受限模式。如果真是这样的话，"按照步骤在受限模式下开始使用NetApp Console" 。

d. 选择*让我们开始吧*。

如果您在创建控制台代理的同一 AWS 账户中拥有 Amazon S3 存储桶，您将看到 Amazon S3 存储系统自动出现在 系统 页面上。 "了解如何通过NetApp ConsoleP 管理 S3 存储桶"

步骤 **6**：提供对**NetApp Console**的权限

安装控制台代理后，提供您设置的 AWS 权限，以便控制台代理可以管理您在 AWS 中的数据和存储基础设施。

IAM 角色

将创建的 IAM 角色附加到控制台代理 EC2 实例。

步骤

1. 转到 Amazon EC2 控制台。
2. 选择*实例*。
3. 选择控制台代理实例。
4. 选择*操作 > 安全 > 修改 IAM 角色*。
5. 选择 IAM 角色并选择 更新 **IAM** 角色。

前往 "NetApp Console"开始使用控制台代理。

AWS 访问密钥

向控制台提供具有所需权限的 IAM 用户的 AWS 访问密钥。

步骤

1. 确保当前在控制台中选择了正确的控制台代理。
2. 选择“管理 **>** 凭证”。
3. 选择*组织凭证*。
4. 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*。

前往 "NetApp Console"开始使用控制台代理。

Azure

Azure 中的控制台代理安装选项

有几种不同的方法可以在 Azure 中创建控制台代理。直接从NetApp Console是最常见的方式。

有以下安装选项可用：

- "直接从NetApp Console创建控制台代理"（这是标准选项）

  此操作将在您选择的 VNet 中启动运行 Linux 和控制台代理软件的 VM。

- "从 Azure 市场创建控制台代理"

此操作还会启动运行 Linux 和控制台代理软件的 VM，但部署直接从 Azure 市场启动，而不是从控制台启动。

- "在您自己的Linux主机上下载并手动安装软件"

您选择的安装选项会影响您如何准备安装。这包括如何为控制台代理提供在 Azure 中验证和管理资源所需的权限。

从NetApp Console在 Azure 中创建控制台代理

要从NetApp Console在 Azure 中创建控制台代理，您需要设置网络、准备 Azure 权限，然后创建控制台代理。

开始之前

- 你应该有一个"了解控制台代理"。
- 你应该回顾一下"控制台代理限制"。

步骤 1：设置网络

确保您计划安装控制台代理的网络位置支持以下要求。这些要求允许控制台代理管理混合云资源。

Azure 区域

如果您使用Cloud Volumes ONTAP，则控制台代理应部署在与其管理的Cloud Volumes ONTAP系统相同的 Azure 区域中，或者部署在 "Azure 区域对"适用于Cloud Volumes ONTAP系统。此要求确保在Cloud Volumes ONTAP及其关联的存储帐户之间使用 Azure Private Link 连接。

"了解Cloud Volumes ONTAP如何使用 Azure Private Link"

VNet 和子网

创建控制台代理时，您需要指定它所在的 VNet 和子网。

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。

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
\ 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。

端点	目的
\ 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。
\ 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。

从**NetApp**控制台联系的端点

当您使用通过 SaaS 层提供的基于 Web 的NetApp Console时，它会联系多个端点来完成数据管理任务。这包括从控制台联系以部署控制台代理的端点。

"查看从NetApp控制台联系的端点列表" 。

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"

您需要在创建控制台代理后实现此网络要求。

步骤 **2**：创建控制台代理部署策略（自定义角色）

您需要创建一个具有在 Azure 中部署控制台代理的权限的自定义角色。

创建一个 Azure 自定义角色，您可以将其分配给您的 Azure 帐户或 Microsoft Entra 服务主体。控制台通过 Azure 进行身份验证，并使用这些权限代表您创建控制台代理。

控制台在 Azure 中部署控制台代理虚拟机，启用 "系统分配的托管标识"，创建所需的角色，并将其分配给虚拟机。"查看控制台如何使用权限" 。

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"

