管理和监测

NetApp Console setup and administration

NetApp
February 11, 2026

目录

管理和监测

NetApp支持帐户

管理与NetApp Console关联的 NSS 凭据

将NetApp支持站点帐户与您的控制台组织关联，以启用存储管理的关键工作流程。这些 NSS 凭证与整个组织相关。

控制台还支持每个用户帐户关联一个 NSS 帐户。"了解如何管理用户级凭证" 。

概述

需要将NetApp支持站点凭据与您的特定控制台帐户序列号关联才能启用以下任务：

- 自带许可证 (BYOL) 时部署Cloud Volumes ONTAP

  需要提供您的 NSS 帐户，以便控制台可以上传您的许可证密钥并启用您购买的期限的订阅。这包括期限续订的自动更新。

- 注册即用即付Cloud Volumes ONTAP系统

  需要提供您的 NSS 帐户才能激活对您的系统的支持并获得对NetApp技术支持资源的访问权限。

- 将Cloud Volumes ONTAP软件升级到最新版本

这些凭证与您的特定控制台帐户序列号相关联。用户可以从*支持 > NSS 管理*访问这些凭据。

添加 **NSS** 帐户

您可以从控制台中的支持信息板添加和管理用于控制台的NetApp支持站点帐户。

当您添加了 NSS 帐户后，控制台会使用此信息进行许可证下载、软件升级验证和未来支持注册等。

您可以将多个 NSS 帐户与您的组织关联；但是，您不能在同一个组织内拥有客户帐户和合作伙伴帐户。

NetApp使用 Microsoft Entra ID 作为特定于支持和许可的身份验证服务的身份提供者。

步骤

1. 在*管理 > 支持*中。
2. 选择*NSS 管理*。
3. 选择*添加 NSS 帐户*。
4. 选择“继续”以重定向到 Microsoft 登录页面。
5. 在登录页面，提供您的NetApp支持站点注册的电子邮件地址和密码。

   成功登录后， NetApp将存储 NSS 用户名。

这是系统生成的映射到您的电子邮件的 ID。在*NSS 管理*页面上，您可以显示来自 ••• 菜单。

- 如果您需要刷新登录凭证令牌，还有一个*更新凭证*选项 ••• 菜单。

  使用此选项会提示您再次登录。请注意，这些帐户的令牌将在 90 天后过期。我们将发布通知来提醒您此事。

下一步是什么？

用户现在可以在创建新的Cloud Volumes ONTAP系统和注册现有Cloud Volumes ONTAP系统时选择帐户。

- "在 AWS 中启动Cloud Volumes ONTAP"
- "在 Azure 中启动Cloud Volumes ONTAP"
- "在 Google Cloud 中启动Cloud Volumes ONTAP"
- "注册现收现付系统"

更新 **NSS** 凭证

出于安全原因，您必须每 90 天更新一次您的 NSS 凭据。如果您的 NSS 凭证已过期，您将在控制台通知中心收到通知。"了解通知中心" 。

过期的凭证可能会影响以下情况，但不限于：

- 许可证更新，这意味着您将无法利用新购买的容量。
- 能够提交和跟踪支持案例。

此外，如果您想更改与您的组织关联的 NSS 帐户，您可以更新与您的组织关联的 NSS 凭据。例如，如果与您的 NSS 帐户关联的人员已离开您的公司。

步骤

1. 在*管理 > 支持*中。
2. 选择*NSS 管理*。
3. 对于要更新的 NSS 帐户，选择 ••• 然后选择*更新凭证*。
4. 当出现提示时，选择“继续”以重定向到 Microsoft 登录页面。

   NetApp使用 Microsoft Entra ID 作为与支持和许可相关的身份验证服务的身份提供者。

5. 在登录页面，提供您的NetApp支持站点注册的电子邮件地址和密码。

将系统附加到不同的 **NSS** 帐户

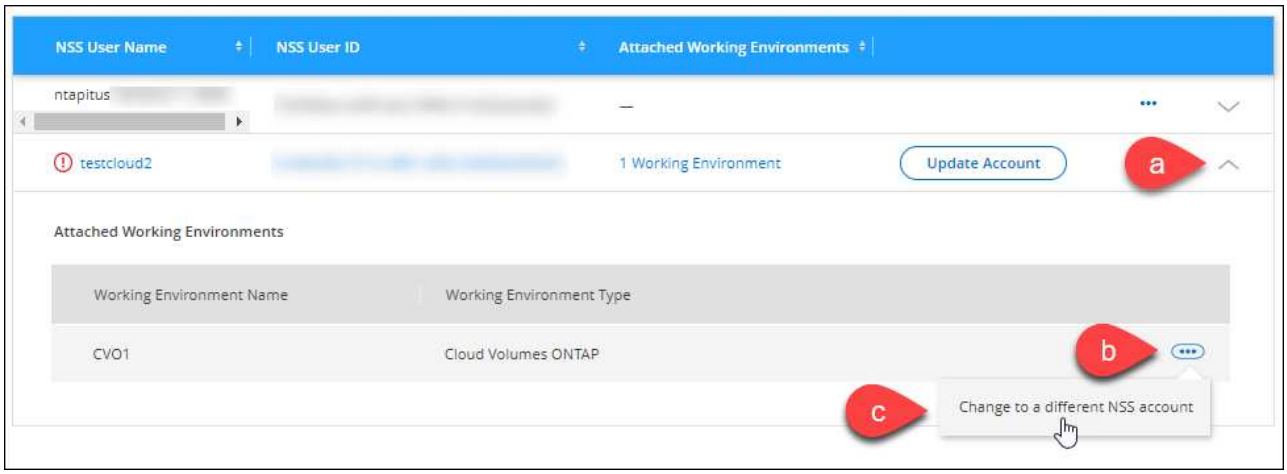
如果您的组织有多个NetApp支持站点帐户，您可以更改与Cloud Volumes ONTAP系统关联的帐户。

您必须首先将帐户与控制台关联。

步骤

1. 在*管理 > 支持*中。
2. 选择*NSS 管理*。

3. 完成以下步骤来更改 NSS 帐户：
   a. 展开系统当前关联的NetApp支持站点帐户的行。
   b. 对于要更改关联的系统，选择 •••
   c. 选择*更改为不同的 NSS 帐户*。



   d. 选择帐户，然后选择*保存*。

显示 **NSS** 帐户的电子邮件地址

为了安全起见，默认情况下不显示与 NSS 帐户关联的电子邮件地址。您可以查看 NSS 帐户的电子邮件地址和关联的用户名。

当您转到 NSS 管理页面时，控制台会为表中的每个帐户生成一个令牌。该令牌包含有关关联电子邮件地址的信息。当您离开页面时，令牌将被删除。信息永远不会被缓存，这有助于保护您的隐私。

步骤

1. 在*管理 > 支持*中。
2. 选择*NSS 管理*。
3. 对于要更新的 NSS 帐户，选择 ••• 然后选择*显示电子邮件地址*。您可以使用复制按钮复制电子邮件地址。

删除 **NSS** 帐户

删除不再想在控制台中使用的所有 NSS 帐户。

您无法删除当前与Cloud Volumes ONTAP系统关联的帐户。你首先需要将这些系统附加到不同的 NSS 帐户。

步骤

1. 在*管理 > 支持*中。
2. 选择*NSS 管理*。
3. 对于要删除的 NSS 帐户，选择 ••• 然后选择*删除*。
4. 选择*删除*进行确认。

管理与您的NetApp Console登录关联的凭据

根据您在控制台中执行的操作，您可能已将ONTAP凭据和NetApp支持站点 (NSS) 凭据与您的用户登录关联。关联这些凭证后，您可以查看和管理它们。例如，如果您更改这些凭据的密码，则需要在控制台中更新密码。

ONTAP凭据

用户需要ONTAP管理员凭据才能在控制台中发现ONTAP集群。但是， ONTAP系统管理器访问取决于您是否使用控制台代理。

无需控制台代理

系统会提示用户输入其ONTAP凭据以访问集群的ONTAP系统管理器。用户可以选择将这些凭据保存在控制台中，这意味着他们不必每次都输入这些凭据。用户凭证仅对相应用户可见，并且可以从用户凭证页面进行管理。

使用控制台代理

默认情况下，不会提示用户输入其ONTAP凭据来访问ONTAP系统管理器。但是，控制台管理员（具有组织管理员角色）可以配置控制台以提示用户输入其ONTAP凭据。启用此设置后，用户每次都需要输入其ONTAP凭据。

"了解更多信息。"

NSS 凭证

与您的NetApp Console登录关联的 NSS 凭据可支持注册、案例管理和访问Digital Advisor。

- 当您访问*支持>资源*并注册支持时，系统会提示您将 NSS 凭据与您的登录名关联。

  这将注册您的组织或帐户以获得支持并激活支持权利。您的组织中只有一个用户必须将NetApp支持站点帐户与其登录名关联，以注册支持并激活支持权利。完成后，“资源”页面将显示您的帐户已注册支持。

  "了解如何注册以获得支持"

- 当您访问*管理 > 支持 > 案例管理*时，如果您还没有输入 NSS 凭证，系统会提示您输入。此页面使您能够创建和管理与您的 NSS 帐户和公司相关的支持案例。
- 当您在控制台中访问Digital Advisor时，系统会提示您输入 NSS 凭据登录Digital Advisor 。

请注意与您的登录名关联的 NSS 帐户的以下事项：

- 该帐户在用户级别进行管理，这意味着其他登录的用户无法查看该帐户。
- 每个用户只能有一个与Digital Advisor和支持案例管理关联的 NSS 帐户。
- 如果您尝试将NetApp支持站点帐户与Cloud Volumes ONTAP系统关联，则只能从添加到您所属组织的 NSS 帐户中进行选择。

  NSS 帐户级凭据与与您的登录关联的 NSS 帐户不同。 NSS 帐户级凭证使您能够使用 BYOL 部署Cloud Volumes ONTAP 、注册 PAYGO 系统并升级其软件。

  "了解有关将 NSS 凭据与您的NetApp Console组织或帐户结合使用的更多信息" 。

管理您的用户凭证

通过更新用户名和密码或删除凭证来管理您的用户凭证。

步骤

1. 选择“管理 > 凭证”。
2. 选择*用户凭证*。
3. 如果您还没有任何用户凭证，您可以选择*添加 NSS 凭证*来添加您的NetApp支持站点帐户。
4. 通过从“操作”菜单中选择以下选项来管理现有凭据：
   - 更新凭据：更新帐户的用户名和密码。
   - 删除凭据：删除与您的控制台登录关联的 NSS 帐户。

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

	可联系经纪人获取信息	无需代理即可购买
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

	可联系经纪人获取信息	无需代理即可购买
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。

端点	目的
\ https://api.bluexp.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com \ https://console.netapp.com \ https://components.console.bluexp.netapp.com \ https://cdn.auth0.com	在NetApp Console中提供功能和服务。
\ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://bluexpinfraprod.azurecr.io	获取控制台代理升级的图像。 • 当您部署新代理时，验证检查会测试与当前端点的连接。如果你使用"先前的端点"，验证检查失败。为了避免此失败，请跳过验证检查。 尽管以前的端点仍然受支持，但NetApp建议尽快将防火墙规则更新到当前端点。"了解如何更新终端节点列表" 。 • 当您更新到防火墙中的当前端点时，您现有的代理将继续工作。

从**NetApp**控制台联系的端点

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

"查看从NetApp控制台联系的端点列表" 。

代理服务器

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

- IP 地址
- 凭据
- HTTPS 证书

端口

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

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

  如果Cloud Volumes ONTAP系统没有出站互联网连接来发送AutoSupport消息，控制台会自动配置这些系

统以使用控制台代理附带的代理服务器。唯一的要求是确保控制台代理的安全组允许通过端口 3128 进行入站连接。部署控制台代理后，您需要打开此端口。

启用 **NTP**

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

创建控制台代理后，您需要实现此网络要求。

步骤 **2**：为控制台代理设置 **AWS** 权限

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

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

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

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

步骤

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

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

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

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

```
        "Condition": {
          "StringLike": {
            "ec2:ResourceTag/OCCMInstance": "*"
          }
        },
        "Resource": [
          "arn:aws:ec2:*:*:instance/*"
        ]
      }
    ]
}
```

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

结果

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

步骤 **3**：创建控制台代理

直接从基于 Web 的控制台创建控制台代理。

关于此任务

- 从控制台创建控制台代理使用默认配置在 AWS 中部署 EC2 实例。创建控制台代理后，请勿切换到具有较少 CPU 或较少 RAM 的较小 EC2 实例。"了解控制台代理的默认配置"。

- 当控制台创建控制台代理时，它会为代理创建一个 IAM 角色和一个配置文件。此角色包括使控制台代理能够管理 AWS 资源的权限。确保在未来版本中添加新权限时更新角色。"了解有关控制台代理的 IAM 策略的更多信息"。

开始之前

您应该具有以下内容：

- AWS 身份验证方法：具有所需权限的 IAM 角色或 IAM 用户的访问密钥。
- 满足组网需求的VPC及子网。
- EC2 实例的密钥对。
- 如果控制台代理需要代理才能访问互联网，则提供有关代理服务器的详细信息。
- 设置"网络要求"。
- 设置"AWS 权限"。

步骤

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

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

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

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

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

   "查看 AWS 的安全组规则" 。

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

如果您仍在使用"先前的端点"用于代理升级，验证失败并出现错误。为了避免这种情况，请取消选中复选框以跳过验证检查。

10. 选择“添加”。

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

结果

该过程完成后，即可从控制台使用控制台代理。

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

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

从 **AWS Marketplace** 创建控制台代理

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

开始之前

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

步骤 **1**：设置网络

确保控制台代理的网络位置满足以下要求以管理混合云资源。

VPC 和子网

创建控制台代理时，您需要指定它所在的 VPC 和子网。

连接到目标网络

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

出站互联网访问

部署控制台代理的网络位置必须具有出站互联网连接才能联系特定端点。

从控制台代理联系的端点

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

下面列出的端点都是 CNAME 条目。

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

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

代理服务器

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

- IP 地址
- 凭据
- HTTPS 证书

端口

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

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

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

启用 **NTP**

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

创建控制台代理后实现此网络访问。

步骤 2：设置 AWS 权限

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

步骤

1. 登录 AWS 控制台并导航到 IAM 服务。
2. 创建策略：
   a. 选择“策略”>“创建策略”。
   b. 选择 **JSON** 并复制并粘贴内容"控制台代理的 IAM 策略"。
   c. 完成剩余步骤以创建策略。

      您可能需要根据计划使用的NetApp数据服务创建第二个策略。对于标准区域，权限分布在两个策略中。由于 AWS 中托管策略的最大字符大小限制，因此需要两个策略。"了解有关控制台代理的 IAM 策略的更多信息" 。
3. 创建 IAM 角色：
   a. 选择*角色 > 创建角色*。
   b. 选择 **AWS** 服务 **> EC2**。
   c. 通过附加刚刚创建的策略来添加权限。
   d. 完成剩余步骤以创建角色。

结果

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

步骤 3：查看实例要求

创建控制台代理时，您需要选择满足以下要求的 EC2 实例类型。

CPU

8 个核心或 8 个 vCPU

RAM

32 GB

AWS EC2 实例类型

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

步骤 4：创建控制台代理

直接从 AWS Marketplace 创建控制台代理。

关于此任务

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

开始之前

您应该具有以下内容：

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

步骤

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

   订阅过程可能需要几分钟。

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

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

7. 按照提示配置并部署实例：

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

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

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

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

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

8. 从连接到控制台代理虚拟机并具有控制台代理 URL 的主机打开 Web 浏览器。
9. 登录后，设置控制台代理：
   a. 指定与控制台代理关联的控制台组织。
   b. 输入系统的名称。
   c. 在*您是否在安全环境中运行？*下保持限制模式处于禁用状态。

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

   d. 选择*让我们开始吧*。

结果

控制台代理现已安装并设置到您的控制台组织。

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

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

在 **AWS** 中手动安装控制台代理

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

开始之前

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

步骤 **1**：查看主机要求

确保运行控制台代理软件的主机满足操作系统、内存和端口要求。

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

专用主机

控制台代理需要专用主机。只要满足以下尺寸要求，任何架构都受支持：

- CPU：8 核或 8 个 vCPU
- 内存：32 GB
- 磁盘空间：建议主机预留165GB空间，分区要求如下：

- `/opt`：必须有 120 GiB 可用空间

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

- `/var`：必须有 40 GiB 可用空间

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

AWS EC2 实例类型

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

虚拟机管理程序

需要经过认证可运行受支持的操作系统的裸机或托管虚拟机管理程序。

操作系统和容器要求

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

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

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

密钥对

创建控制台代理时，您需要选择一个 EC2 密钥对来与实例一起使用。

使用 **IMDSv2** 时的 **PUT** 响应跳数限制

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

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

步骤 2：安装 Podman 或 Docker Engine

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

- Red Hat Enterprise Linux 8 和 9 需要 Podman。

  查看支持的 Podman 版本 。

- Ubuntu 需要 Docker 引擎。

  查看支持的 Docker Engine 版本 。

示例 **1.** 步骤

Podman

按照以下步骤安装和配置 Podman：

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

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

步骤

1. 如果主机上安装了 podman-docker 包，请将其删除。

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

2. 安装 Podman。

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

   a. 对于 Red Hat Enterprise Linux 9.6：

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

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

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

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

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

   c. 对于 Red Hat Enterprise Linux 8：

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

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

3. 启用并启动 podman.socket 服务。

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

4. 安装 python3。

```
sudo dnf install python3
```

5. 如果您的系统上还没有 EPEL 存储库包，请安装它。

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

6. 如果使用 Red Hat Enterprise 9：

   a. 安装EPEL存储库软件包。

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

   +

   a. 安装 podman-compose 包 1.5.0。

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

7. 如果使用的是 Red Hat Enterprise Linux 8：

   a. 安装EPEL存储库软件包。

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

   b. 安装 podman-compose 包 1.0.6。

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

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

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

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

```
podman info | grep networkBackend
```

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

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

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

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

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

v. 重新启动 podman。

```
systemctl restart podman
```

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

```
podman info | grep networkBackend
```

Docker 引擎

按照 Docker 的文档安装 Docker Engine。

步骤

1. "查看 Docker 的安装说明"

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

2. 验证 Docker 是否已启用并正在运行。

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

步骤 **3**：设置网络

请确保网络位置满足以下要求，以便控制台代理能够管理混合云中的资源。

连接到目标网络

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

出站互联网访问

部署控制台代理的网络位置必须具有出站互联网连接才能联系特定端点。

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

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

"为NetApp控制台准备网络" 。

从控制台代理联系的端点

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

下面列出的端点都是 CNAME 条目。

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

端点	目的
\ https://api.bluexp.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com \ https://console.netapp.com \ https://components.console.bluexp.netapp.com \ https://cdn.auth0.com	在NetApp Console中提供功能和服务。
\ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://bluexpinfraprod.azurecr.io	获取控制台代理升级的图像。 • 当您部署新代理时，验证检查会测试与当前端点的连接。如果你使用"先前的端点"，验证检查失败。为了避免此失败，请跳过验证检查。 尽管以前的端点仍然受支持，但NetApp建议尽快将防火墙规则更新到当前端点。"了解如何更新终端节点列表" 。 • 当您更新到防火墙中的当前端点时，您现有的代理将继续工作。

代理服务器

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

- IP 地址
- 凭据
- HTTPS 证书

端口

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

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

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

启用 **NTP**

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

的更多信息"

步骤 **4**：设置控制台的 **AWS** 权限

请使用以下选项之一为NetApp Console提供 AWS 权限：

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

按照步骤准备控制台的权限。

IAM 角色

步骤

1. 登录 AWS 控制台并导航到 IAM 服务。
2. 创建策略：
   a. 选择“策略”>“创建策略”。
   b. 选择 **JSON** 并复制并粘贴内容"控制台代理的 IAM 策略"。
   c. 完成剩余步骤以创建策略。

      根据您计划使用的NetApp数据服务，您可能需要创建第二个策略。对于标准区域，权限分布在两个策略中。由于 AWS 中托管策略的最大字符大小限制，因此需要两个策略。"了解有关控制台代理的 IAM 策略的更多信息" 。
3. 创建 IAM 角色：
   a. 选择*角色 > 创建角色*。
   b. 选择 **AWS** 服务 **> EC2**。
   c. 通过附加刚刚创建的策略来添加权限。
   d. 完成剩余步骤以创建角色。

结果

安装控制台代理后，您现在拥有一个可以与 EC2 实例关联的 IAM 角色。

AWS 访问密钥

步骤

1. 登录 AWS 控制台并导航到 IAM 服务。
2. 创建策略：
   a. 选择“策略”>“创建策略”。
   b. 选择 **JSON** 并复制并粘贴内容"控制台代理的 IAM 策略"。
   c. 完成剩余步骤以创建策略。

      根据您计划使用的NetApp数据服务，您可能需要创建第二个策略。

   对于标准区域，权限分布在两个策略中。由于 AWS 中托管策略的最大字符大小限制，因此需要两个策略。"了解有关控制台代理的 IAM 策略的更多信息" 。
3. 将策略附加到 IAM 用户。
   - "AWS 文档：创建 IAM 角色"
   - "AWS 文档：添加和删除 IAM 策略"
4. 确保用户拥有访问密钥，您可以在安装控制台代理后将其添加到NetApp Console。

结果

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

步骤 **5**：安装控制台代理

完成所有先决条件后，请在您的 Linux 主机上手动安装该软件。

开始之前

您应该具有以下内容：

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

  您可以选择在安装后配置代理服务器，但这样做需要重新启动控制台代理。

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

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

关于此任务

安装后，如果有新版本可用，控制台代理会自动更新。

步骤

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

   ```
   unset http_proxy
   unset https_proxy
   ```

   如果不删除这些系统变量，安装将失败。

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

     选择下载代理安装程序文件或文件的 URL。

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

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

   其中 <version> 是您下载的控制台代理的版本。

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

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

如果您的网络需要代理才能访问互联网，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：

https://ipaddress

2. 登录后，设置控制台代理：

a. 指定与控制台代理关联的组织。

b. 输入系统的名称。

c. 在*您是否在安全环境中运行？*下保持限制模式处于禁用状态。

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

d. 选择*让我们开始吧*。

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

步骤 **6**：提供对**NetApp Console**的权限

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

IAM 角色

将创建的 IAM 角色附加到控制台代理 EC2 实例。

步骤

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

前往 "NetApp Console"开始使用控制台代理。

AWS 访问密钥

向控制台提供具有所需权限的 IAM 用户的 AWS 访问密钥。

步骤

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

前往 "NetApp Console"开始使用控制台代理。

Azure

Azure 中的控制台代理安装选项

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

有以下安装选项可用：

- "直接从NetApp Console创建控制台代理"（这是标准选项）

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

- "从 Azure 市场创建控制台代理"

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

动。

- "在您自己的Linux主机上下载并手动安装软件"

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

从**NetApp Console**在 **Azure** 中创建控制台代理

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

开始之前

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

步骤 **1**：设置网络

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

Azure 区域

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

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

VNet 和子网

创建控制台代理时，您需要指定它所在的 VNet 和子网。

连接到目标网络

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

出站互联网访问

部署控制台代理的网络位置必须具有出站互联网连接才能联系特定端点。

从控制台代理联系的端点

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

下面列出的端点都是 CNAME 条目。

端点	目的
\ https://management.azure.com \ https://login.microsoftonline.com \ https://blob.core.windows.net \ https://core.windows.net	管理 Azure 公共区域中的资源。
\ 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.bluexp.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com \ https://console.netapp.com \ https://components.console.bluexp.netapp.com \ https://cdn.auth0.com	在NetApp Console中提供功能和服务。
\ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://bluexpinfraprod.azurecr.io	获取控制台代理升级的图像。 • 当您部署新代理时，验证检查会测试与当前端点的连接。如果你使用"先前的端点"，验证检查失败。为了避免此失败，请跳过验证检查。 尽管以前的端点仍然受支持，但NetApp建议尽快将防火墙规则更新到当前端点。"了解如何更新终端节点列表" 。 • 当您更新到防火墙中的当前端点时，您现有的代理将继续工作。

从**NetApp**控制台联系的端点

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

"查看从NetApp控制台联系的端点列表" 。

代理服务器

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

- IP 地址
- 凭据
- HTTPS 证书

端口

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

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

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

启用 **NTP**

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

您需要在创建控制台代理后实现此网络要求。

步骤 **2**：创建控制台代理部署策略（自定义角色）

您需要创建一个具有在 Azure 中部署控制台代理的权限的自定义角色。

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

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

请注意，您可以使用 Azure 门户、Azure PowerShell、Azure CLI 或 REST API 创建 Azure 自定义角色。以下步骤展示如何使用 Azure CLI 创建角色。如果您希望使用其他方法，请参阅 "Azure 文档"

步骤

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

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

```
{
  "Name": "Azure SetupAsService",
  "Actions": [
    "Microsoft.Compute/disks/delete",
    "Microsoft.Compute/disks/read",
    "Microsoft.Compute/disks/write",
    "Microsoft.Compute/locations/operations/read",
    "Microsoft.Compute/operations/read",
```

```
    "Microsoft.Compute/virtualMachines/instanceView/read",
    "Microsoft.Compute/virtualMachines/read",
    "Microsoft.Compute/virtualMachines/write",
    "Microsoft.Compute/virtualMachines/delete",
    "Microsoft.Compute/virtualMachines/extensions/write",
    "Microsoft.Compute/virtualMachines/extensions/read",
    "Microsoft.Compute/availabilitySets/read",
    "Microsoft.Network/locations/operationResults/read",
    "Microsoft.Network/locations/operations/read",
    "Microsoft.Network/networkInterfaces/join/action",
    "Microsoft.Network/networkInterfaces/read",
    "Microsoft.Network/networkInterfaces/write",
    "Microsoft.Network/networkInterfaces/delete",
    "Microsoft.Network/networkSecurityGroups/join/action",
    "Microsoft.Network/networkSecurityGroups/read",
    "Microsoft.Network/networkSecurityGroups/write",
    "Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read",
    "Microsoft.Network/virtualNetworks/read",
    "Microsoft.Network/virtualNetworks/subnets/join/action",
    "Microsoft.Network/virtualNetworks/subnets/read",
    "Microsoft.Network/virtualNetworks/subnets/virtualMachines/read",
    "Microsoft.Network/virtualNetworks/virtualMachines/read",
    "Microsoft.Network/publicIPAddresses/write",
    "Microsoft.Network/publicIPAddresses/read",
    "Microsoft.Network/publicIPAddresses/delete",
    "Microsoft.Network/networkSecurityGroups/securityRules/read",
    "Microsoft.Network/networkSecurityGroups/securityRules/write",
    "Microsoft.Network/networkSecurityGroups/securityRules/delete",
    "Microsoft.Network/publicIPAddresses/join/action",

"Microsoft.Network/locations/virtualNetworkAvailableEndpointServices/rea
d",
    "Microsoft.Network/networkInterfaces/ipConfigurations/read",
    "Microsoft.Resources/deployments/operations/read",
    "Microsoft.Resources/deployments/read",
    "Microsoft.Resources/deployments/delete",
    "Microsoft.Resources/deployments/cancel/action",
    "Microsoft.Resources/deployments/validate/action",
    "Microsoft.Resources/resources/read",
    "Microsoft.Resources/subscriptions/operationresults/read",
    "Microsoft.Resources/subscriptions/resourceGroups/delete",
    "Microsoft.Resources/subscriptions/resourceGroups/read",
    "Microsoft.Resources/subscriptions/resourcegroups/resources/read",
    "Microsoft.Resources/subscriptions/resourceGroups/write",
    "Microsoft.Authorization/roleDefinitions/write",
    "Microsoft.Authorization/roleAssignments/write",
```

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

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

2. 通过将 Azure 订阅 ID 添加到可分配范围来修改 JSON。

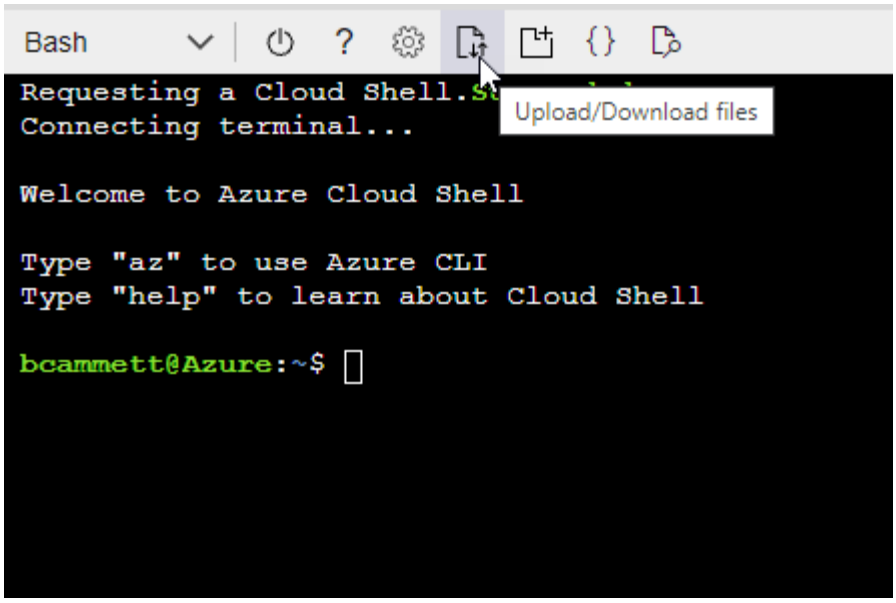
   例子

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

3. 使用 JSON 文件在 Azure 中创建自定义角色。

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

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



c. 输入以下 Azure CLI 命令：

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

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

步骤 **3**：设置身份验证

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

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

按照以下步骤准备其中一种身份验证方法以供控制台使用。

Azure 帐户

将自定义角色分配给将从控制台部署控制台代理的用户。

步骤

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

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

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

服务主体

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

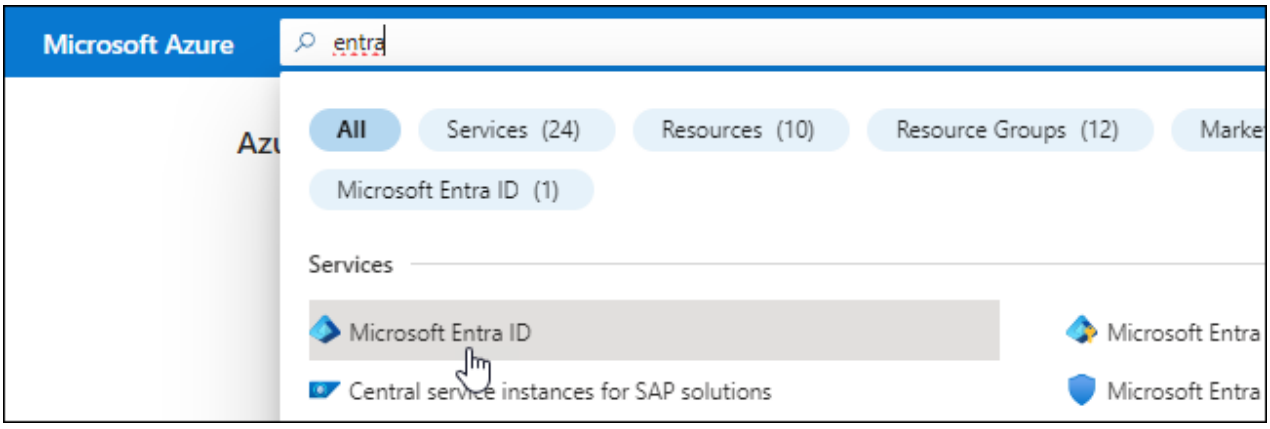
在 Microsoft Entra ID 中创建并设置服务主体，并获取控制台所需的 Azure 凭据。

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

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

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

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



3. 在菜单中，选择*应用程序注册*。
4. 选择*新注册*。
5. 指定有关应用程序的详细信息：

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

6. 选择*注册*。

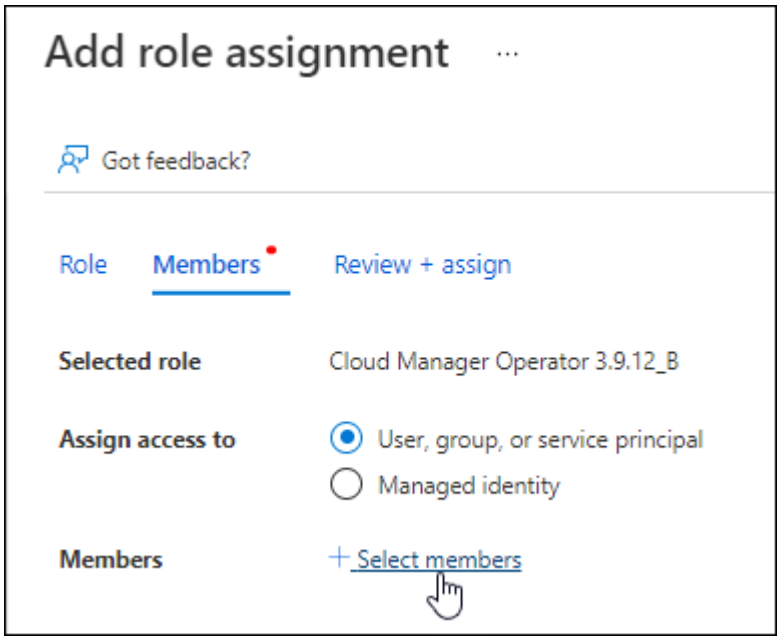
您已创建 AD 应用程序和服务主体。

将自定义角色分配给应用程序

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

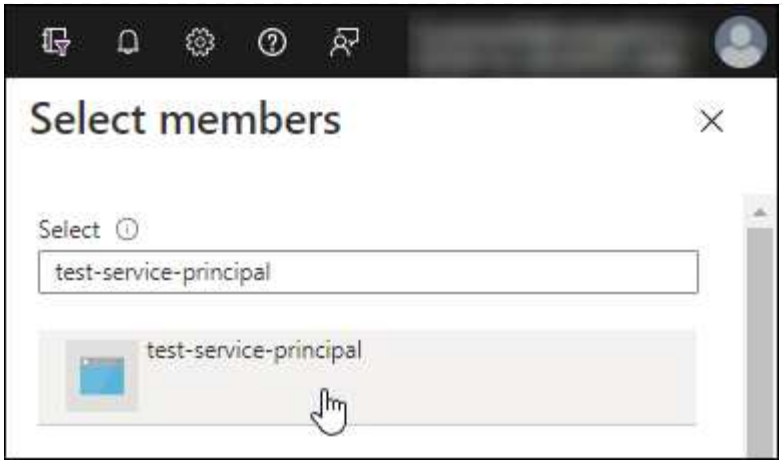
a. 保持选中“用户、组或服务主体”。

b. 单击“选择成员”。



c. 搜索应用程序的名称。

以下是一个例子：



a. 选择应用程序并单击*选择*。

b. 单击“下一步”。

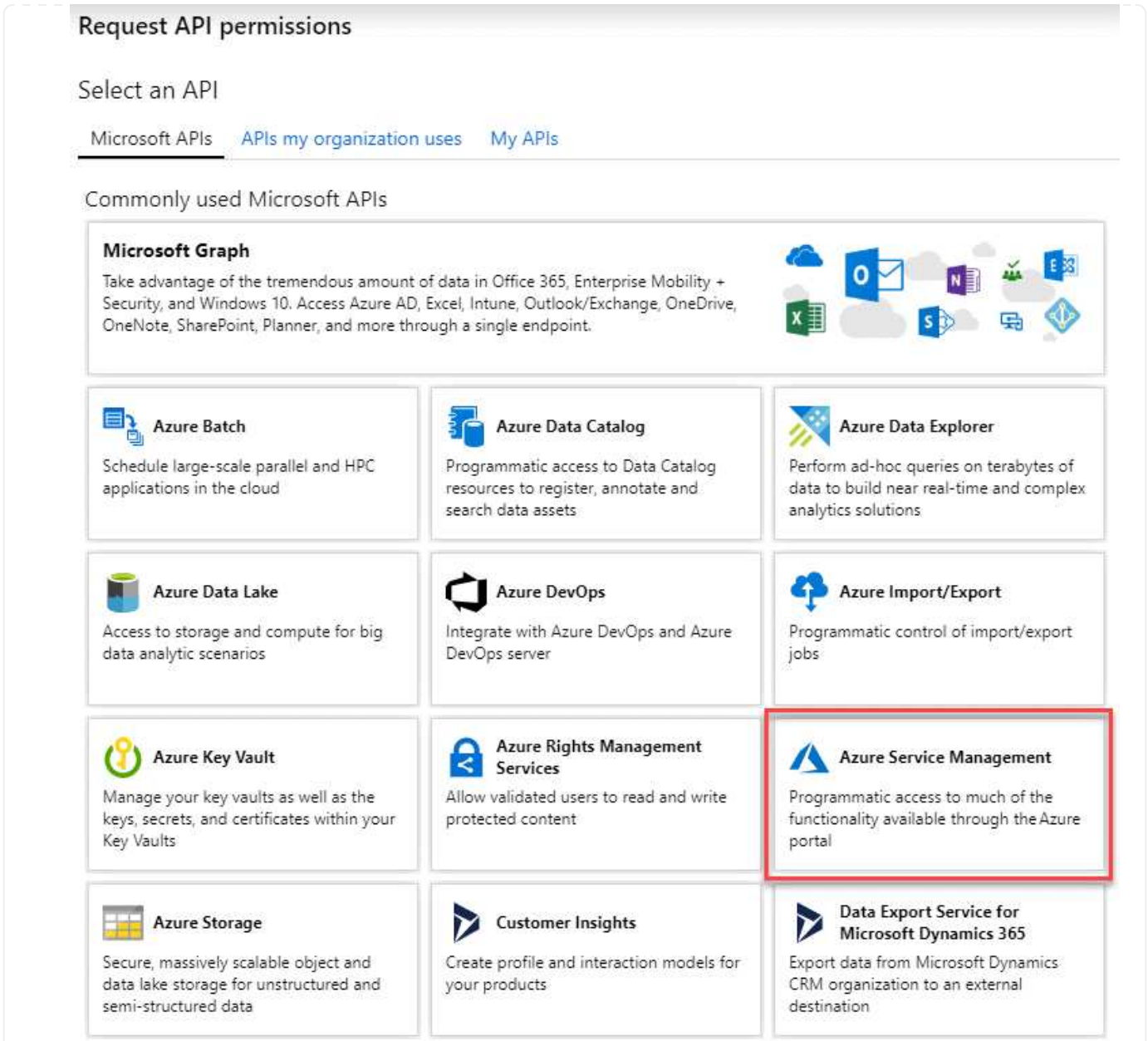
6. 单击*审阅+分配*。

服务主体现在具有部署控制台代理所需的 Azure 权限。

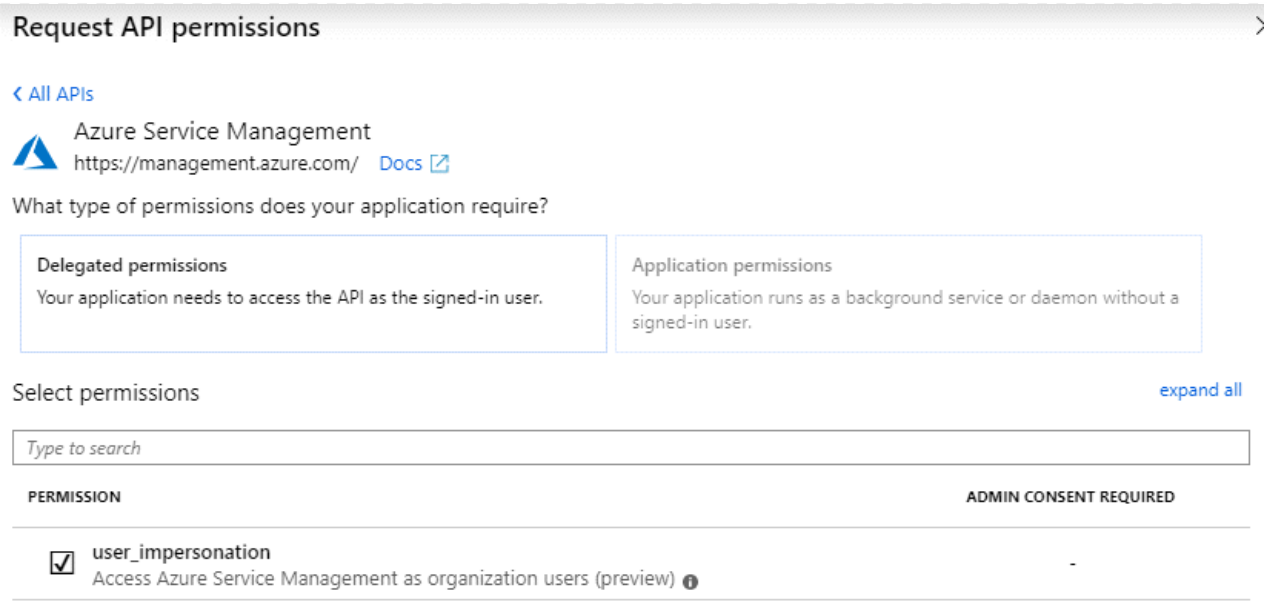
如果您想要管理多个 Azure 订阅中的资源，则必须将服务主体绑定到每个订阅。例如，控制台允许您选择部署Cloud Volumes ONTAP时要使用的订阅。

添加 **Windows Azure** 服务管理 **API** 权限

1. 在*Microsoft Entra ID*服务中，选择*App Registrations*并选择应用程序。
2. 选择*API 权限 > 添加权限*。
3. 在“Microsoft API”下，选择“Azure 服务管理”。

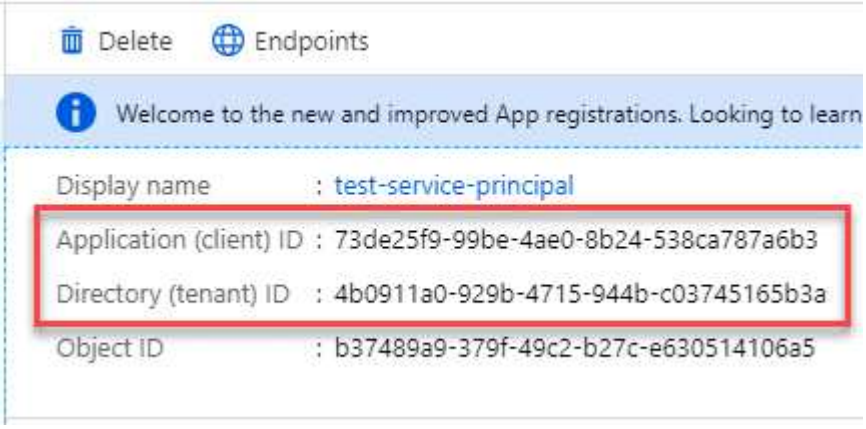


4. 选择*以组织用户身份访问 Azure 服务管理*，然后选择*添加权限*。



获取应用程序的应用程序**ID**和目录**ID**

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



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

创建客户端机密

1. 开启*Microsoft Entra ID*服务。
2. 选择*应用程序注册*并选择您的应用程序。
3. 选择*证书和机密>新客户端机密*。
4. 提供秘密的描述和持续时间。
5. 选择“添加”。
6. 复制客户端机密的值。

结果

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

步骤 **4**：创建控制台代理

直接从NetApp Console创建控制台代理。

关于此任务

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

开始之前

您应该具有以下内容：

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

  "了解如何连接到 Azure 中的 Linux VM"

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

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

步骤

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

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

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

     如果您已经登录 Azure 帐户，则控制台会自动使用该帐户。如果您有多个帐户，那么您可能需要先注销以确保您使用的是正确的帐户。
   - 选择“**Active Directory** 服务主体”以输入有关授予所需权限的 Microsoft Entra 服务主体的信息：
     - 应用程序（客户端）ID
     - 目录（租户）ID
     - 客户端密钥

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

   虚拟机的身份验证方法可以是密码或 SSH 公钥。

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

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

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

   如果您仍在使用"先前的端点"用于代理升级，验证失败并出现错误。为了避免这种情况，请取消选中复选框以跳过验证检查。
9. 选择“添加”。

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

结果

该过程完成后，即可从控制台使用控制台代理。

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

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

从 **Azure** 市场创建控制台代理

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

开始之前

- 你应该有一个"了解控制台代理"。
- 审查"控制台代理限制"。

步骤 **1**：设置网络

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

Azure 区域

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

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

VNet 和子网

创建控制台代理时，您需要指定它所在的 VNet 和子网。

连接到目标网络

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

出站互联网访问

部署控制台代理的网络位置必须具有出站互联网连接才能联系特定端点。

从控制台代理联系的端点

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

下面列出的端点都是 CNAME 条目。

端点	目的
\ https://management.azure.com \ https://login.microsoftonline.com \ https://blob.core.windows.net \ https://core.windows.net	管理 Azure 公共区域中的资源。

端点	目的
\ https://management.chinacloudapi.cn \ https://login.chinacloudapi.cn \ https://blob.core.chinacloudapi.cn \ https://core.chinacloudapi.cn	管理 Azure 中国区域的资源。
\ https://mysupport.netapp.com	获取许可信息并向NetApp支持发送AutoSupport消息。
\ https://signin.b2c.netapp.com	更新NetApp支持站点 (NSS) 凭据或将新的 NSS 凭据添加到NetApp Console。
\ https://support.netapp.com	获取许可信息并向NetApp支持发送AutoSupport消息以及接收Cloud Volumes ONTAP的软件更新。
\ https://api.bluexp.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com \ https://console.netapp.com \ https://components.console.bluexp.netapp.com \ https://cdn.auth0.com	在NetApp Console中提供功能和服务。
\ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://bluexpinfraprod.azurecr.io	获取控制台代理升级的图像。 • 当您部署新代理时，验证检查会测试与当前端点的连接。如果你使用"先前的端点"，验证检查失败。为了避免此失败，请跳过验证检查。 尽管以前的端点仍然受支持，但NetApp建议尽快将防火墙规则更新到当前端点。"了解如何更新终端节点列表" 。 • 当您更新到防火墙中的当前端点时，您现有的代理将继续工作。

代理服务器

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

- IP 地址
- 凭据
- HTTPS 证书

端口

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

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

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

启用 **NTP**

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

创建控制台代理后实现网络要求。

步骤 **2**：查看 **VM** 要求

创建控制台代理时，请选择满足以下要求的虚拟机类型。

CPU

8 个核心或 8 个 vCPU

RAM

32 GB

Azure VM 大小

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

步骤 **3**：设置权限

您可以通过以下方式提供权限：

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

按照以下步骤设置控制台的权限。

自定义角色

请注意，您可以使用 Azure 门户、Azure PowerShell、Azure CLI 或 REST API 创建 Azure 自定义角色。以下步骤展示如何使用 Azure CLI 创建角色。如果您希望使用其他方法，请参阅 "Azure 文档"

步骤

1. 如果您计划在自己的主机上手动安装该软件，请在 VM 上启用系统分配的托管标识，以便您可以通过自定义角色提供所需的 Azure 权限。

   "Microsoft Azure 文档：使用 Azure 门户为 VM 上的 Azure 资源配置托管标识"

