



控制台代理

NetApp Console setup and administration

NetApp

January 27, 2026

目录

控制台代理	1
了解NetApp Console代理	1
控制台代理必须始终处于运行状态	3
支持的位置	3
与云提供商的沟通	3
限制模式	3
如何安装控制台代理	3
云提供商权限	3
代理升级	4
操作系统和虚拟机维护	4
多系统和代理	4
部署控制台代理	5
AWS	5
Azure	30
Google Cloud	76
在本地安装代理	108
维护控制台代理	144
为控制台代理维护 VCenter 或 ESXi 主机	144
安装 CA 签名的证书以进行基于 Web 的控制台访问	147
配置控制台代理以使用代理服务器	149
控制台代理故障排除	151
卸载并删除控制台代理	156
管理云提供商凭证	156
AWS	156
Azure	169
Google Cloud	182

控制台代理

了解NetApp Console代理

您可以使用控制台代理将NetApp Console连接到您的基础架构，并安全地协调跨 AWS、Azure、Google Cloud 或本地环境的存储解决方案，以及使用数据保护服务。

控制台代理使您能够：

- 通过NetApp Console协调存储管理任务，例如配置Cloud Volumes ONTAP、设置存储卷、使用数据分类等等。
- 使用云提供商的 IAM 角色进行身份验证，以实现订阅计费集成。
- 使用高级数据服务（NetApp Backup and Recovery、 NetApp Disaster Recovery、 NetApp Ransomware Resilience和NetApp Cloud Tiering）
- 以受限模式使用控制台。

如果您不需要高级编排或数据保护，则可以集中管理本地ONTAP集群和云原生存储服务，而无需部署代理。此外，还提供监控和数据传输工具。

下表显示了您可以使用和不使用控制台代理时可以使用的功能和服务。

	可联系经纪人获取信息	无需代理即可购买
支持的存储系统：		
适用于ONTAP 的Amazon FSx	是的（发现和管理功能）	是的（仅限探索）
Amazon S3 存储	是	否
Azure Blob 存储	是	是
Azure NetApp Files	是	是
Cloud Volumes ONTAP	是	否
E系列系统	是	否
Google Cloud NetApp Volumes	是	是
Google Cloud 存储桶	是	否
StorageGRID系统	是	否
本地部署ONTAP集群（高级管理和发现）	是的（高级管理和发现）	否（仅限基本发现）

	可联系经纪人获取信息	无需代理即可购买
可用的存储管理服务：		
警报	是	否
自动化中心	是	是
Digital Advisor (Active IQ)	是	否
许可证和订阅管理	是	否
经济效益	是	否
首页仪表盘指标	是的 ²	否
生命周期规划	是	1号
可持续性	是	否
软件更新	是	是
NetApp工作负载	是	是
可用数据服务：		
NetApp Backup and Recovery	是	否
数据分类	是	否
NetApp Cloud Tiering	是	否
NetApp Copy and Sync	是	否
NetApp Disaster Recovery	是	否
NetApp Ransomware Resilience	是	否
NetApp Volume Caching	是	否

¹ 无需控制台代理即可查看生命周期规划，但需要控制台代理才能启动操作。

² 主页上的准确指标需要大小合适且配置正确的控制台代理。

控制台代理必须始终处于运行状态

控制台代理是NetApp Console的基本组成部分。您（客户）有责任确保相关代理随时处于正常运行和可访问状态。控制台可以处理短暂的代理中断，但您必须快速修复基础设施故障。

本文档受 EULA 管辖。按照文档以外的方式操作产品可能会影响其功能和您的 EULA 权利。

支持的位置

您可以在以下位置安装代理：

- Amazon Web Services
- Microsoft Azure

在 Azure 中与其管理的Cloud Volumes ONTAP系统位于同一区域的控制台代理。或者，将其部署在 ["Azure 区域对"](#)。这可确保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"](#)

- Google Cloud

要将控制台和数据服务与 Google Cloud 一起使用，请在 Google Cloud 中部署您的代理。

- 在您的场所

与云提供商的沟通

该代理使用 TLS 1.3 与 AWS、Azure 和 Google Cloud 进行所有通信。

限制模式

要在受限模式下使用控制台，请安装控制台代理并访问在控制台代理上本地运行的控制台界面。

["了解NetApp Console部署模式"](#)。

如何安装控制台代理

您可以直接从控制台、云提供商的市场安装控制台代理，也可以在您自己的 Linux 主机或 VCenter 环境中手动安装软件。

- ["了解NetApp Console部署模式"](#)
- ["开始在标准模式下使用NetApp Console"](#)
- ["开始在受限模式下使用NetApp Console"](#)

云提供商权限

您需要特定权限才能直接从NetApp Console创建控制台代理，并且需要另一组权限来创建控制台代理本身。如果您直接从控制台在 AWS 或 Azure 中创建控制台代理，则控制台将使用其所需的权限创建控制台代理。

在标准模式下使用控制台时，如何提供权限取决于您计划如何创建控制台代理。

要了解如何设置权限，请参阅以下内容：

- 标准模式
 - ["AWS 中的代理安装选项"](#)
 - ["Azure 中的代理安装选项"](#)
 - ["Google Cloud 中的代理安装选项"](#)
 - ["为本地部署设置云权限"](#)
- ["设置限制模式的权限"](#)

要查看控制台代理日常操作所需的确切权限，请参阅以下页面：

- ["了解控制台代理如何使用 AWS 权限"](#)
- ["了解控制台代理如何使用 Azure 权限"](#)
- ["了解控制台代理如何使用 Google Cloud 权限"](#)

您有责任在后续版本中添加新权限时更新控制台代理策略。发行说明列出了新的权限。

代理升级

NetApp每月更新代理软件以添加功能并提高稳定性。某些控制台功能（如Cloud Volumes ONTAP和本地ONTAP集群管理）依赖于控制台代理版本和设置。

当您在云端安装代理时，如果控制台代理可以访问互联网，则会自动更新。

操作系统和虚拟机维护

维护控制台代理主机上的操作系统是您（客户）的责任。例如，您（客户）应按照贵公司的操作系统分发标准程序，对控制台代理主机上的操作系统应用安全更新。

请注意，您（客户）在应用次要安全更新时不需要停止控制台主机上的任何服务。

如果您（客户）需要停止然后启动控制台代理虚拟机，您应该从云提供商的控制台或使用标准的内部管理程序来执行此操作。

[控制台代理必须始终处于运行状态。](#)

多系统和代理

一个代理可以管理多个系统并在控制台中支持数据服务。您可以根据部署规模和使用的数据服务使用单个代理来管理多个系统。

对于大规模部署，请与您的NetApp代表合作来确定您的环境规模。如果遇到问题，请联系NetApp支持。

以下是代理部署的一些示例：

- 您有一个多云环境（例如，AWS 和 Azure），并且您希望在 AWS 中有一个代理，在 Azure 中有一个代理。每个系统都管理在这些环境中运行的Cloud Volumes ONTAP系统。
- 服务提供商可能使用一个控制台组织为其客户提供服务，同时使用另一个组织为其某个业务部门提供灾难恢

复。每个组织都需要自己的代理人。

部署控制台代理

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.bluelxp.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com \ https://console.netapp.com \ https://components.console.bluelxp.netapp.com \ https://cdn.auth0.com	在 NetApp Console 中提供功能和服务。

端点	目的
https://bluexpinfraproduct.eastus2.data.azurecr.io \ https://bluexpinfraproduct.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。如果您使用"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.bluelxp.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com \ https://console.netapp.com \ https://components.console.bluelxp.netapp.com \ https://cdn.auth0.com	在 NetApp Console 中提供功能和服务。

端点	目的
https://bluexpinfraproduct.eastus2.data.azurecr.io \ https://bluexpinfraproduct.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。如果您使用"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.blueexp.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com \ https://console.netapp.com \ https://components.console.blueexp.netapp.com \ https://cdn.auth0.com	在NetApp Console中提供功能和服务。
\ https://bluexpinfraproduct.eastus2.data.azurecr.io \ https://bluexpinfraproduct.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才能访问互联网，则需要添加代理信息。您可以在安装过程中添加显式代理。`--proxy` 和 `--cacert` 参数是可选的，系统不会提示您添加它们。如果您有显式代理服务器，则需要输入如图所示的参数。



如果要配置透明代理，可以在安装完成后进行配置。["了解代理维护控制台"](#)

+

以下是使用 CA 签名证书配置显式代理服务器的示例：

+

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

+

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

```
+ * http://address:port * http://user-name:password@address:port * http://domain-name%92user-  
name:password@address:port * https://address:port * https://user-name:password@address:port *  
https://domain-name%92user-name:password@address:port
```

+ 注意以下事项：

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

+ 例如：

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

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

a. 通过 SSH 连接到控制台代理虚拟机。

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

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

例如：

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

- a. 重新启动控制台代理虚拟机。
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：

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

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。
\ 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。

端点	目的
\ 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.blueexp.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com \ https://console.netapp.com \ https://components.console.blueexp.netapp.com \ https://cdn.auth0.com	在NetApp Console中提供功能和服务。
\ https://blueexpinfraproduct.eastus2.data.azurecr.io \ https://blueexpinfraproduct.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。如果您使用"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/read",
"Microsoft.Network/networkInterfaces/ipConfigurations/read",
"Microsoft.Resources/deployments/operations/read",
"Microsoft.Resources/deployments/read",
"Microsoft.Resources/deployments/delete",
"Microsoft.Resources/deployments/cancel/action",
"Microsoft.Resources/deployments/validate/action",
"Microsoft.Resources/resources/read",
"Microsoft.Resources/subscriptions/operationresults/read",
"Microsoft.Resources/subscriptions/resourceGroups/delete",
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Resources/subscriptions/resourcegroups/resources/read",
"Microsoft.Resources/subscriptions/resourceGroups/write",
"Microsoft.Authorization/roleDefinitions/write",
"Microsoft.Authorization/roleAssignments/write",

```

```

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

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

```

2. 通过将 Azure 订阅 ID 添加到可分配范围来修改 JSON。

例子

```

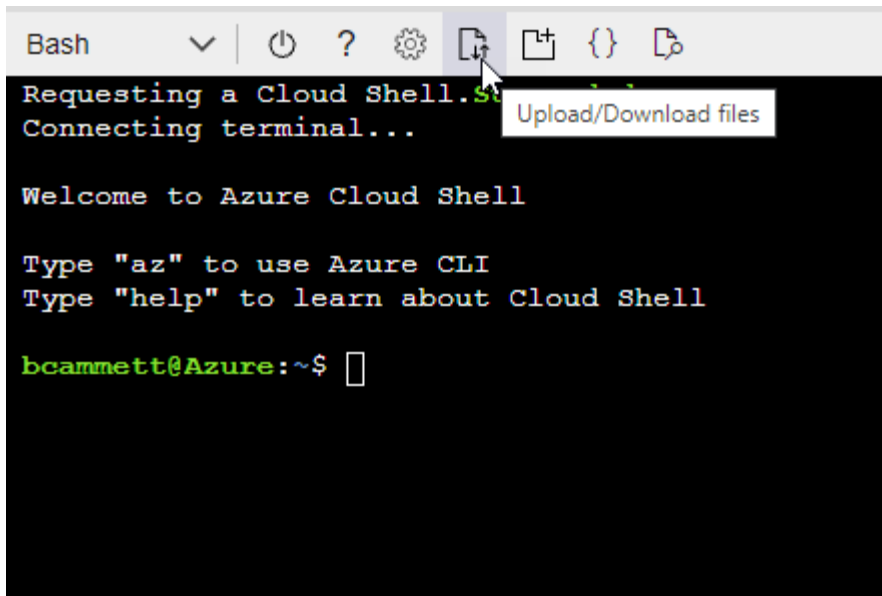
"AssignableScopes": [
    "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzzz"
]

```

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。

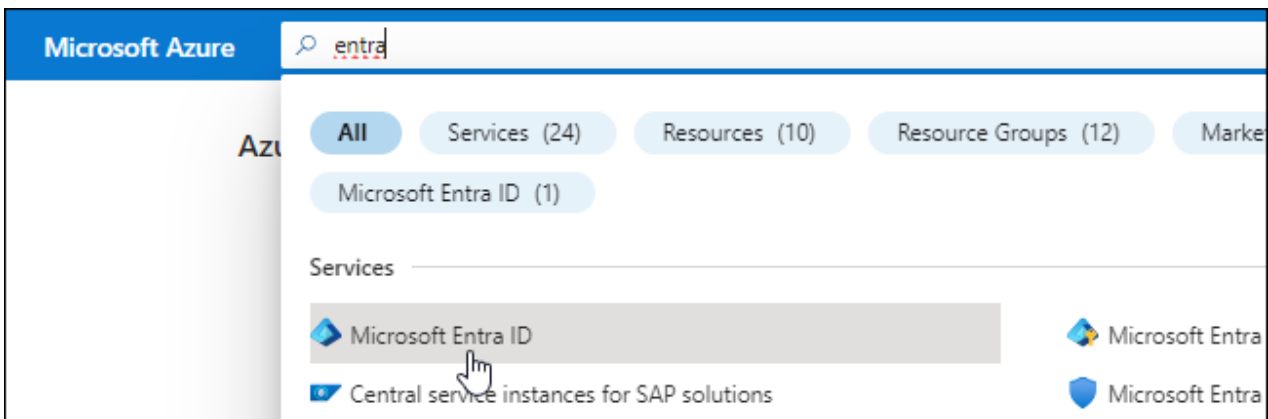
在 Microsoft Entra ID 中创建并设置服务主体，并获取控制台所需的 Azure 凭据。

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：

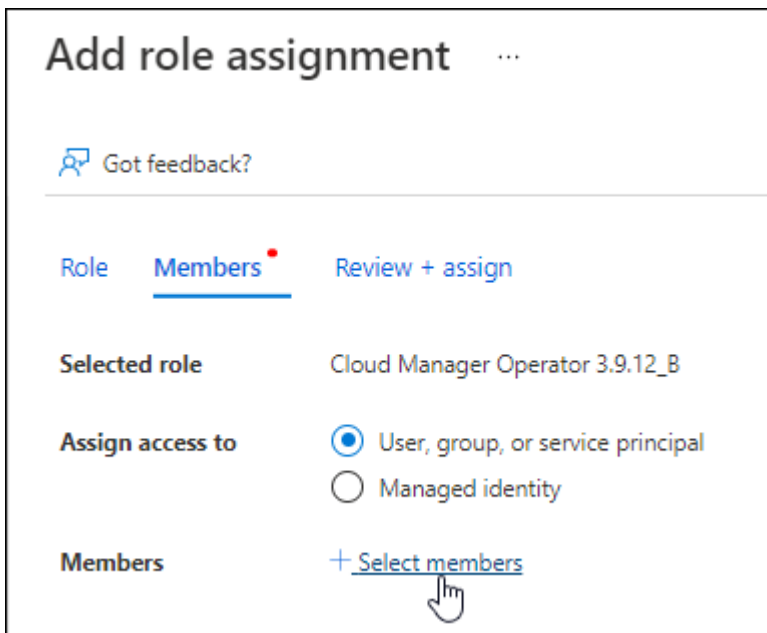
- 名称：输入应用程序的名称。
- 帐户类型：选择帐户类型（任何类型都可以与NetApp Console一起使用）。
- 重定向 **URI**：您可以将此字段留空。

6. 选择*注册*。

您已创建 AD 应用程序和服务主体。

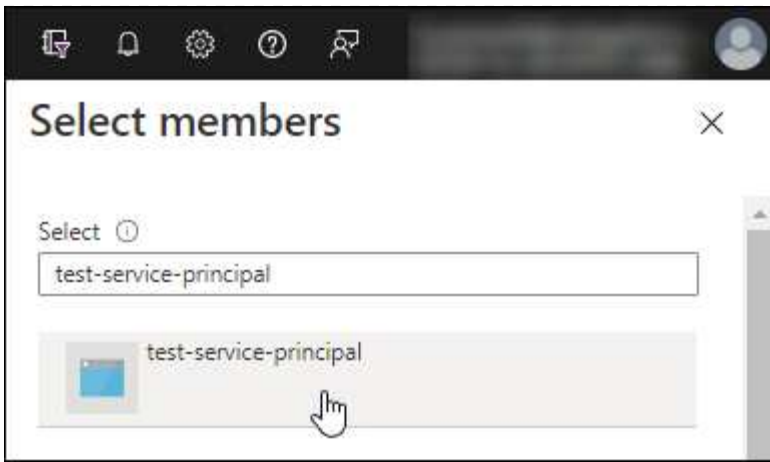
将自定义角色分配给应用程序

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”。

Request API permissions

Select an API

Microsoft APIs APIs my organization uses My APIs

Commonly used Microsoft APIs

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



**Azure Batch**
Schedule large-scale parallel and HPC applications in the cloud

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

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

**Azure Data Lake**
Access to storage and compute for big data analytic scenarios

**Azure DevOps**
Integrate with Azure DevOps and Azure DevOps server

**Azure Import/Export**
Programmatic control of import/export jobs

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

**Azure Rights Management Services**
Allow validated users to read and write protected content

**Azure Service Management**
Programmatic access to much of the functionality available through the Azure portal

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

**Customer Insights**
Create profile and interaction models for your products

**Data Export Service for Microsoft Dynamics 365**
Export data from Microsoft Dynamics CRM organization to an external destination

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

Request API permissions

[< All APIs](#)



Azure Service Management

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

What type of permissions does your application require?

Delegated permissions

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

Application permissions

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

Select permissions

[expand all](#)

Type to search

PERMISSION

ADMIN CONSENT REQUIRED

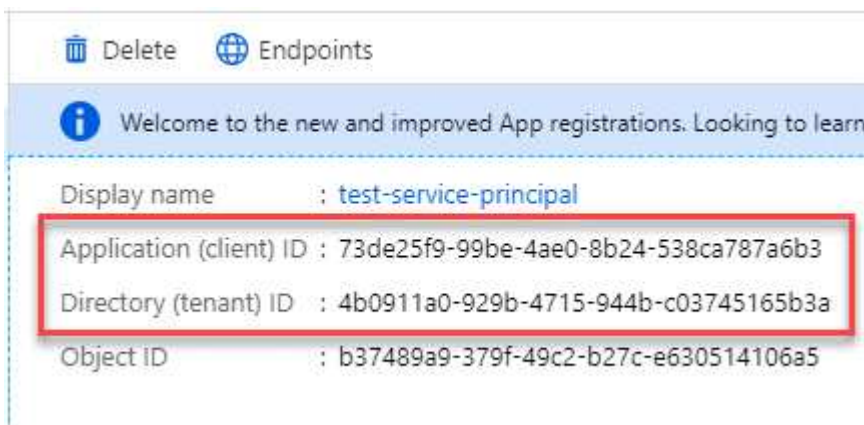


user_impersonation

Access Azure Service Management as organization users (preview)

获取应用程序的应用程序ID和目录ID

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



将 Azure 帐户添加到控制台时，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。

Client secrets

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

[+ New client secret](#)

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

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.blueexp.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com \ https://console.netapp.com \ https://components.console.blueexp.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。如果您使用"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。

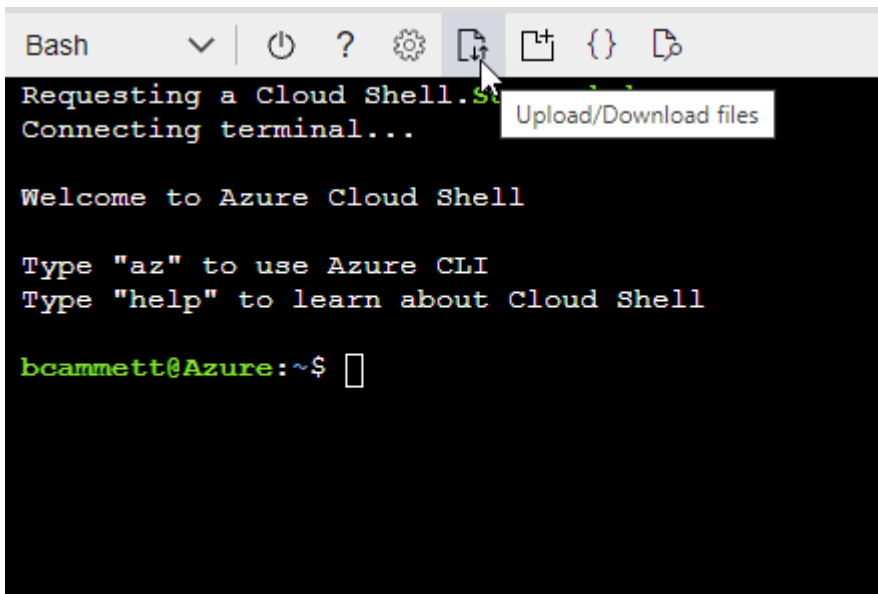
例子