步骤

1. 复制 Azure 中新自定义角色所需的权限并将其保存在 JSON 文件中。

   此自定义角色仅包含从控制台启动 Azure 中的控制台代理 VM 所需的权限。请勿将此政策用于其他情况。当控制台创建控制台代理时，它会将一组新权限应用于控制台代理 VM，使控制台代理能够管理 Azure 资源。

```
{
  "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/rea
d",
    "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. 通过将 Azure 订阅 ID 添加到可分配范围来修改 JSON。

   例子

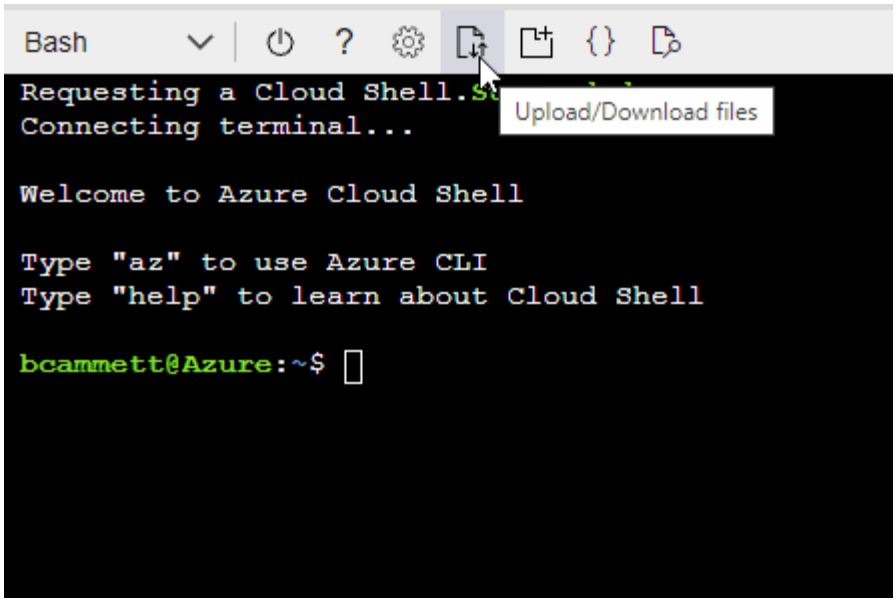
```
"AssignableScopes": [
"/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz"
]
```

3. 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。

   a. 开始 "Azure 云外壳"并选择 Bash 环境。

   b. 上传 JSON 文件。



c. 输入以下 Azure CLI 命令：

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

您现在有一个名为“Azure SetupAsService”的自定义角色。您可以将此自定义角色应用到您的用户帐户或服务主体。

步骤 **3**：设置身份验证

从控制台创建控制台代理时，您需要提供一个登录名，以使控制台能够通过 Azure 进行身份验证并部署 VM。您有两个选择：

1. 出现提示时使用您的 Azure 帐户Sign in。此帐户必须具有特定的 Azure 权限。这是默认选项。
2. 提供有关 Microsoft Entra 服务主体的详细信息。此服务主体还需要特定的权限。

按照以下步骤准备其中一种身份验证方法以供控制台使用。

Azure 帐户

将自定义角色分配给将从控制台部署控制台代理的用户。

步骤

1. 在 Azure 门户中，打开 **Subscriptions** 服务并选择用户的订阅。
2. 单击*访问控制 (IAM)*。
3. 单击*添加*>*添加角色分配*，然后添加权限：
   a. 选择 **Azure SetupAsService** 角色并单击 下一步。

      Azure SetupAsService 是 Azure 控制台代理部署策略中提供的默认名称。如果您为角色选择了不同的名称，则选择该名称。

   b. 保持选中“用户、组或服务主体”。
   c. 单击*选择成员*，选择您的用户帐户，然后单击*选择*。
   d. 单击“下一步”。
   e. 单击*审阅+分配*。

服务主体

您无需使用 Azure 帐户登录，而是可以向控制台提供具有所需权限的 Azure 服务主体的凭据。

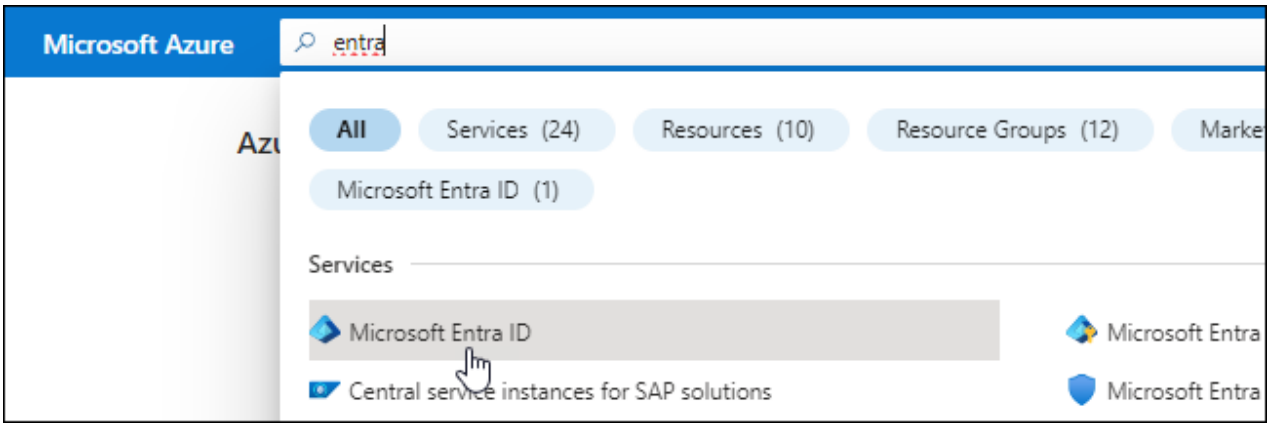
在 Microsoft Entra ID 中创建并设置服务主体，并获取控制台所需的 Azure 凭据。

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*。

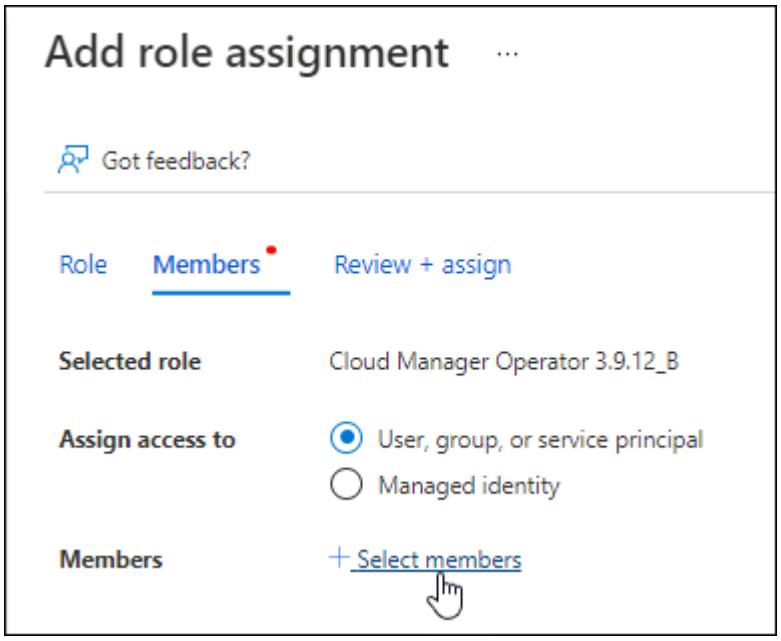
您已创建 AD 应用程序和服务主体。

将自定义角色分配给应用程序

1. 从 Azure 门户打开 **Subscriptions** 服务。
2. 选择订阅。
3. 单击*访问控制 (IAM) > 添加 > 添加角色分配*。
4. 在“角色”选项卡中，选择“控制台操作员”角色，然后单击“下一步”。
5. 在“成员”选项卡中，完成以下步骤：

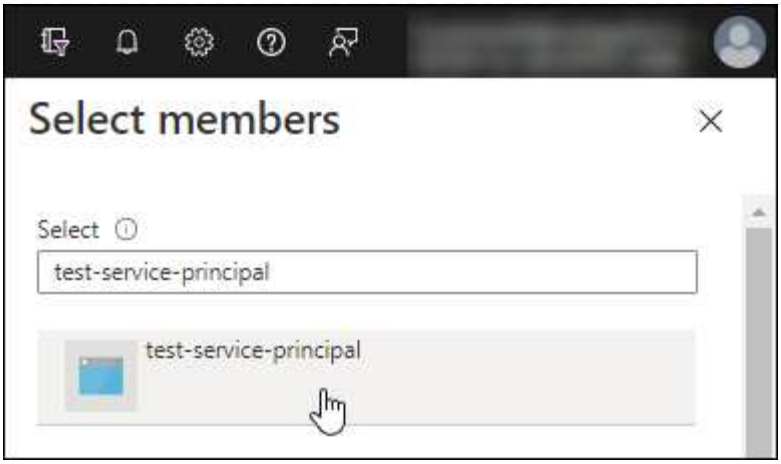
a. 保持选中“用户、组或服务主体”。

b. 单击“选择成员”。



c. 搜索应用程序的名称。

以下是一个例子：



a. 选择应用程序并单击*选择*。

b. 单击“下一步”。

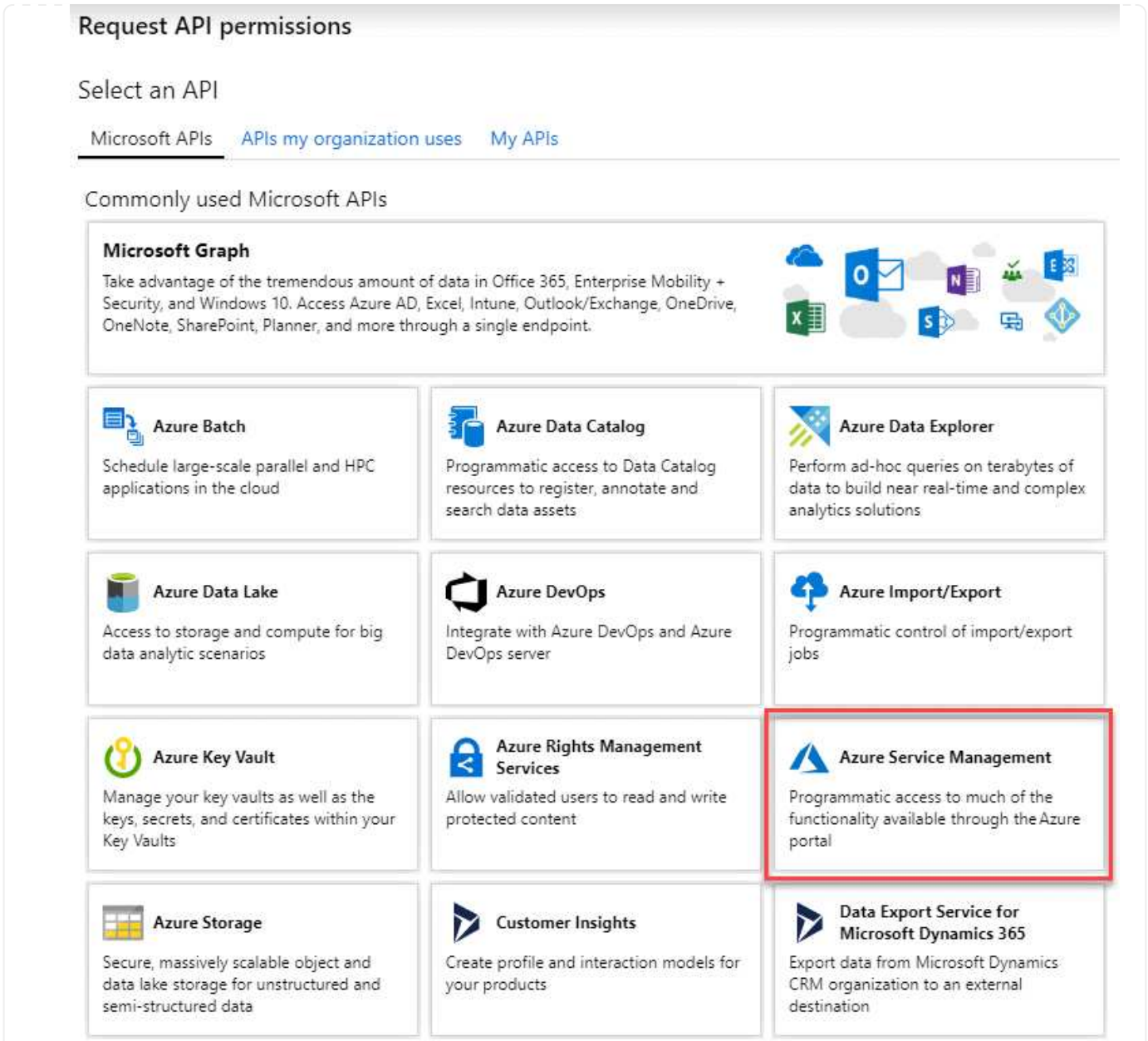
6. 单击*审阅+分配*。

服务主体现在具有部署控制台代理所需的 Azure 权限。

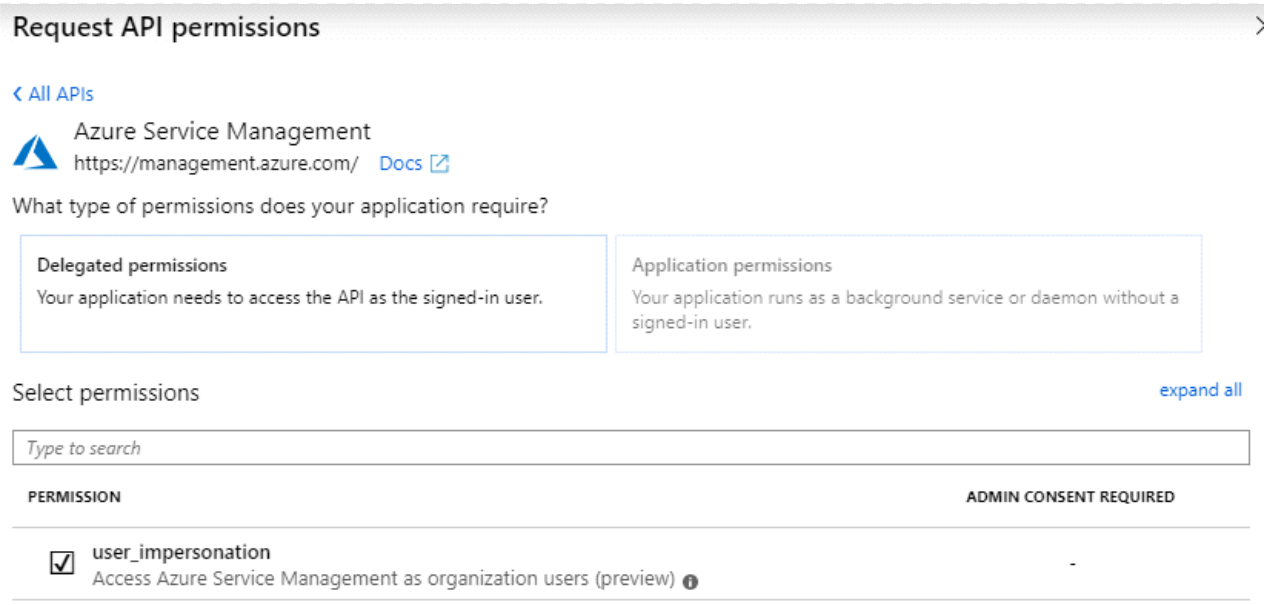
如果您想要管理多个 Azure 订阅中的资源，则必须将服务主体绑定到每个订阅。例如，控制台允许您选择部署Cloud Volumes ONTAP时要使用的订阅。

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”。

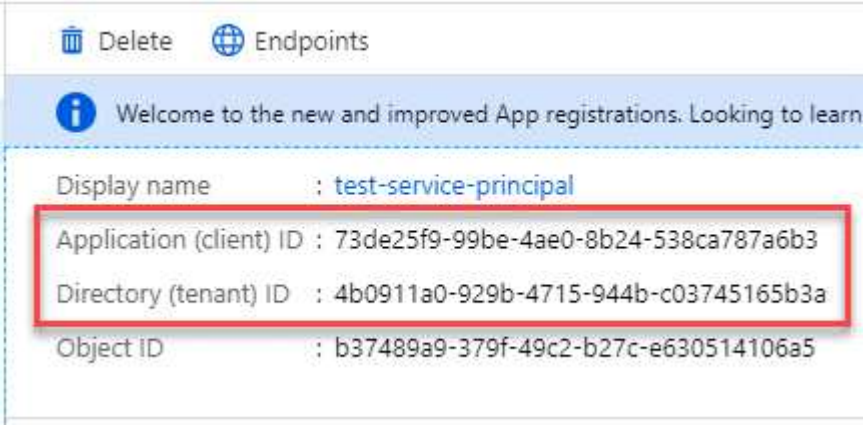


4. 选择*以组织用户身份访问 Azure 服务管理*，然后选择*添加权限*。



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。

结果

您的服务主体现已设置，您应该已经复制了应用程序（客户端）ID、目录（租户）ID 和客户端机密的值。创建控制台代理时，您需要在控制台中输入此信息。

步骤 **4**：创建控制台代理

直接从NetApp Console创建控制台代理。

关于此任务

- 从控制台创建控制台代理会使用默认配置在 Azure 中部署虚拟机。创建控制台代理后，请勿切换到具有较少 CPU 或较少 RAM 的较小 VM 实例。"了解控制台代理的默认配置" 。
- 当控制台部署控制台代理时，它会创建一个自定义角色并将其分配给控制台代理 VM。此角色包括使控制台代理能够管理 Azure 资源的权限。您需要确保角色保持最新，因为在后续版本中添加了新的权限。"了解有关控制台代理的自定义角色的更多信息" 。

开始之前

您应该具有以下内容：

- Azure 订阅。
- 您选择的 Azure 区域中的 VNet 和子网。
- 如果您的组织需要代理来处理所有传出的互联网流量，请提供关于代理服务器的详细信息：
  - IP 地址
  - 凭据
  - HTTPS 证书
- 如果您想对控制台代理虚拟机使用该身份验证方法，则需要 SSH 公钥。身份验证方法的另一种选择是使用密码。

  "了解如何连接到 Azure 中的 Linux VM"
- 如果您不希望控制台自动为控制台代理创建 Azure 角色，则需要创建自己的"使用此页面上的政策"。

  这些权限适用于控制台代理本身。这与您之前为部署控制台代理虚拟机而设置的权限不同。

步骤

1. 选择“管理 > 代理”。
2. 在“概述”页面上，选择“部署代理”>“Azure”

3. 在*审核*页面上，审核部署代理的要求。这些要求也在本页上方详细说明。
4. 在“虚拟机身份验证”页面上，选择与您设置 Azure 权限的方式相匹配的身份验证选项：
   - 选择*登录*登录您的 Microsoft 帐户，该帐户应具有所需的权限。

     该表单由 Microsoft 拥有并托管。您的凭据未提供给NetApp。

     如果您已经登录 Azure 帐户，则控制台会自动使用该帐户。如果您有多个帐户，那么您可能需要先注销以确保您使用的是正确的帐户。
   - 选择“**Active Directory** 服务主体”以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

   了解如何获取服务主体的这些值 。
5. 在“虚拟机身份验证”页面上，选择 Azure 订阅、位置、新资源组或现有资源组，然后为您正在创建的控制台代理虚拟机选择一种身份验证方法。

   虚拟机的身份验证方法可以是密码或 SSH 公钥。

   "了解如何连接到 Azure 中的 Linux VM"
6. 在“详细信息”页面上，输入代理的名称，指定标签，并选择是否希望控制台创建具有所需权限的新角色，或者是否要选择您设置的现有角色"所需的权限"。

   请注意，您可以选择与此角色关联的 Azure 订阅。您选择的每个订阅都为控制台代理提供管理该订阅中的资源的权限（例如， Cloud Volumes ONTAP）。
7. 在“网络”页面上，选择 VNet 和子网，是否启用公共 IP 地址，并可选择指定代理配置。
   - 在“安全组”页面上，选择是否创建新的安全组或是否选择允许所需入站和出站规则的现有安全组。

     "查看 Azure 的安全组规则" 。
8. 检查您的选择以验证您的设置是否正确。
   a. 默认情况下，*验证代理配置*复选框处于选中状态，以便控制台在您部署时验证网络连接要求。如果控制台无法部署代理，它会提供一份报告来帮助您排除故障。如果部署成功，则不会提供报告。

   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，请取消选中复选框以跳过验证检查。
9. 选择“添加”。

   控制台大约需要 10 分钟才能准备好代理。停留在该页面上直到该过程完成。

结果

该过程完成后，即可从控制台使用控制台代理。

如果部署失败，您可以从控制台下载报告和日志来帮助您解决问题。"了解如何解决安装问题。"

如果您在创建控制台代理的同一 Azure 帐户中拥有 Azure Blob 存储，您将看到 Azure Blob 存储自动出现在 系统 页面上。 "了解如何通过NetApp Console管理 Azure Blob 存储"

从 **Azure** 市场创建控制台代理

您可以直接从 Azure 市场在 Azure 中创建控制台代理。要从 Azure 市场创建控制台代理，您需要设置网络、准备 Azure 权限、查看实例要求，然后创建控制台代理。

开始之前

- 你应该有一个"了解控制台代理"。
- 审查"控制台代理限制"。

步骤 **1**：设置网络

确保您计划安装控制台代理的网络位置支持以下要求。这些要求使控制台代理能够管理混合云中的资源。

Azure 区域

如果您使用Cloud Volumes ONTAP，则控制台代理应部署在与其管理的Cloud Volumes ONTAP系统相同的 Azure 区域中，或者部署在 "Azure 区域对"适用于Cloud Volumes ONTAP系统。此要求确保在Cloud Volumes ONTAP及其关联的存储帐户之间使用 Azure Private Link 连接。

"了解Cloud Volumes ONTAP如何使用 Azure Private Link"

VNet 和子网

创建控制台代理时，您需要指定它所在的 VNet 和子网。

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。

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
\ 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。

端点	目的
\ 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。
\ 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"

创建控制台代理后实现网络要求。

步骤 **2**：查看 **VM** 要求

创建控制台代理时，请选择满足以下要求的虚拟机类型。

CPU

8 个核心或 8 个 vCPU

RAM

32 GB

Azure VM 大小

满足 CPU 和 RAM 要求的实例类型。 NetApp推荐 Standard_D8s_v3。

步骤 **3**：设置权限

您可以通过以下方式提供权限：

- 选项 1：使用系统分配的托管标识为 Azure VM 分配自定义角色。
- 选项 2：向控制台提供具有所需权限的 Azure 服务主体的凭据。

按照以下步骤设置控制台的权限。

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"

步骤

1. 如果您计划在自己的主机上手动安装该软件，请在 VM 上启用系统分配的托管标识，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 VM 上的 Azure 资源配置托管标识"

2. 复制"连接器的自定义角色权限"并将它们保存在 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。

   您应该为想要与NetApp Console一起使用的每个 Azure 订阅添加 ID。

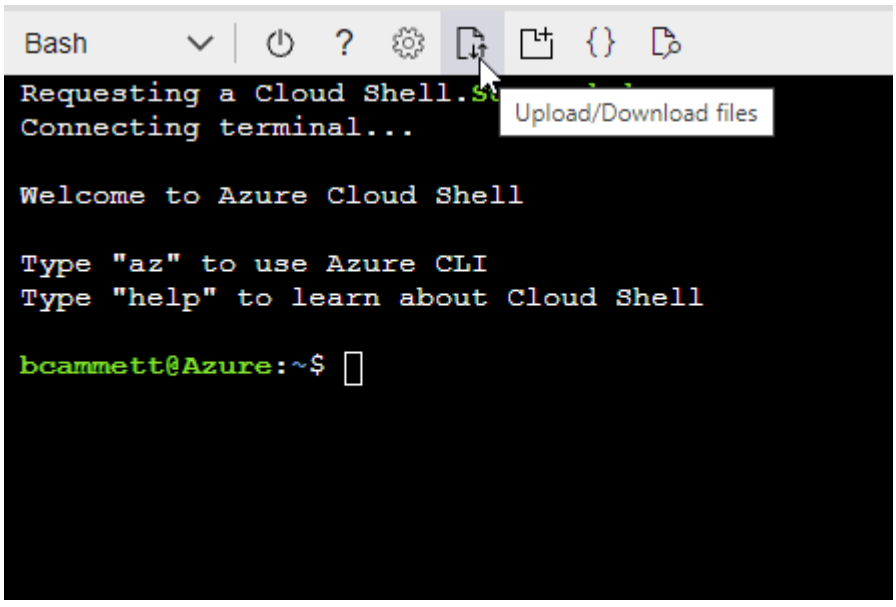
   例子

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

4. 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。

   a. 开始 "Azure 云外壳"并选择 Bash 环境。
   b. 上传 JSON 文件。



c. 使用 Azure CLI 创建自定义角色：

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

服务主体

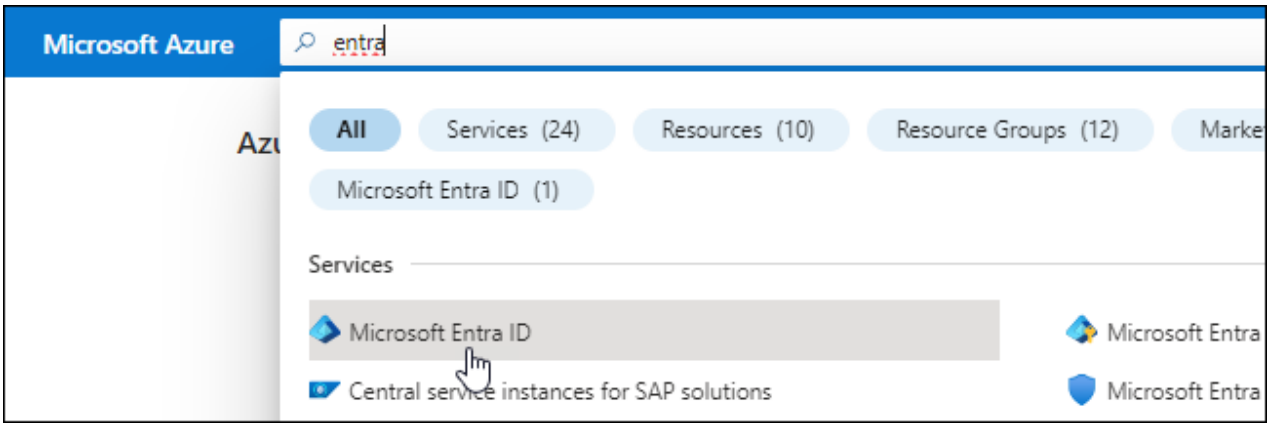
在 Microsoft Entra ID 中创建并设置服务主体，并获取控制台所需的 Azure 凭据。

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。

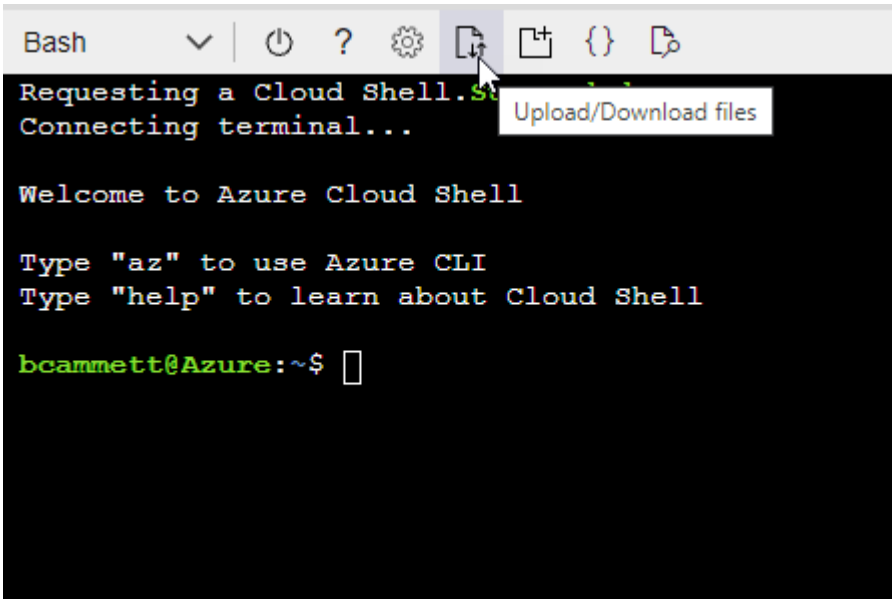
例子