2. 复制"连接器的自定义角色权限"并将它们保存在 JSON 文件中。
3. 通过将 Azure 订阅 ID 添加到可分配范围来修改 JSON 文件。

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

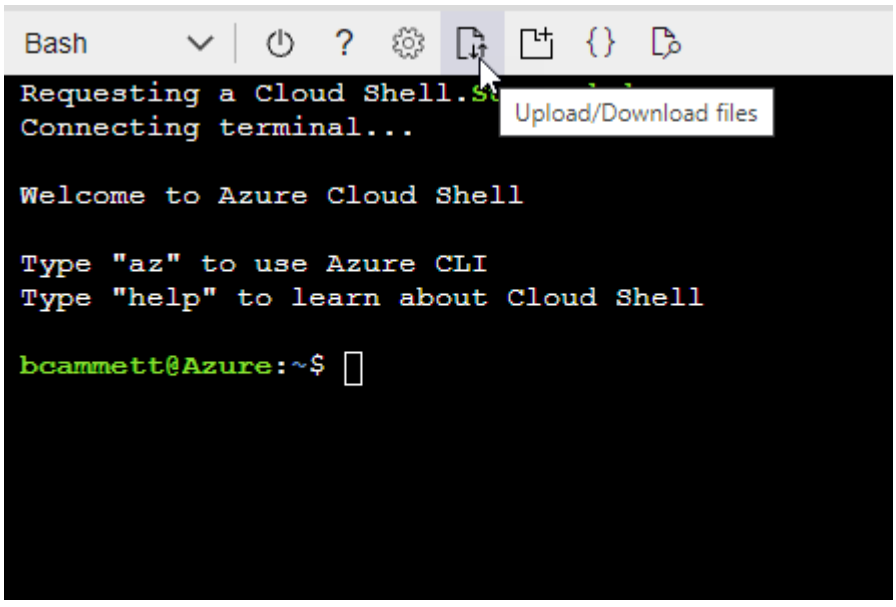
   例子

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

4. 使用 JSON 文件在 Azure 中创建自定义角色。

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

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



c. 使用 Azure CLI 创建自定义角色：

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

服务主体

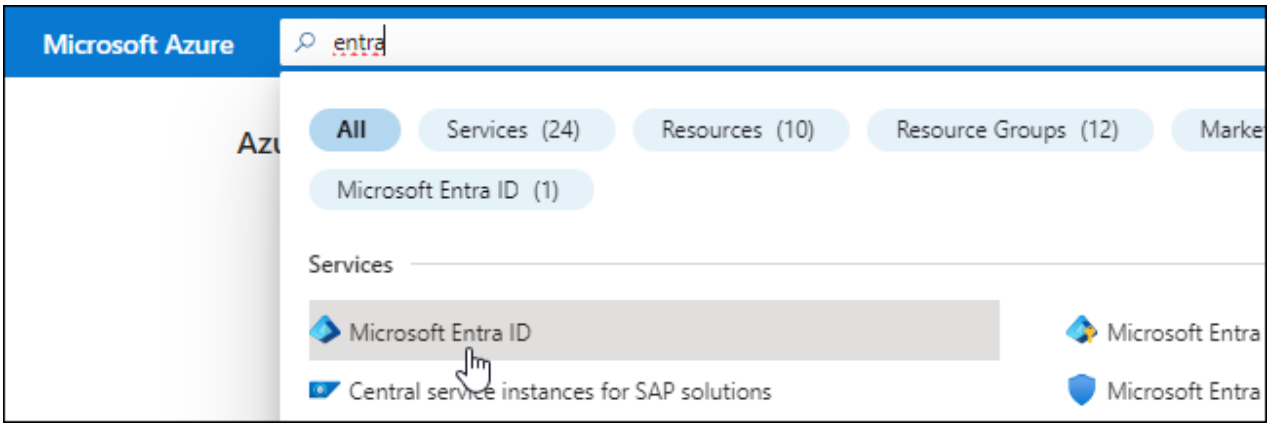
在 Microsoft Entra ID 中创建并设置服务主体，并获取控制台所需的 Azure 凭据。

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

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

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

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



3. 在菜单中，选择*应用程序注册*。
4. 选择*新注册*。
5. 指定有关应用程序的详细信息：
   - 名称：输入应用程序的名称。
   - 帐户类型：选择帐户类型（任何类型都可以与NetApp Console一起使用）。
   - 重定向 **URI**：您可以将此字段留空。
6. 选择*注册*。

   您已创建 AD 应用程序和服务主体。

将应用程序分配给角色

1. 创建自定义角色：

   请注意，您可以使用 Azure 门户、Azure PowerShell、Azure CLI 或 REST API 创建 Azure 自定义角色。以下步骤展示如何使用 Azure CLI 创建角色。如果您希望使用其他方法，请参阅 "Azure 文档"

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

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

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

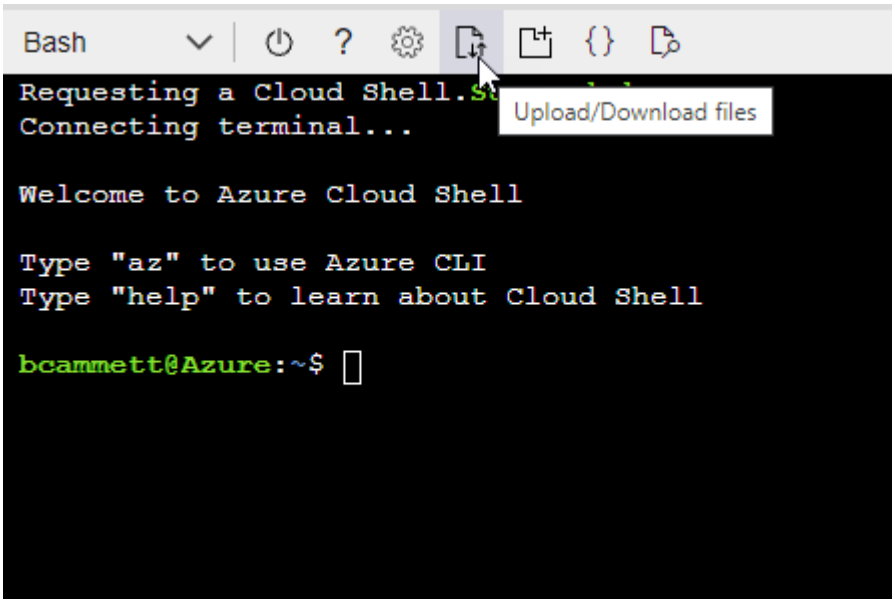
例子

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

c. 使用 JSON 文件在 Azure 中创建自定义角色。

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

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



- 使用 Azure CLI 创建自定义角色：

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

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

2. 将应用程序分配给角色：

a. 从 Azure 门户打开 **Subscriptions** 服务。

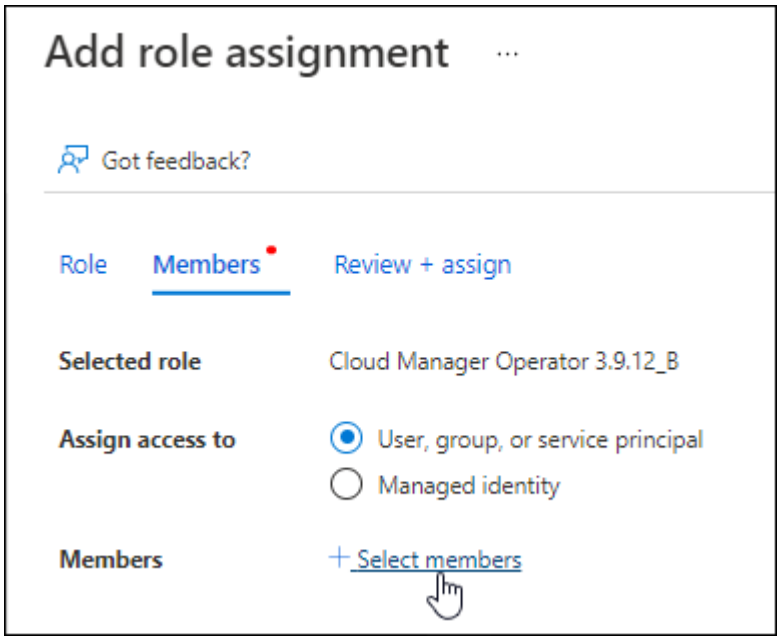
b. 选择订阅。

c. 选择“访问控制 (IAM)”>“添加”>“添加角色分配”。

d. 在*角色*选项卡中，选择*控制台操作员*角色并选择*下一步*。

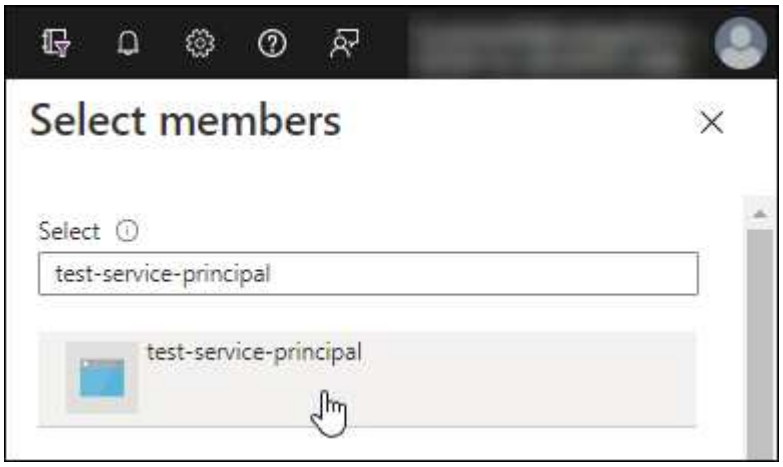
e. 在“成员”选项卡中，完成以下步骤：

- 保持选中“用户、组或服务主体”。
- 选择*选择成员*。



- 搜索应用程序的名称。

  以下是一个例子：



- 选择应用程序并选择*选择*。
- 选择“下一步”。

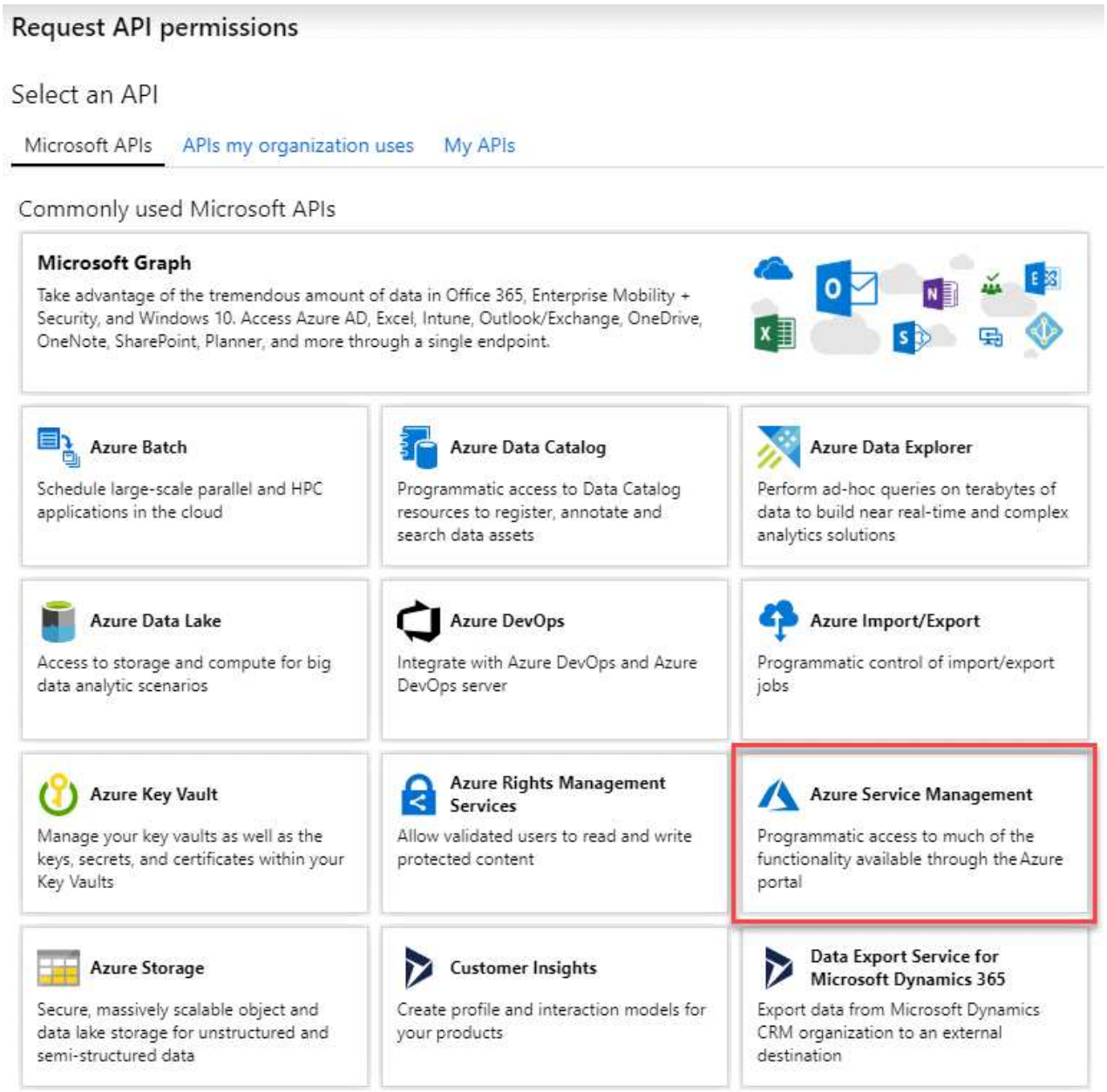
f. 选择*审阅+分配*。

服务主体现在具有部署控制台代理所需的 Azure 权限。

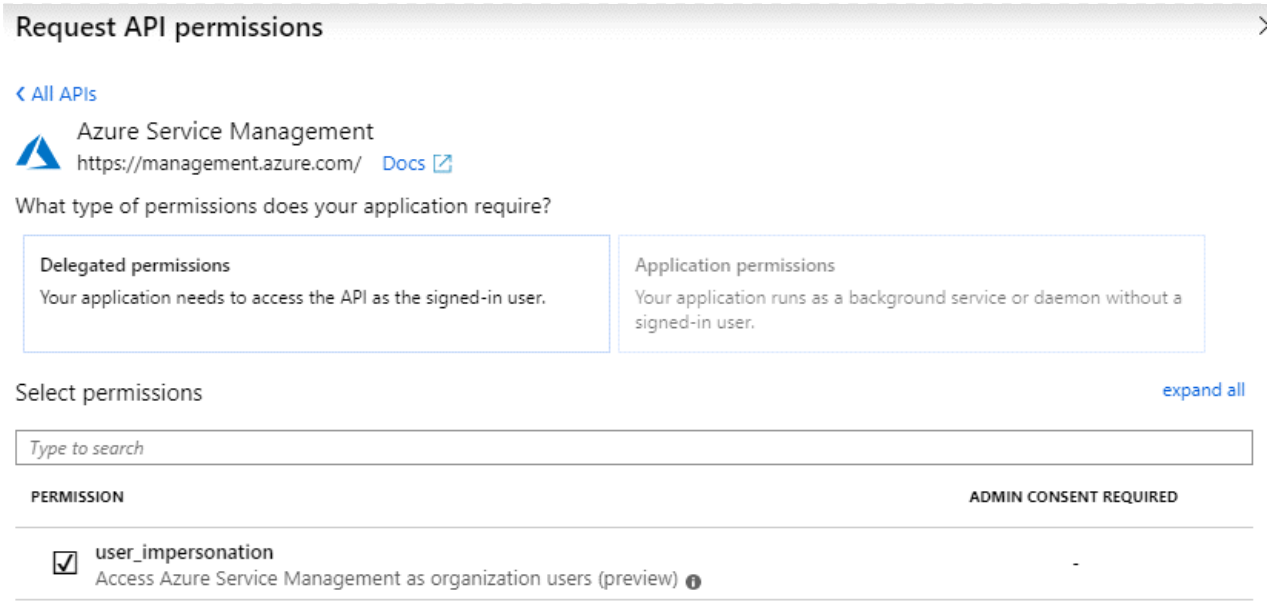
如果您想从多个 Azure 订阅部署Cloud Volumes ONTAP ，则必须将服务主体绑定到每个订阅。在NetApp Console中，您可以选择部署Cloud Volumes ONTAP时要使用的订阅。

添加 **Windows Azure** 服务管理 **API** 权限

1. 在*Microsoft Entra ID*服务中，选择*App Registrations*并选择应用程序。
2. 选择*API 权限 > 添加权限*。
3. 在“Microsoft API”下，选择“Azure 服务管理”。

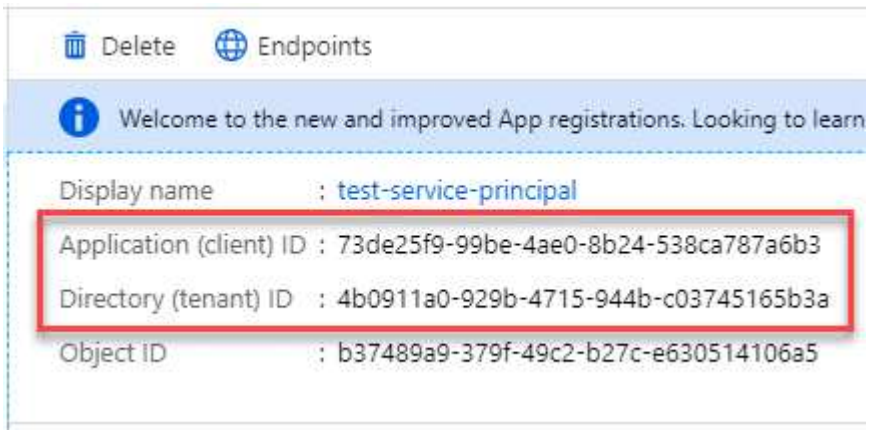


4. 选择*以组织用户身份访问 Azure 服务管理*，然后选择*添加权限*。



获取应用程序的应用程序**ID**和目录**ID**

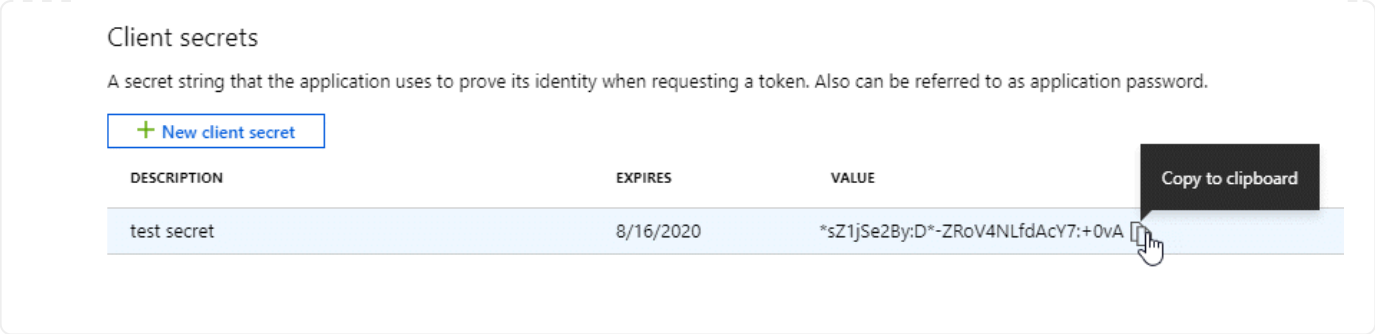
1. 在*Microsoft Entra ID*服务中，选择*App Registrations*并选择应用程序。
2. 复制*应用程序（客户端）ID*和*目录（租户）ID*。



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

创建客户端机密

1. 开启*Microsoft Entra ID*服务。
2. 选择*应用程序注册*并选择您的应用程序。
3. 选择*证书和机密>新客户端机密*。
4. 提供秘密的描述和持续时间。
5. 选择“添加”。
6. 复制客户端机密的值。



步骤 **4**：创建控制台代理

直接从 Azure 市场启动控制台代理。

关于此任务

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

开始之前

您应该具有以下内容：

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

  "了解如何连接到 Azure 中的 Linux VM"

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

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

步骤

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

   "商业区域的 Azure 市场页面"

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

   配置虚拟机时请注意以下事项：

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

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

  "查看 Azure 的安全组规则" 。

- 身份*：在*管理*下，选择*启用系统分配的托管身份*。

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

4. 在“审查 + 创建”页面上，审查您的选择并选择“创建”以开始部署。

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

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

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

   https://ipaddress

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

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

   d. 选择*让我们开始吧*。

结果

现在您已经安装了控制台代理并将其与您的控制台组织一起设置。

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

步骤 **5**：向控制台代理提供权限

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

自定义角色

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

步骤

1. 从 Azure 门户打开“订阅”服务并选择您的订阅。

   从*订阅*服务分配角色很重要，因为这指定了订阅级别的角色分配范围。 _范围_定义了访问适用的资源集。如果您在不同级别（例如，虚拟机级别）指定范围，则您在NetApp Console内完成操作的能力将受到影响。

   "Microsoft Azure 文档：了解 Azure RBAC 的范围"

2. 选择*访问控制 (IAM)* > 添加 > 添加角色分配。
3. 在*角色*选项卡中，选择*控制台操作员*角色并选择*下一步*。

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

4. 在“成员”选项卡中，完成以下步骤：
   a. 分配对*托管身份*的访问权限。
   b. 选择“选择成员”，选择创建控制台代理虚拟机的订阅，在“托管标识”下，选择“虚拟机”，然后选择控制台代理虚拟机。
   c. 选择*选择*。
   d. 选择“下一步”。
   e. 选择*审阅+分配*。
   f. 如果要管理其他 Azure 订阅中的资源，请切换到该订阅，然后重复这些步骤。

下一步是什么?

前往 "NetApp Console"开始使用控制台代理。

服务主体

步骤

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

结果

控制台现在具有代表您在 Azure 中执行操作所需的权限。

在 **Azure** 中手动安装控制台代理

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

开始之前

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

步骤 **1**：查看主机要求

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

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

专用主机

控制台代理需要专用主机。只要满足以下尺寸要求，任何架构都受支持：

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

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

  - `/var`：必须有 40 GiB 可用空间

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

Azure VM 大小

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

虚拟机管理程序

需要经过认证可运行受支持的操作系统的裸机或托管虚拟机管理程序。

操作系统和容器要求

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

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

步骤 **2**：安装 **Podman** 或 **Docker Engine**

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

- Red Hat Enterprise Linux 8 和 9 需要 Podman。

  查看支持的 Podman 版本 。

- Ubuntu 需要 Docker 引擎。

  查看支持的 Docker Engine 版本 。

示例 **2.** 步骤

Podman

按照以下步骤安装和配置 Podman：

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

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

步骤

1. 如果主机上安装了 podman-docker 包，请将其删除。

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

2. 安装 Podman。

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

   a. 对于 Red Hat Enterprise Linux 9.6：

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

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

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

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

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

   c. 对于 Red Hat Enterprise Linux 8：

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

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

3. 启用并启动 podman.socket 服务。

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

4. 安装 python3。

```
sudo dnf install python3
```

5. 如果您的系统上还没有 EPEL 存储库包，请安装它。

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

6. 如果使用 Red Hat Enterprise 9：

   a. 安装EPEL存储库软件包。

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

   +

   a. 安装 podman-compose 包 1.5.0。

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

7. 如果使用的是 Red Hat Enterprise Linux 8：

   a. 安装EPEL存储库软件包。

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

   b. 安装 podman-compose 包 1.0.6。

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

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

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

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

```
podman info | grep networkBackend
```

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

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

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

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

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

v. 重新启动 podman。

```
systemctl restart podman
```

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

```
podman info | grep networkBackend
```

Docker 引擎

按照 Docker 的文档安装 Docker Engine。

步骤

1. "查看 Docker 的安装说明"

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

2. 验证 Docker 是否已启用并正在运行。

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

步骤 **3**：设置网络

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

Azure 区域

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

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

连接到目标网络

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

出站互联网访问

部署控制台代理的网络位置必须具有出站互联网连接才能联系特定端点。

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

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

"为NetApp控制台准备网络" 。

从控制台代理联系的端点

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

下面列出的端点都是 CNAME 条目。

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

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

代理服务器

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

- IP 地址
- 凭据
- HTTPS 证书

端口

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

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

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

启用 **NTP**

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

步骤 **4**：设置控制台代理部署权限

您需要使用以下选项之一向控制台代理提供 Azure 权限：

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

按照步骤为控制台代理准备权限。

为控制台代理部署创建自定义角色

请注意，您可以使用 Azure 门户、Azure PowerShell、Azure CLI 或 REST API 创建 Azure 自定义角色。以下步骤展示如何使用 Azure CLI 创建角色。如果您希望使用其他方法，请参阅 "Azure 文档"

步骤

1. 如果您计划在自己的主机上手动安装该软件，请在 VM 上启用系统分配的托管标识，以便您可以通过自定义角色提供所需的 Azure 权限。

   "Microsoft Azure 文档：使用 Azure 门户为 VM 上的 Azure 资源配置托管标识"

2. 复制"连接器的自定义角色权限"并将它们保存在 JSON 文件中。
3. 通过将 Azure 订阅 ID 添加到可分配范围来修改 JSON 文件。

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

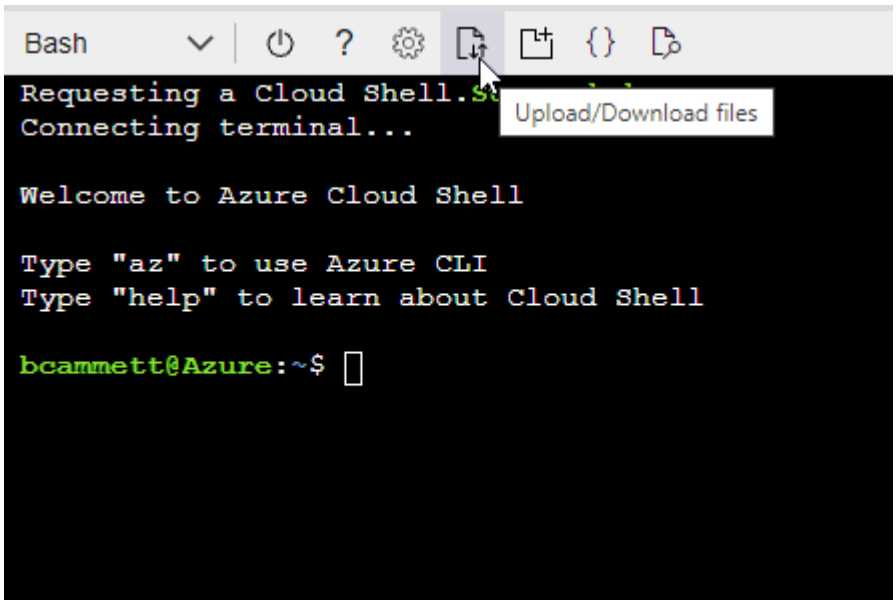
   例子

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

4. 使用 JSON 文件在 Azure 中创建自定义角色。

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

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



c. 使用 Azure CLI 创建自定义角色：

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

服务主体

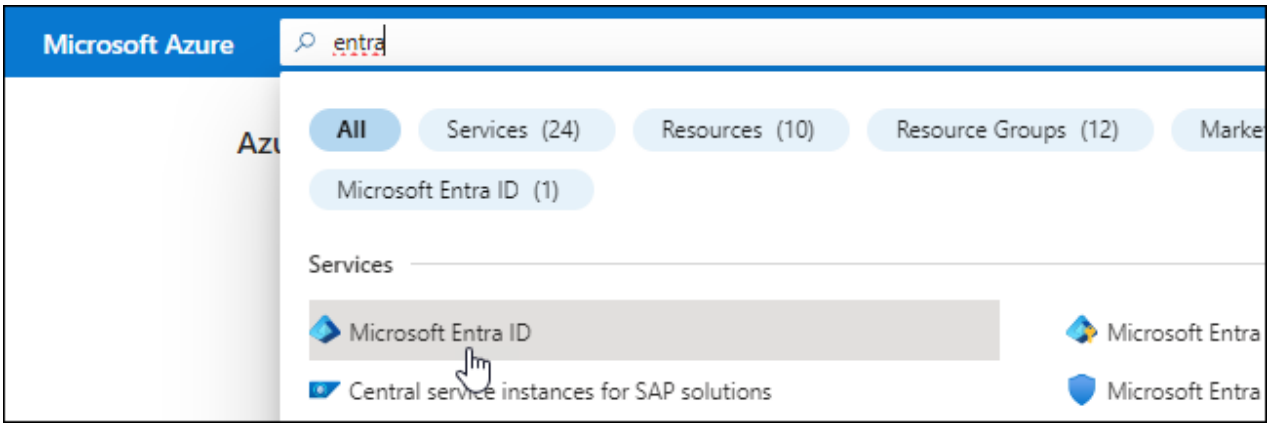
在 Microsoft Entra ID 中创建并设置服务主体，并获取控制台代理所需的 Azure 凭据。

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

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

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

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



3. 在菜单中，选择*应用程序注册*。
4. 选择*新注册*。
5. 指定有关应用程序的详细信息：
   - 名称：输入应用程序的名称。
   - 帐户类型：选择帐户类型（任何类型都可以与NetApp Console一起使用）。
   - 重定向 **URI**：您可以将此字段留空。
6. 选择*注册*。

   您已创建 AD 应用程序和服务主体。

将应用程序分配给角色

1. 创建自定义角色：

   请注意，您可以使用 Azure 门户、Azure PowerShell、Azure CLI 或 REST API 创建 Azure 自定义角色。以下步骤展示如何使用 Azure CLI 创建角色。如果您希望使用其他方法，请参阅 "Azure 文档"

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

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

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

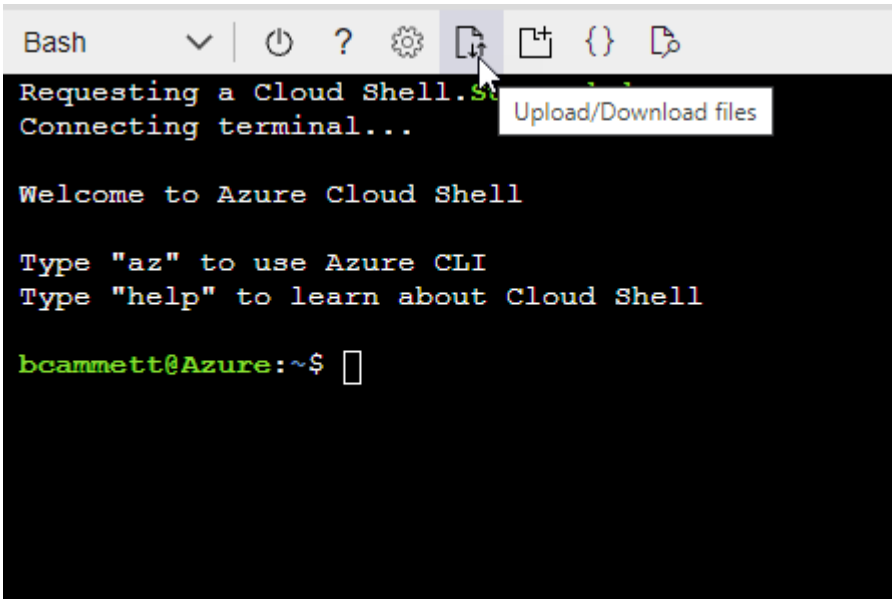
例子

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

c. 使用 JSON 文件在 Azure 中创建自定义角色。

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

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



- 使用 Azure CLI 创建自定义角色：

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

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

2. 将应用程序分配给角色：

a. 从 Azure 门户打开 **Subscriptions** 服务。

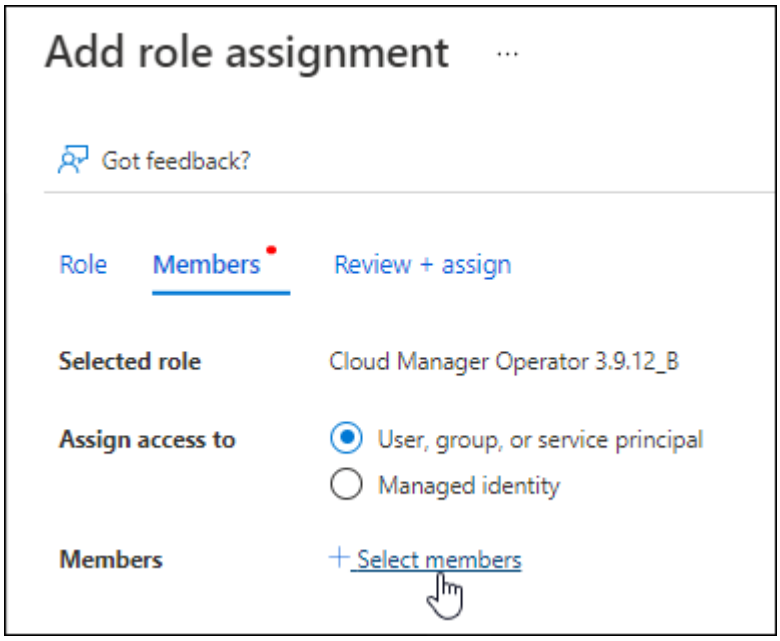
b. 选择订阅。

c. 选择“访问控制 (IAM)”>“添加”>“添加角色分配”。

d. 在*角色*选项卡中，选择*控制台操作员*角色并选择*下一步*。

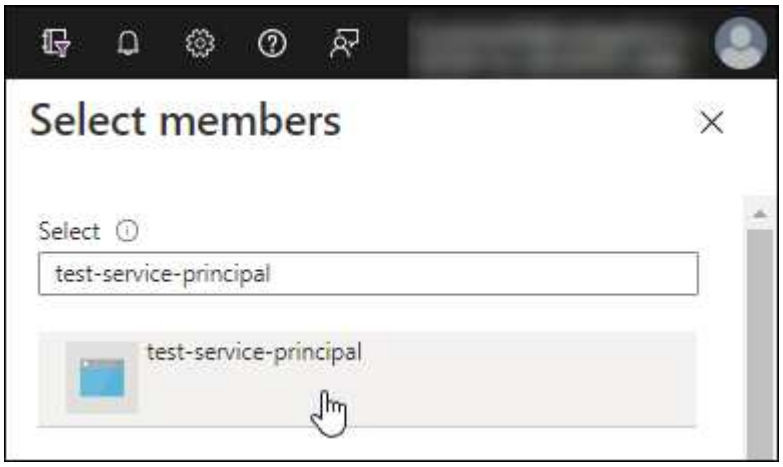
e. 在“成员”选项卡中，完成以下步骤：

- 保持选中“用户、组或服务主体”。
- 选择*选择成员*。



- 搜索应用程序的名称。

  以下是一个例子：



- 选择应用程序并选择*选择*。
- 选择“下一步”。

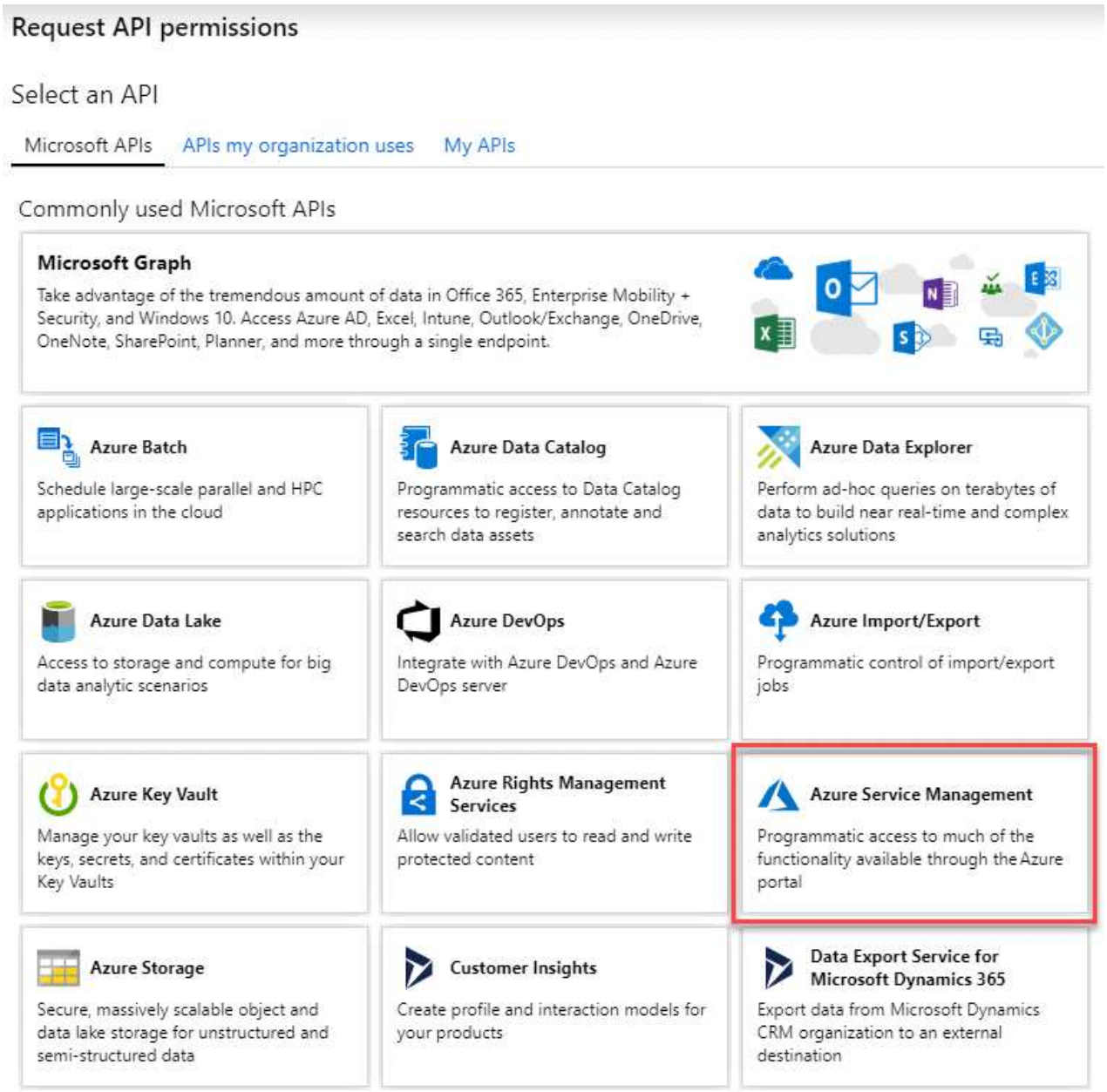
f. 选择*审阅+分配*。

服务主体现在具有部署控制台代理所需的 Azure 权限。

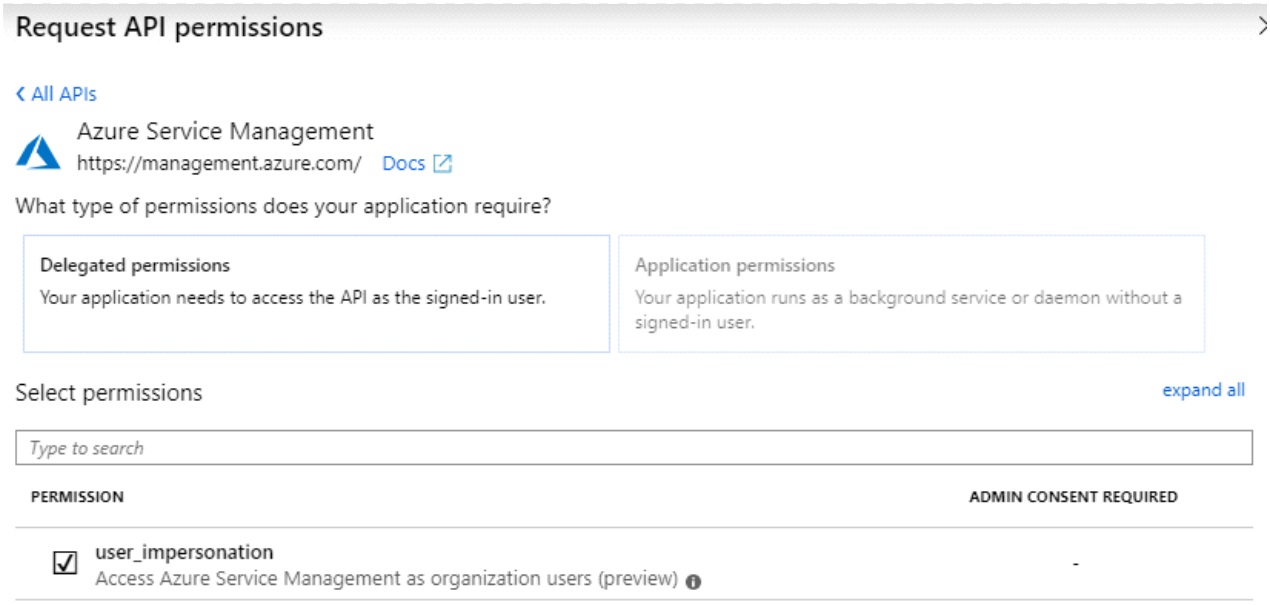
如果您想从多个 Azure 订阅部署Cloud Volumes ONTAP ，则必须将服务主体绑定到每个订阅。在NetApp Console中，您可以选择部署Cloud Volumes ONTAP时要使用的订阅。

添加 **Windows Azure** 服务管理 **API** 权限

1. 在*Microsoft Entra ID*服务中，选择*App Registrations*并选择应用程序。
2. 选择*API 权限 > 添加权限*。
3. 在“Microsoft API”下，选择“Azure 服务管理”。

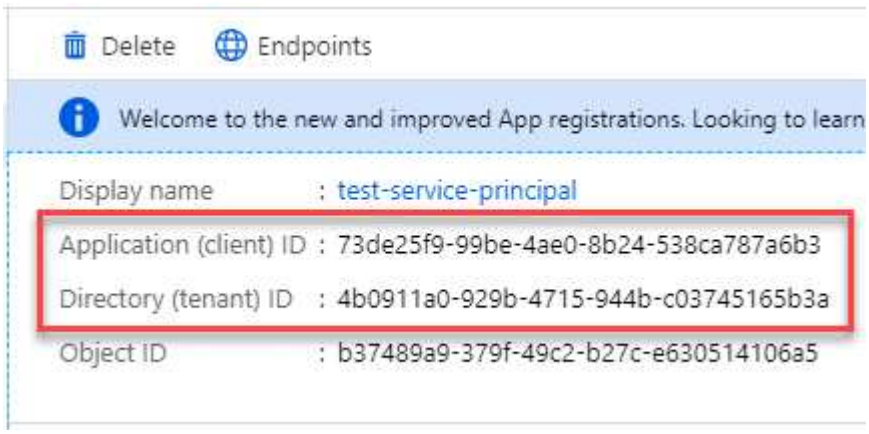


4. 选择*以组织用户身份访问 Azure 服务管理*，然后选择*添加权限*。



获取应用程序的应用程序**ID**和目录**ID**

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



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

创建客户端机密

1. 开启*Microsoft Entra ID*服务。
2. 选择*应用程序注册*并选择您的应用程序。
3. 选择*证书和机密>新客户端机密*。
4. 提供秘密的描述和持续时间。
5. 选择“添加”。
6. 复制客户端机密的值。

结果

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

步骤 **5**：安装控制台代理

前提条件完成后，您可以在自己的 Linux 主机上手动安装该软件。

开始之前

您应该具有以下内容：

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

  您可以选择在安装后配置代理服务器，但这样做需要重新启动控制台代理。

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

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

- 在 Azure 中的 VM 上启用托管标识，以便您可以通过自定义角色提供所需的 Azure 权限。

  "Microsoft Azure 文档：使用 Azure 门户为 VM 上的 Azure 资源配置托管标识"

关于此任务

安装后，如果有新版本可用，控制台代理会自动更新。

步骤

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

```
unset http_proxy
unset https_proxy
```

   如果不删除这些系统变量，安装将失败。

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

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

  选择下载代理安装程序文件或文件的 URL。

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

3. 分配运行脚本的权限。

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

其中 <version> 是您下载的控制台代理的版本。

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

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

如果您的网络需要代理才能访问互联网，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：

   https://ipaddress

2. 登录后，设置控制台代理：

   a. 指定与控制台代理关联的组织。

   b. 输入系统的名称。

   c. 在*您是否在安全环境中运行？*下保持限制模式处于禁用状态。

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

   d. 选择*让我们开始吧*。

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

步骤 6：提供对NetApp Console的权限

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

自定义角色

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

步骤

1. 从 Azure 门户打开“订阅”服务并选择您的订阅。

   从*订阅*服务分配角色很重要，因为这指定了订阅级别的角色分配范围。 _范围_定义了访问适用的资源集。如果您在不同级别（例如，虚拟机级别）指定范围，则您在NetApp Console内完成操作的能力将受到影响。

   "Microsoft Azure 文档：了解 Azure RBAC 的范围"

2. 选择*访问控制 (IAM)* > 添加 > 添加角色分配。
3. 在*角色*选项卡中，选择*控制台操作员*角色并选择*下一步*。

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

4. 在“成员”选项卡中，完成以下步骤：
   a. 分配对*托管身份*的访问权限。
   b. 选择“选择成员”，选择创建控制台代理虚拟机的订阅，在“托管标识”下，选择“虚拟机”，然后选择控制台代理虚拟机。
   c. 选择*选择*。
   d. 选择“下一步”。
   e. 选择*审阅+分配*。
   f. 如果要管理其他 Azure 订阅中的资源，请切换到该订阅，然后重复这些步骤。

下一步是什么?