```
"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

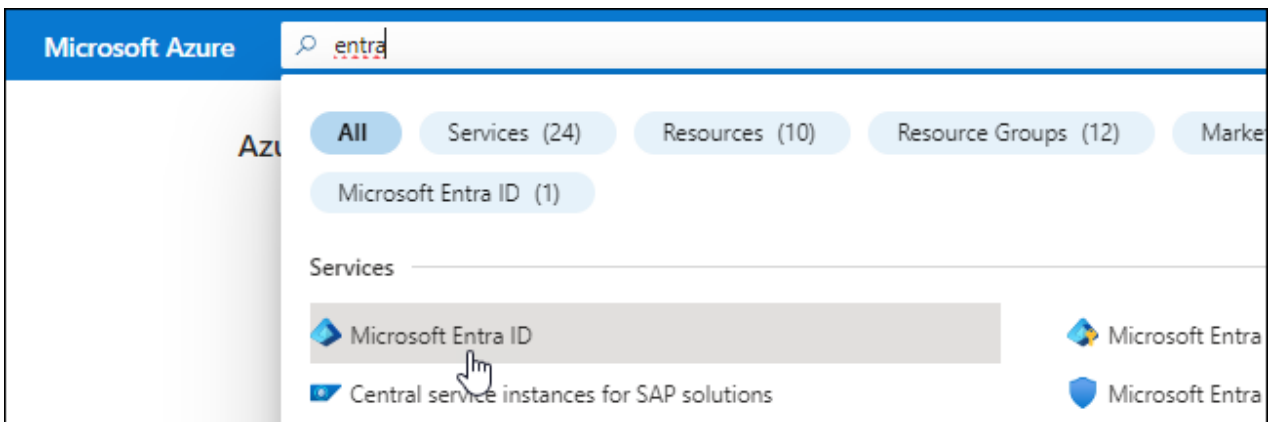
在 Microsoft Entra ID 中创建并设置服务主体，并获取控制台所需的 Azure 凭据。

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。

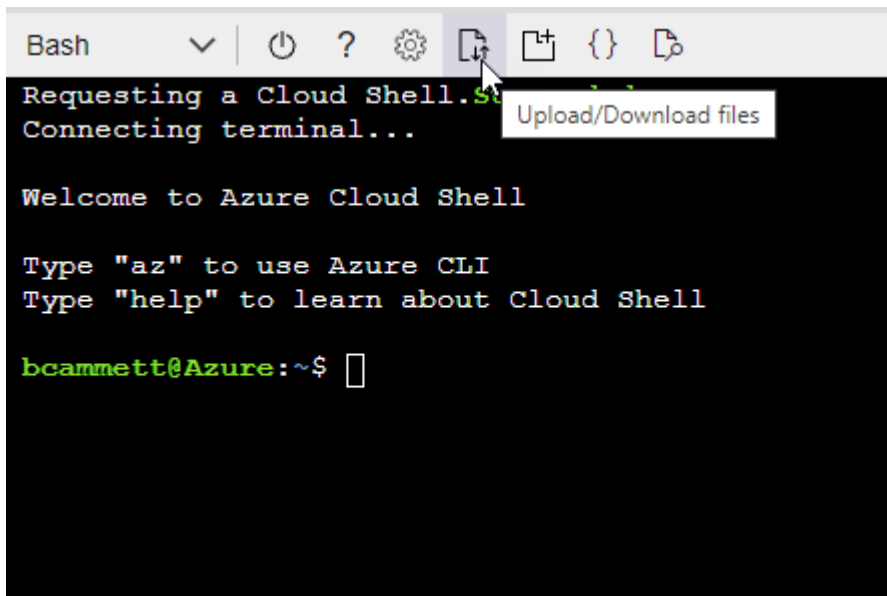
例子

```
"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
```

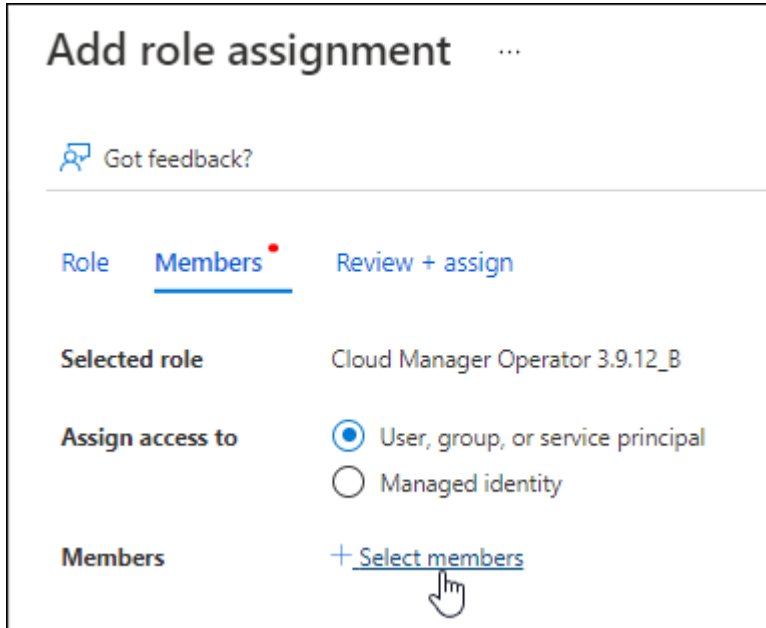
现在您应该有一个名为“控制台操作员”的自定义角色，可以将其分配给控制台代理虚拟机。

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*。

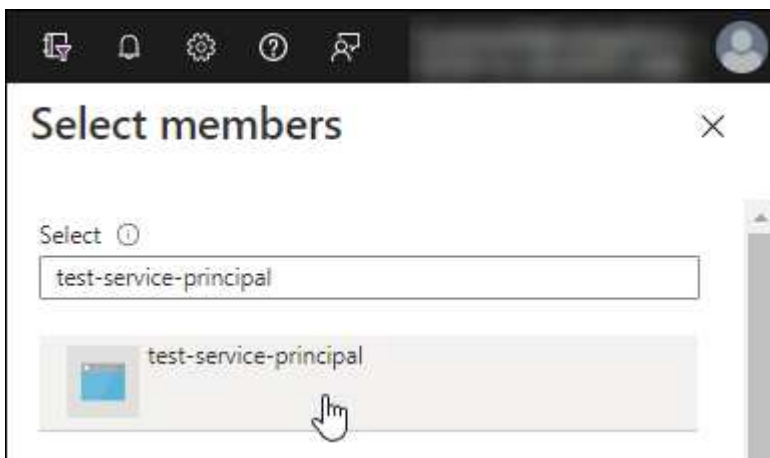
e. 在“成员”选项卡中，完成以下步骤：

- 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”。

Request API permissions

Select an API

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

Commonly used Microsoft APIs

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

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

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

Request API permissions

[< All APIs](#)



Azure Service Management

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

What type of permissions does your application require?

Delegated permissions

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

Application permissions

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

Select permissions

[expand all](#)

Type to search

PERMISSION

ADMIN CONSENT REQUIRED

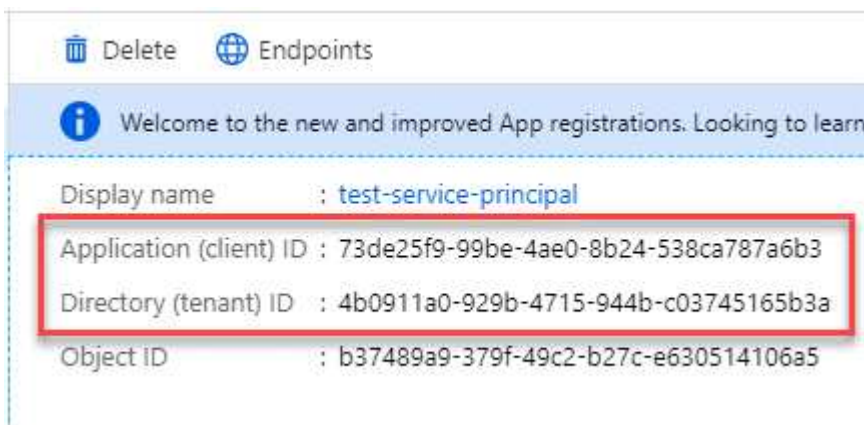


user_impersonation

Access Azure Service Management as organization users (preview)

获取应用程序的应用程序ID和目录ID

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



将 Azure 帐户添加到控制台时，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。

Client secrets

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

+ New client secret

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

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：

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

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.blueexp.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com \ https://console.netapp.com \ https://components.console.blueexp.netapp.com \ https://cdn.auth0.com	在NetApp Console中提供功能和服务。

端点	目的
https://bluexpinfraproduct.eastus2.data.azurecr.io \ https://bluexpinfraproduct.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。如果您使用"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。

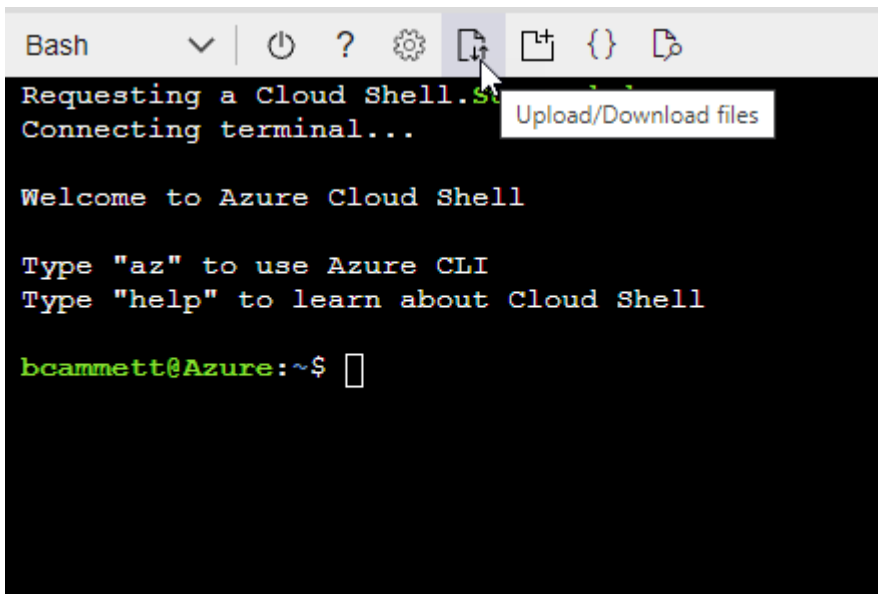
例子

```
"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

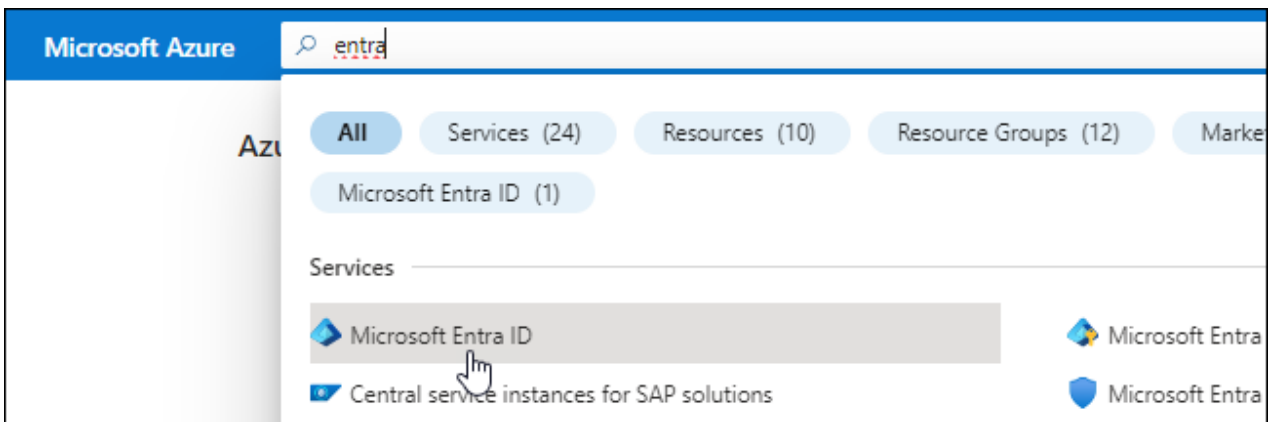
在 Microsoft Entra ID 中创建并设置服务主体，并获取控制台代理所需的 Azure 凭据。

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。

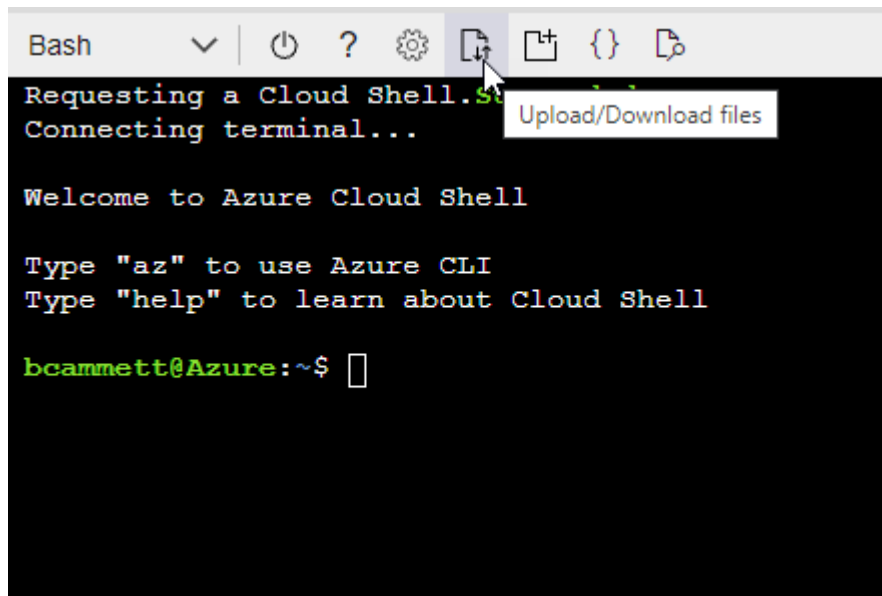
例子

```
"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
```

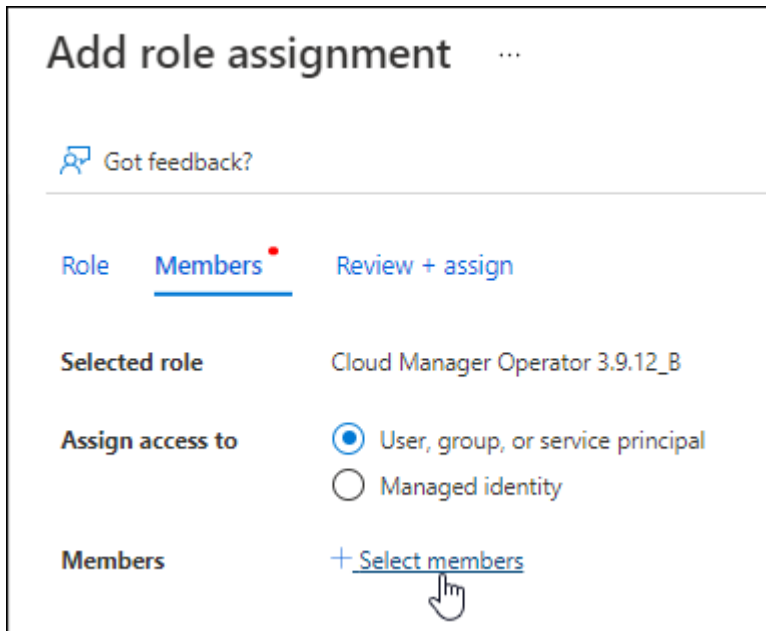
现在您应该有一个名为“控制台操作员”的自定义角色，可以将其分配给控制台代理虚拟机。

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*。

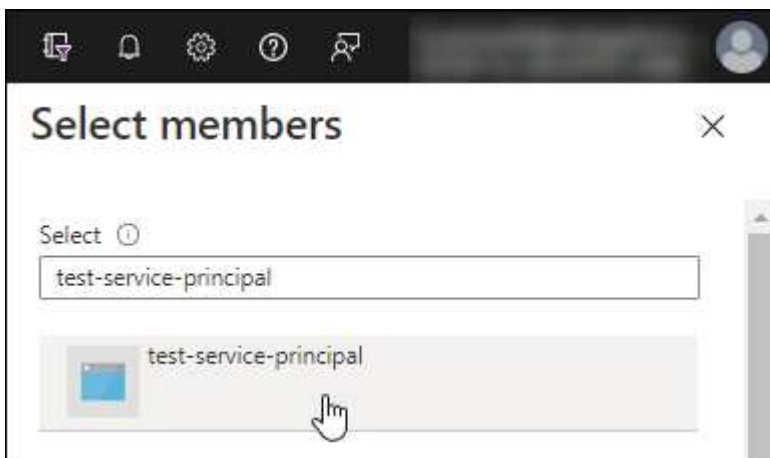
e. 在“成员”选项卡中，完成以下步骤：

- 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”。

Request API permissions

Select an API

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

Commonly used Microsoft APIs

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

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

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

Request API permissions

[< All APIs](#)



Azure Service Management

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

What type of permissions does your application require?

Delegated permissions

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

Application permissions

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

Select permissions

[expand all](#)

Type to search

PERMISSION

ADMIN CONSENT REQUIRED

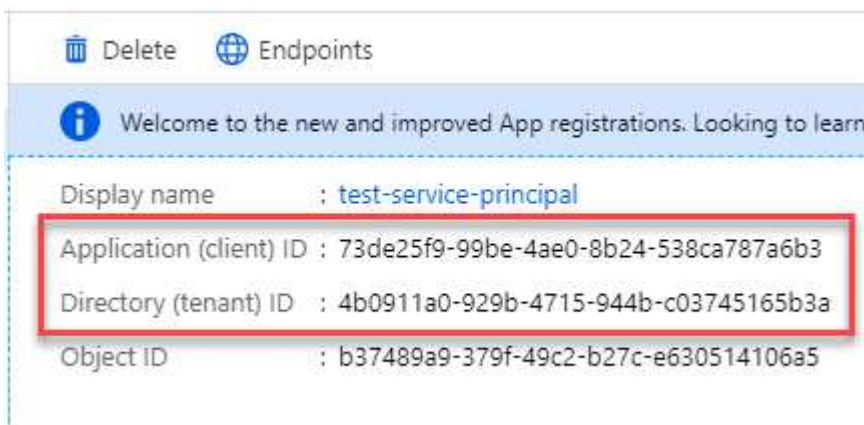


user_impersonation

Access Azure Service Management as organization users (preview)

获取应用程序的应用程序ID和目录ID

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



将 Azure 帐户添加到控制台时，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。

Client secrets

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

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

Copy to clipboard

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才能访问互联网，则需要添加代理信息。您可以在安装过程中添加显式代理。

--proxy 和 --cacert 参数是可选的，系统不会提示您添加它们。如果您有显式代理服务器，则需要输入如图所示的参数。



如果要配置透明代理，可以在安装完成后进行配置。["了解代理维护控制台"](#)

+

以下是使用 CA 签名证书配置显式代理服务器的示例：

+

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

+

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

```
+ * http://address:port * http://user-name:password@address:port * http://domain-name%92user-  
name:password@address:port * https://address:port * https://user-name:password@address:port *  
https://domain-name%92user-name:password@address:port
```

+ 注意以下事项：

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

+ 例如：

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

1. 如果您使用 Podman，则需要调整 aardvark-dns 端口。
 - a. 通过 SSH 连接到控制台代理虚拟机。
 - b. 打开 podman /usr/share/containers/containers.conf 文件并修改 Aardvark DNS 服务的选定端口。例如，将其更改为54。

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

例如：

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

- a. 重新启动控制台代理虚拟机。
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：

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

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.blueexp.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com \ https://console.netapp.com \ https://components.console.blueexp.netapp.com \ https://cdn.auth0.com	在NetApp Console中提供功能和服务。
\ https://blueexpinfraproduct.eastus2.data.azurecr.io \ https://blueexpinfraproduct.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：

- 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"](#)。
- 从 Google Cloud 激活云壳。
- 上传包含所需权限的 YAML 文件。
- 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：

- 从 IAM 和管理服务中，选择 服务帐户 > 创建服务帐户。
- 输入服务帐户详细信息并选择*创建并继续*。
- 选择您刚刚创建的角色。
- 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。

- 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。
- 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
代理服务帐户	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.blueexp.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com \ https://console.netapp.com \ https://components.console.blueexp.netapp.com \ https://cdn.auth0.com	在NetApp Console中提供功能和服务。

端点	目的
https://bluexpinfraproduct.eastus2.data.azurecr.io \ https://bluexpinfraproduct.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。如果您使用"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.preview.get
- config.preview.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
代理服务帐户	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，您需要将其更改为 `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://bluexpinfraproduct.eastus2.data.azurecr.io \ https://bluexpinfraproduct.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。如果您使用"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：

- 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"](#)。
- 从 Google Cloud 激活云壳。
- 上传包含所需权限的 YAML 文件。
- 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：

- 从 IAM 和管理服务中，选择 服务帐户 > 创建服务帐户。
- 输入服务帐户详细信息并选择*创建并继续*。
- 选择您刚刚创建的角色。
- 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。

- 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。
- 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
代理服务帐户	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才能访问互联网，则需要添加代理信息。您可以在安装过程中添加显式代理。

--proxy 和 --cacert 参数是可选的，系统不会提示您添加它们。如果您有显式代理服务器，则需要输入如图所示的参数。



如果要配置透明代理，可以在安装完成后进行配置。["了解代理维护控制台"](#)

+

以下是使用 CA 签名证书配置显式代理服务器的示例：

+

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

+

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