```
"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。

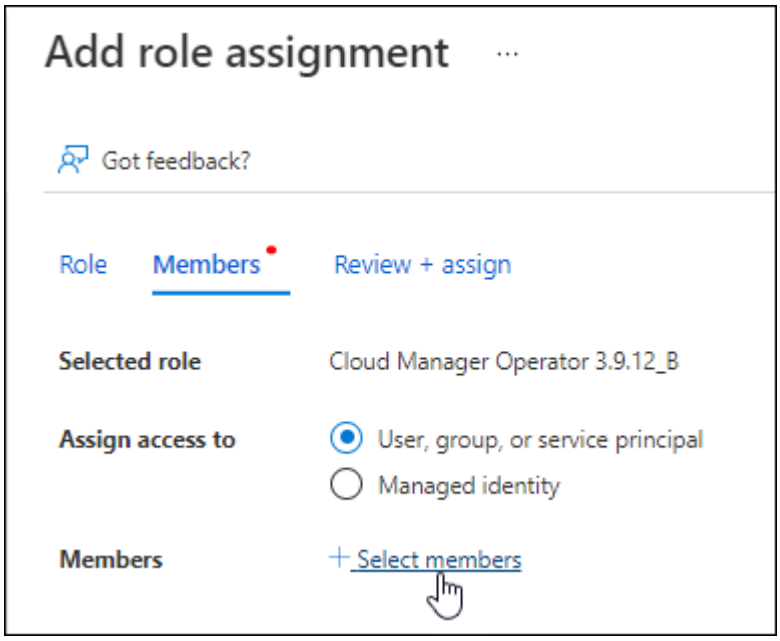
b. 选择订阅。

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*。

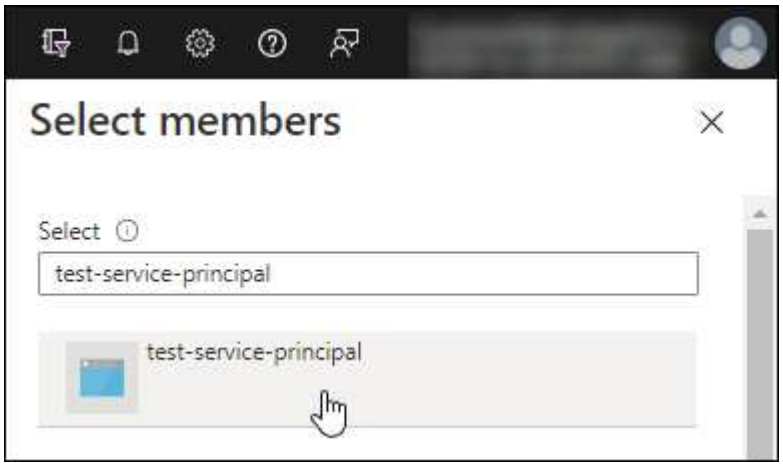
e. 在“成员”选项卡中，完成以下步骤：

- 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”。

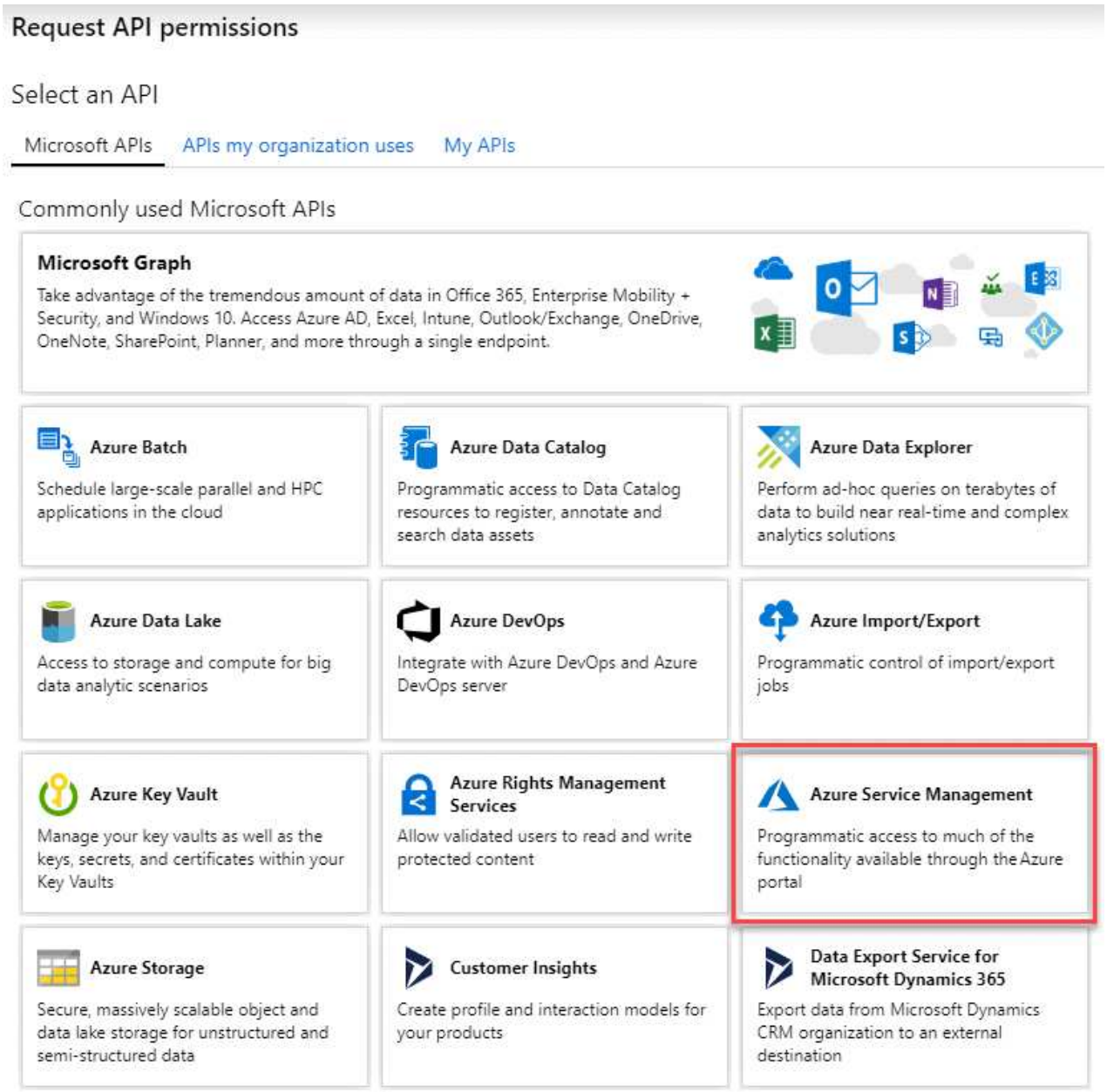
f. 选择*审阅+分配*。

服务主体现在具有部署控制台代理所需的 Azure 权限。

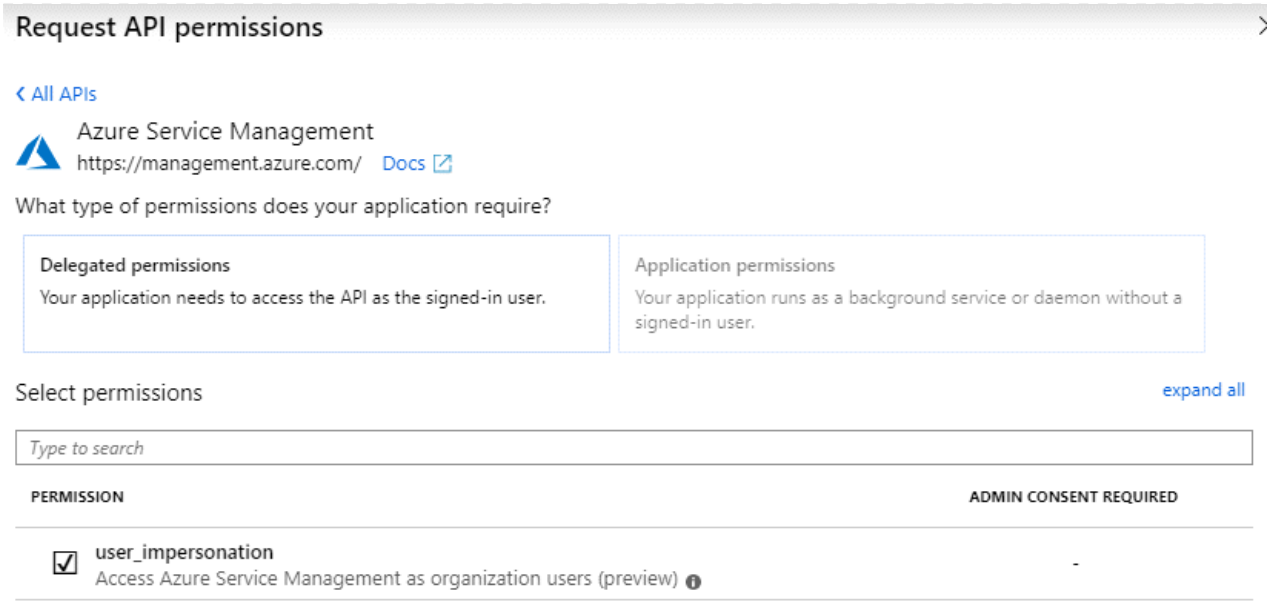
如果您想从多个 Azure 订阅部署Cloud Volumes ONTAP ，则必须将服务主体绑定到每个订阅。在NetApp Console中，您可以选择部署Cloud Volumes ONTAP时要使用的订阅。

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”。

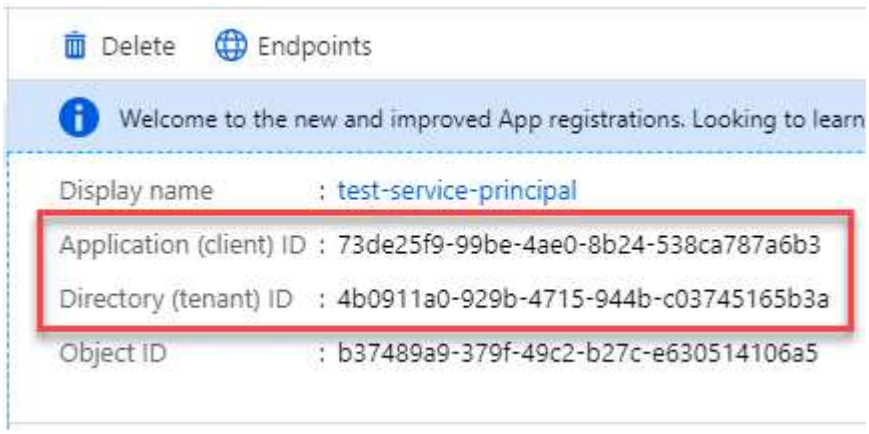


4. 选择*以组织用户身份访问 Azure 服务管理*，然后选择*添加权限*。



获取应用程序的应用程序**ID**和目录**ID**

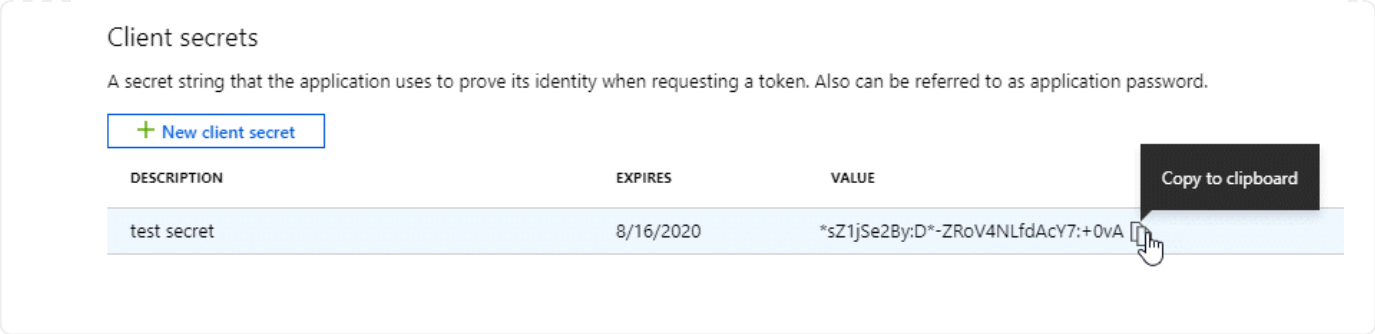
1. 在*Microsoft Entra ID*服务中，选择*App Registrations*并选择应用程序。
2. 复制*应用程序（客户端）ID*和*目录（租户）ID*。



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。



步骤 **4**：创建控制台代理

直接从 Azure 市场启动控制台代理。

关于此任务

从 Azure 市场创建控制台代理会设置具有默认配置的虚拟机。"了解控制台代理的默认配置" 。

开始之前

您应该具有以下内容：

- Azure 订阅。
- 您选择的 Azure 区域中的 VNet 和子网。
- 如果您的组织需要代理来处理所有传出的互联网流量，请提供关于代理服务器的详细信息：
  - IP 地址
  - 凭据
  - HTTPS 证书
- 如果您想对控制台代理虚拟机使用该身份验证方法，则需要 SSH 公钥。身份验证方法的另一种选择是使用密码。

  "了解如何连接到 Azure 中的 Linux VM"

- 如果您不希望控制台自动为控制台代理创建 Azure 角色，则需要创建自己的"使用此页面上的政策"。

  这些权限适用于控制台代理实例本身。这与您之前为部署控制台代理虚拟机而设置的权限不同。

步骤

1. 转到 Azure 市场中的NetApp Console代理 VM 页面。

   "商业区域的 Azure 市场页面"

2. 选择*立即获取*，然后选择*继续*。
3. 从 Azure 门户中，选择“创建”并按照步骤配置虚拟机。

   配置虚拟机时请注意以下事项：

   - **VM** 大小：选择满足 CPU 和 RAM 要求的 VM 大小。我们推荐 Standard_D8s_v3。

- 磁盘：控制台代理可以通过 HDD 或 SSD 磁盘实现最佳性能。
- 网络安全组：控制台代理需要使用 SSH、HTTP 和 HTTPS 的入站连接。

  "查看 Azure 的安全组规则" 。

- 身份*：在*管理*下，选择*启用系统分配的托管身份*。

  此设置很重要，因为托管身份允许控制台代理虚拟机向 Microsoft Entra ID 标识自己，而无需提供任何凭据。 "详细了解 Azure 资源的托管标识" 。

4. 在“审查 + 创建”页面上，审查您的选择并选择“创建”以开始部署。

   Azure 使用指定的设置部署虚拟机。您应该会在大约十分钟内看到虚拟机和控制台代理软件运行。

   如果安装失败，您可以查看日志和报告来帮助您排除故障。"了解如何解决安装问题。"

5. 从连接到控制台代理虚拟机的主机打开 Web 浏览器并输入以下 URL：

   https://ipaddress

6. 登录后，设置控制台代理：
   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。

      保持限制模式处于禁用状态以便在标准模式下使用控制台。仅当您拥有安全的环境并希望断开此帐户与控制台后端服务的连接时，才应启用受限模式。如果真是这样的话，"按照步骤开始在受限模式下使用控制台" 。

   d. 选择*让我们开始吧*。

结果

现在您已经安装了控制台代理并将其与您的控制台组织一起设置。

如果您在创建控制台代理的同一 Azure 订阅中拥有 Azure Blob 存储，您将看到 Azure Blob 存储系统自动出现在“系统”页面上。 "了解如何从控制台管理 Azure Blob 存储"

步骤 **5**：向控制台代理提供权限

现在您已经创建了控制台代理，您需要为其提供之前设置的权限。提供权限使控制台代理能够管理 Azure 中的数据和存储基础结构。

自定义角色

转到 Azure 门户并将 Azure 自定义角色分配给一个或多个订阅的控制台代理虚拟机。

步骤

1. 从 Azure 门户打开“订阅”服务并选择您的订阅。

   从*订阅*服务分配角色很重要，因为这指定了订阅级别的角色分配范围。 _范围_定义了访问适用的资源集。如果您在不同级别（例如，虚拟机级别）指定范围，则您在NetApp Console内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 (IAM)* > 添加 > 添加角色分配。
3. 在*角色*选项卡中，选择*控制台操作员*角色并选择*下一步*。

   控制台操作员是策略中提供的默认名称。如果您为角色选择了不同的名称，则选择该名称。

4. 在“成员”选项卡中，完成以下步骤：
   a. 分配对*托管身份*的访问权限。
   b. 选择“选择成员”，选择创建控制台代理虚拟机的订阅，在“托管标识”下，选择“虚拟机”，然后选择控制台代理虚拟机。
   c. 选择*选择*。
   d. 选择“下一步”。
   e. 选择*审阅+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。

下一步是什么?