前往 "NetApp Console"开始使用控制台代理。

服务主体

步骤

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

结果

控制台代理现在具有代表您在 Azure 中执行操作所需的权限。

Google Cloud

Google Cloud 中的控制台代理安装选项

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

有以下安装选项可用：

- "直接从控制台创建控制台代理"（这是标准选项）

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

- "使用 Google Platform 创建控制台代理"

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

- "在您自己的Linux主机上下载并手动安装软件"

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

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

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

开始之前

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

步骤 1：设置网络

设置网络以确保控制台代理可以管理资源，并连接到目标网络和出站互联网访问。

VPC 和子网

创建控制台代理时，您需要指定它所在的 VPC 和子网。

连接到目标网络

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

出站互联网访问

部署控制台代理的网络位置必须具有出站互联网连接才能联系特定端点。

从控制台代理联系的端点

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

下面列出的端点都是 CNAME 条目。

端点	目的
\ https://www.googleapis.com/compute/v1/ \ https://compute.googleapis.com/compute/v1 \ https://cloudresourcemanager.googleapis.com/v1/projects \ https://www.googleapis.com/compute/beta \ https://storage.googleapis.com/storage/v1 \ https://www.googleapis.com/storage/v1 \ https://iam.googleapis.com/v1 \ https://cloudkms.googleapis.com/v1 \ https://config.googleapis.com/v1/projects	管理 Google Cloud 中的资源。
\ https://mysupport.netapp.com	获取许可信息并向NetApp支持发送AutoSupport消息。
\ https://signin.b2c.netapp.com	更新NetApp支持站点 (NSS) 凭据或将新的 NSS 凭据添加到NetApp Console。
\ https://support.netapp.com	获取许可信息并向NetApp支持发送AutoSupport消息以及接收Cloud Volumes ONTAP的软件更新。
\ https://api.bluexp.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com \ https://console.netapp.com \ https://components.console.bluexp.netapp.com \ https://cdn.auth0.com	在NetApp Console中提供功能和服务。
\ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://bluexpinfraprod.azurecr.io	获取控制台代理升级的图像。 • 当您部署新代理时，验证检查会测试与当前端点的连接。如果你使用"先前的端点"，验证检查失败。为了避免此失败，请跳过验证检查。 尽管以前的端点仍然受支持，但NetApp建议尽快将防火墙规则更新到当前端点。"了解如何更新终端节点列表" 。 • 当您更新到防火墙中的当前端点时，您现有的代理将继续工作。

从**NetApp**控制台联系的端点

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

"查看从NetApp控制台联系的端点列表" 。

代理服务器

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

- IP 地址
- 凭据
- HTTPS 证书

端口

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

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

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

启用 **NTP**

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

创建控制台代理后实现此网络需求。

步骤 **2**：设置权限以创建控制台代理

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

步骤

1. 在 Google 平台中创建自定义角色：

   a. 创建包含以下权限的 YAML 文件：

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

```
- cloudbuild.builds.get
- compute.disks.create
- compute.disks.get
- compute.disks.list
- compute.disks.setLabels
- compute.disks.use
- compute.firewalls.create
- compute.firewalls.delete
- compute.firewalls.get
- compute.firewalls.list
- compute.globalOperations.get
- compute.images.get
- compute.images.getFromFamily
- compute.images.list
- compute.images.useReadOnly
- compute.instances.attachDisk
- compute.instances.create
- compute.instances.get
- compute.instances.list
- compute.instances.setDeletionProtection
- compute.instances.setLabels
- compute.instances.setMachineType
- compute.instances.setMetadata
- compute.instances.setTags
- compute.instances.start
- compute.instances.updateDisplayDevice
- compute.machineTypes.get
- compute.networks.get
- compute.networks.list
- compute.networks.updatePolicy
- compute.projects.get
- compute.regions.get
- compute.regions.list
- compute.subnetworks.get
- compute.subnetworks.list
- compute.zoneOperations.get
- compute.zones.get
- compute.zones.list
- config.deployments.create
- config.operations.get
- config.deployments.delete
- config.deployments.deleteState
- config.deployments.get
- config.deployments.getState
- config.deployments.list
```

```
- config.deployments.update
- config.deployments.updateState
- config.previews.get
- config.previews.list
- config.revisions.get
- config.resources.list
- deploymentmanager.compositeTypes.get
- deploymentmanager.compositeTypes.list
- deploymentmanager.deployments.create
- deploymentmanager.deployments.delete
- deploymentmanager.deployments.get
- deploymentmanager.deployments.list
- deploymentmanager.manifests.get
- deploymentmanager.manifests.list
- deploymentmanager.operations.get
- deploymentmanager.operations.list
- deploymentmanager.resources.get
- deploymentmanager.resources.list
- deploymentmanager.typeProviders.get
- deploymentmanager.typeProviders.list
- deploymentmanager.types.get
- deploymentmanager.types.list
- resourcemanager.projects.get
- compute.instances.setServiceAccount
- iam.serviceAccounts.actAs
- iam.serviceAccounts.create
- iam.serviceAccounts.list
- iam.serviceAccountKeys.create
- storage.buckets.create
- storage.buckets.get
- storage.objects.create
- storage.folders.create
- storage.objects.list
```

b. 从 Google Cloud 激活云壳。

c. 上传包含所需权限的 YAML 文件。

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

以下示例在项目级别创建一个名为“agentDeployment”的角色：

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

"Google Cloud 文档：创建和管理自定义角色"

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

"Google Cloud 文档：授予单个角色"

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

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

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

步骤

1. 在 Google Cloud 中创建自定义角色：

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

   b. 从 Google Cloud 激活云壳。

   c. 上传包含所需权限的 YAML 文件。

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

      以下示例在项目级别创建一个名为“agent”的角色：

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

   "Google Cloud 文档：创建和管理自定义角色"

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

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

   b. 输入服务帐户详细信息并选择*创建并继续*。

   c. 选择您刚刚创建的角色。

   d. 完成剩余步骤以创建角色。

      "Google Cloud 文档：创建服务帐号"

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

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

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

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

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

   有关详细信息，请参阅 "Google Cloud 文档"

步骤 **4**：设置共享 **VPC** 权限

如果您使用共享 VPC 将资源部署到服务项目中，则需要准备好您的权限。

此表仅供参考，当 IAM 配置完成时，您的环境应该反映权限表。

查看共享 **VPC** 权限

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

注：

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

步骤 **5**：启用 **Google Cloud API**

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

步骤

1. 在您的项目中启用以下 Google Cloud API：
   - 云部署管理器 V2 API
   - 云基础设施管理器 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 与客户管理的加密密钥 (CMEK) 一起使用时才需要）
   - Cloud Quotas API（使用 Infrastructure Manager 部署 Cloud Volumes ONTAP 时需要）

"Google Cloud 文档：启用 API"

步骤 **6**：创建控制台代理

直接从控制台创建控制台代理。

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

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

开始之前

您应该具有以下内容：

- 创建控制台代理所需的 Google Cloud 权限以及控制台代理虚拟机的服务帐号。
- 满足组网需求的VPC及子网。
- 如果控制台代理需要代理才能访问互联网，则提供有关代理服务器的详细信息。

步骤

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

     该表单由 Google 拥有并托管。您的凭据未提供给NetApp。
   - 详细信息：输入虚拟机实例的名称，指定标签，选择项目，然后选择具有所需权限的服务帐户（有关详细信息，请参阅上面的部分）。

- 位置：指定实例的区域、区域、VPC 和子网。
- 网络：选择是否启用公共 IP 地址并选择性地指定代理配置。
- 网络标签：如果使用透明代理，则向控制台代理实例添加网络标签。网络标签必须以小写字母开头，并且可以包含小写字母、数字和连字符。标签必须以小写字母或数字结尾。例如，您可以使用标签“console-agent-proxy”。
- 防火墙策略：选择是否创建新的防火墙策略，或者是否选择允许所需入站和出站规则的现有防火墙策略。

  "Google Cloud 中的防火墙规则"

5. 检查您的选择以验证您的设置是否正确。

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

   如果您仍在使用"先前的端点"用于代理升级，验证失败并出现错误。为了避免这种情况，请取消选中复选框以跳过验证检查。

6. 选择“添加”。

   代理大约需要 10 分钟才能准备就绪；请停留在页面上直到该过程完成。

结果

该过程完成后，控制台代理即可使用。

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

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

从 **Google Cloud** 创建控制台代理

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

开始之前

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

步骤 **1**：设置网络

设置网络以使控制台代理能够管理资源并连接到目标网络和互联网。

VPC 和子网

创建控制台代理时，您需要指定它所在的 VPC 和子网。

连接到目标网络

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

出站互联网访问

部署控制台代理的网络位置必须具有出站互联网连接才能联系特定端点。

从控制台代理联系的端点

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

下面列出的端点都是 CNAME 条目。

端点	目的
\ https://www.googleapis.com/compute/v1/ \ https://compute.googleapis.com/compute/v1 \ https://cloudresourcemanager.googleapis.com/v1/projects \ https://www.googleapis.com/compute/beta \ https://storage.googleapis.com/storage/v1 \ https://www.googleapis.com/storage/v1 \ https://iam.googleapis.com/v1 \ https://cloudkms.googleapis.com/v1 \ https://config.googleapis.com/v1/projects	管理 Google Cloud 中的资源。
\ https://mysupport.netapp.com	获取许可信息并向NetApp支持发送AutoSupport消息。
\ https://signin.b2c.netapp.com	更新NetApp支持站点 (NSS) 凭据或将新的 NSS 凭据添加到NetApp Console。
\ https://support.netapp.com	获取许可信息并向NetApp支持发送AutoSupport消息以及接收Cloud Volumes ONTAP的软件更新。
\ https://api.bluexp.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com \ https://console.netapp.com \ https://components.console.bluexp.netapp.com \ https://cdn.auth0.com	在NetApp Console中提供功能和服务。

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

从**NetApp**控制台联系的端点

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

"查看从NetApp控制台联系的端点列表" 。

代理服务器

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

- IP 地址
- 凭据
- HTTPS 证书

端口

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

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

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

启用 **NTP**

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

的更多信息"

创建控制台代理后实现此网络需求。

步骤 **2**：设置权限以创建控制台代理

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

步骤

1. 在 Google 平台中创建自定义角色：

    a. 创建包含以下权限的 YAML 文件：

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

- cloudbuild.builds.get
- compute.disks.create
- compute.disks.get
- compute.disks.list
- compute.disks.setLabels
- compute.disks.use
- compute.firewalls.create
- compute.firewalls.delete
- compute.firewalls.get
- compute.firewalls.list
- compute.globalOperations.get
- compute.images.get
- compute.images.getFromFamily
- compute.images.list
- compute.images.useReadOnly
- compute.instances.attachDisk
- compute.instances.create
- compute.instances.get
- compute.instances.list
- compute.instances.setDeletionProtection
- compute.instances.setLabels
- compute.instances.setMachineType
- compute.instances.setMetadata
- compute.instances.setTags
- compute.instances.start
- compute.instances.updateDisplayDevice
- compute.machineTypes.get
- compute.networks.get
- compute.networks.list
- compute.networks.updatePolicy
- compute.projects.get
- compute.regions.get
- compute.regions.list
- compute.subnetworks.get
- compute.subnetworks.list
- compute.zoneOperations.get
- compute.zones.get
- compute.zones.list
- config.deployments.create
```

```
- config.operations.get
- config.deployments.delete
- config.deployments.deleteState
- config.deployments.get
- config.deployments.getState
- config.deployments.list
- config.deployments.update
- config.deployments.updateState
- config.previews.get
- config.previews.list
- config.revisions.get
- config.resources.list
- deploymentmanager.compositeTypes.get
- deploymentmanager.compositeTypes.list
- deploymentmanager.deployments.create
- deploymentmanager.deployments.delete
- deploymentmanager.deployments.get
- deploymentmanager.deployments.list
- deploymentmanager.manifests.get
- deploymentmanager.manifests.list
- deploymentmanager.operations.get
- deploymentmanager.operations.list
- deploymentmanager.resources.get
- deploymentmanager.resources.list
- deploymentmanager.typeProviders.get
- deploymentmanager.typeProviders.list
- deploymentmanager.types.get
- deploymentmanager.types.list
- resourcemanager.projects.get
- compute.instances.setServiceAccount
- iam.serviceAccounts.actAs
- iam.serviceAccounts.create
- iam.serviceAccounts.list
- iam.serviceAccountKeys.create
- storage.buckets.create
- storage.buckets.get
- storage.objects.create
- storage.folders.create
- storage.objects.list
```

b. 从 Google Cloud 激活云壳。

c. 上传包含所需权限的 YAML 文件。

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

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

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

"Google Cloud 文档：创建和管理自定义角色"

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

"Google Cloud 文档：授予单个角色"

步骤 **3**：设置控制台代理操作的权限

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

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

步骤

1. 在 Google Cloud 中创建自定义角色：

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

   b. 从 Google Cloud 激活云壳。

   c. 上传包含所需权限的 YAML 文件。

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

   以下示例在项目级别创建一个名为“agent”的角色：

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

   "Google Cloud 文档：创建和管理自定义角色"

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

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

   b. 输入服务帐户详细信息并选择*创建并继续*。

   c. 选择您刚刚创建的角色。

   d. 完成剩余步骤以创建角色。

   "Google Cloud 文档：创建服务帐号"

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

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

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

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

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

有关详细信息，请参阅 "Google Cloud 文档"

步骤 **4**：设置共享 **VPC** 权限

如果您使用共享 VPC 将资源部署到服务项目中，则需要准备好您的权限。

此表仅供参考，当 IAM 配置完成时，您的环境应该反映权限表。

查看共享 **VPC** 权限

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

注：

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

步骤 **5**：启用 **Google Cloud API**

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

步骤

1. 在您的项目中启用以下 Google Cloud API：
   - 云部署管理器 V2 API
   - 云基础设施管理器 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 与客户管理的加密密钥 (CMEK) 一起使用时才需要）
- Cloud Quotas API（使用 Infrastructure Manager 部署 Cloud Volumes ONTAP 时需要）

"Google Cloud 文档：启用 API"

步骤 **6**：创建控制台代理

使用 Google Cloud 创建控制台代理。

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

开始之前

您应该具有以下内容：

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

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

步骤

1. 使用您喜欢的方法登录 Google Cloud SDK。

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

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

2. 验证您是否以具有上述部分定义的所需权限的用户身份登录：

   ```
   gcloud auth list
   ```

   输出应显示以下内容，其中 * 用户帐户是要登录的用户帐户：

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

3. 运行 `gcloud compute instances create`命令：

```
gcloud compute instances create <instance-name>
  --machine-type=n2-standard-8
  --image-project=netapp-cloudmanager
  --image-family=cloudmanager
  --scopes=cloud-platform
  --project=<project>
  --service-account=<service-account>
  --zone=<zone>
  --no-address
  --tags <network-tag>
  --network <network-path>
  --subnet <subnet-path>
  --boot-disk-kms-key <kms-key-path>
```

实例名称
: VM 实例所需的实例名称。

项目
: （可选）您想要部署虚拟机的项目。

服务帐户
: 步骤 2 的输出中指定的服务帐户。

区
: 您想要部署虚拟机的区域

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

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

网络路径

（可选）添加要部署控制台代理的网络名称（对于共享 VPC，您需要完整路径）

子网路径

（可选）添加要部署控制台代理的子网名称（对于共享 VPC，您需要完整路径）

kms 密钥路径

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

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

运行该命令将部署控制台代理。控制台代理实例和软件应在大约五分钟内运行。

4. 打开 Web 浏览器并输入控制台代理主机 URL：

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

5. 登录后，设置控制台代理：

   a. 指定与控制台代理关联的控制台组织。

      "了解身份和访问管理" 。

   b. 输入系统的名称。

结果

控制台代理现已安装并设置到您的控制台组织。

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

在 **Google Cloud** 中手动安装控制台代理

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

开始之前

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

步骤 **1**：查看主机要求

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

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

专用主机

控制台代理需要专用主机。只要满足以下尺寸要求，任何架构都受支持：

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

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

  - `/var`：必须有 40 GiB 可用空间

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

Google Cloud 机器类型

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

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

虚拟机管理程序

需要经过认证可运行受支持的操作系统的裸机或托管虚拟机管理程序。

操作系统和容器要求

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

操作系统	支持的操作系统版本	支持的代理版本	所需的容器工具	**SELinux**
Red Hat Enterprise Linux		9.6 • 仅限英语版本。 • 主机必须在 Red Hat 订阅管理中注册。如果未注册，主机将无法在代理安装期间访问存储库来更新所需的第三方软件。	4.0.0 或更高版本，控制台处于标准模式或受限模式	Podman 版本 5.4.0，podman-compose 版本 1.5.0。 查看 Podman 配置要求 。

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

Google Cloud 机器类型

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

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

步骤 **2**：安装 **Podman** 或 **Docker Engine**

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

- Red Hat Enterprise Linux 8 和 9 需要 Podman。

  查看支持的 Podman 版本 。

- Ubuntu 需要 Docker 引擎。

  查看支持的 Docker Engine 版本 。

示例 3. 步骤

Podman

按照以下步骤安装和配置 Podman：

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

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

步骤

1. 如果主机上安装了 podman-docker 包，请将其删除。

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

2. 安装 Podman。

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

   a. 对于 Red Hat Enterprise Linux 9.6：

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

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

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

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

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

   c. 对于 Red Hat Enterprise Linux 8：

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

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

3. 启用并启动 podman.socket 服务。

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

4. 安装 python3。

```
sudo dnf install python3
```

5. 如果您的系统上还没有 EPEL 存储库包，请安装它。

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

6. 如果使用 Red Hat Enterprise 9：

   a. 安装EPEL存储库软件包。

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

   +

   a. 安装 podman-compose 包 1.5.0。

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

7. 如果使用的是 Red Hat Enterprise Linux 8：

   a. 安装EPEL存储库软件包。

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

   b. 安装 podman-compose 包 1.0.6。

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

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

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

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

```
podman info | grep networkBackend
```

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

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

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

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

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

v. 重新启动 podman。

```
systemctl restart podman
```

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

```
podman info | grep networkBackend
```

Docker 引擎

按照 Docker 的文档安装 Docker Engine。

步骤

1. "查看 Docker 的安装说明"

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

2. 验证 Docker 是否已启用并正在运行。

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

步骤 **3**：设置网络

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

连接到目标网络

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

出站互联网访问

部署控制台代理的网络位置必须具有出站互联网连接才能联系特定端点。

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

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

"为NetApp控制台准备网络" 。

从控制台代理联系的端点

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

下面列出的端点都是 CNAME 条目。

端点	目的
\ https://www.googleapis.com/compute/v1/ \ https://compute.googleapis.com/compute/v1 \ https://cloudresourcemanager.googleapis.com/v1/projects \ https://www.googleapis.com/compute/beta \ https://storage.googleapis.com/storage/v1 \ https://www.googleapis.com/storage/v1 \ https://iam.googleapis.com/v1 \ https://cloudkms.googleapis.com/v1 \ https://config.googleapis.com/v1/projects	管理 Google Cloud 中的资源。
\ https://mysupport.netapp.com	获取许可信息并向NetApp支持发送AutoSupport消息。
\ https://signin.b2c.netapp.com	更新NetApp支持站点 (NSS) 凭据或将新的 NSS 凭据添加到NetApp Console。
\ https://support.netapp.com	获取许可信息并向NetApp支持发送AutoSupport消息以及接收Cloud Volumes ONTAP的软件更新。
\ https://api.bluexp.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com \ https://console.netapp.com \ https://components.console.bluexp.netapp.com \ https://cdn.auth0.com	在NetApp Console中提供功能和服务。

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

代理服务器

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

- IP 地址
- 凭据
- HTTPS 证书

端口

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

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

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

启用 **NTP**

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

步骤 **4**：设置控制台代理的权限

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

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

步骤

1. 在 Google Cloud 中创建自定义角色：

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

   b. 从 Google Cloud 激活云壳。

   c. 上传包含所需权限的 YAML 文件。

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

      以下示例在项目级别创建一个名为“agent”的角色：

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

   "Google Cloud 文档：创建和管理自定义角色"

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

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

   b. 输入服务帐户详细信息并选择*创建并继续*。

   c. 选择您刚刚创建的角色。

   d. 完成剩余步骤以创建角色。

      "Google Cloud 文档：创建服务帐号"

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

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

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

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

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

   有关详细信息，请参阅 "Google Cloud 文档"

步骤 **5**：设置共享 **VPC** 权限

如果您使用共享 VPC 将资源部署到服务项目中，则需要准备好您的权限。

此表仅供参考，当 IAM 配置完成时，您的环境应该反映权限表。

查看共享 **VPC** 权限

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

注：

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

第 **6** 步：启用 **Google Cloud API**

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

步骤

1. 在您的项目中启用以下 Google Cloud API：
   - 云部署管理器 V2 API
   - 云基础设施管理器 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 与客户管理的加密密钥 (CMEK) 一起使用时才需要）
- Cloud Quotas API（使用 Infrastructure Manager 部署 Cloud Volumes ONTAP 时需要）

"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：

https://ipaddress

2. 登录后，设置控制台代理：

a. 指定与控制台代理关联的组织。

b. 输入系统的名称。

c. 在*您是否在安全环境中运行？*下保持限制模式处于禁用状态。

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

d. 选择*让我们开始吧*。

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

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

步骤 8：向控制台代理提供权限

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

步骤

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

   "Google Cloud 文档：更改实例的服务帐户和访问范围"

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

在本地安装代理

在本地手动安装控制台代理

在本地安装控制台代理，然后登录并设置它以与您的控制台组织协同工作。

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

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

准备安装控制台代理

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

查看控制台代理主机要求

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

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

专用主机

控制台代理需要专用主机。只要满足以下尺寸要求，任何架构都受支持：

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

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

- `/var`：必须有 40 GiB 可用空间

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

虚拟机管理程序

需要经过认证可运行受支持的操作系统的裸机或托管虚拟机管理程序。

操作系统和容器要求

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

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

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

为控制台代理设置网络访问

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

连接到目标网络

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

出站互联网访问

部署控制台代理的网络位置必须具有出站互联网连接才能联系特定端点。

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

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

"为NetApp控制台准备网络" 。

从控制台代理联系的端点

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

下面列出的端点都是 CNAME 条目。

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

AWS

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

从控制台代理联系的端点

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

下面列出的端点都是 CNAME 条目。

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

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

Azure

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

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

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

代理服务器

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

- IP 地址
- 凭据
- HTTPS 证书

端口

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

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

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

启用 **NTP**

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

为 **AWS** 或 **Azure** 创建控制台代理云权限

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

在安装控制台代理后将凭据添加到控制台代理。

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

AWS

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

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

步骤

1. 登录 AWS 控制台并导航到 IAM 服务。
2. 创建策略：

   a. 选择“策略”>“创建策略”。

   b. 选择 **JSON** 并复制并粘贴内容"控制台代理的 IAM 策略"。

   c. 完成剩余步骤以创建策略。

      根据您计划使用的NetApp数据服务，您可能需要创建第二个策略。

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

3. 将策略附加到 IAM 用户。

   - "AWS 文档：创建 IAM 角色"
   - "AWS 文档：添加和删除 IAM 策略"

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

结果

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

Azure

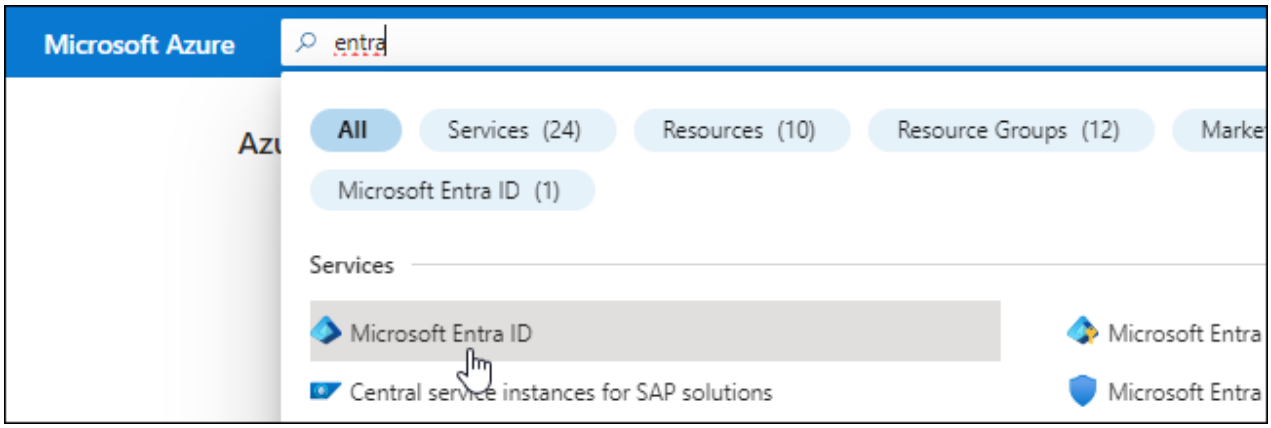
当控制台代理安装在本地时，您需要通过在 Microsoft Entra ID 中设置服务主体并获取控制台代理所需的 Azure 凭据来为控制台代理提供 Azure 权限。

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

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

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

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



3. 在菜单中，选择*应用程序注册*。
4. 选择*新注册*。
5. 指定有关应用程序的详细信息：
   - 名称：输入应用程序的名称。
   - 帐户类型：选择帐户类型（任何类型都可以与NetApp Console一起使用）。
   - 重定向 **URI**：您可以将此字段留空。
6. 选择*注册*。

   您已创建 AD 应用程序和服务主体。

将应用程序分配给角色

1. 创建自定义角色：

   请注意，您可以使用 Azure 门户、Azure PowerShell、Azure CLI 或 REST API 创建 Azure 自定义角色。以下步骤展示如何使用 Azure CLI 创建角色。如果您希望使用其他方法，请参阅 "Azure 文档"

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

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

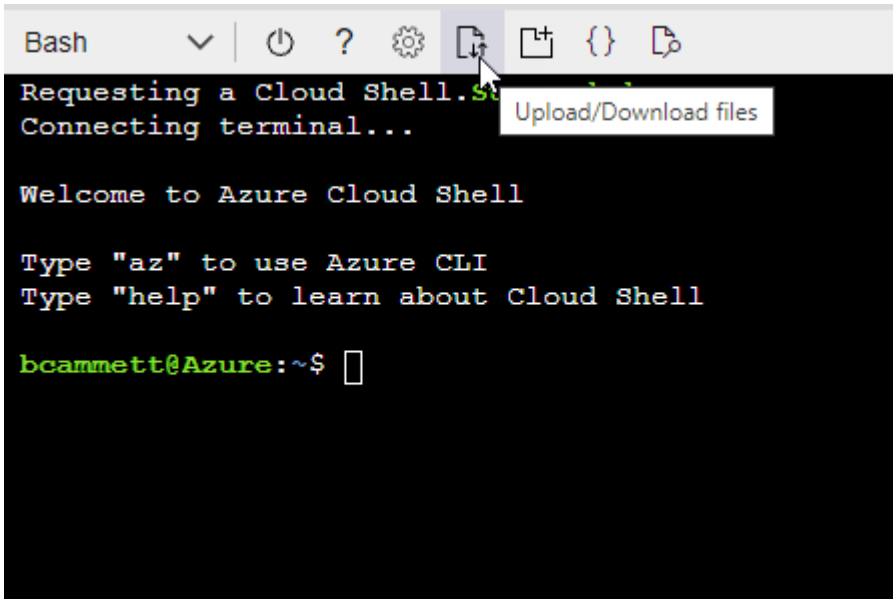
      例子

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

   c. 使用 JSON 文件在 Azure 中创建自定义角色。

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

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



- 使用 Azure CLI 创建自定义角色：

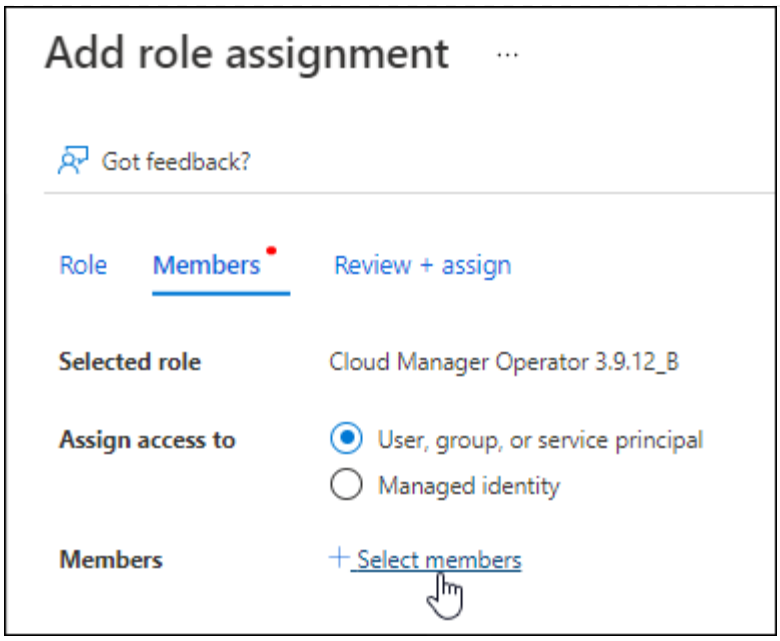
```
az role definition create --role-definition agent_Policy.json
```

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

2. 将应用程序分配给角色：

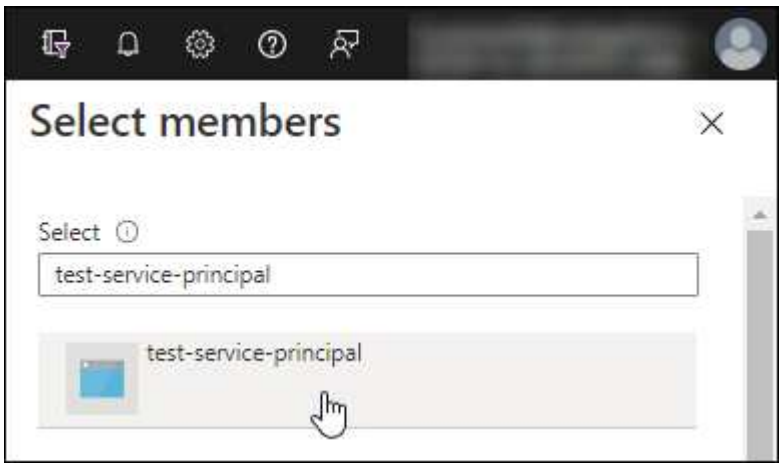
a. 从 Azure 门户打开 **Subscriptions** 服务。
b. 选择订阅。
c. 选择“访问控制 (IAM)”>“添加”>“添加角色分配”。
d. 在*角色*选项卡中，选择*控制台操作员*角色并选择*下一步*。
e. 在“成员”选项卡中，完成以下步骤：

- 保持选中“用户、组或服务主体”。
- 选择*选择成员*。



- 搜索应用程序的名称。

  以下是一个例子：



- 选择应用程序并选择*选择*。
- 选择“下一步”。

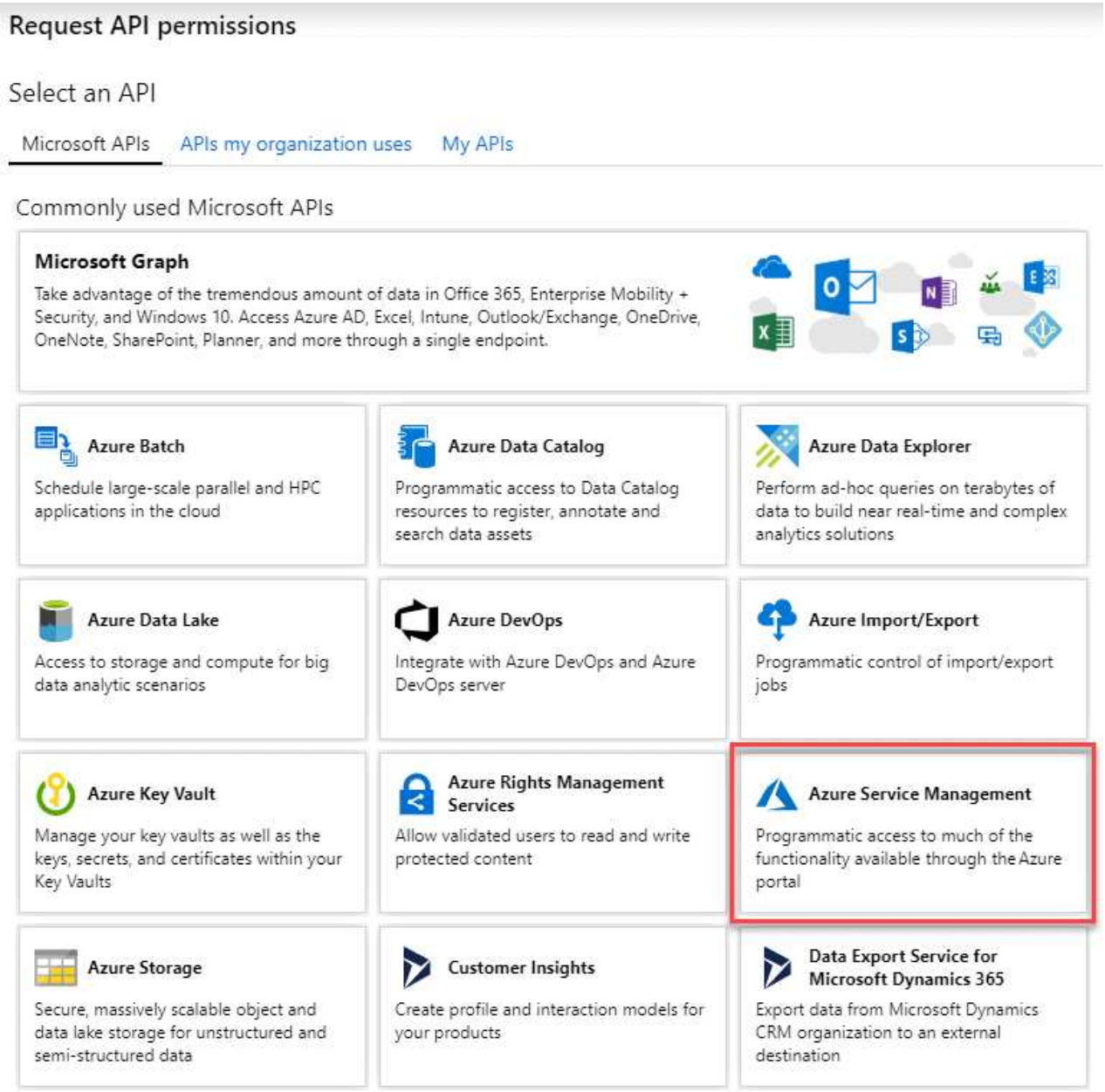
f. 选择*审阅+分配*。

服务主体现在具有部署控制台代理所需的 Azure 权限。

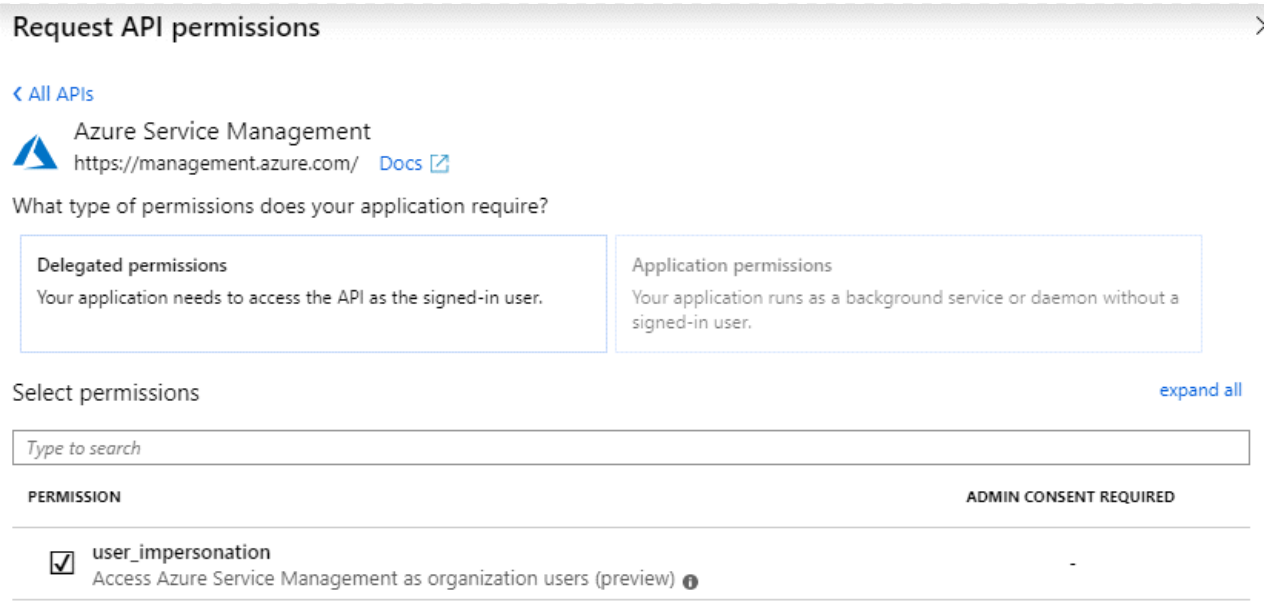
如果您想从多个 Azure 订阅部署Cloud Volumes ONTAP ，则必须将服务主体绑定到每个订阅。在NetApp Console中，您可以选择部署Cloud Volumes ONTAP时要使用的订阅。

添加 **Windows Azure** 服务管理 **API** 权限

1. 在*Microsoft Entra ID*服务中，选择*App Registrations*并选择应用程序。
2. 选择*API 权限 > 添加权限*。
3. 在“Microsoft API”下，选择“Azure 服务管理”。

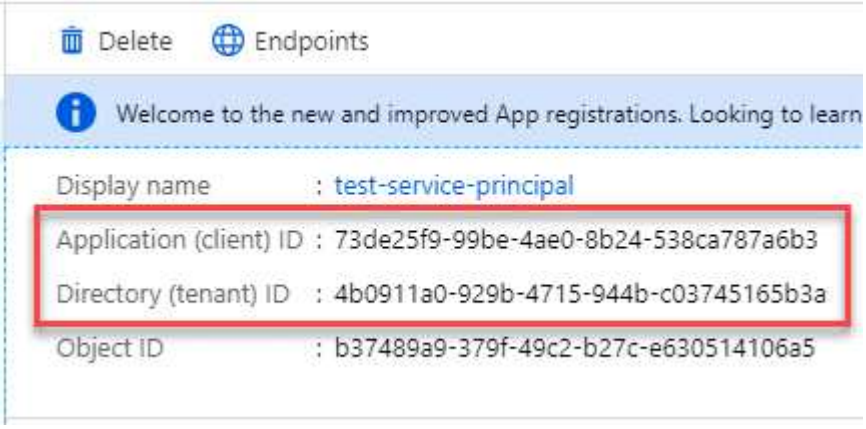


4. 选择*以组织用户身份访问 Azure 服务管理*，然后选择*添加权限*。



获取应用程序的应用程序**ID**和目录**ID**

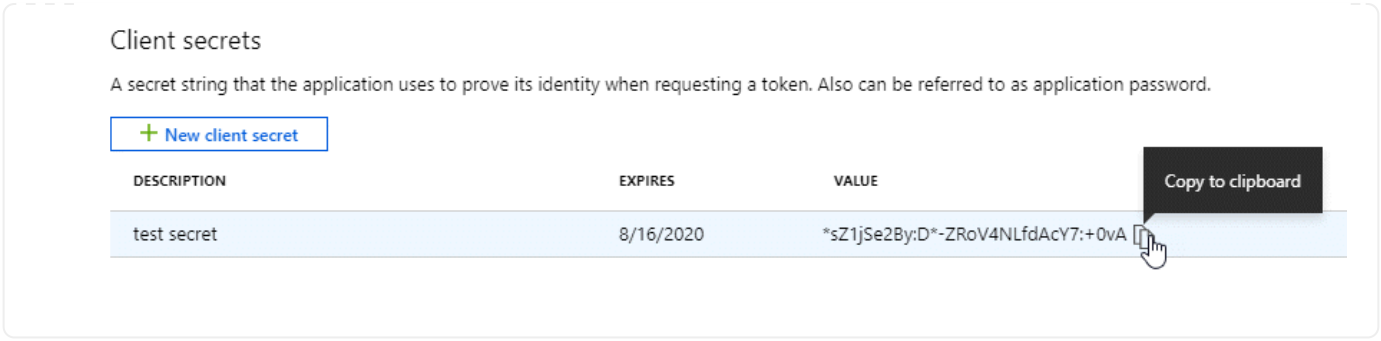
1. 在*Microsoft Entra ID*服务中，选择*App Registrations*并选择应用程序。
2. 复制*应用程序（客户端）ID*和*目录（租户）ID*。



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

创建客户端机密

1. 开启*Microsoft Entra ID*服务。
2. 选择*应用程序注册*并选择您的应用程序。
3. 选择*证书和机密>新客户端机密*。
4. 提供秘密的描述和持续时间。
5. 选择“添加”。
6. 复制客户端机密的值。



手动安装控制台代理

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

安装 **Podman** 或 **Docker Engine**

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

- Red Hat Enterprise Linux 8 和 9 需要 Podman。

  查看支持的 Podman 版本 。

- Ubuntu 需要 Docker 引擎。

  查看支持的 Docker Engine 版本 。

示例 **4.** 步骤

Podman

按照以下步骤安装和配置 Podman：

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

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

步骤

1. 如果主机上安装了 podman-docker 包，请将其删除。

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

2. 安装 Podman。

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

   a. 对于 Red Hat Enterprise Linux 9.6：

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

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

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

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

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

   c. 对于 Red Hat Enterprise Linux 8：

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

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

3. 启用并启动 podman.socket 服务。

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

4. 安装 python3。

```
sudo dnf install python3
```

5. 如果您的系统上还没有 EPEL 存储库包，请安装它。

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

6. 如果使用 Red Hat Enterprise 9：

   a. 安装EPEL存储库软件包。

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

   +

   a. 安装 podman-compose 包 1.5.0。

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

7. 如果使用的是 Red Hat Enterprise Linux 8：

   a. 安装EPEL存储库软件包。

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

   b. 安装 podman-compose 包 1.0.6。

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

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

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

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

```
podman info | grep networkBackend
```

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

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

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

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

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

v. 重新启动 podman。

```
systemctl restart podman
```

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