```
+ * http://address:port * http://user-name:password@address:port * http://domain-name%92user-  
name:password@address:port * https://address:port * https://user-name:password@address:port *  
https://domain-name%92user-name:password@address:port
```

+ 注意以下事项：

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

+ 例如：

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

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

- a. 通过 SSH 连接到控制台代理虚拟机。
- b. 打开 `podman /usr/share/containers/containers.conf` 文件并修改 Aardvark DNS 服务的选定端口。例如，将其更改为54。

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

例如：

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

- a. 重新启动控制台代理虚拟机。
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：

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

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.blueexp.netapp.com \ https://netapp-cloud-account.auth0.com \ https://console.netapp.com \ https://components.console.blueexp.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

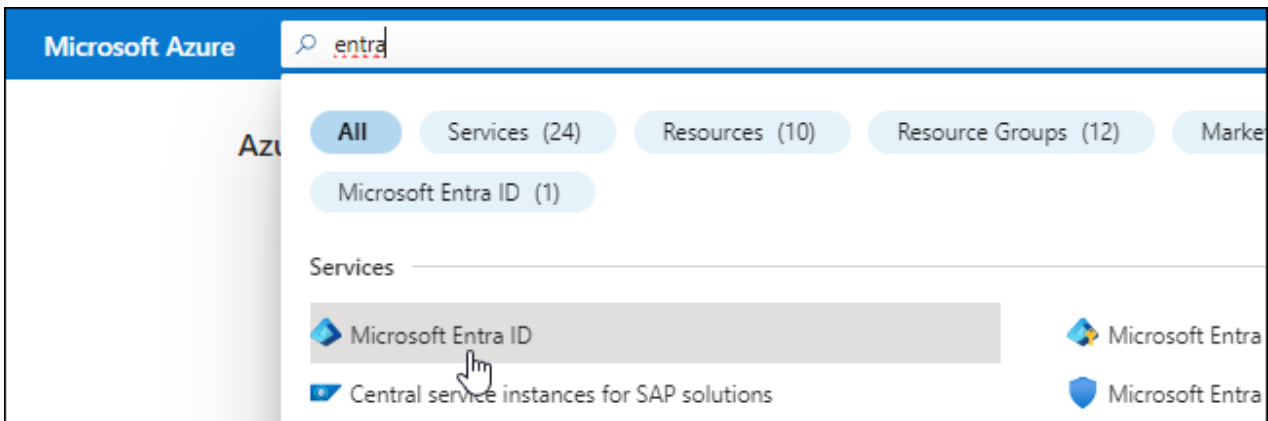
当控制台代理安装在本地时，您需要通过在 Microsoft Entra ID 中设置服务主体并获取控制台代理所需的 Azure 凭据来为控制台代理提供 Azure 权限。

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。

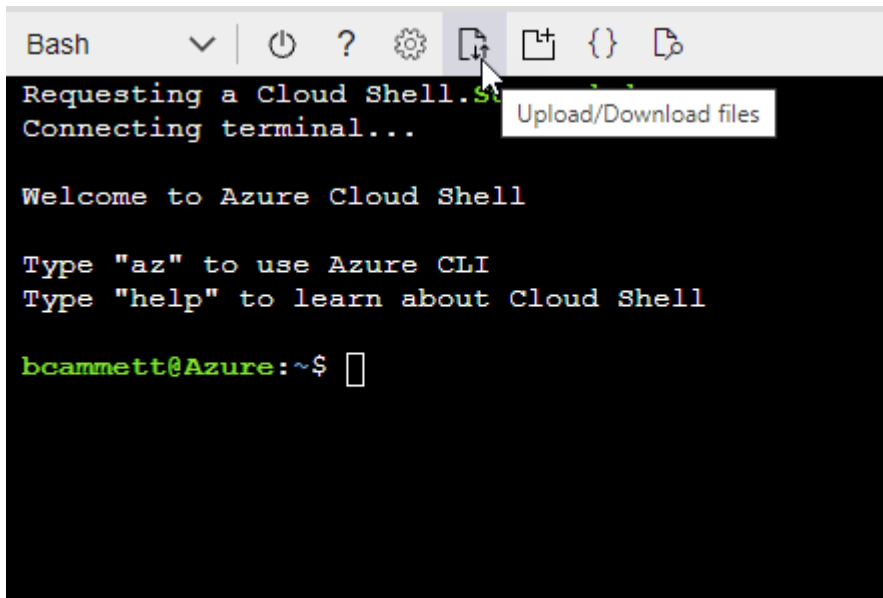
例子

```
"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。



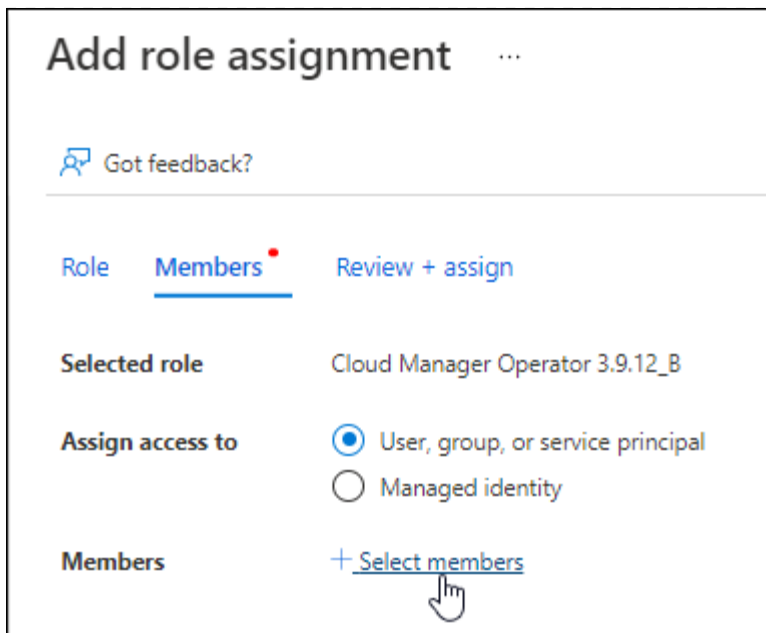
- 使用 Azure CLI 创建自定义角色：

```
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。

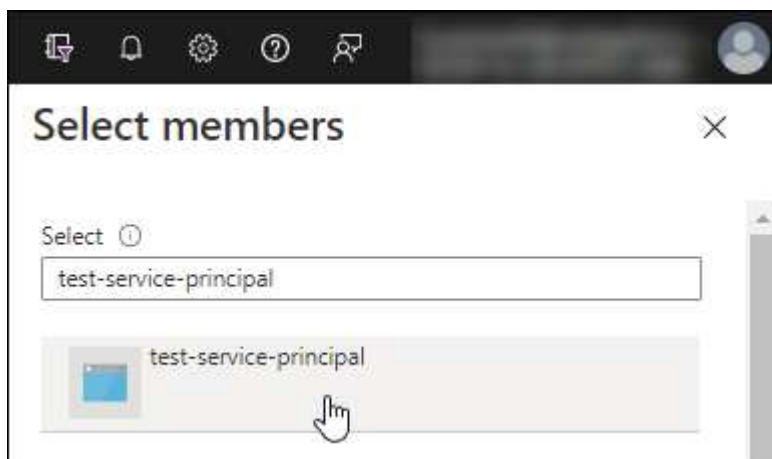
2. 将应用程序分配给角色：

- 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”。

Request API permissions

Select an API

Microsoft APIs APIs my organization uses My APIs

Commonly used Microsoft APIs

Microsoft Graph

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



Azure Batch

Schedule large-scale parallel and HPC applications in the cloud

Azure Data Catalog

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

Azure Data Explorer

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

Azure Data Lake

Access to storage and compute for big data analytic scenarios

Azure DevOps

Integrate with Azure DevOps and Azure DevOps server

Azure Import/Export

Programmatic control of import/export jobs

Azure Key Vault

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

Azure Rights Management Services

Allow validated users to read and write protected content

Azure Service Management

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

Azure Storage

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

Customer Insights

Create profile and interaction models for your products

Data Export Service for Microsoft Dynamics 365

Export data from Microsoft Dynamics CRM organization to an external destination

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

Request API permissions

[< All APIs](#)



Azure Service Management

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

What type of permissions does your application require?

Delegated permissions

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

Application permissions

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

Select permissions

[expand all](#)

Type to search

PERMISSION

ADMIN CONSENT REQUIRED

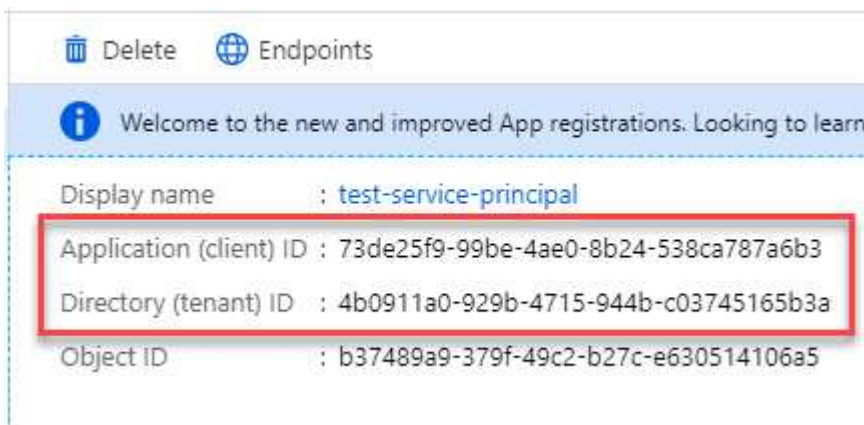


user_impersonation

Access Azure Service Management as organization users (preview)

获取应用程序的应用程序ID和目录ID

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



将 Azure 帐户添加到控制台时，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。

Client secrets

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

[+ New client secret](#)

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

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，您需要将其更改为 `netavark`。
- iii. 安装 `netavark` 和 `aardvark-dns` 使用以下命令：

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

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

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

- v. 重新启动 `podman`。

```
systemctl restart podman
```

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

```
podman info | grep networkBackend
```

Docker 引擎

按照 Docker 的文档安装 Docker Engine。

步骤

1. ["查看 Docker 的安装说明"](#)

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

2. 验证 Docker 是否已启用并正在运行。

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

手动安装控制台代理

在本地现有 Linux 主机上下载并安装控制台代理软件。

开始之前

您应该具有以下内容：

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

您可以选择在安装后配置代理服务器，但这样做需要重新启动控制台代理。

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



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

关于此任务

安装后，如果有新版本可用，控制台代理会自动更新。

步骤

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

```
unset http_proxy
unset https_proxy
```

如果不删除这些系统变量，安装将失败。

2. 下载控制台代理软件，然后将其复制到 Linux 主机。您可以从NetApp Console或NetApp支持网站下载。

- NetApp Console：转到*代理 > 管理 > 部署代理 > 本地部署 > 手动安装*。

选择下载代理安装程序文件或文件的 URL。

- NetApp支持网站（如果您还没有访问控制台的权限，则需要此网站） ["NetApp 支持站点"](#)，

3. 分配运行脚本的权限。

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

其中 <version> 是您下载的控制台代理的版本。

4. 如果在政府云环境中安装，请禁用配置检查。["了解如何禁用手动安装的配置检查。"](#)

5. 运行安装脚本。

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

如果您的网络需要代理才能访问互联网，则需要添加代理信息。您可以在安装过程中添加显式代理。

`--proxy` 和 `--cacert` 参数是可选的，系统不会提示您添加它们。如果您有显式代理服务器，则需要输入如图所示的参数。



如果要配置透明代理，可以在安装完成后进行配置。["了解代理维护控制台"](#)

+

以下是使用 CA 签名证书配置显式代理服务器的示例：

+

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

+

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

```
+ * http://address:port * http://user-name:password@address:port * http://domain-name%92user-  
name:password@address:port * https://address:port * https://user-name:password@address:port *  
https://domain-name%92user-name:password@address:port
```

+ 注意以下事项：

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

+ 例如：

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

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

a. 通过 SSH 连接到控制台代理虚拟机。

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

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

例如：

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

a. 重新启动控制台代理虚拟机。

下一步是什么？

您需要在NetApp Console中注册控制台代理。

使用NetApp Console注册控制台代理

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

步骤

1. 打开 Web 浏览器并输入控制台代理主机 URL：

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

2. 注册或登录。

3. 登录后，设置控制台：

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

当控制台代理安装在本地时，不支持限制模式。

- d. 选择*让我们开始吧*。

向NetApp Console提供云提供商凭据

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

AWS

开始之前

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

步骤

1. 选择“管理 > 凭证”。
2. 选择*组织凭证*。
3. 选择“添加凭据”并按照向导中的步骤操作。
 - a. 凭证位置：选择*Amazon Web Services > 代理。
 - b. 定义凭证：输入 AWS 访问密钥和密钥。
 - c. 市场订阅：通过立即订阅或选择现有订阅将市场订阅与这些凭证关联。
 - d. 审核：确认有关新凭证的详细信息并选择*添加*。

您现在可以前往 ["NetApp Console"](#)开始使用控制台代理。

Azure

开始之前

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

步骤

1. 选择“管理 > 凭证”。
2. 选择“添加凭据”并按照向导中的步骤操作。
 - a. 凭证位置：选择*Microsoft Azure > 代理*。
 - b. 定义凭据：输入有关授予所需权限的 Microsoft Entra 服务主体的信息：
 - 应用程序（客户端）ID
 - 目录（租户）ID
 - 客户端密钥
 - c. 市场订阅：通过立即订阅或选择现有订阅将市场订阅与这些凭证关联。
 - d. 审核：确认有关新凭证的详细信息并选择*添加*。

结果

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

使用 VCenter 在本地安装控制台代理

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



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

准备安装控制台代理

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

查看控制台代理主机要求

在安装控制台代理之前，请确保您的主机满足安装要求。

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



在 vCenter 环境中安装代理，而不是直接在 ESXi 主机上安装。

为控制台代理设置网络访问

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

连接到目标网络

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

出站互联网访问

部署控制台代理的网络位置必须具有出站互联网连接才能联系特定端点。

使用基于 Web 的 NetApp Console 时从计算机联系的端点

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

["为 NetApp 控制台准备网络"](#)。

从控制台代理联系的端点

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

下面列出的端点都是 CNAME 条目。



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

AWS

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

从控制台代理联系的端点

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

下面列出的端点都是 CNAME 条目。

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

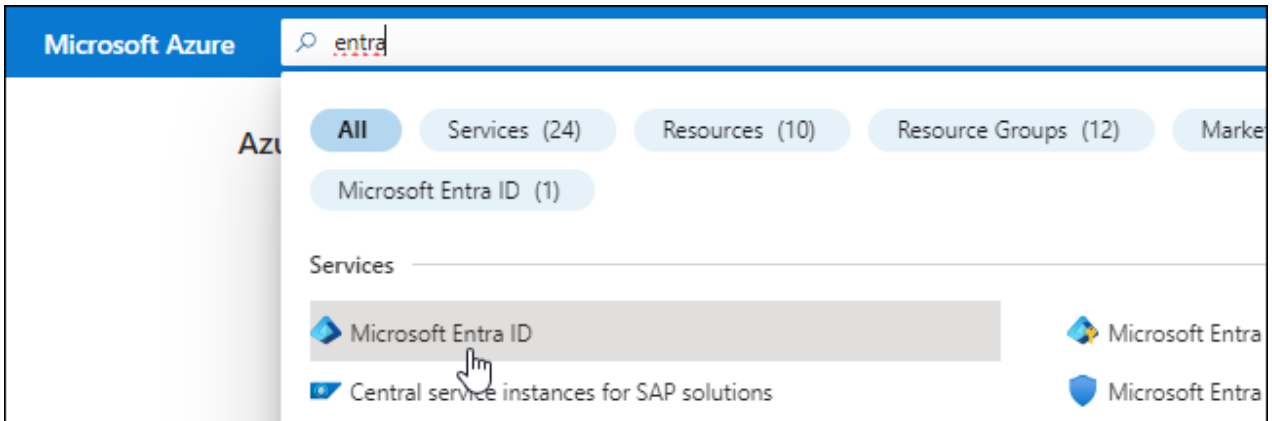
当控制台代理安装在本地时，您需要通过在 Microsoft Entra ID 中设置服务主体并获取控制台代理所需的 Azure 凭据来授予控制台代理 Azure 权限。

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。

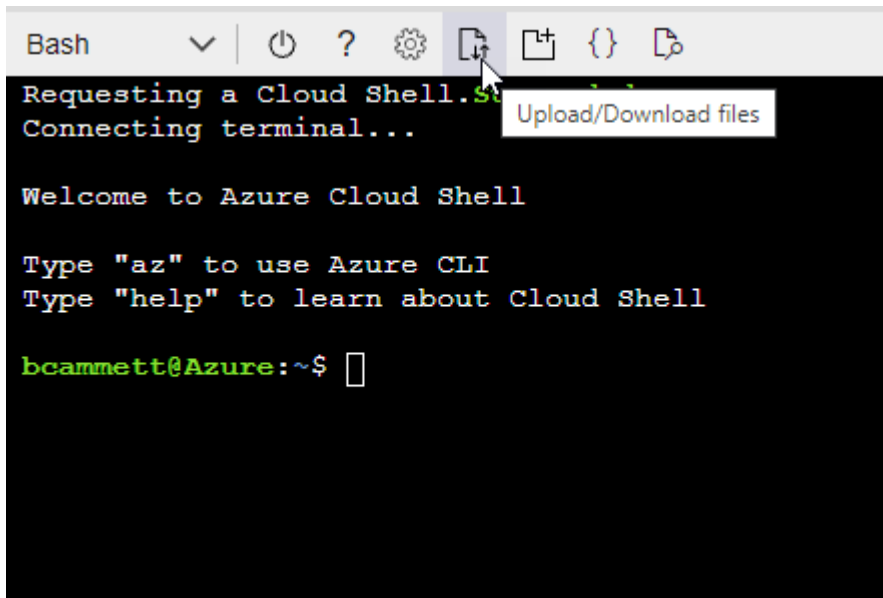
例子