前往 "NetApp Console"开始使用控制台代理。

服务主体

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

控制台现在具有代表您在 Azure 中执行操作所需的权限。

在 Azure 中手动安装控制台代理

要在您自己的 Linux 主机上手动安装控制台代理，您需要查看主机要求、设置网络、准备 Azure 权限、安装控制台代理，然后提供您准备好的权限。

开始之前

- 你应该有一个"了解控制台代理"。
- 你应该回顾一下"控制台代理限制"。

步骤 1：查看主机要求

控制台代理软件必须在满足特定操作系统要求、RAM 要求、端口要求等的主机上运行。

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。

Azure VM 大小

满足 CPU 和 RAM 要求的实例类型。 NetApp推荐 Standard_D8s_v3。

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

步骤 **2**：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 **2.** 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
```

步骤 **3**：设置网络

确保您计划安装控制台代理的网络位置支持以下要求。满足这些要求使控制台代理能够管理混合云环境中的资源和流程。

Azure 区域

如果您使用Cloud Volumes ONTAP，则控制台代理应部署在与其管理的Cloud Volumes ONTAP系统相同的 Azure 区域中，或者部署在 "Azure 区域对"适用于Cloud Volumes ONTAP系统。此要求确保在Cloud Volumes ONTAP及其关联的存储帐户之间使用 Azure Private Link 连接。

"了解Cloud Volumes ONTAP如何使用 Azure Private Link"

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。

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"

步骤 **4**：设置控制台代理部署权限

您需要使用以下选项之一向控制台代理提供 Azure 权限：

- 选项 1：使用系统分配的托管标识为 Azure VM 分配自定义角色。
- 选项 2：向控制台代理提供具有所需权限的 Azure 服务主体的凭据。

按照步骤为控制台代理准备权限。

为控制台代理部署创建自定义角色

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"

步骤

1. 如果您计划在自己的主机上手动安装该软件，请在 VM 上启用系统分配的托管标识，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 VM 上的 Azure 资源配置托管标识"

2. 复制"连接器的自定义角色权限"并将它们保存在 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。

   您应该为想要与NetApp Console一起使用的每个 Azure 订阅添加 ID。

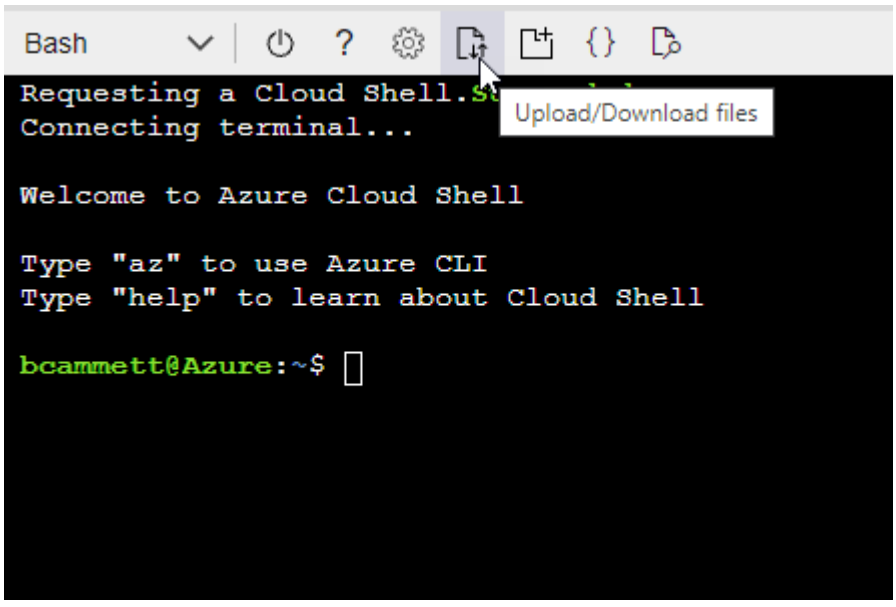
   例子

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

4. 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。

   a. 开始 "Azure 云外壳"并选择 Bash 环境。
   b. 上传 JSON 文件。



c. 使用 Azure CLI 创建自定义角色：

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

服务主体

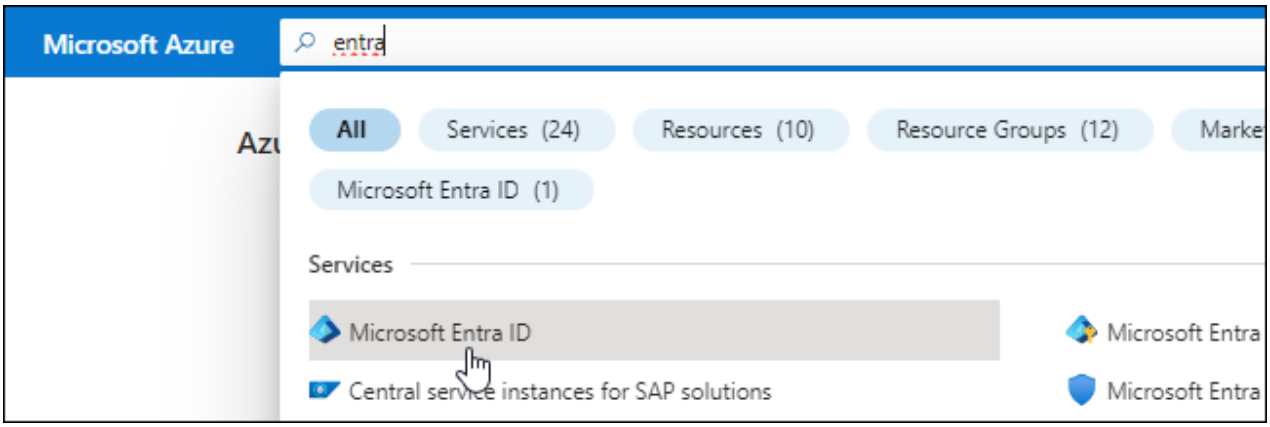
在 Microsoft Entra ID 中创建并设置服务主体，并获取控制台代理所需的 Azure 凭据。

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。

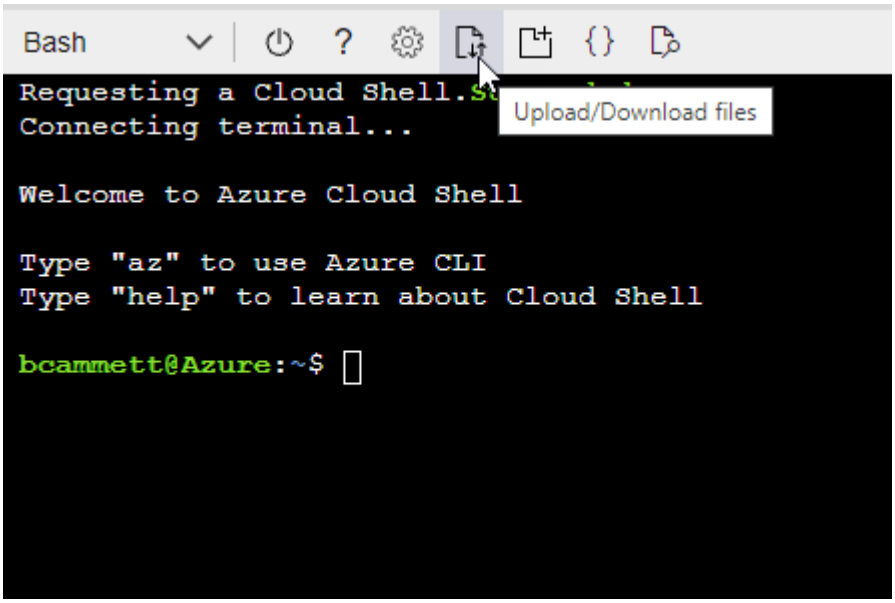
例子

```
"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。

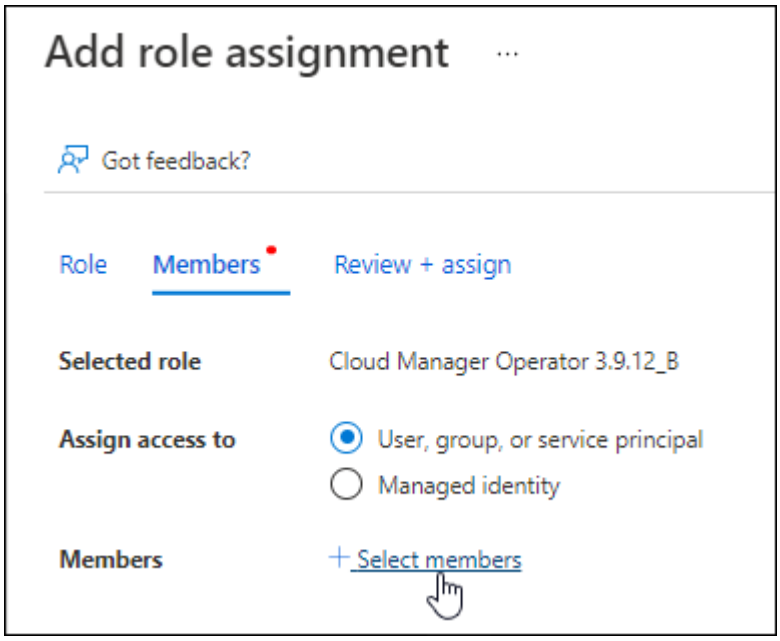
b. 选择订阅。

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*。

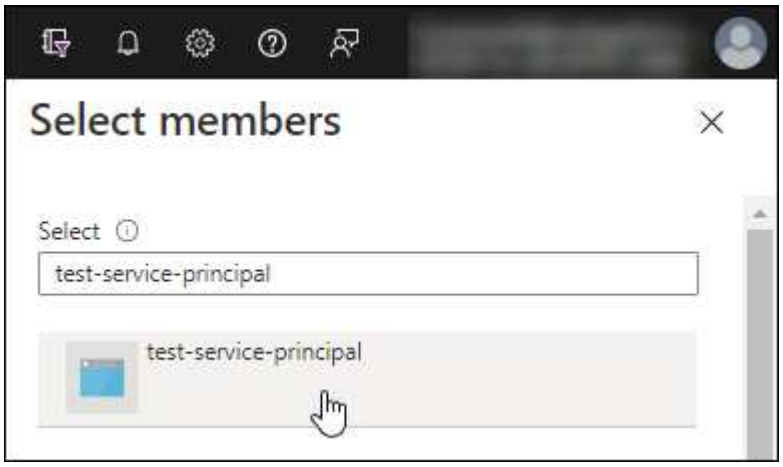
e. 在“成员”选项卡中，完成以下步骤：

- 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”。

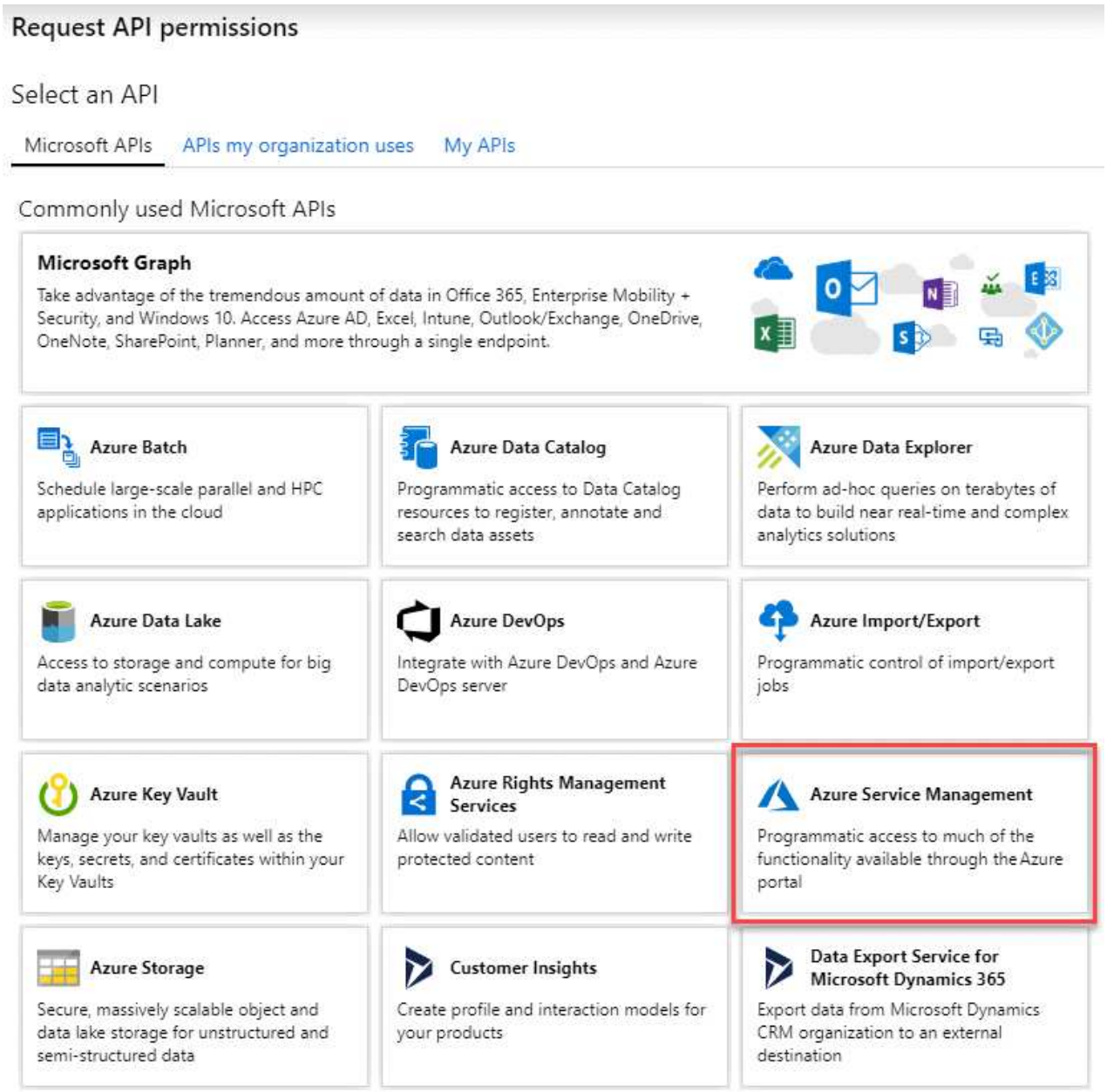
f. 选择*审阅+分配*。

服务主体现在具有部署控制台代理所需的 Azure 权限。

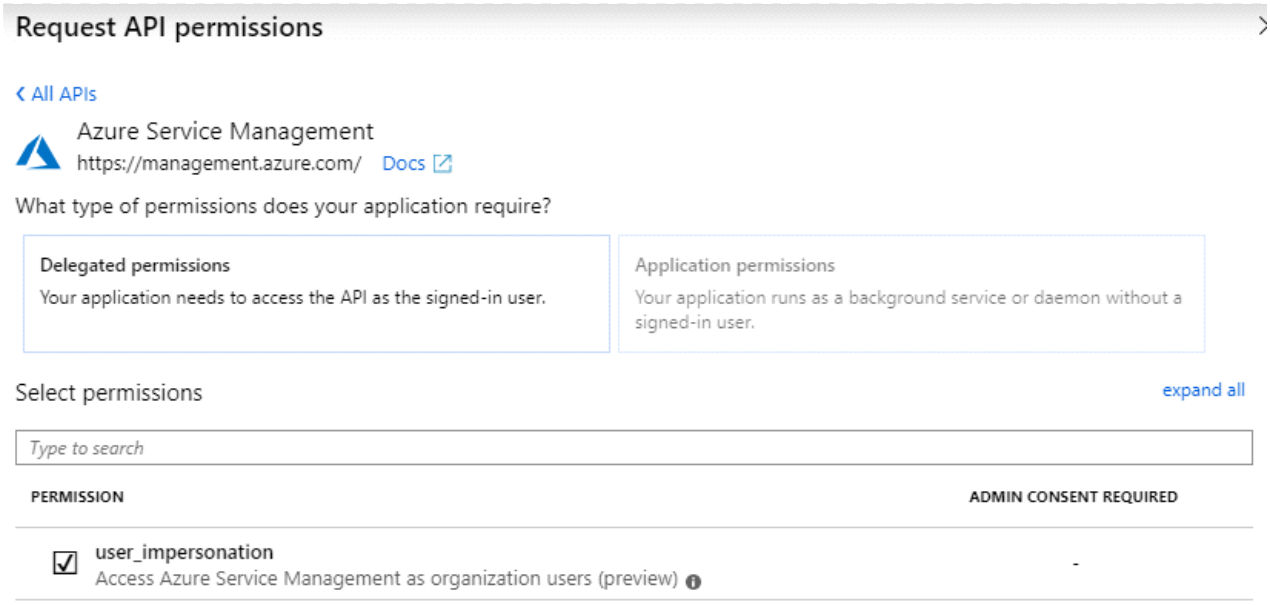
如果您想从多个 Azure 订阅部署Cloud Volumes ONTAP ，则必须将服务主体绑定到每个订阅。在NetApp Console中，您可以选择部署Cloud Volumes ONTAP时要使用的订阅。

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”。

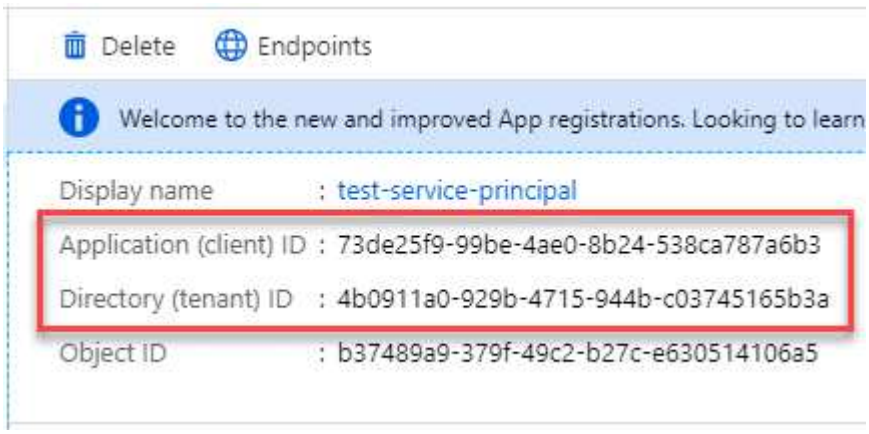


4. 选择*以组织用户身份访问 Azure 服务管理*，然后选择*添加权限*。



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。

结果

您的服务主体现已设置，您应该已经复制了应用程序（客户端）ID、目录（租户）ID 和客户端机密的值。添加 Azure 帐户时，您需要在控制台中输入此信息。

步骤 **5**：安装控制台代理

前提条件完成后，您可以在自己的 Linux 主机上手动安装该软件。

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"。

- 在 Azure 中的 VM 上启用托管标识，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 VM 上的 Azure 资源配置托管标识"

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来访问互联网，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。如果您有明确的代理服务器，则需要按所示方式输入参数。

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控制台代理配置为使用 HTTP 或 HTTPS 代理服务器：

- http://地址:端口
- http://用户名:密码@地址:端口
- http://域名%92用户名:密码@地址:端口
- https://地址:端口
- https://用户名:密码@地址:端口
- https://域名%92用户名:密码@地址:端口

  请注意以下事项：

  - 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 代码，如上所示。
  - 控制台代理不支持包含 @ 字符的用户名或密码。
  - 如果密码包含以下任何特殊字符，则必须在该特殊字符前面加上反斜杠来转义该特殊字符：& 或 !