```
podman info | grep networkBackend
```

Docker 引擎

按照 Docker 的文档安装 Docker Engine。

步骤

1. "查看 Docker 的安装说明"

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

2. 验证 Docker 是否已启用并正在运行。

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

手动安装控制台代理

在本地现有 Linux 主机上下载并安装控制台代理软件。

开始之前

您应该具有以下内容：

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

  您可以选择在安装后配置代理服务器，但这样做需要重新启动控制台代理。

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

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

关于此任务

安装后，如果有新版本可用，控制台代理会自动更新。

步骤

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

   ```
   unset http_proxy
   unset https_proxy
   ```

   如果不删除这些系统变量，安装将失败。

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

     选择下载代理安装程序文件或文件的 URL。

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

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

   其中 <version> 是您下载的控制台代理的版本。

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

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

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

如果要配置透明代理，可以在安装完成后进行配置。 "了解代理维护控制台"

+

以下是使用 CA 签名证书配置显式代理服务器的示例：

+

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

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

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

+ 注意以下事项：

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

+ 例如：

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

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

   a. 通过 SSH 连接到控制台代理虚拟机。

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

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

      例如：

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

   a. 重新启动控制台代理虚拟机。

下一步是什么?

您需要在NetApp Console中注册控制台代理。

使用**NetApp Console**注册控制台代理

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

步骤

1. 打开 Web 浏览器并输入控制台代理主机 URL：

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

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

      当控制台代理安装在本地时，不支持限制模式。

   d. 选择*让我们开始吧*。

向**NetApp Console**提供云提供商凭据

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

AWS

开始之前

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

步骤

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

您现在可以前往 "NetApp Console"开始使用控制台代理。

Azure

开始之前

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

步骤

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

结果

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

使用 **VCenter** 在本地安装控制台代理

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

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

准备安装控制台代理

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

查看控制台代理主机要求

在安装控制台代理之前，请确保您的主机满足安装要求。

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

在 vCenter 环境中安装代理，而不是直接在 ESXi 主机上安装。

为控制台代理设置网络访问

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

连接到目标网络

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

出站互联网访问

部署控制台代理的网络位置必须具有出站互联网连接才能联系特定端点。

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

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

"为NetApp控制台准备网络" 。

从控制台代理联系的端点

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

下面列出的端点都是 CNAME 条目。

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

AWS

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

从控制台代理联系的端点

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

下面列出的端点都是 CNAME 条目。

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

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

Azure

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

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

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

代理服务器

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

- IP 地址
- 凭据
- HTTPS 证书

端口

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

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

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

启用 **NTP**

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

为 **AWS** 或 **Azure** 创建控制台代理云权限

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

以便在安装控制台代理后将凭据添加到控制台代理。

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

AWS

对于本地控制台代理，通过添加 IAM 用户访问密钥提供 AWS 权限。

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

步骤

1. 登录 AWS 控制台并导航到 IAM 服务。
2. 创建策略：

   a. 选择“策略”>“创建策略”。

   b. 选择 **JSON** 并复制并粘贴内容"控制台代理的 IAM 策略"。

   c. 完成剩余步骤以创建策略。

      根据您计划使用的NetApp数据服务，您可能需要创建第二个策略。

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

3. 将策略附加到 IAM 用户。

   - "AWS 文档：创建 IAM 角色"
   - "AWS 文档：添加和删除 IAM 策略"

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

结果

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

Azure

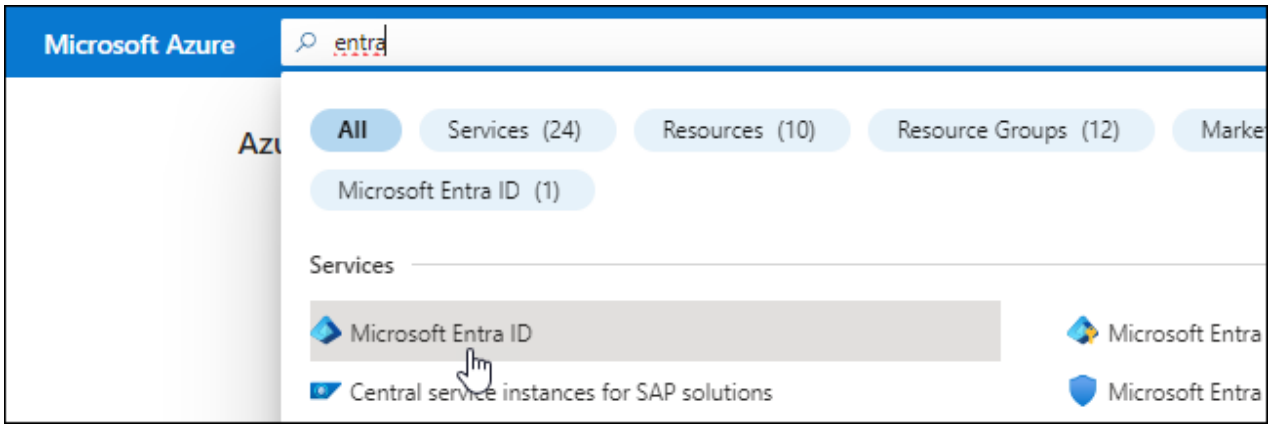
当控制台代理安装在本地时，您需要通过在 Microsoft Entra ID 中设置服务主体并获取控制台代理所需的 Azure 凭据来授予控制台代理 Azure 权限。

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

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

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

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



3. 在菜单中，选择*应用程序注册*。
4. 选择*新注册*。
5. 指定有关应用程序的详细信息：
   - 名称：输入应用程序的名称。
   - 帐户类型：选择帐户类型（任何类型都可以与NetApp Console一起使用）。
   - 重定向 **URI**：您可以将此字段留空。
6. 选择*注册*。

   您已创建 AD 应用程序和服务主体。

将应用程序分配给角色

1. 创建自定义角色：

   请注意，您可以使用 Azure 门户、Azure PowerShell、Azure CLI 或 REST API 创建 Azure 自定义角色。以下步骤展示如何使用 Azure CLI 创建角色。如果您希望使用其他方法，请参阅 "Azure 文档"

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

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

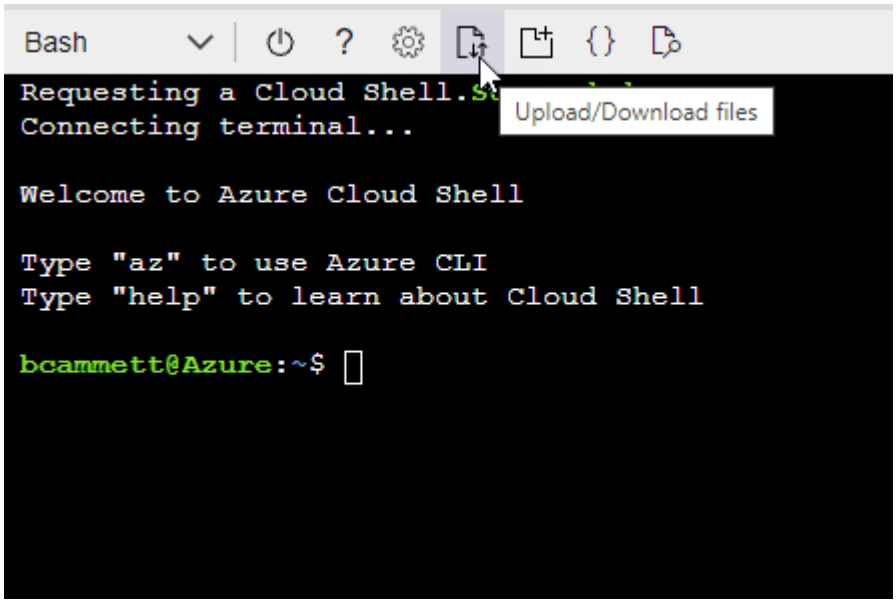
      例子

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

   c. 使用 JSON 文件在 Azure 中创建自定义角色。

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

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



- 使用 Azure CLI 创建自定义角色：

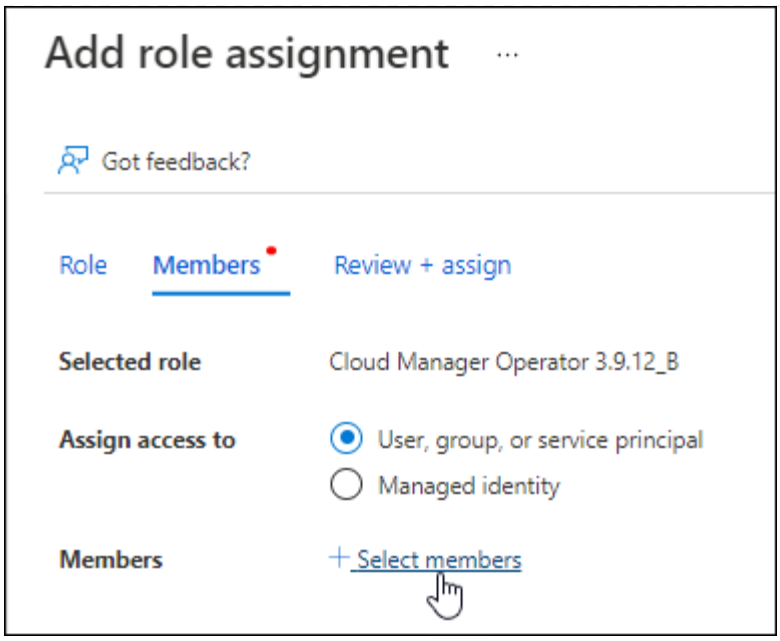
```
az role definition create --role-definition agent_Policy.json
```

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

2. 将应用程序分配给角色：

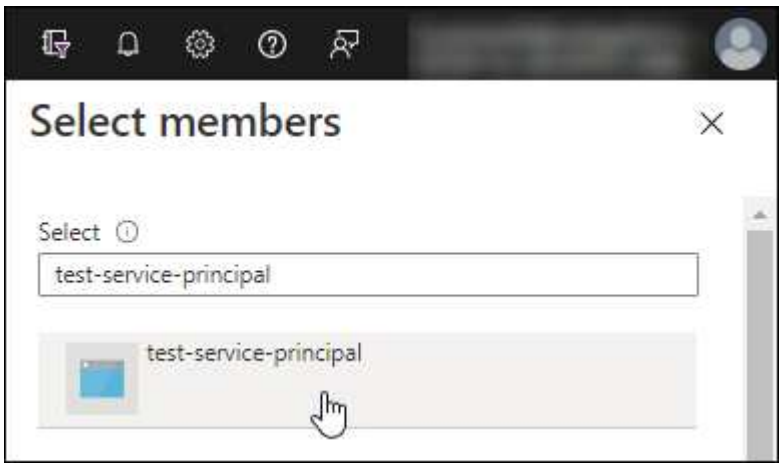
a. 从 Azure 门户打开 **Subscriptions** 服务。
b. 选择订阅。
c. 选择“访问控制 (IAM)”>“添加”>“添加角色分配”。
d. 在*角色*选项卡中，选择*控制台操作员*角色并选择*下一步*。
e. 在“成员”选项卡中，完成以下步骤：

- 保持选中“用户、组或服务主体”。
- 选择*选择成员*。



- 搜索应用程序的名称。

  以下是一个例子：



- 选择应用程序并选择*选择*。
- 选择“下一步”。

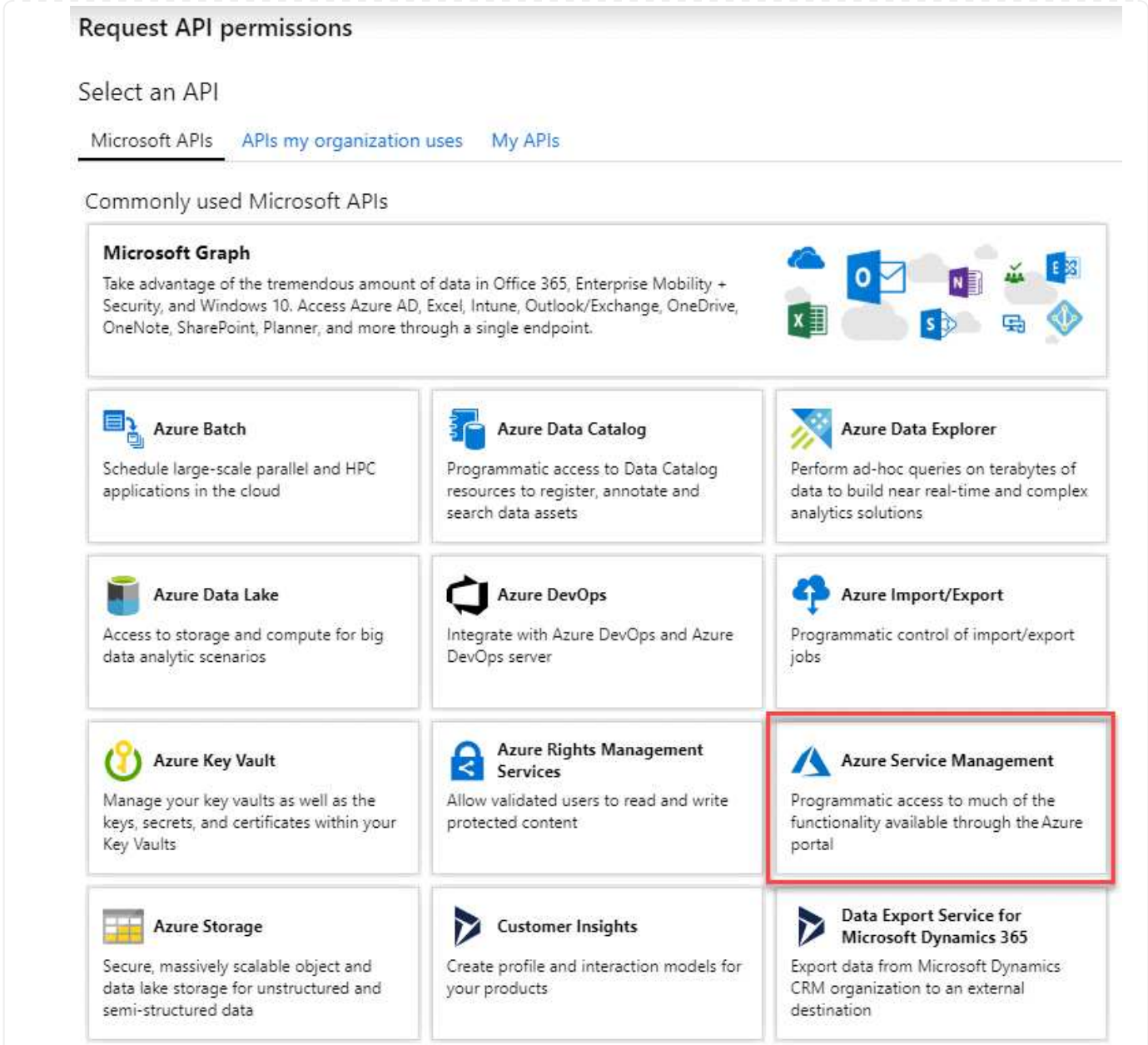
f. 选择*审阅+分配*。

服务主体现在具有部署控制台代理所需的 Azure 权限。

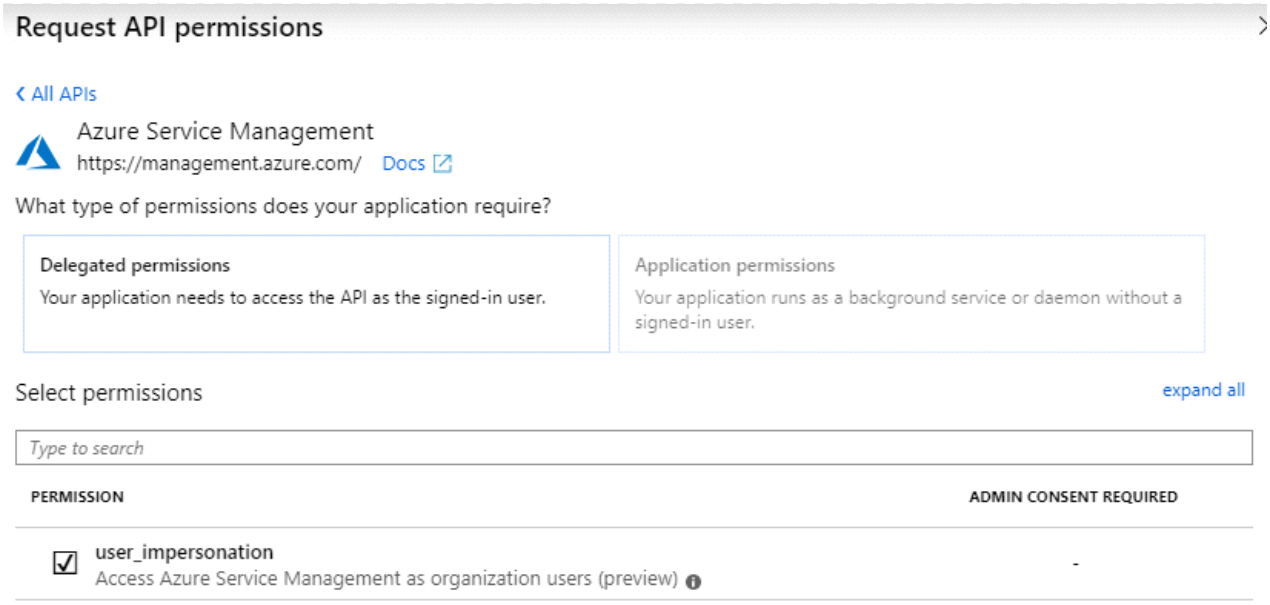
如果您想从多个 Azure 订阅部署Cloud Volumes ONTAP ，则必须将服务主体绑定到每个订阅。在NetApp Console中，您可以选择部署Cloud Volumes ONTAP时要使用的订阅。

添加 **Windows Azure** 服务管理 **API** 权限

1. 在*Microsoft Entra ID*服务中，选择*App Registrations*并选择应用程序。
2. 选择*API 权限 > 添加权限*。
3. 在“Microsoft API”下，选择“Azure 服务管理”。

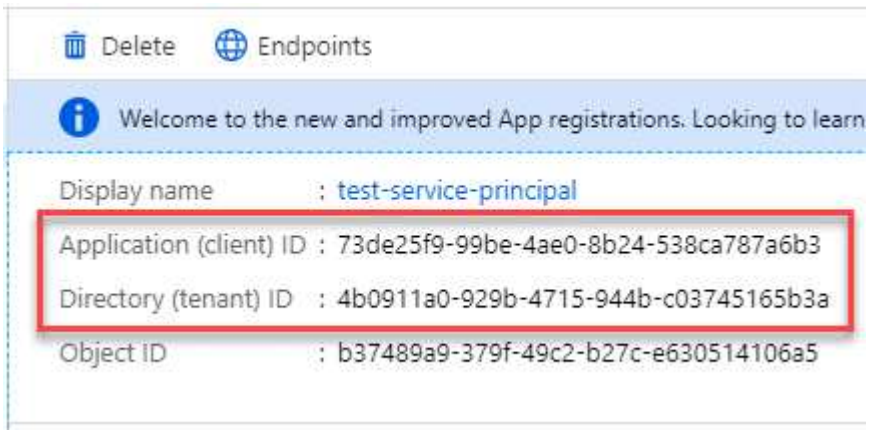


4. 选择*以组织用户身份访问 Azure 服务管理*，然后选择*添加权限*。



获取应用程序的应用程序**ID**和目录**ID**

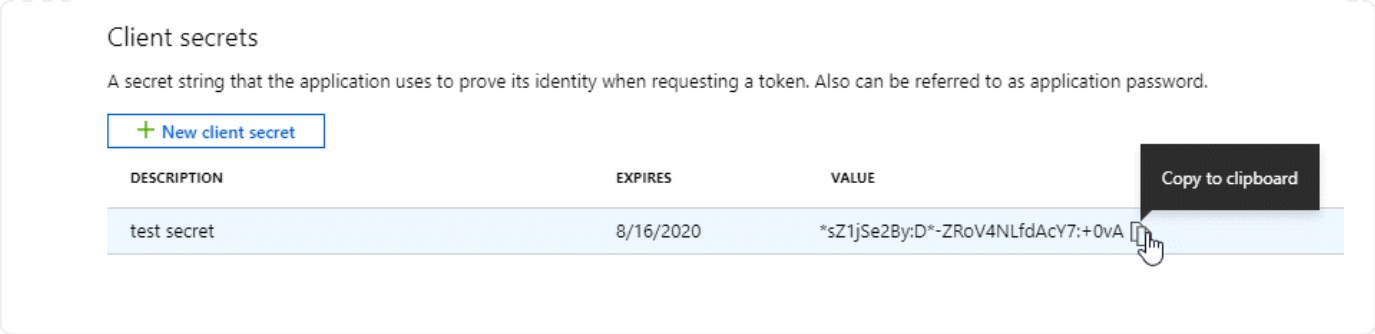
1. 在*Microsoft Entra ID*服务中，选择*App Registrations*并选择应用程序。
2. 复制*应用程序（客户端）ID*和*目录（租户）ID*。



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

创建客户端机密

1. 开启*Microsoft Entra ID*服务。
2. 选择*应用程序注册*并选择您的应用程序。
3. 选择*证书和机密>新客户端机密*。
4. 提供秘密的描述和持续时间。
5. 选择“添加”。
6. 复制客户端机密的值。



在 **VCenter** 环境中安装控制台代理

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

下载 **OVA** 或复制 **URL**

直接从NetApp Console下载 OVA 或复制 OVA URL。

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

在您的 **VCenter** 中部署代理

登录您的 VCenter 环境以部署代理。

步骤

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

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

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

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

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

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

使用**NetApp Console**注册控制台代理

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

步骤

1. 打开 Web 浏览器并输入控制台代理主机 URL：

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

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

      当控制台代理安装在本地时，不支持限制模式。

   d. 选择*让我们开始吧*。

将云提供商凭据添加到控制台

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

AWS

开始之前

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

步骤

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

您现在可以前往 "NetApp Console"开始使用控制台代理。

Azure

开始之前

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

步骤

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

结果

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

本地控制台代理的端口

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

这些入站规则适用于所有NetApp Console部署模式。

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

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*。

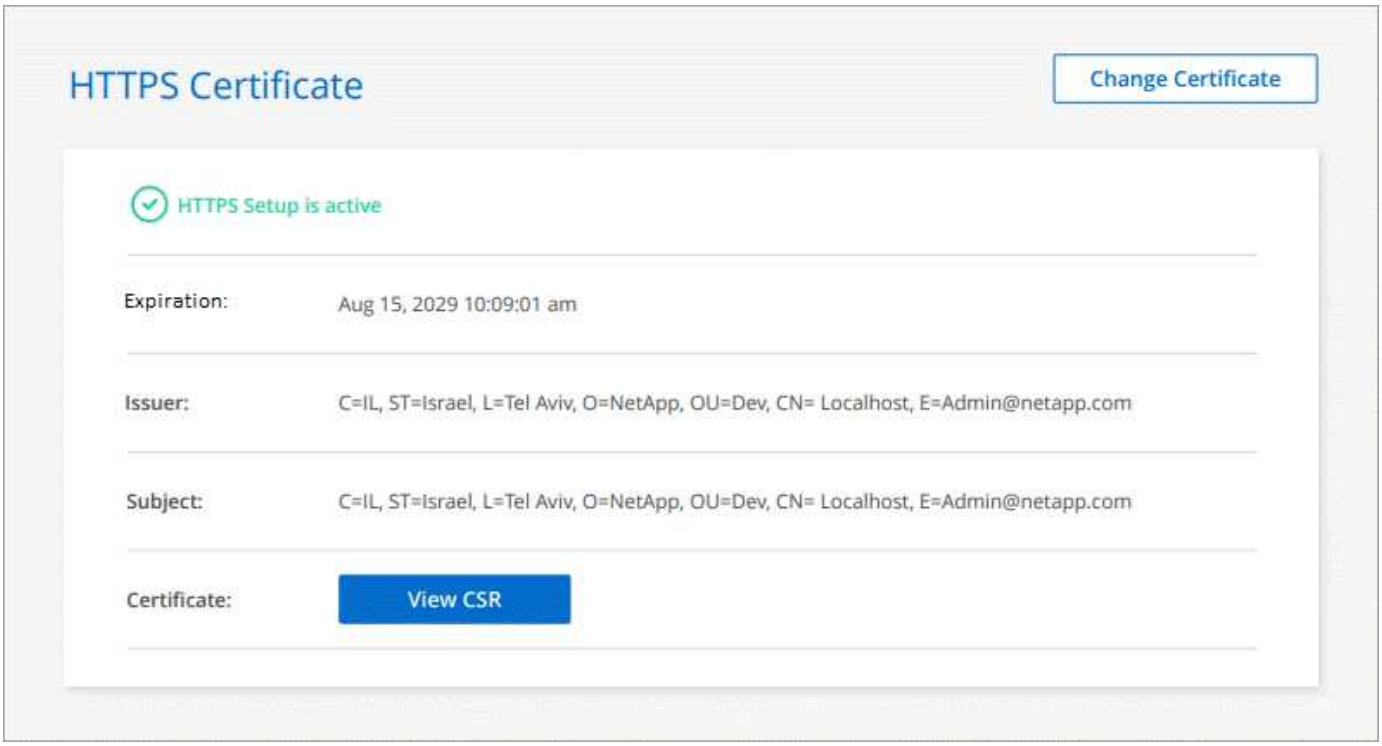
   必须连接控制台代理才能进行编辑。

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 http://address:port或者 https://address:port
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。

错误消息	说明	该怎么办
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。

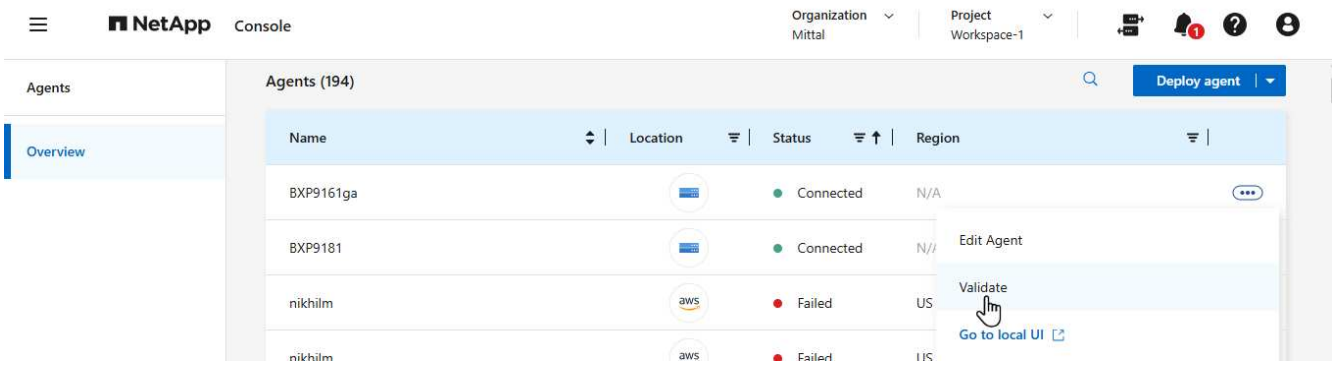
您还可以使用代理维护控制台运行配置检查。"了解更多关于使用 config-checker validate 命令的信息。"

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

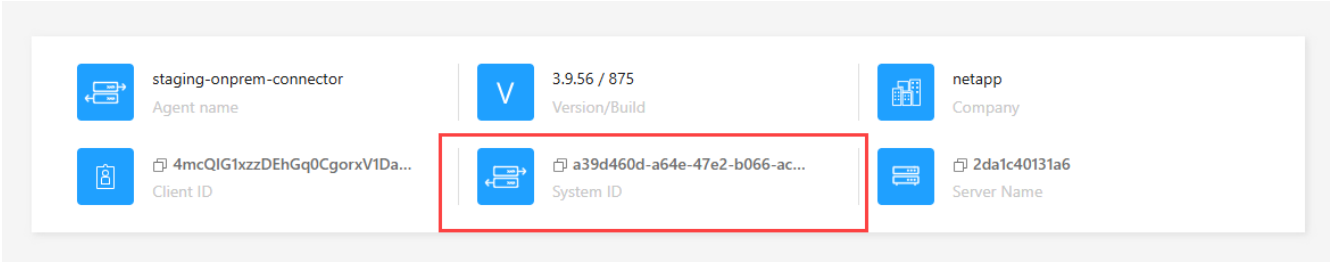
为了帮助您入门，您可能需要控制台代理的系统 ID。该 ID 通常用于许可和故障排除目的。

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。

由于负载平衡， 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

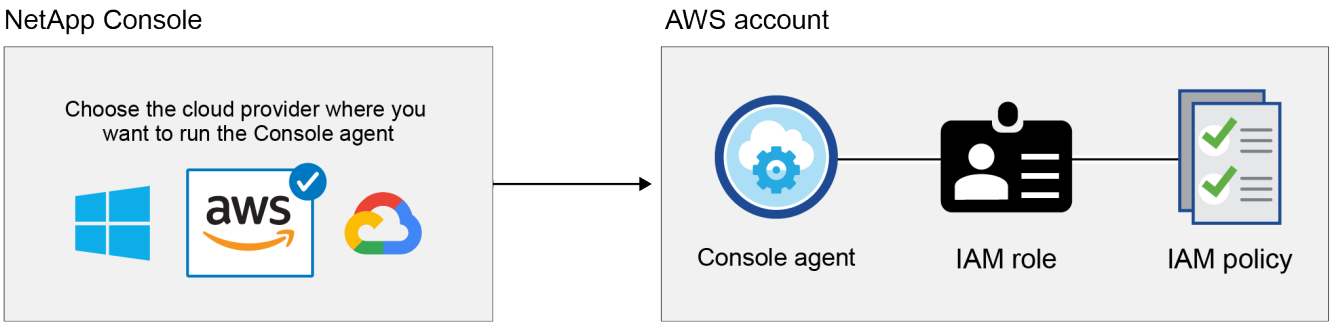
了解NetApp Console中的 AWS 凭证和权限

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。

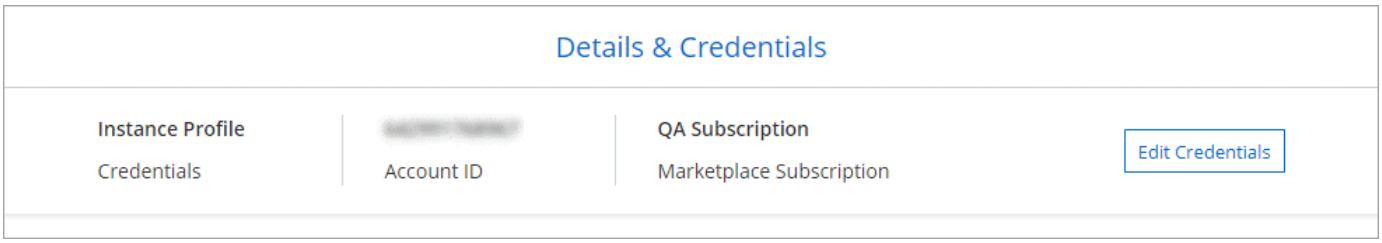
初始 AWS 凭证

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

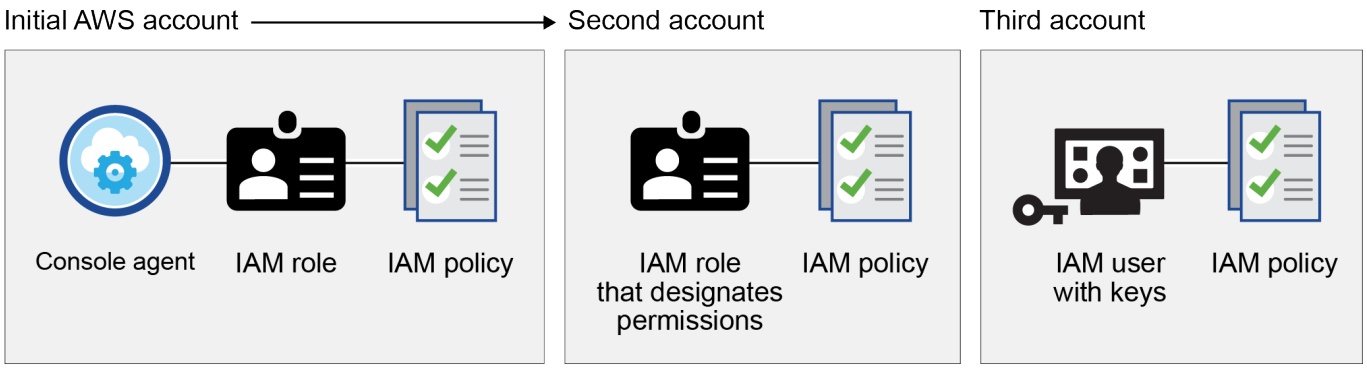
在以下情况下，您可能会向控制台添加其他 AWS 凭证：

- 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。

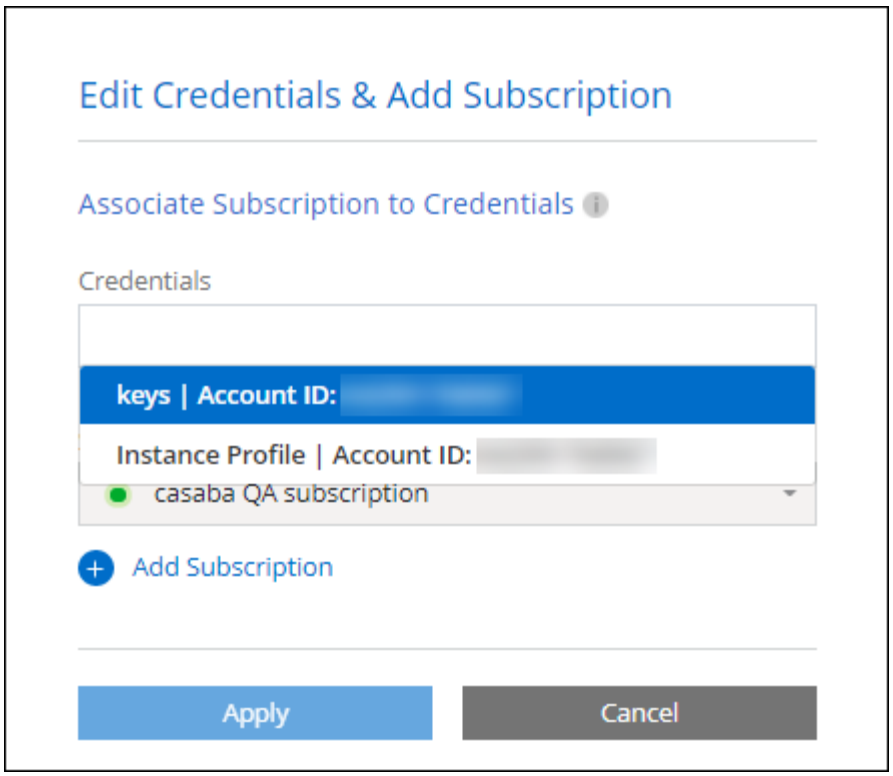
添加 **AWS** 凭证以将控制台代理与另一个 **AWS** 账户一起使用

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：



"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。您可以提供另一个账户中的 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”。

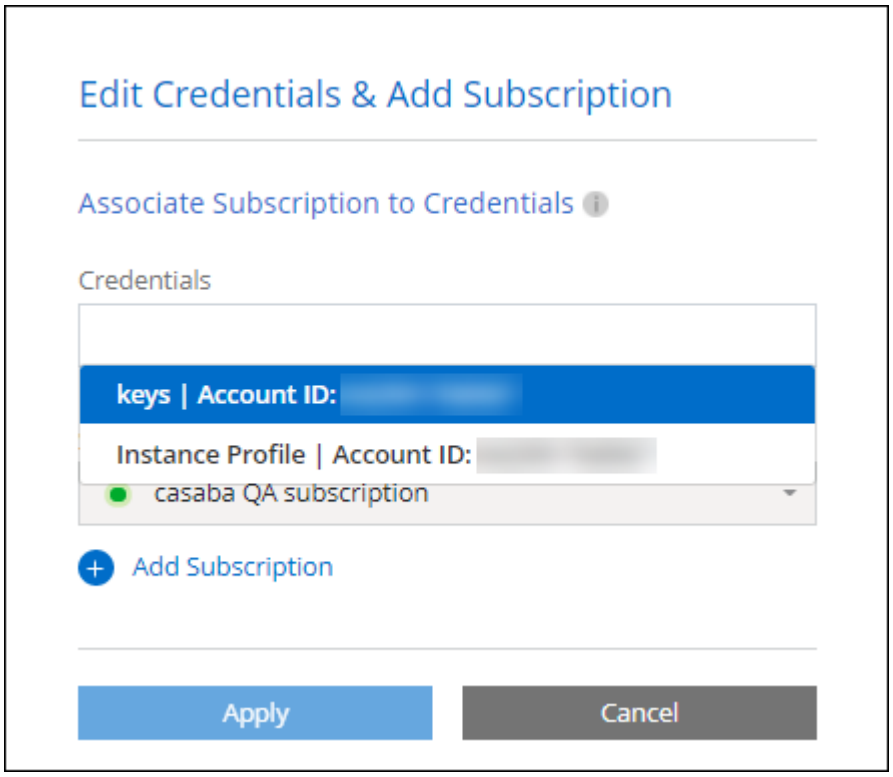
3. 在*组织凭据*页面上，选择*添加凭据*并按照向导中的步骤进行操作。
   a. 凭证位置：选择*Amazon Web Services > 代理*。
   b. 定义凭证：提供受信任的 IAM 角色的 ARN（Amazon 资源名称），或输入 AWS 访问密钥和密钥。
   c. 市场订阅：通过立即订阅或选择现有订阅将市场订阅与这些凭证关联。

      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。



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

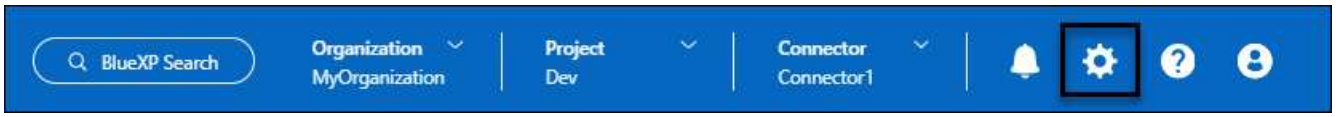
为 IAM 角色提供所需的权限后，将角色 ARN 添加到控制台。

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。

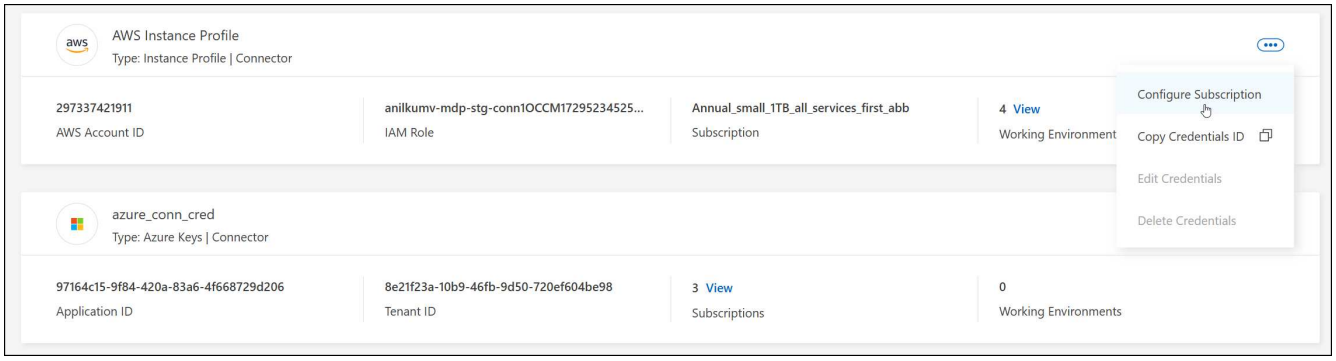
开始之前

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。

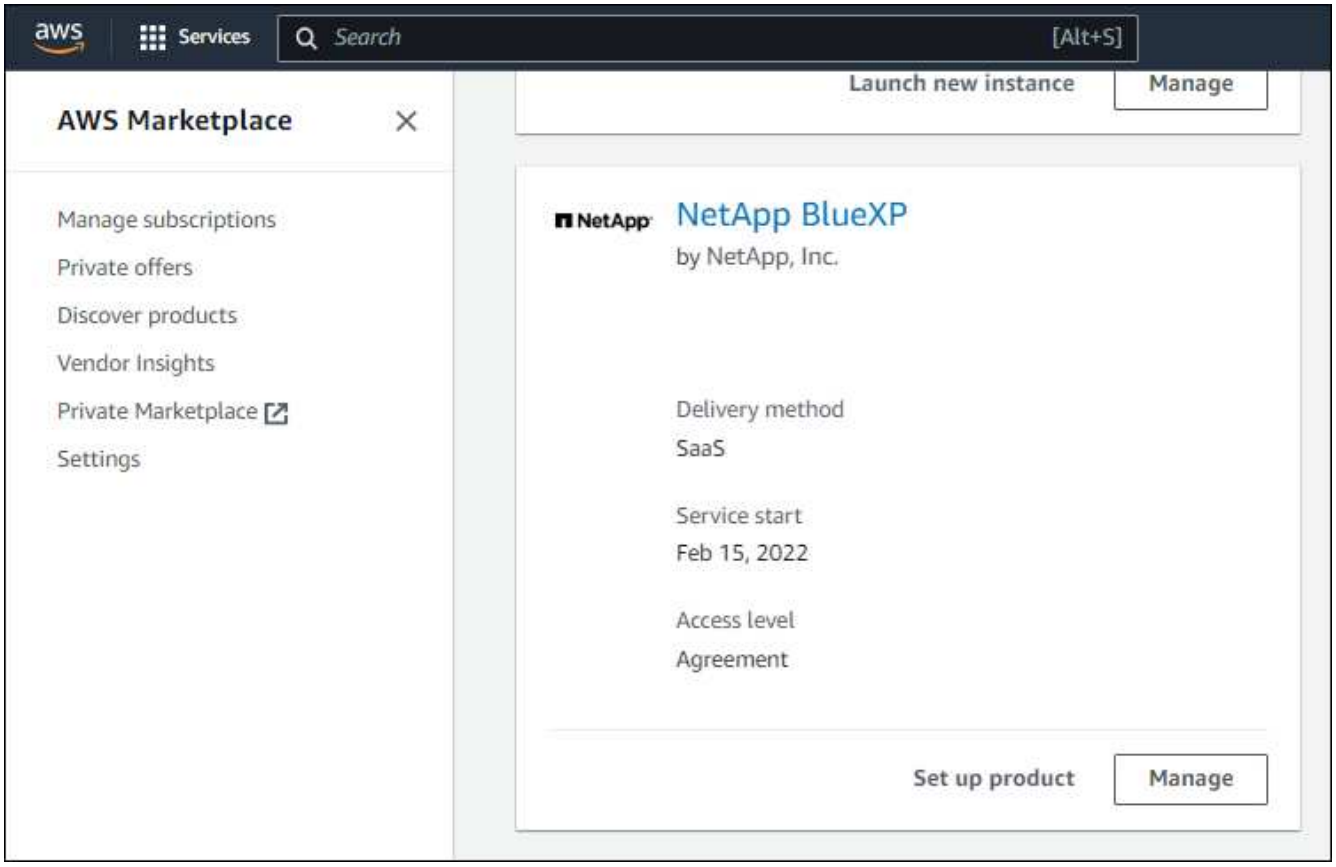
- "了解控制台部署模式"
- "了解控制台身份和访问管理"

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。

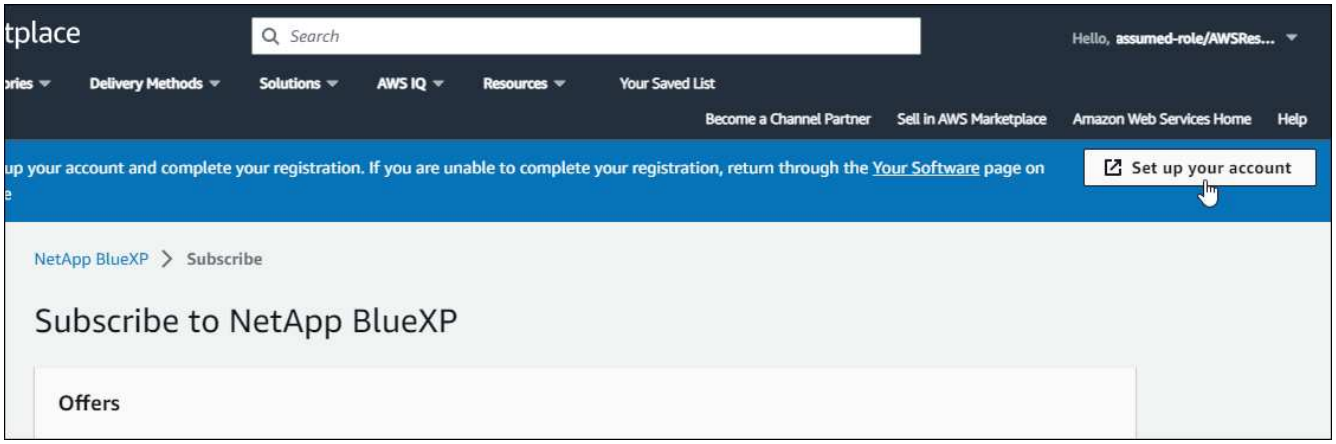
   您只会看到与您当前正在查看的组织或帐户相关的订阅。如果您没有看到您的订阅，请继续执行以下步骤。
2. 登录 AWS 控制台并导航到 **AWS Marketplace** 订阅。
3. 查找订阅。



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。

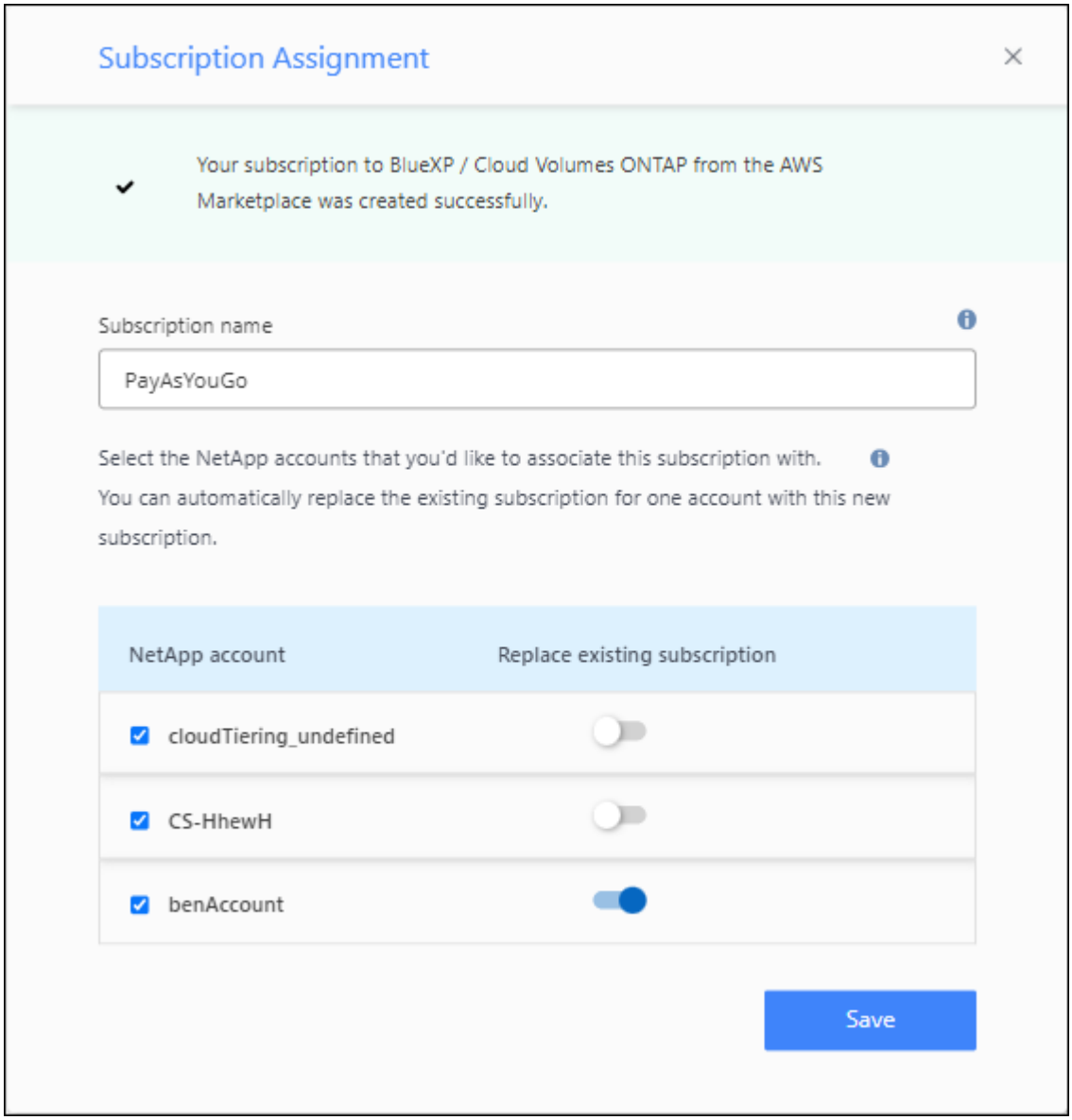
6. 从“订阅分配”页面：

   ◦ 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。

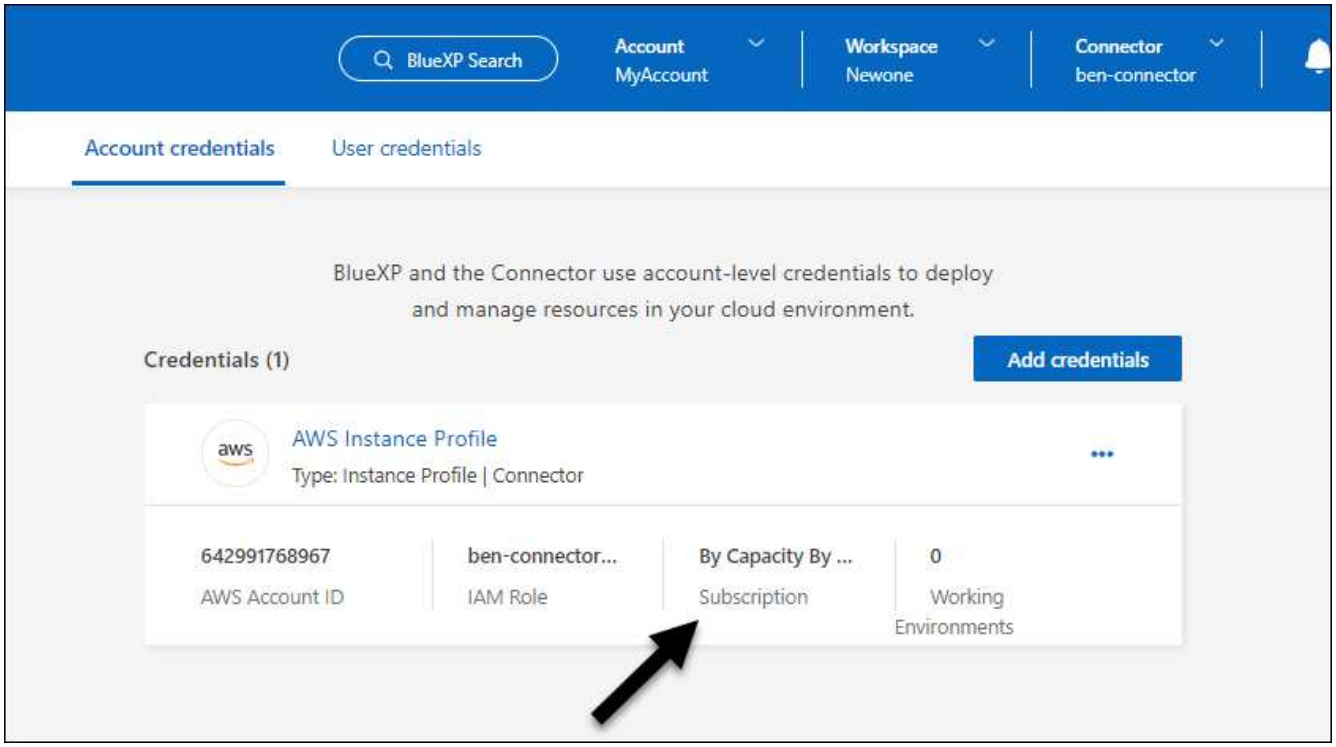
控制台将用这个新订阅替换组织或帐户中所有凭据的现有订阅。如果一组凭证从未与订阅关联，那么这个新订阅将不会与这些凭证关联。

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。



7. 确认订阅与您的组织相关联。
   a. 从导航菜单中，选择*管理>许可证和订阅*。
   b. 选择*订阅*。
   c. 验证您的订阅是否出现。
8. 确认订阅与您的 AWS 凭证相关联。
   a. 选择“管理 > 凭证”。
   b. 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。



编辑凭据

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实例的凭据。

步骤

1. 选择“管理 > 凭证”。
2. 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*。
3. 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。

您无法删除与控制台代理关联的实例配置文件的凭据。

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

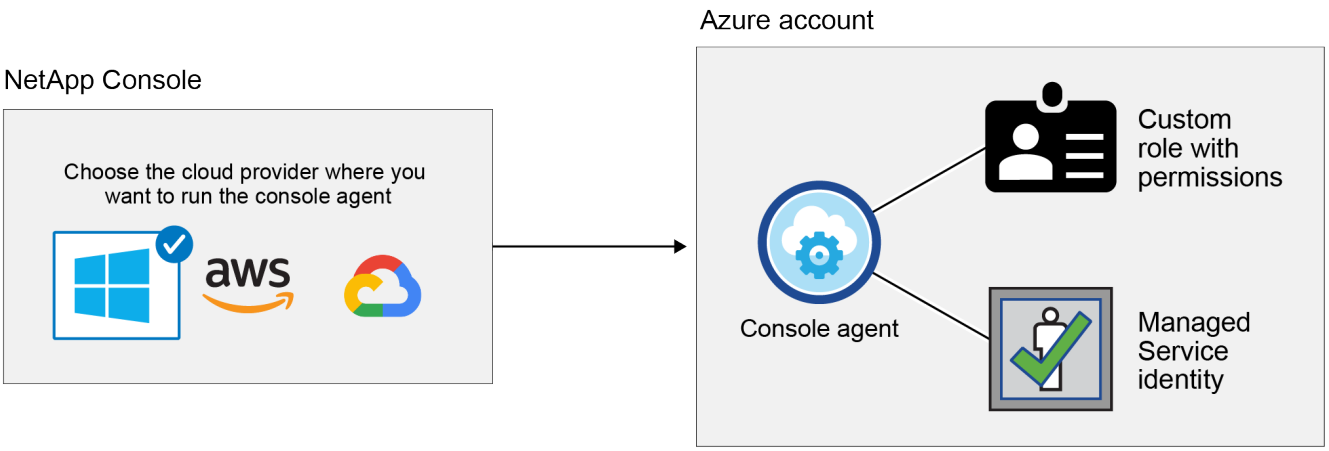
了解NetApp Console中的 Azure 凭据和权限

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。

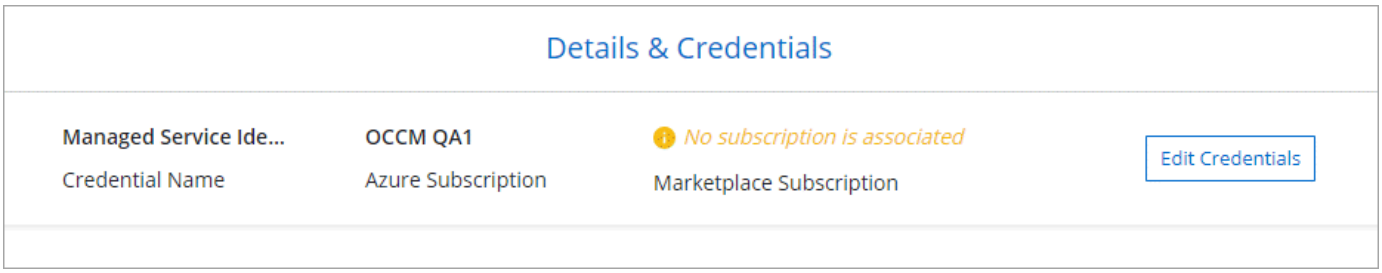
初始 Azure 凭据

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：



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。

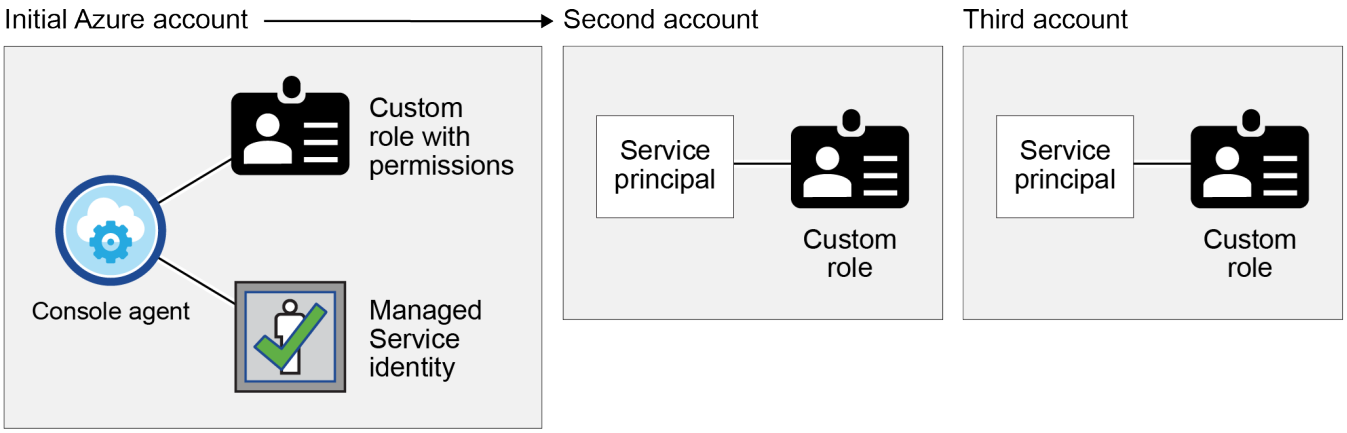
托管标识的其他 Azure 订阅

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

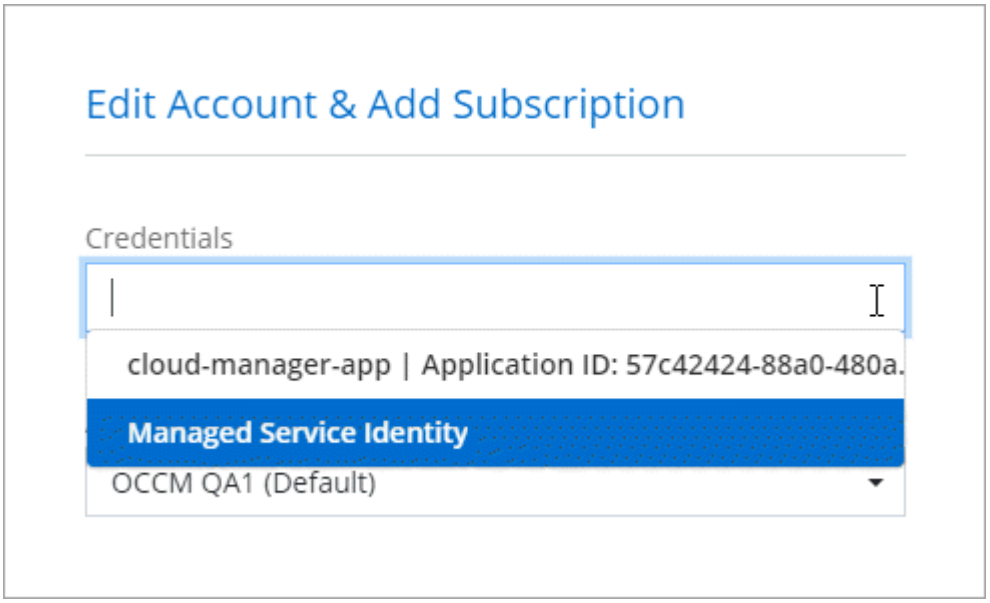
如果要在控制台中使用不同的 Azure 凭据，则必须通过以下方式授予所需的权限"在 Microsoft Entra ID 中创建和

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

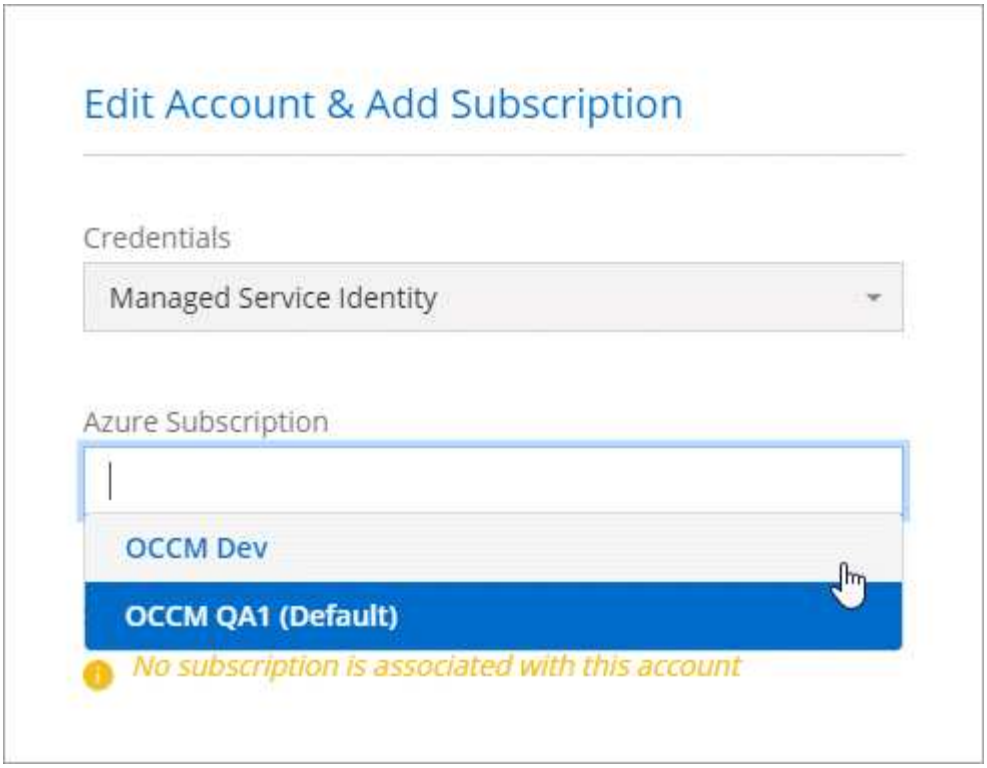
1. 登录 Azure 门户。
2. 打开*订阅*服务，然后选择要部署Cloud Volumes ONTAP 的订阅。
3. 选择*访问控制（IAM）*。
   a. 选择 添加 > 添加角色分配，然后添加权限：
      - 选择*控制台操作员*角色。

        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" 。

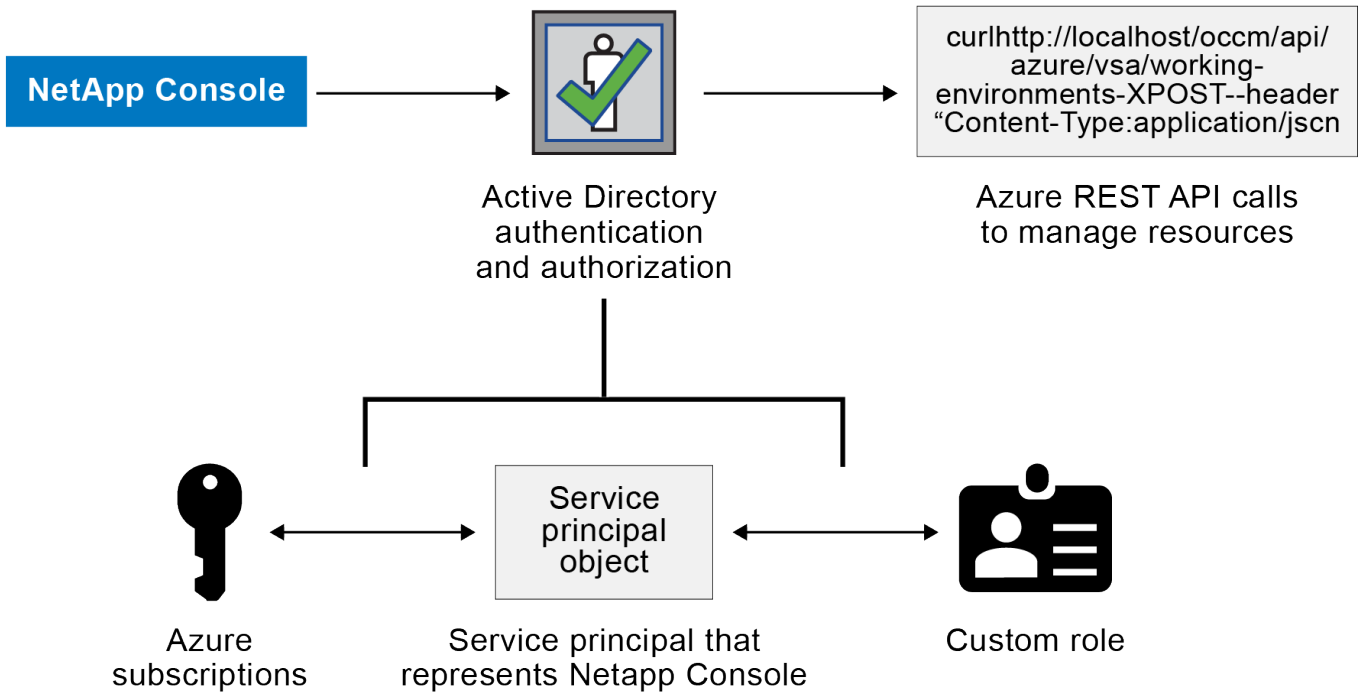
如果您想使用不同的 Azure 凭据部署Cloud Volumes ONTAP ，则必须通过在 Microsoft Entra ID 中为每个 Azure 帐户创建和设置服务主体来授予所需的权限。然后，您可以将新凭据添加到控制台。

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

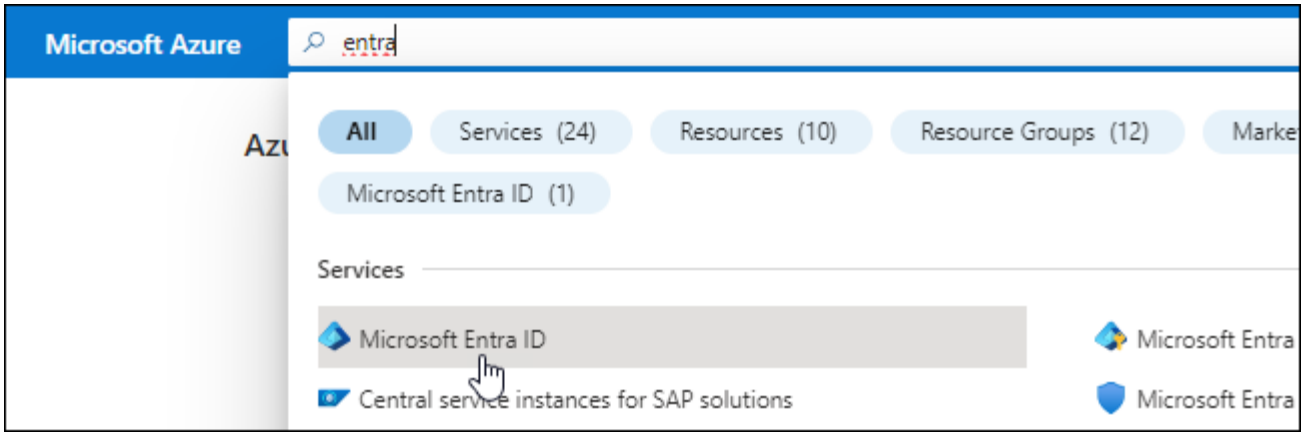
创建控制台可用于基于角色的访问控制的 Microsoft Entra 应用程序和服务主体。

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。

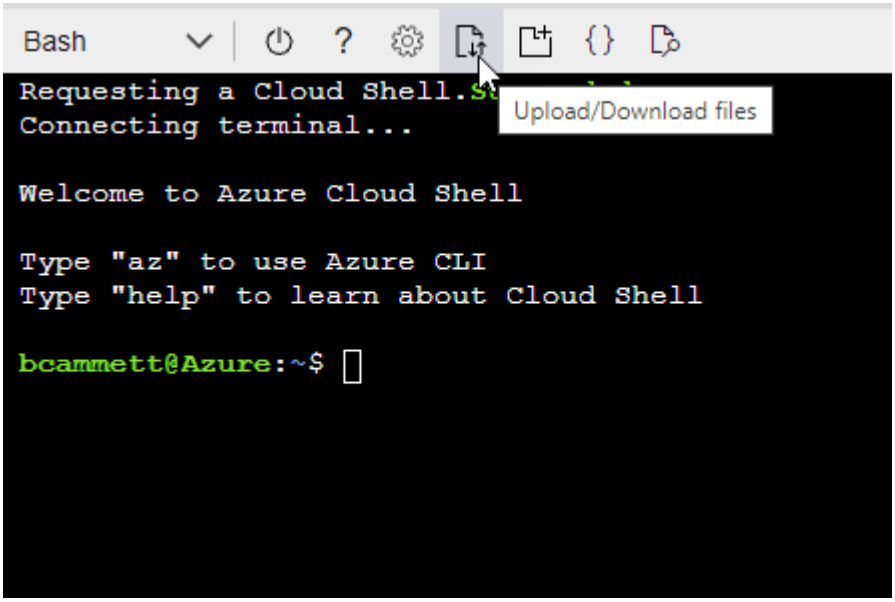
      例子