```
"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。



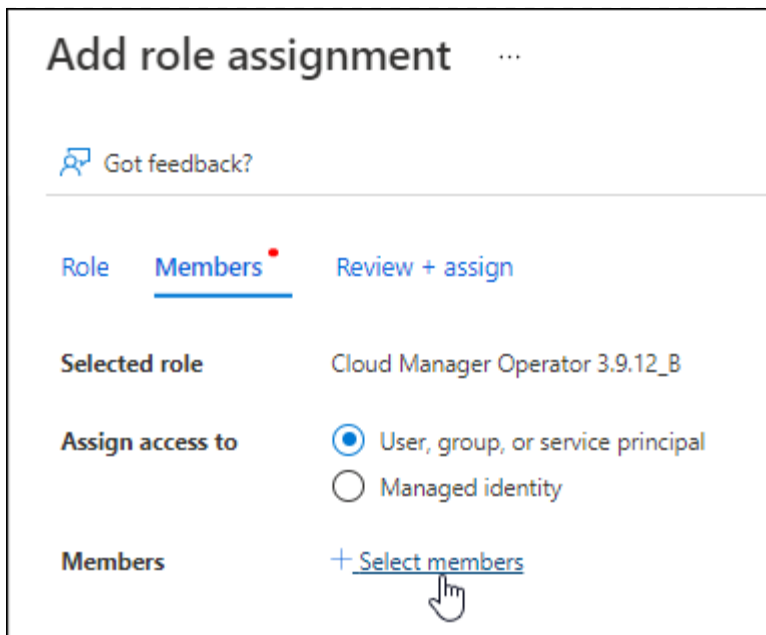
- 使用 Azure CLI 创建自定义角色：

```
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。

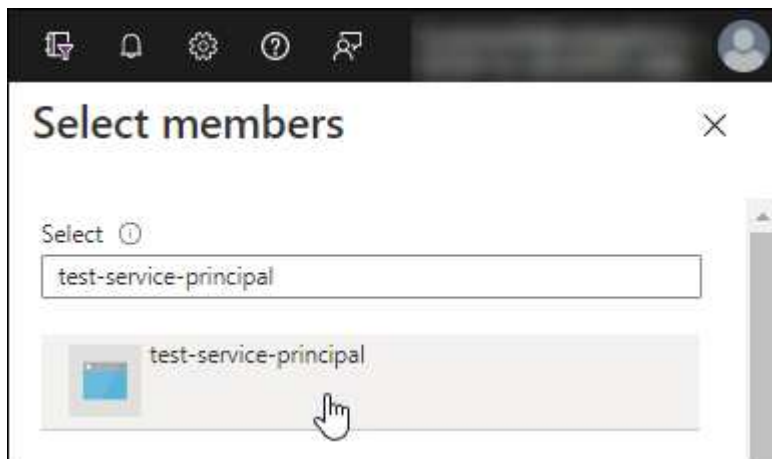
2. 将应用程序分配给角色：

- 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”。

Request API permissions

Select an API

Microsoft APIs APIs my organization uses My APIs

Commonly used Microsoft APIs

Microsoft Graph

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



Azure Batch

Schedule large-scale parallel and HPC applications in the cloud

Azure Data Catalog

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

Azure Data Explorer

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

Azure Data Lake

Access to storage and compute for big data analytic scenarios

Azure DevOps

Integrate with Azure DevOps and Azure DevOps server

Azure Import/Export

Programmatic control of import/export jobs

Azure Key Vault

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

Azure Rights Management Services

Allow validated users to read and write protected content

Azure Service Management

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

Azure Storage

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

Customer Insights

Create profile and interaction models for your products

Data Export Service for Microsoft Dynamics 365

Export data from Microsoft Dynamics CRM organization to an external destination

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

Request API permissions

< All APIs



Azure Service Management

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

What type of permissions does your application require?

Delegated permissions

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

Application permissions

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

Select permissions

[expand all](#)

Type to search

PERMISSION

ADMIN CONSENT REQUIRED

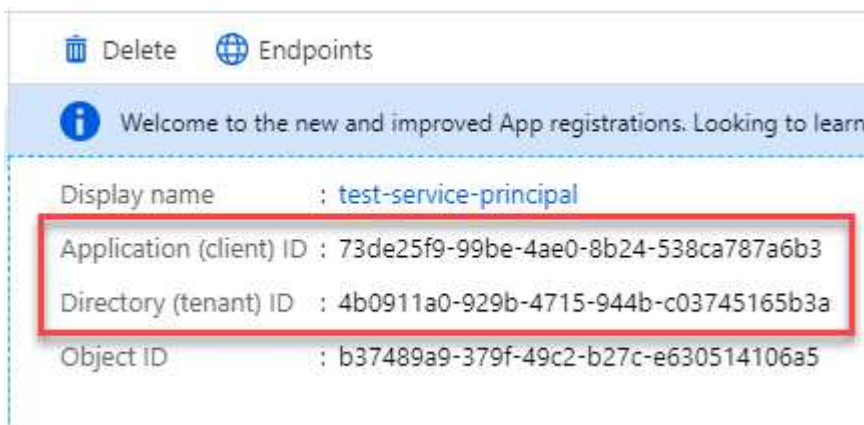


user_impersonation

Access Azure Service Management as organization users (preview)

获取应用程序的应用程序ID和目录ID

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



将 Azure 帐户添加到控制台时，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。

Client secrets

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

[+ New client secret](#)

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

在 VCenter 环境中安装控制台代理

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

下载 OVA 或复制 URL

直接从NetApp Console下载 OVA 或复制 OVA URL。

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

在您的 VCenter 中部署代理

登录您的 VCenter 环境以部署代理。

步骤

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

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

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

10. 选择您想要连接虚拟机的网络，然后选择*下一步*。确保网络为 IPv4 并且具有对所需端点的出站互联网访问权限。

11. 在*自定义模板*窗口中，填写以下字段：

◦ 代理信息

- 如果选择了显式代理，请输入代理服务器主机名或 IP 地址和端口号，以及用户名和密码。
- 如果您选择了透明代理，请上传相应的证书。

◦ 虚拟机配置

- 跳过配置检查：默认情况下未选中此复选框，这意味着代理运行配置检查以验证网络访问。
 - NetApp建议不要选中此框，以便安装包含代理的配置检查。配置检查验证代理是否具有对所需端点的网络访问权限。如果由于连接问题导致部署失败，您可以从代理主机访问验证报告和日志。在某些情况下，如果您确信代理具有网络访问权限，则可以选择跳过检查。例如，如果您仍在[使用"先前的端点"](#)用于代理升级，验证失败并出现错误。为了避免这种情况，请勾选复选框以在不进行验证检查的情况下进行安装。["了解如何更新终端节点列表"](#)。
- 维护密码：设置维护密码 `maint` 允许访问代理维护控制台的用户。
- **NTP 服务器**：指定一个或多个 NTP 服务器进行时间同步。
- **主机名**：设置此虚拟机的主机名。它不能包含搜索域。例如，FQDN console10.searchdomain.company.com 应输入为 console10。
- **主 DNS**：指定用于名称解析的主 DNS 服务器。
- **辅助 DNS**：指定用于名称解析的辅助 DNS 服务器。
- **搜索域**：指定解析主机名时使用的搜索域名。例如，如果 FQDN 是 console10.searchdomain.company.com，则输入 searchdomain.company.com。
- **IPv4 地址**：映射到主机名的 IP 地址。
- **IPv4 子网掩码**：IPv4 地址的子网掩码。
- **IPv4 网关地址**：IPv4 地址的网关地址。

12. 选择“下一步”。

13. 查看“准备完成”窗口中的详细信息，选择“完成”。

vSphere 任务栏显示控制台代理部署的进度。

14. 启动此虚拟机。



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

使用NetApp Console注册控制台代理

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

步骤

1. 打开 Web 浏览器并输入控制台代理主机 URL：

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

2. 注册或登录。

3. 登录后，设置控制台：

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

当控制台代理安装在本地时，不支持限制模式。

- d. 选择*让我们开始吧*。

将云提供商凭据添加到控制台

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

AWS

开始之前

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

步骤

1. 选择“管理 > 凭证”。
2. 选择*组织凭证*。
3. 选择“添加凭据”并按照向导中的步骤操作。
 - a. 凭证位置：选择*Amazon Web Services > 代理。
 - b. 定义凭证：输入 AWS 访问密钥和密钥。
 - c. 市场订阅：通过立即订阅或选择现有订阅将市场订阅与这些凭证关联。
 - d. 审核：确认有关新凭证的详细信息并选择*添加*。

您现在可以前往 ["NetApp Console"](#) 开始使用控制台代理。

Azure

开始之前

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

步骤

1. 选择“管理 > 凭证”。
2. 选择“添加凭据”并按照向导中的步骤操作。
 - a. 凭证位置：选择*Microsoft Azure > 代理*。
 - b. 定义凭据：输入有关授予所需权限的 Microsoft Entra 服务主体的信息：
 - 应用程序（客户端）ID
 - 目录（租户）ID
 - 客户端密钥
 - c. 市场订阅：通过立即订阅或选择现有订阅将市场订阅与这些凭证关联。
 - d. 审核：确认有关新凭证的详细信息并选择*添加*。

结果

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

本地控制台代理的端口

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

这些入站规则适用于所有NetApp Console部署模式。

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

维护控制台代理

为控制台代理维护 VCenter 或 ESXi 主机

部署控制台代理后，您可以对现有的 VCenter 或 ESXi 主机进行更改。例如，您可以增加托管控制台代理的 VM 实例的 CPU 或 RAM。

使用 VM Web 控制台执行以下维护任务：

- 增加磁盘大小
- 重启代理
- 更新静态路由
- 更新搜索域

限制

尚不支持通过控制台升级代理。此外，您只能查看有关 IP 地址、DNS 和网关的信息。

访问虚拟机维护控制台

您可以从 VSphere 客户端访问维护控制台。

步骤

1. 打开 VSphere 客户端并登录到您的 VCenter。
2. 选择托管控制台代理的 VM 实例。
3. 选择*启动 Web 控制台*。
4. 使用创建 VM 实例时指定的用户名和密码登录 VM 实例。用户名是 `maint` 密码是您在创建 VM 实例时指定的密码。

修改主用户密码

您可以更改 `maint` 用户。

步骤

1. 打开 VSphere 客户端并登录到您的 VCenter。
2. 选择托管控制台代理的 VM 实例。
3. 选择*启动 Web 控制台*。

4. 使用创建 VM 实例时指定的用户名和密码登录 VM 实例。用户名是 `maint` 密码是您在创建 VM 实例时指定的密码。
5. 进入 `1` 查看 `System Configuration` 菜单。
6. 进入 `1` 更改维护用户密码并按照屏幕上的提示进行操作。

增加虚拟机实例的 CPU 或 RAM

您可以增加托管控制台代理的 VM 实例的 CPU 或 RAM。

在您的 VCenter 或 ESXi 主机中编辑 VM 实例设置，然后使用维护控制台应用更改。

VSphere 客户端中的步骤

1. 打开 VSphere 客户端并登录到您的 VCenter。
2. 选择托管控制台代理的 VM 实例。
3. 右键单击 VM 实例并选择*编辑设置*。
4. 增加用于 /opt 或 /var 分区的硬盘空间。
 - a. 选择“硬盘 2”以增加用于 /opt 的硬盘空间。
 - b. 选择*硬盘 3* 来增加 /var 使用的硬盘空间。
5. 保存更改。

维护控制台中的步骤

1. 打开 VSphere 客户端并登录到您的 VCenter。
2. 选择托管控制台代理的 VM 实例。
3. 选择*启动 Web 控制台*。
4. 使用创建 VM 实例时指定的用户名和密码登录 VM 实例。用户名是 `maint` 密码是您在创建 VM 实例时指定的密码。
5. 进入 `1` to view the `System Configuration` 菜单。
6. 进入 `2` 并按照屏幕上的提示进行操作。控制台扫描新设置并增加分区的大小。

查看代理虚拟机的网络设置

查看 VSphere 客户端中代理 VM 的网络设置以确认或排除网络问题。您只能查看（不能更新）以下网络设置：IP 地址和 DNS 详细信息。

步骤

1. 打开 VSphere 客户端并登录到您的 VCenter。
2. 选择托管控制台代理的 VM 实例。
3. 选择*启动 Web 控制台*。
4. 使用创建 VM 实例时指定的用户名和密码登录 VM 实例。用户名是 `maint` 密码是您在创建 VM 实例时指定的密码。
5. 进入 `2` 查看 `Network Configuration` 菜单。
6. 输入 1 到 6 之间的数字来查看相应的网络设置。

更新代理虚拟机的静态路由

根据需要添加、更新或删除代理虚拟机的静态路由。

步骤

1. 打开 VSphere 客户端并登录到您的 VCenter。
2. 选择托管控制台代理的 VM 实例。
3. 选择*启动 Web 控制台*。
4. 使用创建 VM 实例时指定的用户名和密码登录 VM 实例。用户名是 `maint` 密码是您在创建 VM 实例时指定的密码。
5. 进入 `2` 查看 `Network Configuration` 菜单。
6. 进入 `7` 更新静态路由并按照屏幕上的提示进行操作。
7. 按 Enter。
8. 或者，进行其他更改。
9. 进入 `9` 提交您的更改。

更新代理虚拟机的域搜索设置

您可以更新代理虚拟机的搜索域设置。

步骤

1. 打开 VSphere 客户端并登录到您的 VCenter。
2. 选择托管控制台代理的 VM 实例。
3. 选择*启动 Web 控制台*。
4. 使用创建 VM 实例时指定的用户名和密码登录 VM 实例。用户名是 `maint` 密码是您在创建 VM 实例时指定的密码。
5. 进入 `2` 查看 `Network Configuration` 菜单。
6. 进入 `8` 更新域搜索设置并按照屏幕上的提示进行操作。
7. 按 Enter。
8. 或者，进行其他更改。
9. 进入 `9` 提交您的更改。

访问代理诊断工具

访问诊断工具来解决控制台代理的问题。NetApp 支持可能会在解决问题时要求您执行此操作。

步骤

1. 打开 VSphere 客户端并登录到您的 VCenter。
2. 选择托管控制台代理的 VM 实例。
3. 选择*启动 Web 控制台*。
4. 使用创建 VM 实例时指定的用户名和密码登录 VM 实例。用户名是 `maint` 密码是您在创建 VM 实例时指定的密码。

5. 进入 `3` 查看支持和诊断菜单。
6. 进入 `1` 访问诊断工具并按照屏幕上的提示进行操作。 + 例如，您可以验证所有代理服务是否正在运行。["检查控制台代理状态"](#)。

远程访问代理诊断工具

您可以使用 Putty 等工具远程访问诊断工具。通过分配一次性密码启用对代理 VM 的 SSH 访问。

SSH 访问支持复制和粘贴等高级终端功能。

步骤

1. 打开 VSphere 客户端并登录到您的 VCenter。
2. 选择托管控制台代理的 VM 实例。
3. 选择*启动 Web 控制台*。
4. 使用创建 VM 实例时指定的用户名和密码登录 VM 实例。用户名是 `maint` 密码是您在创建 VM 实例时指定的密码。
5. 进入 `3` 查看 `Support and Diagnostics` 菜单。
6. 进入 `2` 访问诊断工具并按照屏幕上的提示配置 24 小时后过期的一次性密码。
7. 使用 SSH 工具（例如 Putty）通过用户名连接到代理虚拟机 `diag` 以及您配置的一次性密码。

安装 CA 签名的证书以进行基于 Web 的控制台访问

当您在受限模式下使用 NetApp Console 时，可以从部署在云区域或本地的控制台代理虚拟机访问用户界面。默认情况下，控制台使用自签名 SSL 证书为控制台代理上运行的基于 Web 的控制台提供安全的 HTTPS 访问。

如果您的业务需要，您可以安装由证书颁发机构 (CA) 签名的证书，它比自签名证书提供更好的安全保护。安装证书后，当用户访问基于 Web 的控制台时，控制台将使用 CA 签名的证书。

安装 HTTPS 证书

安装由 CA 签名的证书，以便安全访问在控制台代理上运行的基于 Web 的控制台。

关于此任务

您可以使用以下选项之一安装证书：

- 从控制台生成证书签名请求 (CSR)，将证书请求提交给 CA，然后在控制台代理上安装 CA 签名的证书。

控制台用于生成 CSR 的密钥对存储在控制台代理内部。当您在控制台代理上安装证书时，控制台会自动检索相同的密钥对（私钥）。

- 安装您已有的 CA 签名证书。

使用此选项，CSR 不会通过控制台生成。您单独生成 CSR 并将私钥存储在外部。安装证书时，您需要向控制台提供私钥。

步骤

1. 选择“管理 > 代理”。
2. 在*概述*页面上，选择控制台代理的操作菜单并选择*HTTPS 设置*。

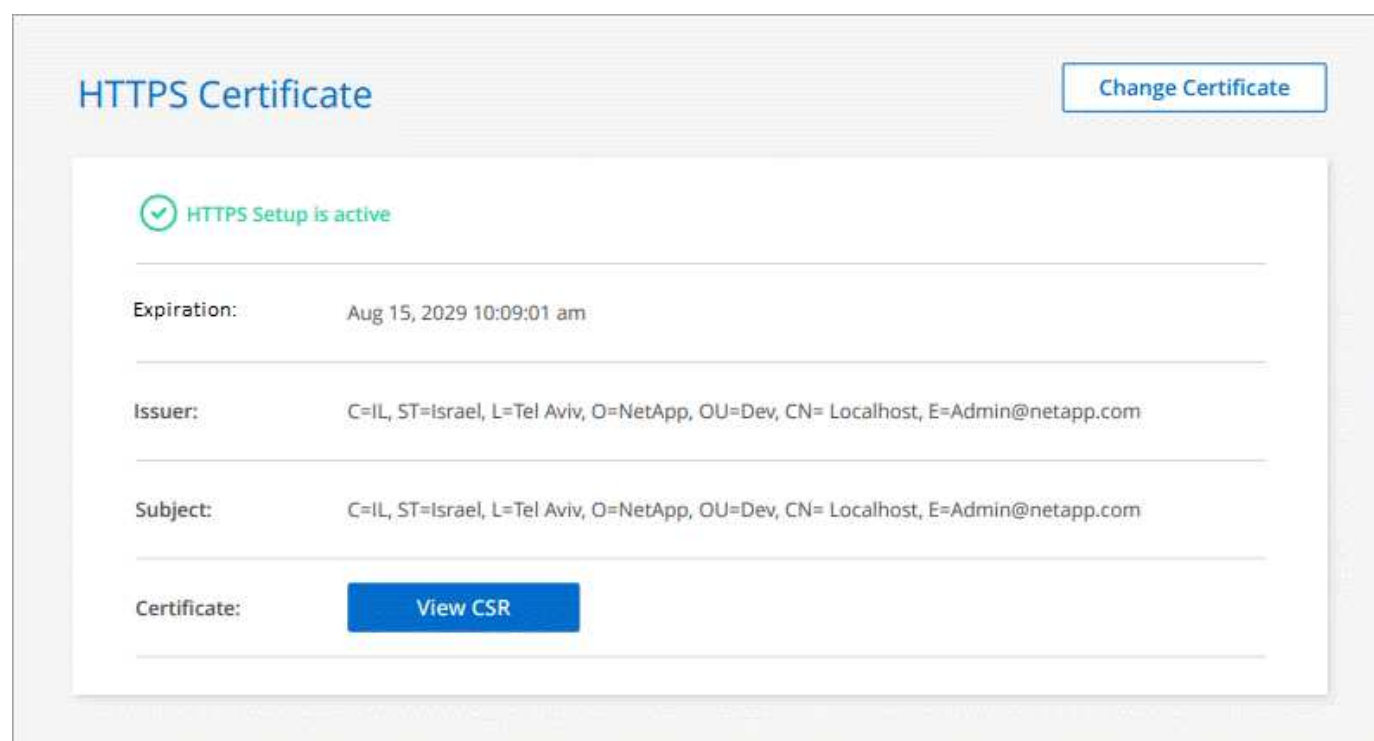
必须连接控制台代理才能进行编辑。

3. 在 HTTPS 设置页面中，通过生成证书签名请求 (CSR) 或安装您自己的 CA 签名证书来安装证书：

选项	描述
生成 CSR	a. 输入控制台代理主机的主机名或 DNS（其通用名称），然后选择 生成 CSR。 - 控制台显示证书签名请求。 b. 使用 CSR 向 CA 提交 SSL 证书请求。 - 证书必须使用隐私增强邮件 (PEM) Base-64 编码的 X.509 格式。 c. 上传证书文件，然后选择*安装*。
安装您自己的 CA 签名证书	a. 选择*安装 CA 签名证书*。 b. 加载证书文件和私钥，然后选择*安装*。 - 证书必须使用隐私增强邮件 (PEM) Base-64 编码的 X.509 格式。

结果

控制台代理现在使用 CA 签名的证书来提供安全的 HTTPS 访问。下图显示了配置为安全访问的代理：



续订控制台 HTTPS 证书

您应该在代理的 HTTPS 证书到期之前更新它，以确保安全访问。如果您未在证书到期前续订，则当用户使用 HTTPS 访问 Web 控制台时会出现警告。

步骤

1. 选择“管理 > 代理”。
2. 在*概述*页面上，选择控制台代理的操作菜单并选择*HTTPS 设置*。

显示有关证书的详细信息，包括到期日期。

3. 选择*更改证书*并按照步骤生成 CSR 或安装您自己的 CA 签名证书。

配置控制台代理以使用代理服务器

如果您的公司政策要求您使用代理服务器进行所有与互联网的通信，那么您需要配置您的代理以使用该代理服务器。如果您在安装期间没有将控制台代理配置为使用代理服务器，那么您可以随时将控制台代理配置为使用该代理服务器。

代理的代理服务器无需公共 IP 或 NAT 网关即可实现出站互联网访问。代理服务器仅为控制台代理提供出站连接，而不为 Cloud Volumes ONTAP 系统提供出站连接。

如果 Cloud Volumes ONTAP 系统缺少出站互联网访问，控制台会将其配置为使用控制台代理的代理服务器。您必须确保控制台代理的安全组允许通过端口 3128 进行入站连接。部署控制台代理后打开此端口。

如果控制台代理本身没有出站互联网连接，Cloud Volumes ONTAP 系统将无法使用配置的代理服务器。

支持的配置

- 为 Cloud Volumes ONTAP 系统提供服务的代理支持透明代理服务器。如果您将 NetApp 数据服务与 Cloud Volumes ONTAP 一起使用，请为 Cloud Volumes ONTAP 创建专用代理，您可以在其中使用透明代理服务器。
- 所有代理都支持显式代理服务器，包括管理 Cloud Volumes ONTAP 系统的代理和管理 NetApp 数据服务的代理。
- HTTP 和 HTTPS。
- 代理服务器可以位于云端或您的网络中。



一旦配置了代理，您就无法更改代理类型。如果需要更改代理类型，请删除控制台代理并添加具有新代理类型的新代理。

在控制台代理上启用显式代理

当您将控制台代理配置为使用代理服务器时，该代理及其管理的 Cloud Volumes ONTAP 系统（包括任何 HA 中介）都会使用代理服务器。

此操作重新启动控制台代理。在继续之前，请验证控制台代理是否空闲。

步骤

1. 选择“管理 > 代理”。

2. 在*概览*页面上，选择控制台代理的操作菜单，然后选择*编辑代理*。

控制台代理必须处于活动状态才能对其进行编辑。

3. 选择*HTTP 代理配置*。
4. 在配置类型字段中选择*显式代理*。
5. 选择*启用代理*。
6. 使用语法指定服务器 `<a href="http://<em>address:port</em>" class="bare">http://<em>address:port</em></a>`或者 `<a href="https://<em>address:port</em>" class="bare">https://<em>address:port</em></a>`
7. 如果服务器需要基本身份验证，请指定用户名和密码。

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，您必须输入 \ 的 ASCII 代码，如下所示：domain-name%92user-name

例如：netapp%92proxy

- 控制台不支持包含 @ 字符的密码。

8. 选择*保存*。

为控制台代理启用透明代理

仅Cloud Volumes ONTAP支持在控制台代理上使用透明代理。如果您除了Cloud Volumes ONTAP之外还使用NetApp数据服务，则应创建一个单独的代理来用于数据服务或用于Cloud Volumes ONTAP。

启用透明代理前，请确保满足以下要求：

- 代理与透明代理服务器安装在同一网络上。
- 代理服务器上启用了 TLS 检查。
- 您有一个 PEM 格式的证书，与透明代理服务器上使用的证书相匹配。
- 您不要将控制台代理用于除Cloud Volumes ONTAP之外的任何NetApp数据服务。

要配置现有代理以使用透明代理服务器，您可以使用控制台代理维护工具，该工具可通过控制台代理主机上的命令行获取。

当您配置代理服务器时，控制台代理将重新启动。在继续之前，请验证控制台代理是否空闲。

步骤

确保您拥有代理服务器的 PEM 格式的证书文件。如果您没有证书，请联系您的网络管理员获取证书。

1. 在控制台代理主机上打开命令行界面。
2. 导航到控制台代理维护工具目录： `/opt/application/netapp/service-manager-2/agent-maint-console`
3. 运行以下命令启用透明代理，其中 `/home/ubuntu/<certificate-file>.pem` 是您拥有的代理服务器证书文件的目录和名称：

