NetApp控制台设置和管理文档

NetApp Console setup and administration

NetApp
October 07, 2025

目录

NetApp控制台设置和管理文档

发行说明

什么是新的

了解NetApp控制台管理功能的新增功能：身份和访问管理 (IAM)、控制台代理、云提供商凭据等。

2025年10月6日

BlueXP现在是NetApp控制台

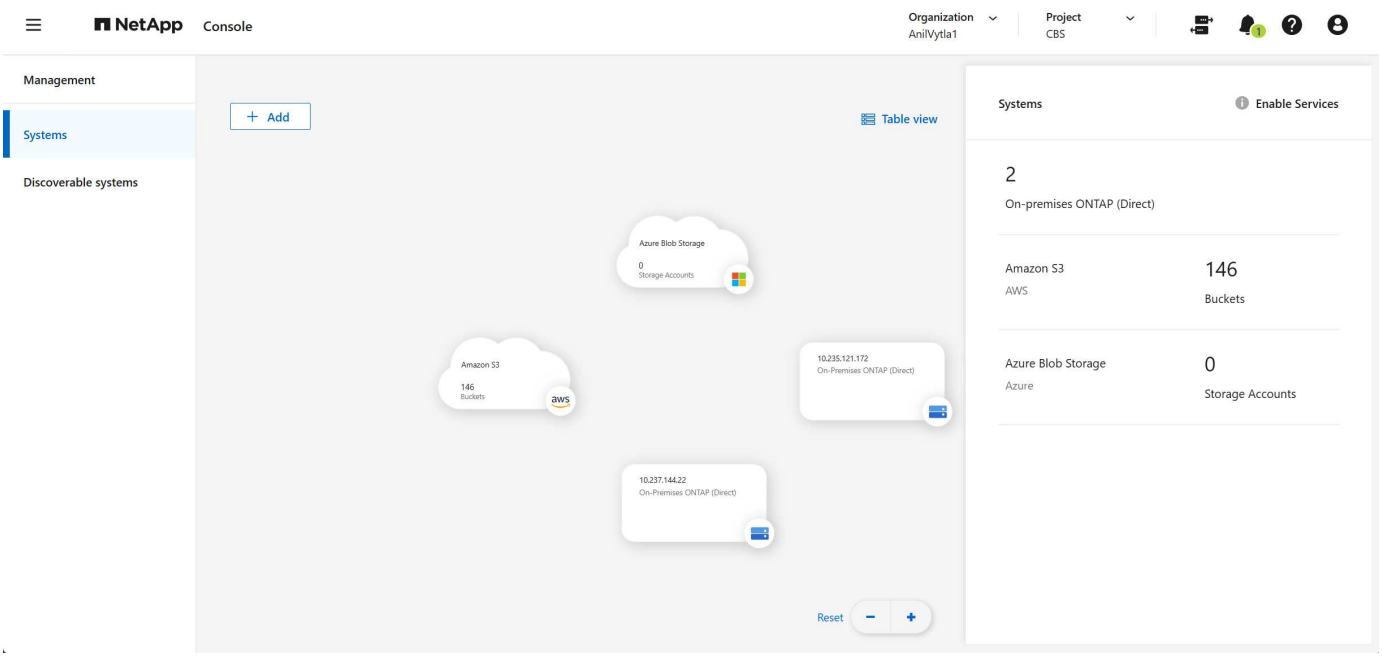
NetApp控制台建立在增强和重组的BlueXP基础之上，可在企业级内部和云环境中集中管理NetApp存储和NetApp数据服务，提供实时洞察、更快的工作流程以及高度安全且合规的简化管理。

导航菜单和页面

NetApp将大多数菜单选项移至左侧导航窗格，并重新组织菜单以便在NetApp控制台中更轻松地导航。

画布被系统页面取代

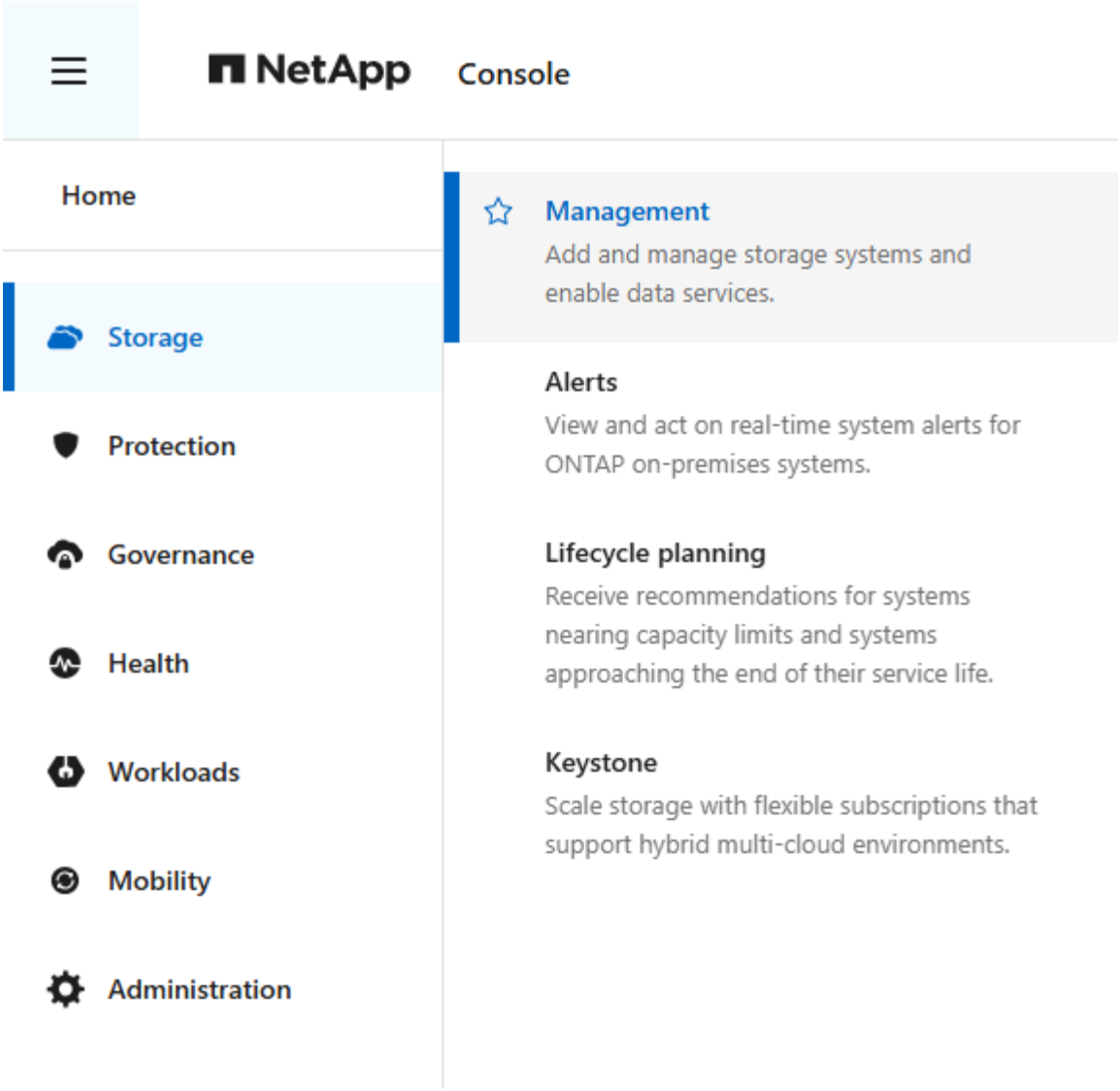
NetApp将 Canvas 重命名为 **Systems** 页面。从“存储 **>** 管理”菜单导航到“系统”页面。



扩展存储菜单

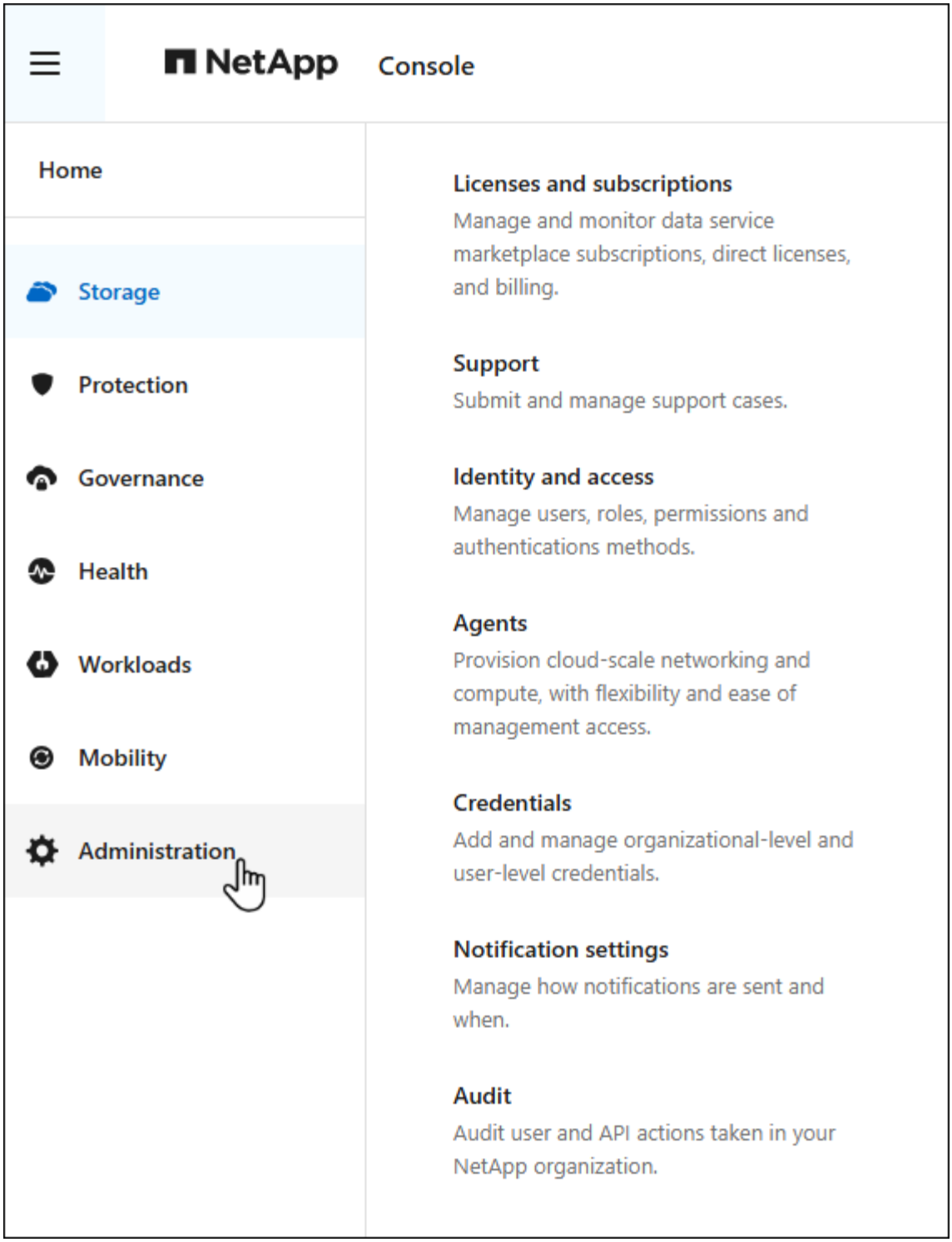
存储*菜单包括*警报，用于查看ONTAP系统警报和*生命周期规划*（以前称为*经济效率*），用于识别未使用或未充分利用的资源。

NetApp已将Keystone移至 存储 菜单，您可以在其中管理您的NetApp Keystone订阅并查看您的使用情况。



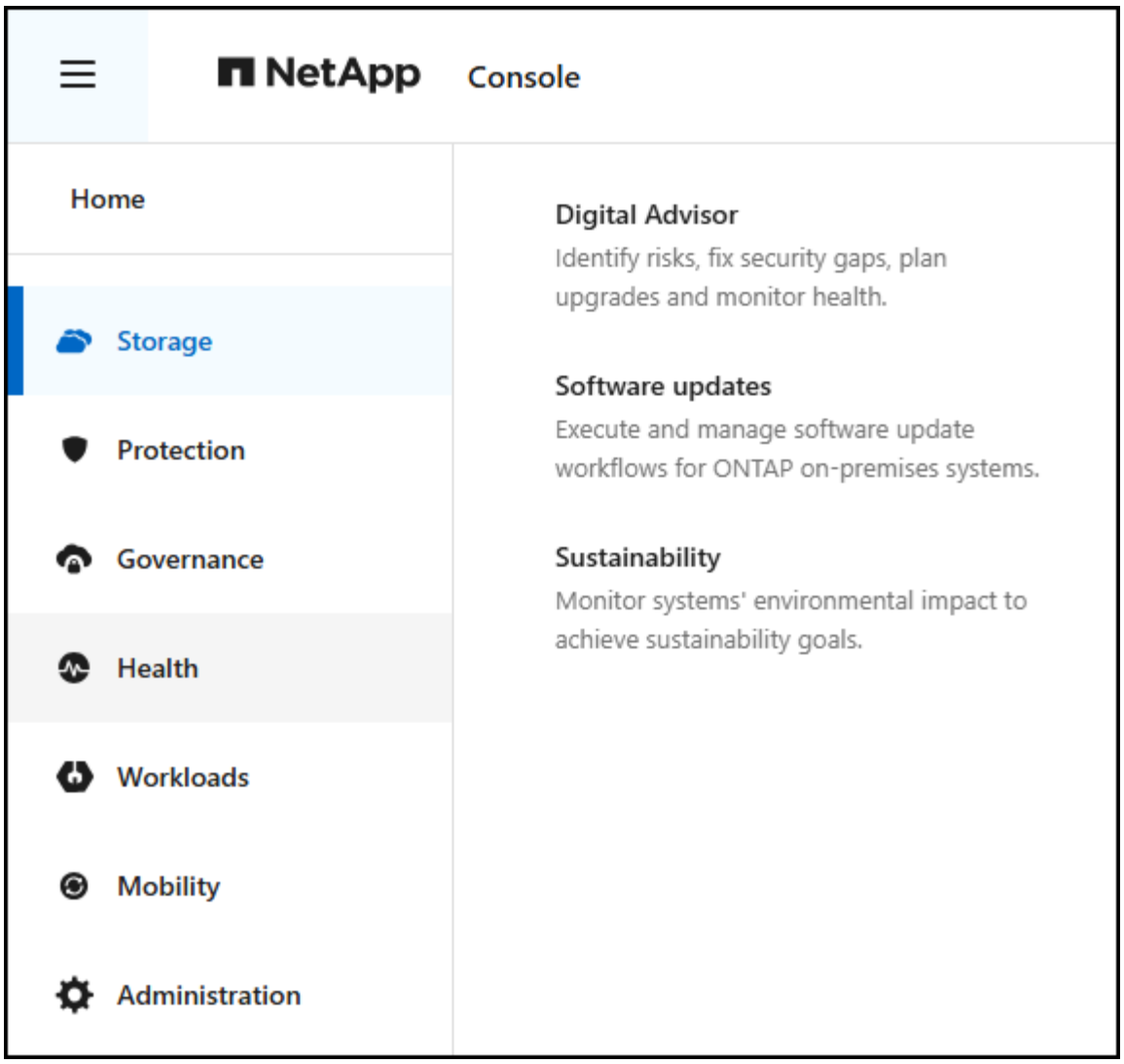
管理菜单

使用集中式*管理*菜单来管理NetApp控制台、支持案例、许可证和订阅（以前称为数字钱包）。



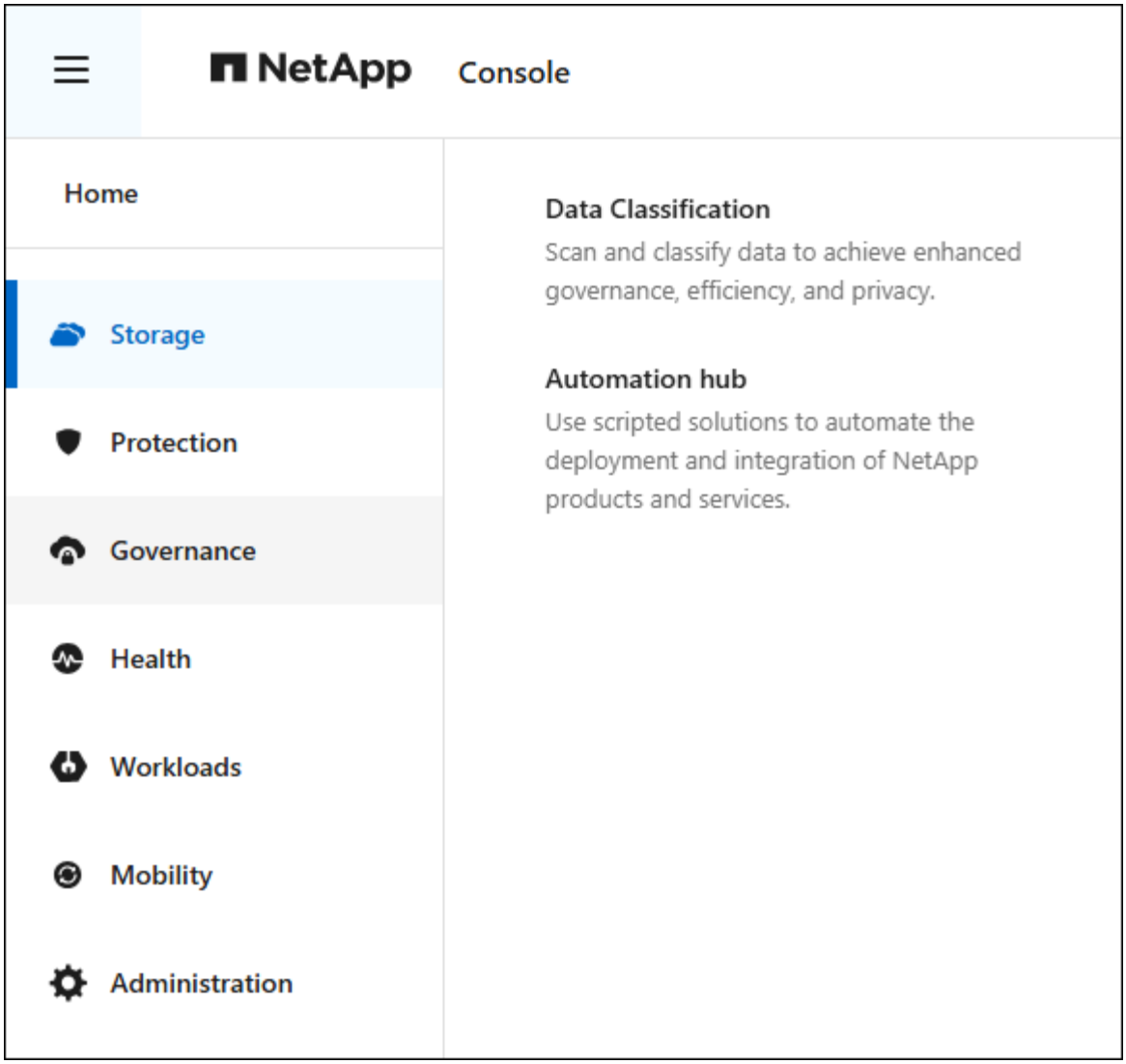
健康菜单

高效的*健康*菜单包括*软件更新*（您可以在其中管理ONTAP软件更新）、可持续性（您可以在其中监控对环境的影响）和*Digital Advisor*（您可以在其中获得主动建议以优化您的存储环境）。



治理菜单

治理*菜单包括*数据分类，您可以在其中管理数据分类和合规性，以及*自动化中心*，您可以在其中创建和管理自动化工作流程。



元素、数据服务和功能的命名更加直观

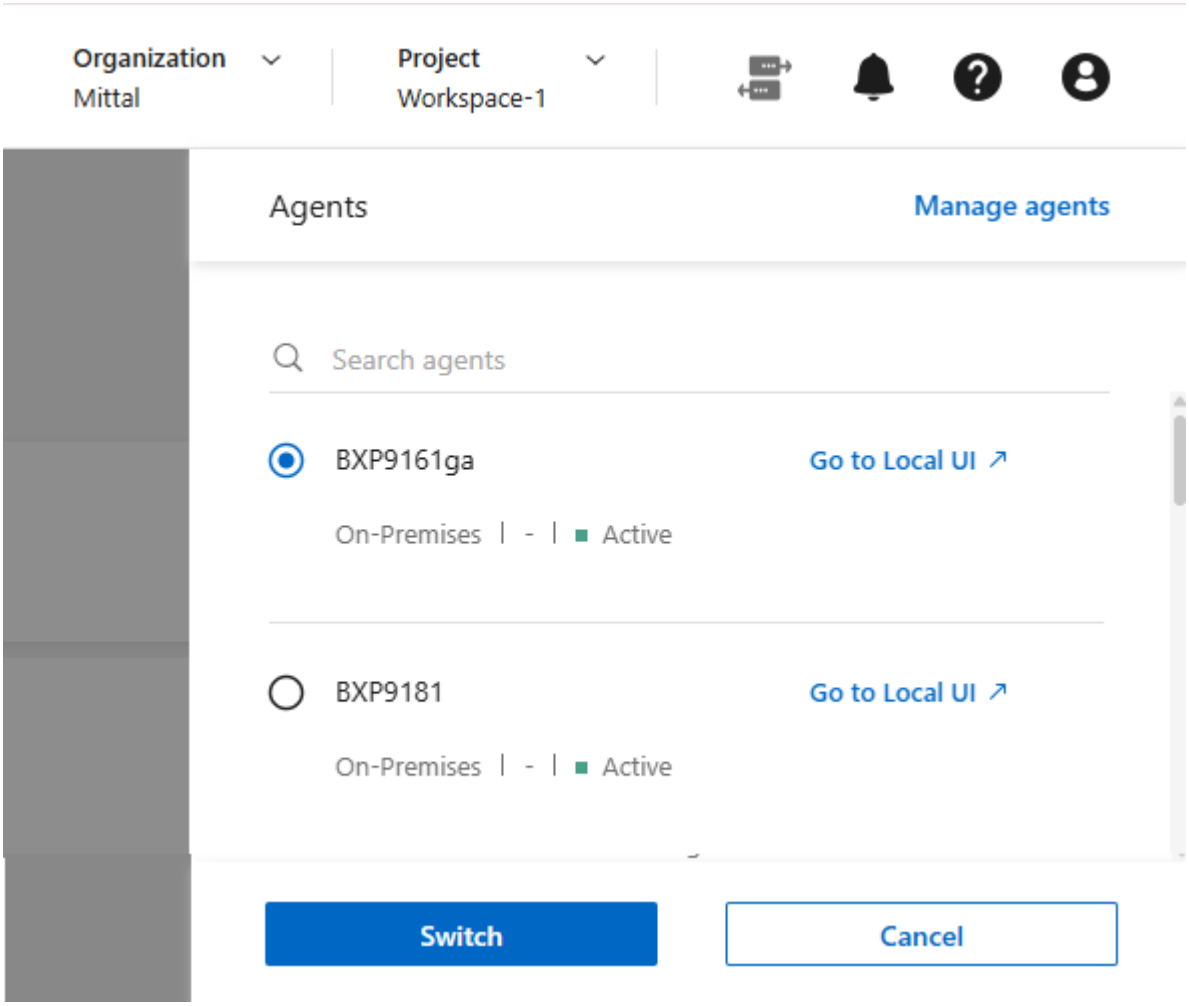
NetApp重命名了几个元素、数据服务和功能以明确其用途。主要变化包括：

曾用名	* NetApp控制台名称*
连接器	控制台代理。 从*管理>代理*菜单查看、添加和管理您的代理。
时间线页面	审计页面 从*管理>审计*菜单查看审计控制台活动。
工作环境	系统 从*存储>管理*菜单查看、添加和管理您的系统。

曾用名	* NetApp控制台名称*
BlueXP勒索软件防护	NetApp勒索软件恢复能力。 勒索软件恢复能力可帮助您保护数据并从勒索软件攻击中快速恢复。
BlueXP经济效率	生命周期规划。 生命周期规划可帮助您识别未使用和未充分利用的资源来优化存储成本。 从*存储>生命周期规划*菜单访问生命周期规划。
BlueXP digital wallet	许可证和订阅 从*管理>许可证和订阅*菜单访问您的许可证和订阅。

控制台代理

从*管理>代理*菜单访问和管理您的控制台代理。 NetApp已更改了为“系统”页面（以前称为“Canvas”）选择控制台代理的方式。 NetApp已将连接器菜单名称替换为图标，允许您选择要查看系统的控制台代理。