```
"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。

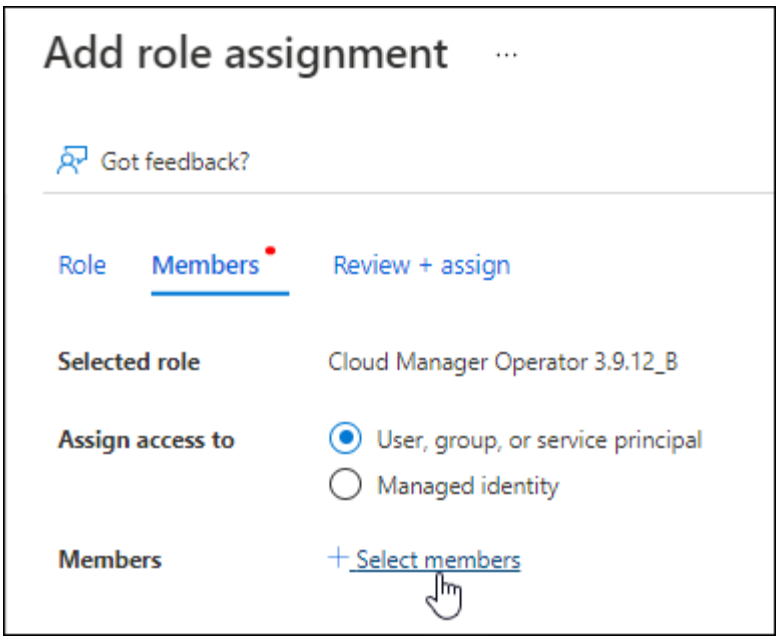
b. 选择订阅。

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*。

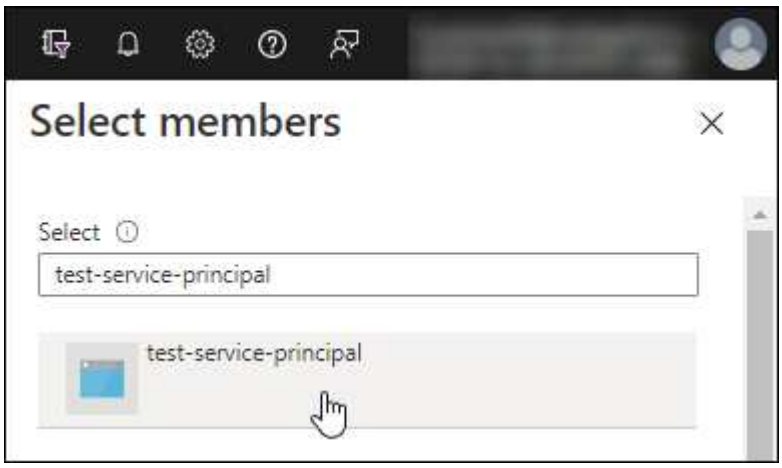
e. 在“成员”选项卡中，完成以下步骤：

- 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。

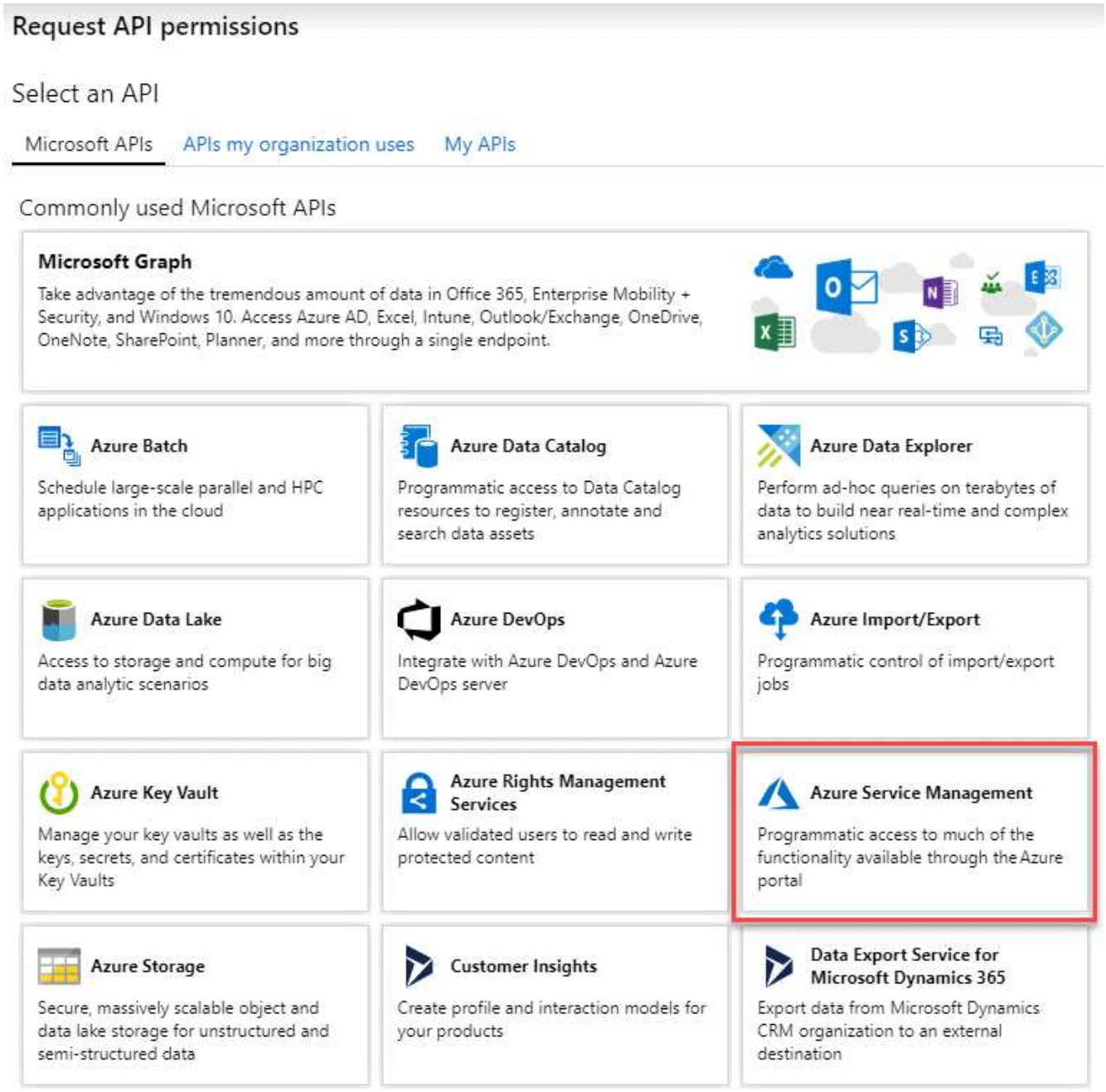
如果您想从多个 Azure 订阅部署Cloud Volumes ONTAP ，则必须将服务主体绑定到每个订阅。在NetApp Console中，您可以选择部署Cloud Volumes ONTAP时要使用的订阅。

添加 **Windows Azure** 服务管理 **API** 权限

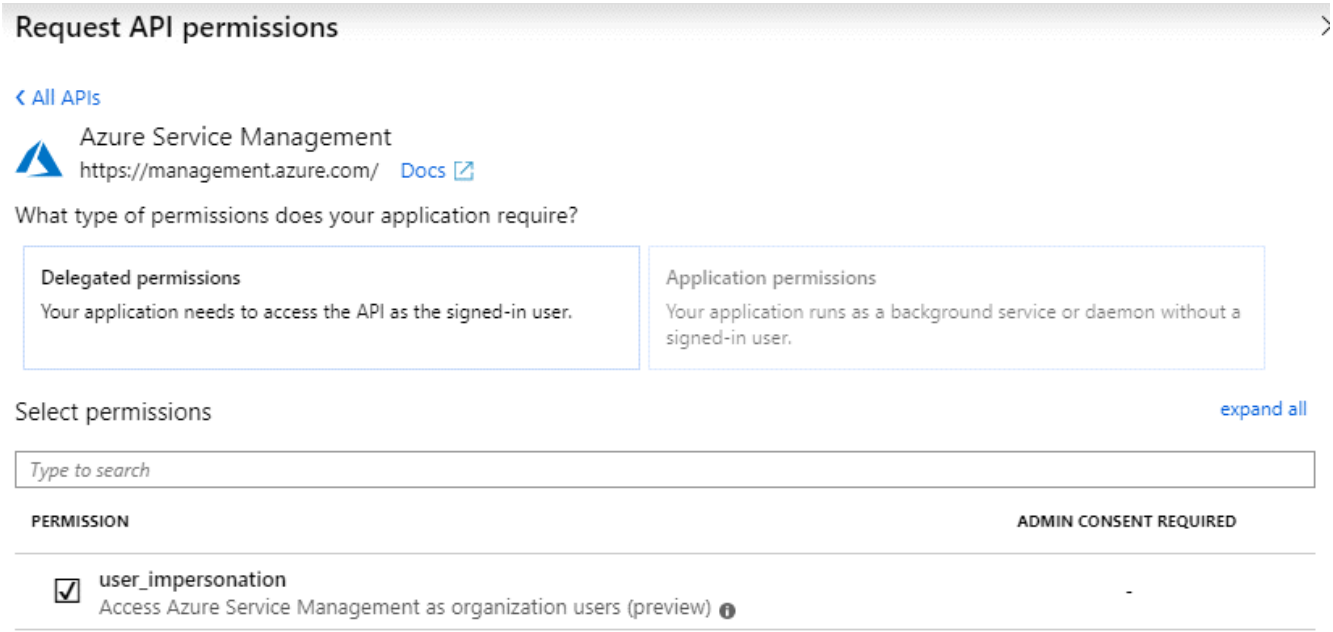
您必须为服务主体分配“Windows Azure 服务管理 API”权限。

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”。



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

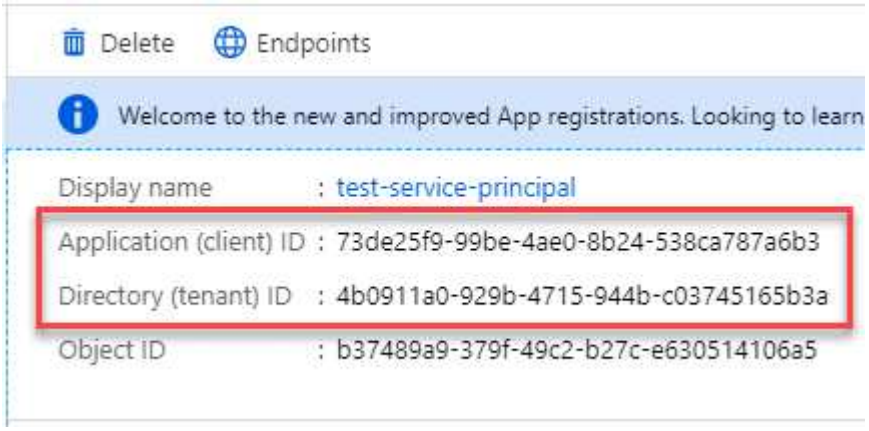


获取应用程序**ID**和目录**ID**

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。

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

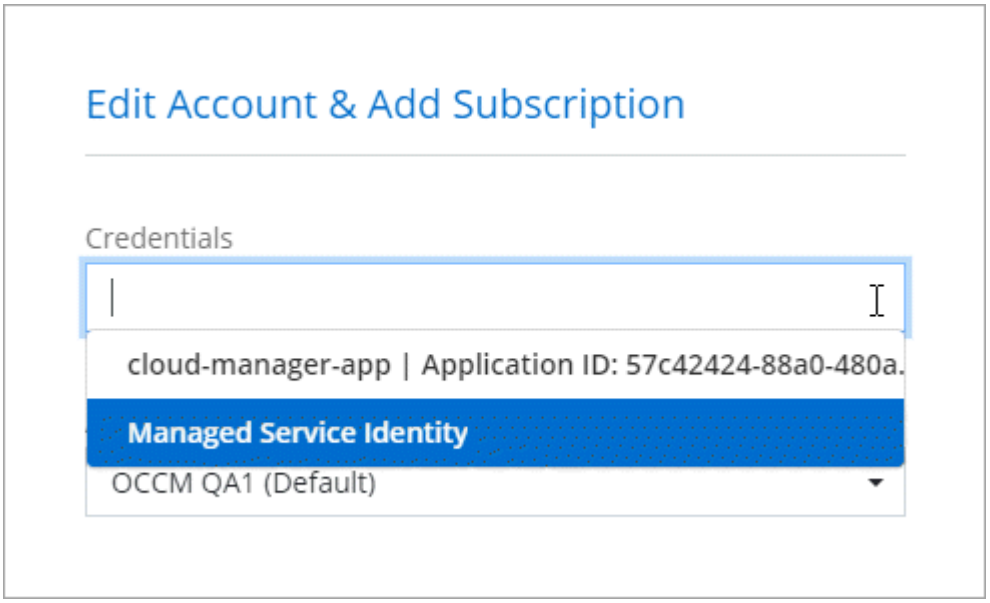
您需要先创建控制台代理，然后才能更改控制台设置。"了解如何创建控制台代理" 。

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、编辑凭据和删除凭据来管理已添加到控制台的 Azure 凭据。

将 **Azure** 市场订阅关联到凭据

将 Azure 凭据添加到控制台后，您可以将 Azure 市场订阅与这些凭据关联。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。

在将凭据添加到控制台后，可以在两种情况下关联 Azure 市场订阅：

- 当您最初将凭据添加到控制台时，您没有关联订阅。
- 您想要更改与 Azure 凭据关联的 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. 要将凭据与新订阅关联，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。

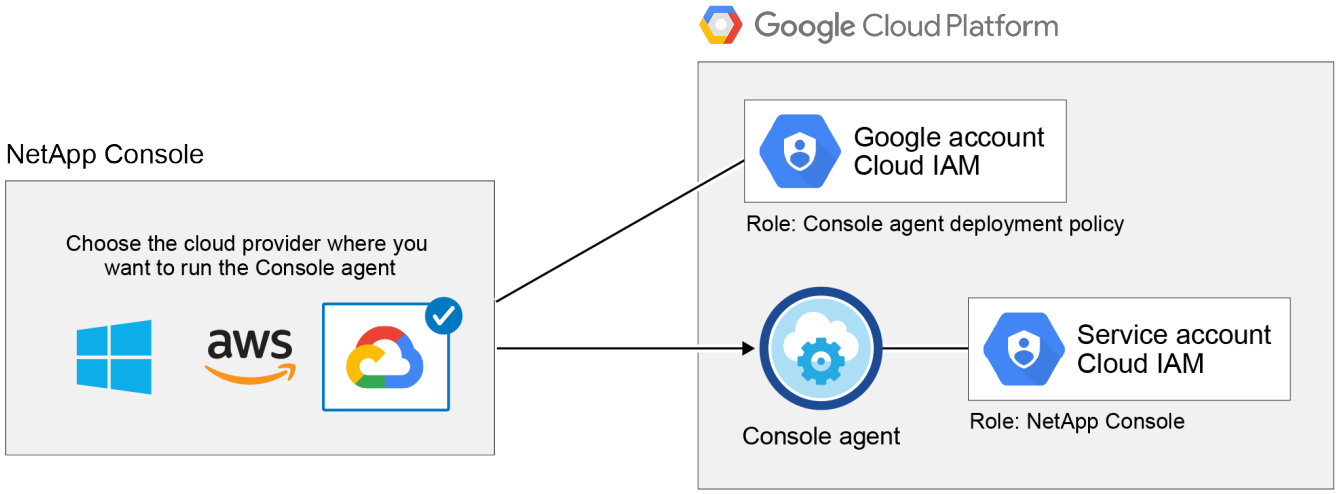
NetApp Console的项目和权限

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 **NetApp Console** 的 **Google Cloud** 凭据和订阅

您可以通过关联市场订阅和疑难解答订阅流程来管理与 Console 代理 VM 实例关联的 Google Cloud 凭据。这两项任务都可确保您可以使用市场订阅来支付数据服务费用。

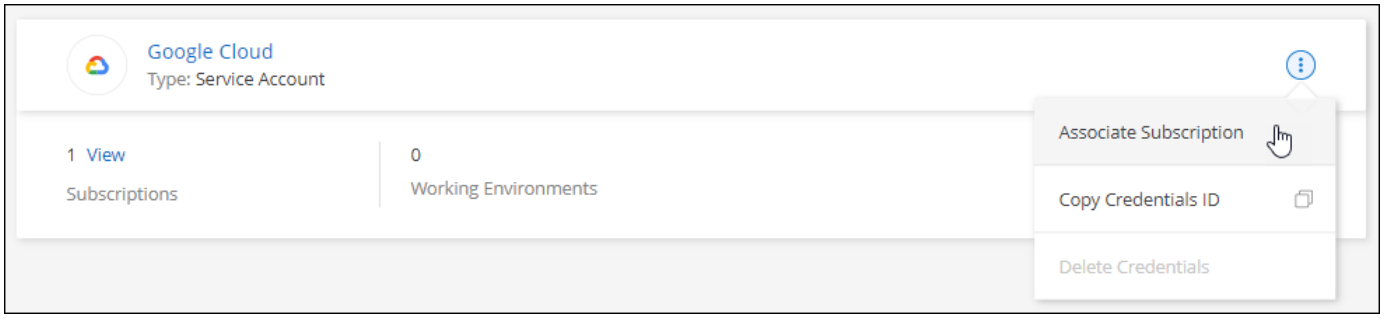
将 **Marketplace** 订阅与 **Google Cloud** 凭据关联

在 Google Cloud 中部署 Console 代理时，Console 将创建与 Console 代理 VM 实例关联的默认凭据集。您可以随时更改与这些凭据相关联的 Google Cloud Marketplace 订阅。此订阅使您能够创建即用即付的 Cloud Volumes ONTAP 系统，并使用其他数据服务。

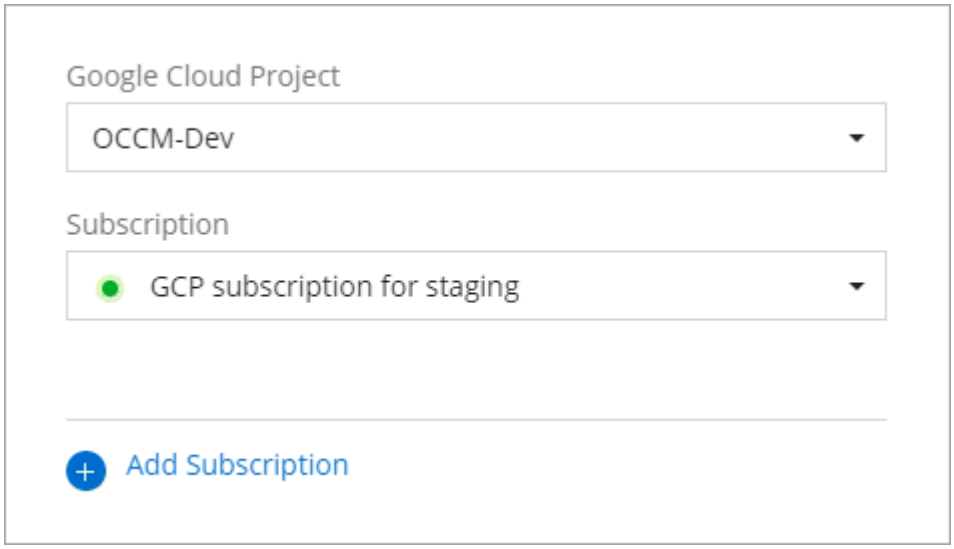
用新的订阅替换当前的市场订阅会更改任何现有Cloud Volumes ONTAP系统和所有新系统的市场订阅。

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*。



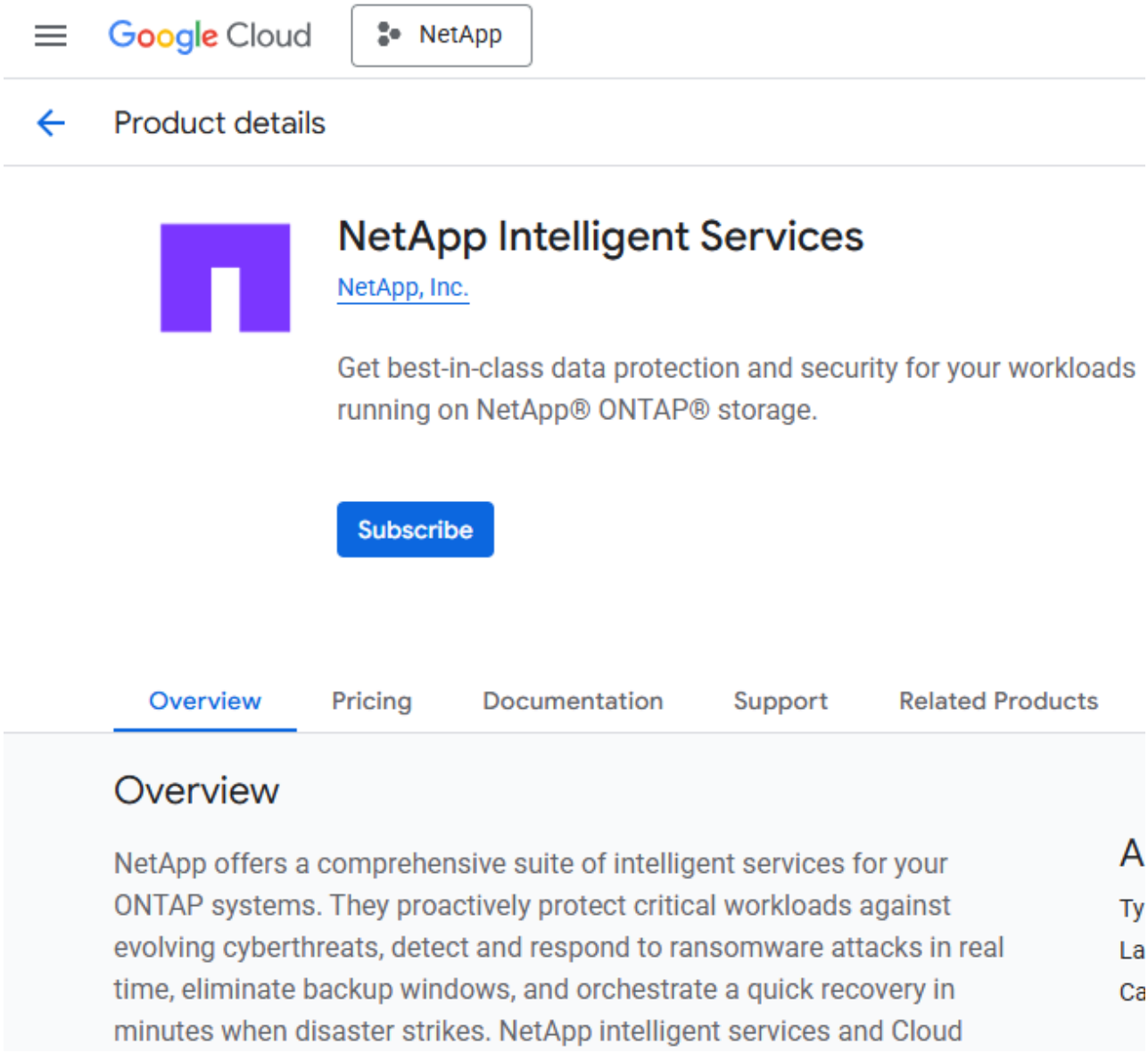
1. 要使用选定的凭据配置现有订阅，请从下拉列表中选择一个 Google Cloud 项目和订阅，然后选择*配置*。



2. 如果您还没有订阅，请选择*添加订阅>继续*并按照 Google Cloud Marketplace 中的步骤操作。

在完成以下步骤之前，请确保您在 Google Cloud 帐户中同时拥有 Billing Admin 权限以及NetApp Console登录权限。

a. 在您被重定向到 "Google Cloud Marketplace 上的NetApp Intelligent Services页面"，确保在顶部导航菜单中选择了正确的项目。



b. 选择*订阅*。

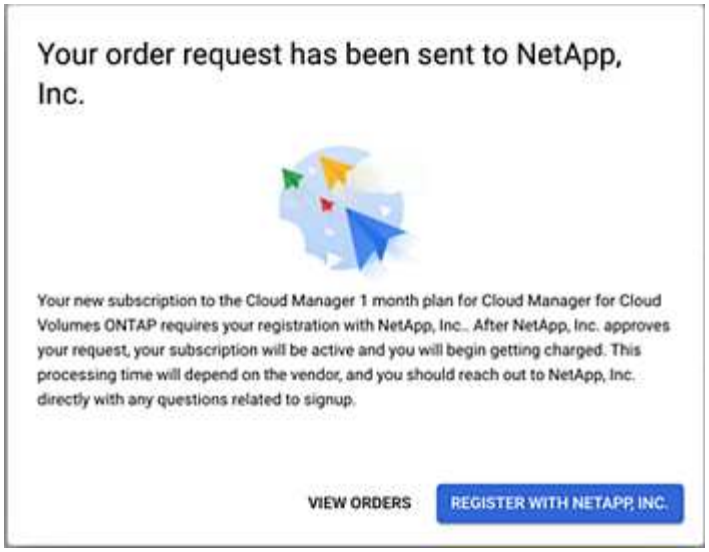
c. 选择适当的结算账户并同意条款和条件。

d. 选择*订阅*。

此步骤将您的转移请求发送给NetApp。

e. 在弹出的对话框中，选择*向NetApp, Inc. 注册*。

必须完成此步骤才能将 Google Cloud 订阅与您的控制台组织或帐户关联。直到您从此页面重定向并登录到控制台后，链接订阅的过程才完成。



f. 完成“订阅分配”页面上的步骤：

> 如果您组织中的某人已经从您的结算帐户中订阅了市场，那么您将被重定向到 "NetApp Console中的Cloud Volumes ONTAP页面"反而。如果这是意外情况，请联系您的NetApp销售团队。 Google 为每个 Google 结算帐户仅启用一项订阅。

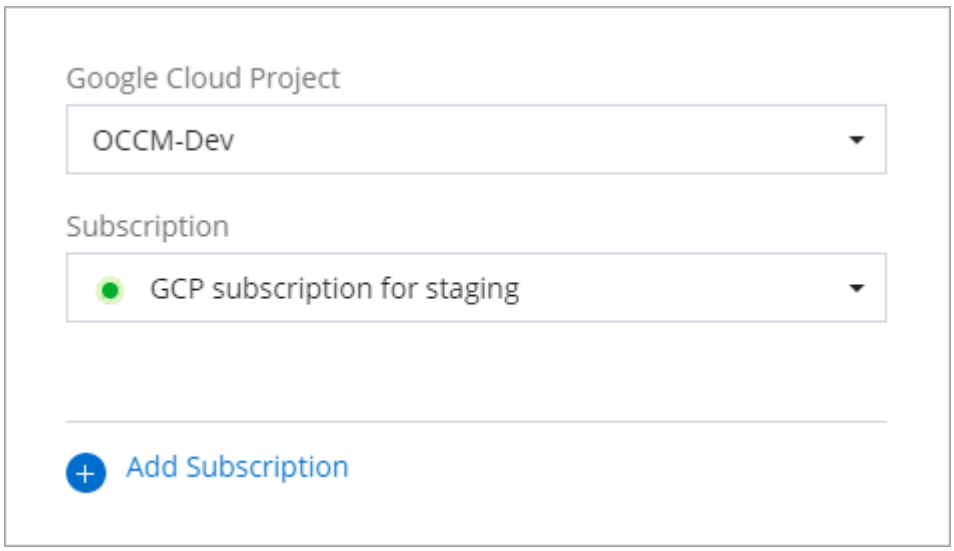
- 选择您想要与此订阅关联的控制台组织。
- 在“替换现有订阅”字段中，选择是否要用这个新订阅自动替换一个组织的现有订阅。

  控制台将用这个新订阅替换组织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*。

3. 此过程完成后，导航回控制台中的“凭据”页面并选择此新订阅。

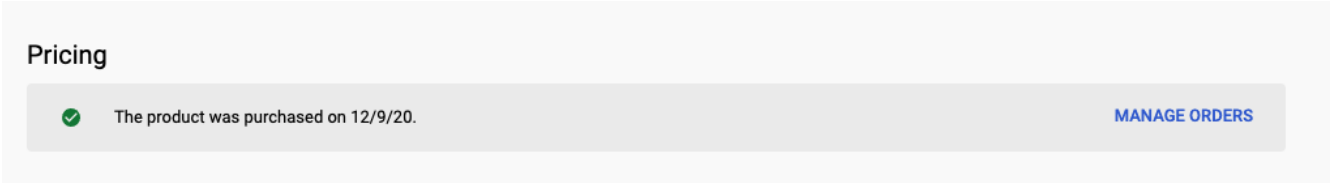


排查 **Marketplace** 订阅流程故障

有时，通过 Google Cloud Marketplace 订阅 NetApp 数据服务可能会因权限不正确或意外未遵循重定向到 Console 而变得分散。如果发生这种情况，请使用以下步骤完成订阅过程。

步骤

1. 导航到 "Google Cloud Marketplace 上的 NetApp 页面"以查看订单状态。如果页面显示 **Manage on Provider**，请向下滚动并选择 **Manage Orders**。



   - 如果订单显示绿色复选标记，而这是意外情况，则可能已经订阅了使用同一账单账号的其他组织成员。如果这是出乎意料的，或者您需要此订阅的详细信息，请联系您的 NetApp 销售团队。

   - 如果订单显示时钟和 **Pending** 状态，请返回 marketplace 页面，然后选择 **Manage on Provider** 以完成上述流程。

身份和访问管理

了解NetApp Console身份和访问管理

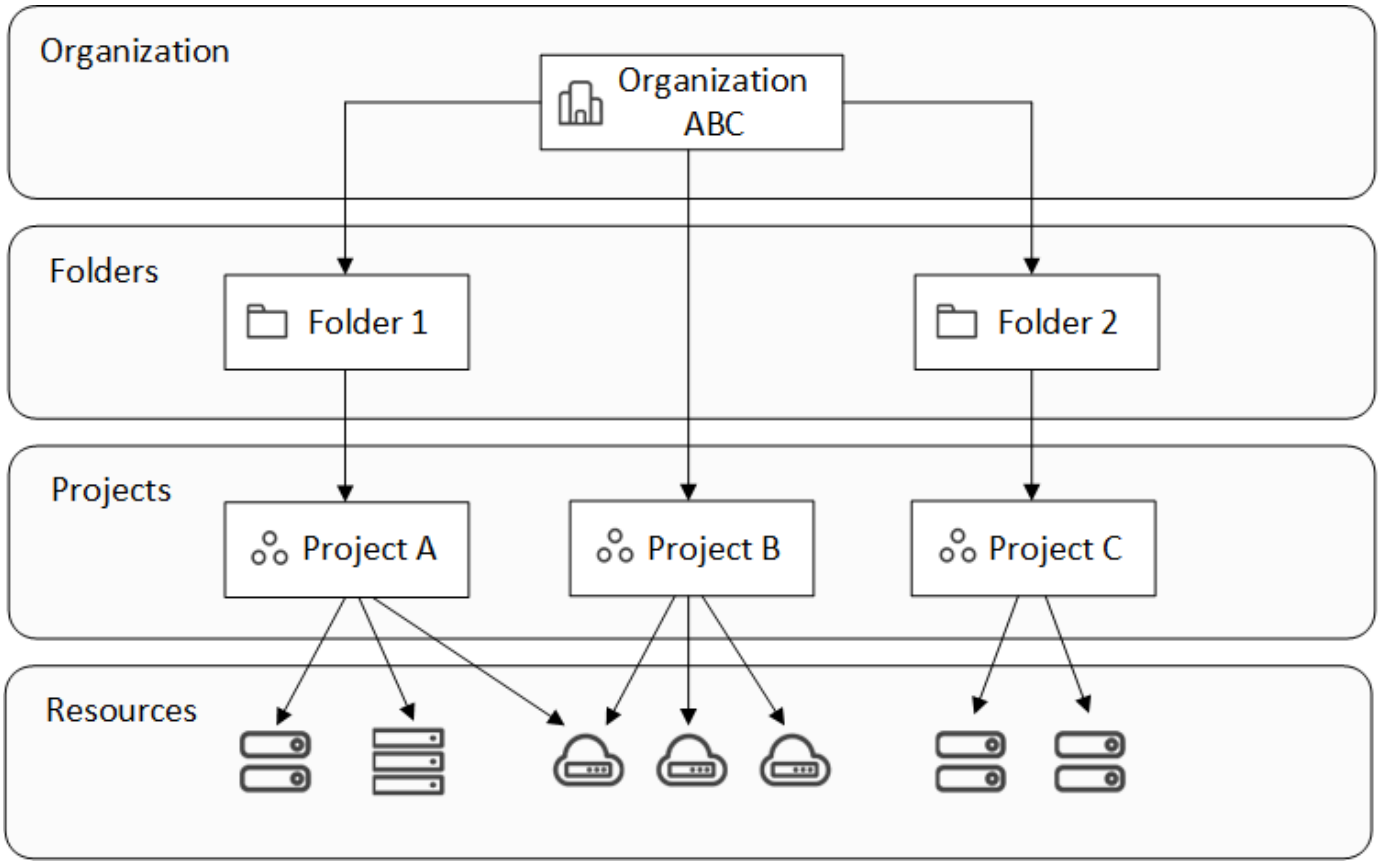
使用NetApp控制台的身份和访问管理 (IAM) 来组织您的NetApp资源，并根据您的业务结构（按位置、部门或项目）控制访问权限。

资源按层级排列：组织位于顶层，其次是文件夹（可以包含其他文件夹或项目），然后是项目，项目包含存储系统、工作负载和代理。

在组织、文件夹或项目级别分配访问角色，以便用户有权访问资源。

您必须拥有_超级管理员_、_组织管理员_或_文件夹或项目管理员_角色才能在NetApp Console中管理 IAM。

下图从基本层面说明了这一层次结构。



]