```
./agent-maint-console proxy add -c /home/ubuntu/<certificate-file>.pem
```

确保证书文件为 PEM 格式并与命令位于同一目录中，或者指定证书文件的完整路径。

```
./agent-maint-console proxy add -c /home/ubuntu/<certificate-file>.pem
```

修改控制台代理的透明代理

您可以使用以下方法更新控制台代理现有的透明代理服务器：`proxy update`通过使用命令来移除透明代理服务器 `proxy remove`命令。更多信息，请查阅相关文档。["代理维护控制台"](#)。



一旦配置了代理，您就无法更改代理类型。如果需要更改代理类型，请删除控制台代理并添加具有新代理类型的新代理。

如果控制台代理无法访问互联网，请更新它

如果您的网络代理配置发生变化，您的代理可能会失去对互联网的访问权限。例如，如果有人更改了代理服务器的密码或更新了证书。在这种情况下，您需要直接从控制台代理主机访问 UI 并更新设置。确保您可以通过网络访问控制台代理主机，并且可以登录控制台。

启用直接 API 流量

如果您已将控制台代理配置为使用代理服务器，则可以在控制台代理上启用直接 API 流量，以便直接向云提供商服务发送 API 调用，而无需通过代理。在 AWS、Azure 或 Google Cloud 中运行的代理支持此选项。

如果您禁用带有 Cloud Volumes ONTAP 的 Azure Private Links 并使用服务端点，请启用直接 API 流量。否则，流量将无法正确路由。

["了解有关将 Azure Private Link 或服务端点与 Cloud Volumes ONTAP 结合使用的更多信息"](#)

步骤

1. 选择“管理 > 代理”。
2. 在*概览*页面上，选择控制台代理的操作菜单，然后选择*编辑代理*。

控制台代理必须处于活动状态才能对其进行编辑。

3. 选择*支持直接 API 流量*。
4. 选中复选框以启用该选项，然后选择*保存*。

控制台代理故障排除

要解决控制台代理的问题，您可以自行验证问题或与 NetApp 支持人员合作，他们可能会询问您的系统 ID、代理版本或最新的 AutoSupport 消息。

如果您有 NetApp 支持站点帐户，您还可以查看["NetApp 知识库"](#)。

常见错误消息和解决方法

此表列出了常见的错误信息以及解决方法：

错误消息	说明	该怎么办
无法加载控制台代理 UI	代理安装失败	• 验证服务管理器服务是否处于活动状态。 • 验证所有容器是否正在运行。 • 确保您的防火墙允许访问端口 8888 的服务。 • 如果仍有问题，请联系客服。
无法访问NetApp代理 UI	尝试访问代理的 IP 地址时会出现此消息。如果代理没有正确的网络访问权限或不稳定，则代理可能无法初始化。	• 连接到控制台代理。 • 验证 Service Manager 服务 • 验证代理是否具有所需的网络访问权限。"了解有关所需网络访问端点的更多信息。"
无法加载代理设置	当您尝试访问代理设置页面时，控制台会显示此消息。	• 检查 OCCM 容器是否正在运行并正常工作。 • 如果问题仍然存在，请联系支持人员。
无法加载代理的支持信息。	如果代理无法访问您的支持帐户，则会显示此消息。	• 确认代理程序拥有对所需端点的出站访问权限。"了解有关所需网络访问端点的更多信息。"

检查控制台代理状态

使用以下命令之一来验证您的控制台代理。所有服务的状态都应为“正在运行”。如果不是这种情况，请联系NetApp支持。



有关访问控制台代理诊断的详细信息，请参阅以下主题：

- ["检查控制台代理状态（适用于 Linux 主机部署）"](#)
- ["检查控制台代理状态（针对 VCenter 部署）"](#)

Docker（用于 Ubuntu 和 VCenter 部署）

```
docker ps -a
```

Podman（用于 RedHat Enterprise Linux 部署）

```
podman ps -a
```

查看控制台代理版本

查看控制台代理版本以确认升级或与您的NetApp代表共享。

步骤

1. 选择*管理>支持>代理*。

控制台在页面顶部显示版本。

验证网络访问

确保控制台代理具有所需的网络访问权限。["了解有关所需网络接入点的更多信息。"](#)

对控制台代理运行配置检查

从控制台或代理维护控制台对控制台代理运行配置检查，以确保它们已连接。

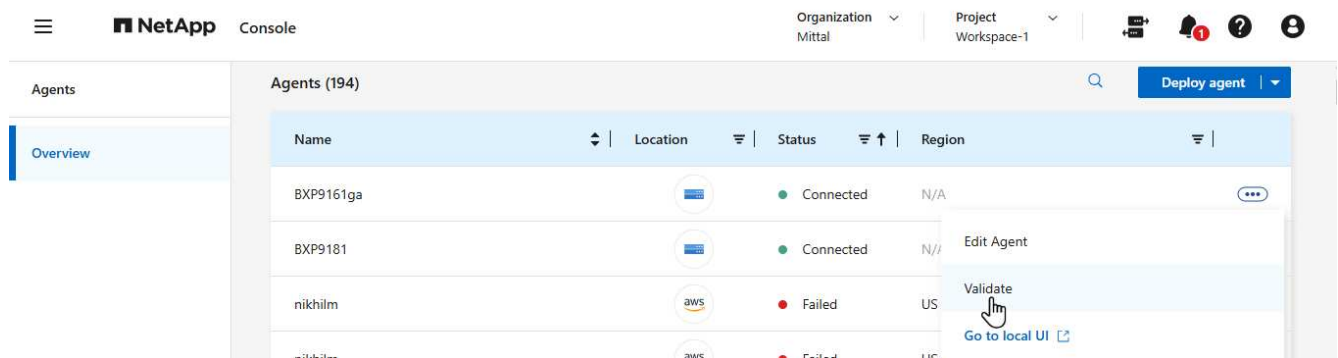
您还可以使用代理维护控制台运行配置检查。["了解更多关于使用 config-checker validate 命令的信息。"](#)



您只能验证状态为“已连接”的代理。

控制台操作步骤

1. 选择“管理 > 代理”。
2. 选择要检查的控制台代理的操作菜单，然后选择“验证”。



验证过程最多可能需要 15 分钟。结果会在完成后显示。

控制台代理安装问题

如果安装失败，请查看报告和日志以解决问题。

您还可以直接从以下目录中的控制台代理主机访问 JSON 格式的验证报告和配置日志：

```
/tmp/netapp-console-agents/logs  
  
/tmp/netapp-console-agents/results.json
```



- 对于新代理部署，NetApp会检查以下端点：["此处列出"](#)。如果您使用之前用于升级的端点，则此配置检查将失败并出现错误，["此处列出"](#)。NetApp建议您尽快更新防火墙规则，以允许访问当前端点并阻止访问以前的端点["了解如何更新您的网络"](#)。
- 如果您更新防火墙中的端点，您现有的代理将继续工作。

禁用手动安装的配置检查

有时您可能需要禁用在安装期间验证出站连接的配置检查。例如，在政府云环境中手动安装代理时，需要禁用配置检查，否则安装将失败。

步骤

您可以通过在 `com/opt/application/netapp/service-manager-2/config.json` 文件中设置 `skipConfigCheck` 标志来禁用配置检查。默认情况下，此标志设置为 `false`，并且配置检查会验证代理的出站访问。将此标志设置为 `true` 以禁用检查。在完成此步骤之前，请先熟悉 JSON 语法。

要重新启用配置检查，请使用以下步骤并将 `_skipConfigCheck_` 标志设置为 `false`。

步骤

1. 以 `root` 身份或使用 `sudo` 权限访问控制台代理主机。
2. 创建 `/opt/application/netapp/service-manager-2/config.json` 文件的备份副本，以确保您可以恢复更改。
3. 通过运行以下命令停止服务管理器 2 服务：

```
systemctl stop netapp-service-manager.service
```

1. 编辑 `/opt/application/netapp/service-manager-2/config.json` 文件并将 `skipConfigCheck` 标志的值更改为 `true`。

```
"skipConfigCheck": true
```

2. 保存您的文件。
3. 通过运行以下命令重新启动服务管理器 2 服务：

```
systemctl restart netapp-service-manager.service
```

与NetApp支持部门合作

如果您无法解决控制台代理的问题，您可能需要联系NetApp支持。NetApp支持人员可能会要求您提供控制台代理 ID，或者如果他们还没有控制台代理日志，则要求您将控制台代理日志发送给他们。

查找控制台代理 ID

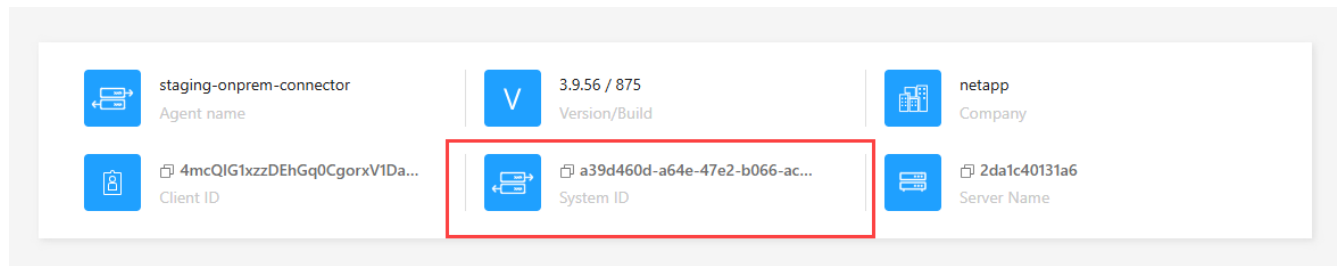
为了帮助您入门，您可能需要控制台代理的系统 ID。该 ID 通常用于许可和故障排除目的。

步骤

1. 选择*管理>支持>代理*。

您可以在页面顶部找到系统 ID。

例子



2. 将鼠标悬停在 ID 上并单击即可复制它。

下载或发送AutoSupport消息

如果您遇到问题，NetApp可能会要求您向NetApp支持发送AutoSupport消息以进行故障排除。



由于负载均衡，NetApp Console最多需要五个小时才能发送AutoSupport消息。对于紧急通信，请下载文件并手动发送。

步骤

1. 选择*管理>支持>代理*。
2. 根据您需要向NetApp支持发送信息的方式，选择以下选项之一：
 - a. 选择将AutoSupport消息下载到本地计算机的选项。然后，您可以使用首选方法将其发送给NetApp支持。
 - b. 选择“发送AutoSupport”以将消息直接发送给NetApp支持。

修复使用 **Google Cloud NAT** 网关时下载失败的问题

控制台代理会自动下载Cloud Volumes ONTAP 的软件更新。如果您的配置使用 Google Cloud NAT 网关，则可能导致下载失败。您可以通过限制软件映像划分的部分数来解决此问题。此步骤必须使用 API 完成。

步骤

1. 向 /occm/config 提交 PUT 请求，并将以下 JSON 作为正文：

```
{
  "maxDownloadSessions": 32
}
```

maxDownloadSessions 的值可以是 1 或任何大于 1 的整数。如果值为1，则下载的图像不会被分割。

请注意，32 是一个示例值。该值取决于您的 NAT 配置和同时会话的数量。

["了解有关 /occm/config API 调用的更多信息"](#)

从**NetApp**知识库获取帮助

["查看NetApp支持团队创建的故障排除信息"](#)。

卸载并删除控制台代理

卸载控制台代理以解决问题或将其从主机中永久删除。您需要使用的步骤取决于您使用的部署模式。从环境中删除控制台代理后，您可以将其从控制台中删除。

["了解NetApp Console部署模式"](#)。

使用标准或受限模式时卸载代理

如果您使用的是标准模式或受限模式（换句话说，代理主机具有出站连接），那么您应该按照以下步骤卸载代理。

步骤

1. 连接到代理的 Linux VM。
2. 从 Linux 主机运行卸载脚本：