例如：

http://bxpproxyuser:netapp1\!@地址:3128

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"

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。
2. 等待安装完成。

   安装结束时，如果您指定了代理服务器，控制台代理服务 (occm) 将重新启动两次。

如果安装失败，您可以查看安装报告和日志来帮助您解决问题。"了解如何解决安装问题。"

1. 从连接到控制台代理虚拟机的主机打开 Web 浏览器并输入以下 URL：

   https://ipaddress

2. 登录后，设置控制台代理：
   a. 指定与控制台代理关联的组织。
   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。

      您应该保持限制模式处于禁用状态，因为这些步骤描述了如何在标准模式下使用控制台。仅当您拥有安全的环境并希望断开此帐户与后端服务的连接时，才应启用受限模式。如果真是这样的话，"按照步骤在受限模式下开始使用NetApp Console" 。

   d. 选择*让我们开始吧*。

如果您在创建控制台代理的同一 Azure 订阅中拥有 Azure Blob 存储，您将看到 Azure Blob 存储系统自动出现在“系统”页面上。 "了解如何通过NetApp Console管理 Azure Blob 存储"

步骤 **6**：提供对**NetApp Console**的权限

现在您已经安装了控制台代理，您需要为控制台代理提供您之前设置的 Azure 权限。提供权限使控制台能够管理 Azure 中的数据和存储基础结构。

自定义角色

转到 Azure 门户并将 Azure 自定义角色分配给一个或多个订阅的控制台代理虚拟机。

步骤

1. 从 Azure 门户打开“订阅”服务并选择您的订阅。

   从*订阅*服务分配角色很重要，因为这指定了订阅级别的角色分配范围。 _范围_定义了访问适用的资源集。如果您在不同级别（例如，虚拟机级别）指定范围，则您在NetApp Console内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 (IAM)* > 添加 > 添加角色分配。
3. 在*角色*选项卡中，选择*控制台操作员*角色并选择*下一步*。

   控制台操作员是策略中提供的默认名称。如果您为角色选择了不同的名称，则选择该名称。

4. 在“成员”选项卡中，完成以下步骤：
   a. 分配对*托管身份*的访问权限。
   b. 选择“选择成员”，选择创建控制台代理虚拟机的订阅，在“托管标识”下，选择“虚拟机”，然后选择控制台代理虚拟机。
   c. 选择*选择*。
   d. 选择“下一步”。
   e. 选择*审阅+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。

下一步是什么?

前往 "NetApp Console"开始使用控制台代理。

服务主体

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。

Google Cloud

Google Cloud 中的控制台代理安装选项

有几种不同的方法可以在 Google Cloud 中创建控制台代理。直接从NetApp Console是最常见的方式。 ---

有以下安装选项可用：

- "直接从控制台创建控制台代理"（这是标准选项）

  此操作将在您选择的 VPC 中启动运行 Linux 和控制台代理软件的 VM 实例。

- "使用 Google Platform 创建控制台代理"

  此操作还会启动运行 Linux 和控制台代理软件的 VM 实例，但部署直接从 Google Cloud 启动，而不是从控制台启动。

- "在您自己的Linux主机上下载并手动安装软件"

您选择的安装选项会影响您如何准备安装。这包括如何向控制台提供验证身份和管理 Google Cloud 中的资源所需的权限。

通过NetApp Console在 Google Cloud 中创建控制台代理

您可以从控制台在 Google Cloud 中创建控制台代理。您需要设置网络、准备 Google Cloud 权限、启用 Google Cloud API，然后创建控制台代理。

开始之前

- 你应该有一个"了解控制台代理"。
- 你应该回顾一下"控制台代理限制"。

步骤 1：设置网络

设置网络以确保控制台代理可以管理资源，并连接到目标网络和出站互联网访问。

VPC 和子网

创建控制台代理时，您需要指定它所在的 VPC 和子网。

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。

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
\ 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://config.googleapis.com/v1/projects	管理 Google Cloud 中的资源。
\ 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。

从**NetApp**控制台联系的端点

当您使用通过 SaaS 层提供的基于 Web 的NetApp Console时，它会联系多个端点来完成数据管理任务。这包括从控制台联系以部署控制台代理的端点。

"查看从NetApp控制台联系的端点列表" 。

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"

创建控制台代理后实现此网络需求。

步骤 **2**：设置权限以创建控制台代理

在从控制台部署控制台代理之前，您需要为部署控制台代理 VM 的 Google 平台用户设置权限。

步骤

1. 在 Google 平台中创建自定义角色：

   a. 创建包含以下权限的 YAML 文件：

```
title: Console agent deployment policy
description: Permissions for the user who deploys the Console agent
stage: GA
includedPermissions:

- cloudbuild.builds.get
- 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
- config.deployments.create
- config.operations.get
- config.deployments.delete
- config.deployments.deleteState
- config.deployments.get
- config.deployments.getState
- config.deployments.list
- config.deployments.update
- config.deployments.updateState
- config.previews.get
- config.previews.list
- config.revisions.get
- config.resources.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.actAs
- iam.serviceAccounts.create
- iam.serviceAccounts.list
- iam.serviceAccountKeys.create
- storage.buckets.create
- storage.buckets.get
```

```
- storage.objects.create
- storage.folders.create
- storage.objects.list
```

b. 从 Google Cloud 激活云壳。

c. 上传包含所需权限的 YAML 文件。

d. 使用创建自定义角色 `gcloud iam roles create`命令。

以下示例在项目级别创建一个名为“agentDeployment”的角色：

gcloud iam roles create connectorDeployment --project=myproject --file=agent-deployment.yaml

"Google Cloud 文档：创建和管理自定义角色"

2. 将此自定义角色分配给将从控制台或使用 gcloud 部署控制台代理的用户。

"Google Cloud 文档：授予单个角色"

步骤 **3**：创建一个 **Google Cloud** 服务帐户以与代理一起使用。

需要一个 Google Cloud 服务帐号来向控制台代理提供控制台管理 Google Cloud 中的资源所需的权限。创建控制台代理时，您需要将此服务帐户与控制台代理 VM 关联。

在后续版本中添加新权限时，您有责任更新自定义角色。如果需要新的权限，它们将在发行说明中列出。

步骤

1. 在 Google Cloud 中创建自定义角色：

a. 创建一个包含以下内容的 YAML 文件"控制台代理的服务帐户权限"。

b. 从 Google Cloud 激活云壳。

c. 上传包含所需权限的 YAML 文件。

d. 使用创建自定义角色 `gcloud iam roles create`命令。

以下示例在项目级别创建一个名为“agent”的角色：

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

"Google Cloud 文档：创建和管理自定义角色"

2. 在 Google Cloud 中创建服务帐号并将角色分配给该服务帐号：

a. 从 IAM 和管理服务中，选择 服务帐户 > 创建服务帐户。

b. 输入服务帐户详细信息并选择*创建并继续*。

c. 选择您刚刚创建的角色。

d. 完成剩余步骤以创建角色。

"Google Cloud 文档：创建服务帐号"

3. 如果您计划在与控制台代理所在项目不同的项目中部署Cloud Volumes ONTAP系统，则需要为控制台代理的服务帐户提供对这些项目的访问权限。

   例如，假设控制台代理位于项目 1 中，而您想要在项目 2 中创建Cloud Volumes ONTAP系统。您需要授予项目 2 中的服务帐户访问权限。

   a. 从 IAM 和管理服务中，选择您想要创建Cloud Volumes ONTAP系统的 Google Cloud 项目。

   b. 在 **IAM** 页面上，选择 授予访问权限 并提供所需的详细信息。

      - 输入控制台代理服务帐户的电子邮件。
      - 选择控制台代理的自定义角色。
      - 选择*保存*。

   有关详细信息，请参阅 "Google Cloud 文档"

步骤 **4**：设置共享 **VPC** 权限

如果您使用共享 VPC 将资源部署到服务项目中，则需要准备好您的权限。

此表仅供参考，当 IAM 配置完成时，您的环境应该反映权限表。

查看共享 **VPC** 权限

身份	创造者	主办地点	服务项目权限	宿主项目权限	目的
Google 帐户部署代理	自定义	服务项目	"代理部署策略"	计算.网络用户	在服务项目中部署代理
代理服务账户	自定义	服务项目	"代理服务帐户策略"	计算.网络用户部署管理器.编辑器	部署和维护服务项目中的Cloud Volumes ONTAP和服务
Cloud Volumes ONTAP 服务帐户	自定义	服务项目	storage.admin 成员： NetApp Console服务帐户作为 serviceAccount.user	不适用	（可选）适用于NetApp Cloud Tiering和NetApp Backup and Recovery
Google API 服务代理	Google Cloud	服务项目	（默认）编辑器	计算.网络用户	代表部署与 Google Cloud API 进行交互。允许控制台使用共享网络。
Google Compute Engine 默认服务帐户	Google Cloud	服务项目	（默认）编辑器	计算.网络用户	代表部署部署 Google Cloud 实例和计算基础架构。允许控制台使用共享网络。

注：

1. 如果您没有将防火墙规则传递给部署并选择让控制台为您创建规则，则仅主机项目才需要 deploymentmanager.editor。如果未指定规则， NetApp Console将在主机项目中创建一个包含 VPC0 防火墙规则的部署。
2. 仅当您未将防火墙规则传递给部署并选择让控制台为您创建它们时，才需要firewall.create 和firewall.delete。这些权限位于控制台帐户 .yaml 文件中。如果您使用共享 VPC 部署 HA 对，这些权限将用于为 VPC1、2 和 3 创建防火墙规则。对于所有其他部署，这些权限也将用于为 VPC0 创建规则。
3. 对于 Cloud Tiering，分层服务帐户必须在服务帐户上具有 serviceAccount.user 角色，而不仅仅是在项目级别。目前，如果您在项目级别分配 serviceAccount.user，则使用 getIAMPolicy 查询服务帐户时不会显示权限。

步骤 **5**：启用 **Google Cloud API**

在部署控制台代理和Cloud Volumes ONTAP之前，您必须启用多个 Google Cloud API。

步骤

1. 在您的项目中启用以下 Google Cloud API：
   - 云基础设施管理器 API
   - 云部署管理器 V2 API
   - 云日志 API

- 云资源管理器 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NetApp Backup and Recovery与客户管理加密密钥 (CMEK) 结合使用时才需要）

"Google Cloud 文档：启用 API"

步骤 **6**：创建控制台代理

直接从控制台创建控制台代理。

创建控制台代理会使用默认配置在 Google Cloud 中部署虚拟机实例。创建控制台代理后，请勿切换到具有较少 CPU 或较少 RAM 的较小 VM 实例。"了解控制台代理的默认配置" 。

在 Google Cloud 中部署代理时，代理会创建一个存储桶来存储部署文件。

开始之前

您应该具有以下内容：

- 创建控制台代理所需的 Google Cloud 权限以及控制台代理虚拟机的服务帐号。
- 满足组网需求的VPC及子网。
- 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。

步骤

1. 选择“管理 **>** 代理”。
2. 在“概览”页面上，选择“部署代理”>“Google Cloud”
3. 在*部署代理*页面上，查看您需要的详细信息。您有两个选择：
   a. 选择“继续”以使用产品内指南准备部署。产品内指南中的每个步骤都包含文档此页面上的信息。
   b. 如果您已按照此页面上的步骤做好准备，请选择“跳至部署”。
4. 按照向导中的步骤创建控制台代理：
   - 如果出现提示，请登录您的 Google 帐户，该帐户应该具有创建虚拟机实例所需的权限。

     该表单由 Google 拥有并托管。您的凭据未提供给NetApp。

   - 详细信息：输入虚拟机实例的名称，指定标签，选择项目，然后选择具有所需权限的服务帐户（有关详细信息，请参阅上面的部分）。
   - 位置：指定实例的区域、区域、VPC 和子网。
   - 网络：选择是否启用公共 IP 地址并选择性地指定代理配置。
   - 网络标签：如果使用透明代理，则向控制台代理实例添加网络标签。网络标签必须以小写字母开头，并且可以包含小写字母、数字和连字符。标签必须以小写字母或数字结尾。例如，您可以使用标签“console-agent-proxy”。

- 防火墙策略：选择是否创建新的防火墙策略，或者是否选择允许所需入站和出站规则的现有防火墙策略。

  "Google Cloud 中的防火墙规则"

5. 检查您的选择以验证您的设置是否正确。

   a. 默认情况下，*验证代理配置*复选框处于选中状态，以便控制台在您部署时验证网络连接要求。如果控制台无法部署代理，它会提供一份报告来帮助您排除故障。如果部署成功，则不会提供报告。

   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，请取消选中复选框以跳过验证检查。

6. 选择“添加”。

   代理大约需要 10 分钟才能准备就绪；请停留在页面上直到该过程完成。

结果

该过程完成后，控制台代理即可使用。

如果部署失败，您可以从控制台下载报告和日志来帮助您解决问题。"了解如何解决安装问题。"

如果您在创建控制台代理的同一 Google Cloud 帐户中拥有 Google Cloud Storage 存储桶，您将看到 Google Cloud Storage 系统自动出现在 **Systems** 页面上。 "了解如何通过控制台管理 Google 云端存储"

从 **Google Cloud** 创建控制台代理

要使用 Google Cloud 在 Google Cloud 中创建控制台代理，您需要设置网络、准备 Google Cloud 权限、启用 Google Cloud API，然后创建控制台代理。

开始之前

- 你应该有一个"了解控制台代理"。
- 你应该回顾一下"控制台代理限制"。

步骤 **1**：设置网络

设置网络以使控制台代理能够管理资源并连接到目标网络和互联网。

VPC 和子网

创建控制台代理时，您需要指定它所在的 VPC 和子网。

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。

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
\ 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://config.googleapis.com/v1/projects	管理 Google Cloud 中的资源。
\ 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。
\ 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。

从**NetApp**控制台联系的端点

当您使用通过 SaaS 层提供的基于 Web 的NetApp Console时，它会联系多个端点来完成数据管理任务。这包括从控制台联系以部署控制台代理的端点。

"查看从NetApp控制台联系的端点列表" 。

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"

创建控制台代理后实现此网络需求。

步骤 **2**：设置权限以创建控制台代理

为 Google Cloud 用户设置权限以从 Google Cloud 部署控制台代理虚拟机。

步骤

1. 在 Google 平台中创建自定义角色：

   a. 创建包含以下权限的 YAML 文件：

```
title: Console agent deployment policy
description: Permissions for the user who deploys the Console
agent
stage: GA
includedPermissions:

- cloudbuild.builds.get
- 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
- config.deployments.create
```

```
- config.operations.get
- config.deployments.delete
- config.deployments.deleteState
- config.deployments.get
- config.deployments.getState
- config.deployments.list
- config.deployments.update
- config.deployments.updateState
- config.previews.get
- config.previews.list
- config.revisions.get
- config.resources.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.actAs
- iam.serviceAccounts.create
- iam.serviceAccounts.list
- iam.serviceAccountKeys.create
- storage.buckets.create
- storage.buckets.get
- storage.objects.create
- storage.folders.create
- storage.objects.list
```

b. 从 Google Cloud 激活云壳。

c. 上传包含所需权限的 YAML 文件。

d. 使用创建自定义角色 `gcloud iam roles create`命令。

以下示例在项目级别创建一个名为“connectorDeployment”的角色：

gcloud iam 角色创建 connectorDeployment --project=myproject --file=connector-deployment.yaml