身份和访问管理组件

在NetApp Console中，您可以使用三个主要组件来组织存储资源：组织组件、资源组件和用户访问组件。

组织内的项目和文件夹

在您的 IAM 结构中，您使用三个组织组件：组织、项目和文件夹。您可以通过为用户分配以下任何级别的角色来授予他们访问权限。

组织

_组织_是控制台 IAM 系统的顶层，通常代表您的公司。您的组织由文件夹、项目、成员、角色和资源组成。代理与组织内的特定项目相关联。

项目

项目用于提供对存储资源的访问。必须先将资源分配给项目，其他人才能访问这些资源。您可以将多个资源分配给一个项目，也可以创建多个项目。然后，您可以为用户分配项目权限，使他们能够访问项目中的资源。

例如，您可以根据需要，将本地ONTAP系统与单个项目或组织中的所有项目关联起来。

"了解如何向您的组织添加项目。"

文件夹

将相关项目分组到_文件夹_中，以便按位置、站点或业务部门进行组织。您无法直接将资源与文件夹关联，但将用户分配到文件夹级别的角色，即可使其访问该文件夹中的所有项目。

"了解如何向您的组织添加文件夹。"

资源

resource 是 NetApp Console 知道并可以分配给项目的实体。*Resources* 包括存储系统、Keystone 订阅、某些 NetApp Backup and Recovery 工作负载以及 NetApp Console 代理。

+ 必须先将资源与项目关联，其他人才能访问该资源。

+

例如，您可以将Cloud Volumes ONTAP系统与一个项目或组织中的所有项目关联起来。资源的分配方式取决于贵组织的需求。

+

"了解如何将资源关联到项目。"

存储系统和**Keystone**订阅

存储系统是您在 NetApp Console 中管理的主要资源。NetApp Console 支持本地和云存储系统的管理。必须将存储系统添加到项目中，以便分配给项目的人员可以访问它。

存储系统

存储系统会自动与添加它们的项目关联，但您可以从*资源*页面将其与其他项目或文件夹关联。您无法将 FSx for NetApp ONTAP 存储系统与项目或文件夹关联，但您可以在*系统*页面或从工作负载中查看它们。

Keystone订阅

Keystone订阅也是您可以与项目关联的资源，以便授予用户在NetApp Console中访问订阅的权限。

备份和恢复工作负载（**Oracle** 和 **Microsoft SQL Server**）

一些 Backup and Recovery 工作负载也被视为资源。您可以分配用户权限来访问 Backup and

控制台代理

组织管理员创建控制台代理来管理存储系统并启用NetApp数据服务。代理最初与创建它们的项目关联，但管理员可以从“代理”页面将它们添加到其他项目或文件夹。

将代理与项目关联起来，可以管理该项目中的资源；而将代理与文件夹关联起来，可以让文件夹或项目管理员决定哪些项目应该使用该代理。代理人必须与特定项目关联才能提供管理能力。

"了解如何将代理商与项目关联起来。"

成员及角色

成员

您的组织的成员是用户帐户或服务帐户。应用程序通常使用服务帐户来完成指定的任务，而无需人工干预。

成员注册NetApp Console后，您需要将他们添加到您的组织中。添加完成后，您可以为他们分配角色，以便授予他们访问资源的权限。您可以手动从控制台添加服务帐户，也可以通过NetApp ConsoleIAM API 自动创建和管理服务帐户。

"了解如何向您的组织添加成员。"

访问角色

控制台提供您可以分配给组织成员的访问角色。

将成员与角色关联时，您可以为整个组织、特定文件夹或特定项目授予该角色。您选择的角色赋予成员对层次结构中选定部分的资源的权限。

NetApp Console提供细粒度的角色控制，遵循“最小权限”原则，这意味着访问角色旨在仅向用户授予其所需的权限。

这意味着随着用户职责的增加，他们可能会被分配多个角色。

"了解访问角色" 。

IAM 策略示例

小型组织战略

对于用户少于 50 人且采用集中式存储管理的组织，可以考虑使用超级管理员和超级查看者角色的简化方法。

示例：**ABC**公司（**5**人团队）

- 组织结构： 单一组织，下设 3 个项目（生产、开发、备份）
- 角色：
  - 2 位高级成员：拥有*超级管理员*角色，可获得完整的管理权限
  - 3 名团队成员：*超级查看者*角色，拥有监控权限但无修改权限
- 代理策略：所有项目都关联一个代理，以实现资源共享访问。
- 优势：简化管理，降低角色复杂性，适合需要广泛访问权限的团队

多区域企业战略

对于拥有区域运营和专业团队的大型组织，应采用层级式方法，用文件夹表示地理或业务单元边界。

例如：**XYZ**公司（跨国公司）

- 结构： 组织结构 > 区域文件夹（北美、欧洲、亚太） > 每个区域的项目文件夹
- 平台角色：
  - 1 组织管理：全球监督和政策管理
  - 3 文件夹或项目管理员：区域控制（每个区域一个）
  - 1 联盟管理员：企业身份提供商集成
- 按区域划分的存储角色：
  - 9 存储管理员：发现和管理指定区域中的存储系统
  - 2 存储查看器：监控跨区域的存储资源
  - 1 系统健康专家：无需修改系统即可管理存储健康状况
- 数据服务角色：

    - 备份和恢复管理员：按项目根据备份职责而定
    - 勒索软件恢复管理员：负责跨项目的安全团队监控
- 代理策略：与相应地理项目相关的区域代理
- 优势： 通过角色分离、区域自主权和遵守当地法规来增强安全性

部门专业化战略

对于拥有需要特定数据服务访问权限的专业团队的组织，应根据职能职责进行有针对性的角色分配。

例如：**TechCorp**（一家中型科技公司）

- 结构： 组织 > 部门文件夹（IT、安全、开发） > 项目特定资源
- 专业岗位：
    - 安全团队：*勒索软件恢复管理员*和*分类查看器*角色
    - 备份团队：备份和恢复超级管理员，负责全面的备份操作
    - 开发团队：测试环境管理存储管理员
    - 合规团队：运营支持分析师，负责监控和支持案例管理
- 代理策略： 根据资源所有权将代理与部门项目关联起来
- 优势： 可定制的访问控制、更高的运营效率以及明确的专项任务责任划分

NetApp Console中 **IAM** 的后续步骤

- "开始使用NetApp Console中的 IAM"
- "监控或审计 IAM 活动"
- "了解NetApp Console IAM 的 API"

开始在**NetApp Console**中使用身份和访问权限

当您注册NetApp Console时，系统会提示您创建一个新的组织。该组织包括一名成员（组织管理员）和一个默认项目。要设置身份和访问管理 (IAM) 来满足您的业务需求，您需要自定义组织的层次结构、添加其他成员、添加或发现资源，并在整个层次结构中关联这些资源。

您需要拥有*组织管理员*或*超级管理员*权限才能管理组织的身份和访问权限。拥有*文件夹或项目管理员*权限，您只能管理您有权访问的文件夹和项目。

按照以下步骤建立一个新组织。该顺序可能会根据您组织的需求而有所不同。

编辑默认项目或添加到组织的层次结构

使用默认项目或创建与您的业务层次结构相匹配的其他项目和文件夹。

"了解如何使用文件夹和项目来组织资源" 。

2 将成员与您的组织关联

用户注册NetApp Console后，您必须明确地将他们添加到您的 Console 组织中。您还可以选择向您的组织添加服务帐户。

"了解如何管理成员及其权限" 。

3 添加或发现资源

向控制台添加或发现资源（系统）。组织成员从项目内部管理系统。

了解如何创建或发现资源：

- "Amazon FSx for NetApp ONTAP"
- "Azure NetApp Files"
- "Cloud Volumes ONTAP"
- "E系列系统"
- "本地ONTAP集群"
- "StorageGRID"

4 将资源与其他项目关联

在控制台中添加或发现系统会自动将资源与当前选定的项目关联。要使该资源可用于组织中的另一个项目，请将其与相应的项目关联。如果使用控制台代理来管理资源，请将控制台代理与相应的项目关联。

- "了解如何管理组织的资源层次结构" 。
- "了解如何将控制台代理与文件夹或项目关联" 。

相关信息

- "了解NetApp Console中的身份和访问管理"
- "了解身份和访问 API"

设置您的控制台组织

将文件夹和项目添加到**NetApp Console**组织

添加文件夹和项目，以匹配您的业务结构。创建文件夹和项目后，您可以将资源与它们关联起来，并管理成员对这些项目的访问权限。

创建新组织时，控制台会自动为您创建一个项目。大多数组织都需要多个项目，以及文件夹来保持井然有序。"了解NetApp Console中的资源层次结构"。

使用文件夹和项目来组织资源

在NetApp Console中，组织包含文件夹和项目，可帮助您组织资源。文件夹可以帮助您对相关项目进行分组，项目可以帮助您管理资源和成员访问权限。

文件夹

文件夹可以帮助您整理相关项目。您可以创建嵌套文件夹来表示组织结构的不同层级。例如，您可以为每个业务部门创建一个顶级文件夹，然后在该业务部门内为不同的团队创建子文件夹。然后，您可以在文件夹内创建项目。

文件夹还可以通过角色继承更有效地管理成员访问权限。在文件夹级别为成员分配角色时，他们将继承所有子项目和文件夹的权限。

文件夹是一种组织工具，对于没有 IAM 权限的成员（例如组织管理员、文件夹或项目管理员或超级管理员角色）是不可见的。成员访问的是项目，而不是文件夹。

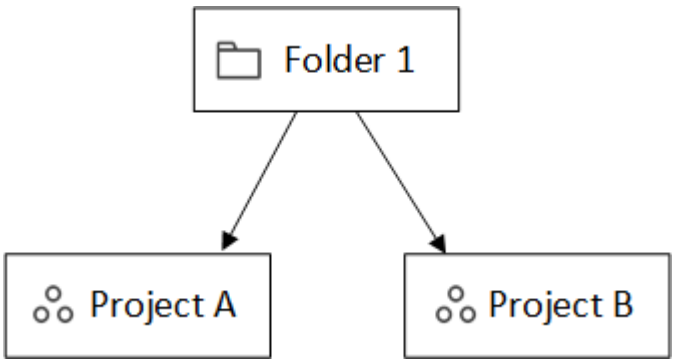
组织管理员可以通过创建文件夹来委派管理职责。创建文件夹后，组织管理员可以为特定文件夹分配文件夹管理员或项目管理员角色。这些成员无需访问整个组织即可管理该文件夹内的所有项目。

文件夹可以包含其他文件夹或项目作为子文件夹，但不能直接关联资源。资源必须与项目关联。

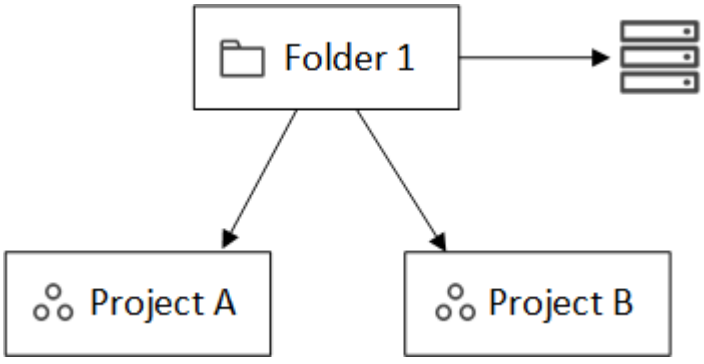
何时将资源与文件夹关联

_组织管理员_可以将资源与文件夹关联，以便_文件夹或项目管理员_可以将其链接到文件夹中的相应项目。

例如，假设您有一个包含两个项目的文件夹：

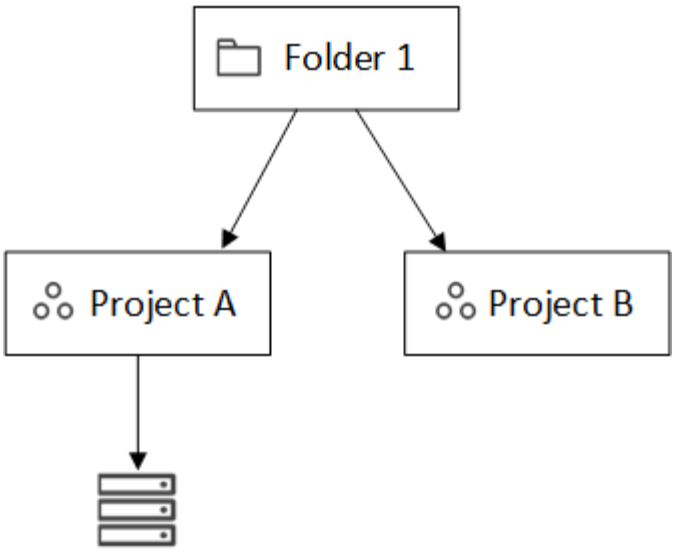


_组织管理员_可以将资源与文件夹关联：



将资源与文件夹关联并不会使所有项目都可以访问它；只有文件夹或项目管理员可以看到它。 _文件夹或项目管理员_决定哪些项目可以访问它，并将资源与适当的项目关联。

在此示例中，管理员将资源与项目 A 关联：



拥有项目 A 权限的成员现在可以访问该资源。

项目

将资源与项目关联起来，以便成员进行管理。资源必须与项目关联才能进行管理和用户访问。

一个组织可以有一个或多个项目。项目可以直接位于组织下，也可以位于文件夹内。如果使用代理来发现项目中的资源，则还必须将该代理与该项目关联起来。

用户可在“系统”页面上浏览已分配的项目，以管理与每个项目相关的资源。

添加文件夹或项目

添加项目以管理资源，添加文件夹以对相关项目进行分组。创建新组织时，控制台会包含一个项目。

您可以在组织的资源结构中创建最多七级的文件夹和项目。根据需要创建嵌套文件夹来整理资源。

步骤

1. 选择*管理>身份和访问*。
2. 选择*组织*。
3. 从*组织*页面中，选择*添加文件夹或项目*。
4. 选择*文件夹*或*项目*。
5. 请输入文件夹或项目详细信息：
   - 名称和位置：输入文件夹或项目的名称并选择其位置。您可以将文件夹或项目放置在组织下，也可以放置在其他文件夹内。
   - 资源：选择要与此文件夹或项目关联的资源。如果您尚未向主机添加存储系统，您可以稍后执行此步骤。

只有当文件夹中的资源被分配给某个项目后，成员才能访问这些资源。使用文件夹临时存放资源，直到创建必要的项目为止。这可以帮助组织管理员将资源分配委派给文件夹或项目管理员，然后由该管理员将资源分配给文件夹内的项目。

- 访问权限：选择*添加成员*以分配访问权限和角色。您可以随时向项目或文件夹中添加或删除成员。

  "了解访问角色" 。

6. 选择“添加”。

重命名文件夹或项目

根据需要重命名文件夹或项目。重命名不会影响相关资源或成员访问权限。

步骤

1. 从“组织”页面，导航到表中的项目或文件夹，选择 ••• 然后选择*编辑文件夹*或*编辑项目*。
2. 在*编辑*页面上，输入新名称并选择*应用*。

删除文件夹或项目

删除不再需要的文件夹和项目，例如团队重组或项目完成后。

删除文件夹或项目之前，请确保其中不包含任何资源。了解如何移除资源。

步骤

1. 从“组织”页面，导航到表中的项目或文件夹，选择 ••• 然后选择*删除*。
2. 确认您要删除文件夹或项目。

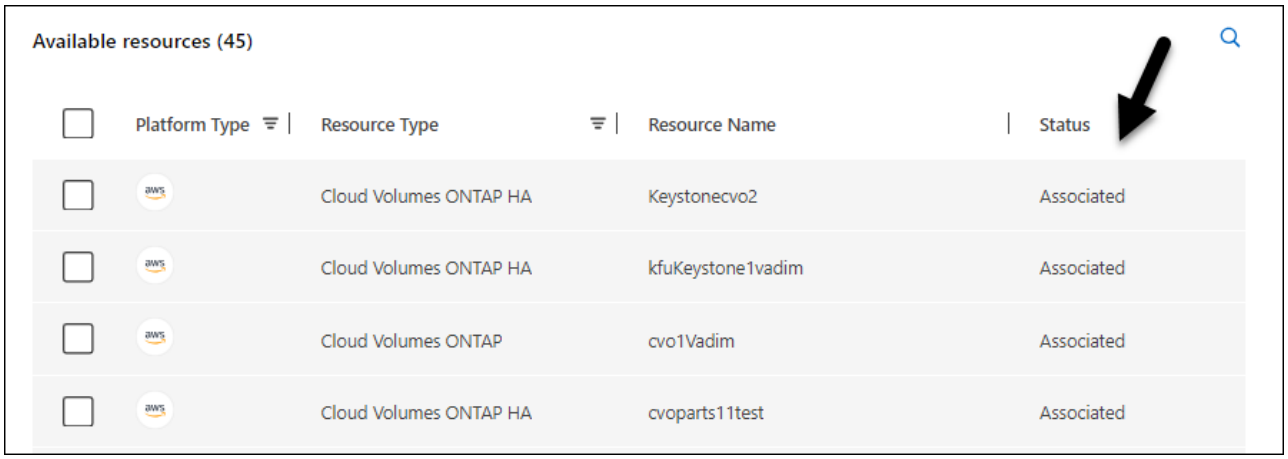
查看与文件夹或项目关联的资源

查看哪些资源和成员与文件夹或项目相关联。

步骤

1. 从“组织”页面，导航到表中的项目或文件夹，选择 ••• 然后选择*编辑文件夹*或*编辑项目*。

2. 在*编辑*页面上，您可以通过展开*资源*或*访问*部分来查看有关所选文件夹或项目的详细信息。
   - 选择“资源”来查看相关资源。在表中，“状态”列标识与文件夹或项目相关的资源。



更改与文件夹或项目关联的资源

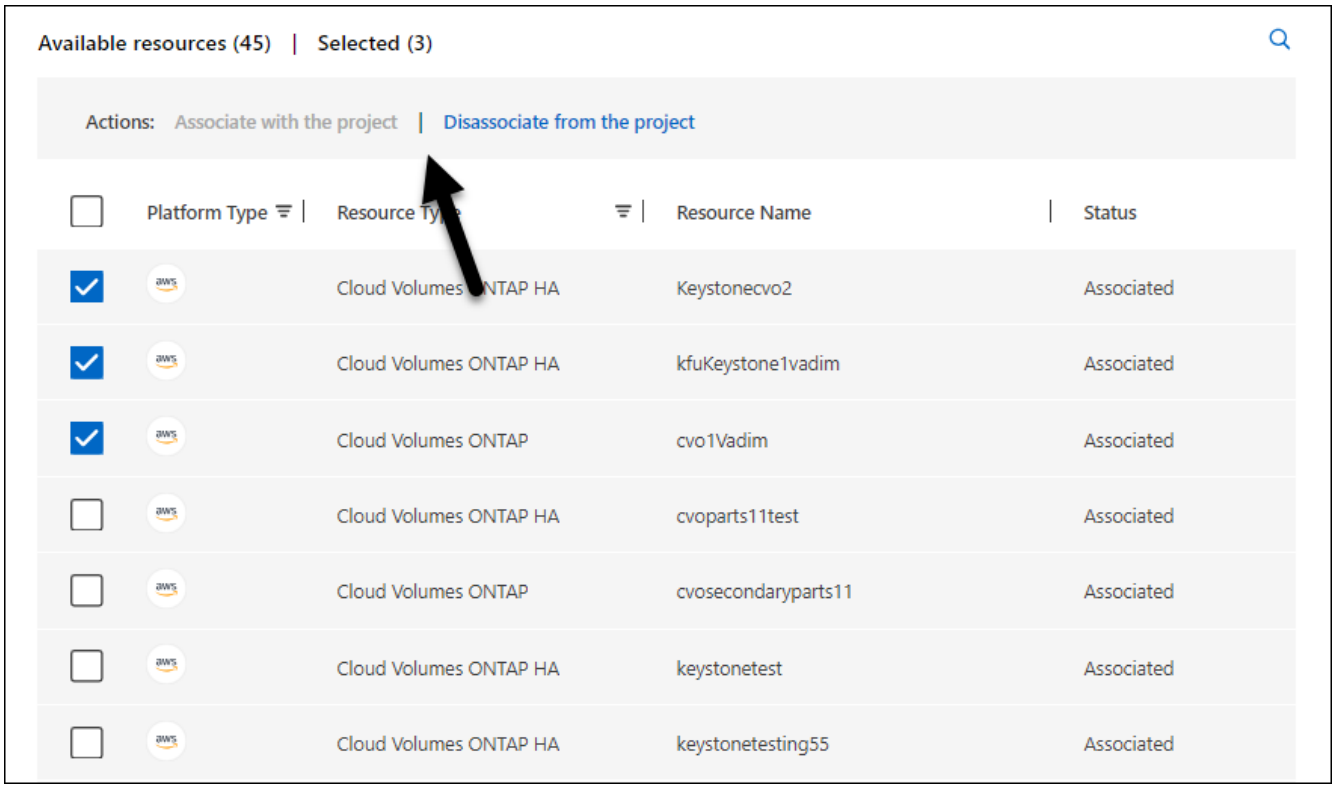
您可以根据组织的需求变化更改与文件夹或项目关联的资源。

步骤

1. 从“组织”页面，导航到表中的项目或文件夹，选择 ••• 然后选择*编辑文件夹*或*编辑项目*。
2. 在*编辑*页面上，选择*资源*。

   在表中，“状态”列标识与文件夹或项目相关的资源。

3. 选择您想要关联或取消关联的资源。
4. 根据您选择的资源，选择“与项目关联”或“与项目取消关联”。



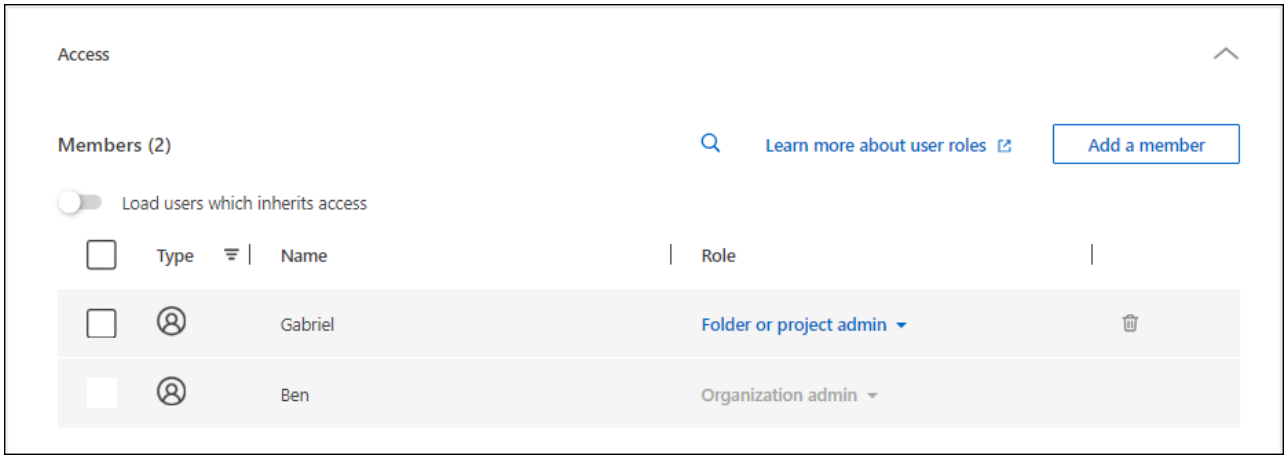
5. 选择*应用*。

查看与文件夹或项目关联的成员

您可以从“组织”页面查看与文件夹或项目关联的成员。

步骤

1. 从“组织”页面，导航到表中的项目或文件夹，选择 ••• 然后选择*编辑文件夹*或*编辑项目*。
2. 在*编辑*页面上，选择*访问*以查看有权访问所选文件夹或项目的成员列表。
   - 选择*访问*来查看有权访问该文件夹或项目的成员。



修改成员对文件夹或项目的访问权限

修改成员访问权限以控制资源访问。请记住，在文件夹级别分配的角色将被所有子项目和文件夹继承。

如果成员访问权限是从文件夹或组织级别继承的，则无法在较低级别更改成员访问权限。更改更高层级成员的权限以更改访问权限。或者，您可以 "从“会员”页面管理权限"。

步骤

1. 从“组织”页面，导航到表中的项目或文件夹，选择 ••• 然后选择*编辑文件夹*或*编辑项目*。
2. 在*编辑*页面上，选择*访问*以查看有权访问所选文件夹或项目的成员列表。
3. 修改会员访问权限：
   - 添加成员：选择您想要添加到文件夹或项目的成员并为他们分配角色。
   - 更改成员的角色：对于具有组织管理员以外角色的任何成员，选择其现有角色，然后选择新角色。
   - 删除成员访问权限：对于在您正在查看的文件夹或项目中定义了角色的成员，您可以删除他们的访问权限。
4. 选择*应用*。

相关信息

- "了解NetApp Console中的身份和访问权限"
- "开始使用身份和访问权限"
- "了解身份和访问 API"

在**NetApp Console**中向文件夹和项目添加资源

通过将用户添加到NetApp Console组织中的项目和文件夹来控制用户对资源的访问权限。授予项目级用户访问权限。

资源是指控制台所感知到的实体，例如存储资源、控制台代理或备份和恢复工作负载。

您可以在控制台的“资源”页面中查看和管理资源。

控制台资源类型

您可以将多种类型的资源关联到NetApp Console组织中的项目：

存储资源

存储资源是组织中最常见的资源类型，包括本地存储系统和云存储系统。在控制台中添加存储系统时，您可以将其添加到文件夹或项目中。在此之前，控制台会将其标记为未发现，并且不会在“资源”页面上显示它。

控制台代理

如果您使用控制台代理来发现存储系统，请将该代理添加到同一文件夹或项目中。这允许用户执行代理启用的功能，例如数据服务或控制台原生存储管理。您可以从控制台的“代理”页面向文件夹或项目中添加代理。"了解如何将控制台代理与文件夹或项目关联"。

Keystone订阅

如果您的组织拥有Keystone订阅，您可以在“资源”页面上查看它们。您可以将Keystone订阅与文件夹或项目关联起来，以便向拥有这些文件夹或项目权限的成员提供访问权限。

查看组织中的资源

您可以查看与您的组织相关的已发现和未发现的资源。系统会查找存储资源，并将其标记为未发现，直到您将其添加到控制台为止。

控制台会将Amazon FSx for NetApp ONTAP资源从“资源”页面中排除，因为用户无法将其与角色关联。您可以在“系统”页面或“工作负载”中查看这些资源。

步骤

1. 选择*管理>身份和访问*。
2. 选择*资源*。
3. 选择*高级搜索和过滤*。
4. 利用现有选项查找资源：
   - 按资源名称搜索：输入文本字符串并选择*添加*。
   - 平台：选择一个或多个平台，例如 Amazon Web Services。
   - 资源：选择一个或多个资源，例如Cloud Volumes ONTAP。
   - 组织、文件夹或项目：选择整个组织、特定文件夹或特定项目。
5. 选择*搜索*。

将资源与文件夹和项目关联

将资源关联到文件夹或项目，使其可供具有该文件夹或项目权限的成员使用。

步骤

1. 从“资源”页面，导航到表中的资源，选择 ••• 然后选择*关联到文件夹或项目*。
2. 选择一个文件夹或项目，然后选择*接受*。
3. 要关联其他文件夹或项目，请选择*添加文件夹或项目*，然后选择该文件夹或项目。

   请注意，您只能从您拥有管理员权限的文件夹和项目中进行选择。

4. 选择*关联资源*。
   - 如果您将资源与项目关联，则拥有这些项目权限的成员现在可以从控制台访问该资源。
   - 如果您将资源与文件夹关联，则_文件夹或项目管理员_现在可以访问该资源并将其与文件夹内的项目关联。"了解如何将资源与文件夹关联"。

完成后

如果您使用控制台代理发现资源，请将控制台代理与项目关联以授予访问权限。否则，没有“组织管理员”角色的成员将无法访问控制台代理及其相关资源。

"了解如何将控制台代理与文件夹或项目关联"。

查看与资源关联的文件夹和项目

您可以查看与特定资源关联的文件夹和项目。

如果您需要了解哪些组织成员有权访问该资源，您可以"查看有权访问与资源关联的文件夹和项目的成员"。

步骤

1. 从“资源”页面，导航到表中的资源，选择 ••• 然后选择*查看详细信息*。

以下示例显示了与一个项目关联的资源。

要查看哪些组织成员有权访问该资源，"查看有权访问关联文件夹和项目的成员" 。

从文件夹或项目中删除资源

要从文件夹或项目中删除资源，请删除其关联。这样可以防止成员管理该文件夹或项目中的资源。

要从整个组织中删除已发现的资源，请转到“系统”页面并删除该系统。

步骤

1. 从“资源”页面，导航到表中的资源，选择 ••• 然后选择*查看详细信息*。
2. 要从文件夹或项目中移除资源，请选择 在文件夹或项目旁边。
3. 选择“删除”以移除关联。

相关信息

- "了解NetApp Console中的身份和访问权限"
- "开始在NetApp Console中使用身份和访问权限"
- "了解身份和访问 API"

将控制台代理与其他文件夹和项目关联

将控制台代理与特定项目关联起来，以实现资源管理和数据服务访问。通过控制台代理发现的资源需要资源和代理都与同一个项目关联，才能实现团队访问。

超级管理员和组织管理员可以创建代理，并将任何代理与任何项目或文件夹关联起来。文件夹或项目管理员只能将现有代理与他们拥有权限的文件夹和项目关联起来。"详细了解文件夹或项目管理员可以完成的操作"。

步骤

1. 选择*管理>身份和访问*>*代理*。
2. 从表中，找到要关联的控制台代理。

   使用表格上方的搜索功能查找特定的控制台代理或按资源层次结构过滤表格。

3. 要查看链接到控制台代理的文件夹和项目，请选择 ••• 然后选择*查看详细信息*。

   该页面显示与控制台代理关联的文件夹和项目的详细信息。

4. 选择*关联到文件夹或项目*。
5. 选择一个文件夹或项目，然后选择*接受*。
6. 要将控制台代理与其他文件夹或项目关联，请选择*添加文件夹或项目*，然后选择该文件夹或项目。
7. 选择*关联代理*。

完成后

将控制台代理的资源与“资源”页面中的相同文件夹和项目关联。

"了解如何将资源与文件夹和项目关联" 。

相关信息

- "了解NetApp Console代理"
- "了解NetApp Console身份和访问管理"
- "开始使用身份和访问权限"
- "了解身份和访问管理的 API"

将用户添加到您的控制台组织

将用户添加到**NetApp Console**组织

在控制台中，您可以根据访问角色授予用户对项目或文件夹的访问权限。_访问角色_包含一组权限，使成员（用户或服务帐户）能够在资源层次结构的指定级别执行特定操作。

所需访问权限

超级管理员、组织管理员或文件夹或项目管理员（对于他们管理的文件夹和项目）。"了解访问角色"。

了解如何在**NetApp Console**中授予访问权限

NetApp Console使用基于角色的访问控制 (RBAC) 来管理权限。可以单独为用户分配角色，也可以通过联合组为用户分配角色。每个角色都定义了对特定资源允许的操作。

请注意以下关于在NetApp Console中授予访问权限的事项：

- 所有用户必须先注册NetApp Console，然后才能获得资源访问权限。
- 即使用户是已分配角色的联合组的成员，也必须在控制台中明确地为每个用户分配角色，然后他们才能访问资源。
- 您可以直接从控制台添加服务帐户并为其分配角色。

向您的组织添加成员

NetApp Console支持三种类型的成员：用户帐户、服务帐户和联合组。

即使用户属于联合组，也必须先注册NetApp Console，然后才能添加他们并分配角色。直接在控制台中创建服务帐户。

所有成员必须至少被明确分配一个角色才能访问资源。

添加成员时，选择资源级别（组织、文件夹或项目），并分配一个或多个具有所需权限的角色。

添加用户

用户注册NetApp Console，但组织管理员、文件夹管理员或项目管理员必须将他们添加到组织、文件夹或项目中，以便他们能够访问资源。

开始之前：

用户必须已经注册了NetApp Console。如果他们还没有注册，请引导他们…… "注册NetApp Console。"

如果要添加属于联合组的用户，请确保该用户已注册NetApp Console，并在控制台中明确分配了角色。NetApp建议分配最低访问权限角色，例如组织查看者。

步骤

1. 选择*管理>身份和访问*。
2. 选择*成员*。
3. 选择*添加成员*。
4. 对于*会员类型*，保持选择*用户*。
5. 对于*用户的电子邮件*，输入与其创建的登录相关联的用户的电子邮件地址。
6. 使用“选择组织、文件夹或项目”部分来选择成员应具有权限的资源层次结构级别。

   请注意以下事项：

   - 您只能选择您拥有权限的文件夹和项目。
   - 选择组织或文件夹时，即授予该成员对其所有内容的访问权限。
   - 您只能在组织级别分配*组织管理员*角色。
7. 选择一个类别，然后选择一个*角色*，该角色为成员提供与您选择的组织、文件夹或项目相关的资源的权限。

   "了解访问角色" 。
8. 要授予对更多文件夹、项目或角色的访问权限，请选择“添加角色”，选择文件夹、项目或角色类别，然后选择角色。
9. 选择“添加”。

   控制台会通过电子邮件向用户发送操作说明。

添加服务帐户

服务帐户允许您自动执行任务并安全地连接到控制台 API。对于简单的设置，可以选择客户端 ID 和密钥；对于自动化或云原生环境，可以选择 JWT（JSON Web Token）以获得更强的安全性。选择符合您安全要求的方法。

开始之前：

对于 JWT 身份验证，请准备您的公钥或证书。

步骤

1. 选择*管理>身份和访问*。
2. 选择*成员*。
3. 选择*添加成员*。
4. 对于*会员类型*，选择*服务帐户*。
5. 输入服务帐户的名称。
6. 要使用 JWT 身份验证，请选择“使用私钥 JWT 身份验证”，然后上传您的 RSA 公钥或证书。如果使用客户端 ID 和密钥，则跳过此步骤。

   您的 X.509 证书。它必须是 PEM、CRT 或 CER 格式。

a. 设置证书到期通知。您可以选择七天或三十天。到期通知将通过电子邮件发送给具有超级管理员或组织管理员角色的用户，并在控制台中显示。

7. 使用“选择组织、文件夹或项目”部分来选择成员应具有权限的资源层次结构级别。

   请注意以下事项：

   - 您只能从您有权限的文件夹和项目中进行选择。
   - 选择一个组织或文件夹将授予成员对其所有内容的权限。
   - 您只能在组织级别分配*组织管理员*角色。

8. 选择一个*类别*，然后选择一个*角色*，授予成员对所选组织、文件夹或项目中的资源的权限。

   "了解访问角色" 。

9. 要授予对更多文件夹、项目或角色的访问权限，请选择“添加角色”，选择文件夹、项目或角色类别，然后选择角色。

10. 如果您没有选择使用 JWT 身份验证，请下载或复制客户端 ID 和客户端密钥。

    控制台只会显示一次客户端密钥。请妥善备份；如果丢失，您可以稍后重新创建。

11. 如果您选择 JWT 身份验证，请下载或复制客户端 ID 和 JWT 受众群体。控制台只会显示此信息一次，之后无法再检索。

12. 选择*关闭*。

向您的组织添加联合组

您可以将身份提供商 (IdP) 中的联合组添加到您的组织，并为其分配一个或多个角色。联合组的成员将继承您在控制台中分配给该组的角色。

在为联合组分配角色之前，请确保以下事项：

- 在身份提供商 (IdP) 和控制台之间建立联盟。 "了解如何建立联邦。"
- 该组必须已存在于您的身份提供商 (IdP) 中，并且已被分配对控制台的应用程序访问权限。
- 属于该组的用户必须已经注册了NetApp Console，并且已被明确分配了控制台中的角色。NetApp建议分配最低访问权限角色，例如组织查看者。

步骤

1. 选择*管理>身份和访问*。
2. 选择*成员*。
3. 选择*添加成员*。
4. 对于“成员类型”，请选择“联合组”。
5. 选择该团体所属的联邦。
6. 对于“组名称”，请输入您身份提供商 (IdP) 中组的确切名称。
7. 使用“选择组织、文件夹或项目”部分来选择成员应具有权限的资源层次结构级别。

   请注意以下事项：

- 您只能从您有权限的文件夹和项目中进行选择。
- 选择一个组织或文件夹将授予成员对其所有内容的权限。
- 您只能在组织级别分配*组织管理员*角色。

8. 选择一个*类别*，然后选择一个*角色*，授予成员对所选组织、文件夹或项目中的资源的权限。

   "了解访问角色" 。

9. 要授予对更多文件夹、项目或角色的访问权限，请选择“添加角色”，选择文件夹、项目或角色类别，然后选择角色。

相关信息

- "了解NetApp Console中的身份和访问管理"
- "开始使用身份和访问权限"
- "NetApp Console访问角色"
- "了解身份和访问 API"

管理用户访问权限和安全

了解**NetApp Console**基于角色的访问控制 **(RBAC)**

使用基于角色的访问控制 (RBAC) 管理用户对NetApp Console的访问，在组织、文件夹或项目级别分配预定义角色。每个角色都授予特定的权限，定义用户在其分配的权限范围内可以执行哪些操作。

NetApp在设计控制台角色时遵循最小权限原则，因此每个角色仅包含其任务所需的权限。这种方法通过限制每个成员所需的访问权限来增强安全性。

将资源整理成文件夹和项目后，为组织成员分配特定文件夹或项目的角色，使他们只能履行自己的职责。

例如，您可以为特定项目级别的成员分配勒索软件恢复管理员角色，允许他们对该项目内的资源执行勒索软件恢复操作，而无需授予他们对整个组织的更广泛访问权限。同一用户可以被授予组织内多个项目的角色。

您可以根据用户的职责，为同一范围或不同范围的用户分配多个角色。例如，规模较小的组织可能会让同一用户在组织层面管理勒索软件恢复和备份与恢复任务，而规模较大的组织可能会在项目层面为每个角色分配不同的用户。

控制台组织成员的类型

NetApp Console组织中有三种类型的成员：* 用户帐户：登录到NetApp Console以管理资源的个人用户。用户必须先注册NetApp Console，然后才能被添加到组织中。* 服务帐户：应用程序或服务通过 API 与NetApp Console交互时使用的非人类帐户。您可以将服务帐户直接添加到您的控制台组织中。* 联合组：从您的身份提供商 (IdP) 同步的组，允许您集中管理多个用户的访问权限。联合组中的每个用户都必须先注册NetApp Console，并被添加到您的组织中，且拥有相应的访问角色，然后才能访问授予该组的资源。

"了解如何向您的组织添加成员。"

NetApp Console中的预定义角色

NetApp Console包含预定义角色，您可以将其分配给组织成员。每个角色都包含权限，用于指定成员在其分配的范围（组织、文件夹或项目）内可以执行哪些操作。

NetApp Console角色采用最小权限原则，确保成员仅拥有完成任务所需的权限，并按角色提供的访问权限类型对其进行分类：

- 平台角色：提供控制台管理权限
- 数据服务角色：提供管理特定数据服务的权限，例如勒索软件恢复和备份与恢复。
- 应用程序角色：提供管理存储以及审核控制台事件和警报的权限

您可以根据成员的职责为其分配多个角色。例如，您可以为特定项目为一名成员分配勒索软件恢复管理员角色和备份与恢复管理员角色。

"了解NetApp Console中可用的预定义角色"。

在NetApp Console中管理成员访问权限

管理您在控制台组织中的成员访问权限。分配角色以设置权限。成员离开时将其移除。

所需访问权限

超级管理员、组织管理员或文件夹或项目管理员（对于他们管理的文件夹和项目）。链接：reference-iam-predefined-roles.html[了解访问角色]。

您可以按项目或文件夹分配访问角色。例如，可以为用户分配两个特定项目的角色，或者在文件夹级别分配角色，从而授予用户对文件夹中所有项目的勒索软件恢复管理员角色。

请先添加文件夹和项目，然后再分配用户访问权限。 "了解如何添加文件夹和项目。"

了解如何在NetApp Console中授予访问权限

NetApp Console使用基于角色的访问控制 (RBAC) 模型来管理用户权限。您可以单独或通过联合组为成员分配预定义的角色。您可以向服务帐户以及联合组添加和分配角色。每个角色都定义了成员可以在相关资源上执行哪些操作。

请注意以下关于在NetApp Console中授予访问权限的事项：

- 所有用户必须先注册NetApp Console，然后才能获得资源访问权限。
- 即使用户是已分配角色的联合组的成员，也必须在控制台中明确地为每个用户分配角色，然后他们才能访问资源。
- 您可以直接从控制台添加服务帐户并为其分配角色。

使用角色继承

在NetApp Console中，当您在组织、文件夹或项目级别分配角色时，所选范围内的所有资源都会自动继承该角色。例如，文件夹级角色适用于所有包含的项目，而项目级角色适用于该项目内的所有资源。

查看组织成员

要了解成员可用的资源和权限，您可以查看在组织资源层次结构的不同级别分配给该成员的角色。"了解如何使用角色来控制对控制台资源的访问。"

步骤

1. 选择*管理>身份和访问*。
2. 选择*成员*。

   *成员*表列出了您组织的成员。

3. 从“成员”页面，导航到表中的成员，选择 ••• 然后选择*查看详细信息*。

查看分配给成员的角色

您可以查看他们目前被分配的角色。

如果您具有_文件夹或项目管理员_角色，则该页面将显示组织中的所有成员。但是，您只能查看和管理您拥有权限的文件夹和项目的成员权限。"详细了解文件夹或项目管理员可以完成的操作" 。

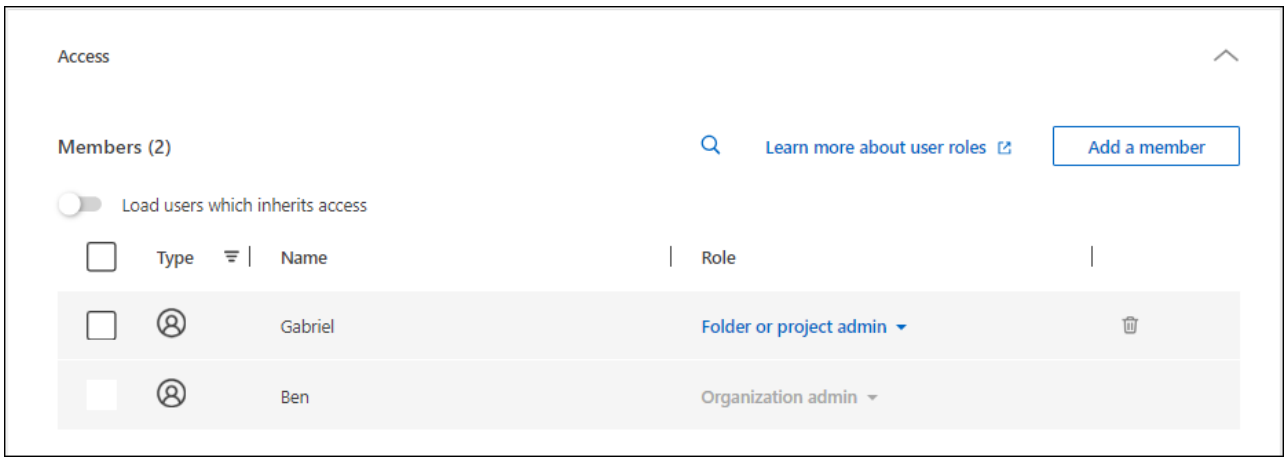
1. 在“成员”页面中，导航至表格中的某个成员，然后选择 ••• 然后选择“查看详情”。
2. 在表格中，展开您想要查看成员分配角色的组织、文件夹或项目的相应行，然后在“角色”列中选择“查看”。

查看与文件夹或项目关联的成员

您可以查看哪些成员有权访问特定文件夹或项目。

步骤

1. 选择*管理>身份和访问*。
2. 选择*组织*。
3. 从“组织”页面，导航到表中的项目或文件夹，选择 ••• 然后选择*编辑文件夹*或*编辑项目*。
   - 选择*访问*来查看有权访问该文件夹或项目的成员。



分配或修改成员访问权限

用户注册NetApp Console后，您可以将他们添加到您的组织并分配角色，以便向他们提供资源访问权限。 "了解如何向您的组织添加成员。"

您可以根据需要添加或删除角色来调整成员的访问权限。

为成员添加访问角色

您通常在向组织添加成员时分配角色，但您可以随时通过删除或添加角色来更新它。

您可以为用户分配组织、文件夹或项目的访问角色。

成员可以在同一个项目内或不同的项目中担任多个角色。例如，规模较小的组织可能会将所有可用的访问角色分配给同一用户，而规模较大的组织可能会让用户执行更专业的任务。或者，您也可以在组织级别为一名用户分配勒索软件恢复管理员角色。在这个例子中，用户可以对组织内的所有项目执行勒索软件恢复任务。

您的访问角色策略应与您组织NetApp资源的方式保持一致。

步骤

1. 选择*管理>身份和访问*。
2. 选择*成员*。
3. 选择成员选项卡之一：用户、服务帐户*或*联合组。
4. 选择操作菜单 ••• 在您想要分配角色的成员旁边，选择“添加角色”。
5. 要添加角色，请完成对话框中的步骤：
   - 选择组织、文件夹或项目：选择成员应具有权限的资源层次结构级别。

     如果您选择组织或文件夹，则该成员将拥有该组织或文件夹内所有内容的权限。
   - 选择类别：选择角色类别。"了解访问角色" 。
   - 选择*角色*：选择一个角色，该角色为成员提供与您选择的组织、文件夹或项目相关的资源的权限。
   - 添加角色：如果您想提供对组织内其他文件夹或项目的访问权限，请选择*添加角色*，指定另一个文件夹或项目或角色类别，然后选择一个角色类别和相应的角色。
6. 选择*添加新角色*。

更改成员的指定角色

更改成员角色以更新其访问权限。

> 必须为用户分配至少一个角色。您不能删除用户的所有角色。如果您需要删除所有角色，则必须从组织中删除该用户。

步骤

1. 选择*管理>身份和访问*。
2. 选择*成员*。
3. 选择成员选项卡之一：用户、服务帐户*或*联合组。

4. 从“成员”页面，导航到表中的成员，选择 ••• 然后选择*查看详细信息*。
5. 在表格中，展开要更改成员分配角色的组织、文件夹或项目的相应行，然后在“角色”列中选择“查看”以查看分配给该成员的角色。
6. 您可以更改成员的现有角色或删除角色。
   a. 要更改成员的角色，请选择要更改的角色旁边的“更改”。您只能将角色更改为同一角色类别内的角色。例如，您可以从一个数据服务角色更改为另一个数据服务角色。确认更改。
   b. 要取消分配成员的角色，请选择 🗑 在角色旁边，点击即可从成员中移除相应的角色。您将被要求确认删除操作。

从您的组织中移除成员

如果成员离开您的组织，则将其从组织中移除。

删除成员时，系统会撤销其控制台权限，但保留其控制台和NetApp支持站点帐户。

联邦成员

- 当联合用户从您的身份提供商 (IdP) 中移除时，他们将自动失去对NetApp Console的访问权限。但您仍然应该将它们从您的控制台组织中删除，以保持您的成员列表是最新的。
- 如果您从身份提供商 (IdP) 中的联合组中移除用户，他们将失去与该组关联的控制台访问权限。但是，他们仍然保留在控制台中分配给他们的明确角色所关联的任何访问权限。

步骤

1. 选择*管理>身份和访问*。
2. 选择*成员*。
3. 选择成员选项卡之一：用户、服务帐户*或*联合组。
4. 从“成员”页面，导航到表中的成员，选择 ••• 然后选择*删除用户*。
5. 确认您要从组织中删除该成员。

用户安全

通过管理成员安全设置，确保用户对NetApp Console组织的访问权限。您可以重置用户密码、管理多因素身份验证 (MFA) 以及重新创建服务帐户凭据。

所需访问权限

超级管理员、组织管理员或文件夹或项目管理员（对于他们管理的文件夹和项目）。链接：reference-iam-predefined-roles.html[了解访问角色]。