您还可以从*管理>代理*菜单管理您的代理。

控制台代理 4.0.0

此版本的控制台代理包括安全改进、错误修复和以下新功能。

4.0.0 版本适用于标准模式和限制模式。

整合并减少所需的网络端点

NetApp减少了控制台和控制台代理所需的网络端点，增强了安全性并简化了部署。重要的是，4.0.0 版本之前的所有部署都将继续得到全面支持。虽然以前的端点仍然可供现有代理使用，但NetApp强烈建议在确认代理升级成功后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" 。
- "了解有关所需端点的更多信息。"

支持 **VCenter** 部署控制台代理

您可以使用 OVA 文件在 VMware 环境中部署控制台代理。 OVA 文件包含一个预配置的 VM 映像，其中包含控制台代理软件和用于连接到NetApp控制台的设置。可直接从NetApp控制台下载文件或部署 URL。"了解如何在 VMware 环境中部署控制台代理。"

VMware 的控制台代理 OVA 提供了预配置的 VM 映像以便快速部署。

失败代理部署的验证报告

当您从NetApp控制台部署控制台代理时，您现在可以选择验证代理配置。如果控制台无法部署代理，它会提供可下载的报告来帮助您排除故障。

改进了控制台代理的故障排除

控制台代理已改进错误消息，可帮助您更好地了解问题。"了解如何排除控制台代理故障。"

NetApp控制台

NetApp控制台管理包括以下新功能：

主页仪表板

NetApp控制台的主页仪表板提供存储基础设施的实时可见性，包括健康状况、容量、许可证状态和数据服务等指标。"了解有关主页的更多信息。"

NetApp助手

具有组织管理员角色的新用户可以使用NetApp助手配置控制台，包括添加代理、链接NetApp支持帐户以及添加存储系统。"了解NetApp助手。"

服务帐户身份验证

NetApp控制台支持使用系统生成的客户端 ID 和密钥或客户管理的 JWT 进行服务帐户身份验证，从而允许组织选择最适合其安全要求和集成工作流程的方法。私钥 JWT 客户端身份验证使用非对称加密，比传统的客户端 ID 和秘密方法提供更强的安全性。私钥 JWT 客户端身份验证使用非对称加密，在客户环境中保证私钥的安全，降

低凭证被盗风险，并提高自动化堆栈和客户端应用程序的安全性。"了解如何添加服务帐户。"

会话超时

系统会在 24 小时后或用户关闭网络浏览器时注销用户。

支持组织之间的伙伴关系

您可以在NetApp控制台中创建合作伙伴关系，让合作伙伴跨组织边界安全地管理NetApp资源，从而使协作更轻松、安全性更强。"学习如何管理合作关系" 。

超级管理员和超级查看者角色

添加了*超级管理员*和*超级查看者*角色。 *超级管理员*授予对控制台功能、存储和数据服务的完全管理访问权限。 *超级查看器*为审计员和利益相关者提供只读可见性。这些角色对于高级成员较少、访问权限较广的小型团队很有用。为了提高安全性和可审计性，鼓励组织谨慎使用*超级管理员*访问权限，并尽可能分配细粒度的角色。"了解有关访问角色的更多信息。"

勒索软件抵御能力的额外作用

添加了*勒索软件弹性用户行为管理员*角色和*勒索软件弹性用户行为查看器*角色。这些角色分别允许用户配置和查看用户行为和分析数据。"了解有关访问角色的更多信息。"

删除了支持聊天

NetApp已从NetApp控制台中删除了支持聊天功能。使用“管理”>“支持”页面来创建和管理支持案例。

2025年8月11日

连接器 **3.9.55**

BlueXP Connector 的此版本包括安全性改进和错误修复。

3.9.55 版本适用于标准模式和限制模式。

日语支持

BlueXP UI 现已提供日语版本。如果您的浏览器语言是日语， BlueXP会以日语显示。要访问日语文档，请使用文档网站上的语言菜单。

运营弹性功能

操作弹性功能已从BlueXP中删除。如果遇到问题，请联系NetApp支持。

BlueXP身份和访问管理（**IAM**）

BlueXP中的身份和访问管理现在提供以下功能。

运营支持的新访问角色

BlueXP现在支持运营支持分析师角色。此角色授予用户监控存储警报、查看BlueXP审计时间线以及输入和跟

踪NetApp支持案例的权限。

"了解有关使用访问角色的更多信息。"

2025年7月31日

私人模式发布（**3.9.54**）

新的私人模式版本现已可从 "NetApp 支持站点"

3.9.54 版本包括以下BlueXP组件和服务的更新。

组件或服务	此版本中包含的版本	自上次私人模式发布以来的变化
连接器	3.9.54, 3.9.53	前往 "BlueXP页面中的新功能"并参考版本 3.9.54 和 3.9.53 所包含的更改。
备份和恢复	2025年7月28日	前往 "BlueXP backup and recovery页面中的新功能"并参考 2025 年 7 月版本中包含的更改。
分类	2025 年 7 月 14 日（版本 1.45）	前往 "BlueXP classification页面中的新功能"。

有关私人模式的更多详细信息，包括如何升级，请参阅以下内容：

- "了解私人模式"
- "了解如何在私人模式下开始使用BlueXP"
- "了解如何在使用私有模式时升级连接器"

2025 年 7 月 21 日

支持Google Cloud NetApp Volumes

您现在可以在BlueXP中查看Google Cloud NetApp Volumes 。"了解有关Google Cloud NetApp Volumes 的更多信息。"

BlueXP身份和访问管理（IAM）

Google Cloud NetApp Volumes的新访问角色

BlueXP现在支持对以下存储系统使用访问角色：

- Google Cloud NetApp Volumes

"了解有关使用访问角色的更多信息。"

2025 年 7 月 14 日

连接器 **3.9.54**

此版本的BlueXP Connector 包括安全性改进、错误修复以及以下新功能：

- 支持专用于支持Cloud Volumes ONTAP服务的连接器的透明代理。"了解有关配置透明代理的更多信息。"
- 当连接器部署在 Google Cloud 环境中时，能够使用网络标签来帮助路由连接器流量。
- 连接器健康监控的附加产品内通知，包括 CPU 和 RAM 使用情况。

目前，3.9.54 版本适用于标准模式和限制模式。

BlueXP身份和访问管理（**IAM**）

BlueXP中的身份和访问管理现在提供以下功能：

- 支持私有模式下的 IAM，允许您管理BlueXP服务和应用程序的用户访问和权限。
- 简化身份联合的管理，包括更轻松的导航、更清晰的联合连接配置选项以及改进的现有联合的可见性。
- 访问BlueXP backup and recovery、 BlueXP disaster recovery和联合管理的角色。

支持私有模式下的 **IAM**

BlueXP现在支持私有模式下的 IAM，允许您管理BlueXP服务和应用程序的用户访问和权限。此增强功能使私人模式客户能够利用基于角色的访问控制 (RBAC) 来获得更好的安全性和合规性。

"了解有关BlueXP中的 IAM 的更多信息。"

简化身份联合管理

BlueXP现在提供了更直观的界面来管理身份联合。这包括更轻松的导航、更清晰的联合连接配置选项以及改进的现有联合可见性。

通过身份联合启用单点登录 (SSO) 允许用户使用其公司凭证登录BlueXP 。这提高了安全性，减少了密码的使用，并简化了入职流程。

系统将提示您将任何现有的联合连接导入新界面以获取对新管理功能的访问权限。这使您能够利用最新的增强功能，而无需重新创建联合连接。"了解有关将现有联合连接导入BlueXP 的更多信息。"

改进的联合管理允许您：

- 将多个已验证的域添加到联合连接，允许您将多个域与同一个身份提供商 (IdP) 一起使用。
- 在需要时禁用或删除联合连接，让您控制用户访问和安全。
- 使用 IAM 角色控制对联合管理的访问。

"了解有关BlueXP中的身份联合的更多信息。"

BlueXP backup and recovery、 **BlueXP disaster recovery**和联合管理的新访问角色

BlueXP现在支持使用 IAM 角色实现以下功能和数据服务：

- BlueXP backup and recovery

- BlueXP disaster recovery
- 联邦

"了解有关使用访问角色的更多信息。"

2025年6月9日

连接器 3.9.53

BlueXP Connector 的此版本包括安全性改进和错误修复。

3.9.53 版本适用于标准模式和限制模式。

磁盘空间使用情况警报

通知中心现在包含连接器上磁盘空间使用情况的警报。"了解更多信息。"

审计改进

时间线现在包括用户的登录和注销事件。您可以看到登录活动的时间，这有助于审计和安全监控。具有组织管理员角色的 API 用户可以通过添加以下信息来查看登录用户的电子邮件地址 `includeUserData=true``参数如下： `/audit/<account_id>?includeUserData=true` 。

BlueXP中提供Keystone订阅管理

您可以从BlueXP管理您的NetApp Keystone订阅。

"了解BlueXP中的Keystone订阅管理。"

BlueXP身份和访问管理（IAM）

多重身份验证 (MFA)

非联合用户可以为其BlueXP帐户启用 MFA 以提高安全性。管理员可以管理 MFA 设置，包括根据需要为用户重置或禁用 MFA。这仅在标准模式下受支持。

"了解如何为自己设置多重身份验证。" "了解如何为用户管理多重身份验证。"

工作负载

您现在可以从BlueXP中的凭证页面查看和删除Amazon FSx for NetApp ONTAP凭证。

2025年5月29日

私人模式发布（3.9.52）

新的私人模式版本现已可从 "NetApp 支持站点"

3.9.52 版本包括以下BlueXP组件和服务的更新。

组件或服务	此版本中包含的版本	自上次私人模式发布以来的变化
连接器	3.9.52, 3.9.51	前往 "BlueXP连接器页面中的新功能"并参考版本 3.9.52 和 3.9.50 所包含的更改。
备份和恢复	2025年5月12日	前往 "BlueXP backup and recovery页面中的新功能"并参考 2025 年 5 月版本中包含的更改。
分类	2025 年 5 月 12 日（版本 1.43）	前往 "BlueXP classification页面中的新功能"并参考 1.38 至 1.371.41 版本中包含的更改。

有关私人模式的更多详细信息，包括如何升级，请参阅以下内容：

- "了解私人模式"
- "了解如何在私人模式下开始使用BlueXP"
- "了解如何在使用私有模式时升级连接器"

2025年5月12日

连接器 3.9.52

BlueXP Connector 的此版本包括一些小的安全改进和错误修复，以及一些额外的更新。

目前，3.9.52 版本适用于标准模式和限制模式。

支持 Docker 27 和 Docker 28

连接器现在支持 Docker 27 和 Docker 28。

Cloud Volumes ONTAP

当连接器不合规或停机超过 14 天时， Cloud Volumes ONTAP节点不再关闭。当Cloud Volumes ONTAP失去对连接器的访问权限时，它仍会发送事件管理消息。此更改是为了确保即使连接器长时间处于关闭状态， Cloud Volumes ONTAP仍可继续运行。它不会改变连接器的合规性要求。

BlueXP中提供Keystone管理

BlueXP中的NetApp Keystone测试版增加了对Keystone管理的访问权限。您可以从BlueXP左侧导航栏访问NetApp Keystone测试版的注册页面。

BlueXP身份和访问管理（IAM）

新的存储管理角色

存储管理员、系统健康专家和存储查看器角色可用，可以分配给用户。

这些角色使您能够管理组织中的谁可以发现和管理存储资源，以及查看存储健康信息和执行软件更新。

这些角色支持控制对以下存储资源的访问：

- E系列系统
- StorageGRID系统
- 本地ONTAP系统

您还可以使用这些角色来控制对以下BlueXP服务的访问：

- 软件更新
- 数字顾问
- 运营弹性
- 经济效益
- 可持续性

已添加以下角色：

- 存储管理员

  管理组织内存储资源的存储健康、治理和发现。该角色还可以对存储资源执行软件更新。

- 系统健康专家

  管理组织内存储资源的存储健康和治理。该角色还可以对存储资源执行软件更新。此角色不能修改或删除工作环境。

- 存储查看器

  查看存储健康信息和治理数据。

  "了解访问角色。"

2025年4月14日

连接器 3.9.51

BlueXP Connector 的此版本包含一些小的安全改进和错误修复。

目前，3.9.51 版本适用于标准模式和限制模式。

连接器下载的安全端点现在支持备份和恢复以及勒索软件保护

如果您正在使用备份和恢复或勒索软件保护，您现在可以使用安全端点进行连接器下载。"了解连接器下载的安全端点。"

BlueXP身份和访问管理（IAM）

- 必须为没有组织管理员或文件夹或项目管理员的用户分配勒索软件保护角色才能访问勒索软件保护。您可以为用户分配以下两个角色之一：勒索软件保护管理员或勒索软件保护查看者。
- 没有组织管理员或文件夹或项目管理员的用户必须分配Keystone角色才能访问Keystone。您可以为用户分配两个角色之一： Keystone管理员或Keystone查看者。

"了解访问角色。"

- 如果您具有组织管理员或文件夹或项目管理员角色，您现在可以将Keystone订阅与 IAM 项目关联。将Keystone订阅与 IAM 项目关联允许您在BlueXP中控制对Keystone的访问。

2025年3月28日

私人模式发布（**3.9.50**）

新的私人模式版本现已可从 "NetApp 支持站点"

3.9.50 版本包括以下BlueXP组件和服务的更新。

组件或服务	此版本中包含的版本	自上次私人模式发布以来的变化
连接器	3.9.50, 3.9.49	前往 "BlueXP连接器页面中的新功能"并参考版本 3.9.50 和 3.9.49 所包含的更改。
备份和恢复	2025年3月17日	前往 "BlueXP backup and recovery页面中的新功能"并参考 2024 年 3 月版本中包含的更改。
分类	2025 年 3 月 10 日（版本 1.41）	前往 "BlueXP classification页面中的新功能"并参考 1.38 至 1.371.41 版本中包含的更改。

有关私人模式的更多详细信息，包括如何升级，请参阅以下内容：

- "了解私人模式"
- "了解如何在私人模式下开始使用BlueXP"
- "了解如何在使用私有模式时升级连接器"

2025年3月10日

连接器 **3.9.50**

BlueXP Connector 的此版本包含一些小的安全改进和错误修复。

- 现在，操作系统上启用了 SELinux 的连接器支持对Cloud Volumes ONTAP系统的管理。

  "了解有关 SELinux 的更多信息"

目前，3.9.50 版本适用于标准模式和限制模式。

NetApp Keystone测试版现已在**BlueXP**中推出

NetApp Keystone即将由BlueXP推出，目前处于测试阶段。您可以从BlueXP左侧导航栏访问NetApp Keystone测试版的注册页面。

2025年3月6日

连接器 3.9.49 更新

BlueXP使用连接器时ONTAP系统管理器访问

BlueXP管理员（具有组织管理员角色的用户）可以配置BlueXP以提示用户输入其ONTAP凭据以访问ONTAP系统管理器。启用此设置后，用户每次都需要输入其ONTAP凭据，因为它们不存储在BlueXP中。

此功能在连接器版本 3.9.49 及更高版本中可用。"了解如何配置凭据设置。" 。

连接器 3.9.48 更新

能够禁用连接器的自动升级设置

您可以禁用连接器的自动升级功能。

当您在标准模式或受限模式下使用BlueXP时，只要连接器具有出站互联网访问权限以获取软件更新， BlueXP就会自动将您的连接器升级到最新版本。如果您需要手动管理连接器的升级时间，现在可以禁用标准模式或受限模式的自动升级。

此更改不会影响BlueXP私人模式，在该模式下您必须始终自行升级连接器。

此功能在连接器版本 3.9.48 及更高版本中可用。

"了解如何禁用连接器的自动升级。"

2025年2月18日

私人模式发布（3.9.48）

新的私人模式版本现已可从 "NetApp 支持站点"

3.9.48 版本包括以下BlueXP组件和服务的更新。

组件或服务	此版本中包含的版本	自上次私人模式发布以来的变化
连接器	3.9.48	前往 "BlueXP连接器页面中的新功能"并参考 3.9.48 版本所包含的更改。
备份和恢复	2025年2月21日	前往 "BlueXP backup and recovery 页面中的新功能"并参考 2025 年 2 月版本中包含的更改。
分类	2025 年 1 月 22 日（版本 1.39）	前往 "BlueXP classification页面中的新功能"并参考 1.39 版本中包含的更改。

2025年2月10日

连接器 3.9.49

BlueXP Connector 的此版本包含一些小的安全改进和错误修复。

目前，3.9.49 版本适用于标准模式和限制模式。

BlueXP身份和访问管理 (IAM)

- 支持为BlueXP用户分配多个角色。
- 支持在BlueXP组织（Org/folder/project）的多个资源上分配角色
- 角色现在与两个类别之一相关联：平台和数据服务。

限制模式现在使用BlueXP IAM

BlueXP身份和访问管理 (IAM) 现在以受限模式使用。

BlueXP身份和访问管理 (IAM) 是一种资源和访问管理模型，它取代并增强了在标准和受限模式下使用BlueXP时BlueXP帐户提供的先前功能。

相关信息

- "了解BlueXP IAM"
- "开始使用BlueXP IAM"

BlueXP IAM 提供更精细的资源和权限管理：

- 顶级_组织_使您能够管理各个_项目_的访问权限。
- _文件夹_使您能够将相关项目分组在一起。
- 增强的资源管理使您能够将资源与一个或多个文件夹或项目关联。

  例如，您可以将一个Cloud Volumes ONTAP系统与多个项目关联。

- 增强的访问管理使您能够为组织层次结构不同级别的成员分配角色。

这些增强功能可以更好地控制用户可以执行的操作和可以访问的资源。

BlueXP IAM 在受限模式下如何影响您的现有帐户

当您登录BlueXP时，您会注意到以下变化：

- 您的_帐户_现在称为_组织_
- 您的_工作区_现在称为_项目_
- 用户角色的名称已更改：
  - 帐户管理员 现为 组织管理员
  - 工作区管理员_现在是_文件夹或项目管理员
  - 合规性查看器_现为_分类查看器
- 在“设置”下，您可以访问BlueXP身份和访问管理以利用这些增强功能

请注意以下事项：

- 您的现有用户或工作环境没有任何变化。
- 虽然角色的名称已经改变，但从权限的角度来看并没有什么区别。用户将继续可以访问与以前相同的工作环境。
- 您登录BlueXP的方式没有任何变化。 BlueXP IAM 与NetApp云登录、 NetApp支持站点凭证和联合连接配合使用，就像BlueXP帐户一样。
- 如果您有多个BlueXP帐户，那么您现在就有多个BlueXP组织。

BlueXP IAM 的 API

此更改为BlueXP IAM 引入了一个新的 API，但它与以前的租赁 API 向后兼容。 "了解BlueXP IAM 的 API"

支持的部署模式

在标准和受限模式下使用BlueXP时支持BlueXP IAM。如果您在私人模式下使用BlueXP ，那么您将继续使用BlueXP *account* 来管理工作区、用户和资源。

私人模式发布（**3.9.48**）

新的私人模式版本现已可从 "NetApp 支持站点"

3.9.48 版本包括以下BlueXP组件和服务的更新。

组件或服务	此版本中包含的版本	自上次私人模式发布以来的变化
连接器	3.9.48	前往 "BlueXP连接器页面中的新功能"并参考 3.9.48 版本所包含的更改。
备份和恢复	2025年2月21日	前往 "BlueXP backup and recovery页面中的新功能"并参考 2025 年 2 月版本中包含的更改。
分类	2025 年 1 月 22 日（版本 1.39）	前往 "BlueXP classification页面中的新功能"并参考 1.39 版本中包含的更改。

2025年1月13日

连接器 **3.9.48**

BlueXP Connector 的此版本包含一些小的安全改进和错误修复。

目前，3.9.48 版本适用于标准模式和限制模式。

BlueXP身份和访问管理

- 资源页面现在显示未发现的资源。未发现的资源是BlueXP知道但您尚未为其创建工作环境的存储资源。例如，数字顾问中显示的尚未具有工作环境的资源在资源页面上显示为未发现的资源。
- Amazon FSx for NetApp ONTAP资源不会显示在 IAM 资源页面上，因为您无法将它们与 IAM 角色关联。您可以在各自的画布上或从工作负载中查看这些资源。

为其他**BlueXP**服务创建支持案例

注册BlueXP以获得支持后，您可以直接从BlueXP基于 Web 的控制台创建支持案例。创建案例时，您需要选择与该问题相关的服务。

从此版本开始，您现在可以创建支持案例并将其与其他BlueXP服务关联：

- BlueXP disaster recovery
- BlueXP ransomware protection

"了解有关创建支持案例的更多信息" 。

2024年12月16日

用于获取连接器图像的新安全端点

当您安装连接器或发生自动升级时，连接器会联系存储库来下载用于安装或升级的映像。默认情况下，连接器始终联系以下端点：

- https://*.blob.core.windows.net
- \ https://cloudmanagerinfraprod.azurecr.io

第一个端点包含一个通配符，因为我们无法提供明确的位置。存储库的负载平衡由服务提供商管理，这意味着下载可以从不同的端点进行。

为了提高安全性，连接器现在可以从专用端点下载安装和升级图像：

- \ https://bluexpinfraprod.eastus2.data.azurecr.io
- \ https://bluexpinfraprod.azurecr.io

我们建议您从防火墙规则中删除现有端点并允许新端点，然后开始使用这些新端点。

从连接器 3.9.47 版本开始支持这些新端点。与连接器的先前版本不具有向后兼容性。

请注意以下事项：

- 现有的端点仍然受支持。如果您不想使用新的端点，则无需进行任何更改。
- 连接器首先联系现有的端点。如果这些端点无法访问，连接器会自动联系新的端点。
- 以下场景不支持新端点：
  - 如果连接器安装在政府区域。
  - 如果您将连接器与BlueXP backup and recovery或BlueXP ransomware protection一起使用。

  对于这两种情况，您都可以继续使用现有的端点。

2024年12月9日

连接器 **3.9.47**

此版本的BlueXP连接器包括错误修复和对连接器安装期间联系的端点的更改。

目前，3.9.47 版本适用于标准模式和限制模式。

安装期间联系**NetApp**支持的端点
当您手动安装连接器时，安装程序不再联系 \ https://support.netapp.com.

安装程序仍然联系 \ https://mysupport.netapp.com.