```
/opt/application/netapp/service-manager-2/uninstall.sh [silent]
```

silent 运行脚本而不提示您确认。

从控制台中删除控制台代理

如果您删除了代理虚拟机或卸载了代理，则应将其从控制台的代理列表中删除。删除代理虚拟机或卸载代理软件后，代理在控制台中会显示“已断开连接”的状态。

删除控制台代理时请注意以下事项：

- 此操作不会删除虚拟机。
- 此操作无法恢复 - 一旦删除控制台代理，就无法将其添加回来。

步骤

1. 选择“管理 > 代理”。
2. 在“概览”页面上，选择已断开连接的代理的操作菜单，然后选择“移除代理”。
3. 输入代理人的姓名进行确认，然后选择*删除*。

管理云提供商凭证

AWS

了解**NetApp Console**中的 **AWS** 凭证和权限

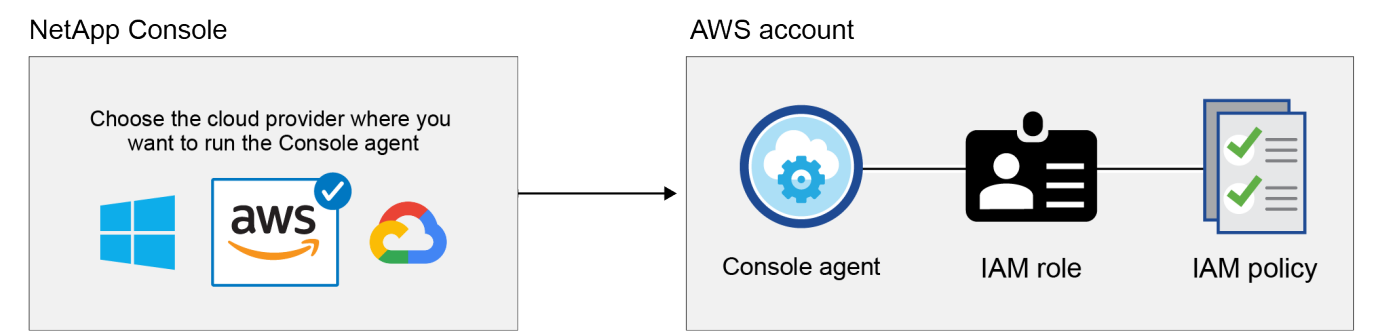
您可以通过**NetApp Console**直接管理 AWS 凭证和市场订阅，通过在控制台代理部署期间提供适当的 IAM 凭证并将其与 AWS Marketplace 订阅关联以进行计费，来确保Cloud

Volumes ONTAP和其他数据服务的安全部署。

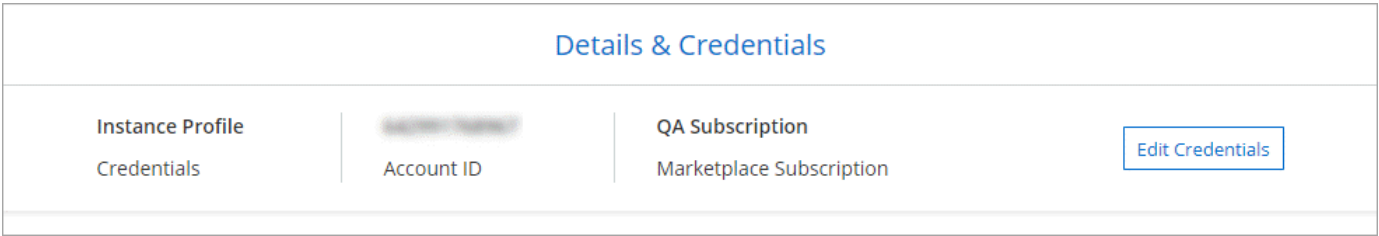
初始 **AWS** 凭证

从控制台部署控制台代理时，您需要提供 IAM 角色的 ARN 或 IAM 用户的访问密钥。身份验证方法必须具有在 AWS 中部署控制台代理的权限。所需权限列于表中["AWS代理部署策略"](#)。

当控制台在 AWS 中启动控制台代理时，它会为代理创建一个 IAM 角色和一个配置文件。它还附加了一项策略，为控制台代理提供管理该 AWS 账户内的资源和流程的权限。["查看代理如何使用权限"](#)。



如果您添加新的Cloud Volumes ONTAP系统，控制台将默认选择以下 AWS 凭证：



使用初始 AWS 凭证部署所有Cloud Volumes ONTAP系统，或者您可以添加其他凭证。

额外的 **AWS** 凭证

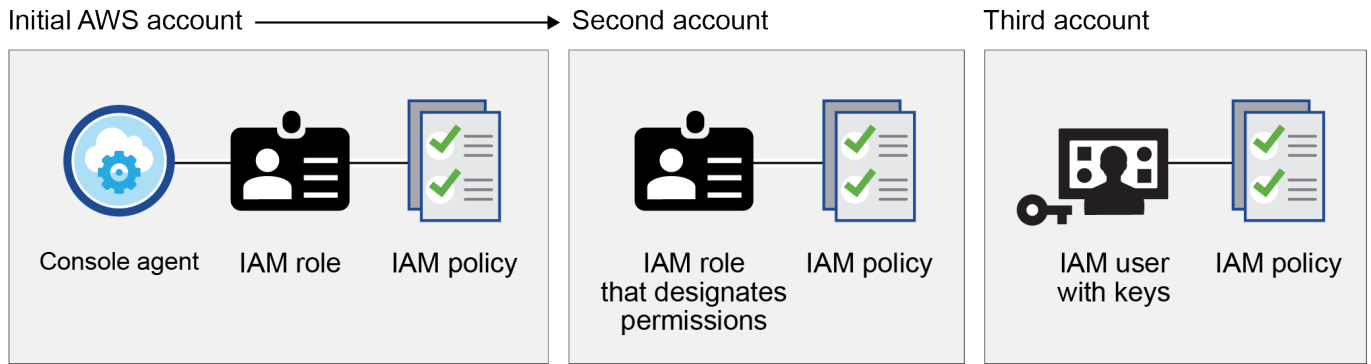
在以下情况下，您可能会向控制台添加其他 AWS 凭证：

- 要将您现有的控制台代理与额外的 AWS 账户一起使用，请执行以下操作：
- 在特定 AWS 账户中创建新代理
- 创建和管理 FSx for ONTAP文件系统

请参阅以下部分以了解更多详细信息。

添加 **AWS** 凭证以将控制台代理与另一个 **AWS** 账户一起使用

要将控制台与额外的 AWS 账户一起使用，请提供 AWS 密钥或受信任账户中角色的 ARN。下图显示了两个附加账户，一个通过受信任账户中的 IAM 角色提供权限，另一个通过 IAM 用户的 AWS 密钥提供权限：



您可以通过指定 IAM 角色的 Amazon 资源名称 (ARN) 或 IAM 用户的 AWS 密钥，将帐户凭证添加到控制台。

例如，您可以在创建新的Cloud Volumes ONTAP系统时在凭据之间切换：

Edit Credentials & Add Subscription

Associate Subscription to Credentials ⓘ

Credentials

- keys | Account ID: [redacted]
- Instance Profile | Account ID: [redacted]
- casaba QA subscription

+ Add Subscription

Apply Cancel

["了解如何将 AWS 凭证添加到现有代理。"](#)

添加 **AWS** 凭证以创建控制台代理

添加 AWS 凭证即可获得创建控制台代理的权限。

["了解如何将 AWS 凭证添加到控制台以创建控制台代理"](#)

为 **FSx for ONTAP** 添加 **AWS** 凭证

将 AWS 凭证添加到控制台以提供创建和管理 FSx for ONTAP 系统所需的权限。

["了解如何将 AWS 凭证添加到 Amazon FSx for ONTAP 控制台"](#)

凭证和市场订阅

您必须将添加到控制台代理的凭证与 AWS Marketplace 订阅关联起来，才能按小时费率 (PAYGO) 支付 Cloud Volumes ONTAP 费用，并通过年度合同支付其他 NetApp 数据服务费用。["了解如何关联 AWS 订阅"](#)。

请注意以下有关 AWS 凭证和市场订阅的事项：

- 您只能将一个 AWS Marketplace 订阅与一组 AWS 凭证关联
- 您可以使用新的订阅替换现有的市场订阅

常见问题解答

以下问题与凭证和订阅有关。

如何安全地轮换我的 **AWS** 凭证？

如上文所述，控制台允许您通过几种方式提供 AWS 凭证：与控制台代理关联的 IAM 角色、在受信任的账户中承担 IAM 角色或提供 AWS 访问密钥。

对于前两个选项，控制台使用 AWS 安全令牌服务来获取不断轮换的临时凭证。这个流程是最佳实践——它既自动化又安全。

如果您向控制台提供 AWS 访问密钥，则应通过定期在控制台中更新密钥来轮换密钥。这是一个完全手动的过程。

我可以更改 **Cloud Volumes ONTAP** 系统的 **AWS Marketplace** 订阅吗？

是的，你可以。当您更改与一组凭证关联的 AWS Marketplace 订阅时，所有现有和新的 Cloud Volumes ONTAP 系统都将根据新订阅收费。

["了解如何关联 AWS 订阅"](#)。

我可以添加多个 **AWS** 凭证，每个凭证都有不同的市场订阅吗？

属于同一 AWS 账户的所有 AWS 凭证都将与同一个 AWS Marketplace 订阅相关联。

如果您有属于不同 AWS 账户的多个 AWS 凭证，则这些凭证可以与同一个 AWS Marketplace 订阅或不同的订阅相关联。

我可以将现有的 **Cloud Volumes ONTAP** 系统移动到不同的 **AWS** 账户吗？

不可以，无法将与您的 Cloud Volumes ONTAP 系统关联的 AWS 资源移动到其他 AWS 账户。

凭证如何用于市场部署和本地部署？

以上部分描述了控制台代理的推荐部署方法，即从控制台部署。您还可以从 AWS Marketplace 在 AWS 中部署代理，也可以在您自己的 Linux 主机或 VCenter 中手动安装控制台代理软件。

如果您使用市场，则权限以相同的方式提供。您只需手动创建和设置 IAM 角色，然后为任何其他帐户提供权限。

对于本地部署，您无法为控制台设置 IAM 角色，但可以使用 AWS 访问密钥提供权限。

要了解如何设置权限，请参阅以下页面：

- 标准模式
 - ["设置 AWS Marketplace 部署的权限"](#)
 - ["设置本地部署的权限"](#)
- 限制模式
 - ["设置限制模式的权限"](#)

管理NetApp Console的 AWS 凭证和市场订阅

添加和管理 AWS 凭证，以便您从NetApp Console部署和管理 AWS 帐户中的云资源。如果您管理多个 AWS Marketplace 订阅，则可以从“凭证”页面将每个订阅分配给不同的 AWS 凭证。

概述

您可以将 AWS 凭证添加到现有的控制台代理或直接添加到控制台：

- 向现有代理添加额外的 AWS 凭证

将 AWS 凭证添加到控制台代理以管理云资源。[了解如何将 AWS 凭证添加到控制台代理](#)。

- 将 AWS 凭证添加到控制台以创建控制台代理

向控制台添加新的 AWS 凭证可提供创建控制台代理所需的权限。[了解如何将 AWS 凭证添加到NetApp Console](#)。

- 将 AWS 凭证添加到 FSx for ONTAP控制台

将新的 AWS 凭证添加到控制台以创建和管理 FSx for ONTAP。["了解如何设置 FSx for ONTAP 的权限"](#)

如何轮换凭证

NetApp Console允许您通过几种方式提供 AWS 凭证：与代理实例关联的 IAM 角色、在受信任的帐户中承担 IAM 角色或提供 AWS 访问密钥。["了解有关 AWS 凭证和权限的更多信息"](#)。

对于前两个选项，控制台使用 AWS 安全令牌服务来获取不断轮换的临时凭证。这个过程是最佳实践，因为它是自动的并且是安全的。

通过在控制台中更新来手动轮换 AWS 访问密钥。

向控制台代理添加附加凭据

向控制台代理添加额外的 AWS 凭证，以便它具有管理公共云环境中的资源和流程所需的权限。您可以提供另一个帐户中的 IAM 角色的 ARN，也可以提供 AWS 访问密钥。

["了解NetApp Console如何使用 AWS 凭证和权限"](#)。

授予权限

在将 AWS 凭证添加到控制台代理之前授予权限。这些权限允许控制台代理管理该 AWS 账户内的资源和流程。您可以使用受信任账户或 AWS 密钥中角色的 ARN 来提供权限。



如果您从控制台部署了控制台代理，它会自动为您部署控制台代理的账户添加 AWS 凭证。这确保了管理资源所需的必要权限。

选择

- [通过承担另一个账户中的 IAM 角色来授予权限](#)
- [通过提供 AWS 密钥授予权限](#)

通过承担另一个账户中的 IAM 角色来授予权限

您可以使用 IAM 角色在部署控制台代理的源 AWS 账户与其他 AWS 账户之间建立信任关系。然后，您将向控制台提供来自受信任账户的 IAM 角色的 ARN。

如果控制台代理安装在本地，则无法使用此身份验证方法。您必须使用 AWS 密钥。

步骤

1. 转到您想要为控制台代理提供权限的目标账户中的 IAM 控制台。
2. 在访问管理下，选择*角色>创建角色*并按照步骤创建角色。

请务必执行以下操作：

- 在 受信任实体类型 下，选择 **AWS 账户**。
- 选择“其他 AWS 账户”，并输入控制台代理实例所在账户的 ID。
- 通过复制并粘贴以下内容来创建所需的策略["控制台代理的 IAM 策略"](#)。

3. 复制 IAM 角色的角色 ARN，以便稍后将其粘贴到控制台中。

结果

该帐户具有所需的权限。[您现在可以将凭证添加到控制台代理](#)。

通过提供 AWS 密钥授予权限

如果您想为 IAM 用户提供带有 AWS 密钥的控制台，则需要向该用户授予所需的权限。控制台 IAM 策略定义了控制台允许使用的 AWS 操作和资源。

如果本地安装了控制台代理，则必须使用此身份验证方法。您不能使用 IAM 角色。

步骤

1. 从 IAM 控制台，通过复制并粘贴以下内容来创建策略["控制台代理的 IAM 策略"](#)。

["AWS 文档：创建 IAM 策略"](#)

2. 将策略附加到 IAM 角色或 IAM 用户。

- ["AWS 文档：创建 IAM 角色"](#)

- ["AWS 文档：添加和删除 IAM 策略"](#)

将凭证添加到现有代理

为 AWS 账户提供所需权限后，您可以将该账户的凭证添加到现有代理。这使您可以使用相同的代理在该帐户中启动Cloud Volumes ONTAP系统。



您的云提供商中的新凭证可能需要几分钟才能生效。

步骤

1. 使用顶部导航栏选择要添加凭据的控制台代理。
2. 在左侧导航栏中，选择“管理”>“凭据”。
3. 在*组织凭据*页面上，选择*添加凭据*并按照向导中的步骤进行操作。
 - a. 凭证位置：选择*Amazon Web Services > 代理*。
 - b. 定义凭证：提供受信任的 IAM 角色的 ARN（Amazon 资源名称），或输入 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。

要按小时费率（PAYGO）或年度合同支付服务费用，您必须将 AWS 凭证与您的 AWS Marketplace 订阅关联起来。

- d. 审核：确认有关新凭证的详细信息并选择*添加*。

结果

现在，您可以在向控制台添加订阅时从“详细信息和凭据”页面切换到不同的凭据集。

Edit Credentials & Add Subscription

Associate Subscription to Credentials ⓘ

Credentials

keys | Account ID: [redacted]

Instance Profile | Account ID: [redacted]

casaba QA subscription

+ Add Subscription

Apply

Cancel

将凭据添加到控制台以创建控制台代理

通过提供 IAM 角色的 ARN 来添加 AWS 凭证，该角色授予创建控制台代理所需的权限。您可以在创建新代理时选择这些凭据。

设置 IAM 角色

设置一个 IAM 角色，使 NetApp Console 软件即服务 (SaaS) 层能够承担该角色。

步骤

1. 转到目标账户中的 IAM 控制台。
2. 在访问管理下，选择*角色>创建角色*并按照步骤创建角色。

请务必执行以下操作：

- 在 受信任实体类型 下，选择 **AWS** 账户。
- 选择“另一个 AWS 账户”并输入 NetApp Console SaaS 的 ID：952013314444
- 具体来说，对于 Amazon FSx for NetApp ONTAP，编辑 信任关系 策略以包含“AWS”：
“arn:aws:iam::952013314444:root”。

例如，该策略应如下所示：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::952013314444:root",
        "Service": "ec2.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

+

参考[“AWS 身份和访问管理 \(IAM\) 文档”](#)有关 IAM 中跨账户资源访问的更多信息。

- 创建一个包含创建控制台代理所需权限的策略。
 - [“查看 FSx for ONTAP 所需的权限”](#)
 - [“查看代理部署策略”](#)

3. 复制 IAM 角色的角色 ARN，以便您可以在下一步中将其粘贴到控制台中。

结果

IAM 角色现在具有所需的权限。 [您现在可以将其添加到控制台。](#)

添加凭据

为 IAM 角色提供所需的权限后，将角色 ARN 添加到控制台。

开始之前

如果您刚刚创建了 IAM 角色，则可能需要几分钟才能使用它们。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. 在*组织凭据*页面上，选择*添加凭据*并按照向导中的步骤进行操作。
 - a. 凭证位置：选择*Amazon Web Services > 控制台*。
 - b. 定义凭证：提供 IAM 角色的 ARN（Amazon 资源名称）。
 - c. 审核：确认有关新凭证的详细信息并选择*添加*。

向**Amazon FSx for ONTAP**控制台添加凭证

有关详细信息，请参阅 ["Amazon FSx for ONTAP 的控制台文档"](#)

配置 AWS 订阅

添加 AWS 凭证后，您可以使用这些凭证配置 AWS Marketplace 订阅。通过订阅，您可以按小时费率（PAYGO）或使用年度合同支付 NetApp 数据服务和 Cloud Volumes ONTAP 的费用。