重置用户密码（仅限本地用户）

组织管理员无法重置本地用户的用户密码。但是，他们可以指导用户重置自己的密码。

指示用户通过选择“忘记密码？”从控制台登录页面重置密码。

此选项不适用于联合组织中的用户。

管理用户的多重身份验证 **(MFA)**

如果用户失去对其 MFA 设备的访问权限，您可以删除或禁用其 MFA 配置。

多因素身份验证仅适用于本地用户。联合身份验证用户无法启用多因素身份验证 (MFA)。

用户移除多因素身份验证后，登录时必须重新设置多因素身份验证。如果用户暂时无法访问其 MFA 设备，他们可以使用已保存的恢复代码登录。

如果他们没有恢复代码，请暂时禁用 MFA 以允许登录。当您为用户禁用 MFA 时，它只会禁用八个小时，然后自动重新启用。在此期间，用户无需 MFA 即可登录一次。八小时后，用户必须使用 MFA 才能登录。

要管理用户的多重身份验证，您必须拥有与受影响用户位于同一域的电子邮件地址。

步骤

1. 选择*管理>身份和访问*。
2. 选择*成员*。

   *成员*表列出了您组织的成员。

3. 从“成员”页面，导航到表中的成员，选择 ••• 然后选择*管理多重身份验证*。
4. 选择是否删除或禁用用户的 MFA 配置。

重新创建服务帐户的凭据

如果您丢失或需要更新服务凭证，可以创建新的凭证。

创建新凭证会删除旧凭证。您不能使用旧的凭据。

步骤

1. 选择*管理>身份和访问*。
2. 选择*成员*。
3. 在“成员”表中，导航到服务帐户，选择 ••• 然后选择*重新创建秘密*。
4. 选择*重新创建*。
5. 下载或复制客户端 ID 和客户端密钥。

   控制台只会显示一次客户端密钥。请务必复制或下载并妥善保存。

NetApp Console访问角色

了解**NetApp Console**访问角色

NetApp Console中的身份和访问管理 (IAM) 提供了预定义的角色，您可以将这些角色分配给组织中不同资源层次的成员。在分配这些角色之前，您应该了解每个角色包含的权限。角色分为以下类别：平台、应用程序和数据服务。

平台角色

平台角色授予NetApp Console管理权限，包括角色分配和用户管理。控制台具有多种平台角色。

平台角色	职责
"组织管理员"	允许用户不受限制地访问组织内的所有项目和文件夹，向任何项目或文件夹添加成员，以及执行任何任务和使用任何没有明确关联角色的数据服务。具有此角色的用户可以通过创建文件夹和项目、分配角色、添加用户以及管理系统（如果他们拥有适当的凭据）来管理您的组织。这是唯一可以创建控制台代理的访问角色。
"文件夹或项目管理员"	允许用户不受限制地访问分配的项目和文件夹。可以将成员添加到他们管理的文件夹或项目中，以及执行任何任务并在他们被分配的文件夹或项目内的资源上使用任何数据服务或应用程序。文件夹或项目管理员无法创建控制台代理。
"联盟管理员"	允许用户使用控制台创建和管理联合，从而实现单点登录 (SSO)。
"联邦查看器"	允许用户使用控制台查看现有的联合。无法创建或管理联盟。
"合作伙伴管理员"	允许用户创建和管理合作关系。
"合作伙伴查看器"	允许用户查看现有的合作关系。无法创建或管理合作关系。
"超级管理员"	为用户提供管理员角色的子集。此角色专为可能不需要在多个用户之间分配控制台职责的小型组织而设计。
"超级观众"	为用户提供子集查看者角色。此角色专为可能不需要在多个用户之间分配控制台职责的小型组织而设计。

应用程序角色

以下是应用程序类别中的角色列表。每个角色在其指定范围内授予特定的权限。没有所需应用程序或平台角色的用户无法访问相应的应用程序。

应用程序角色	职责
"Google Cloud NetApp Volumes管理员"	具有Google Cloud NetApp Volumes角色的用户可以发现和管理Google Cloud NetApp Volumes。
"Google Cloud NetApp Volumes查看器"	具有Google Cloud NetApp Volumes用户角色的用户可以查看Google Cloud NetApp Volumes。
"Keystone管理员"	具有Keystone管理员角色的用户可以创建服务请求。允许用户监控和查看他们正在访问的Keystone租户内的使用情况、资源和管理详细信息。
"Keystone查看器"	具有Keystone查看者角色的用户不能创建服务请求。允许用户监控和查看他们正在访问的Keystone租户内的消费、资产和管理信息。
ONTAP调解器设置角色	具有ONTAP调解器设置角色的服务帐户可以创建服务请求。服务帐户中需要此角色来配置"ONTAP云调解器"。
"运营支持分析师"	提供对警报和监控工具的访问以及输入和管理支持案例的能力。
"存储管理员"	管理存储健康和治理功能，发现存储资源，以及修改和删除现有系统。
"存储查看器"	查看存储健康和治理功能，以及查看以前发现的存储资源。无法发现、修改或删除现有的存储系统。

应用程序角色	职责
"系统健康专家"	管理存储和健康和治理功能，存储管理员的所有权限，但不能修改或删除现有系统。

数据服务角色

以下是数据服务类别中的角色列表。每个角色在其指定范围内授予特定的权限。没有所需数据服务角色或平台角色的用户将无法访问数据服务。

数据服务角色	职责
"备份和恢复超级管理员"	在NetApp Backup and Recovery中执行任何操作。
"备份和恢复管理员"	执行本地快照备份、复制到二级存储以及备份到对象存储。
"备份和恢复恢复管理员"	恢复备份和恢复中的工作负载。
"备份和恢复克隆管理员"	在备份和恢复中克隆应用程序和数据。
"备份和恢复查看器"	查看备份和恢复信息。
"灾难恢复管理员"	在NetApp Disaster Recovery服务中执行任何操作。
"灾难恢复故障转移管理员"	执行故障转移和迁移。
"灾难恢复应用程序管理员"	创建复制计划、更改复制计划并启动测试故障转移。
"灾难恢复查看器"	仅查看信息。
分类查看器	允许用户查看NetApp Data Classification扫描结果。具有此角色的用户可以查看合规性信息并生成他们有权访问的资源的报告。这些用户无法启用或禁用卷、存储桶或数据库模式的扫描。分类功能没有管理员角色。
"勒索软件抵御能力管理员"	管理NetApp Ransomware Resilience的“保护”、“警报”、“恢复”、“设置”和“报告”选项卡上的操作。
"勒索软件恢复力查看器"	在 Ransomware Resilience 中查看工作负载数据、查看警报数据、下载恢复数据和下载报告。
"勒索软件恢复用户行为管理员"	在勒索软件恢复中配置、管理和查看可疑用户行为检测、警报和监控。
"勒索软件恢复用户行为查看器"	查看勒索软件恢复中的可疑用户行为警报和见解。
SnapCenter管理员	提供使用NetApp Backup and Recovery从本地ONTAP集群备份应用程序快照的功能。具有此角色的成员可以完成以下操作：* 从“备份和恢复”>“应用程序”完成任何操作* 管理他们具有权限的项目和文件夹中的所有系统* 使用所有NetApp Console服务SnapCenter没有查看者角色。

相关链接

- "了解NetApp Console身份和访问管理"
- "开始使用NetApp Console IAM"
- "管理NetApp Console成员及其权限"
- "了解NetApp Console IAM 的 API"

为用户分配平台角色，以授予管理NetApp Console、分配角色、添加用户、创建控制台代理和管理联合的权限。

大型跨国组织的组织角色示例

XYZ 公司按地区（北美、欧洲和亚太地区）组织数据存储访问，从而提供区域控制和集中监督。

XYZ 公司控制台中的*组织管理员*为每个区域创建一个初始组织和单独的文件夹。每个区域的*文件夹或项目管理员*在该区域的文件夹中组织项目（及相关资源）。

具有“文件夹或项目管理员”角色的区域管理员通过添加资源和用户来主动管理他们的文件夹。这些区域管理员还可以添加、删除或重命名他们管理的文件夹和项目。*组织管理员*继承任何新资源的权限，保持整个组织的存储使用情况的可见性。

在同一个组织内，一名用户被分配了*联合管理员*角色来管理该组织与其企业 IdP 的联合。该用户可以添加或删除联合组织，但不能管理组织内的用户或资源。*组织管理员*为用户分配*联合查看者*角色，以检查联合状态并查看联合组织。

下表列出了每个控制台平台角色可以执行的操作。

组织管理角色

任务	组织管理员	文件夹或项目管理员
创建代理	是	否
从控制台创建、修改或删除系统（添加或发现系统）	是	是
创建文件夹和项目，包括删除	是	否
重命名现有文件夹和项目	是	是
分配角色并添加用户	是	是
将资源与文件夹和项目关联	是	是
将代理与文件夹和项目关联	是	否
从文件夹和项目中删除代理	是	否
管理代理（编辑证书、设置等）	是	否
从管理 > 凭证管理凭证	是	是
创建、管理和查看联合	是	否
通过控制台注册支持并提交案例	是	是
使用与显式访问角色无关的数据服务	是	是
查看审核页面和通知	是	是

联盟角色

任务	联盟管理员	联邦查看器
创建联盟	是	否

任务	联盟管理员	联邦查看器
验证域名	是	否
将域添加到联合	是	否
禁用和删除联盟	是	否
测试联盟	是	否
查看联盟及其详细信息	是	是

合作伙伴角色

任务	合作伙伴管理员	合作伙伴查看器
可以建立合作关系	是	否
为合作伙伴成员分配角色	是	否
可以向合作关系添加成员	是	否
可以查看组织合作关系详细信息	是	是

超级管理员和查看者角色

*超级管理员*角色提供管理控制台功能、存储和数据服务的完全访问权限。这个角色适合那些监督行政和治理的人。相比之下，“超级查看者”角色提供只读访问权限，非常适合需要查看信息而不进行更改的审计员或利益相关者。

组织应谨慎使用*超级管理员*访问权限，以最大限度地降低安全风险并符合最小特权原则。大多数组织应该分配具有必要权限的细粒度角色，以降低风险并提高可审计性。

超级角色示例

ABC 公司拥有一个由五人组成的小团队，利用NetApp Console进行数据服务和存储管理。他们没有分配多个角色，而是将“超级管理员”角色分配给两名高级团队成员，由他们负责所有管理任务，包括用户管理和资源配置。其余三名团队成员被分配了*超级查看者*角色，允许他们监控存储健康和数据服务状态，但无法修改设置。

角色	继承的角色
超级管理员	• 组织管理员 • 文件夹或项目管理员 • 联盟管理员 • 合作伙伴管理员 • 勒索软件抵御能力管理员 • 灾难恢复管理员 • 备份超级管理员 • 存储管理员 • Keystone管理员 • Google Cloud NetApp Volumes管理员
超级观众	• 组织查看器 • 联邦查看器 • 合作伙伴查看器 • 勒索软件恢复力查看器 • 灾难恢复查看器 • 备份查看器 • 存储查看器 • Keystone查看器 • Google Cloud NetApp Volumes查看器

应用程序角色

NetApp Console中的Google Cloud NetApp Volumes角色

您可以为用户分配以下角色，以便他们能够访问NetApp Console中的Google Cloud NetApp Volumes。

Google Cloud NetApp Volumes使用以下角色：

- * Google Cloud NetApp Volumes管理员*：在控制台中发现和管理Google Cloud NetApp Volumes 。
- * Google Cloud NetApp Volumes查看器*：在控制台中查看Google Cloud NetApp Volumes 。

NetApp Console中的Keystone访问角色

Keystone角色提供对Keystone仪表板的访问权限，并允许用户查看和管理他们的Keystone订阅。 Keystone角色有两种： Keystone管理员和Keystone查看者。这两个角色的主要区

别在于他们在Keystone中可以采取的行动。 Keystone管理员角色是唯一允许创建服务请求或修改订阅的角色。

NetApp Console中的**Keystone**角色示例

XYZ 公司有四名来自不同部门的存储工程师查看Keystone订阅信息。虽然所有这些用户都需要监控Keystone订阅，但只有团队负责人才被允许提出服务请求。团队中的三名成员被赋予 * Keystone查看者* 角色，而团队负责人被赋予 * Keystone管理员* 角色，以便对公司的服务请求进行控制。

下表列出了每个Keystone角色可以执行的操作。

特征和动作	**Keystone**管理员	**Keystone**查看器
查看以下选项卡：订阅、资产、监控和管理	是	是
* Keystone订阅页面*：		
查看订阅	是	是
修改或续订	是	否
* Keystone资产页面*：		
查看资产	是	是
管理资产	是	否
* Keystone警报页面*：		
查看警报	是	是
管理警报	是	否
为自己创建提醒	是	是
Licenses and subscriptions：		
可以查看许可证和订阅	是	是
* Keystone报告页面*：		
下载报告	是	是
管理报告	是	是
为自己创建报告	是	是
服务请求：		
创建服务请求	是	否

特征和动作	Keystone管理员	Keystone查看器
查看组织内任何用户创建的服务请求	是	是

NetApp Console的运营支持分析师访问角色

您可以将运营支持分析师角色分配给用户，以便他们能够访问警报和监控功能。具有此角色的用户还可以打开支持案例。

运营支持分析师

任务	可以执行
从“设置”>“凭证”管理自己的用户凭证	是
查看发现的资源	是
通过控制台注册支持并提交案例	是
查看审核页面和通知	是
查看、下载和配置警报	是

NetApp Console的存储访问角色

您可以为用户分配以下角色，以便他们访问NetApp Console中的存储管理功能。您可以为用户分配管理角色来管理存储或分配查看者角色来监控。

NetApp Console合作伙伴 API 不提供这些角色。

管理员可以为用户分配以下存储资源和功能的存储角色：

存储资源：

- 本地ONTAP集群
- StorageGRID
- E 系列

控制台服务和功能：

- 数字顾问
- 软件更新
- 生命周期规划
- 可持续性

NetApp Console中的存储角色示例

XYZ 公司是一家跨国公司，拥有庞大的存储工程师和存储管理员团队。它们允许该团队管理其所在地区的存储资产，同时限制对核心控制台任务（如用户管理、代理创建和许可证管理）的访问。

在一个由 12 人组成的团队中，有两名用户被赋予“存储查看者”角色，这使他们能够监控与他们被分配到的控制台项目相关的存储资源。其余九人被赋予*存储管理员*角色，包括管理软件更新、通过控制台访问ONTAP系统管理器以及发现存储资源（添加系统）的能力。团队中的一名成员被赋予*系统健康专家*角色，以便他们可以管理其所在区域的存储资源的健康状况，但不能修改或删除任何系统。此人还可以对其所分配项目的存储资源执行软件更新。

该组织还有两个具有“组织管理员”角色的用户，他们可以管理控制台的所有方面，包括用户管理、代理创建和许可证管理，还有几个具有“文件夹或项目管理员”角色的用户，他们可以对分配到的文件夹和项目执行控制台管理任务。

下表显示了每个存储角色执行的操作。

特征和动作	存储管理员	系统健康专家	存储查看器
存储管理：			
发现新资源（创建系统）	是	是	否
查看发现的系统	是	是	否
从控制台删除系统	是	否	否
修改系统	是	否	否
创建代理	否	否	否
数字顾问			
查看所有页面和功能	是	是	是
Licenses and subscriptions			
查看所有页面和功能	否	否	否
软件更新			
查看登陆页面和建议	是	是	是
审查潜在的版本建议和主要优点	是	是	是
查看集群的更新详细信息	是	是	是
运行更新前检查并下载升级计划	是	是	是
安装软件更新	是	是	否
生命周期规划			
审查容量规划状态	是	是	是

特征和动作	存储管理员	系统健康专家	存储查看器
选择下一步行动（最佳实践、层级）	是	否	否
将冷数据分层到云存储并释放存储空间	是	是	否
设置提醒	是	是	是
可持续性			
查看仪表板和建议	是	是	是
下载报告数据	是	是	是
编辑碳减排百分比	是	是	否
修复建议	是	是	否
推迟建议	是	是	否
系统管理员访问			
可以输入凭证	是	是	否
证书			
用户凭据	是	是	否

数据服务角色

NetApp Console中的NetApp Backup and Recovery角色

您可以为用户分配以下角色，以便他们访问控制台内的NetApp Backup and Recovery 。备份和恢复角色使您可以灵活地为用户分配特定于他们需要在组织内完成的任务的角色。如何分配角色取决于您自己的业务和存储管理实践。

该服务使用特定于NetApp Backup and Recovery 的以下角色。

- 备份和恢复超级管理员：在NetApp Backup and Recovery中执行任何操作。
- 备份和恢复备份管理员：在NetApp Backup and Recovery中执行备份到本地快照、复制到二级存储以及备份到对象存储操作。
- 备份和恢复恢复管理员：使用NetApp Backup and Recovery恢复工作负载。
- 备份和恢复克隆管理：使用NetApp Backup and Recovery克隆应用程序和数据。
- 备份和恢复查看器：查看NetApp Backup and Recovery中的信息，但不执行任何操作。

有关所有NetApp Console访问角色的详细信息，请参阅 "控制台设置和管理文档"。

用于常见操作的角色

下表列出了每个NetApp Backup and Recovery角色可以针对所有工作负载执行的操作。

特征和动作	备份和恢复超级管理员	备份和恢复备份管理员	备份和恢复恢复管理员	备份和恢复克隆管理员	备份和恢复查看器
添加、编辑或删除主机	是	否	否	否	否
安装插件	是	否	否	否	否
添加凭据（主机、实例、vCenter）	是	否	否	否	否
查看仪表板和所有选项卡	是	是	是	是	是
开始免费试用	是	否	否	否	否
启动工作负载发现	否	是	是	是	否
查看许可证信息	是	是	是	是	是
激活许可证	是	否	否	否	否
查看主机	是	是	是	是	是
时间表：					
激活计划	是	是	是	是	否
暂停时间表	是	是	是	是	否
政策与保护：					
查看保护计划	是	是	是	是	是
创建、修改或删除保护计划	是	是	否	否	否
恢复工作负载	是	否	是	否	否
创建、拆分或删除克隆	是	否	否	是	否
创建、修改或删除策略	是	是	否	否	否
报告：					
查看报告	是	是	是	是	是

特征和动作	备份和恢复超级管理员	备份和恢复备份管理员	备份和恢复恢复管理员	备份和恢复克隆管理员	备份和恢复查看器
创建报告	是	是	是	是	否
删除报告	是	否	否	否	否
从**SnapCenter**导入并管理主机：					
查看导入的SnapCenter数据	是	是	是	是	是
从SnapCenter导入数据	是	是	否	否	否
管理（迁移）主机	是	是	否	否	否
配置设置：					
配置日志目录	是	是	是	否	否
关联或删除实例凭证	是	是	是	否	否
桶：					
查看存储桶	是	是	是	是	是
创建、编辑或删除存储桶	是	是	否	否	否

用于特定于工作负载的操作的角色

下表列出了每个NetApp Backup and Recovery角色可以针对特定工作负载执行的操作。

Kubernetes 工作负载

该表显示了每个NetApp Backup and Recovery角色可以针对特定于 Kubernetes 工作负载的操作执行的操作。

特征和动作	备份和恢复超级管理员	备份和恢复备份管理员	备份和恢复恢复管理员	备份和恢复查看器
查看集群、命名空间、存储类别和 API 资源	是	是	是	是
添加新的 Kubernetes 集群	是	是	否	否
更新集群配置	是	否	否	否
从管理中删除集群	是	否	否	否
查看应用程序	是	是	是	是

特征和动作	备份和恢复超级管理员	备份和恢复备份管理员	备份和恢复恢复管理员	备份和恢复查看器
创建和定义新的应用程序	是	是	否	否
更新应用程序配置	是	是	否	否
从管理中删除应用程序	是	是	否	否
查看受保护的资源和备份状态	是	是	是	是
创建备份并使用策略保护应用程序	是	是	否	否
取消保护应用程序并删除备份	是	是	否	否
查看恢复点和资源查看器结果	是	是	是	是
从恢复点还原应用程序	是	否	是	否
查看 Kubernetes 备份策略	是	是	是	是
创建 Kubernetes 备份策略	是	是	是	否
更新备份策略	是	是	是	否
删除备份策略	是	是	是	否
查看执行钩子和钩子源	是	是	是	是
创建执行钩子和钩子源	是	是	是	否
更新执行钩子和钩子源	是	是	是	否
删除执行钩子和钩子源	是	是	是	否
查看执行钩子模板	是	是	是	是
创建执行钩子模板	是	是	是	否
更新执行钩子模板	是	是	是	否
删除执行钩子模板	是	是	是	否

特征和动作	备份和恢复超级管理员	备份和恢复备份管理员	备份和恢复恢复管理员	备份和恢复查看器
查看工作负载摘要和分析仪表板	是	是	是	是
查看StorageGRID存储桶和存储目标	是	是	是	是

NetApp Console中的NetApp Disaster Recovery角色

您可以为用户分配以下角色，以便他们访问控制台内的NetApp Disaster Recovery。灾难恢复角色使您可以灵活地为用户分配特定于他们需要在组织内完成的任务的角色。如何分配角色取决于您自己的业务和存储管理实践。

灾难恢复使用以下角色：

- 灾难恢复管理员：执行任何操作。
- 灾难恢复故障转移管理：执行故障转移和迁移。
- 灾难恢复应用程序管理员：创建复制计划。修改复制计划。开始测试故障转移。
- 灾难恢复查看器：仅查看信息。

下表列出了每个角色可以执行的操作。

特征和动作	灾难恢复管理员	灾难恢复故障转移管理员	灾难恢复应用程序管理员	灾难恢复查看器
查看仪表板和所有选项卡	是	是	是	是
开始免费试用	是	否	否	否
启动工作负载发现	是	否	否	否
查看许可证信息	是	是	是	是
激活许可证	是	否	是	否
在“站点”选项卡上：				
查看网站	是	是	是	是
添加、修改或删除站点	是	否	否	否
在复制计划选项卡上：				
查看复制计划	是	是	是	是
查看复制计划详细信息	是	是	是	是

特征和动作	灾难恢复管理员	灾难恢复故障转移管理员	灾难恢复应用程序管理员	灾难恢复查看器
创建或修改复制计划	是	是	是	否
创建报告	是	否	否	否
查看快照	是	是	是	是
执行故障转移测试	是	是	是	否
执行故障转移	是	是	否	否
执行故障回复	是	是	否	否
执行迁移	是	是	否	否
在资源组选项卡上：				
查看资源组	是	是	是	是
创建、修改或删除资源组	是	否	是	否
在“作业监控”选项卡上：				
查看职位	是	否	是	是
取消作业	是	是	是	否

NetApp Console的勒索软件恢复访问角色

勒索软件恢复角色为用户提供对NetApp Ransomware Resilience的访问权限。勒索软件恢复能力支持以下角色：

基线角色

- 勒索软件恢复管理员 - 配置勒索软件恢复设置；调查并响应加密警报
- 勒索软件恢复力查看器 - 查看加密事件、报告和发现设置

用户行为活动角色"可疑用户活动检测"警报提供对文件活动事件等数据的可见性；这些警报包括文件名和用户执行的文件操作（例如读取、写入、删除、重命名）。为了限制这些数据的可见性，只有具有这些角色的用户才能管理或查看这些警报。

- 勒索软件恢复用户行为管理员 - 激活可疑用户活动检测，调查并响应可疑用户活动警报
- 勒索软件恢复用户行为查看器 - 查看可疑用户活动警报

用户行为角色不是独立角色；它们旨在添加到勒索软件恢复管理员或查看者角色中。有关详细信息，请参阅 [用户行为角色]。

有关每个角色的详细描述，请参阅下表。

基线角色

下表描述了勒索软件恢复管理员和查看者角色可执行的操作。

特征和动作	勒索软件抵御能力管理员	勒索软件恢复力查看器
查看仪表板和所有选项卡	是	是
在仪表板上更新推荐状态	是	否
开始免费试用	是	否
启动工作负载发现	是	否
启动工作负载的重新发现	是	否
在“保护”选项卡上：		
添加、修改或删除加密策略的保护计划	是	否
保护工作负载	是	否
通过数据分类识别敏感数据的暴露	是	否
列出保护计划和细节	是	是
列出保护组	是	是
查看保护组详细信息	是	是
创建、编辑或删除保护组	是	否
下载数据	是	是
在“警报”选项卡上：		
查看加密警报和警报详细信息	是	是
编辑加密事件状态	是	否

特征和动作	勒索软件抵御能力管理员	勒索软件恢复力查看器
标记加密警报以供恢复	是	否
查看加密事件详细信息	是	是
解除或解决加密事件	是	否
获取加密事件中受影响文件的完整列表	是	否
下载加密事件警报数据	是	是
阻止用户（使用工作负载安全代理配置）	是	否
在“恢复”选项卡上：		
下载加密事件中受影响的文件	是	否
从加密事件中恢复工作负载	是	否
从加密事件下载恢复数据	是	是
下载加密事件报告	是	是
在“设置”选项卡上：		
添加或修改备份目标	是	否
列出备份目的地	是	是
查看已连接的 SIEM 目标	是	是
添加或修改 SIEM 目标	是	否
配置准备演练	是	否
开始、重置或编辑准备情况演练	是	否
审查准备演习状态	是	是
更新发现配置	是	否
查看发现配置	是	是
在“报告”选项卡上：		

特征和动作	勒索软件抵御能力管理员	勒索软件恢复力查看器
下载报告	是	是

用户行为角色

要配置可疑用户行为设置并响应警报，用户必须具有勒索软件恢复用户行为管理员角色。要仅查看可疑用户行为警报，用户应具有勒索软件恢复用户行为查看者角色。

应将用户行为角色授予具有现有勒索软件恢复管理员或查看者权限且需要访问"可疑用户活动设置和警报"。例如，具有勒索软件恢复管理员角色的用户应该获得勒索软件恢复用户行为管理员角色来配置用户活动代理并阻止或解除阻止用户。不应将勒索软件恢复用户行为管理员角色授予勒索软件恢复查看者。

要激活可疑用户活动检测，您必须具有控制台组织管理员角色。

下表描述了勒索软件恢复用户行为管理员和查看者角色可执行的操作。

特征和动作	勒索软件恢复用户行为管理员	勒索软件恢复用户行为查看器
在“设置”选项卡上：		
创建、修改或删除用户活动代理	是	否
创建或删除用户目录连接器	是	否
暂停或恢复数据收集器	是	否
进行数据泄露准备演习	是	否
在“保护”选项卡上：		
添加、修改或删除可疑用户行为策略的保护计划	是	否
在“警报”选项卡上：		
查看用户活动警报和警报详细信息	是	是
编辑用户活动事件状态	是	否
标记用户活动警报以供恢复	是	否
查看用户活动事件详细信息	是	是
解除或解决用户活动事件	是	否
获取可疑用户受影响文件的完整列表	是	是

特征和动作	勒索软件恢复用户行为管理员	勒索软件恢复用户行为查看器
下载用户活动事件警报数据	是	是
阻止或取消阻止用户	是	否
在“恢复”选项卡上：		
下载用户活动事件受影响的文件	是	否
从用户活动事件恢复工作负载	是	否
从用户活动事件下载恢复数据	是	是
从用户活动事件下载报告	是	是

身份和访问 API

组织和项目 ID

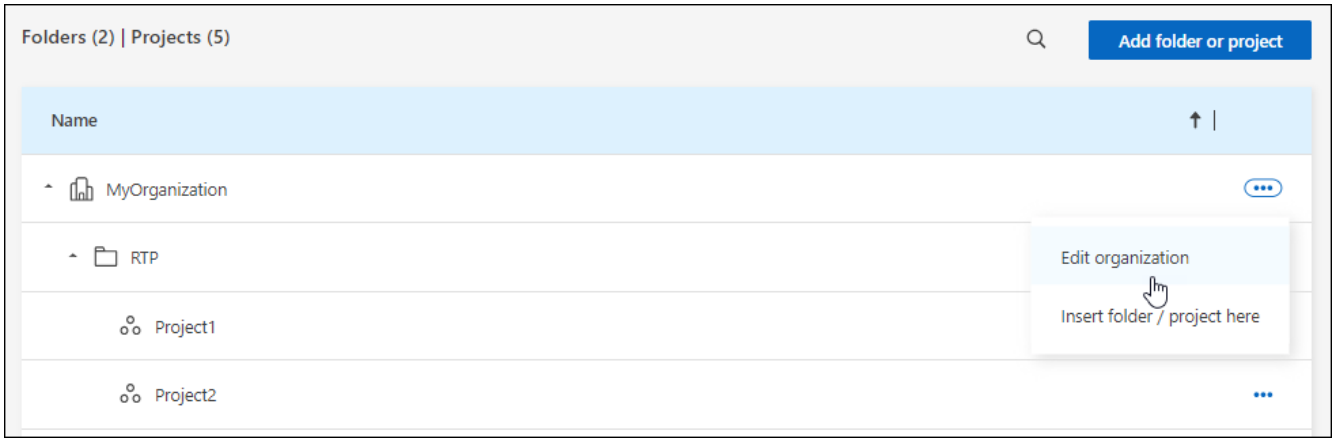
您的NetApp Console组织有一个名称和一个 ID。您可以为您的组织选择一个名称以帮助识别它。您可能还需要检索某些集成的组织 ID。

重命名您的组织

您可以重命名您的组织。如果您支持的不仅仅是组织，这将很有帮助。

步骤

1. 选择*管理>身份和访问*。
2. 选择*组织*。
3. 从“组织”页面，导航到表格的第一行，选择 ••• 然后选择*编辑组织*。



4. 输入新的组织名称并选择*应用*。

获取组织 ID

组织 ID 用于与控制台的某些集成。

您可以从组织页面查看组织 ID，并根据需要将其复制到剪贴板。

步骤

1. 选择*管理>身份和访问*>*组织*。
2. 在*组织*页面上，在摘要栏中查找您的组织 ID 并将其复制到剪贴板。您可以保存它以供以后使用，或者直接将其复制到需要使用它的地方。

获取项目ID

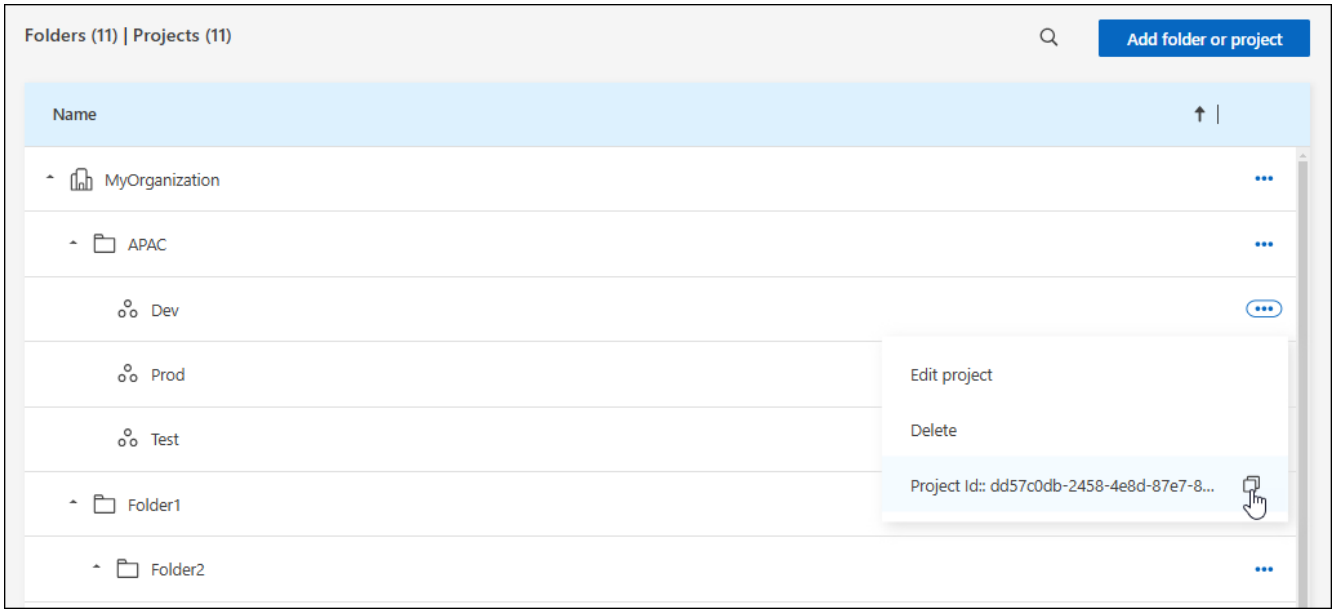
如果您使用 API，则需要获取项目的 ID。例如，创建Cloud Volumes ONTAP系统时。

步骤

1. 从“组织”页面，导航到表中的项目并选择 •••

   显示项目 ID。

2. 要复制 ID，请选择复制按钮。



相关信息

- "了解身份和访问管理"
- "开始使用身份和访问权限"
- "了解身份和访问 API"

安全与合规

身份联合

使用NetApp Console的身份联合实现单点登录

单点登录（联合）允许用户使用其公司凭证登录NetApp Console，从而简化了登录过程并增强了安全性。您可以使用身份提供商 (IdP) 或NetApp支持站点启用单点登录 (SSO)。

所需角色

组织管理员、联盟管理员、联盟查看器。"了解有关访问角色的更多信息。"

使用 NetApp Support Site 单点登录

与NetApp支持站点联合允许用户使用相同的凭据登录控制台、 Active IQ Digital Advisor和其他相关应用程序。

如果您与NetApp支持站点联合，则您不能与您的企业身份管理提供商联合。选择最适合您组织的一种。

步骤

1. 下载并完成 "NetApp联合申请表"。
2. 将表格提交至表格中指定的电子邮件地址。

   NetApp支持团队将审核并处理您的请求。

使用身份提供程序单一登录

您可以与身份提供商建立联合连接，以启用控制台的单点登录 (SSO)。该过程涉及配置您的身份提供商以信任NetApp作为服务提供商，然后在控制台中创建连接。

如果您之前使用NetApp Cloud Central（控制台的外部应用程序）配置了联合，则需要使用联合页面导入联合以在控制台内进行管理。"了解如何导入您的联盟。"

支持的身份提供者

NetApp支持以下联合协议和身份提供程序：

协议

- 安全断言标记语言 (SAML) 身份提供者
- Active Directory 联合身份验证服务 (AD FS)

身份提供者

- 微软Entra ID
- Ping联邦

与NetApp Console联合工作流程

NetApp仅支持服务提供商发起的（SP发起的） SSO。您需要首先配置身份提供者以信任NetApp作为服务提供商。然后，您可以在控制台中创建使用身份提供者配置的连接。

您可以与您的电子邮件域或您拥有的其他域联合。要与不同于您的电子邮件域的域联合，请首先验证您拥有该域。


验证您的域名（如果不使用您的电子邮件域名）

要与不同于您的电子邮件域的域联合，请验证您拥有该域。您无需任何额外步骤即可联合您的电子邮件域。


配置您的 **IdP** 以信任**NetApp**作为服务提供商

通过创建新应用程序并提供 ACS URL、实体 ID 或其他凭证信息等详细信息，将您的身份提供商配置为信任NetApp 。服务提供商信息因身份提供商而异，因此请参阅特定身份提供商的文档以了解详细信息。您需要与您的 IdP 管理员合作来完成此步骤。


在控制台中创建联合连接

提供来自身份提供商的 SAML 元数据 URL 或文件以创建连接。此信息用于建立控制台和您的身份提供者之间的信任关系。您提供的信息取决于您使用的 IdP。例如，如果您使用 Microsoft Entra ID，则需要提供客户端 ID、密钥和域。


在控制台中测试您的联盟

在启用联合连接之前对其进行测试。使用控制台中联合页面上的测试选项来验证您的测试用户是否可以成功进行身份验证。如果测试成功，则可以启用连接。


在控制台中启用您的连接

启用连接后，用户可以使用其公司凭证登录控制台。

查看相应协议或 IdP 的主题以开始：

- "与 AD FS 设置联合连接"
- "与 Microsoft Entra ID 建立联合连接"
- "使用 PingFederate 设置联合连接"
- "与 SAML 身份提供商建立联合连接"

域验证

验证联合连接的电子邮件域

如果您想要与不同于您的电子邮件域的域联合，您必须首先验证您拥有该域。您只能使用已验证的域进行联合。

必需角色

需要联盟管理员角色来创建和管理联盟。联盟查看者可以查看联盟页面。"了解有关访问角色的更多信息。"

验证您的域名涉及向您的域名的 DNS 设置添加 TXT 记录。此记录用于证明您拥有该域并允许NetApp Console

信任该域进行联合。您可能需要与您的 IT 或网络管理员协调来完成此步骤。

步骤

1. 选择*管理>身份和访问*。
2. 选择“**Federation**”以查看“**Federations**”页面。
3. 选择*配置新联合*。
4. 选择*验证域名所有权*。
5. 输入您要验证的域名并选择*继续*。
6. 复制提供的 TXT 记录。
7. 转到您域的 DNS 设置并配置作为您域的 TXT 记录提供的 TXT 值。如果需要，请与您的 IT 或网络管理员合作。
8. 添加TXT记录后，返回控制台并选择*验证*。

配置联合

将**NetApp Console**与 **Active Directory** 联合服务 **(AD FS)** 联合起来

将您的 Active Directory 联合身份验证服务 (AD FS) 与NetApp Console联合起来，以便为NetApp Console启用单点登录 (SSO)。这允许用户使用他们的公司凭证登录控制台。

必需角色

需要联盟管理员角色来创建和管理联盟。联盟查看者可以查看联盟页面。"了解有关访问角色的更多信息。"

您可以与您的企业 IdP 或NetApp支持站点联合。 NetApp建议选择其中一个，但不要同时选择两者。

NetApp仅支持服务提供商发起的（SP发起的） SSO。首先，配置身份提供者以信任NetApp Console作为服务提供者。然后，使用您的身份提供商的配置在控制台中创建连接。

您可以与 AD FS 服务器建立联合，以启用NetApp Console的单点登录 (SSO)。该过程涉及配置您的 AD FS 以信任控制台作为服务提供商，然后在NetApp Console中创建连接。

步骤

1. 选择*管理>身份和访问*。
2. 选择“**Federation**”以查看“**Federations**”页面。
3. 选择*配置新联合*。
4. 输入您的域名详细信息：
   a. 选择您是否要使用已验证的域名或您的电子邮件域名。电子邮件域是与您登录的帐户关联的域。
   b. 输入您正在配置的联盟的名称。
   c. 如果您选择已验证的域，请从列表中选择该域。
5. 选择“下一步”。
6. 对于您的连接方法，选择*协议*，然后选择*Active Directory 联合身份验证服务 (AD FS)*。

7. 选择“下一步”。
8. 在您的 AD FS 服务器中创建依赖方信任。您可以使用 PowerShell 或在 AD FS 服务器上手动配置它。有关如何创建信赖方信任的详细信息，请参阅 AD FS 文档。

    a. 使用以下脚本通过 PowerShell 创建信任：

    ```
    (new-object Net.WebClient -property @{Encoding = [Text.Encoding]
    ::UTF8}).DownloadString("https://raw.github.com/auth0/AD FS-
    auth0/master/AD FS.ps1") | iex
    AddRelyingParty "urn:auth0:netapp-cloud-account" "https://netapp-
    cloud-account.auth0.com/login/callback"
    ```

    b. 或者，您可以在 AD FS 管理控制台中手动创建信任。创建信任时使用以下NetApp Console值：

    - 创建依赖信任标识符时，使用 **YOUR_TENANT** 值： `netapp-cloud-account`
    - 当您选择 启用对 **WS-Federation** 的支持 时，请使用 **YOUR_AUTH0_DOMAIN** 值： `netapp-cloud-account.auth0.com`

    c. 创建信任后，从 AD FS 服务器复制元数据 URL 或下载联合元数据文件。您需要此 URL 或文件来完成控制台中的连接。

    NetApp建议使用元数据 URL 让NetApp Console自动检索最新的 AD FS 配置。如果您下载联合元数据文件，则每当 AD FS 配置发生更改时，都需要在NetApp Console中手动更新它。

9. 返回控制台，然后选择“下一步”来创建连接。
10. 创建与 AD FS 的连接。

    a. 输入您在上一步中从 AD FS 服务器复制的 **AD FS URL** 或上传您从 AD FS 服务器下载的联合元数据文件。

11. 选择*创建连接*。建立连接可能需要几秒钟。
12. 选择“下一步”。
13. 选择*测试连接*来测试您的连接。您将被引导至 IdP 服务器的登录页面。使用您的身份提供商凭据登录。登录后，返回控制台启用连接。

    在受限模式下使用控制台时，请将 URL 复制到隐身浏览器窗口或单独的浏览器中，以登录到您的身份提供商 (IdP)。

14. 在控制台中，选择“下一步”以查看摘要页面。
15. 设置通知。

    您可以选择七天或三十天。系统会通过电子邮件向具有以下角色的任何用户发送到期通知，并在控制台中显示这些通知：超级管理员、组织管理员、联盟管理员和联盟查看者。

16. 查看联盟详细信息，然后选择“启用联盟”。
17. 选择“完成”以完成该过程。

启用联合身份验证后，用户可以使用其企业凭据登录NetApp Console。

与您的 Microsoft Entra ID IdP 提供商联合，为NetApp Console启用单点登录 (SSO)。这允许用户使用他们的公司凭证登录。

必需角色

需要联盟管理员角色来创建和管理联盟。联盟查看者可以查看联盟页面。"了解有关访问角色的更多信息。"

> 您可以与您的企业 IdP 或NetApp支持站点联合。 NetApp建议选择其中一个，但不要同时选择两者。

NetApp仅支持服务提供商发起的（SP发起的） SSO。您需要首先配置身份提供者以信任NetApp作为服务提供商。然后，您可以在控制台中创建使用身份提供者配置的连接。

您可以与 Microsoft Entra ID 建立联合连接，以启用控制台的单点登录 (SSO)。该过程涉及配置您的 Microsoft Entra ID 以信任控制台作为服务提供商，然后在控制台中创建连接。

步骤

1. 选择*管理>身份和访问*。
2. 选择“**Federation**”以查看“**Federations**”页面。
3. 选择*配置新联合*。

域名详细信息

1. 输入您的域名详细信息：
   a. 选择您是否要使用已验证的域名或您的电子邮件域名。电子邮件域是与您登录的帐户关联的域。
   b. 输入您正在配置的联盟的名称。
   c. 如果您选择已验证的域，请从列表中选择该域。
2. 选择“下一步”。

连接方法

1. 对于您的连接方法，选择*提供商*，然后选择*Microsoft Entra ID*。
2. 选择“下一步”。

配置说明

1. 配置您的 Microsoft Entra ID 以信任NetApp作为服务提供商。您需要在 Microsoft Entra ID 服务器上执行此步骤。
   a. 注册 Microsoft Entra ID 应用程序以信任控制台时，请使用以下值：
      - 对于 重定向 **URL** ，使用 `https://services.cloud.netapp.com`
      - 对于 回复 **URL**，使用 `https://netapp-cloud-account.auth0.com/login/callback`
   b. 为您的 Microsoft Entra ID 应用创建客户端机密。您需要提供客户端 ID、客户端密钥和 Entra ID 域名来完成联合。

2. 返回控制台，然后选择“下一步”来创建连接。

创建连接

1. 使用 Microsoft Entra ID 创建连接
   a. 输入您在上一步中创建的客户端 ID 和客户端密钥。
   b. 输入 Microsoft Entra ID 域名。
2. 选择*创建连接*。系统在几秒钟内建立连接。

测试并启用连接

1. 选择“下一步”。
2. 选择*测试连接*来测试您的连接。您将被引导至 IdP 服务器的登录页面。使用您的身份提供商凭据登录。登录后，返回控制台启用连接。

   在受限模式下使用控制台时，请将 URL 复制到隐身浏览器窗口或单独的浏览器中，以登录到您的身份提供商 (IdP)。

3. 在控制台中，选择“下一步”以查看摘要页面。
4. 设置通知。

   您可以选择七天或三十天。系统会通过电子邮件向具有以下角色的任何用户发送到期通知，并在控制台中显示这些通知：超级管理员、组织管理员、联盟管理员和联盟查看者。

5. 查看联盟详细信息，然后选择“启用联盟”。
6. 选择“完成”以完成该过程。

启用联合身份验证后，用户可以使用其企业凭据登录NetApp Console。

使用 **PingFederate** 联合**NetApp Console**

与您的 PingFederate IdP 提供商联合，为NetApp Console启用单点登录 (SSO)。这允许用户使用他们的公司凭证登录。

必需角色

需要联盟管理员角色来创建和管理联盟。联盟查看者可以查看联盟页面。"了解有关访问角色的更多信息。"

您可以与您的企业 IdP 或NetApp支持站点联合。 NetApp建议选择其中一个，但不要同时选择两者。

NetApp仅支持服务提供商发起的（SP发起的） SSO。您需要首先配置身份提供者以信任NetApp作为服务提供商。然后，您可以在控制台中创建使用身份提供者配置的连接。

您可以使用 PingFederate 设置联合连接，以启用控制台的单点登录 (SSO)。该过程涉及配置您的 PingFederate 服务器以信任控制台作为服务提供商，然后在控制台中创建连接。

步骤

1. 选择*管理>身份和访问*。
2. 选择“**Federation**”以查看“**Federations**”页面。
3. 选择*配置新联合*。
4. 输入您的域名详细信息：
   a. 选择您是否要使用已验证的域名或您的电子邮件域名。电子邮件域是与您登录的帐户关联的域。
   b. 输入您正在配置的联盟的名称。
   c. 如果您选择已验证的域，请从列表中选择该域。
5. 选择“下一步”。
6. 对于您的连接方法，选择*提供商*，然后选择*PingFederate*。
7. 选择“下一步”。
8. 配置您的 PingFederate 服务器以信任NetApp作为服务提供商。您需要在 PingFederate 服务器上执行此步骤。
   a. 配置 PingFederate 以信任NetApp Console时，请使用以下值：
      - 对于 回复 **URL** 或 断言消费者服务 **(ACS) URL**，使用 `https://netapp-cloud-account.auth0.com/login/callback`
      - 对于*注销 URL*，使用 `https://netapp-cloud-account.auth0.com/logout`
      - 对于*受众/实体 ID*，使用 `urn:auth0:netapp-cloud-account:<fed-domain-name-saml>`其中 `<fed-domain-name-pingfederate>` 是联合的域名。例如，如果您的域名是 `example.com`，受众/实体 ID 将是 `urn:auth0:netappcloud-account:fed-example-com-pingfederate`。
   b. 复制 PingFederate 服务器 URL。在控制台中创建连接时，您将需要此 URL。
   c. 从您的 PingFederate 服务器下载 X.509 证书。它需要采用 Base64 编码的 PEM 格式（.pem、.crt、.cer）。
9. 返回控制台，然后选择“下一步”来创建连接。
10. 使用 PingFederate 创建连接
    a. 输入您在上一步中复制的 PingFederate 服务器 URL。
    b. 上传 X.509 签名证书。证书必须采用 PEM、CER 或 CRT 格式。
11. 选择*创建连接*。系统在几秒钟内建立连接。
12. 选择“下一步”。
13. 选择*测试连接*来测试您的连接。您将被引导至 IdP 服务器的登录页面。使用您的身份提供商凭据登录。登录后，返回控制台启用连接。

    在受限模式下使用控制台时，请将 URL 复制到隐身浏览器窗口或单独的浏览器中，以登录到您的身份提供商 (IdP)。

14. 在控制台中，选择“下一步”以查看摘要页面。
15. 设置通知。

    您可以选择七天或三十天。系统会通过电子邮件向具有以下角色的任何用户发送到期通知，并在控制台中显

示这些通知：超级管理员、组织管理员、联盟管理员和联盟查看者。

16. 查看联盟详细信息，然后选择“启用联盟”。
17. 选择“完成”以完成该过程。

启用联合身份验证后，用户可以使用其企业凭据登录NetApp Console。

与 **SAML** 身份提供商联合

与您的 SAML 2.0 IdP 提供商联合，为 NEtApp 控制台启用单点登录 (SSO)。这允许用户使用他们的公司凭证登录。

所需角色

需要联盟管理员角色来创建和管理联盟。联盟查看者可以查看联盟页面。"了解有关访问角色的更多信息。"