BlueXP身份和访问管理

连接器页面仅列出当前可用的连接器。它不再显示您已删除的连接器。

2024年11月26日

私人模式发布（**3.9.46**）

新的私人模式版本现已可从 "NetApp 支持站点"

3.9.46 版本包括以下BlueXP组件和服务的更新。

组件或服务	此版本中包含的版本	自上次私人模式发布以来的变化
连接器	3.9.46	轻微的安全改进和错误修复
备份和恢复	2024年11月22日	前往 "BlueXP backup and recovery页面中的新功能"并参考 2024 年 11 月版本中包含的更改
分类	2024 年 11 月 4 日（版本 1.37）	前往 "BlueXP classification页面中的新功能"并参考 1.32 至 1.37 版本中包含的更改
Cloud Volumes ONTAP管理	2024年11月11日	前往 "Cloud Volumes ONTAP管理页面的新增功能"并参考 2024 年 10 月和 2024 年 11 月版本中包含的更改
本地ONTAP集群管理	2024年11月26日	前往 "本地ONTAP集群管理页面的新增功能"并参考 2024 年 11 月版本中包含的更改

虽然BlueXP digital wallet和BlueXP replication也包含在私人模式中，但与之前的私人模式版本相比没有任何变化。

有关私人模式的更多详细信息，包括如何升级，请参阅以下内容：

- "了解私人模式"
- "了解如何在私人模式下开始使用BlueXP"
- "了解如何在使用私有模式时升级连接器"

2024年11月11日

连接器 **3.9.46**

BlueXP Connector 的此版本包含一些小的安全改进和错误修复。

目前，3.9.46 版本适用于标准模式和限制模式。

IAM 项目的 **ID**

您现在可以从BlueXP身份和访问管理中查看项目的 ID。您可能需要在进行 API 调用时使用该 ID。

"了解如何获取项目 ID" 。

2024年10月10日

连接器 **3.9.45** 补丁

此补丁包括错误修复。

2024年10月7日

BlueXP身份和访问管理

BlueXP身份和访问管理 (IAM) 是一种新的资源和访问管理模型，它取代并增强了在标准模式下使用BlueXP时BlueXP帐户提供的先前功能。

BlueXP IAM 提供更精细的资源和权限管理：

- 顶级_组织_使您能够管理各个_项目_的访问权限。
- _文件夹_使您能够将相关项目分组在一起。
- 增强的资源管理使您能够将资源与一个或多个文件夹或项目关联。

  例如，您可以将一个Cloud Volumes ONTAP系统与多个项目关联。

- 增强的访问管理使您能够为组织层次结构不同级别的成员分配角色。

这些增强功能可以更好地控制用户可以执行的操作和可以访问的资源。

BlueXP IAM 如何影响您的现有帐户

当您登录BlueXP时，您会注意到以下变化：

- 您的_帐户_现在称为_组织_
- 您的_工作区_现在称为_项目_
- 用户角色的名称已更改：
  - 帐户管理员 现为 组织管理员
  - 工作区管理员_现在是_文件夹或项目管理员

- 合规性查看器_现为_分类查看器

- 在“设置”下，您可以访问BlueXP身份和访问管理以利用这些增强功能

请注意以下事项：

- 您的现有用户或工作环境没有任何变化。
- 虽然角色的名称已经改变，但从权限的角度来看并没有什么区别。用户将继续可以访问与以前相同的工作环境。
- 您登录BlueXP的方式没有任何变化。 BlueXP IAM 与NetApp云登录、 NetApp支持站点凭证和联合连接配合使用，就像BlueXP帐户一样。
- 如果您有多个BlueXP帐户，那么您现在就有多个BlueXP组织。

BlueXP IAM 的 **API**

此更改为BlueXP IAM 引入了一个新的 API，但它与以前的租赁 API 向后兼容。 "了解BlueXP IAM 的 API"

支持的部署模式

在标准模式下使用BlueXP时支持BlueXP IAM。如果您在受限模式或私人模式下使用BlueXP ，那么您将继续使用BlueXP _帐户_来管理工作区、用户和资源。

下一步

- "了解BlueXP IAM"
- "开始使用BlueXP IAM"

连接器 **3.9.45**

此版本包括扩展的操作系统支持和错误修复。

3.9.45 版本适用于标准模式和限制模式。

支持 **Ubuntu 24.04 LTS**

从 3.9.45 版本开始， BlueXP现在支持在标准模式或受限模式下使用BlueXP时在 Ubuntu 24.04 LTS 主机上新安装 Connector。

"查看连接器主机要求" 。

RHEL 主机支持 **SELinux**

BlueXP现在支持在强制模式或许可模式下启用 SELinux 的 Red Hat Enterprise Linux 主机的连接器。

对 SELinux 的支持从 3.9.40 版本开始适用于标准模式和限制模式，从 3.9.42 版本开始适用于私有模式。

请注意以下限制：

- BlueXP不支持 Ubuntu 主机的 SELinux。
- 操作系统上启用了 SELinux 的连接器不支持对Cloud Volumes ONTAP系统的管理。

"了解有关 SELinux 的更多信息"

2024年9月30日

私人模式发布（**3.9.44**）

现在可以从NetApp支持站点下载新的私有模式版本。

此版本包括支持私人模式的以下版本的BlueXP组件和服务。

服务	包含的版本
连接器	3.9.44
备份和恢复	2024年9月27日
分类	2024 年 5 月 15 日（版本 1.31）
Cloud Volumes ONTAP管理	2024年9月9日
数字钱包	2023 年 7 月 30 日
本地ONTAP集群管理	2024年4月22日
复制	2022年9月18日

对于连接器，3.9.44 私有模式版本包括 2024 年 8 月和 2024 年 9 月版本中引入的更新。最值得注意的是，支持 Red Hat Enterprise Linux 9.4。

要了解有关这些BlueXP组件和服务版本中包含的内容的更多信息，请参阅每个BlueXP服务的发行说明：

- "2024 年 9 月发布的 Connector 中的新增功能"
- "2024 年 8 月发布的 Connector 中的新增功能"
- "BlueXP backup and recovery的新功能"
- "BlueXP classification的新功能"
- "BlueXP中的Cloud Volumes ONTAP管理有哪些新功能"

有关私人模式的更多详细信息，包括如何升级，请参阅以下内容：

- "了解私人模式"
- "了解如何在私人模式下开始使用BlueXP"
- "了解如何在使用私有模式时升级连接器"

2024年9月9日

连接器 **3.9.44**

此版本包括对 Docker Engine 26 的支持、对 SSL 证书的增强以及错误修复。

3.9.44 版本适用于标准模式和限制模式。

新安装支持 **Docker Engine 26**

从 Connector 3.9.44 版本开始，Docker Engine 26 现在支持在 Ubuntu 主机上安装_new_ Connector。

如果您有在 3.9.44 版本之前创建的现有连接器，那么 Docker Engine 25.0.5 仍然是 Ubuntu 主机上支持的最高版本。

"了解有关 Docker Engine 要求的更多信息" 。

更新了本地 **UI** 访问的 **SSL** 证书

当您在受限模式或私有模式下使用BlueXP时，可以从部署在云区域或本地的连接器虚拟机访问用户界面。默认情况下， BlueXP使用自签名 SSL 证书为在连接器上运行的基于 Web 的控制台提供安全的 HTTPS 访问。

在此版本中，我们对新的和现有的连接器的 SSL 证书进行了更改：

- 证书的通用名称现在与短主机名匹配
- 证书主体备用名称是主机的完全限定域名 (FQDN)

支持 **RHEL 9.4**

现在，在标准模式或受限模式下使用BlueXP时， BlueXP支持在 Red Hat Enterprise Linux 9.4 主机上安装连接器。

从 Connector 3.9.40 版本开始支持 RHEL 9.4。

标准模式和限制模式支持的 RHEL 版本的更新列表现在包括以下内容：

- 8.6 至 8.10
- 9.1 至 9.4

"了解连接器对 RHEL 8 和 9 的支持" 。

所有 **RHEL** 版本均支持 **Podman 4.9.4**

Podman 4.9.4 现已支持所有受支持的 Red Hat Enterprise Linux 版本。版本 4.9.4 之前仅支持 RHEL 8.10。

更新后支持的 Podman 版本列表包括 Red Hat Enterprise Linux 主机的 4.6.1 和 4.9.4。

从 Connector 3.9.40 版本开始，RHEL 主机需要 Podman。

"了解连接器对 RHEL 8 和 9 的支持" 。

更新了 **AWS** 和 **Azure** 权限

我们更新了连接器的 AWS 和 Azure 策略，以删除不再需要的权限。这些权限与BlueXP边缘缓存以及 Kubernetes 集群的发现和管理有关，自 2024 年 8 月起不再受支持。

- "了解 AWS 策略中的变化" 。
- "了解 Azure 策略中的变更" 。

2024年8月22日

连接器 **3.9.43** 补丁

我们更新了连接器以支持Cloud Volumes ONTAP 9.15.1 版本。

对此版本的支持包括对 Azure 连接器策略的更新。该策略现在包括以下权限：

```
"Microsoft.Compute/virtualMachineScaleSets/write",
"Microsoft.Compute/virtualMachineScaleSets/read",
"Microsoft.Compute/virtualMachineScaleSets/delete"
```

Cloud Volumes ONTAP支持虚拟机规模集需要这些权限。如果您有现有的连接器并且想要使用此新功能，则需要将这些权限添加到与您的 Azure 凭据关联的自定义角色。

- "了解Cloud Volumes ONTAP 9.15.1 版本"
- "查看连接器的 Azure 权限" 。

2024年8月8日

连接器 **3.9.43**

此版本包含一些小的改进和错误修复。

3.9.43 版本适用于标准模式和限制模式。

更新了 **CPU** 和 **RAM** 要求

为了提供更高的可靠性并提高BlueXP和 Connector 的性能，我们现在需要为 Connector 虚拟机提供额外的 CPU 和 RAM：

- CPU：8 核或 8 个 vCPU（之前的要求是 4 个）
- RAM：32 GB（之前的要求是 14 GB）

由于这一变化，从BlueXP或云提供商的市场部署连接器时的默认 VM 实例类型如下：

- AWS：t3.2xlarge
- Azure：Standard_D8s_v3
- 谷歌云：n2-standard-8

更新后的 CPU 和 RAM 要求适用于所有新连接器。对于现有的连接器，建议增加 CPU 和 RAM 以提供更高的性能和可靠性。

支持 **RHEL 8.10** 的 **Podman 4.9.4**

现在，在 Red Hat Enterprise Linux 8.10 主机上安装连接器时支持 Podman 版本 4.9.4。

身份联合的用户验证

如果您将身份联合与BlueXP结合使用，则每个首次登录BlueXP 的用户都需要填写一份快速表格来验证其身份。

2024年7月31日

私人模式发布（**3.9.42**）

现在可以从NetApp支持站点下载新的私有模式版本。

支持 **RHEL 8** 和 **9**

此版本包括在私人模式下使用BlueXP时在 Red Hat Enterprise Linux 8 或 9 主机上安装连接器的支持。支持以下版本的 RHEL：

- 8.6 至 8.10
- 9.1 至 9.3

Podman 是这些操作系统所必需的容器编排工具。

您应该了解 Podman 的要求、已知的限制、操作系统支持的摘要、如果您有 RHEL 7 主机该怎么做、如何开始等等。

"了解连接器对 RHEL 8 和 9 的支持" 。

此版本包含的版本

此版本包括支持私人模式的以下版本的BlueXP服务。

服务	包含的版本
连接器	3.9.42
备份和恢复	2024年7月18日
分类	2024 年 7 月 1 日（版本 1.33）
Cloud Volumes ONTAP管理	2024年6月10日
数字钱包	2023 年 7 月 30 日
本地ONTAP集群管理	2023 年 7 月 30 日
复制	2022年9月18日

要了解有关这些BlueXP服务版本中包含的内容的更多信息，请参阅每个BlueXP服务的发行说明。

- "了解私人模式"
- "了解如何在私人模式下开始使用BlueXP"
- "了解如何在使用私有模式时升级连接器"
- "了解BlueXP backup and recovery的新功能"
- "了解BlueXP classification的新功能"
- "了解BlueXP中Cloud Volumes ONTAP管理的新功能"

2024年7月15日

支持 **RHEL 8.10**

BlueXP现在支持在使用标准模式或受限模式时在 Red Hat Enterprise Linux 8.10 主机上安装连接器。

从 Connector 3.9.40 版本开始支持 RHEL 8.10。

"了解连接器对 RHEL 8 和 9 的支持" 。

2024年7月8日

连接器 **3.9.42**

此版本包括一些小改进、错误修复以及对 AWS 加拿大西部（卡尔加里）地区连接器的支持。

3.9.42 版本适用于标准模式和限制模式。

更新了 **Docker Engine** 要求

当连接器安装在 Ubuntu 主机上时，Docker Engine 的最低支持版本现在为 23.0.6。之前是 19.3.1。

最高支持版本仍为25.0.5。

"查看连接器主机要求" 。

现在需要电子邮件验证

现在，注册BlueXP 的新用户需要验证他们的电子邮件地址才能登录。

2024年6月12日

连接器 **3.9.41**

BlueXP Connector 的此版本包含一些小的安全改进和错误修复。

3.9.41 版本适用于标准模式和限制模式。

2024年6月4日

私人模式发布（**3.9.40**）

现在可以从NetApp支持站点下载新的私有模式版本。此版本包括支持私人模式的以下版本的BlueXP服务。

请注意，此私有模式版本不包括对 Red Hat Enterprise Linux 8 和 9 的连接器的支持。

服务	包含的版本
连接器	3.9.40
备份和恢复	2024年5月17日
分类	2024 年 5 月 15 日（版本 1.31）

服务	包含的版本
Cloud Volumes ONTAP管理	2024年5月17日
数字钱包	2023 年 7 月 30 日
本地ONTAP集群管理	2023 年 7 月 30 日
复制	2022年9月18日

要了解有关这些BlueXP服务版本中包含的内容的更多信息，请参阅每个BlueXP服务的发行说明。

- "了解私人模式"
- "了解如何在私人模式下开始使用BlueXP"
- "了解如何在使用私有模式时升级连接器"
- "了解BlueXP backup and recovery的新功能"
- "了解BlueXP classification的新功能"
- "了解BlueXP中Cloud Volumes ONTAP管理的新功能"

2024年5月17日

连接器 3.9.40

BlueXP Connector 的此版本包括对其他操作系统的支持、小的安全改进和错误修复。

目前，3.9.40 版本适用于标准模式和限制模式。

支持 RHEL 8 和 9

在标准模式或限制模式下使用BlueXP时，运行以下版本的 Red Hat Enterprise Linux 且安装了_new_ Connector 的主机现在支持该连接器：

- 8.6 至 8.9
- 9.1 至 9.3

Podman 是这些操作系统所必需的容器编排工具。

您应该了解 Podman 的要求、已知的限制、操作系统支持的摘要、如果您有 RHEL 7 主机该怎么做、如何开始等等。

"了解连接器对 RHEL 8 和 9 的支持" 。

终止对 RHEL 7 和 CentOS 7 的支持

2024 年 6 月 30 日，RHEL 7 将达到维护终止（EOM），而 CentOS 7 将达到生命周期终止（EOL）。NetApp 将继续支持这些 Linux 发行版上的 Connector，直到 2024 年 6 月 30 日。

"了解如果现有的 Connector 在 RHEL 7 或 CentOS 7 上运行，该怎么办" 。

AWS 权限更新

在 3.9.38 版本中，我们更新了 AWS 的连接器策略以包含“ec2:DescribeAvailabilityZones”权限。现在需要此权限来支持具有Cloud Volumes ONTAP 的AWS 本地区域。

- "查看连接器的 AWS 权限" 。
- "了解有关 AWS 本地区域支持的更多信息"

NetApp控制台的已知限制

已知限制标识了该产品的此版本不支持或不能与其正确互操作的平台、设备或功能。仔细审查这些限制。

这些限制特定于 NEtApp 控制台和管理的设置：代理、软件即服务 (SaaS) 平台等等。

控制台代理限制

可能与 **172** 范围内的 **IP** 地址冲突

NetApp控制台部署了一个具有两个接口的代理，这两个接口的 IP 地址分别在 172.17.0.0/16 和 172.18.0.0/16 范围内。

如果您的网络具有配置了这些范围之一的子网，那么您可能会遇到控制台连接失败的情况。例如，在控制台中发现本地ONTAP集群可能会失败。

请参阅知识库文章"代理IP与现有网络冲突"有关如何更改代理接口的 IP 地址的说明。

不支持 **SSL** 解密

控制台不支持启用 SSL 解密的防火墙配置。如果启用了 SSL 解密，控制台中会出现错误消息，并且代理实例显示为非活动状态。

为了增强安全性，您可以选择"安装由证书颁发机构 (CA) 签名的 HTTPS 证书"。

加载本地 **UI** 时出现空白页

如果您加载在代理上运行的基于 Web 的控制台，界面有时可能无法显示，而只会显示空白页。

此问题与缓存问题有关。解决方法是使用隐身或私人网络浏览器会话。

不支持共享 **Linux** 主机

与其他应用程序共享的虚拟机不支持该代理。 VM 必须专用于代理软件。

第三方代理和扩展

代理虚拟机不支持第三方代理或虚拟机扩展。

受支持的 **Linux** 操作系统的变更

NetApp有时会在特定的 Linux 操作系统上添加和删除对控制台代理的支持，了解此支持如何影响您现有的控制台代理。

支持的操作系统

NetApp支持具有以下 Linux 操作系统的代理。

标准模式

手动安装

- Ubuntu 24.04 LTS
- Ubuntu 22.04 LTS
- Red Hat Enterprise Linux
  - 8.6 至 8.10
  - 9.1 至 9.4

从**NetApp**控制台部署

Ubuntu 22.04 LTS

从 **AWS Marketplace** 部署

Ubuntu 22.04 LTS

从 **Azure** 市场部署

Ubuntu 22.04 LTS

限制模式

手动安装

- Ubuntu 24.04 LTS
- Ubuntu 22.04 LTS
- Red Hat Enterprise Linux
  - 8.6 至 8.10
  - 9.1 至 9.4

从 **AWS Marketplace** 部署

Ubuntu 22.04 LTS

从 **Azure** 市场部署

Ubuntu 22.04 LTS

私人模式

手动安装

- Ubuntu 22.04 LTS
- Red Hat Enterprise Linux
  - 8.6 至 8.10
  - 9.1 至 9.4

支持 **RHEL 8** 和 **9**

请注意以下有关 RHEL 8 和 9 的支持：

限制

如果您在本地的 RHEL 8 或 9 主机上安装代理，则支持NetApp数据分类。如果 RHEL 8 或 9 主机位于 AWS、Azure 或 Google Cloud 中，则不受支持。

容器编排工具

在 RHEL 8 或 9 主机上安装控制台代理时，必须使用 Podman 工具作为容器编排工具。 RHEL 8 和 9 不支持 Docker Engine。

部署模式

在标准模式和受限模式下使用控制台时支持 RHEL 8 和 9。

支持的控制台代理版本

NetApp从以下版本的控制台代理开始支持 RHEL 8 和 9：

- 3.9.40 在标准模式或限制模式下使用控制台时

仅限新的手动安装

在您的本地或云中运行的主机上手动安装代理时，RHEL 8 和 9 支持_新_代理安装。

RHEL 升级

如果您在 RHEL 7 主机上运行现有代理， NetApp不支持将 RHEL 7 操作系统升级到 RHEL 8 或 9。了解有关 RHEL 7 或 CentOS 7 上现有控制台代理的更多信息 。

终止对 **RHEL 7** 和 **CentOS 7** 的支持

2024 年 6 月 30 日，RHEL 7 达到维护终止 (EOM)，而 CentOS 7 达到生命周期终止 (EOL)。 NetApp将于 2024 年 6 月 30 日停止对这些 Linux 发行版上的代理的支持。

"Red Hat：关于 Red Hat Enterprise Linux 7 维护终止你需要知道的事"

RHEL 7 或 **CentOS 7** 上的现有控制台代理

如果您现有的代理在 RHEL 7 或 CentOS 7 上运行， NetApp不支持将操作系统升级或转换为 RHEL 8 或 9。您需要在受支持的操作系统上创建一个新的代理。

1. 设置 RHEL 8 或 9 主机。
2. 安装 Podman。
3. 安装一个_新_代理。
4. 配置代理以发现先前代理所管理的系统。

相关信息

如何开始使用 **RHEL 8** 和 **9**

有关主机要求、Podman 要求以及安装 Podman 和 Cagent 的步骤的详细信息，请参阅以下页面：

标准模式

- "在本地安装并设置控制台代理"
- "在 AWS 中手动安装控制台代理"
- "在 Azure 中手动安装控制台代理"
- "在 Google Cloud 中手动安装控制台代理"

限制模式

"准备在受限模式下部署"

如何重新发现你的系统

部署新的控制台代理后，请参阅以下页面来重新发现您的系统。

- "添加现有的Cloud Volumes ONTAP系统"
- "发现本地ONTAP集群"
- "创建或发现 FSx for ONTAP系统"
- "创建Azure NetApp Files系统"
- "探索 E 系列系统"
- "了解StorageGRID系统"

开始使用

学习基础知识

了解**NetApp**控制台

NetApp控制台在企业级内部和云环境中提供对NetApp存储和NetApp数据服务的集中管理，提供实时洞察、更快的工作流程和简化的管理，高度安全且合规。

它是一种服务 (SaaS) 平台，提供存储管理、数据移动性、数据保护以及数据分析和控制。管理功能通过基于 Web 的控制台和 API 提供。

功能

该控制台通过集成数据服务统一混合多云的存储管理和保护，以保护和优化数据。

集中存储管理

使用控制台发现、部署和管理云和本地存储。

支持的云和本地存储

您可以从控制台管理以下类型的存储：

云存储解决方案

- Amazon FSx for NetApp ONTAP
- Azure NetApp Files
- Cloud Volumes ONTAP
- Google Cloud NetApp Volumes

本地闪存和对象存储

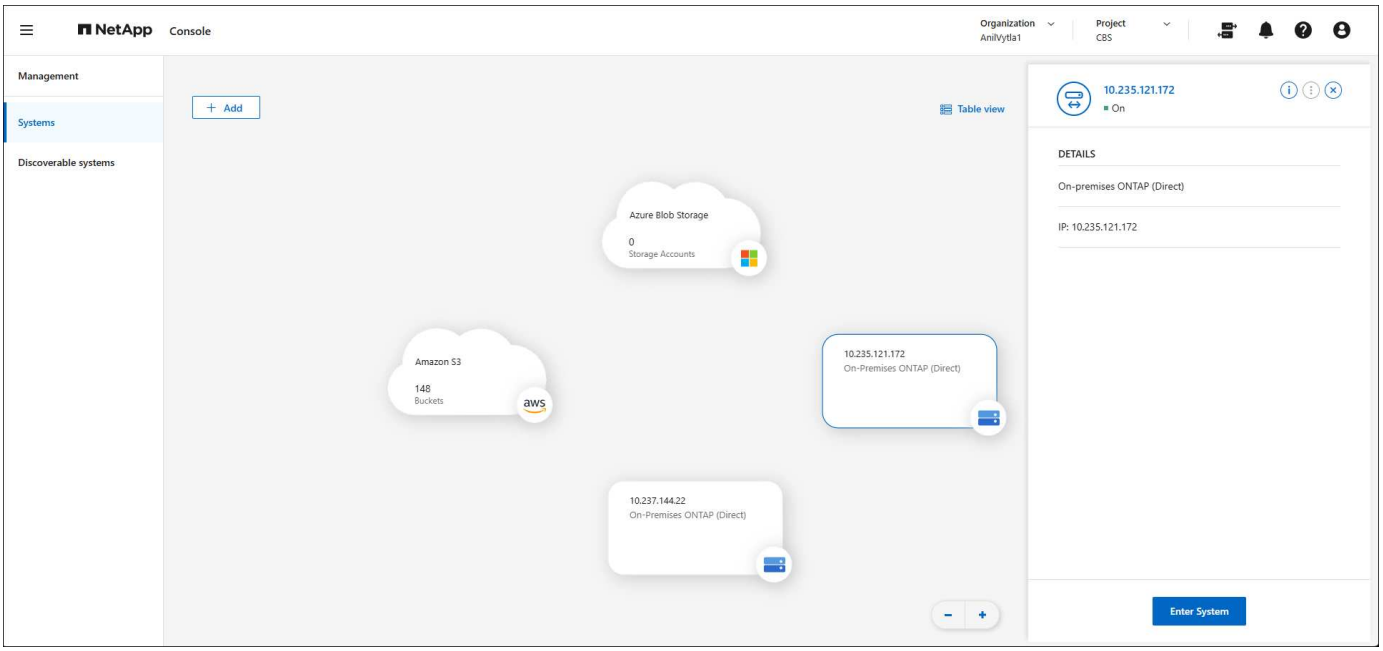
- E系列系统
- ONTAP集群
- StorageGRID系统

云对象存储

- Amazon S3 存储
- Azure Blob 存储
- Google Cloud Storage

存储管理

在控制台中，*systems* 代表已发现或已部署的存储。您可以选择一个系统将其与NetApp数据服务集成或管理存储，例如添加卷。



集成数据服务和存储管理，以保护、保障和优化数据

控制台提供数据服务以保护和维护存储可用性。

存储警报
: 查看与ONTAP环境中的容量、可用性、性能、保护和安全性相关的问题。

自动化中心
: 使用脚本解决方案来自动化NetApp产品和服务的部署和集成。

NetApp备份和恢复
: 备份和恢复云和本地数据。

NetApp数据分类
: 让您的应用程序数据和云环境隐私做好准备。

NetApp复制和同步
: 在本地和云数据存储之间同步数据。

NetApp数字顾问 **(Active IQ)**
: 使用预测分析和主动支持来优化您的数据基础设施。

许可证和订阅
: 管理和监控您的许可证和订阅。

NetApp灾难恢复
: 使用 VMware Cloud on Amazon FSx for ONTAP作为灾难恢复站点来保护本地 VMware 工作负载。

生命周期规划
: 识别当前或预测容量较低的集群并实施数据分层或额外容量建议。

NetApp勒索软件抵御能力

检测可能导致勒索软件攻击的异常。保护和恢复工作负载。

NetApp复制

在存储系统之间复制数据以支持备份和灾难恢复。

软件更新

自动评估、规划和执行ONTAP升级。

可持续性仪表板

分析存储系统的可持续性。

NetApp云分层

将您的本地ONTAP存储扩展到云端。

NetApp卷缓存

创建可写的缓存卷以加快数据访问速度或卸载访问量大的卷的流量。

NetApp工作负载

使用Amazon FSx for NetApp ONTAP设计、设置和操作关键工作负载。

"了解有关NetApp控制台和可用数据服务的更多信息"

支持的云提供商

该控制台使您能够管理云存储并使用 Amazon Web Services、Microsoft Azure 和 Google Cloud 中的云服务。

成本

NetApp控制台是免费的。如果您在云中部署控制台代理或使用在云中部署的受限模式，则会产生费用。某些NetApp数据服务会产生相关费用。https://bluexp.netapp.com/pricing["了解NetApp数据服务定价"^]

NetApp控制台的工作原理

NetApp控制台是一个基于 Web 的控制台，通过 SaaS 层、资源和访问管理系统、管理存储系统和启用NetApp数据服务的控制台代理以及不同的部署模式提供，以满足您的业务需求。