"Google Cloud 文档：创建和管理自定义角色"

2. 将此自定义角色分配给从 Google Cloud 部署控制台代理的用户。

"Google Cloud 文档：授予单个角色"

步骤 **3**：设置控制台代理操作的权限

需要一个 Google Cloud 服务帐号来向控制台代理提供控制台管理 Google Cloud 中的资源所需的权限。创建控制台代理时，您需要将此服务帐户与控制台代理 VM 关联。

在后续版本中添加新权限时，您有责任更新自定义角色。如果需要新的权限，它们将在发行说明中列出。

步骤

1. 在 Google Cloud 中创建自定义角色：

   a. 创建一个包含以下内容的 YAML 文件"控制台代理的服务帐户权限"。

   b. 从 Google Cloud 激活云壳。

   c. 上传包含所需权限的 YAML 文件。

   d. 使用创建自定义角色 `gcloud iam roles create`命令。

   以下示例在项目级别创建一个名为“agent”的角色：

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

   "Google Cloud 文档：创建和管理自定义角色"

2. 在 Google Cloud 中创建服务帐号并将角色分配给该服务帐号：

   a. 从 IAM 和管理服务中，选择 服务帐户 **>** 创建服务帐户。

   b. 输入服务帐户详细信息并选择*创建并继续*。

   c. 选择您刚刚创建的角色。

   d. 完成剩余步骤以创建角色。

   "Google Cloud 文档：创建服务帐号"

3. 如果您计划在与控制台代理所在项目不同的项目中部署Cloud Volumes ONTAP系统，则需要为控制台代理的服务帐户提供对这些项目的访问权限。

   例如，假设控制台代理位于项目 1 中，而您想要在项目 2 中创建Cloud Volumes ONTAP系统。您需要授予项目 2 中的服务帐户访问权限。

   a. 从 IAM 和管理服务中，选择您想要创建Cloud Volumes ONTAP系统的 Google Cloud 项目。

   b. 在 **IAM** 页面上，选择 授予访问权限 并提供所需的详细信息。

- 输入控制台代理服务帐户的电子邮件。
- 选择控制台代理的自定义角色。
- 选择*保存*。

有关详细信息，请参阅 "Google Cloud 文档"

步骤 **4**：设置共享 **VPC** 权限

如果您使用共享 VPC 将资源部署到服务项目中，则需要准备好您的权限。

此表仅供参考，当 IAM 配置完成时，您的环境应该反映权限表。

查看共享 **VPC** 权限

身份	创造者	主办地点	服务项目权限	宿主项目权限	目的
Google 帐户部署代理	自定义	服务项目	"代理部署策略"	计算.网络用户	在服务项目中部署代理
代理服务账户	自定义	服务项目	"代理服务帐户策略"	计算.网络用户部署管理器.编辑器	部署和维护服务项目中的Cloud Volumes ONTAP和服务
Cloud Volumes ONTAP 服务帐户	自定义	服务项目	storage.admin 成员： NetApp Console服务帐户作为 serviceAccount.user	不适用	（可选）适用于NetApp Cloud Tiering和NetApp Backup and Recovery
Google API 服务代理	Google Cloud	服务项目	（默认）编辑器	计算.网络用户	代表部署与 Google Cloud API 进行交互。允许控制台使用共享网络。
Google Compute Engine 默认服务帐户	Google Cloud	服务项目	（默认）编辑器	计算.网络用户	代表部署部署 Google Cloud 实例和计算基础架构。允许控制台使用共享网络。

注：

1. 如果您没有将防火墙规则传递给部署并选择让控制台为您创建规则，则仅主机项目才需要 deploymentmanager.editor。如果未指定规则， NetApp Console将在主机项目中创建一个包含 VPC0 防火墙规则的部署。
2. 仅当您未将防火墙规则传递给部署并选择让控制台为您创建它们时，才需要firewall.create 和firewall.delete。这些权限位于控制台帐户 .yaml 文件中。如果您使用共享 VPC 部署 HA 对，这些权限将用于为 VPC1、2 和 3 创建防火墙规则。对于所有其他部署，这些权限也将用于为 VPC0 创建规则。
3. 对于 Cloud Tiering，分层服务帐户必须在服务帐户上具有 serviceAccount.user 角色，而不仅仅是在项目级别。目前，如果您在项目级别分配 serviceAccount.user，则使用 getIAMPolicy 查询服务帐户时不会显示权限。

步骤 **5**：启用 **Google Cloud API**

在部署控制台代理和Cloud Volumes ONTAP之前，启用多个 Google Cloud API。

步骤

1. 在您的项目中启用以下 Google Cloud API：
   - 云基础设施管理器 API
   - 云部署管理器 V2 API
   - 云日志 API

- 云资源管理器 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NetApp Backup and Recovery与客户管理加密密钥 (CMEK) 结合使用时才需要）

"Google Cloud 文档：启用 API"

步骤 **6**：创建控制台代理

使用 Google Cloud 创建控制台代理。

创建控制台代理会使用默认配置在 Google Cloud 中部署虚拟机实例。创建控制台代理后，请勿切换到具有较少 CPU 或较少 RAM 的较小 VM 实例。"了解控制台代理的默认配置" 。

开始之前

您应该具有以下内容：

- 创建控制台代理所需的 Google Cloud 权限以及控制台代理虚拟机的服务帐号。
- 满足组网需求的VPC及子网。
- 了解 VM 实例要求。
  - **CPU**：8 核或 8 个 vCPU
  - 内存：32 GB
  - 机器类型：我们推荐 n2-standard-8。

    Google Cloud 在具有支持 Shielded VM 功能的操作系统的 VM 实例上支持控制台代理。

步骤

1. 使用您喜欢的方法登录 Google Cloud SDK。

   此示例使用安装了 gcloud SDK 的本地 shell，但您也可以使用 Google Cloud Shell。

   有关 Google Cloud SDK 的更多信息，请访问"Google Cloud SDK 文档页面"。

2. 验证您是否以具有上述部分定义的所需权限的用户身份登录：

   ```
   gcloud auth list
   ```

   输出应显示以下内容，其中 * 用户帐户是要登录的用户帐户：

```
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. 运行 `gcloud compute instances create`命令：

```
gcloud compute instances create <instance-name>
  --machine-type=n2-standard-8
  --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>
```

实例名称
: VM 实例所需的实例名称。

项目
: （可选）您想要部署虚拟机的项目。

服务帐户
: 步骤 2 的输出中指定的服务帐户。

区
: 您想要部署虚拟机的区域

无地址
: （可选）不使用外部 IP 地址（您需要云 NAT 或代理将流量路由到公共互联网）

网络标签
: （可选）添加网络标记，使用标记将防火墙规则链接到控制台代理实例

网络路径

（可选）添加要部署控制台代理的网络名称（对于共享 VPC，您需要完整路径）

子网路径

（可选）添加要部署控制台代理的子网名称（对于共享 VPC，您需要完整路径）

kms 密钥路径

（可选）添加 KMS 密钥来加密控制台代理的磁盘（还需要应用 IAM 权限）

有关这些标志的更多信息，请访问"Google Cloud 计算 SDK 文档"。

运行该命令将部署控制台代理。控制台代理实例和软件应在大约五分钟内运行。

4. 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。

5. 登录后，设置控制台代理：

   a. 指定与控制台代理关联的控制台组织。

      "了解身份和访问管理" 。

   b. 输入系统的名称。

结果

控制台代理现已安装并设置到您的控制台组织。

打开 Web 浏览器并转到 "NetApp Console"开始使用控制台代理。

在 **Google Cloud** 中手动安装控制台代理

要在您自己的 Linux 主机上手动安装控制台代理，您需要查看主机要求、设置网络、准备 Google Cloud 权限、启用 Google Cloud API、安装控制台，然后提供您准备好的权限。

开始之前

- 你应该有一个"了解控制台代理"。
- 你应该回顾一下"控制台代理限制"。

步骤 **1**：查看主机要求

控制台代理软件必须在满足特定操作系统要求、RAM 要求、端口要求等的主机上运行。

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。

Google Cloud 机器类型

满足 CPU 和 RAM 要求的实例类型。NetApp推荐 n2-standard-8。

Google Cloud 虚拟机实例上的控制台代理支持以下操作系统： "受防护的虚拟机功能"

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 。

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
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

Google Cloud 机器类型

满足 CPU 和 RAM 要求的实例类型。NetApp推荐 n2-standard-8。

Google Cloud 虚拟机实例上的控制台代理支持以下操作系统： "受防护的虚拟机功能"

步骤 **2**：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 3. 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
```

步骤 **3**：设置网络

设置您的网络，以便控制台代理可以管理混合云环境中的资源和流程。例如，您需要确保可以连接到目标网络并且可以进行出站互联网访问。

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。

端点	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://config.googleapis.com/v1/projects	管理 Google Cloud 中的资源。
\ 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"

步骤 **4**：设置控制台代理的权限

需要一个 Google Cloud 服务帐号来向控制台代理提供控制台管理 Google Cloud 中的资源所需的权限。创建控制台代理时，您需要将此服务帐户与控制台代理 VM 关联。

在后续版本中添加新权限时，您有责任更新自定义角色。如果需要新的权限，它们将在发行说明中列出。

步骤

1. 在 Google Cloud 中创建自定义角色：

   a. 创建一个包含以下内容的 YAML 文件"控制台代理的服务帐户权限"。

   b. 从 Google Cloud 激活云壳。

   c. 上传包含所需权限的 YAML 文件。

   d. 使用创建自定义角色 `gcloud iam roles create`命令。

      以下示例在项目级别创建一个名为“agent”的角色：

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

   "Google Cloud 文档：创建和管理自定义角色"

2. 在 Google Cloud 中创建服务帐号并将角色分配给该服务帐号：

   a. 从 IAM 和管理服务中，选择 服务帐户 **>** 创建服务帐户。

   b. 输入服务帐户详细信息并选择*创建并继续*。

   c. 选择您刚刚创建的角色。

   d. 完成剩余步骤以创建角色。

      "Google Cloud 文档：创建服务帐号"

3. 如果您计划在与控制台代理所在项目不同的项目中部署Cloud Volumes ONTAP系统，则需要为控制台代理的服务帐户提供对这些项目的访问权限。

   例如，假设控制台代理位于项目 1 中，而您想要在项目 2 中创建Cloud Volumes ONTAP系统。您需要授予项目 2 中的服务帐户访问权限。

   a. 从 IAM 和管理服务中，选择您想要创建Cloud Volumes ONTAP系统的 Google Cloud 项目。

   b. 在 **IAM** 页面上，选择 授予访问权限 并提供所需的详细信息。

      - 输入控制台代理服务帐户的电子邮件。
      - 选择控制台代理的自定义角色。
      - 选择*保存*。

   有关详细信息，请参阅 "Google Cloud 文档"

步骤 **5**：设置共享 **VPC** 权限

如果您使用共享 VPC 将资源部署到服务项目中，则需要准备好您的权限。

此表仅供参考，当 IAM 配置完成时，您的环境应该反映权限表。

查看共享 **VPC** 权限

身份	创造者	主办地点	服务项目权限	宿主项目权限	目的
Google 帐户部署代理	自定义	服务项目	"代理部署策略"	计算.网络用户	在服务项目中部署代理
代理服务账户	自定义	服务项目	"代理服务帐户策略"	计算.网络用户部署管理器.编辑器	部署和维护服务项目中的Cloud Volumes ONTAP和服务
Cloud Volumes ONTAP 服务帐户	自定义	服务项目	storage.admin 成员： NetApp Console服务帐户作为 serviceAccount.user	不适用	（可选）适用于NetApp Cloud Tiering和NetApp Backup and Recovery
Google API 服务代理	Google Cloud	服务项目	（默认）编辑器	计算.网络用户	代表部署与 Google Cloud API 进行交互。允许控制台使用共享网络。
Google Compute Engine 默认服务帐户	Google Cloud	服务项目	（默认）编辑器	计算.网络用户	代表部署部署 Google Cloud 实例和计算基础架构。允许控制台使用共享网络。

注：

1. 如果您没有将防火墙规则传递给部署并选择让控制台为您创建规则，则仅主机项目才需要 deploymentmanager.editor。如果未指定规则， NetApp Console将在主机项目中创建一个包含 VPC0 防火墙规则的部署。
2. 仅当您未将防火墙规则传递给部署并选择让控制台为您创建它们时，才需要firewall.create 和firewall.delete。这些权限位于控制台帐户 .yaml 文件中。如果您使用共享 VPC 部署 HA 对，这些权限将用于为 VPC1、2 和 3 创建防火墙规则。对于所有其他部署，这些权限也将用于为 VPC0 创建规则。
3. 对于 Cloud Tiering，分层服务帐户必须在服务帐户上具有 serviceAccount.user 角色，而不仅仅是在项目级别。目前，如果您在项目级别分配 serviceAccount.user，则使用 getIAMPolicy 查询服务帐户时不会显示权限。

第 **6** 步：启用 **Google Cloud API**

在 Google Cloud 中部署控制台代理之前，必须启用多个 Google Cloud API。

步骤

1. 在您的项目中启用以下 Google Cloud API：
   - 云基础设施管理器 API
   - 云部署管理器 V2 API
   - 云日志 API

- 云资源管理器 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NetApp Backup and Recovery与客户管理加密密钥 (CMEK) 结合使用时才需要）

"Google Cloud 文档：启用 API"

步骤 **7**：安装控制台代理

前提条件完成后，您可以在自己的 Linux 主机上手动安装该软件。

部署代理时，系统还会创建一个 Google Cloud 存储桶来存储部署文件。

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来访问互联网，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。如果您有明确的代理服务器，则需要按所示方式输入参数。

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控制台代理配置为使用 HTTP 或 HTTPS 代理服务器：

- http://地址:端口
- http://用户名:密码@地址:端口
- http://域名%92用户名:密码@地址:端口
- https://地址:端口
- https://用户名:密码@地址:端口
- https://域名%92用户名:密码@地址:端口

请注意以下事项：

- 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 代码，如上所示。
- 控制台代理不支持包含 @ 字符的用户名或密码。
- 如果密码包含以下任何特殊字符，则必须在该特殊字符前面加上反斜杠来转义该特殊字符：& 或 !