您可以与您的企业 IdP 或NetApp支持站点联合。你不能与两者结成联盟。

NetApp仅支持服务提供商发起的（SP发起的） SSO。您需要首先配置身份提供者以信任NetApp作为服务提供商。然后，您可以在控制台中创建使用身份提供者配置的连接。

您可以与 SAML 2.0 提供商建立联合连接，以便为控制台启用单点登录 (SSO)。该过程涉及配置您的提供商以信任NetApp作为服务提供商，然后在控制台中创建连接。

步骤

1. 选择*管理>身份和访问*。
2. 选择“**Federation**”以查看“**Federations**”页面。
3. 选择*配置新联合*。
4. 输入您的域名详细信息：
   a. 选择您是否要使用已验证的域名或您的电子邮件域名。电子邮件域是与您登录的帐户关联的域。
   b. 输入您正在配置的联盟的名称。
   c. 如果您选择已验证的域，请从列表中选择该域。
5. 选择“下一步”。
6. 对于您的连接方法，选择*协议*，然后选择*SAML 身份提供者*。
7. 选择“下一步”。
8. 配置您的 SAML 身份提供商以信任NetApp作为服务提供商。您需要在 SAML 提供商服务器上执行此步骤。
   a. 确保您的 IdP 具有属性 `email`设置为用户的电子邮件地址。这是控制台正确识别用户所必需的：

```
<saml:AttributeStatement
xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <saml:Attribute Name="email"
NameFormat="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName">
        <saml:AttributeValue
xsi:type="xs:string">email@domain.com</saml:AttributeValue>
    </saml:Attribute>
</saml:AttributeStatement>
```

1. 在控制台中注册 SAML 应用程序时，请使用以下值：
   - 对于 回复 **URL** 或 断言消费者服务 **(ACS) URL**，使用 `https://netapp-cloud-account.auth0.com/login/callback`
   - 对于*注销 URL*，使用 `https://netapp-cloud-account.auth0.com/logout`
   - 对于*受众/实体 ID*，使用 `urn:auth0:netapp-cloud-account:<fed-domain-name-saml>`其中 `<fed-domain-name-saml>` 是您想要用于联合的域名。例如，如果您的域名是 `example.com`，受众/实体 ID 将是 `urn:auth0:netapp-cloud-account:fed-example-com-samlp`。
2. 创建信任后，从 SAML 提供商服务器复制以下值：
   - 登录网址
   - 退出 URL（可选）
3. 从您的 SAML 提供商服务器下载 X.509 证书。它需要采用 PEM、CER 或 CRT 格式。
   a. 返回控制台，然后选择“下一步”来创建连接。
   b. 使用 SAML 创建连接。
4. 输入您的 SAML 服务器的 登录 **URL**。
5. 上传从 SAML 提供商服务器下载的 X.509 证书。
6. 或者，输入您的 SAML 服务器的 退出 **URL**。
   a. 选择*创建连接*。系统在几秒钟内建立连接。
   b. 选择“下一步”。
   c. 选择*测试连接*来测试您的连接。您将被引导至 IdP 服务器的登录页面。使用您的身份提供商凭据登录。登录后，返回控制台启用连接。

      在受限模式下使用控制台时，请将 URL 复制到隐身浏览器窗口或单独的浏览器中，以登录到您的身份提供商 (IdP)。

   d. 在控制台中，选择“下一步”以查看摘要页面。
   e. 设置通知。

      您可以选择七天或三十天。系统会通过电子邮件向具有以下角色的任何用户发送到期通知，并在控制台中显示这些通知：超级管理员、组织管理员、联盟管理员和联盟查看者。

f. 查看联盟详细信息，然后选择“启用联盟”。

g. 选择“完成”以完成该过程。

启用联合身份验证后，用户可以使用其企业凭据登录NetApp Console。

管理联盟

在NetApp Console中管理联合

您可以在NetApp Console中管理您的联合。您可以禁用它，更新过期的凭据，以及在不再需要它时禁用它。

必需角色

需要联盟管理员角色来创建和管理联盟。联盟查看者可以查看联盟页面。"了解有关访问角色的更多信息。"

您还可以向现有联盟添加额外的已验证域，从而允许您为联盟连接使用多个域。

- 如果您使用NetApp Cloud Central 配置了联合，请通过 **Federation** 页面导入它以在控制台中进行管理。"了解如何导入您的联盟"
- 您可以在“审核”页面上查看联盟管理事件，例如启用、禁用和更新联盟。 "了解有关在NetApp Console中监控操作的更多信息。"

启用联盟

如果您已经创建了联盟但尚未启用，您可以通过*联盟*页面启用它。启用联合允许与联合关联的用户使用其公司凭据登录控制台。在启用联合之前，请先成功创建并测试联合。

步骤

1. 选择*管理>身份和访问*。
2. 选择“**Federation**”选项卡。
3. 选择操作菜单 ••• 旁边的您想要启用的联盟并选择*启用*。

将已验证的域添加到现有联合

您可以在控制台中将已验证的域添加到现有联合，以便使用具有相同身份提供商 (IdP) 的多个域。

您必须先在控制台中验证该域，然后才能将其添加到联合中。如果您尚未验证域名，可以按照以下步骤进行验证"在控制台中验证您的域"。

步骤

1. 选择*管理>身份和访问*。
2. 选择“**Federation**”选项卡。
3. 选择操作菜单 ⋮ 在您要添加已验证域的联盟旁边，然后选择*更新域*。 *更新域*对话框显示已与此联合关联的域。
4. 从可用域列表中选择一个已验证的域。
5. 选择*更新*。新域用户可以在 30 秒内获得联合控制台访问权限。

更新即将到期的联合连接

您可以在控制台中更新联合的详细信息。例如，如果证书或客户端机密等凭证过期，则需要更新联合。在需要时，更新通知日期以提醒您在连接到期之前更新连接。

在更新您的 IdP 之前，请先更新控制台以避免登录问题。在此过程中保持登录控制台。

步骤

1. 选择*管理>身份和访问*。
2. 选择“**Federation**”选项卡。
3. 选择要更新的联合旁边的操作菜单（三个垂直点），然后选择*更新联合*。
4. 根据需要更新联盟的详细信息。
5. 选择*更新*。

测试现有的联盟

测试现有联合的连接以验证其是否正常工作。这可以帮助您识别联盟中的任何问题并进行故障排除。

步骤

1. 选择*管理>身份和访问*。
2. 选择“**Federation**”选项卡。
3. 选择操作菜单旁边的您想要添加已验证域的联盟，然后选择*测试连接*。
4. 选择*测试*。系统提示您使用公司凭证登录。如果连接成功，您将被重定向到NetApp Console。如果连接失败，您会看到一条错误消息，表明联合存在问题。
5. 选择“完成”返回“联合”选项卡。

禁用联合

如果您不再需要联合，您可以禁用它。这可以防止与联盟关联的用户使用其公司凭证登录控制台。如果需要，您可以稍后重新启用联合。

在删除联合之前，请先禁用它，例如在停用 IdP 或停止联合时。如果需要的话，您可以稍后重新启用它。

步骤

1. 选择*管理>身份和访问*。
2. 选择“**Federation**”选项卡。
3. 选择操作菜单在您要添加已验证域的联盟旁边，然后选择*禁用*。

删除联盟

如果您不再需要联盟，您可以将其删除。这将删除联合并阻止与联合关联的任何用户使用其公司凭据登录控制台。例如，如果 IdP 被停用或者不再需要联合。

删除联合后，您将无法恢复它。您必须创建一个新的联盟。

您必须先禁用联合，然后才能删除它。一旦删除联盟，就无法恢复删除。

步骤

1. 选择“管理”>“身份和访问”。
2. 选择“**Federations**”以查看“**Federations**”页面。
3. 选择操作菜单：在您要添加已验证域的联盟旁边，然后选择*删除*。

将您的联合导入**NetApp Console**

如果您之前已通过NetApp Cloud Central（ NetApp Console的外部应用程序）设置联合，则联合页面会提示您将现有的联合连接导入控制台，以便您可以在新界面中对其进行管理。然后，您可以利用最新的增强功能，而无需重新创建联合连接。

导入现有联盟后，您可以从“联盟”页面管理该联盟。"了解有关管理联盟的更多信息。"

所需角色

组织管理员或联盟管理员。"了解有关访问角色的更多信息。"

步骤

1. 选择*管理>身份和访问*。
2. 选择“**Federation**”选项卡。
3. 选择*导入联合*。

强制实施**ONTAP Advanced View**（**ONTAP**系统管理器）的**ONTAP**权限

默认情况下，控制台代理凭据允许用户访问高级视图（ONTAP系统管理器）。您可以提示用户输入他们的ONTAP凭据。这可确保用户在Cloud Volumes ONTAP和ONTAP本地集群中使用ONTAP集群时应用其ONTAP权限。

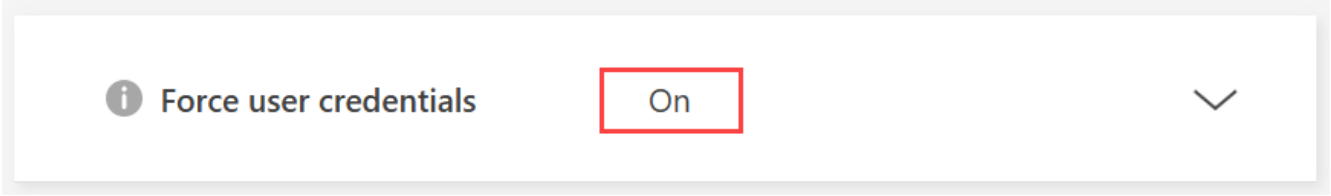
您必须具有组织管理员角色才能编辑控制台代理设置。

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. 展开*强制凭证*选项。
4. 选中复选框以启用*强制凭证*选项，然后选择*保存*。
5. 验证“强制凭证”选项是否已启用。



为NetApp Console组织启用只读模式

为安全起见，您可以为NetApp Console组织启用只读模式。在只读模式下，用户可以查看资源和设置，但不能进行任何更改。

在只读模式下，具有管理员角色的用户必须手动提升权限才能进行更改，这确保了更改是有意为之的。

所需访问权限

超级管理员或组织管理员。

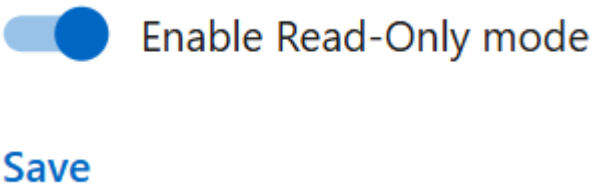
为您的控制台组织启用只读模式

启用只读模式以限制对控制台组织的更改。所有用户仍然可以查看资源。拥有管理员角色的用户，如果不手动提升权限，则无法在控制台中执行任何操作。

启用只读模式后，用户会看到一个横幅，通知他们该组织处于只读模式。用户必须前往用户设置来提升其角色。

步骤

1. 选择*管理>身份和访问*。
2. 在“组织”选项卡中，选择要设置为只读模式的组织的“编辑组织设置”。
3. 在“只读模式”部分，将开关拨到“开”位置启用只读模式，然后选择“保存”。



以初始组织管理员身份注册**NetApp Console**

如果贵公司还没有NetApp Console组织，请注册创建一个。第一个用户是管理员，负责管理帐户和权限。您可以稍后更新角色并添加管理员。

步骤

1. 打开 Web 浏览器并转到 "NetApp Console"
2. 如果您拥有NetApp支持站点帐户，请直接在“登录”页面上输入与您的帐户关联的电子邮件地址。

   控制台会在您首次登录时使用您的NetApp支持站点凭据进行注册。

3. 如果您想通过创建控制台登录来注册，请选择*注册*。
   a. 在*注册*页面上，输入所需信息并选择*下一步*。

      注册表格中只允许使用英文字符。

   b. 检查您的收件箱，查找来自NetApp的电子邮件，其中包含验证您的电子邮件地址的说明。

      请验证您的电子邮件地址以完成注册。

4. 登录后，请阅读并接受最终用户许可协议。
5. 在“欢迎”页面上，创建一个组织。
6. 选择*让我们开始吧*。

+ 作为首次担任管理员的用户，请按照引导流程添加存储、创建控制台代理等。 "了解如何使用控制台助手。"

下一步

作为管理员，在完成控制台助手中包含的步骤后，您应该规划身份和访问策略，将用户添加到您的组织，并分配角色。 "了解NetApp Console的身份和访问管理"

如果组织已存在，请注册或登录**NetApp Console**。

如果贵公司已有NetApp Console组织，请注册或登录以访问它。您的注册或登录方式取决于您的公司是否使用身份联合或拥有NetApp支持站点凭据。如果还没有，请创建NetApp Console登录帐户。

步骤

1. 打开 Web 浏览器并转到 "NetApp Console"
2. 如果您拥有NetApp支持站点帐户，或者您的公司已设置单点登录 (SSO)，请在“登录”页面上输入您关联的电子邮件地址或 SSO 凭据。按照提示完成登录。

   在这两种情况下，您都会在初始登录时注册控制台。

3. 如果您想通过创建控制台登录来注册，请选择*注册*。
   a. 在*注册*页面上，输入所需信息并选择*下一步*。

      注册表格中只允许使用英文字符。

   b. 检查您的收件箱，查找来自NetApp的电子邮件，其中包含验证您的电子邮件地址的说明。

      请验证您的电子邮件地址以完成注册。

4. 登录后，请阅读并接受最终用户许可协议。
5. 如果系统提示您创建组织，请关闭对话框并告知控制台管理员，以便他们可以将您添加到控制台组织并授予您访问权限。 "了解如何联系组织管理员。"

下一步

获得组织访问权限后，即可开始管理存储和使用分配给您的数据服务。

管理组织合作伙伴关系

NetApp Console 中的组织伙伴关系

在NetApp Console中创建组织间的合作伙伴关系，可以让合作伙伴安全地跨组织边界管理NetApp资源，从而简化协作并增强安全性。

必需角色

合作伙伴管理员"了解有关访问角色的更多信息。"

合作伙伴关系允许使用控制台中的角色驱动关系跨组织安全地管理NetApp资源。发起组织授予对其资源的访问权限，而接受组织提供被授予访问权限的用户或服务帐户。合作伙伴关系是通过自助服务工作流程建立的，使发起组织能够完全控制共享的资源、分配的角色以及根据需要加入、管理或撤销合作伙伴访问权限的能力。

客户可以授权 MSP 或经销商来管理NetApp环境，而无需复杂的设置。客户可以控制合作伙伴可以访问哪些集群以及他们拥有哪些角色，并且可以随时撤销访问权限以维护安全性和合规性。

作为合作伙伴，您可以获得跨客户环境的集中可见性和控制力。您可以轻松切换到客户的组织来管理资源、运行数据服务并在定义的边界内监控健康状况，从而减少自定义工具并确保与每个客户的政策保持一致。

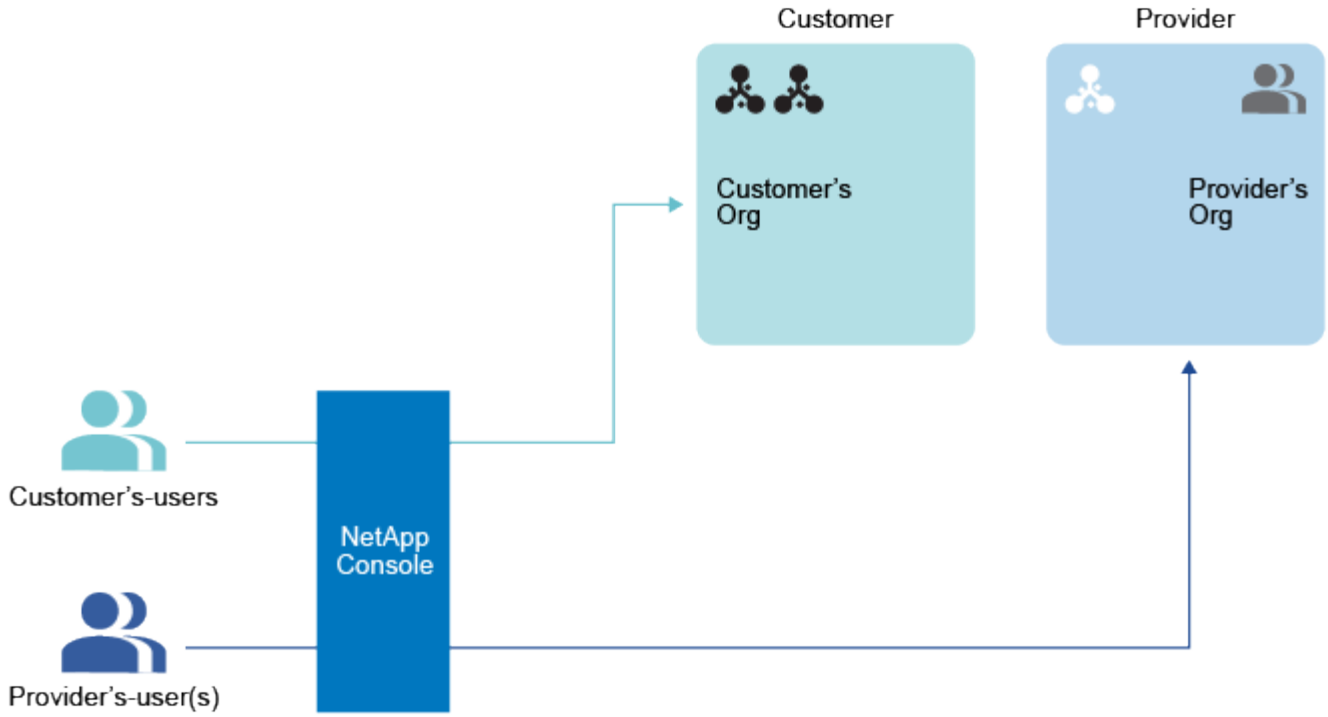
1. 为一个或多个用户分配合作伙伴管理员角色

为发起和接收组织中的一个或多个用户分配 Partnership admin 角色，以创建和管理伙伴关系。您可以将 Partnership viewer 角色分配给只需要查看伙伴关系而不需要管理的用户。

2. 与发起组织共享您的组织 **ID**

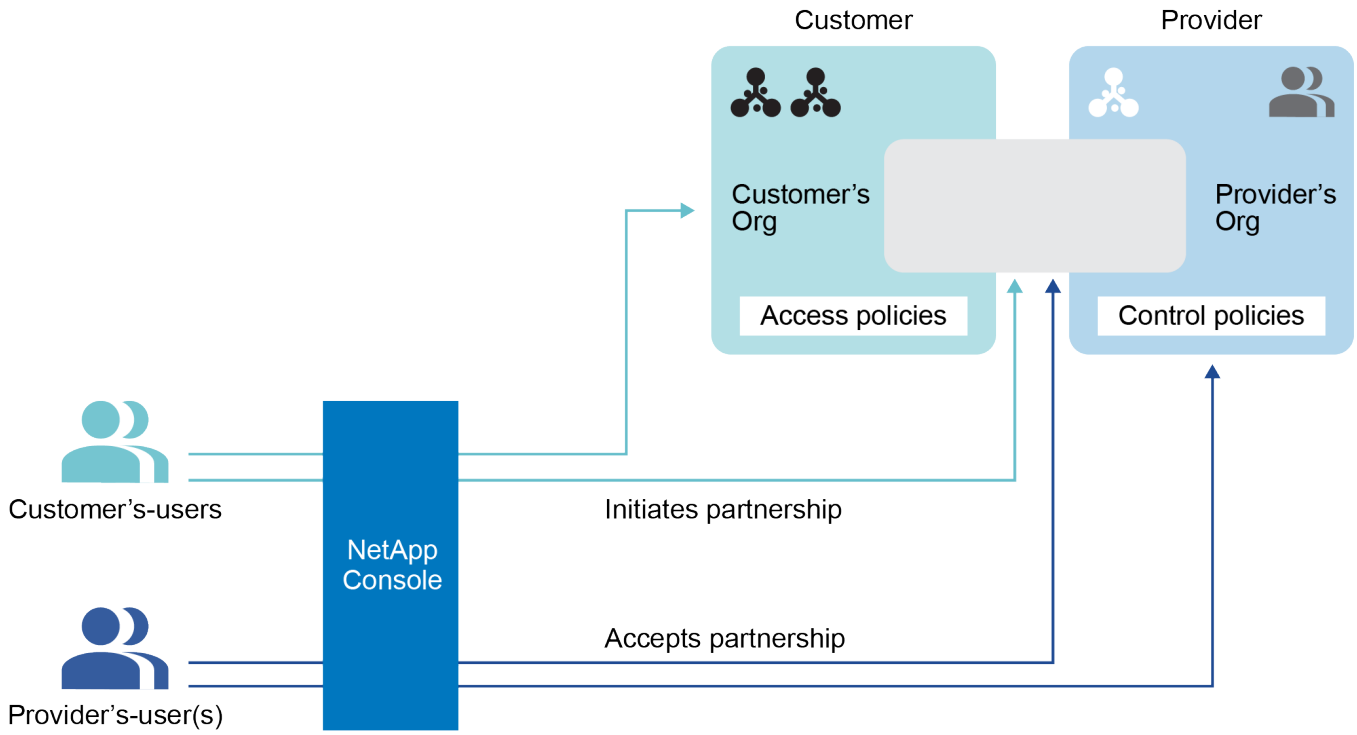
要发起合作关系，发起者必须知道目标组织的组织 ID。只有相应的组织可以访问此组织 ID。通过电子邮件或其他方式直接与NetApp Console之外的发起组织共享。

发起组织是授予其资源访问权限的组织。



3 在**NetApp Console**内建立合作关系

发起合作关系的组织通过从NetApp Console发送合作关系请求来发起合作关系。



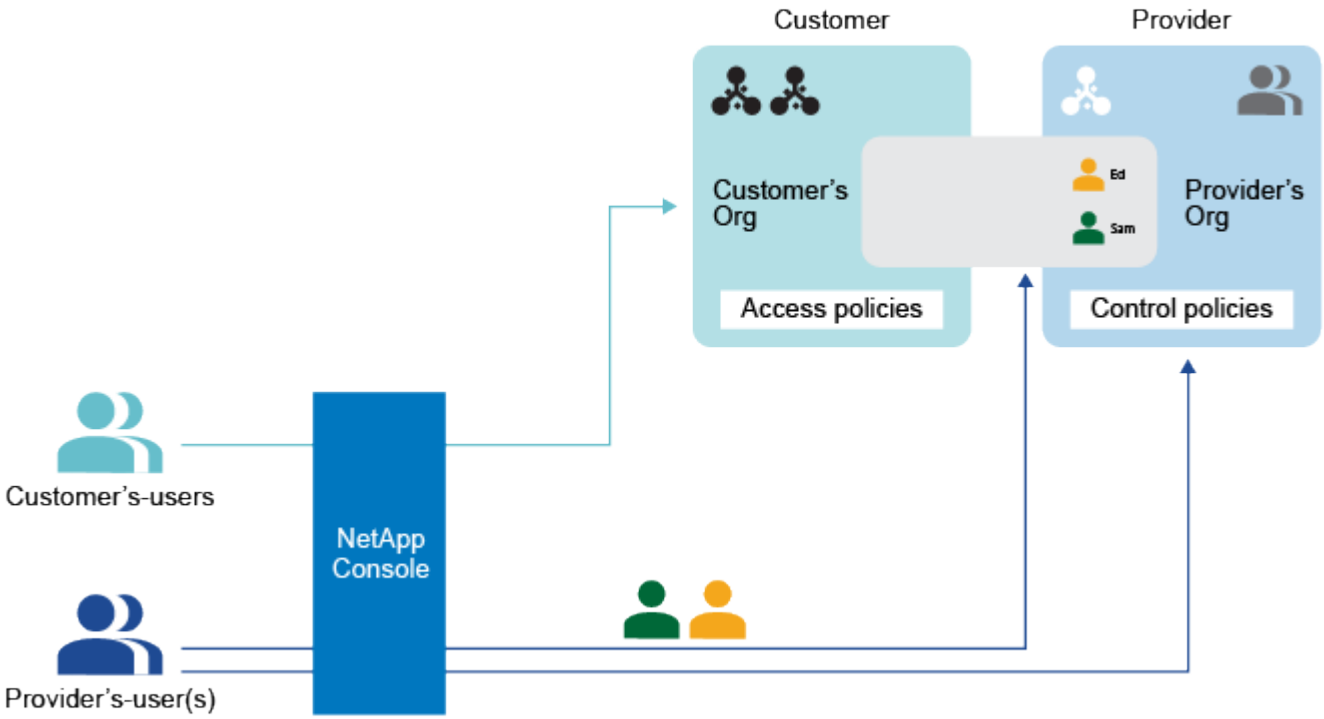
4 批准合作

接收组织必须接受该请求。

接收组织是被授予资源访问权限的组织。

5 将用户分配到合作关系

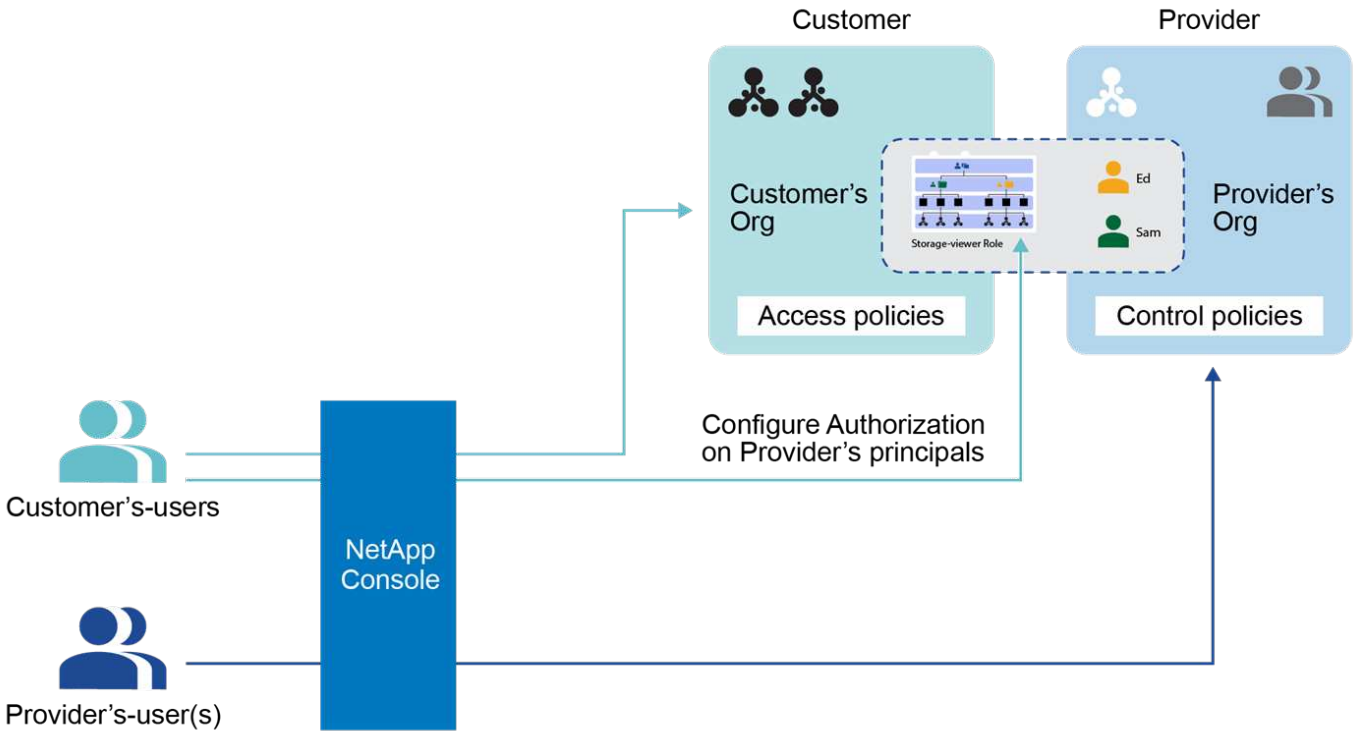
接收组织将您组织中的特定用户或服务帐户分配给合作伙伴关系。发起组织为这些用户分配角色。



6 授予指定用户对资源的访问权限

如果您是发起组织，您可以向分配给合作关系的用户授予特定资源的访问权限。您可以随时撤销访问权限。

您可以通过为组织内的特定项目或文件夹分配角色来实现此目的。



在NetApp Console中管理合作伙伴关系

建立合作伙伴关系，在您的组织和值得信赖的合作伙伴之间建立安全、可管理的连接，以实现协作式NetApp资源管理。

通过合作伙伴关系，您可以通过控制台中的角色驱动关系安全地跨边界管理NetApp资源。发起组织授予对其资源的访问权限，而接受组织提供被授予访问权限的用户或服务帐户。合作伙伴关系是通过自助服务工作流程建立的，使发起组织能够完全控制共享的资源、分配的角色以及根据需要加入、管理或撤销合作伙伴访问权限的能力。

必需角色

需要“合作伙伴关系管理员”角色来创建和管理合作伙伴关系。 *合作伙伴查看者*可以查看合作伙伴页面。"了解有关访问角色的更多信息。"

建立组织伙伴关系

如果您知道其他组织的组织 ID，您可以请求与其建立合作关系。接收组织必须批准该请求，合作关系才能继续进行。

在开始之前，请确保您拥有合作伙伴组织的组织 ID，并且已被分配 合作伙伴管理员 角色。

步骤

1. 选择*管理>身份和访问*。
2. 选择“合作伙伴关系”选项卡。
3. 选择*添加合作伙伴关系*。
4. 在*创建合作伙伴关系*对话框中，输入请求合作伙伴的合作伙伴组织 ID，然后选择*添加*。

合作请求被发送给合作伙伴组织以供批准。您可以在*合作伙伴关系*页面上查看合作请求的状态。

批准组织合作关系

接收组织必须接受组织合作请求，合作才能继续进行。您必须具有*合作伙伴关系管理员*角色才能批准和管理合作伙伴关系。

步骤

1. 选择*管理>身份和访问*。
2. 选择*合作伙伴关系*。
3. 选择“已收到合作关系”选项卡。
4. 导航到您想要批准的合作关系并选择 ••• 然后选择*批准*。
5. 查看合作关系的详细信息，包括请求合作关系的组织的名称和组织 ID，然后选择“下一步”。
6. 可选，将组织成员添加到合作伙伴关系并选择*应用*。

   您可以随时通过*合作伙伴*页面添加其他成员。

   您添加的任何成员都会在合作伙伴的组织中可见，合作伙伴可以在其中将他们分配给资源。

结果

您批准的合作关系现在显示状态为*已建立*。任一组织中具有 **Partnership admim** 或 **Partnership viewer** 角色的用户都可以查看合作关系。

查看合作关系状态

查看您的合作关系状态。

所需角色

合作伙伴关系管理员、合作伙伴关系查看者。"了解有关访问角色的更多信息。"

步骤

1. 选择*管理>身份和访问*。
2. 选择*合作伙伴关系*。
3. 选择“已发起的合作关系”或“已接收的合作关系”选项卡。
4. 查看显示合作关系及其状态的相应表格。

禁用组织合作关系

您必须是发起组织的成员才能禁用合作关系。禁用合作关系将立即撤销您组织中与合作伙伴组织共享的任何资源的访问权限。

所需角色

合伙管理员。"了解有关访问角色的更多信息。"

步骤

1. 选择*管理>身份和访问*。
2. 选择*合作伙伴关系*。
3. 选择“已启动的合作伙伴关系”选项卡。
4. 查看显示合作关系及其状态的相应表格。
5. 导航到您想要禁用的已启动合作关系并选择 ••• 然后选择*禁用*。

管理合作组织的成员

您可以通过将用户添加到合作伙伴组织来将用户添加到合作伙伴关系。添加用户后，合作伙伴组织负责为他们分配组织中特定资源的角色。

必需角色

需要“合作伙伴关系管理员”角色来创建和管理合作伙伴关系。 *合作伙伴查看者*可以查看合作伙伴页面。"了解有关访问角色的更多信息。"

您可以随时从合作关系中移除用户。从合作关系中移除用户会立即撤销其对合作伙伴组织中任何资源的访问权限。

向合作关系添加成员

当您向合作伙伴关系添加成员时，合作伙伴组织的*合作伙伴关系管理员*必须为他们分配组织中特定资源的角色，然后他们才能访问这些资源。

将成员添加到合作伙伴关系后，这些成员将显示为合作伙伴组织中的成员，合作伙伴可以在其中为他们分配资源。

步骤

1. 选择*管理>身份和访问*。
2. 选择*合作伙伴关系*。
3. 选择“已收到合作关系”选项卡。
4. 选择操作菜单 ••• 在您想要添加成员的已建立的合作关系旁边，选择“添加成员”。
5. 选择一个或多个要添加到合作关系中的成员，然后选择*添加*。

从合作关系中移除成员

您可以随时从合作关系中移除成员。从合作关系中移除用户会立即撤销其对合作伙伴组织中任何资源的访问权限。

如果您想调整成员拥有的角色或他们可以访问的资源，合作伙伴组织的合作伙伴管理员必须进行这些更改。

步骤

1. 选择*管理>身份和访问*。
2. 选择*合作伙伴关系*。
3. 选择“已收到合作关系”选项卡。
4. 选择操作菜单 ••• 在您想要删除的成员旁边，选择“删除关联”。

5. 通过在对话框中选择“删除”来确认该操作。

查看用户的角色信息

您可以查看已分配给用户的角色以及相关资源。

您不能更改与用户关联的角色。如果您对所提供的资源或角色有任何疑问，请联系合作伙伴组织的管理员。

步骤

1. 选择*管理>身份和访问*。
2. 选择*合作伙伴关系*。
3. 选择“已收到合作关系”选项卡。
4. 从“成员”页面，导航到表中的成员，选择 ••• 然后选择*查看详细信息*。
5. 在表格中，展开您想要查看成员分配角色的组织、文件夹或项目的相应行，然后选择“角色”列中的数字。

为合作伙伴用户提供资源访问

您可以通过为合作伙伴用户分配组织内文件夹和项目的特定角色来授予他们访问权限。

必需角色

合伙管理员。"了解有关访问角色的更多信息。"

合作伙伴组织必须先将成员添加到合作伙伴关系中，然后您才能为他们分配组织中资源的角色。"了解如何向合作关系添加成员。"

了解合作伙伴用户的角色

您可以按照管理自己的角色的方式来管理合作伙伴组织成员的角色。然而，并非所有角色都适合合作伙伴用户。特别是，您不能授予合作伙伴用户允许软件更新的角色。更新ONTAP软件通常需要直接网络访问。

您可以为合作伙伴用户分配以下角色：

- "组织管理员"
- "文件夹或项目管理员"
- "联盟管理员"
- "联邦查看器"
- "备份和恢复管理员"
- "备份查看器"
- "恢复管理员"
- "克隆管理员"
- "灾难恢复管理员"
- "灾难恢复故障转移管理员"
- "灾难恢复应用程序管理员"

- "灾难恢复查看器"
- "运营支持分析师"
- "分类查看器"

"了解有关预定义角色的更多信息"

向合作伙伴用户添加角色

您可以通过向成员添加角色来提供对组织资源的访问权限。分配角色时，您指定一个资源和一个角色。您可以为一个用户分配多个角色。

例如，如果您有两个项目，并且希望同一个用户同时拥有这两个项目的备份和恢复管理员角色，则您需要为每个项目的用户提供该角色。同样，如果您想为同一个项目的用户提供两个不同的角色，则需要分别分配每个角色。

步骤

1. 选择*管理>身份和访问*。
2. 选择*合作伙伴关系*。
3. 选择*合作伙伴关系已启动*选项卡。
4. 选择操作菜单 ••• 在您想要查看的已建立的合作关系旁边，选择“查看详细信息”。

   *成员*列表显示合作伙伴组织已添加到合作伙伴关系的成员。

5. 选择操作菜单 ••• 在您想要分配角色的成员旁边，选择“添加角色”。
6. 要添加角色，请完成对话框中的步骤：
   - 选择组织、文件夹或项目：选择成员应具有权限的资源层次结构级别。

     如果您选择组织或文件夹，则该成员将拥有该组织或文件夹内所有内容的权限。

   - 选择类别：选择角色类别。"了解访问角色" 。
   - 选择*角色*：选择一个角色，该角色为成员提供与您选择的组织、文件夹或项目相关的资源的权限。
   - 添加角色：如果您想提供对组织内其他文件夹或项目的访问权限，请选择*添加角色*，指定另一个文件夹或项目或角色类别，然后选择一个角色类别和相应的角色。
7. 选择*添加新角色*。

更改或删除合作伙伴用户的角色

您可以更改或删除分配给合作伙伴组织成员的角色。

步骤

1. 选择*管理>身份和访问*。
2. 选择*合作伙伴关系*。
3. 选择*合作伙伴关系已启动*选项卡。
4. 选择操作菜单 ••• 在您想要查看的已建立的合作关系旁边，选择“查看详细信息”。

   *成员*列表显示合作伙伴组织已添加到合作伙伴关系的成员。

5. 从“成员”页面，导航到表中的成员，选择 ••• 然后选择*查看详细信息*。
6. 在表格中，展开要更改成员分配角色的组织、文件夹或项目的相应行，然后在“角色”列中选择“查看”以查看分配给该成员的角色。
7. 您可以更改成员的现有角色或删除角色。
   a. 要更改成员的角色，请选择要更改的角色旁边的“更改”。您只能将角色更改为同一角色类别内的角色。例如，您可以从一个数据服务角色更改为另一个数据服务角色。确认更改。
   b. 要取消分配成员的角色，请选择 🗑 在角色旁边，点击即可从成员中移除相应的角色。您将被要求确认删除操作。

在合作组织工作

一旦您在合作伙伴组织中被赋予角色，您就可以切换到该组织并执行您有权执行的操作。

使用组织菜单在您的组织和您有权访问的任何合作伙伴组织之间切换。"了解有关切换组织和项目的更多信息。"

您将能够看到合作伙伴组织中与您共享的资源，并根据分配给您的角色执行操作。与您的合作伙伴管理员合作，确保您拥有需要访问的资源的适当角色。

监控NetApp Console操作

您可以监视控制台正在执行的操作的状态，以查看是否存在需要解决的问题。您可以从审核页面、通知中心查看状态，或将通知发送到您的电子邮件。

该表通过比较突出了审计页面和通知中心的功能。

通知中心	审计页面
显示事件和动作的高级状态	提供每个事件或行动的详细信息以供进一步调查
显示当前登录会话的状态（注销后，该信息不会出现在通知中心）	保留上个月的状态
仅显示在用户界面中发起的操作	显示来自 UI 或 API 的所有操作
显示用户发起的操作	显示所有操作，无论是用户发起的还是系统发起的
按重要性过滤结果	按服务、操作、用户、状态等进行过滤
提供向用户和其他人发送电子邮件通知的功能	没有电子邮件功能

从审核页面审核用户活动

使用审计页面来识别谁执行了操作或其状态。

审计页面显示用户为管理您的组织或帐户而完成的操作。这包括关联用户、创建系统、创建代理等管理操作。

您还可以核实是谁向组织添加了成员，或者项目是否已成功删除。

步骤

1. 选择“管理”>“审计”。

2. 使用表格上方的过滤器来更改表格中显示的操作。

   例如，您可以使用*服务*过滤器显示与特定服务相关的操作，或者可以使用*用户*过滤器显示与特定用户帐户相关的操作。

从审计页面下载审计日志

您可以将审计日志从审计页面下载到 CSV 文件中。这使您能够记录用户在您的组织中执行的操作。 CSV 文件包含下载的 CSV 文件中的所有列，无论审计页面上的过滤器或显示的列如何。

步骤

1. 在*审计*页面中，选择表格右上角的下载图标。

使用通知中心监控活动

通知跟踪控制台操作以确认成功。它们使您能够查看在当前登录会话期间启动的许多控制台操作的状态。并非所有控制台服务都会将信息报告到通知中心。

您可以通过选择通知铃来显示通知（  ）在菜单栏中。铃铛中小气泡的颜色表示处于活动状态的最高级别严重性通知。因此，如果您看到红色气泡，则表示有重要的通知需要您查看。

您还可以配置控制台通过电子邮件发送某些类型的通知，这样即使您未登录系统也可以了解重要的系统活动。电子邮件可以发送给您组织中的任何用户，或任何其他需要了解某些类型的系统活动的收件人。了解如何设置电子邮件通知设置。

比较通知中心和警报

通知中心使您能够查看已启动的操作的状态并为某些类型的系统活动设置警报通知。同时，警报使您能够查看ONTAP存储环境中与容量、可用性、性能、保护和安全性相关的问题或潜在风险。

"了解有关NetApp Console警报的更多信息"

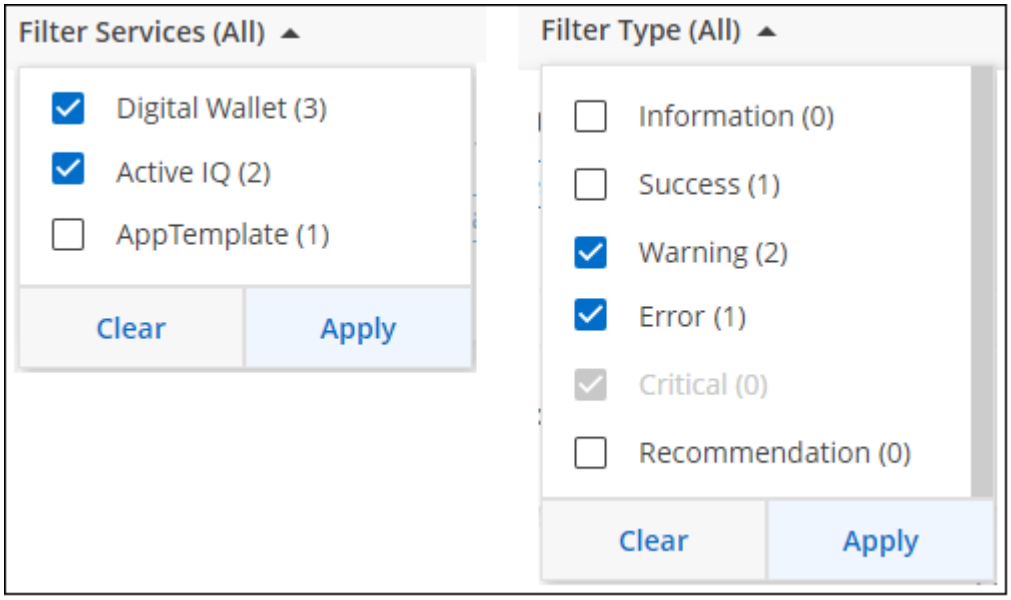
通知类型

控制台将通知分为以下类别：

通知类型	描述
批判的	出现问题，如果不立即采取纠正措施，可能会导致服务中断。
错误	一项行动或过程以失败告终，或者如果不采取纠正措施则可能导致失败。
警告	您应该注意这个问题，以确保其不会达到严重程度。这种严重程度的通知不会导致服务中断，并且可能不需要立即采取纠正措施。
建议	系统建议您采取行动来改进系统或某项服务；例如：节省成本、新服务建议、推荐安全配置等。
信息	提供有关操作或过程的附加信息的消息。
成功	动作或过程成功完成。

过滤通知

默认情况下，您会在通知中心看到所有活动通知。您可以过滤看到的通知，以仅显示对您重要的通知。您可以按“服务”和通知“类型”进行过滤。



例如，如果您只想查看控制台操作的“错误”和“警告”通知，请选择这些条目，您将只看到这些类型的通知。

关闭通知

如果您不再需要查看通知，可以从页面中删除它们。您可以单独或一次性关闭所有通知。

要关闭所有通知，请在通知中心选择⋮并选择*全部关闭*。

要关闭单个通知，请将光标悬停在通知上并选择*关闭*。

设置电子邮件通知设置

您可以通过电子邮件发送特定类型的通知，这样即使您未登录也可以获知重要的系统活动。电子邮件可以发送给您组织或帐户中的任何用户，或任何其他需要了解某些类型的系统活动的收件人。

- 控制台发送代理、许可证和订阅、 NetApp Copy and Sync以及NetApp Backup and Recovery的电子邮件通知。
- 当控制台代理安装在没有互联网访问的站点时，不支持发送电子邮件通知。

您在通知中心设置的过滤器不会决定您通过电子邮件收到的通知类型。默认情况下，任何组织管理员都会收到所有“关键”和“建议”通知的电子邮件。这些通知涵盖所有服务 - 您不能选择仅接收某些服务的通知，例如代理或NetApp Backup and Recovery。

所有其他用户和收件人都配置为不接收任何通知电子邮件 - 因此您需要为任何其他用户配置通知设置。

您必须具有组织管理员角色才能自定义通知设置。

步骤

1. 选择*管理>通知设置*。
2. 选择*组织用户*或*其他收件人*。

   *其他收件人*页面允许您配置控制台以通知控制台组织的成员。

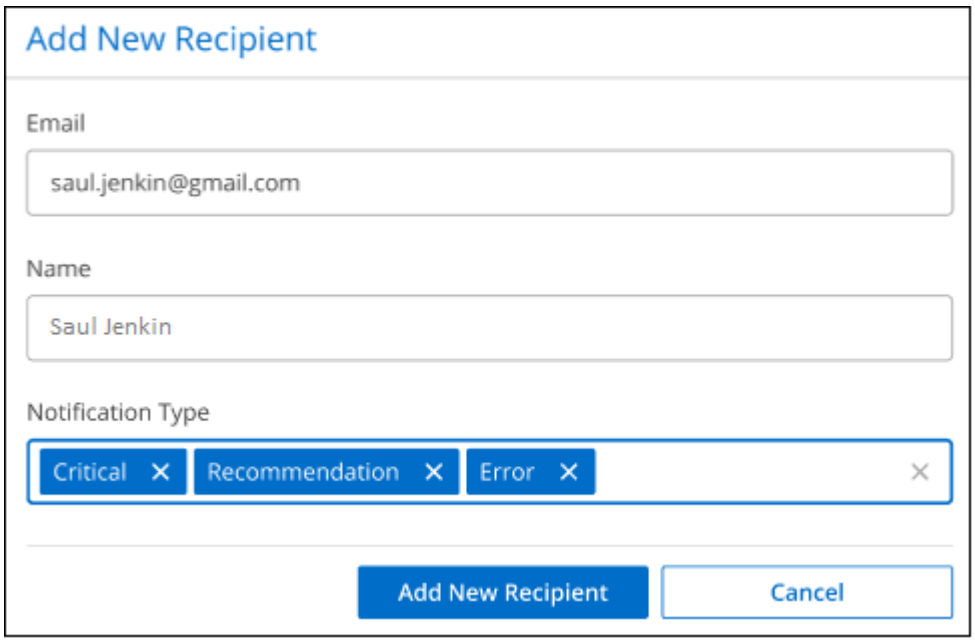
3. 从“组织用户”页面或“其他收件人”页面中选择一个或多个用户，然后选择要发送的通知类型：
   - 要对单个用户进行更改，请选择该用户的通知列中的菜单，检查要发送的通知类型，然后选择*应用*。
   - 要对多个用户进行更改，请选中每个用户的复选框，选择*管理电子邮件通知*，检查要发送的通知类型，然后选择*应用*。

添加其他电子邮件收件人

_组织用户_页面中显示的用户是从您的组织或帐户中的用户自动填充的。您可以在“其他收件人”页面中为其他无权访问控制台但需要收到某些类型的警报和通知的个人或团体添加电子邮件地址。

步骤

1. 从*通知设置*页面中，选择*添加新收件人*。



2. 输入姓名、电子邮件地址，选择收件人将收到的通知类型，然后选择*添加新收件人*。