软件即服务

您可以通过 "基于网络的界面"和 API。这种 SaaS 体验使您能够在最新功能发布时自动访问它们。

身份和访问管理 **(IAM)**

控制台为资源和访问管理提供身份和访问管理 (IAM)。此 IAM 模型提供资源和权限的细粒度管理：

- 顶级组织使您能够管理各个项目之间的访问权限
- 文件夹 使您可以将相关项目分组在一起
- 资源管理使您可以将资源与一个或多个文件夹或项目关联

- 访问管理使您能够为组织层次结构中不同级别的成员分配角色
- "了解有关NetApp控制台中的 IAM 的更多信息"

控制台代理

一些附加功能和数据服务需要控制台代理。它使您能够管理本地和云环境中的资源和流程。您需要它来管理一些系统（例如， Cloud Volumes ONTAP）并使用一些NetApp数据服务。

"了解有关控制台代理的更多信息" 。

部署模式

NetApp为NetApp控制台提供了两种部署模式：_标准模式_使用软件即服务 (SaaS) 层实现全部功能，而_受限模式_限制出站连接。

NetApp继续为不需要出站连接的站点提供BlueXP 。 BlueXP仅在私人模式下可用。"了解没有互联网连接的站点的BlueXP （私人模式）。"

"了解有关部署模式的更多信息" 。

SOC 2 类型 **2** 认证

一家独立的注册会计师事务所和服务审计师审查了控制台，并确认其根据适用的信托服务标准实现了 SOC 2 类型 2 报告。

"查看 NetApp 的 SOC 2 报告"

了解**NetApp**控制台代理

_控制台代理_在您的云网络或本地网络中运行。您可以使用控制台代理将NetApp控制台服务连接到您的存储环境。

没有控制台代理您可以做什么

如果您不部署控制台代理，则某些控制台功能和服务可用：

- Amazon FSx for NetApp ONTAP

  某些操作需要控制台代理或NetApp Workloads 链接。 "了解哪些操作需要控制台代理或链接"

- 自动化中心
- Azure NetApp Files

  您不需要控制台代理来管理Azure NetApp Files，但需要使用NetApp数据分类来扫描Azure NetApp Files。

- Google Cloud NetApp Volumes
- NetApp复制和同步
- 数字顾问
- 监控许可证使用情况，订阅监控需要控制台代理

通常，您无需使用控制台代理即可向NetApp控制台添加许可证。

需要代理来添加Cloud Volumes ONTAP _基于节点的_许可证，因为数据来自安装在Cloud Volumes ONTAP系统上的许可证。

- 直接发现本地ONTAP集群

  您不需要控制台代理即可将本地ONTAP集群添加到控制台，但需要控制台代理来添加其他控制台功能和数据服务。

  "了解有关本地ONTAP集群的发现和管理选项的更多信息"

- 软件更新
- 可持续性
- NetApp工作负载

当需要控制台代理时

在标准模式下，控制台需要控制台代理来执行以下操作：

- 警报
- Amazon FSx for ONTAP管理功能
- Amazon S3 存储
- Azure Blob 存储
- NetApp备份和恢复
- 数据分类
- Cloud Volumes ONTAP
- NetApp灾难恢复
- E系列系统
- 经济效率[1]
- Google Cloud Storage 存储桶
- 本地ONTAP集群与NetApp数据服务的集成
- NetApp勒索软件抵御能力
- StorageGRID系统
- NetApp云分层
- NetApp卷缓存

[1] 您无需控制台代理即可访问这些服务，但需要控制台代理来启动操作。

您始终需要一个控制台代理才能在受限模式下使用控制台。

控制台代理必须始终处于运行状态

控制台代理是NetApp控制台的基本组成部分。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控制台部署模式" 。

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。如何开始取决于您是在标准模式还是受限模式下使用控制台。

- "了解NetApp控制台部署模式"
- "开始在标准模式下使用NetApp控制台"
- "开始在受限模式下使用NetApp控制台"

云权限

您需要特定权限才能直接从NetApp控制台创建控制台代理，并且需要另一组权限来创建控制台代理实例本身。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。

在标准或受限模式下，如果控制台代理可以访问互联网，它将自动更新。

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。

了解NetApp控制台部署模式

NetApp控制台提供多种部署模式，使您能够满足您的业务和安全需求。

- _标准模式_利用软件即服务 (SaaS) 层来提供完整的功能。用户通过基于 Web 的托管界面访问控制台
- _限制模式_适用于有连接限制并希望在自己的公共云中安装NetApp控制台的组织。用户通过托管在其云环境中的控制台代理上的基于 Web 的界面访问控制台。

  NetApp Console 在受限模式下限制流量、通信和数据，您必须确保您的环境（本地和云端）符合所需的规定。

概述

每种部署模式在出站连接、位置、安装、身份验证、数据服务和收费方法方面有所不同。

标准模式

您可以从基于 Web 的控制台使用 SaaS 服务。根据您计划使用的数据服务和功能，控制台组织管理员将创建一个或多个控制台代理来管理混合云环境中的数据。

此模式使用公共互联网上的加密数据传输。

限制模式

您在云中（在政府、主权或商业区域）安装控制台代理，并且它与NetApp控制台 SaaS 层的出站连接有限。

这种模式通常由州和地方政府以及受监管的公司使用。

了解有关 SaaS 层的出站连接的更多信息 。

BlueXP私人模式（仅限旧版**BlueXP**界面）

BlueXP私有模式（传统BlueXP接口）通常用于没有互联网连接的本地环境和安全云区域，其中包括 AWS Secret Cloud、AWS Top Secret Cloud 和 Azure IL6。 NetApp继续通过传统的BlueXP界面支持这些环境。"BlueXP私人模式的 PDF 文档"

下表提供了NetApp控制台的比较。

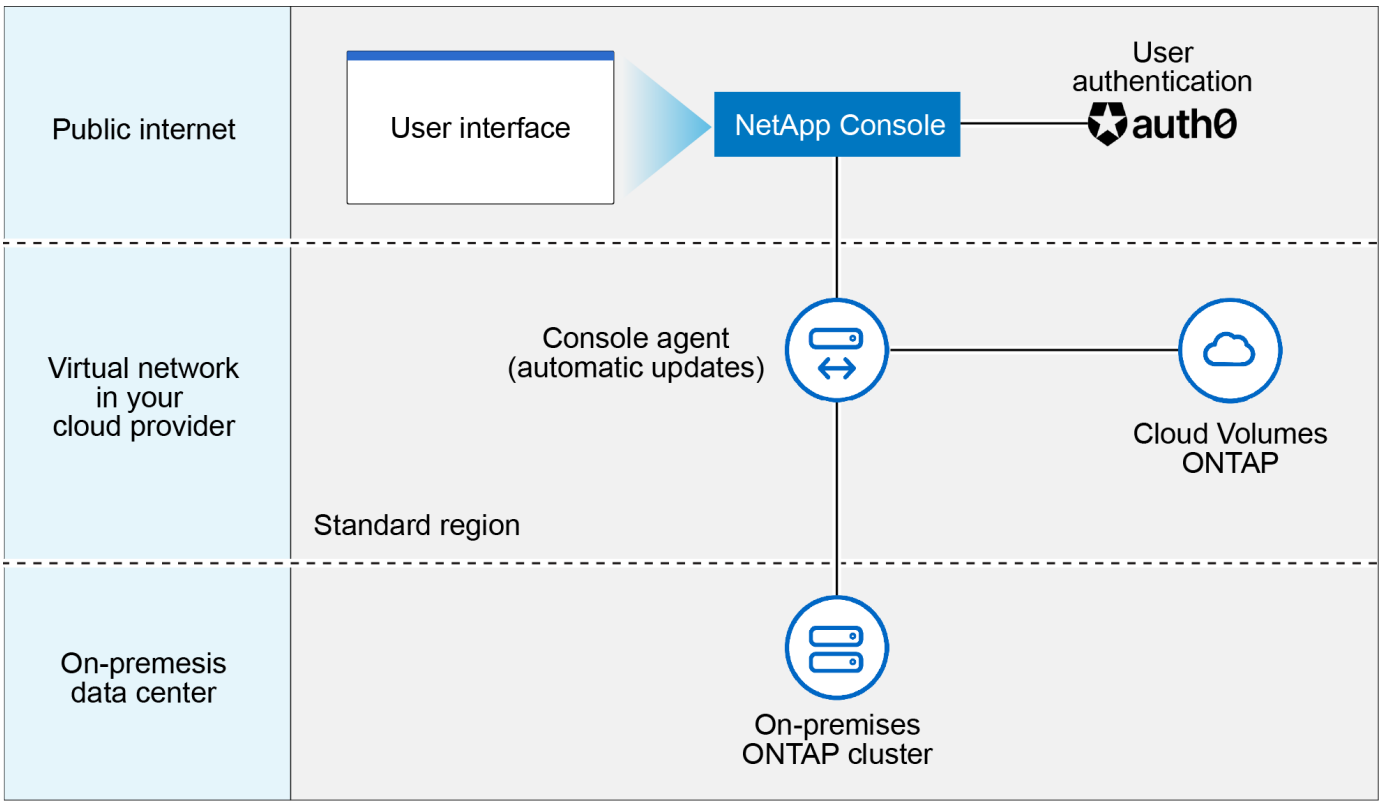
	标准模式	限制模式
需要连接到**NetApp Console SaaS** 层吗?	是	仅限出站
需要连接到您的云提供商吗?	是	是的，在该地区
控制台代理安装	从控制台、云市场或手动安装	云市场或手动安装
控制台代理升级	自动升级	自动升级
UI 访问	从控制台 SaaS 层	从代理虚拟机本地
API 端点	控制台 SaaS 层	控制台代理
身份验证	通过使用 auth0、NSS 登录或身份联合的 SaaS	通过使用 auth0 或身份联合的 SaaS

	标准模式	限制模式
多因素身份验证	适用于本地用户	不可用
存储和数据服务	全部支持	许多人受到支持
数据服务许可选项	市场订阅和 BYOL	市场订阅和 BYOL

阅读以下部分以了解有关这些模式的更多信息，包括支持哪些NetApp控制台功能和服务。

标准模式

下图是标准模式部署的示例。



控制台在标准模式下的工作方式如下：

出站沟通

需要从控制台代理到控制台 SaaS 层、到云提供商的公开可用资源以及到日常操作的其他基本组件的连接。

- "代理在 AWS 中联系的终端节点"
- "代理在 Azure 中联系的终结点"
- "代理在 Google Cloud 中联系的端点"

代理支持的位置

在标准模式下，代理在云端或您的场所受支持。

控制台代理安装

您可以使用以下方法之一安装代理：

- 从控制台
- 来自 AWS 或 Azure 市场
- 来自 Google Cloud SDK
- 在数据中心或云中的 Linux 主机上手动使用安装程序
- 在您的 VCenter 环境中使用提供的 OVA。

控制台代理升级

NetApp每月自动升级您的代理。

用户界面访问

可以通过 SaaS 层提供的基于 Web 的控制台访问用户界面。

API 端点

API 调用针对以下端点：\ https://api.bluexp.netapp.com

身份验证

使用 auth0 或NetApp支持站点 (NSS) 登录进行身份验证。身份联合可用。

支持的数据服务

支持所有NetApp数据服务。"了解有关NetApp数据服务的更多信息" 。

支持的许可选项

标准模式支持市场订阅和 BYOL；但是，支持的许可选项取决于您使用的NetApp数据服务。查看每项服务的文档以了解有关可用许可选项的更多信息。

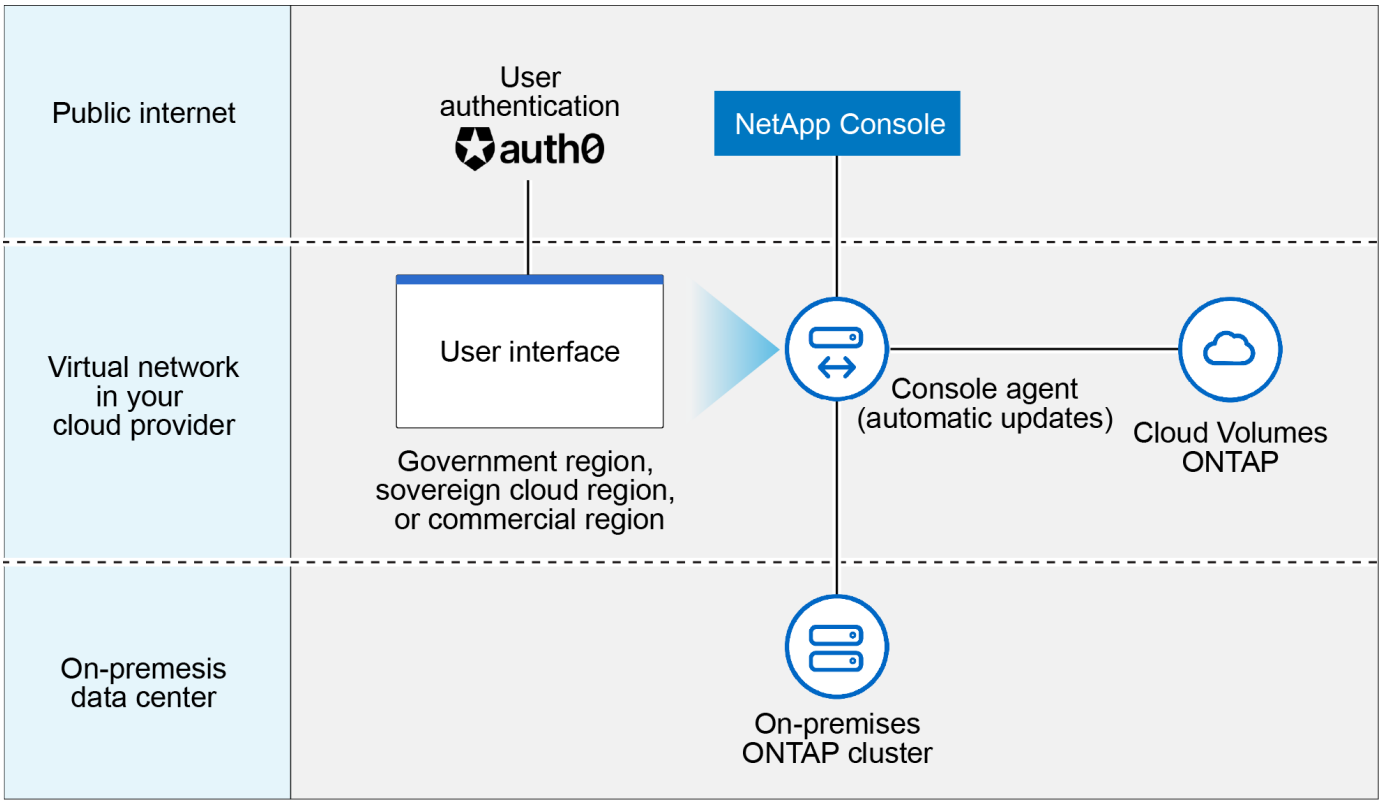
如何开始使用标准模式

前往 "NetApp控制台"并注册。

"了解如何开始使用标准模式" 。

限制模式

下图是限制模式部署的示例。



控制台在限制模式下的工作方式如下：

出站沟通

代理需要与控制台 SaaS 层建立出站连接，以实现数据服务、软件升级、身份验证和元数据传输。

控制台 SaaS 层不会发起与代理的通信。代理启动与控制台 SaaS 层的所有通信，根据需要提取或推送数据。

还需要与区域内的云提供商资源建立连接。

代理支持的位置

在受限模式下，代理在云中受支持：在政府区域、主权区域或商业区域。

控制台代理安装

您可以从 AWS 或 Azure 市场安装，也可以在您自己的 Linux 主机上手动安装，或者在您的 VCenter 环境中使用可下载的 OVA。

控制台代理升级

NetApp每月自动更新您的代理软件。

用户界面访问

您可以从部署在云区域中的代理虚拟机访问用户界面。

API 端点

对代理虚拟机进行 API 调用。

身份验证

通过 auth0 提供身份验证。身份联合也可用。

支持的存储管理和数据服务

以下存储和数据服务具有受限模式：

支持的服务	笔记
Azure NetApp Files	全力支持
备份和恢复	在政府区域和商业区域受限制模式支持。不支持在具有限制模式的主权区域使用。在受限模式下，NetApp Backup and Recovery 仅支持ONTAP卷数据的备份和恢复。 "查看ONTAP数据支持的备份目标列表"不支持应用程序数据和虚拟机数据的备份和恢复。
NetApp数据分类	在政府区域内受限制模式支持。不支持商业区域或具有限制模式的主权区域。
Cloud Volumes ONTAP	全力支持
许可证和订阅	您可以使用下面列出的受限模式支持的许可选项访问许可证和订阅信息。
本地ONTAP集群	使用控制台代理的发现和不使用控制台代理的发现（直接发现）均受支持。当您发现没有控制台代理的本地集群时，高级视图（系统管理器）不受支持。
复制	在政府区域内受限制模式支持。不支持商业区域或具有限制模式的主权区域。

支持的许可选项

限制模式支持以下许可选项：

- 市场订阅（按小时和按年合同）

  请注意以下事项：

  - 对于Cloud Volumes ONTAP，仅支持基于容量的许可。
  - 在 Azure 中，不支持与政府区域签订年度合同。
- BYOL

  对于Cloud Volumes ONTAP，BYOL 支持基于容量的许可和基于节点的许可。

如何开始使用受限模式

创建NetApp控制台组织时，您需要启用受限模式。

如果您还没有组织，当您第一次从手动安装的控制台代理或从云提供商的市场创建的控制台代理登录控制台时，系统会提示您创建组织并启用受限模式。

创建组织后，您无法更改限制模式设置。

"了解如何开始使用受限模式" 。

服务和功能比较

下表可以帮助您快速识别受限模式支持哪些服务和功能。

请注意，某些服务可能会受到限制。有关如何在受限模式下支持这些服务的更多详细信息，请参阅上面的部分。

产品领域	**NetApp**数据服务或功能	限制模式
存储 表格的此部分列出了对从控制台管理存储系统的支持。它没有指出NetApp Backup and Recovery 支持的备份目标。	适用于ONTAP 的Amazon FSx	否
	Amazon S3	否
	Azure Blob	否
	Azure NetApp Files	是
	Cloud Volumes ONTAP	是
	Google Cloud NetApp Volumes	否
	Google Cloud Storage	否
	本地ONTAP集群	是
	E 系列	否
	StorageGRID	否
数据服务	NetApp备份和恢复	是的https://docs.netapp.com/us-en/bluexp-backup-recovery/prev-ontap-protect-journey.html#support-for-sites-with-limited-internet-connectivity["查看ONTAP卷数据支持的备份目标列表"^]
	NetApp数据分类	是
	NetApp复制和同步	否
	NetApp灾难恢复	否
	NetApp勒索软件抵御能力	否
	NetApp复制	是
	NetApp云分层	否
	NetApp卷缓存	否
	NetApp工作负载工厂	否

产品领域	**NetApp**数据服务或功能	限制模式
特征	警报	否
	Digital Advisor	否
	许可证和订阅管理	是
	身份和访问管理	是
	凭据	是
	联邦	是
	生命周期规划	否
	多因素身份验证	是
	NSS 账户	是
	通知	是
	搜索	是
	软件更新	否
	可持续性	否
	审核	是

开始使用**NetApp**助手

开始使用**NetApp**控制台助手

如果您是首次使用NetApp控制台并具有组织管理员角色的用户，则可以使用控制台助手指导您完成初始设置过程。该助手可帮助您添加NetApp支持站点 (NSS) 帐户、添加控制台代理、添加集群以及添加许可证或订阅，从而更轻松地开始管理数据。

访问控制台助手所需的角色

控制台助手仅供具有组织管理员角色的用户使用。

控制台助手什么时候出现？

在完成强制性设置任务之前，控制台助手可在NetApp控制台主页上使用。

使用助手完成这些任务，其中一些是必需的：

- 添加NetApp支持站点 (NSS) 帐户。
- 通过部署控制台代理（强制步骤）连接到您的存储资产。
- 通过添加或发现集群来管理您的系统（强制步骤）。
- 添加市场订阅或 PAYGO 许可证。
- 开放数据服务链接。

启用控制台助手

默认情况下， NetApp控制台会在主页上为首次具有组织管理员角色的用户显示控制台助手。

只有当您或其他人完成必填项后，您才可以自行解散助手。完成必填项后，您组织中的所有用户都会关闭助手，并且不会再次出现。

使用控制台助手开始

控制台助手将指导您完成以下任务来设置NetApp控制台环境：

- 添加NetApp支持站点 (NSS) 帐户。
- 通过在本地或云端部署控制台代理来连接到您的存储资产。您可以手动部署它，也可以通过下载 OVA 来部署它。此步骤是必需的。
- 通过添加或发现集群来管理您的系统。此步骤是必需的。
- 添加市场订阅或 PAYGO 许可证。
- 了解有关NetApp数据服务的更多信息。

开始使用标准模式

入门工作流程（标准模式）

通过为控制台准备网络、注册并创建帐户以及（可选）创建控制台代理，以标准模式开始使用NetApp控制台。

在标准模式下，您可以访问由NetApp作为软件即服务 (SaaS) 产品托管的基于 Web 的控制台。在开始之前，请确保您了解"部署模式"和"控制台代理"。

1 "准备使用NetApp控制台的网络"

访问NetApp控制台的计算机应该与特定端点建立连接。如果您的网络限制出站访问，您应该确保允许这些端点。

2 "注册并创建组织"

前往 "NetApp控制台"并注册。您将可以选择创建一个组织，但如果您的公司已经有现有组织，则应跳过该步骤。

此时，您已登录并可以开始管理存储和使用Digital Advisor、 Amazon FSx for ONTAP、 Azure NetApp Files等服务。"了解没有控制台代理您可以做什么" 。

3 创建控制台代理

高级存储管理功能和某些NetApp数据服务要求您安装控制台代理。控制台代理使控制台能够管理混合云环境中的资源和流程。

您可以在云或本地网络中创建控制台代理。

- "详细了解何时需要控制台代理以及它们如何工作"
- "了解如何在 AWS 中创建控制台代理"
- "了解如何在 Azure 中创建控制台代理"
- "了解如何在 Google Cloud 中创建控制台代理"
- "了解如何在本地创建控制台代理"

要使用NetApp智能数据服务管理 Google Cloud 中的存储和数据，请确保控制台代理在 Google Cloud 中运行。

4 "订阅**NetApp**智能服务（可选）"

通过您的云提供商注册NetApp智能服务，按小时付费（PAYGO）或通过年度合同付费。 NetApp智能服务包括NetApp备份和恢复、 Cloud Volumes ONTAP、 NetApp云分层、 NetApp勒索软件恢复和NetApp灾难恢复。 NetApp数据分类包含在您的订阅中，无需额外付费。

准备**NetApp**控制台的网络访问

NetApp Console、 NetApp Console 代理和NetApp数据服务需要出站互联网访问以及联系必要端点的能力。

您需要为以下操作设置网络访问：

- 以软件即服务 (SaaS) 形式访问NetApp控制台的计算机
- 部署在本地或云中安装的控制台代理的网络位置。
- 某些NetApp数据服务的附加端点，包括Cloud Volumes ONTAP。

NetApp减少了控制台和控制台代理所需的网络端点，增强了安全性并简化了部署。重要的是，4.0.0 版本之前的所有部署都将继续得到全面支持。虽然以前的端点仍然可供现有代理使用，但NetApp强烈建议在确认代理升级成功后将防火墙规则更新到当前端点。"了解如何更新您的端点列表。"

NetApp控制台联系的端点

访问NetApp控制台的每台计算机都必须连接到下面列出的端点。

系统在两种情况下联系这些端点：

- 从计算机访问 "NetApp控制台"作为软件即服务（SaaS）。
- 从直接访问控制台代理主机的计算机，可以登录并进行设置，也可以从代理主机访问控制台。

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://support.netapp.com	获取许可信息并向NetApp支持发送AutoSupport消息。

端点	目的
\ 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控制台。
\ 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控制台中提供功能和服务。
\ 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。

为控制台代理准备网络

您可以在本地或云中安装控制台代理，它会联系端点以完成控制台发起的操作。

控制台代理必须能够访问与NetApp控制台相同的端点，以及根据安装代理的位置而定的其他端点。

在安装控制台代理之前设置网络端点访问。

- "为控制台代理设置 AWS 网络访问"
- "为控制台代理设置 Azure 网络访问"
- "为控制台代理设置 Google Cloud 网络访问"
- "为控制台代理设置本地网络访问"

为**Cloud Volumes ONTAP**准备网络

一些NetApp数据服务以及Cloud Volumes ONTAP要求代理具有额外的出站互联网访问权限。

Cloud Volumes ONTAP的端点

- "AWS 中的Cloud Volumes ONTAP端点"
- "Azure 中的Cloud Volumes ONTAP端点"
- "Google Cloud 中Cloud Volumes ONTAP的端点"

"请参阅相应的NetApp数据服务文档。"