在添加凭证后，您可以在两种情况下配置 AWS Marketplace 订阅：

- 最初添加凭据时您没有配置订阅。
- 您想要更改配置为 AWS 凭证的 AWS Marketplace 订阅。

用新的订阅替换当前的市场订阅会更改任何现有 Cloud Volumes ONTAP 系统和所有新系统的市场订阅。

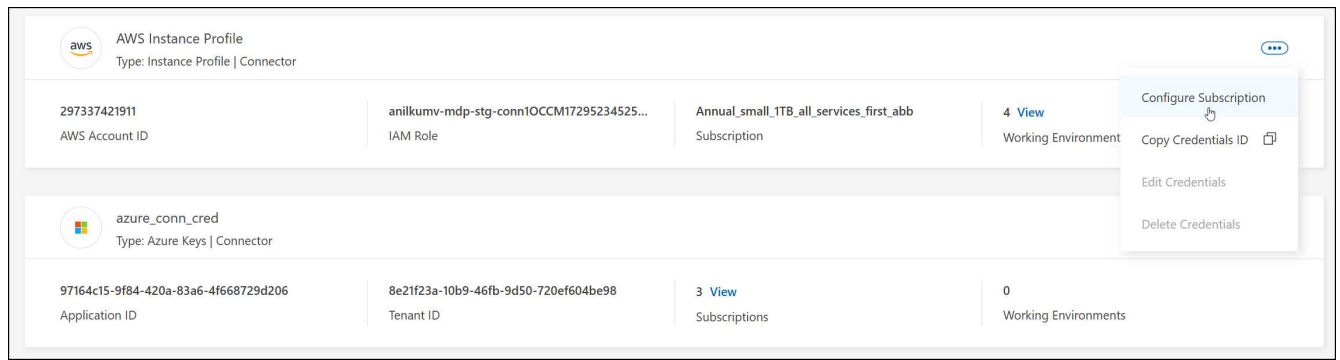
开始之前

您需要先创建控制台代理，然后才能配置订阅。["了解如何创建控制台代理"](#)。

步骤

1. 选择“管理 > 凭证”。
2. 选择*组织凭证*。
3. 选择与控制台代理关联的一组凭据的操作菜单，然后选择*配置订阅*。

您必须选择与控制台代理关联的凭据。您无法将市场订阅与与 NetApp Console 关联的凭据关联。



4. 要将凭据与现有订阅关联，请从下拉列表中选择订阅并选择*配置*。
5. 要将凭证与新订阅关联，请选择“添加订阅”>“继续”，然后按照 AWS Marketplace 中的步骤操作：
 - a. 选择“查看购买选项”。
 - b. 选择*订阅*。
 - c. 选择*设置您的帐户*。

您将被重定向到 NetApp Console。

- d. 从“订阅分配”页面：
 - 选择您想要与此订阅关联的控制台组织或帐户。
 - 在“替换现有订阅”字段中，选择是否要用这个新订阅自动替换一个组织或帐户的现有订阅。

控制台将用这个新订阅替换组织或帐户中所有凭据的现有订阅。如果一组凭证从未与订阅关联，那么这个新订阅将不会与这些凭证关联。

对于所有其他组织或帐户，您需要重复这些步骤来手动关联订阅。

- 选择*保存*。

将现有订阅与您的组织关联

当您从 AWS Marketplace 订阅时，流程的最后一步是将订阅与您的组织关联。如果您没有完成此步骤，那么您就无法在您的组织中使用该订阅。

- ["了解控制台部署模式"](#)
- ["了解控制台身份和访问管理"](#)

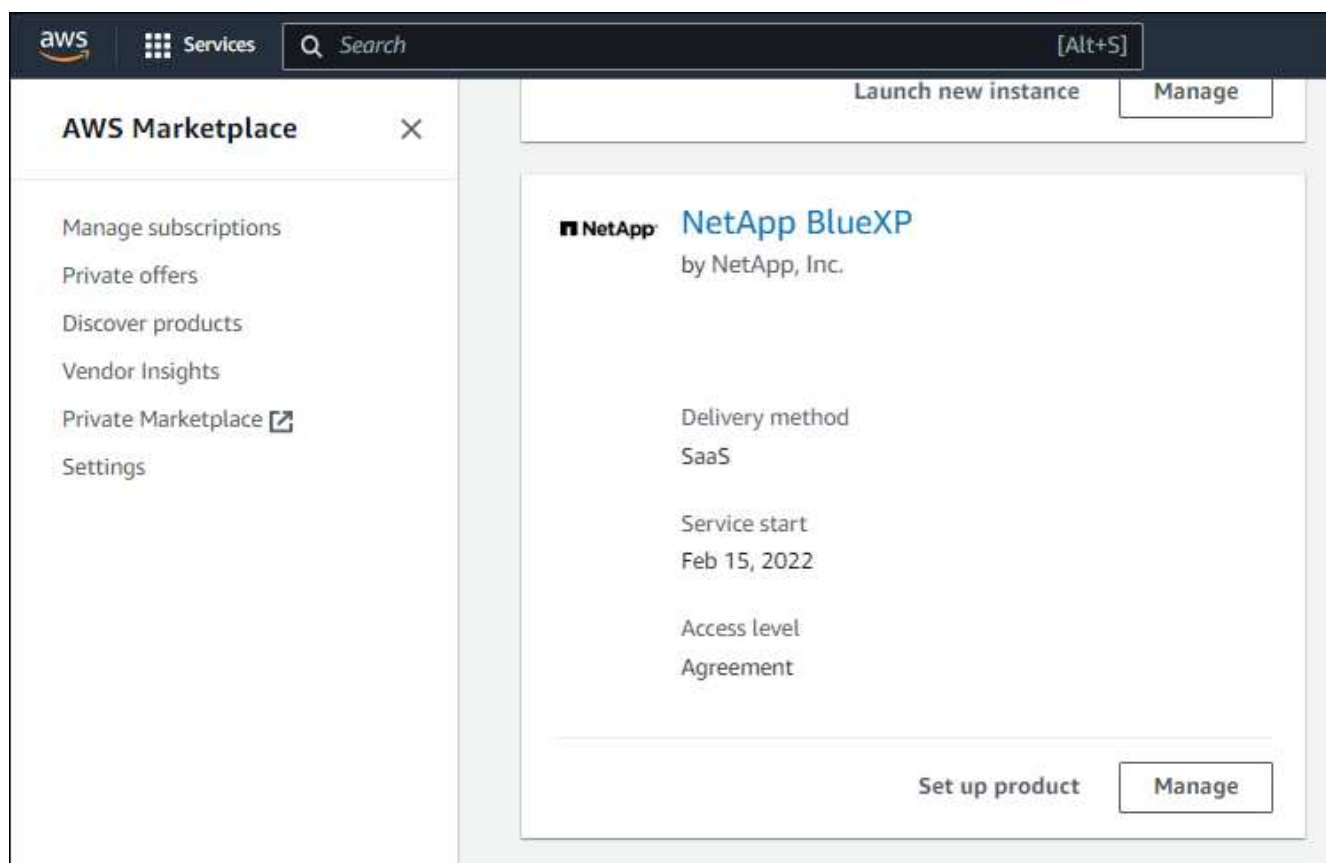
如果您从 AWS Marketplace 订阅了 NetApp Intelligent Services，但错过了将订阅与您的帐户关联的步骤，请按照以下步骤操作。

步骤

1. 确认您没有将您的订阅与您的控制台组织关联。
 - a. 从导航菜单中，选择*管理>Licenses and subscriptions*。
 - b. 选择*订阅*。
 - c. 确认您的订阅没有出现。

您只会看到与您当前正在查看的组织或帐户相关的订阅。如果您没有看到您的订阅，请继续执行以下步骤。

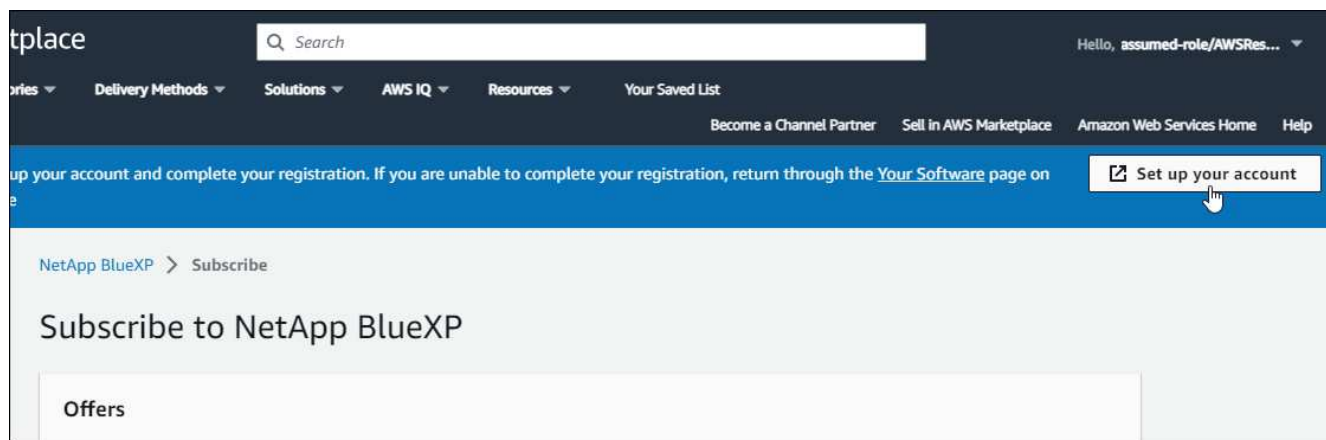
2. 登录 AWS 控制台并导航到 **AWS Marketplace** 订阅。
3. 查找订阅。



4. 选择*设置产品*。

订阅优惠页面应在新的浏览器选项卡或窗口中加载。

5. 选择*设置您的帐户*。



netapp.com 上的 **Subscription Assignment** 页面应在新浏览器选项卡或窗口中加载。

请注意，系统可能会提示您先登录控制台。

6. 从“订阅分配”页面：

- 选择您想要与此订阅关联的控制台组织或帐户。
- 在“替换现有订阅”字段中，选择是否要用这个新订阅自动替换一个组织或帐户的现有订阅。

控制台将用这个新订阅替换组织或帐户中所有凭据的现有订阅。如果一组凭证从未与订阅关联，那么这个新订阅将不会与这些凭证关联。

对于所有其他组织或帐户，您需要重复这些步骤来手动关联订阅。

Subscription Assignment [X]

✓ Your subscription to BlueXP / Cloud Volumes ONTAP from the AWS Marketplace was created successfully.

Subscription name i

PayAsYouGo

Select the NetApp accounts that you'd like to associate this subscription with. i

You can automatically replace the existing subscription for one account with this new subscription.

NetApp account	Replace existing subscription
☒ cloudTiering_undefined	☐
☒ CS-HhewH	☐
☒ benAccount	☒

Save

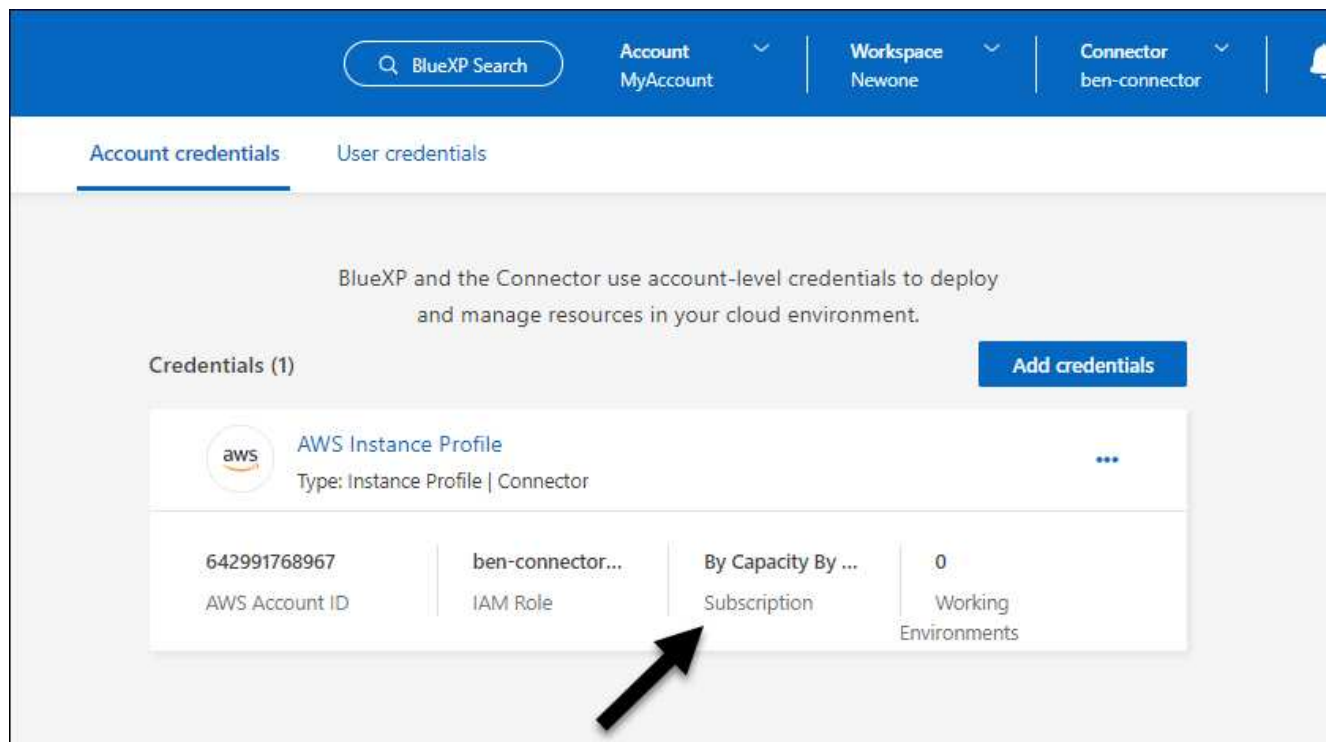
7. 确认订阅与您的组织相关联。

- 从导航菜单中，选择*管理>许可证和订阅*。
- 选择*订阅*。
- 验证您的订阅是否出现。

8. 确认订阅与您的 AWS 凭证相关联。

- 选择“管理 > 凭证”。
- 在“组织凭证”页面上，验证订阅是否与您的 AWS 凭证关联。

这是一个例子。



编辑凭证

通过更改帐户类型（AWS 密钥或承担角色）、编辑名称或更新凭证本身（密钥或角色 ARN）来编辑您的 AWS 凭证。



您无法编辑与控制台代理实例或Amazon FSx for ONTAP实例关联的实例配置文件的凭证。您只能重命名 FSx for ONTAP实例的凭证。

步骤

- 选择“管理 > 凭证”。
- 在“组织凭证”页面上，选择一组凭证的操作菜单，然后选择“编辑凭证”。
- 进行所需的更改，然后选择“应用”。

删除凭证

如果您不再需要一组凭证，您可以删除它们。您只能删除与系统无关的凭证。



您无法删除与控制台代理关联的实例配置文件的凭证。

步骤

1. 选择“管理 > 凭证”。
2. 在*组织凭据*或*帐户凭据*页面上，选择一组凭据的操作菜单，然后选择*删除凭据*。
3. 选择*删除*进行确认。

Azure

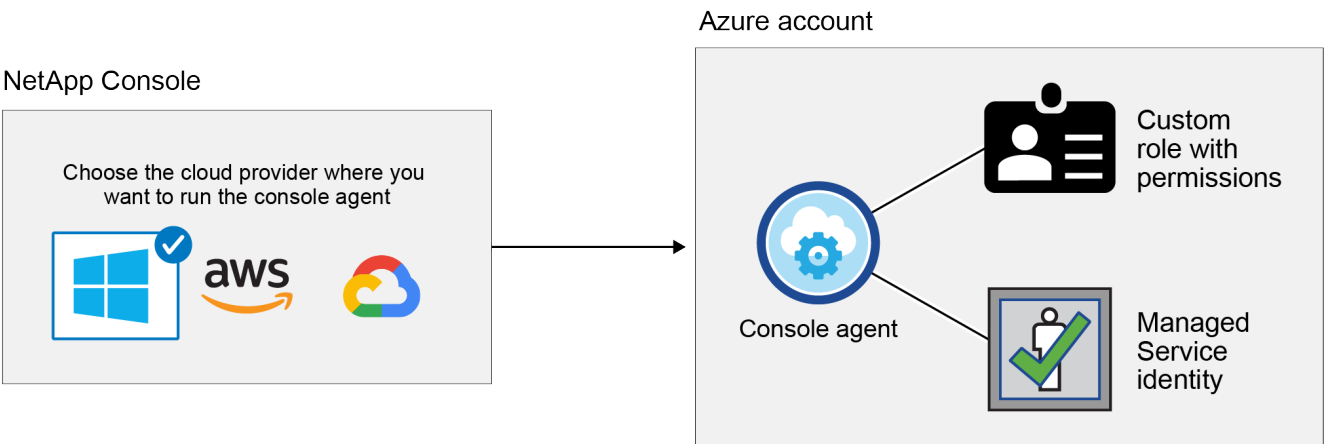
了解NetApp Console中的 Azure 凭据和权限

了解NetApp Console如何使用 Azure 凭据代表您执行操作以及这些凭据如何与市场订阅相关联。了解这些详细信息有助于您管理一个或多个 Azure 订阅的凭据。例如，您可能想了解何时向控制台添加其他 Azure 凭据。

初始 Azure 凭据

从控制台部署控制台代理时，您需要使用具有部署控制台代理虚拟机权限的 Azure 帐户或服务主体。所需权限列于“[Azure 的代理部署策略](#)”。

当控制台在 Azure 中部署控制台代理虚拟机时，它会启用 [“系统分配的托管标识”](#)在虚拟机上，创建自定义角色，并将其分配给虚拟机。该角色为控制台提供管理该 Azure 订阅内的资源和流程所需的权限。[“查看控制台如何使用权限”](#)。



如果您为Cloud Volumes ONTAP创建新系统，控制台将默认选择以下 Azure 凭据：

Details & Credentials			
Managed Service Ide...	OCCM QA1	No subscription is associated	Edit Credentials
Credential Name	Azure Subscription	Marketplace Subscription	

您可以使用初始 Azure 凭据部署所有Cloud Volumes ONTAP系统，也可以添加其他凭据。

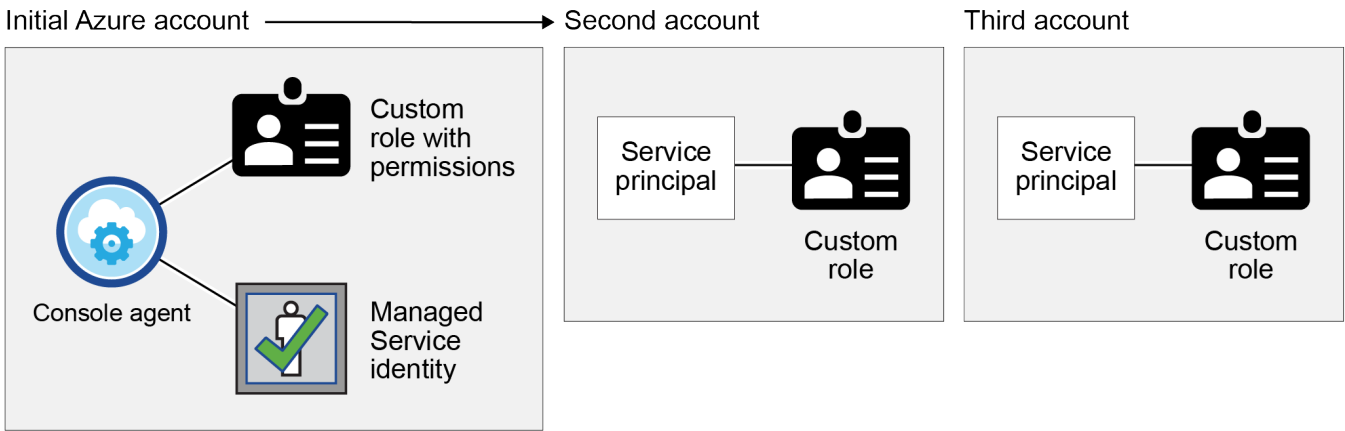
托管标识的其他 Azure 订阅

分配给控制台代理 VM 的系统分配托管标识与您启动控制台代理的订阅相关联。如果您想选择不同的 Azure 订

阅，则需要["将托管标识与这些订阅关联"](#)。

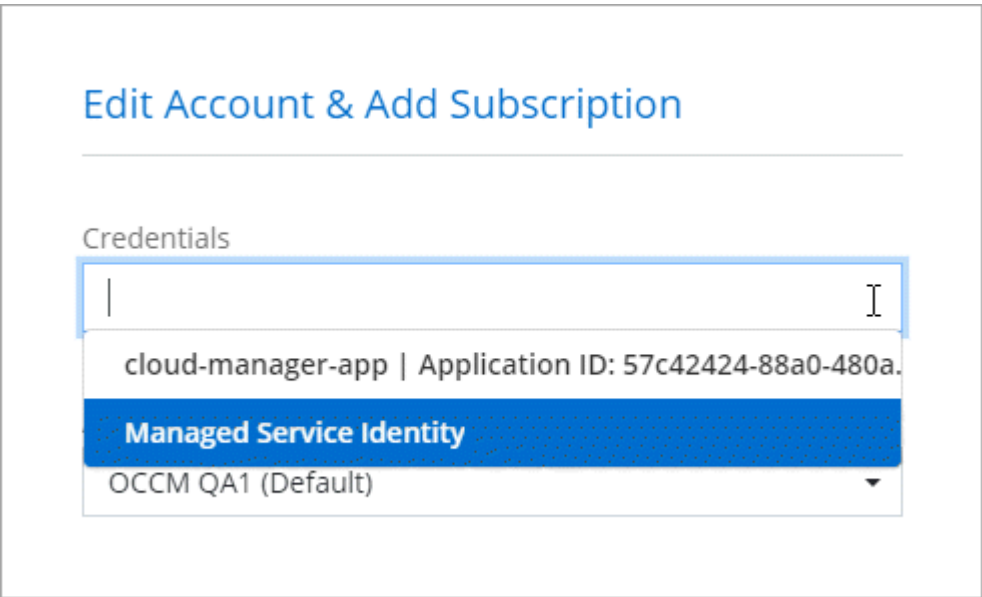
其他 Azure 凭据

如果要在控制台中使用不同的 Azure 凭据，则必须通过以下方式授予所需的权限["在 Microsoft Entra ID 中创建和设置服务主体"](#)对于每个 Azure 帐户。下图显示了另外两个帐户，每个帐户都设置了服务主体和提供权限的自定义角色：



那么你会["将帐户凭据添加到控制台"](#)通过提供有关 AD 服务主体的详细信息。

例如，您可以在创建新的Cloud Volumes ONTAP系统时在凭据之间切换：



凭证和市场订阅

您添加到控制台代理的凭据必须与 Azure Marketplace 订阅相关联，以便您可以按小时费率（PAYGO）或NetApp数据服务或通过年度合同支付Cloud Volumes ONTAP费用。

["了解如何关联 Azure 订阅"](#)。

请注意有关 Azure 凭据和市场订阅的以下事项：

- 只能将一个 Azure 市场订阅与一组 Azure 凭据关联
- 您可以使用新的订阅替换现有的市场订阅

常见问题解答

以下问题与凭证和订阅有关。

我可以更改**Cloud Volumes ONTAP**系统的 **Azure Marketplace** 订阅吗？

是的，你可以。当您更改与一组 Azure 凭据关联的 Azure 市场订阅时，所有现有和新的**Cloud Volumes ONTAP**系统都将根据新订阅收费。

["了解如何关联 Azure 订阅"](#)。

我可以添加多个 **Azure** 凭据，每个凭据都有不同的市场订阅吗？

属于同一 Azure 订阅的所有 Azure 凭据都将与同一 Azure 市场订阅相关联。

如果您有属于不同 Azure 订阅的多个 Azure 凭据，则这些凭据可以与同一个 Azure 市场订阅或不同的市场订阅相关联。

我可以将现有的**Cloud Volumes ONTAP**系统移动到不同的 **Azure** 订阅吗？

不可以，无法将与您的**Cloud Volumes ONTAP**系统关联的 Azure 资源移动到其他 Azure 订阅。

凭证如何用于市场部署和本地部署？

以上部分描述了控制台代理的推荐部署方法，即从控制台部署。您还可以从 Azure 市场在 Azure 中部署控制台代理，并且可以在自己的 Linux 主机上安装控制台代理软件。

如果您使用 Marketplace，您可以通过向控制台代理 VM 和系统分配的托管身份分配自定义角色来提供权限，或者您可以使用 Microsoft Entra 服务主体。

对于本地部署，您无法为控制台代理设置托管标识，但可以使用服务主体提供权限。

要了解如何设置权限，请参阅以下页面：

- 标准模式
 - ["设置 Azure 市场部署的权限"](#)
 - ["设置本地部署的权限"](#)
- 限制模式
 - ["设置限制模式的权限"](#)

管理**NetApp Console**的 **Azure** 凭据和市场订阅

添加和管理 Azure 凭据，以便**NetApp Console**具有在 Azure 订阅中部署和管理云资源所需的权限。如果您管理多个 Azure 市场订阅，则可以从“凭据”页面将每个订阅分配给不同的 Azure 凭据。

概述

有两种方法可以在控制台中添加额外的 Azure 订阅和凭据。

1. 将其他 Azure 订阅与 Azure 托管标识关联。
2. 要使用不同的 Azure 凭据部署 Cloud Volumes ONTAP，请使用服务主体授予 Azure 权限并将其凭据添加到控制台。

将其他 Azure 订阅与托管标识关联 Associate additional Azure subscriptions with a managed identity

控制台使您能够选择要部署 Cloud Volumes ONTAP 的 Azure 凭据和 Azure 订阅。除非关联 ["托管标识"](#) 通过这些订阅。

关于此任务

托管身份 ["初始 Azure 帐户"](#) 当您从控制台部署控制台代理时。部署控制台代理时，控制台会将控制台操作员角色分配给控制台代理虚拟机。

步骤

1. 登录 Azure 门户。
2. 打开 ["订阅"](#) 服务，然后选择要部署 Cloud Volumes ONTAP 的订阅。
3. 选择 ["访问控制 \(IAM\)"](#)。
 - a. 选择 [添加 > 添加角色分配](#)，然后添加权限：

- 选择 ["控制台操作员"](#) 角色。



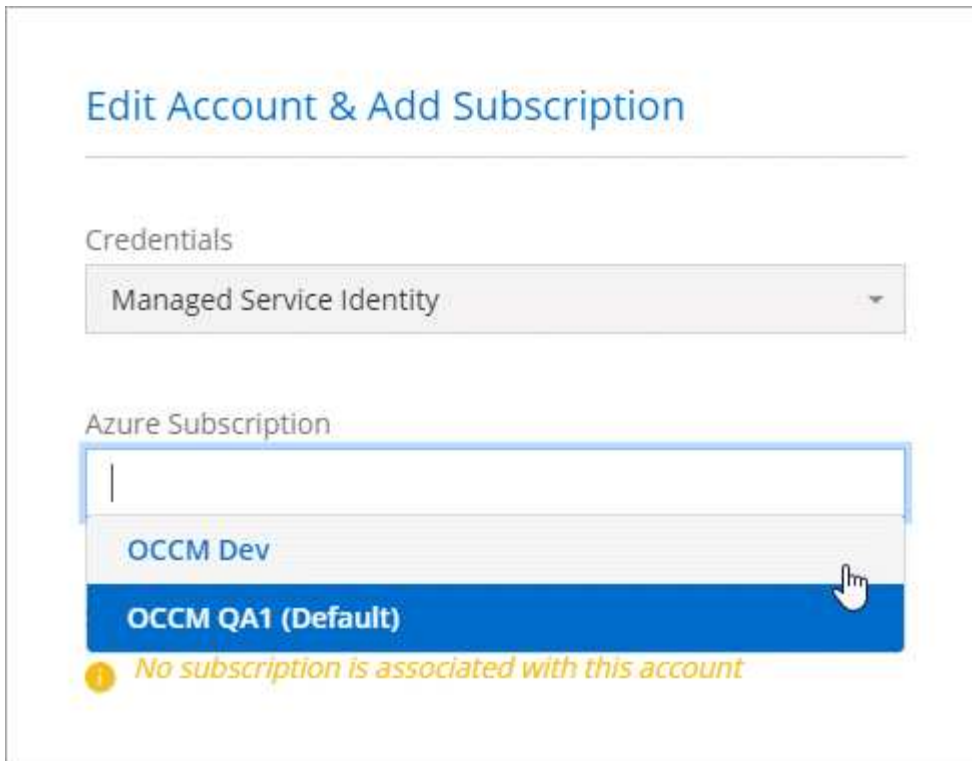
控制台操作员是控制台代理策略中提供的默认名称。如果您为角色选择了不同的名称，则选择该名称。

- 分配对 ["虚拟机"](#) 的访问权限。
- 选择创建控制台代理虚拟机的订阅。
- 选择一个控制台代理虚拟机。
- 选择 ["保存"](#)。

4. 重复这些步骤以获得更多订阅。

结果

创建新系统时，您现在可以从多个 Azure 订阅中选择托管标识配置文件。



向NetApp Console添加其他 **Azure** 凭据

从控制台部署控制台代理时，控制台会在具有所需权限的虚拟机上启用系统分配的托管标识。当您为Cloud Volumes ONTAP创建新系统时，控制台会默认选择这些 Azure 凭据。



如果您在现有系统上手动安装了控制台代理软件，则不会添加初始凭据集。[了解 Azure 凭据和权限](#)。

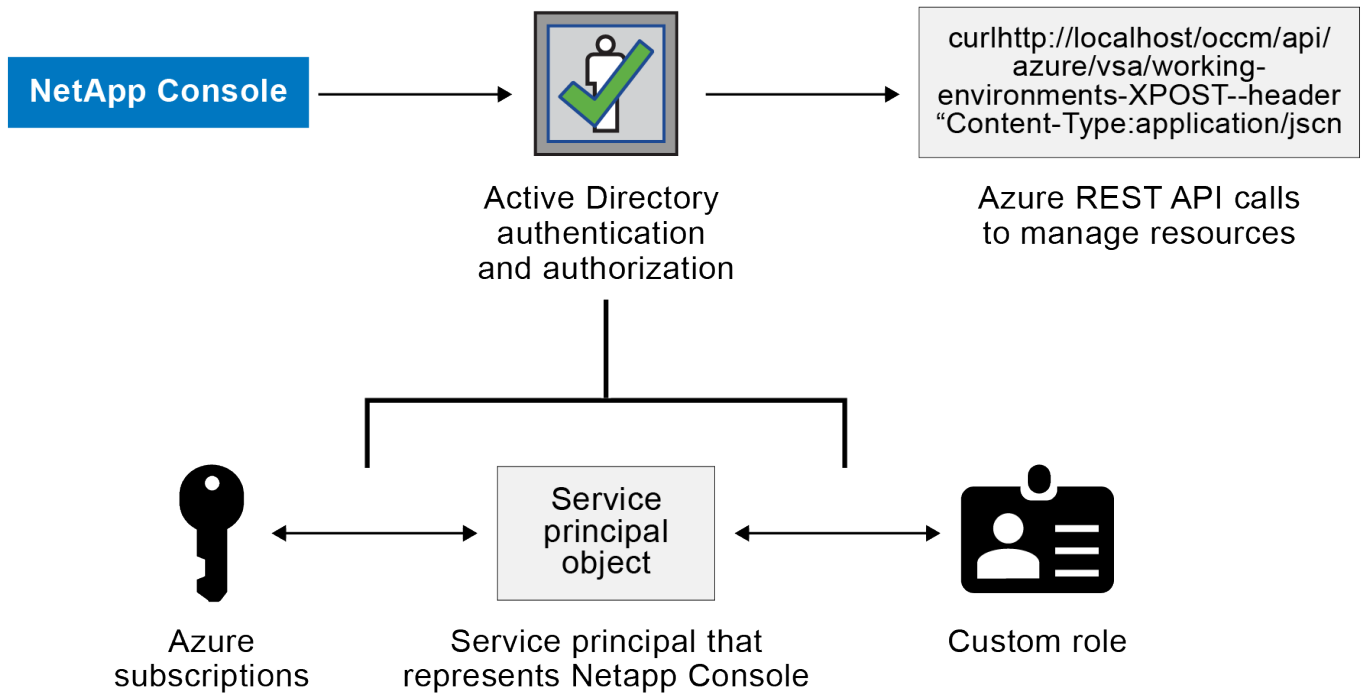
如果您想使用不同的 Azure 凭据部署Cloud Volumes ONTAP，则必须通过在 Microsoft Entra ID 中为每个 Azure 帐户创建和设置服务主体来授予所需的权限。然后，您可以将新凭据添加到控制台。

使用服务主体授予 **Azure** 权限

控制台需要权限才能在 Azure 中执行操作。您可以通过在 Microsoft Entra ID 中创建和设置服务主体并获取控制台所需的 Azure 凭据来向 Azure 帐户授予所需的权限。

关于此任务

下图描述了控制台如何获取在 Azure 中执行操作的权限。服务主体对象与一个或多个 Azure 订阅绑定，代表 Microsoft Entra ID 中的控制台，并分配给允许所需权限的自定义角色。



步骤

1. 创建 [Microsoft Entra 应用程序](#)。
2. [\[将应用程序分配给角色\]](#)。
3. 添加 [Windows Azure 服务管理 API 权限](#)。
4. 获取应用程序ID和目录ID。
5. [\[创建客户端机密\]](#)。

创建 **Microsoft Entra** 应用程序

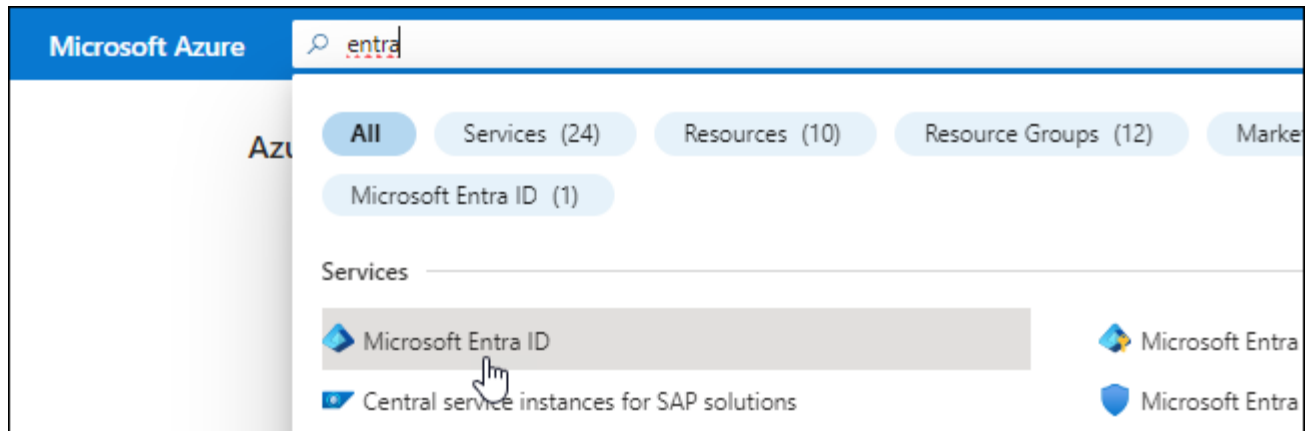
创建控制台可用于基于角色的访问控制的 **Microsoft Entra** 应用程序和服务主体。

步骤

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

您必须将服务主体绑定到一个或多个 Azure 订阅，并为其分配自定义“控制台操作员”角色，以便控制台在 Azure 中拥有权限。

步骤

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。

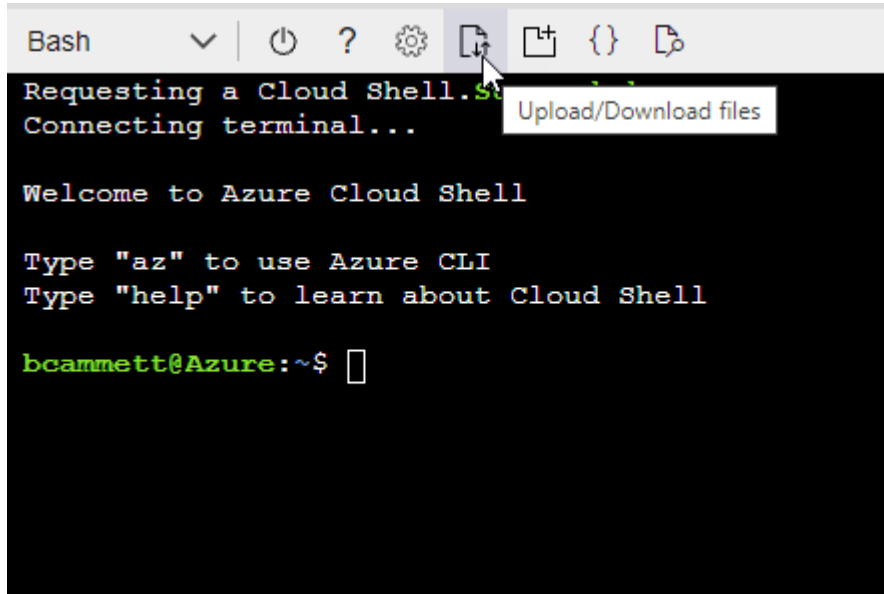
例子