例如：

http://bxpproxyuser:netapp1\!@地址:3128

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"

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。

2. 等待安装完成。

安装结束时，如果您指定了代理服务器，控制台代理服务 (occm) 将重新启动两次。

如果安装失败，您可以查看安装报告和日志来帮助您解决问题。"了解如何解决安装问题。"

1. 从连接到控制台代理虚拟机的主机打开 Web 浏览器并输入以下 URL：

   https://ipaddress

2. 登录后，设置控制台代理：

   a. 指定与控制台代理关联的组织。

   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。

      您应该保持限制模式处于禁用状态，因为这些步骤描述了如何在标准模式下使用控制台。仅当您拥有安全的环境并希望断开此帐户与后端服务的连接时，才应启用受限模式。如果真是这样的话，"按照步骤在受限模式下开始使用NetApp Console" 。

   d. 选择*让我们开始吧*。

      如果安装失败，您可以查看日志和报告来帮助您排除故障。"了解如何解决安装问题。"

如果您在创建控制台代理的同一 Google Cloud 帐户中拥有 Google Cloud Storage 存储桶，您将看到 Google Cloud Storage 系统自动出现在 **Systems** 页面上。 "了解如何通过NetApp Console管理 Google Cloud Storage"

步骤 **8**：向控制台代理提供权限

您需要向控制台代理提供您之前设置的 Google Cloud 权限。提供权限可使控制台代理管理 Google Cloud 中的数据和存储基础架构。

步骤

1. 转到 Google Cloud 门户并将服务帐户分配给控制台代理 VM 实例。

   "Google Cloud 文档：更改实例的服务帐户和访问范围"

2. 如果您想管理其他 Google Cloud 项目中的资源，请通过将具有控制台代理角色的服务帐号添加到该项目来授予访问权限。您需要对每个项目重复此步骤。

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 。

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**
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

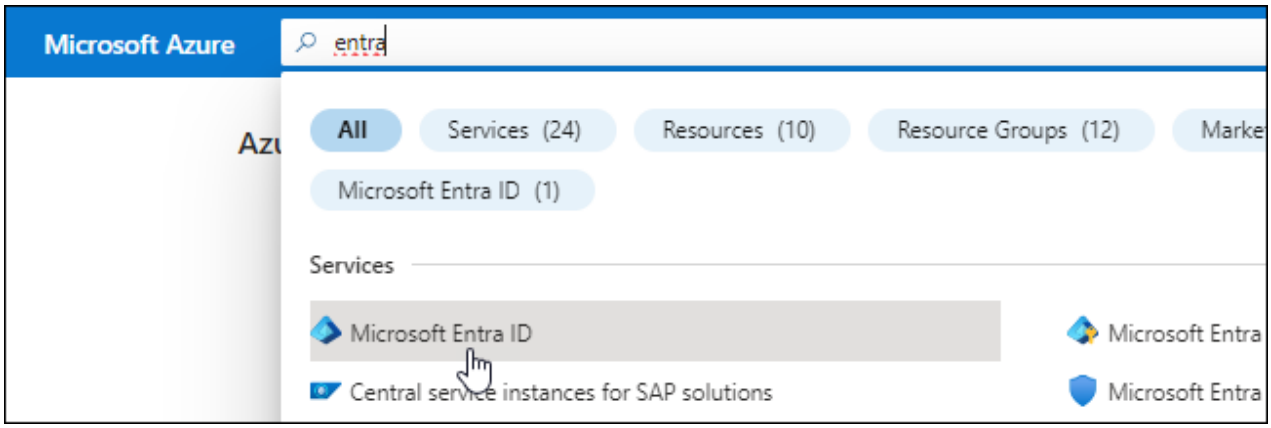
当控制台代理安装在本地时，您需要通过在 Microsoft Entra ID 中设置服务主体并获取控制台代理所需的 Azure 凭据来为控制台代理提供 Azure 权限。

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。

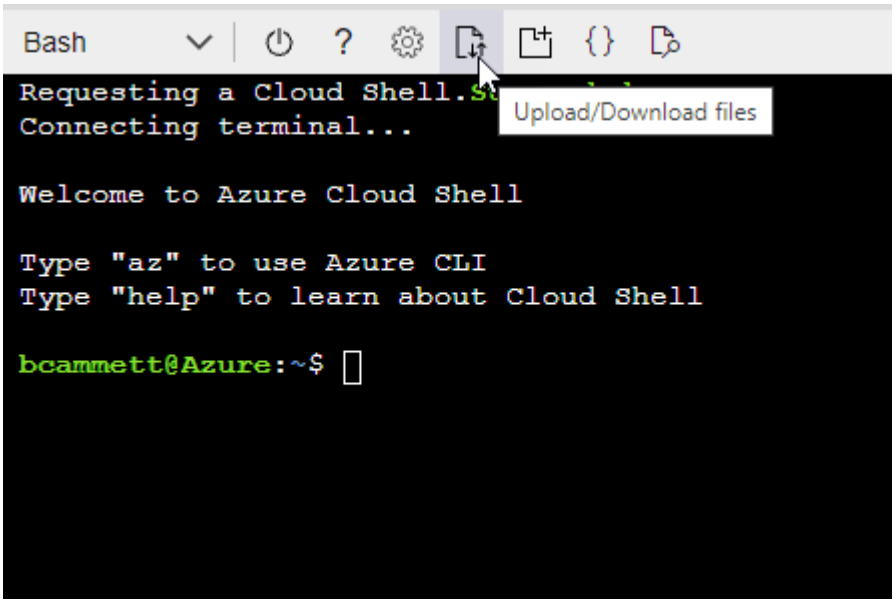
      例子

      ```
      "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：

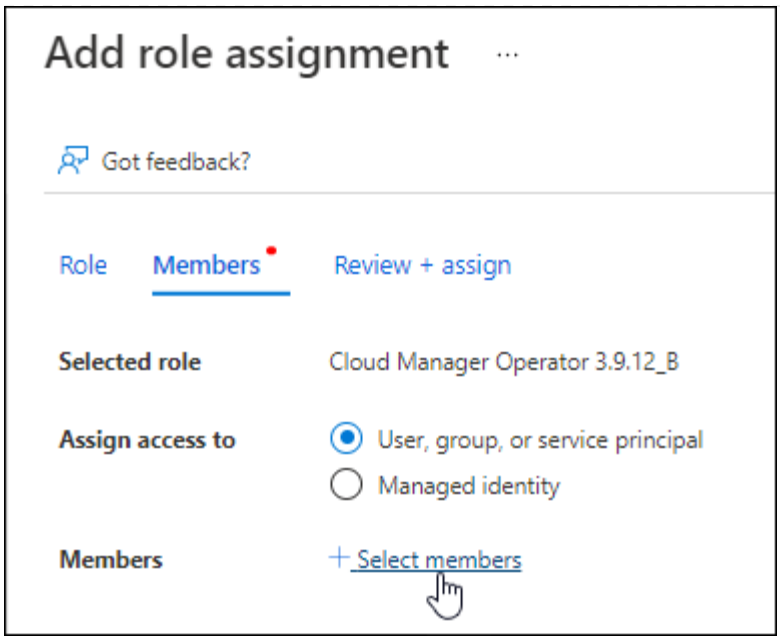
```
az role definition create --role-definition agent_Policy.json
```

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：

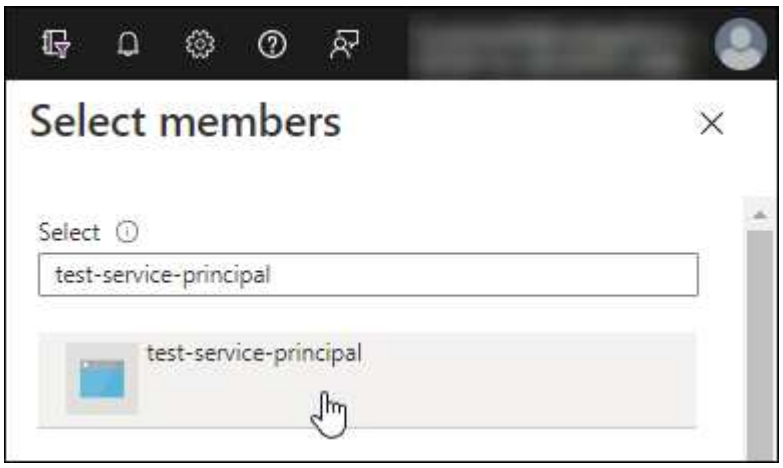
   a. 从 Azure 门户打开 **Subscriptions** 服务。
   b. 选择订阅。
   c. 选择“访问控制 (IAM)”>“添加”>“添加角色分配”。
   d. 在*角色*选项卡中，选择*控制台操作员*角色并选择*下一步*。
   e. 在“成员”选项卡中，完成以下步骤：

      - 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”。

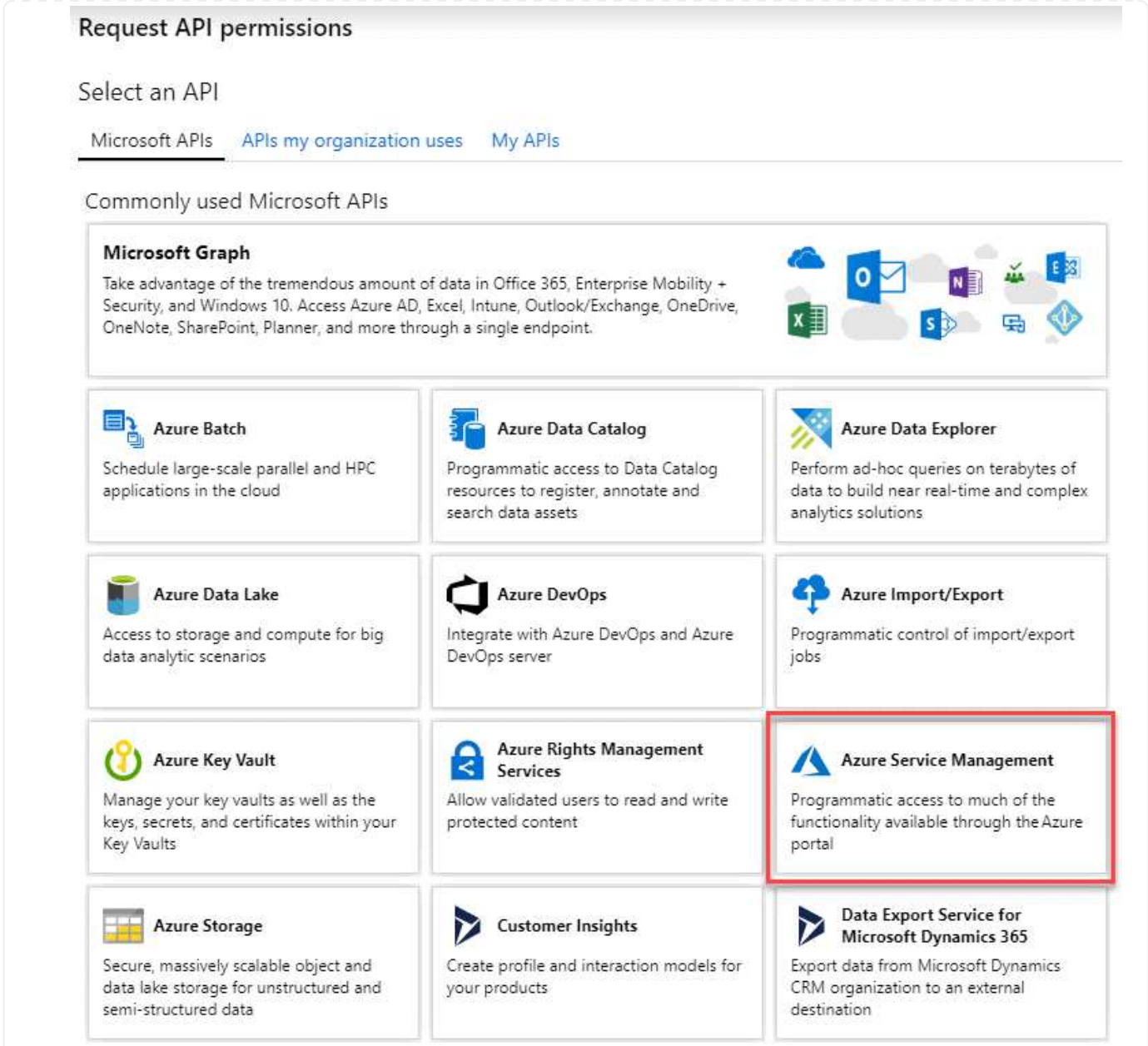
f. 选择*审阅+分配*。

服务主体现在具有部署控制台代理所需的 Azure 权限。

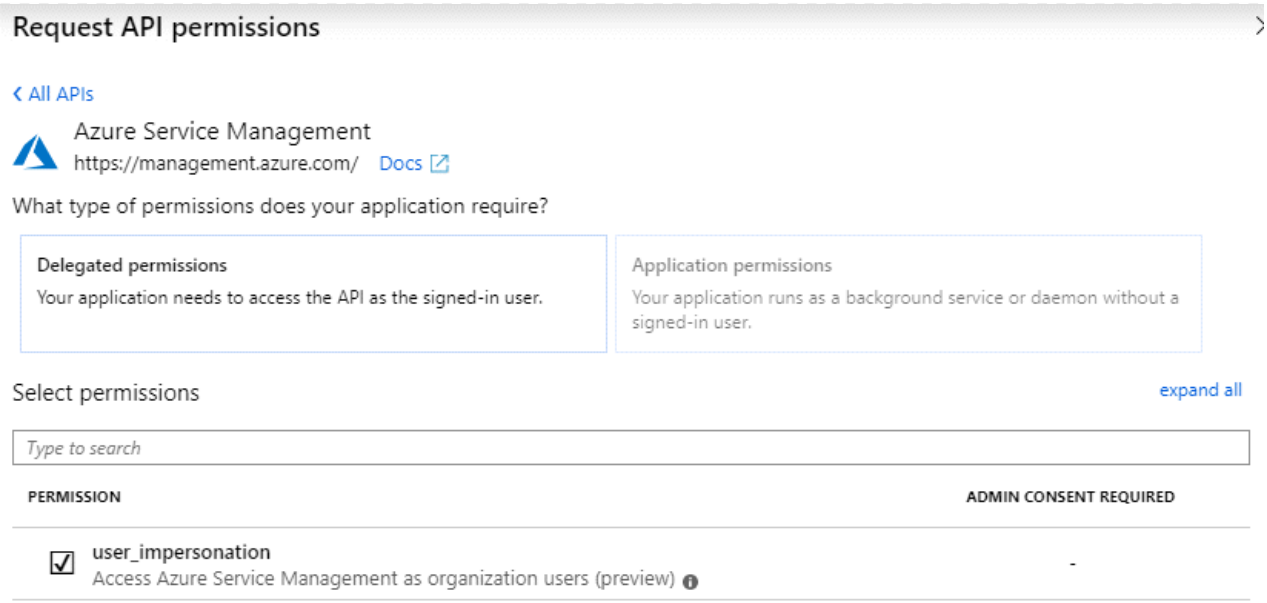
如果您想从多个 Azure 订阅部署Cloud Volumes ONTAP ，则必须将服务主体绑定到每个订阅。在NetApp Console中，您可以选择部署Cloud Volumes ONTAP时要使用的订阅。

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”。

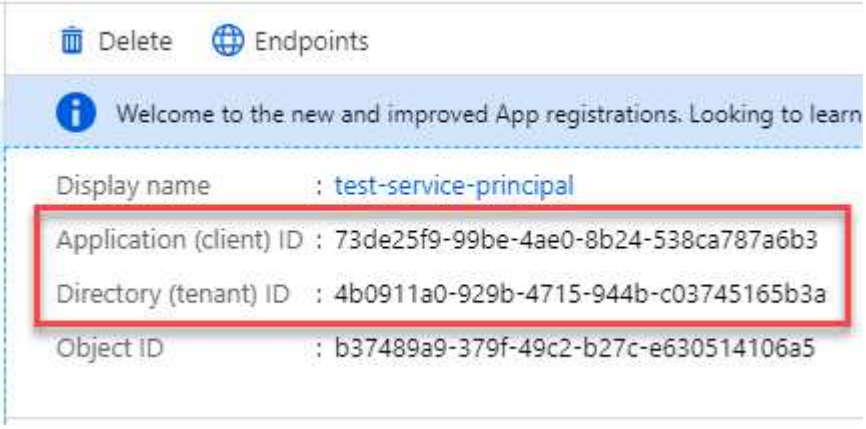


4. 选择*以组织用户身份访问 Azure 服务管理*，然后选择*添加权限*。



获取应用程序的应用程序**ID**和目录**ID**

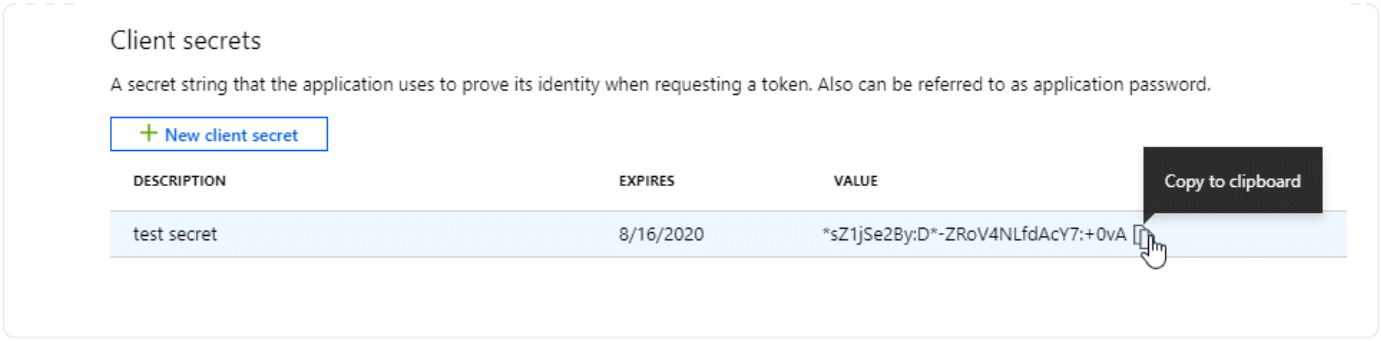
1. 在*Microsoft Entra ID*服务中，选择*App Registrations*并选择应用程序。
2. 复制*应用程序（客户端）ID*和*目录（租户）ID*。



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 **4.** 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来访问互联网，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。如果您有明确的代理服务器，则需要按所示方式输入参数。

   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控制台代理配置为使用 HTTP 或 HTTPS 代理服务器：

- http://地址:端口
- http://用户名:密码@地址:端口
- http://域名%92用户名:密码@地址:端口
- https://地址:端口
- https://用户名:密码@地址:端口
- https://域名%92用户名:密码@地址:端口

  请注意以下事项：

  - 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 代码，如上所示。
  - 控制台代理不支持包含 @ 字符的用户名或密码。
  - 如果密码包含以下任何特殊字符，则必须在该特殊字符前面加上反斜杠来转义该特殊字符：& 或 !