注册或登录NetApp控制台

可以通过基于 Web 的控制台访问NetApp控制台。要开始使用控制台，您的第一步是注册或使用您的NetApp支持站点凭据登录，或者创建NetApp控制台登录。

关于此任务

首次访问控制台时，您可以使用以下选项之一注册或登录：

NetApp控制台登录

您可以通过创建登录名来注册。此身份验证方法要求您指定您的电子邮件地址和密码。验证电子邮件地址后，您可以登录并创建一个组织（如果您还不属于任何组织）。

NetApp支持站点 **(NSS)** 凭证

如果您已有NetApp支持站点凭证，则无需注册控制台。您使用 NSS 凭据登录，然后控制台会提示您创建一个组织（如果您还不属于任何组织）。

您将收到一次性密码 (OTP) 到注册的电子邮件地址。每次登录尝试都会生成一个新的 OTP。

联合连接

如果您的公司已经拥有NetApp控制台实例，则您的控制台管理员可能已经设置了单点登录，以使用来自您的公司目录（联合身份）的凭据登录。

"了解如何将身份联合与NetApp控制台结合使用" 。

步骤

1. 打开 Web 浏览器并转到 "NetApp控制台"
2. 如果您有NetApp支持站点帐户或已设置身份联合，请在“登录”页面直接输入与您的帐户关联的电子邮件地址。

   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*。

      请注意，注册表中只允许输入英文字符。

   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。

      您必须先执行此步骤才能登录控制台。
4. 登录后，请查看最终用户许可协议并接受条款。

   如果您的用户帐户尚不属于控制台组织，系统将提示您创建一个。
5. 在*欢迎*页面上，输入您的控制台组织的名称。

   控制台定义组织是控制台身份和访问管理 (IAM) 中的顶级元素。"了解 IAM" 。

   如果您的企业已经有一个组织并且您想加入该组织，请关闭控制台并要求组织管理员将您与该组织关联。添加后，您可以登录并访问控制台组织。"了解如何向现有组织添加成员" 。

6. 选择*让我们开始吧*。

创建控制台代理

AWS

AWS 中的控制台代理安装选项

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

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控制台在 AWS 中创建控制台代理

您可以直接从NetApp控制台在 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"
\ https://mysupport.netapp.com	获取许可信息并向NetApp支持发送AutoSupport消息。
\ https://support.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控制台。
\ 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控制台中提供功能和服务。

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控制台时，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数据分类来扫描公司数据源，则应在控制台代理和NetApp数据分类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 中部署控制台代理实例。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 中的控制台代理实例所需的权限。

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 中的控制台代理实例所需的权限。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实例，使控制台代理能够管理 AWS 资源。"查看控制台代理实例本身所需的权限" 。

```
{
  "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，它会为实例创建一个 IAM 角色和一个实例配置文件。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。
   - 输入实例的名称。
   - 向实例添加自定义标签（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，为实例指定 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 分钟才能准备好实例。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控制台管理 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"
\ https://mysupport.netapp.com	获取许可信息并向NetApp支持发送AutoSupport消息。
\ https://support.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控制台。
\ 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控制台中提供功能和服务。
\ 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数据分类来扫描公司数据源，则应在控制台代理和NetApp数据分类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

满足上述 CPU 和 RAM 要求的实例类型。我们推荐 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控制台代理列表"
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控制台" 。
   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控制台"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控制台管理 S3 存储桶"

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

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

与其他应用程序共享的主机不支持控制台代理。该主机必须是专用主机。主机可以是满足以下大小要求的任何架构：

- 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 Docker 或 Podman 的设计目的是在此目录中创建容器。具体来说，他们将在 `/var/lib/containers/storage`目录。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	9.1 至 9.4 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 查看 Podman 配置要求 。	在强制模式或宽容模式下受支持 • 操作系统上启用了 SELinux 的代理不支持对Cloud Volumes ONTAP系统的管理。
Ubuntu	24.04 LTS	3.9.45 或更高版本， NetApp控制台处于标准模式或受限模式	Docker Engine 23.06 至 28.0.0。	不支持

AWS EC2 实例类型

满足上述 CPU 和 RAM 要求的实例类型。我们推荐 t3.2xlarge。

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

如果在 EC2 实例上启用了 IMDSv2（这是新 EC2 实例的默认设置），则必须将实例上的 PUT 响应跳数限制更改为 3。如果您不更改 EC2 实例的限制，则在尝试设置代理时会收到 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"

/opt 中的磁盘空间

必须有 100 GiB 可用空间

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

/var 中的磁盘空间

必须有 20 GiB 可用空间

控制台代理需要此空间 `/var`因为 Docker 或 Podman 的设计目的是在此目录中创建容器。具体来说，他们将在 `/var/lib/containers/storage`目录。外部安装或符号链接不适用于此空间。

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 软件包版本 1.0.6
- 将 podman-compose 添加到 PATH 环境变量
- 如果使用 Red Hat Enterprise Linux 8，请验证您的 Podman 版本使用的是 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。

   对于 Red Hat Enterprise Linux 9：

```
sudo dnf install podman-2:<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 。

   对于 Red Hat Enterprise Linux 8：

```
sudo dnf install podman-3:<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。
6. 如果使用 Red Hat Enterprise：

   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。

   对于 Red Hat Enterprise Linux 9：

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

   对于 Red Hat Enterprise Linux 8：

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

7. 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。

8. 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。

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

      ```
      podman info | grep networkBackend
      ```

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

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

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

   d. 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。

9. 重新启动 podman。

```
systemctl restart podman
```

10. 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。

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**控制台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"
\ https://mysupport.netapp.com	获取许可信息并向NetApp支持发送AutoSupport消息。
\ https://support.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控制台。
\ 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控制台中提供功能和服务。
\ 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数据分类来扫描公司数据源，则应在控制台代理和NetApp数据分类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

您需要使用以下选项之一向NetApp控制台提供 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控制台。

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

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"。

关于此任务

NetApp支持站点上提供的安装程序可能是早期版本。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. 从下载控制台代理软件 "NetApp 支持站点"，然后将其复制到Linux主机上。

   您应该下载适用于您的网络或云中的“在线”代理安装程序。

3. 分配运行脚本的权限。

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

   其中 <version> 是您下载的控制台代理的版本。

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

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

   如果您的网络需要代理来访问互联网，则需要添加代理信息。您可以添加透明或显式代理。 --proxy 和

--cacert 参数是可选的，系统不会提示您添加它们。如果您有代理服务器，则需要输入所示的参数。

以下是使用 CA 签名证书配置显式代理服务器的示例：

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

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

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

  请注意以下事项：

  - 用户可以是本地用户或域用户。
  - 对于域用户，您必须使用 \ 的 ASCII 代码，如上所示。
  - 控制台代理不支持包含 @ 字符的用户名或密码。
  - 如果密码包含以下任何特殊字符，则必须在该特殊字符前面加上反斜杠来转义该特殊字符：& 或 !

    例如：

http://bxpproxyuser:netapp1\!@地址:3128

`--cacert`指定用于控制台代理和代理服务器之间的 HTTPS 访问的 CA 签名证书。 HTTPS代理服务器、拦截代理服务器、透明代理服务器都需要此参数。

+ 下面是配置透明代理服务器的示例。配置透明代理时，不需要定义代理服务器。您只需将 CA 签名的证书添加到控制台代理主机：

+

```
./NetApp_Console_Agent_Cloud_v4.0.0 --cacert /tmp/cacert/certificate.cer
```

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
...
# 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
...
Esc:wq
```

c. 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控制台" 。

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**控制台的权限

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

IAM 角色

将您之前创建的 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控制台"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控制台"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控制台是最常见的方式。

有以下安装选项可用：

- "直接从NetApp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 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**控制台在 **Azure** 中创建控制台代理

要从NetApp控制台在 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://support.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控制台。
\ 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控制台中提供功能和服务。
\ 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控制台时，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数据分类来扫描公司数据源，则应在控制台代理和NetApp数据分类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实例。

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。

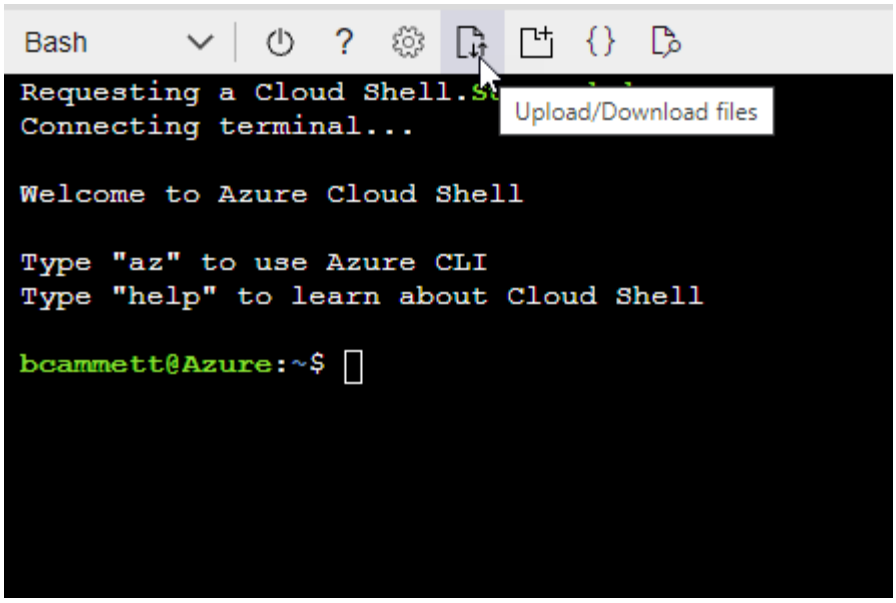
   例子

```
"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。

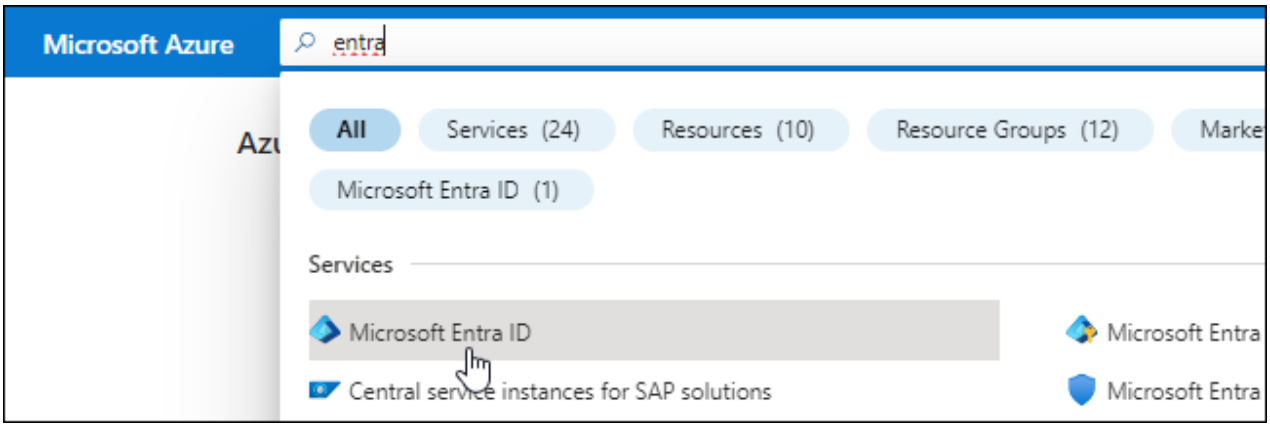
在 Microsoft Entra ID 中创建并设置服务主体，并获取控制台所需的 Azure 凭据。

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控制台一起使用）。
- 重定向 **URI**：您可以将此字段留空。

6. 选择*注册*。

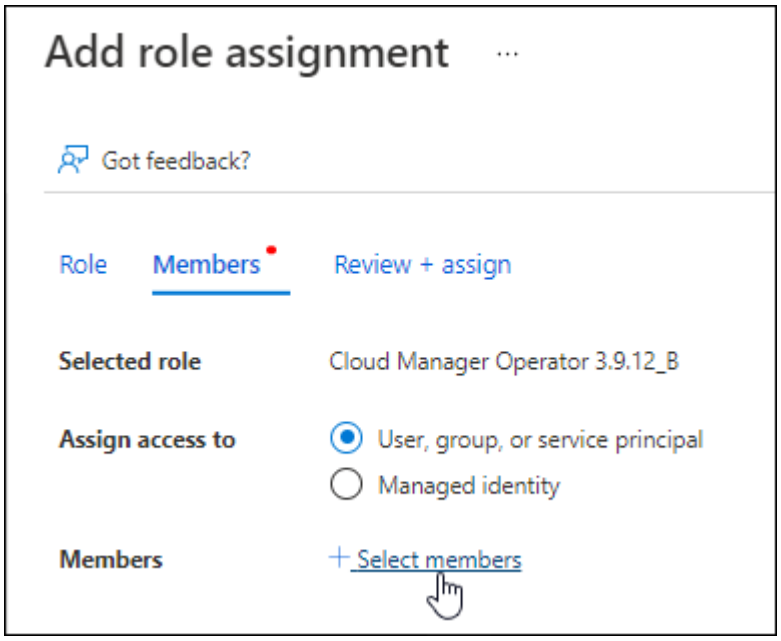
您已创建 AD 应用程序和服务主体。

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：

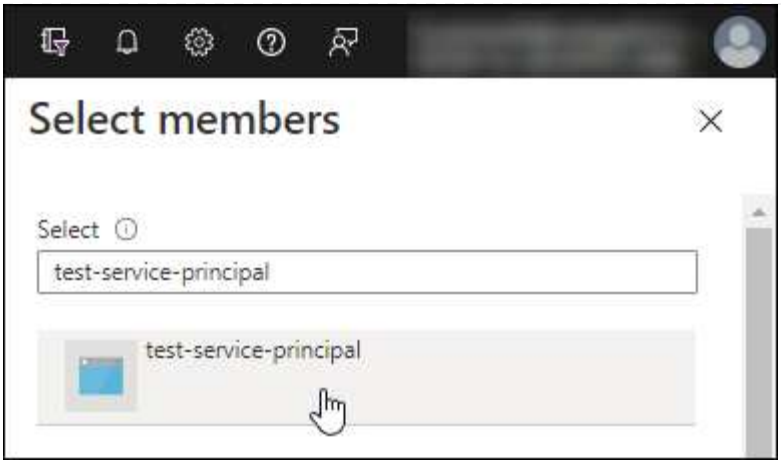
a. 保持选中“用户、组或服务主体”。

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”。

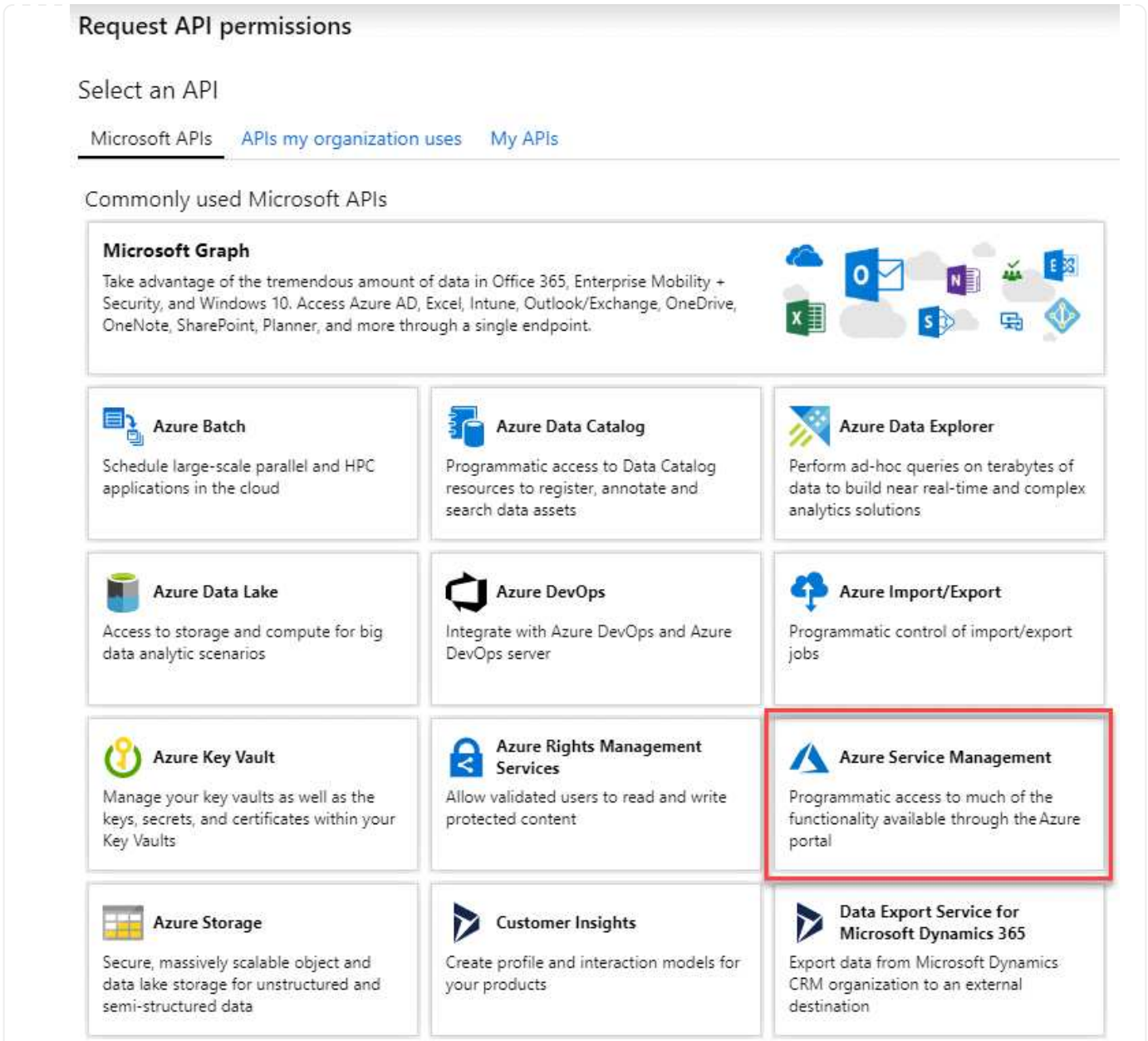
6. 单击*审阅+分配*。

服务主体现在具有部署控制台代理所需的 Azure 权限。

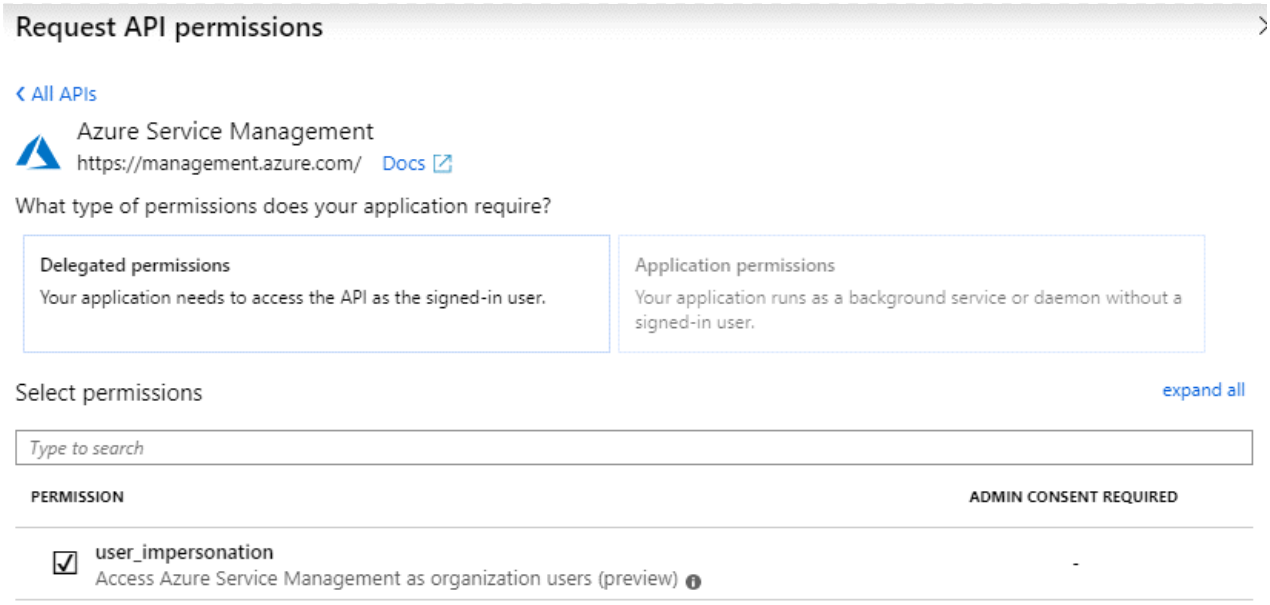
如果您想要管理多个 Azure 订阅中的资源，则必须将服务主体绑定到每个订阅。例如，控制台允许您选择部署Cloud Volumes ONTAP时要使用的订阅。

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”。

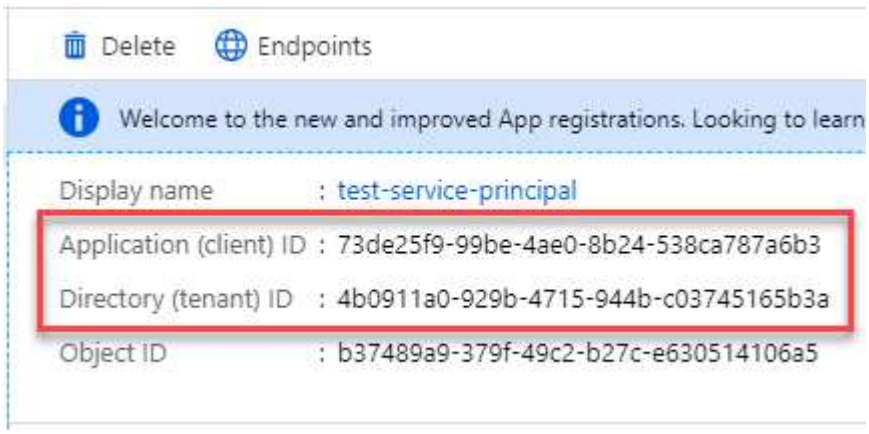


4. 选择*以组织用户身份访问 Azure 服务管理*，然后选择*添加权限*。



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. 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
     - 客户端机密

   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，输入实例的名称，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 分钟才能准备好实例。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 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控制台管理 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://support.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控制台。
\ 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控制台中提供功能和服务。
\ 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数据分类来扫描公司数据源，则应在控制台代理和NetApp数据分类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

满足上述 CPU 和 RAM 要求的实例类型。我们推荐 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控制台一起使用的每个 Azure 订阅添加 ID。

   例子

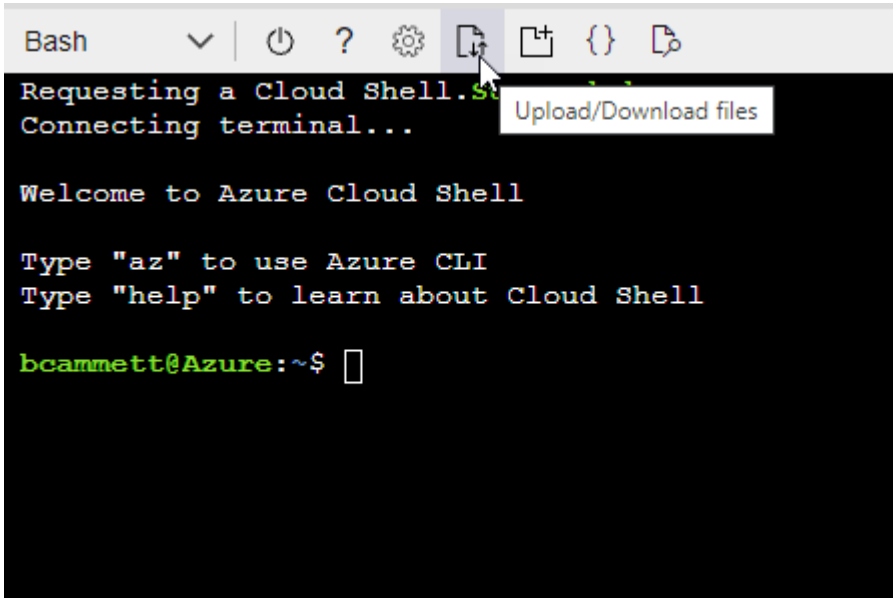
   ```
   "AssignableScopes": [
   "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
   "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
   "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
   ```

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 Connector_Policy.json
```