```
"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。



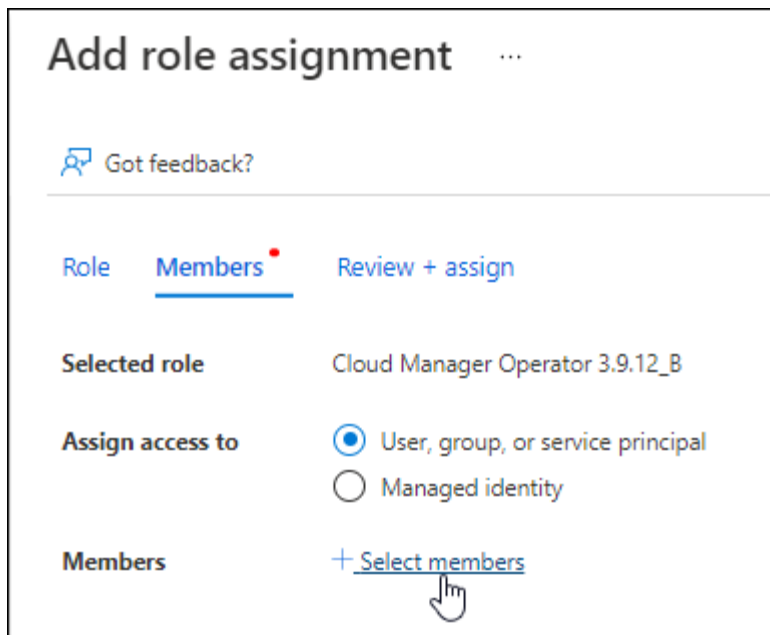
- 使用 Azure CLI 创建自定义角色：

```
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。

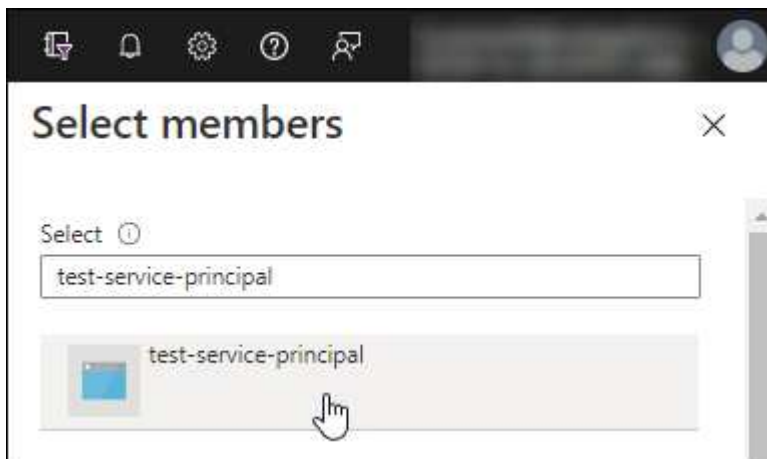
2. 将应用程序分配给角色：

- 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

您必须为服务主体分配“Windows Azure 服务管理 API”权限。

步骤

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”。

Request API permissions

Select an API

Microsoft APIs APIs my organization uses My APIs

Commonly used Microsoft APIs

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

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

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

Request API permissions

[← All APIs](#)



Azure Service Management

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

What type of permissions does your application require?

Delegated permissions

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

Application permissions

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

Select permissions

[expand all](#)

Type to search

PERMISSION

ADMIN CONSENT REQUIRED



user_impersonation

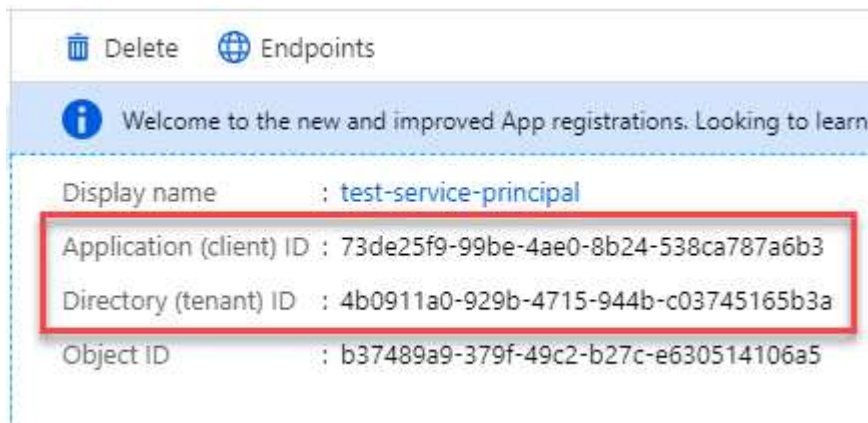
Access Azure Service Management as organization users (preview) ⓘ

获取应用程序ID和目录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。

步骤

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

创建客户端密钥并将其值提供给控制台以使用 Microsoft Entra ID 进行身份验证。

步骤

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。

Client secrets

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

+ New client secret

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

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。

将凭据添加到控制台

为 Azure 帐户提供所需权限后，您可以将该帐户的凭据添加到控制台。完成此步骤后，您可以使用不同的 Azure 凭据启动Cloud Volumes ONTAP 。

开始之前

如果您刚刚在云提供商中创建了这些凭据，则可能需要几分钟才能使用它们。等待几分钟，然后将凭据添加到控制台。

开始之前

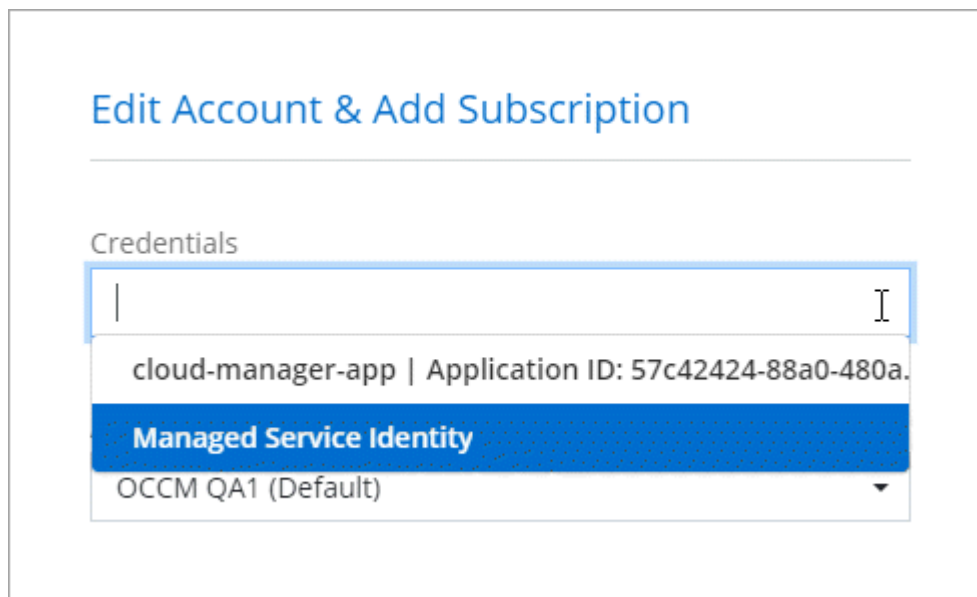
您需要先创建控制台代理，然后才能更改控制台设置。[了解如何创建控制台代理](#)。

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

您可以从“详细信息和凭证”页面切换到另一组凭证 ["将系统添加到控制台时"](#)



管理现有凭证

通过关联 Marketplace 订阅、编辑凭证和删除凭证来管理已添加到控制台的 Azure 凭证。

将 **Azure** 市场订阅关联到凭证

将 Azure 凭证添加到控制台后，您可以将 Azure 市场订阅与这些凭证关联。您可以使用订阅来创建按使用量付费的 Cloud Volumes ONTAP 系统并访问 NetApp 数据服务。

在将凭证添加到控制台后，可以在两种情况下关联 Azure 市场订阅：

- 当您最初将凭证添加到控制台时，您没有关联订阅。
- 您想要更改与 Azure 凭证关联的 Azure 市场订阅。

替换当前的市场订阅会针对现有和新的 Cloud Volumes ONTAP 系统进行更新。

步骤

1. 选择“管理 > 凭证”。
2. 选择*组织凭证*。
3. 选择与控制台代理关联的一组凭证的操作菜单，然后选择*配置订阅*。

您必须选择与控制台代理关联的凭证。您无法将市场订阅与与 NetApp Console 关联的凭证关联。

4. 要将凭证与现有订阅关联，请从下拉列表中选择订阅并选择*配置*。
5. 要将凭证与新订阅关联，请选择“添加订阅”>“继续”，然后按照 Azure 市场中的步骤操作：
 - a. 如果出现提示，请登录您的 Azure 帐户。
 - b. 选择*订阅*。
 - c. 填写表格并选择*订阅*。

- d. 订阅过程完成后，选择*立即配置帐户*。

您将被重定向到NetApp Console。

- e. 从“订阅分配”页面：

- 选择您想要与此订阅关联的控制台组织或帐户。
- 在“替换现有订阅”字段中，选择是否要用这个新订阅自动替换一个组织或帐户的现有订阅。

控制台将用这个新订阅替换组织或帐户中所有凭据的现有订阅。如果一组凭证从未与订阅关联，那么这个新订阅将不会与这些凭证关联。

对于所有其他组织或帐户，您需要重复这些步骤来手动关联订阅。

- 选择*保存*。

编辑凭据

在控制台中编辑您的 Azure 凭据。例如，如果为服务主体应用程序创建了新的密钥，您可以更新客户端密钥。

步骤

1. 选择“管理 > 凭证”。
2. 选择*组织凭证*。
3. 选择一组凭证的操作菜单，然后选择*编辑凭证*。
4. 进行所需的更改，然后选择*应用*。

删除凭据

如果您不再需要一组凭证，您可以删除它们。您只能删除与系统无关的凭据。

步骤

1. 选择“管理 > 凭证”。
2. 选择*组织凭证*。
3. 在*组织凭证*页面上，选择一组凭证的操作菜单，然后选择*删除凭证*。
4. 选择*删除*进行确认。

Google Cloud

了解 Google Cloud 项目和权限

了解NetApp Console如何使用 Google Cloud 凭证代表您执行操作以及这些凭证如何与市场订阅相关联。了解这些详细信息有助于您管理一个或多个 Google Cloud 项目的凭据。例如，您可能想要了解与控制台代理 VM 关联的服务帐户。

NetApp Console的项目和权限

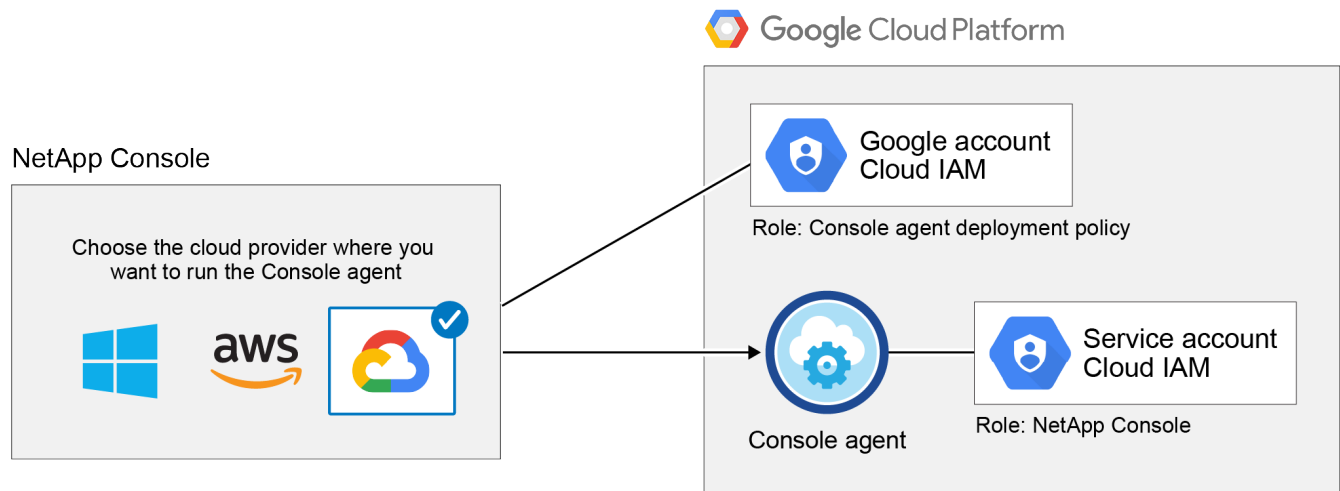
您必须先部署控制台代理，然后才能使用控制台管理 Google Cloud 项目中的资源。代理不能在您的场所或不同

的云提供商中运行。

直接从控制台部署控制台代理之前，必须具备两组权限：

1. 您需要使用具有从控制台启动控制台代理权限的 Google 帐户部署控制台代理。
2. 部署控制台代理时，系统会提示您选择 **"服务帐户"** 对于代理控制台从服务帐户获取权限来创建和管理 Cloud Volumes ONTAP 系统、使用 NetApp 备份和恢复管理备份等等。通过将自定义角色附加到服务帐户来提供权限。

下图描述了上面第 1 项和第 2 项中描述的权限要求：



要了解如何设置权限，请参阅以下页面：

- ["设置标准模式的 Google Cloud 权限"](#)
- ["设置限制模式的权限"](#)

凭证和市场订阅

当您在 Google Cloud 中部署控制台代理时，控制台会为控制台代理所在项目中的 Google Cloud 服务帐号创建一组默认凭据。这些凭证必须与 Google Cloud Marketplace 订阅相关联，以便您可以支付 Cloud Volumes ONTAP 和 NetApp 数据服务的费用。

["了解如何关联 Google Cloud Marketplace 订阅"](#)。

请注意以下有关 Google Cloud 凭据和市场订阅的事项：

- 一个控制台代理只能关联一组 Google Cloud 凭据
- 您只能将一个 Google Cloud Marketplace 订阅与凭据关联
- 您可以使用新的订阅替换现有的市场订阅

Cloud Volumes ONTAP 项目

Cloud Volumes ONTAP 可以与控制台代理位于同一项目中，也可以位于不同的项目中。要在不同的项目中部署 Cloud Volumes ONTAP，您需要首先将控制台代理服务帐户和角色添加到该项目。

- ["了解如何设置服务帐户"](#)
- ["了解如何在 Google Cloud 中部署Cloud Volumes ONTAP并选择项目"](#)

管理 **Google Cloud** 部署的控制台代理权限

NetApp有时会在将控制台代理部署到 Google Cloud 时更新用于该代理的服务帐户所需的权限。

["核实所需的 Google 权限列表"](#)。

使用 Google Cloud 控制台更新分配给服务帐号的 IAM 角色，使其与新的权限集匹配。

["Google Cloud 文档：编辑自定义角色"](#)

版权信息

版权所有 © 2026 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本文档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

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

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

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

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

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

商标信息

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