    例如：

http://bxpproxyuser:netapp1\!@地址:3128

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"

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

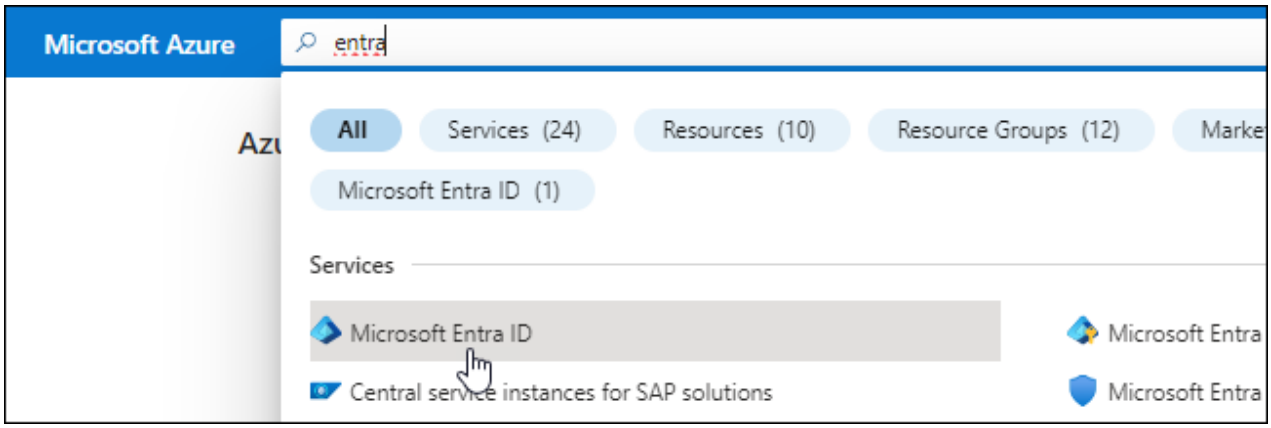
当控制台代理安装在本地时，您需要通过在 Microsoft Entra ID 中设置服务主体并获取控制台代理所需的 Azure 凭据来授予控制台代理 Azure 权限。

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。

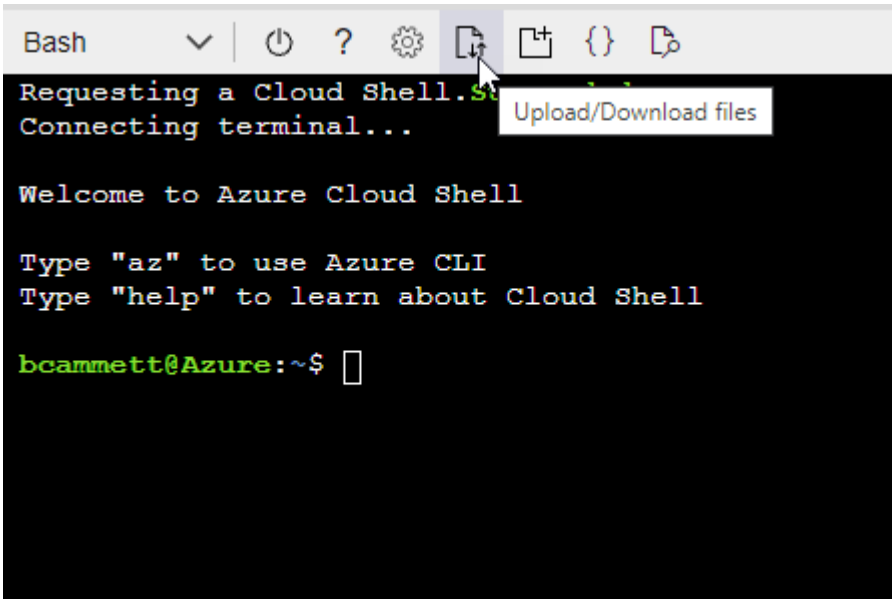
      例子

      ```
      "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：

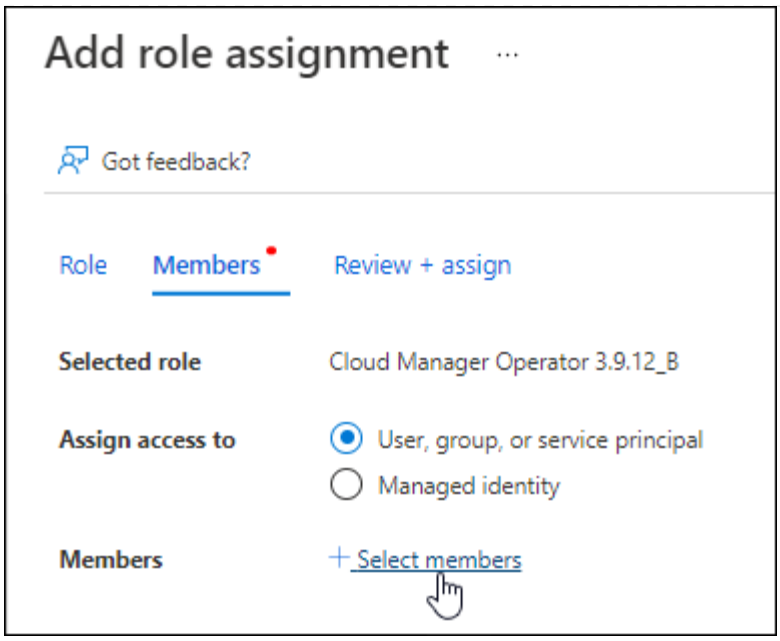
```
az role definition create --role-definition agent_Policy.json
```

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：

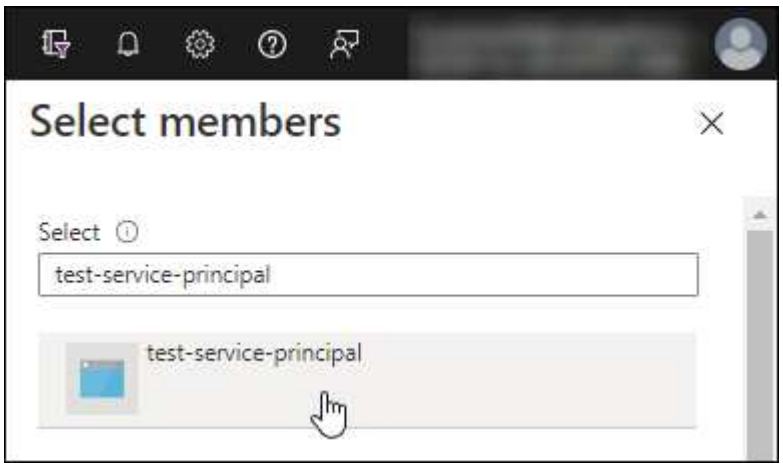
a. 从 Azure 门户打开 **Subscriptions** 服务。
b. 选择订阅。
c. 选择“访问控制 (IAM)”>“添加”>“添加角色分配”。
d. 在*角色*选项卡中，选择*控制台操作员*角色并选择*下一步*。
e. 在“成员”选项卡中，完成以下步骤：

- 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”。

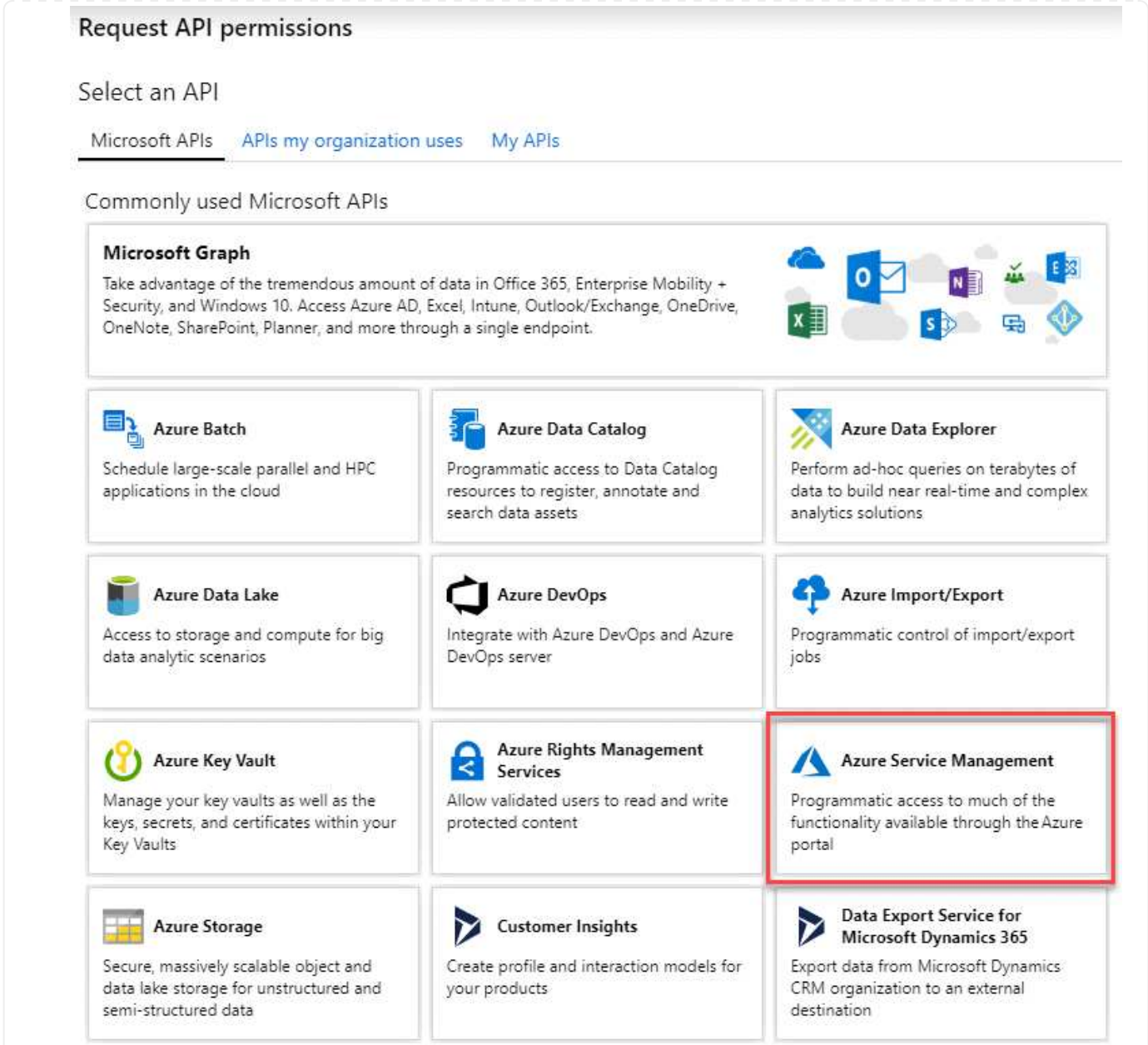
f. 选择*审阅+分配*。

服务主体现在具有部署控制台代理所需的 Azure 权限。

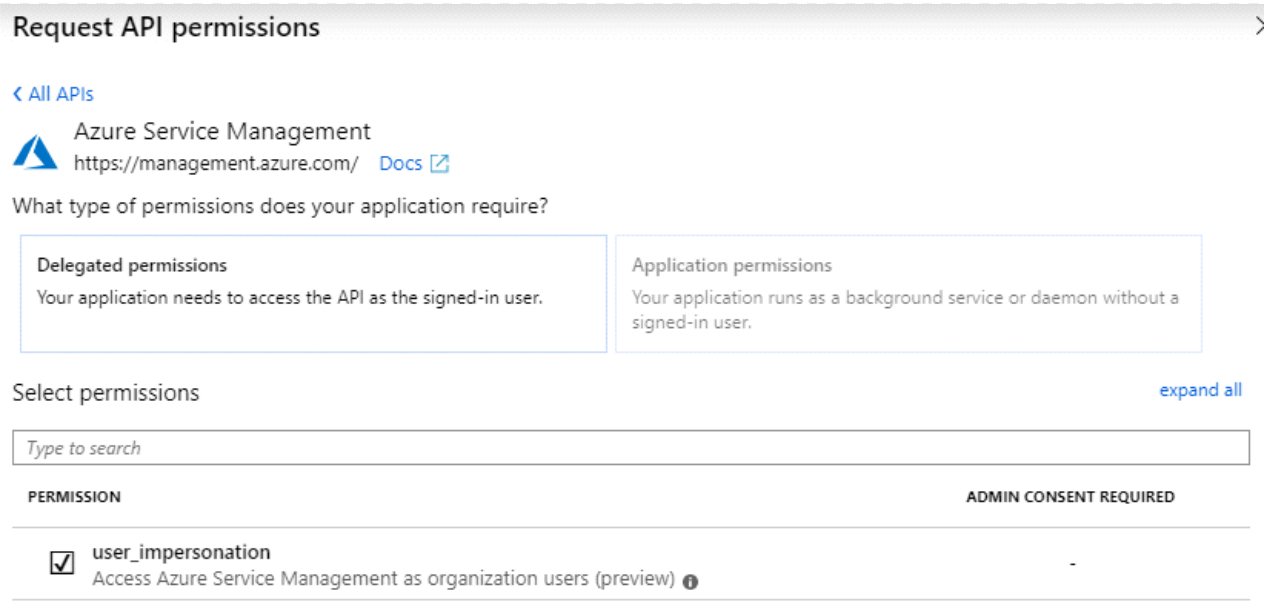
如果您想从多个 Azure 订阅部署Cloud Volumes ONTAP ，则必须将服务主体绑定到每个订阅。在NetApp Console中，您可以选择部署Cloud Volumes ONTAP时要使用的订阅。

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”。

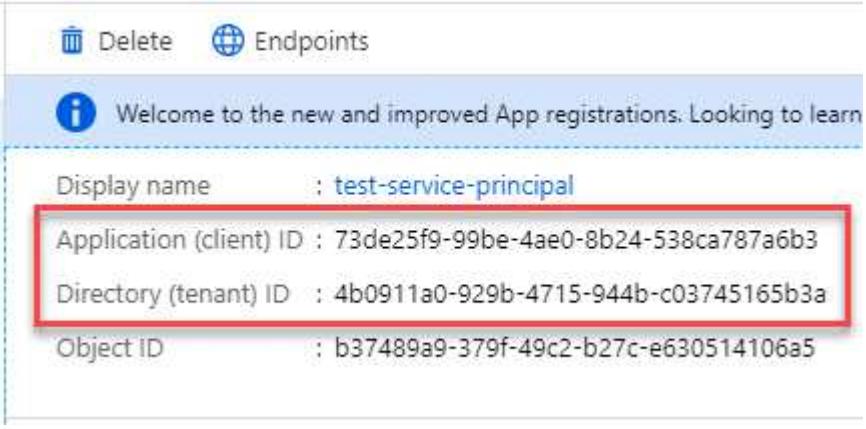


4. 选择*以组织用户身份访问 Azure 服务管理*，然后选择*添加权限*。



获取应用程序的应用程序**ID**和目录**ID**

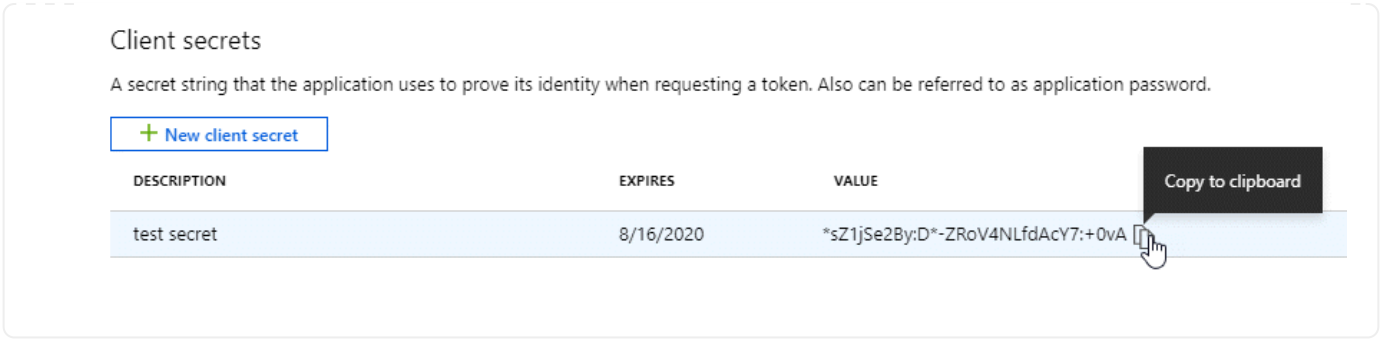
1. 在*Microsoft Entra ID*服务中，选择*App Registrations*并选择应用程序。
2. 复制*应用程序（客户端）ID*和*目录（租户）ID*。



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。