服务主体

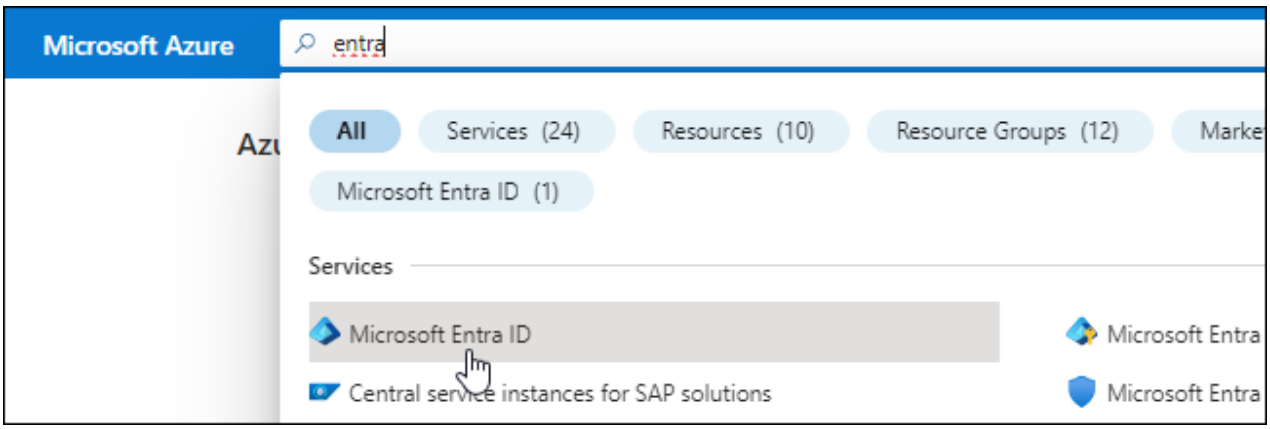
在 Microsoft Entra ID 中创建并设置服务主体，并获取控制台所需的 Azure 凭据。

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控制台一起使用）。
   - 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。

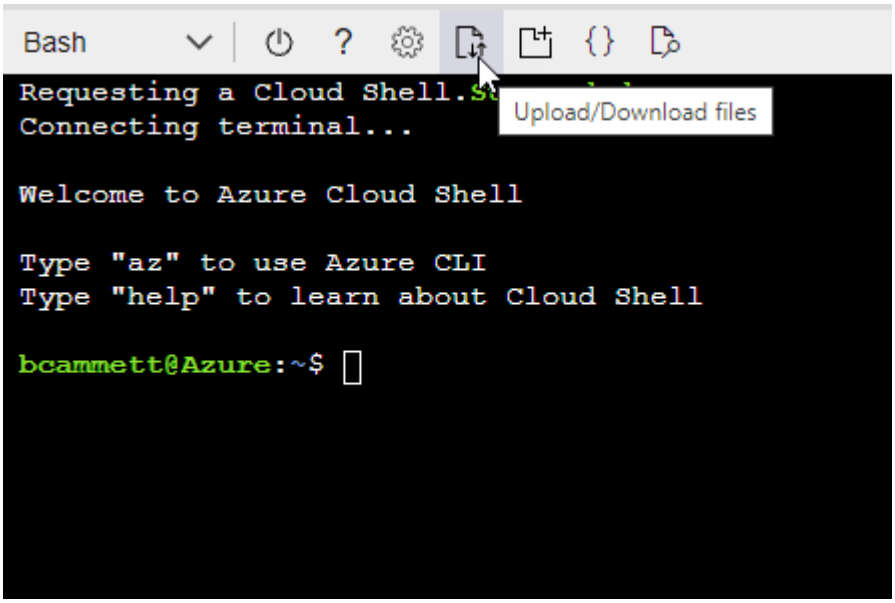
例子

```
"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
Connector_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。

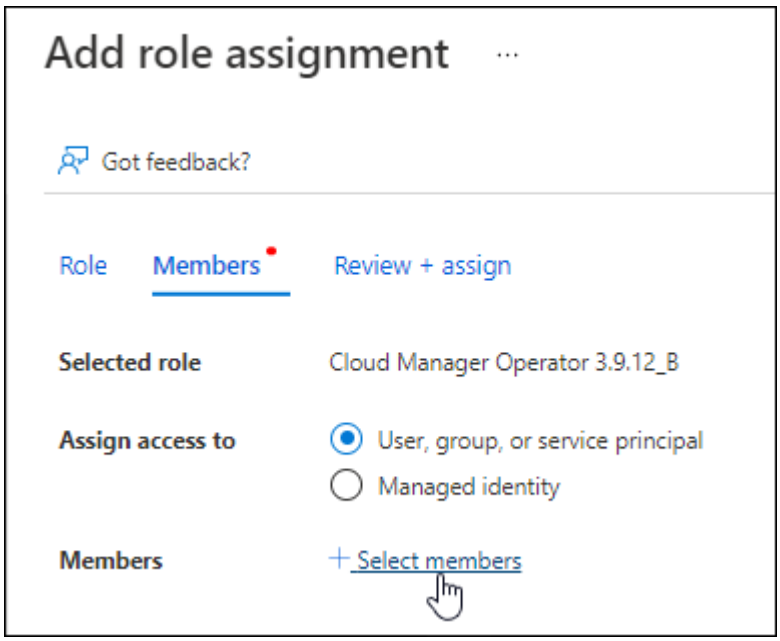
b. 选择订阅。

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*。

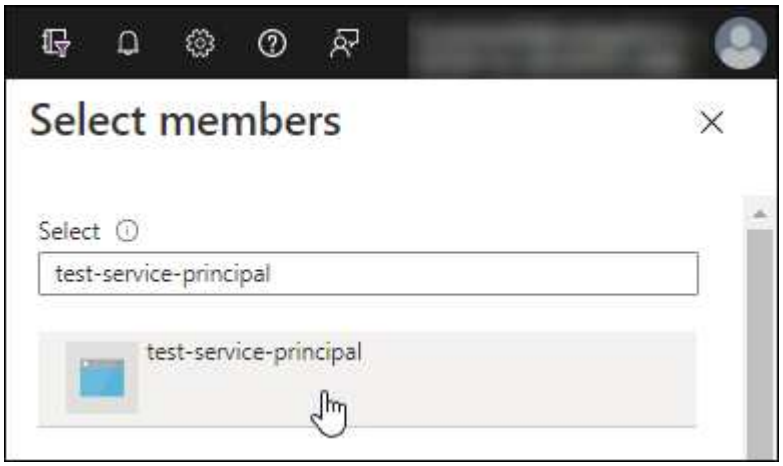
e. 在“成员”选项卡中，完成以下步骤：

- 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”。

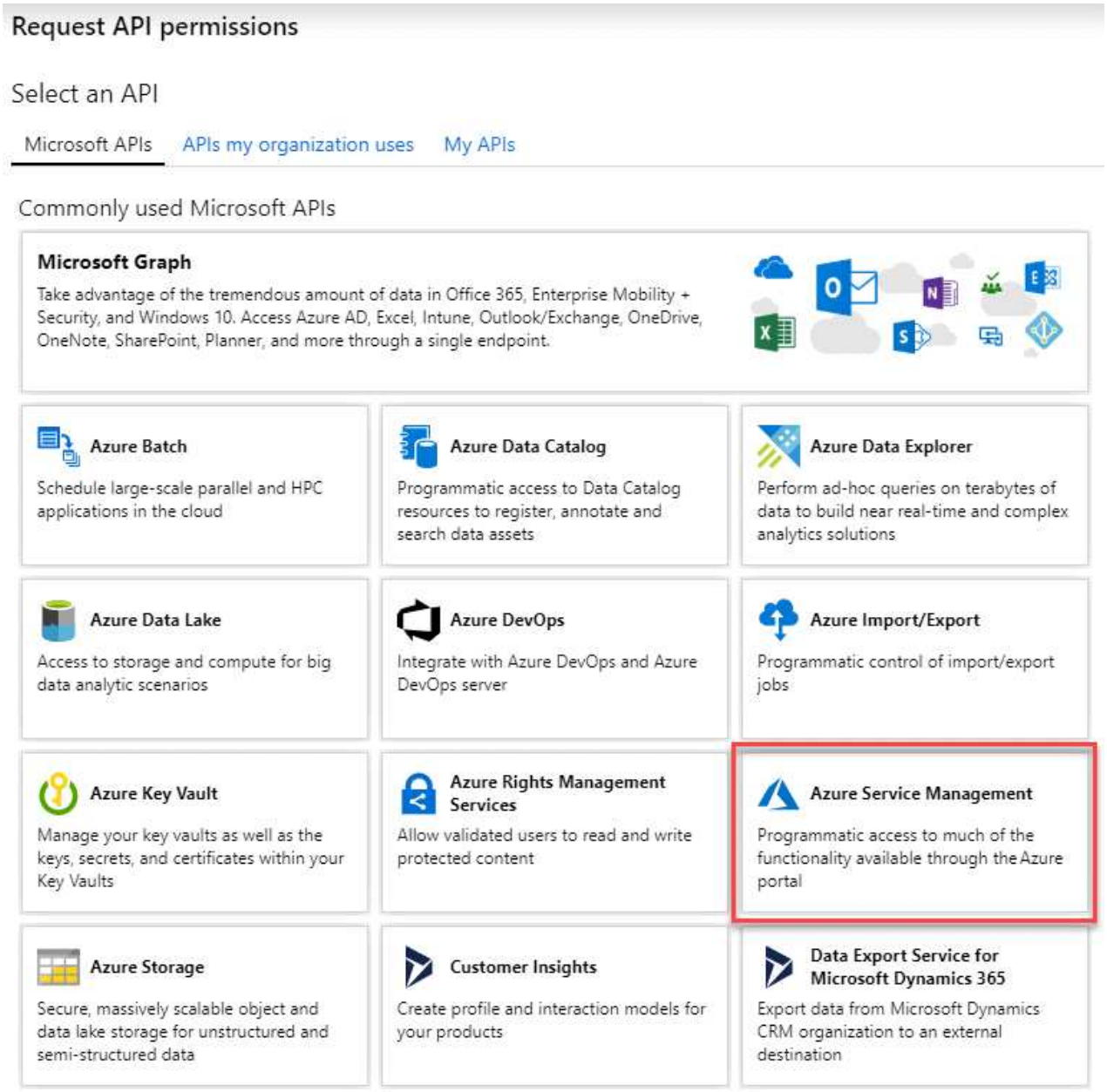
f. 选择*审阅+分配*。

服务主体现在具有部署控制台代理所需的 Azure 权限。

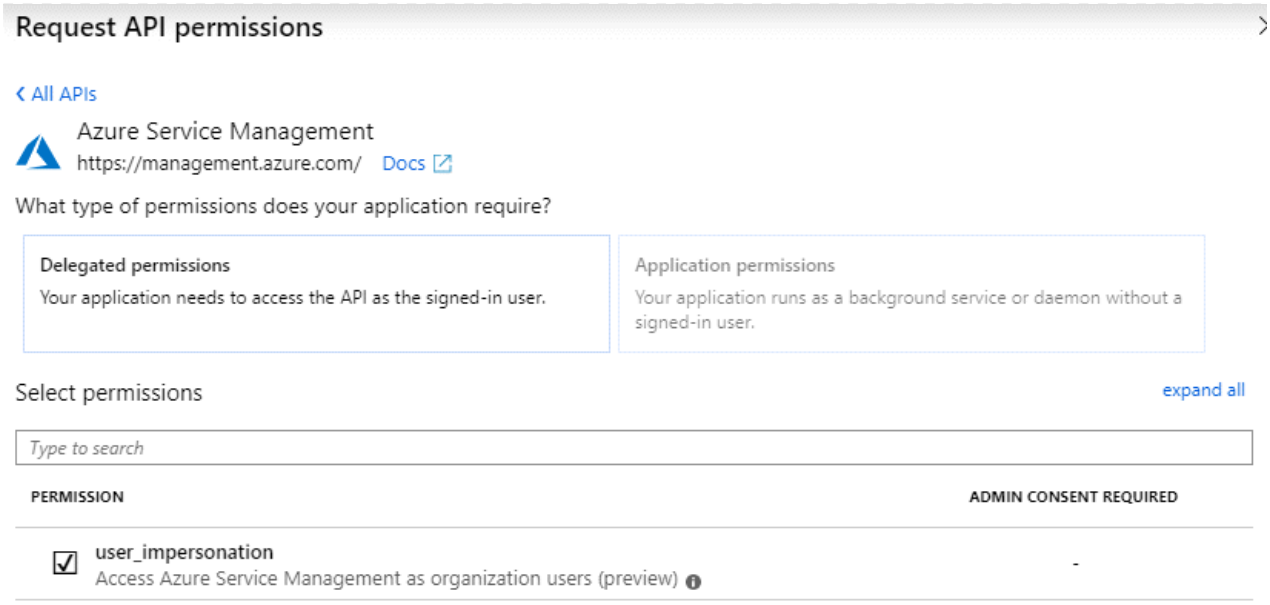
如果您想从多个 Azure 订阅部署Cloud Volumes ONTAP ，则必须将服务主体绑定到每个订阅。在NetApp控制台中，您可以选择部署Cloud Volumes ONTAP时要使用的订阅。

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”。

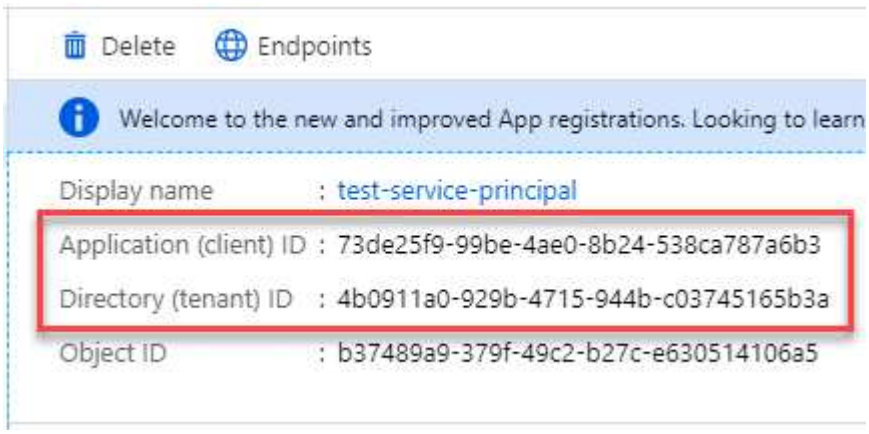


4. 选择*以组织用户身份访问 Azure 服务管理*，然后选择*添加权限*。



获取应用程序的应用程序**ID**和目录**ID**

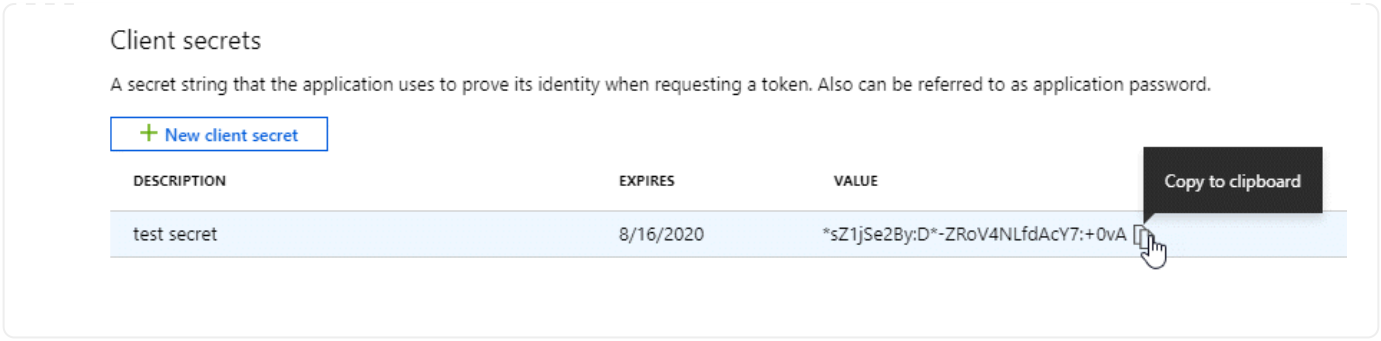
1. 在*Microsoft Entra ID*服务中，选择*App Registrations*并选择应用程序。
2. 复制*应用程序（客户端）ID*和*目录（租户）ID*。



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控制台代理 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控制台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控制台"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
      - 客户端机密
   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

与其他应用程序共享的主机不支持控制台代理。该主机必须是专用主机。主机可以是满足以下大小要求的任何架构：

- 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 Docker 或 Podman 的设计目的是在此目录中创建容器。具体来说，他们将在 `/var/lib/containers/storage`目录。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	9.1 至 9.4 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 查看 Podman 配置要求 。	在强制模式或宽容模式下受支持 • 操作系统上启用了 SELinux 的代理不支持对Cloud Volumes ONTAP系统的管理。
Ubuntu	24.04 LTS	3.9.45 或更高版本， NetApp控制台处于标准模式或受限模式	Docker Engine 23.06 至 28.0.0。	不支持

Azure VM 大小

满足上述 CPU 和 RAM 要求的实例类型。我们推荐 Standard_D8s_v3。

/opt 中的磁盘空间

必须有 100 GiB 可用空间

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

/var 中的磁盘空间

必须有 20 GiB 可用空间

控制台代理需要此空间 `/var`因为 Docker 或 Podman 的设计目的是在此目录中创建容器。具体来说，他们将在 `/var/lib/containers/storage`目录。外部安装或符号链接不适用于此空间。

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 软件包版本 1.0.6
- 将 podman-compose 添加到 PATH 环境变量
- 如果使用 Red Hat Enterprise Linux 8，请验证您的 Podman 版本使用的是 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。

   对于 Red Hat Enterprise Linux 9：

```
sudo dnf install podman-2:<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 。

   对于 Red Hat Enterprise Linux 8：

```
sudo dnf install podman-3:<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。
6. 如果使用 Red Hat Enterprise：

   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。

   对于 Red Hat Enterprise Linux 9：

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

   对于 Red Hat Enterprise Linux 8：

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

7. 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。

8. 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。

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

      ```
      podman info | grep networkBackend
      ```

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

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

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

   d. 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。

9. 重新启动 podman。

```
systemctl restart podman
```

10. 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**控制台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://support.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控制台。
\ 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控制台中提供功能和服务。
\ 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数据分类来扫描公司数据源，则应在控制台代理和NetApp数据分类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控制台一起使用的每个 Azure 订阅添加 ID。

   例子

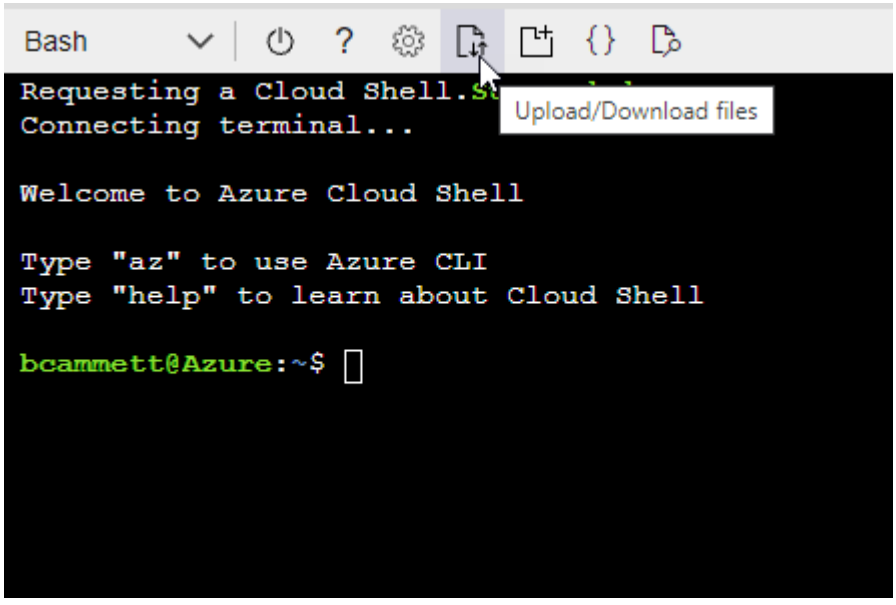
   ```
   "AssignableScopes": [
   "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
   "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
   "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
   ```

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 Connector_Policy.json
```

服务主体

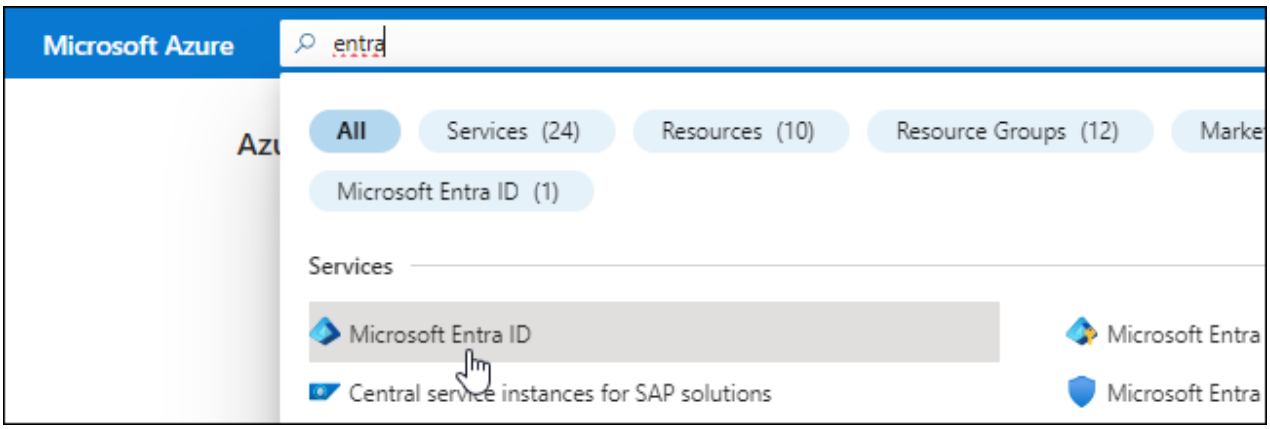
在 Microsoft Entra ID 中创建并设置服务主体，并获取控制台代理所需的 Azure 凭据。

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控制台一起使用）。
   - 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。

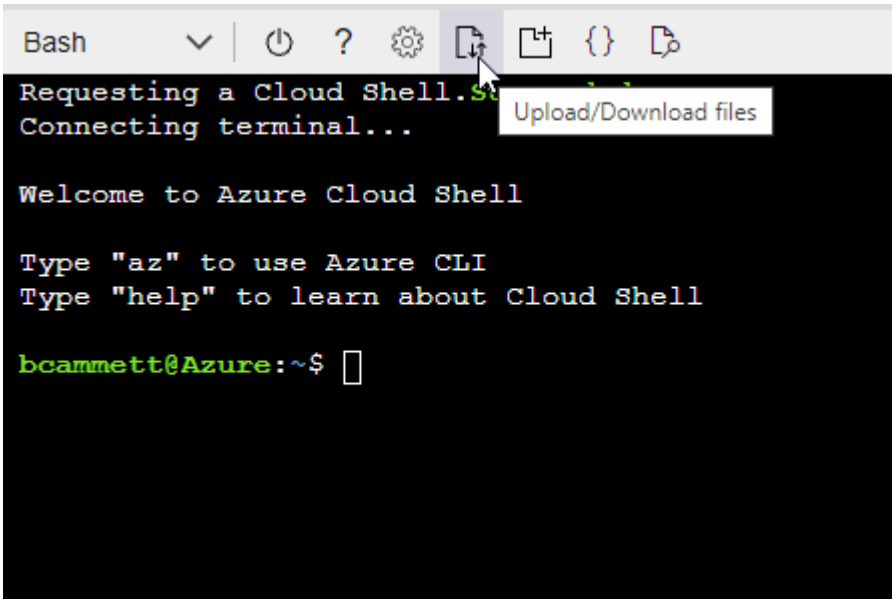
例子

```
"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
Connector_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。

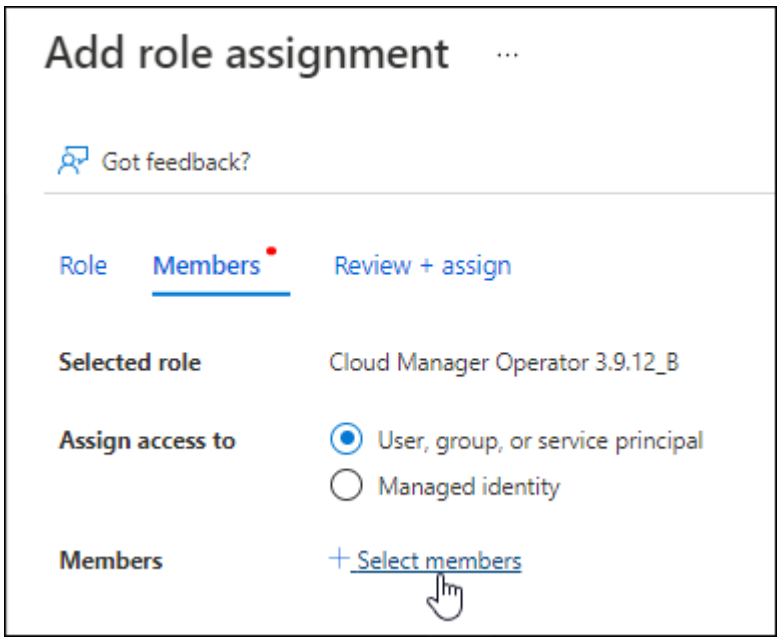
b. 选择订阅。

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*。

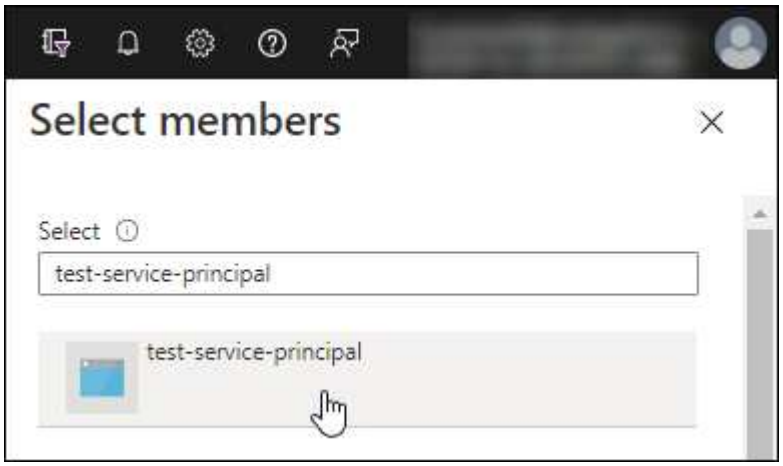
e. 在“成员”选项卡中，完成以下步骤：

- 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”。

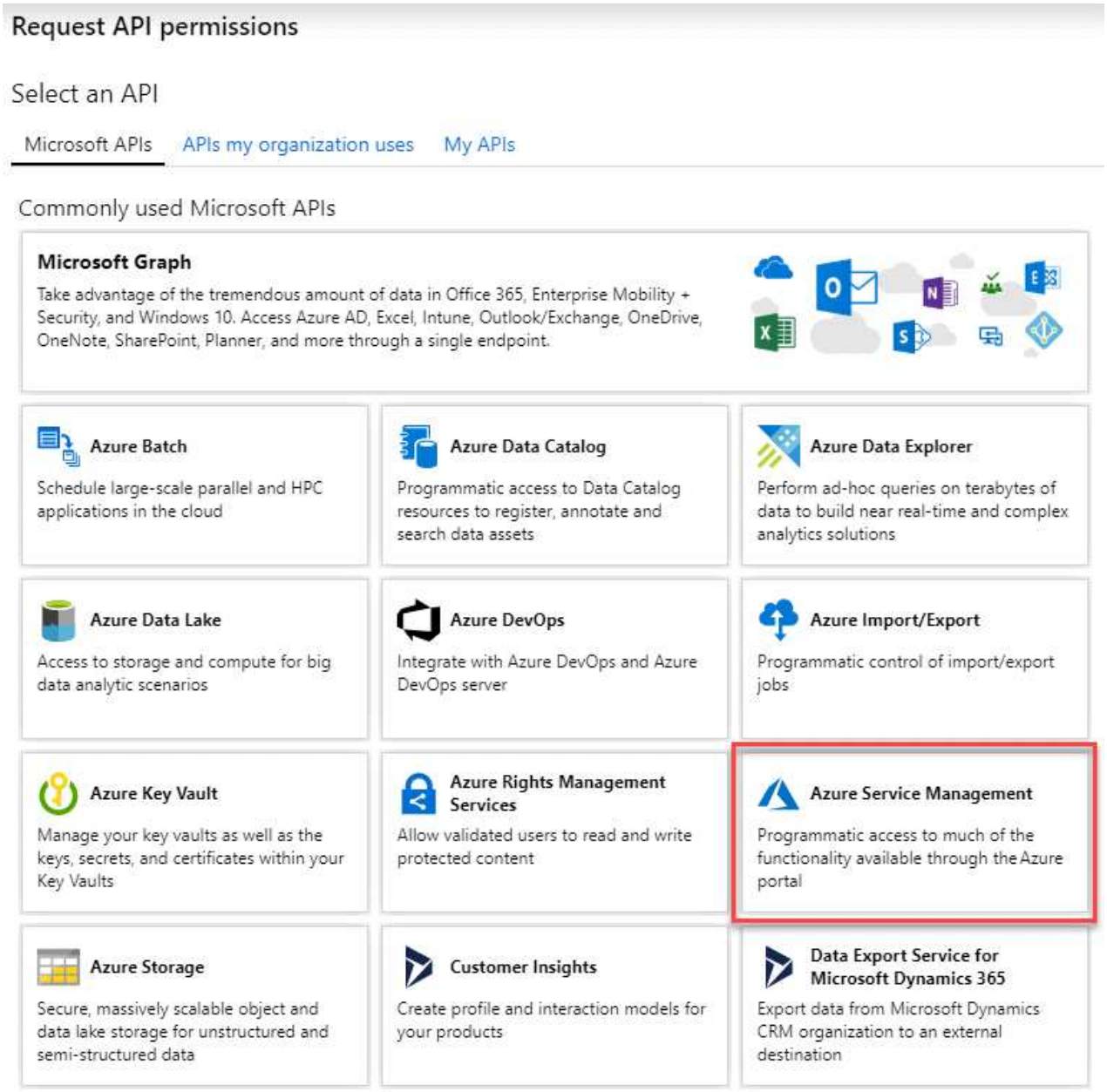
f. 选择*审阅+分配*。

服务主体现在具有部署控制台代理所需的 Azure 权限。

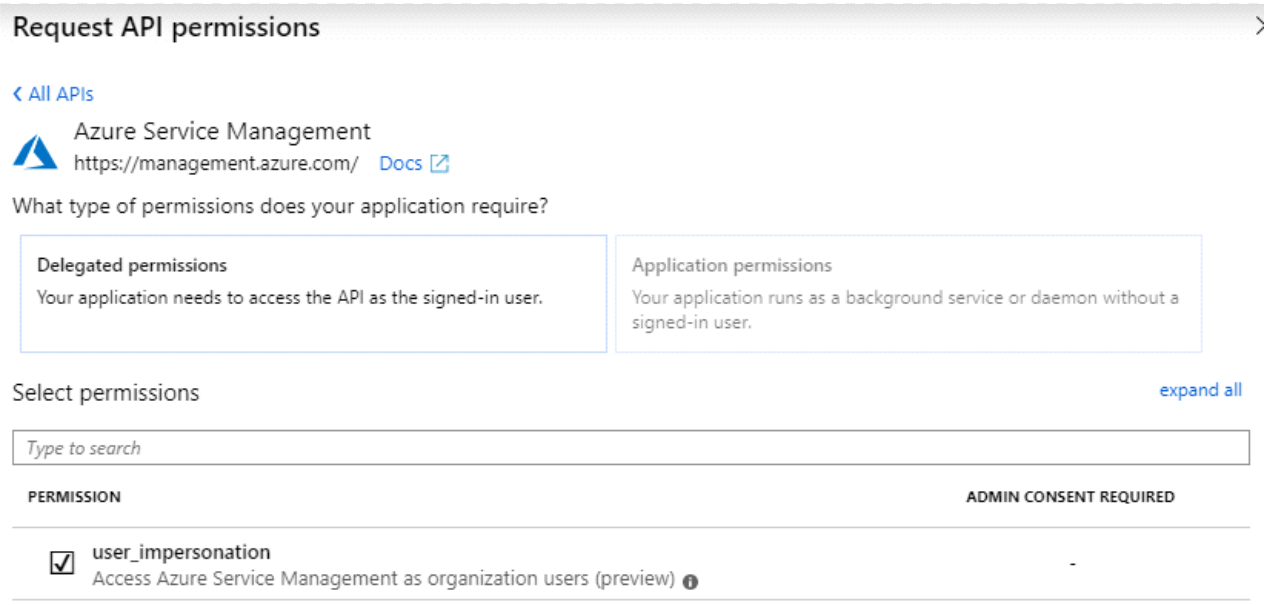
如果您想从多个 Azure 订阅部署Cloud Volumes ONTAP ，则必须将服务主体绑定到每个订阅。在NetApp控制台中，您可以选择部署Cloud Volumes ONTAP时要使用的订阅。

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”。

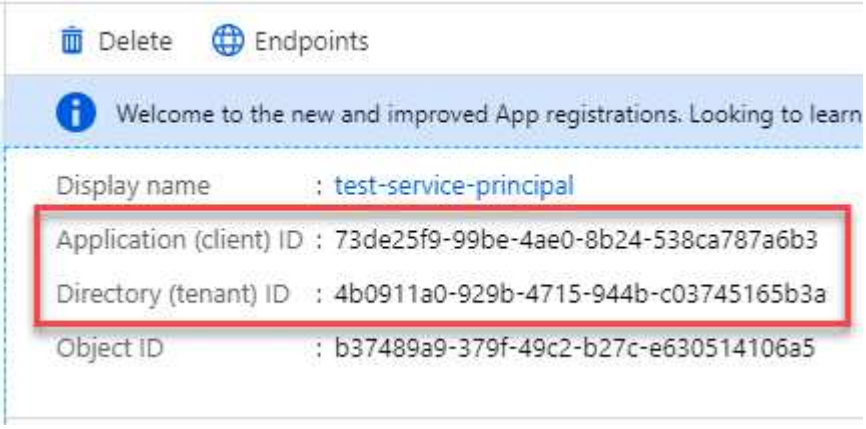


4. 选择*以组织用户身份访问 Azure 服务管理*，然后选择*添加权限*。



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

NetApp支持站点上提供的安装程序可能是早期版本。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. 从下载控制台代理软件 "NetApp 支持站点"，然后将其复制到Linux主机上。

您应该下载适用于您的网络或云中的“在线”代理安装程序。

3. 分配运行脚本的权限。

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

其中 <version> 是您下载的控制台代理的版本。

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

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

如果您的网络需要代理来访问互联网，则需要添加代理信息。您可以添加透明或显式代理。 --proxy 和 --cacert 参数是可选的，系统不会提示您添加它们。如果您有代理服务器，则需要输入所示的参数。

以下是使用 CA 签名证书配置显式代理服务器的示例：

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

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

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

  请注意以下事项：

  - 用户可以是本地用户或域用户。
  - 对于域用户，您必须使用 \ 的 ASCII 代码，如上所示。
  - 控制台代理不支持包含 @ 字符的用户名或密码。
  - 如果密码包含以下任何特殊字符，则必须在该特殊字符前面加上反斜杠来转义该特殊字符：& 或 !

    例如：

http://bxpproxyuser:netapp1\!@地址:3128

`--cacert`指定用于控制台代理和代理服务器之间的 HTTPS 访问的 CA 签名证书。 HTTPS代理服务器、拦截代理服务器、透明代理服务器都需要此参数。

+ 下面是配置透明代理服务器的示例。配置透明代理时，不需要定义代理服务器。您只需将 CA 签名的证书添加到控制台代理主机：

+

```
./NetApp_Console_Agent_Cloud_v4.0.0 --cacert /tmp/cacert/certificate.cer
```

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
      ...
      # 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
      ...
      Esc:wq
      ```

   c. 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控制台" 。

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控制台管理 Azure Blob 存储"

步骤 **6**：提供对**NetApp**控制台的权限

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控制台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控制台"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
      - 客户端机密
   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控制台是最常见的方式。 ---

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控制台在 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://www.googleapis.com/deploymentmanager/v2/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://support.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控制台。
\ 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控制台中提供功能和服务。
\ 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控制台时，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数据分类来扫描公司数据源，则应在控制台代理和NetApp数据分类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:
- 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
- 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.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**：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“connector”的角色：

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

"Google Cloud 文档：创建和管理自定义角色"

2. 在 Google Cloud 中创建服务帐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控制台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
   - 云日志 API
   - 云资源管理器 API

- 计算引擎 API
- 身份和访问管理 (IAM) API
- 云密钥管理服务 (KMS) API

  （仅当您计划将NetApp Backup and Recovery 与客户管理加密密钥 (CMEK) 结合使用时才需要）

"Google Cloud 文档：启用 API"

步骤 **6**：创建控制台代理

直接从控制台创建控制台代理。

关于此任务

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。
- 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”。

   实例大约需要 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://www.googleapis.com/deploymentmanager/v2/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://support.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控制台。
\ 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控制台中提供功能和服务。
\ 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控制台时，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数据分类来扫描公司数据源，则应在控制台代理和NetApp数据分类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 NetApp Console
agent
stage: GA
includedPermissions:
- 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
- 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.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“connector”的角色：

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

"Google Cloud 文档：创建和管理自定义角色"

2. 在 Google Cloud 中创建服务帐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控制台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
   - 云日志 API
   - 云资源管理器 API

- 计算引擎 API
- 身份和访问管理 (IAM) API
- 云密钥管理服务 (KMS) API

  （仅当您计划将NetApp Backup and Recovery 与客户管理加密密钥 (CMEK) 结合使用时才需要）

"Google Cloud 文档：启用 API"

步骤 **6**：创建控制台代理

使用 Google Cloud 创建控制台代理。

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

开始之前

您应该具有以下内容：

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

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

步骤

1. 使用您喜欢的方法登录 Google Cloud SDK。

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

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

2. 验证您是否以具有上述部分定义的所需权限的用户身份登录：

   ```
   gcloud auth list
   ```

   输出应显示以下内容，其中 * 用户帐户是要登录的用户帐户：

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

3. 运行 `gcloud compute instances create`命令：

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

实例名称
: VM 实例所需的实例名称。

项目
: （可选）您想要部署虚拟机的项目。

服务帐户
: 步骤 2 的输出中指定的服务帐户。

区
: 您想要部署虚拟机的区域

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

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

网络路径

（可选）添加要部署控制台代理的网络名称（对于共享 VPC，您需要完整路径）

子网路径

（可选）添加要部署控制台代理的子网名称（对于共享 VPC，您需要完整路径）

kms 密钥路径

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

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

运行该命令将部署控制台代理。控制台代理实例和软件应在大约五分钟内运行。

4. 打开 Web 浏览器并输入控制台代理主机 URL：

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

5. 登录后，设置控制台代理：

   a. 指定与控制台代理关联的控制台组织。

      "了解身份和访问管理" 。

   b. 输入系统的名称。

结果

控制台代理现已安装并设置到您的控制台组织。

打开 Web 浏览器并转到 "NetApp控制台"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

与其他应用程序共享的主机不支持控制台代理。该主机必须是专用主机。主机可以是满足以下大小要求的任何架构：

- 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 Docker 或 Podman 的设计目的是在此目录中创建容器。具体来说，他们将在 `/var/lib/containers/storage`目录。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	9.1 至 9.4 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 查看 Podman 配置要求 。	在强制模式或宽容模式下受支持 • 操作系统上启用了 SELinux 的代理不支持对Cloud Volumes ONTAP系统的管理。
Ubuntu	24.04 LTS	3.9.45 或更高版本， NetApp控制台处于标准模式或受限模式	Docker Engine 23.06 至 28.0.0。	不支持

Google Cloud 机器类型

满足上述 CPU 和 RAM 要求的实例类型。我们推荐 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"

/opt 中的磁盘空间

必须有 100 GiB 可用空间

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

/var 中的磁盘空间

必须有 20 GiB 可用空间

控制台代理需要此空间 `/var`因为 Docker 或 Podman 的设计目的是在此目录中创建容器。具体来说，他们将在 `/var/lib/containers/storage`目录。外部安装或符号链接不适用于此空间。

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 软件包版本 1.0.6
- 将 podman-compose 添加到 PATH 环境变量
- 如果使用 Red Hat Enterprise Linux 8，请验证您的 Podman 版本使用的是 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。

   对于 Red Hat Enterprise Linux 9：

```
sudo dnf install podman-2:<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 。

   对于 Red Hat Enterprise Linux 8：

```
sudo dnf install podman-3:<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。
6. 如果使用 Red Hat Enterprise：

   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。

   对于 Red Hat Enterprise Linux 9：

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

   对于 Red Hat Enterprise Linux 8：

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

7. 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。

8. 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。

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

      ```
      podman info | grep networkBackend
      ```

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

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

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

   d. 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。

9. 重新启动 podman。

```
systemctl restart podman
```

10. 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**控制台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://www.googleapis.com/deploymentmanager/v2/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://support.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控制台。
\ 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控制台中提供功能和服务。
\ 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数据分类来扫描公司数据源，则应在控制台代理和NetApp数据分类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“connector”的角色：

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

   "Google Cloud 文档：创建和管理自定义角色"

2. 在 Google Cloud 中创建服务帐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控制台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Cloud Volumes ONTAP系统之前，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
   - 云日志 API
   - 云资源管理器 API

- 计算引擎 API
- 身份和访问管理 (IAM) API
- 云密钥管理服务 (KMS) API

  （仅当您计划将NetApp Backup and Recovery 与客户管理加密密钥 (CMEK) 结合使用时才需要）

"Google Cloud 文档：启用 API"

步骤 **7**：安装控制台代理

前提条件完成后，您可以在自己的 Linux 主机上手动安装该软件。

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

NetApp支持站点上提供的安装程序可能是早期版本。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. 从下载控制台代理软件 "NetApp 支持站点"，然后将其复制到Linux主机上。

   您应该下载适用于您的网络或云中的“在线”代理安装程序。

3. 分配运行脚本的权限。

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

   其中 <version> 是您下载的控制台代理的版本。

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

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

如果您的网络需要代理来访问互联网，则需要添加代理信息。您可以添加透明或显式代理。 --proxy 和 --cacert 参数是可选的，系统不会提示您添加它们。如果您有代理服务器，则需要输入所示的参数。

以下是使用 CA 签名证书配置显式代理服务器的示例：

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

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

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

  请注意以下事项：

  - 用户可以是本地用户或域用户。
  - 对于域用户，您必须使用 \ 的 ASCII 代码，如上所示。
  - 控制台代理不支持包含 @ 字符的用户名或密码。
  - 如果密码包含以下任何特殊字符，则必须在该特殊字符前面加上反斜杠来转义该特殊字符：& 或 !

    例如：

http://bxpproxyuser:netapp1\!@地址:3128

`--cacert`指定用于控制台代理和代理服务器之间的 HTTPS 访问的 CA 签名证书。 HTTPS代理服务器、拦截代理服务器、透明代理服务器都需要此参数。

+ 下面是配置透明代理服务器的示例。配置透明代理时，不需要定义代理服务器。您只需将 CA 签名的证书添加到控制台代理主机：

+

```
./NetApp_Console_Agent_Cloud_v4.0.0 --cacert /tmp/cacert/certificate.cer
```

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
...
# 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
...
Esc:wq
```

   c. 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控制台" 。

   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控制台管理 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

与其他应用程序共享的主机不支持控制台代理。该主机必须是专用主机。主机可以是满足以下大小要求的任何架构：

- 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 Docker 或 Podman 的设计目的是在此目录中创建容器。具体来说，他们将在 `/var/lib/containers/storage`目录。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	9.1 至 9.4 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 查看 Podman 配置要求 。	在强制模式或宽容模式下受支持 • 操作系统上启用了 SELinux 的代理不支持对Cloud Volumes ONTAP系统的管理。
Ubuntu	24.04 LTS	3.9.45 或更高版本， NetApp控制台处于标准模式或受限模式	Docker Engine 23.06 至 28.0.0。	不支持

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**控制台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"
\ https://mysupport.netapp.com	获取许可信息并向NetApp支持发送AutoSupport消息。
\ https://support.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控制台。
\ 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控制台中提供功能和服务。

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://support.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控制台。
\ 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控制台中提供功能和服务。

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数据分类来扫描公司数据源，则应在控制台代理和NetApp数据分类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控制台。

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

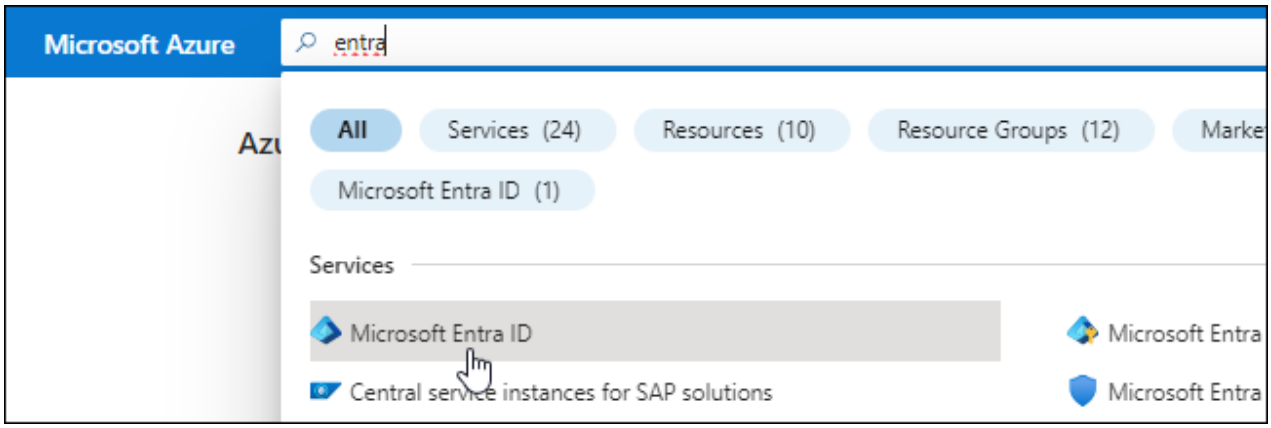
当控制台代理安装在本地时，您需要通过在 Microsoft Entra ID 中设置服务主体并获取控制台代理所需的 Azure 凭据来为控制台代理提供 Azure 权限。

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控制台一起使用）。
   - 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

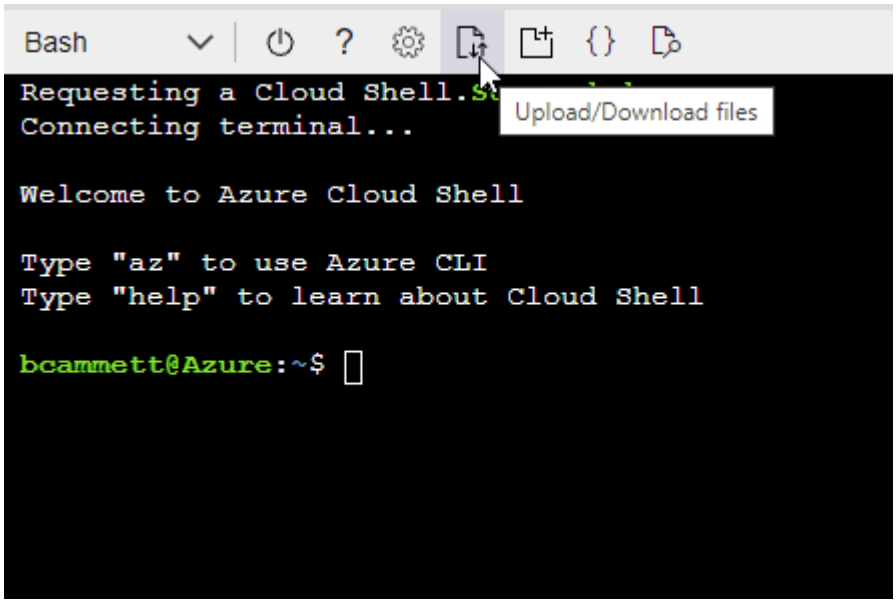
      ```
      "AssignableScopes": [
      "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
      "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
      "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
      ```

   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
Connector_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。

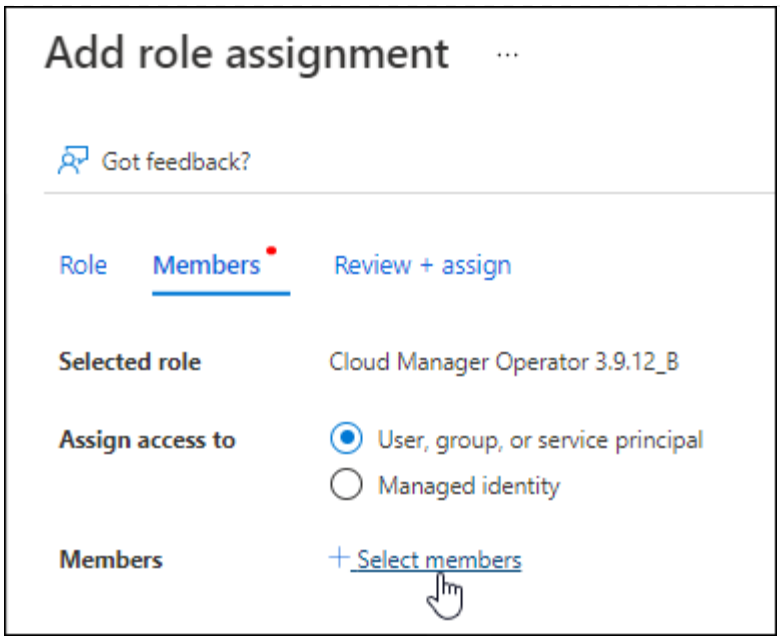
b. 选择订阅。

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*。

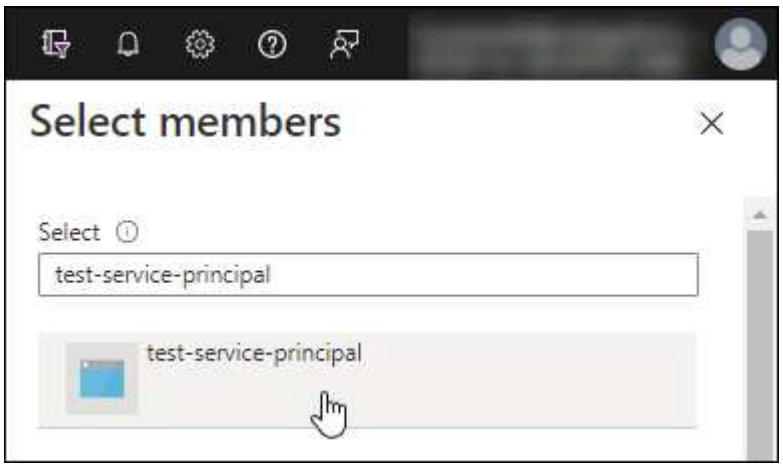
e. 在“成员”选项卡中，完成以下步骤：

- 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”。

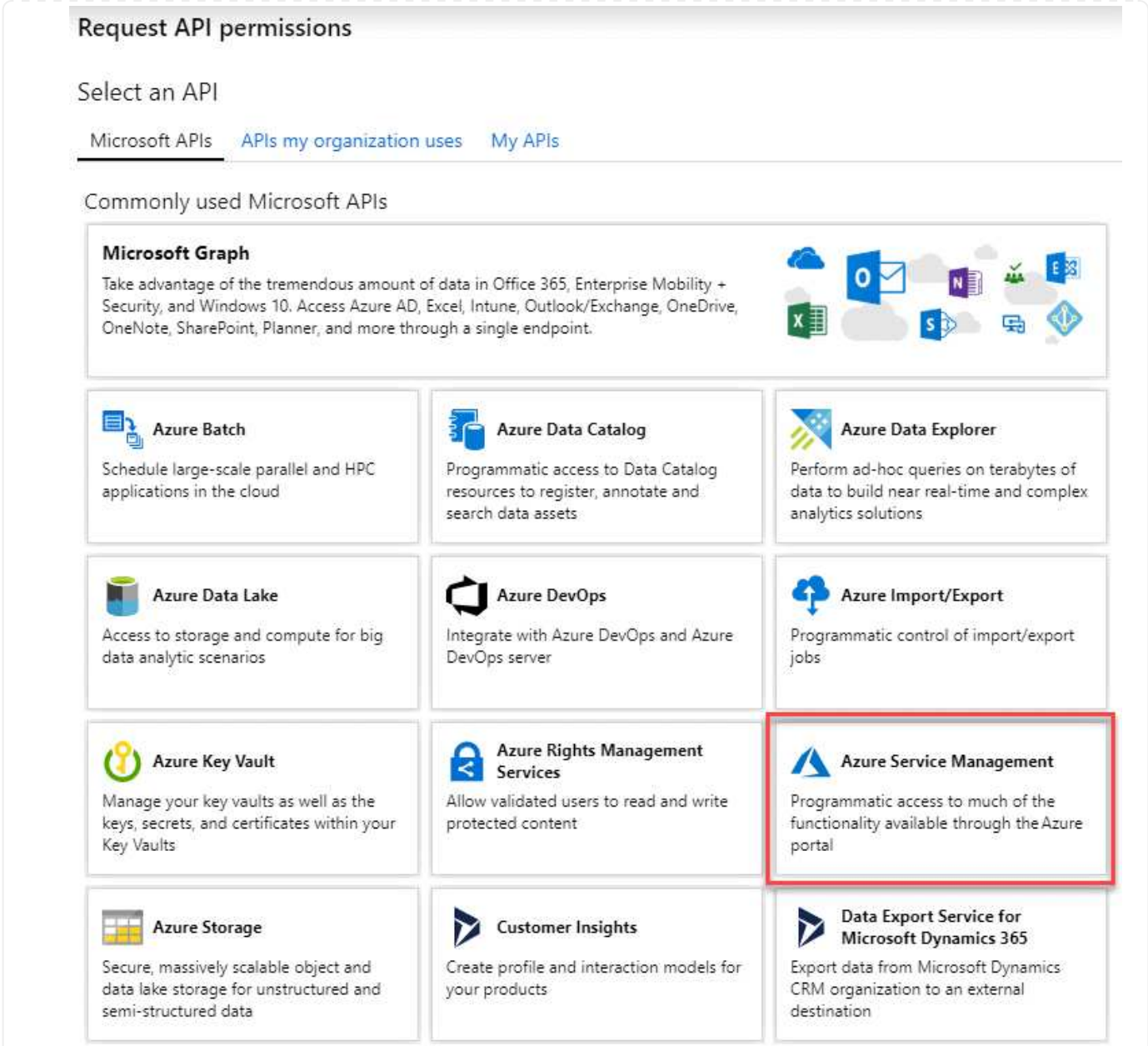
f. 选择*审阅+分配*。

服务主体现在具有部署控制台代理所需的 Azure 权限。

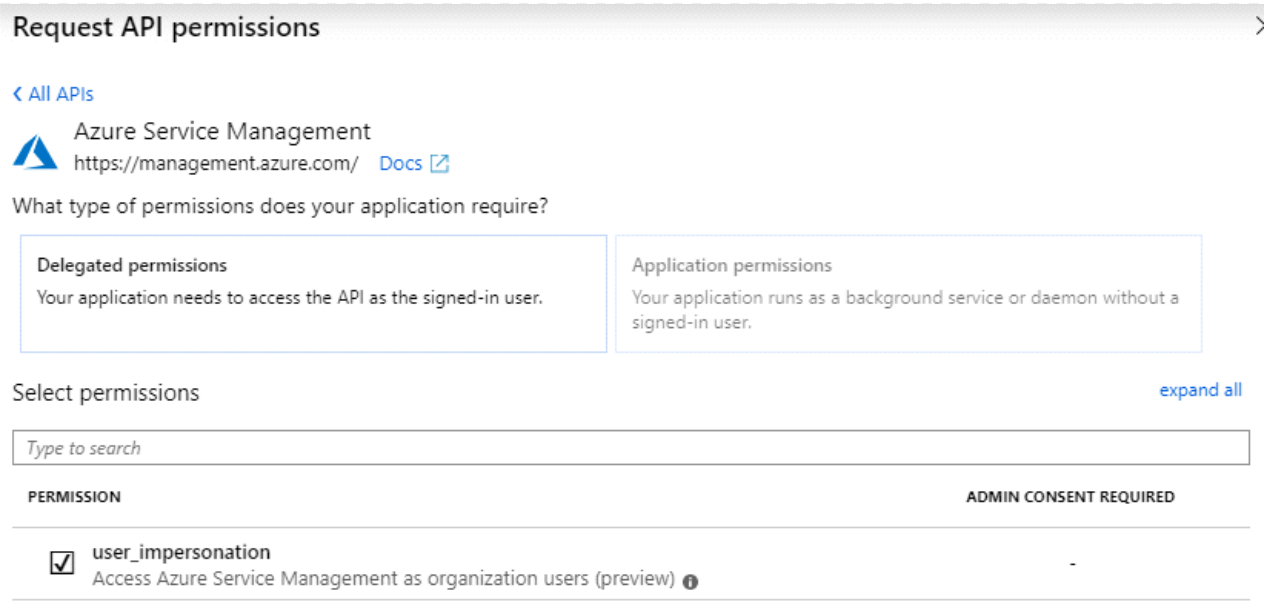
如果您想从多个 Azure 订阅部署Cloud Volumes ONTAP ，则必须将服务主体绑定到每个订阅。在NetApp控制台中，您可以选择部署Cloud Volumes ONTAP时要使用的订阅。

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”。

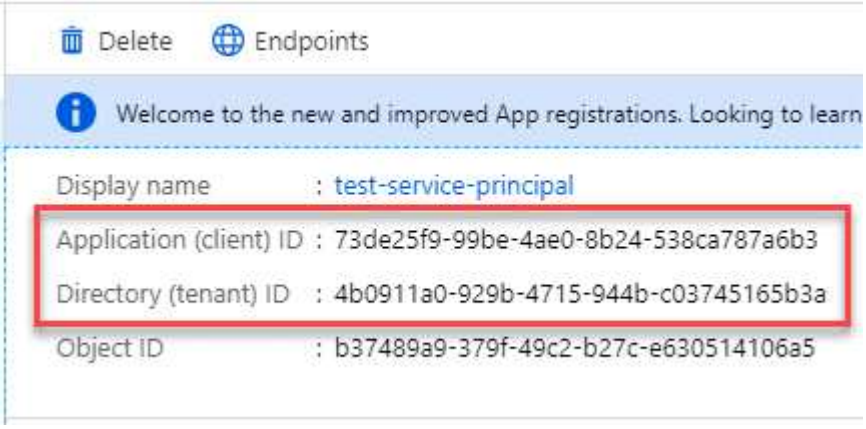


4. 选择*以组织用户身份访问 Azure 服务管理*，然后选择*添加权限*。



获取应用程序的应用程序**ID**和目录**ID**

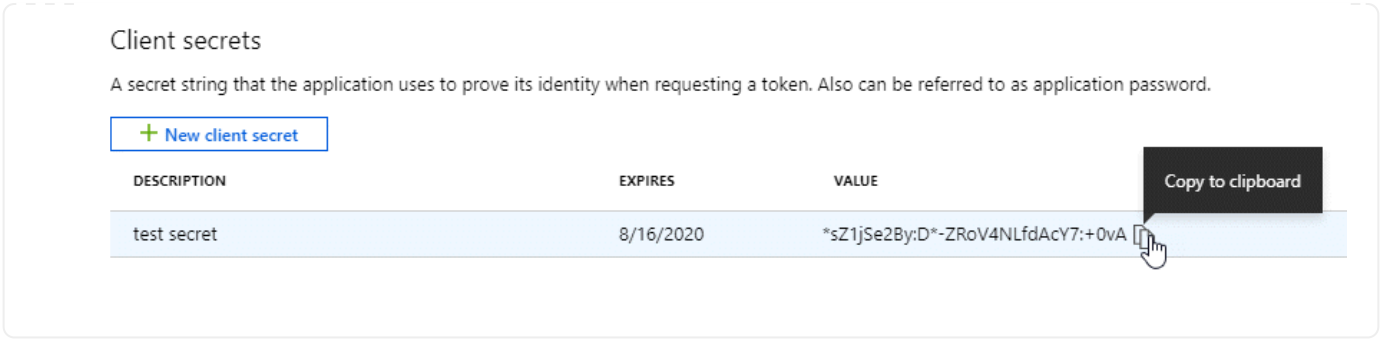
1. 在*Microsoft Entra ID*服务中，选择*App Registrations*并选择应用程序。
2. 复制*应用程序（客户端）ID*和*目录（租户）ID*。



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 软件包版本 1.0.6
- 将 podman-compose 添加到 PATH 环境变量
- 如果使用 Red Hat Enterprise Linux 8，请验证您的 Podman 版本使用的是 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。

   对于 Red Hat Enterprise Linux 9：

```
sudo dnf install podman-2:<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 。

   对于 Red Hat Enterprise Linux 8：

```
sudo dnf install podman-3:<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。
6. 如果使用 Red Hat Enterprise：

   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。

   对于 Red Hat Enterprise Linux 9：

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

   对于 Red Hat Enterprise Linux 8：

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

7. 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。

8. 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。

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

      ```
      podman info | grep networkBackend
      ```

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

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

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

   d. 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。

9. 重新启动 podman。

```
systemctl restart podman
```

10. 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

NetApp支持站点上提供的安装程序可能是早期版本。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. 从下载控制台代理软件 "NetApp 支持站点"，然后将其复制到Linux主机上。

您应该下载适用于您的网络或云中的“在线”代理安装程序。

3. 分配运行脚本的权限。

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

其中 <version> 是您下载的控制台代理的版本。

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

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

如果您的网络需要代理来访问互联网，则需要添加代理信息。您可以添加透明或显式代理。 --proxy 和 --cacert 参数是可选的，系统不会提示您添加它们。如果您有代理服务器，则需要输入所示的参数。

以下是使用 CA 签名证书配置显式代理服务器的示例：

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

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

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

请注意以下事项：

- 用户可以是本地用户或域用户。
- 对于域用户，您必须使用 \ 的 ASCII 代码，如上所示。
- 控制台代理不支持包含 @ 字符的用户名或密码。
- 如果密码包含以下任何特殊字符，则必须在该特殊字符前面加上反斜杠来转义该特殊字符：& 或 !

  例如：

http://bxpproxyuser:netapp1\!@地址:3128

`--cacert`指定用于控制台代理和代理服务器之间的 HTTPS 访问的 CA 签名证书。 HTTPS代理服务器、拦截代理服务器、透明代理服务器都需要此参数。

+ 下面是配置透明代理服务器的示例。配置透明代理时，不需要定义代理服务器。您只需将 CA 签名的证书添加到控制台代理主机：

+

```
./NetApp_Console_Agent_Cloud_v4.0.0 --cacert /tmp/cacert/certificate.cer
```

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
      ...
      # 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
      ...
      Esc:wq
      ```

   c. 重新启动控制台代理虚拟机。

下一步是什么?

您需要在NetApp控制台中注册控制台代理。

使用NetApp控制台注册控制台代理

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控制台提供云提供商凭据

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控制台"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
      - 客户端机密
   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控制台"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控制台下载 OVA 或获取 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**控制台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"
\ https://mysupport.netapp.com	获取许可信息并向NetApp支持发送AutoSupport消息。
\ https://support.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控制台。
\ 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控制台中提供功能和服务。

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://support.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控制台。
\ 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控制台中提供功能和服务。

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数据分类来扫描公司数据源，则应在控制台代理和NetApp数据分类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 用户访问密钥来提供 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控制台。

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

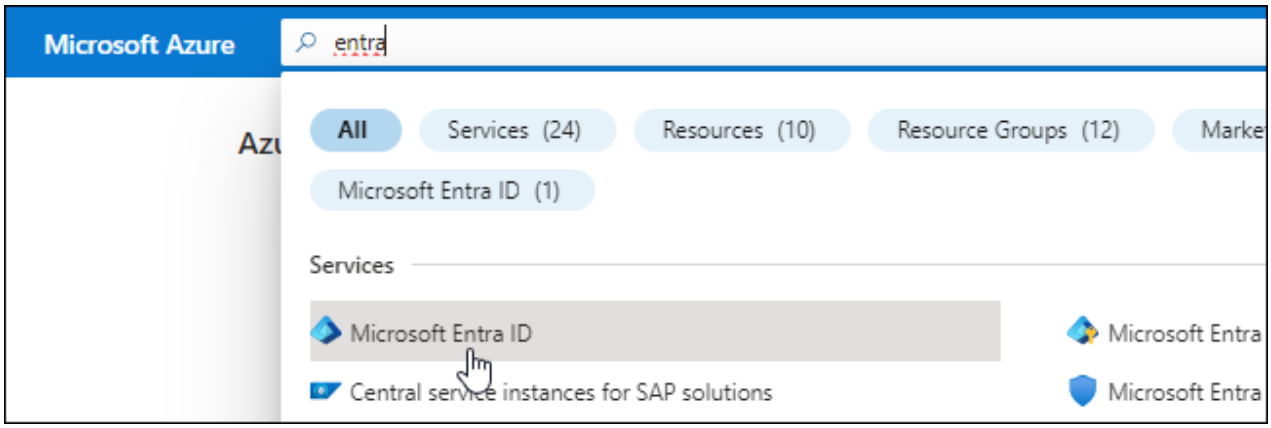
当控制台代理安装在本地时，您需要通过在 Microsoft Entra ID 中设置服务主体并获取控制台代理所需的 Azure 凭据来授予控制台代理 Azure 权限。

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控制台一起使用）。
   - 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

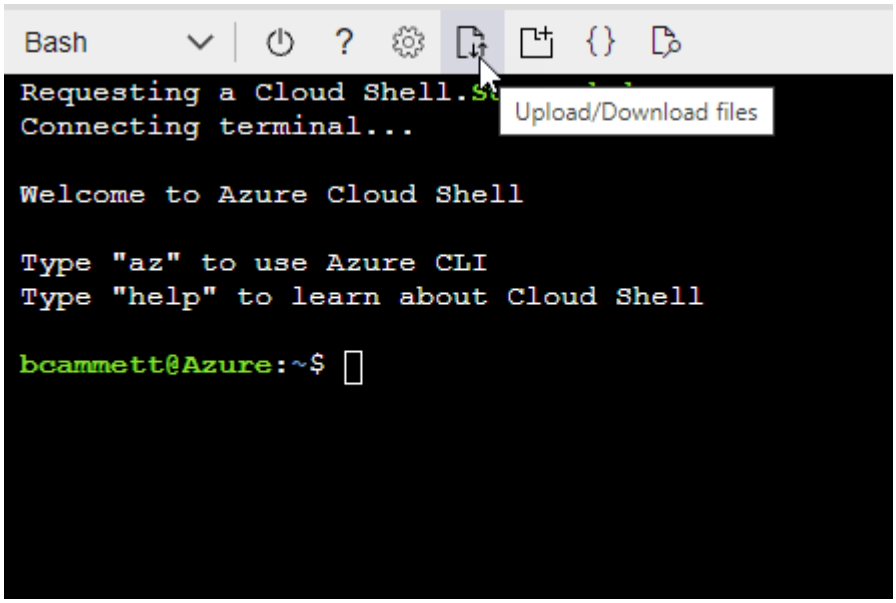
      ```
      "AssignableScopes": [
      "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
      "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
      "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
      ```

   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
Connector_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。

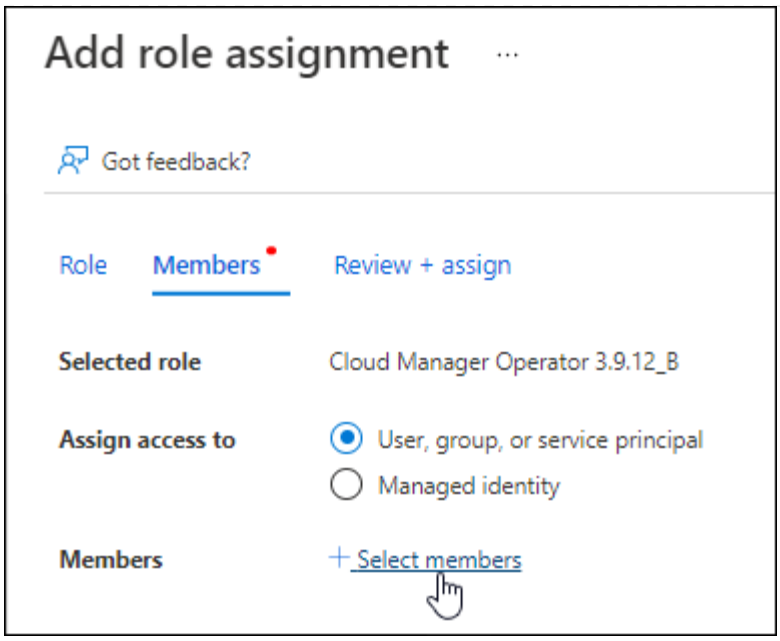
b. 选择订阅。

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*。

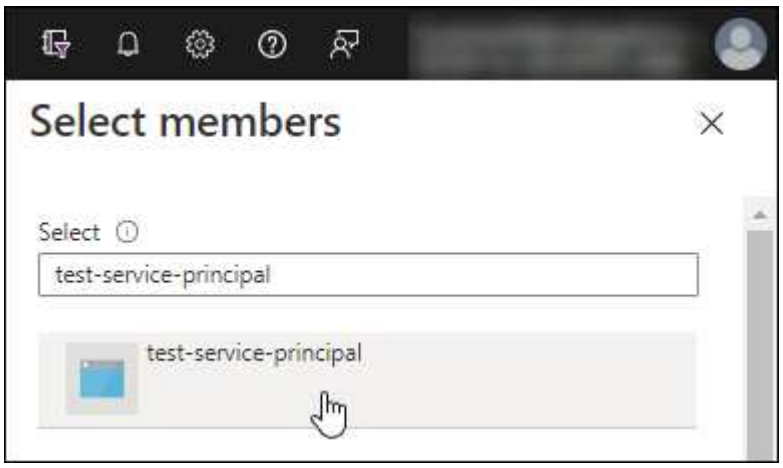
e. 在“成员”选项卡中，完成以下步骤：

- 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”。

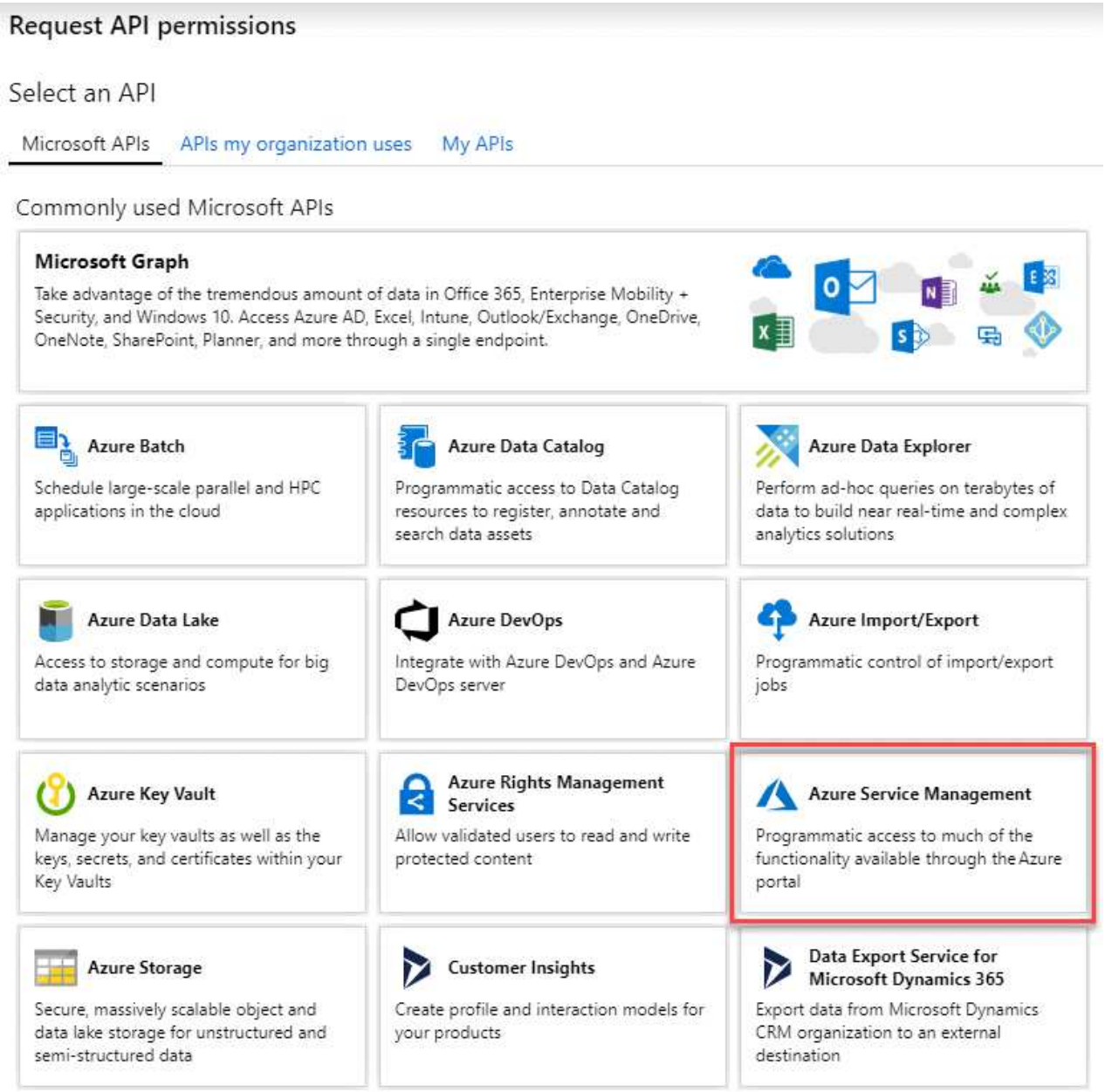
f. 选择*审阅+分配*。

服务主体现在具有部署控制台代理所需的 Azure 权限。

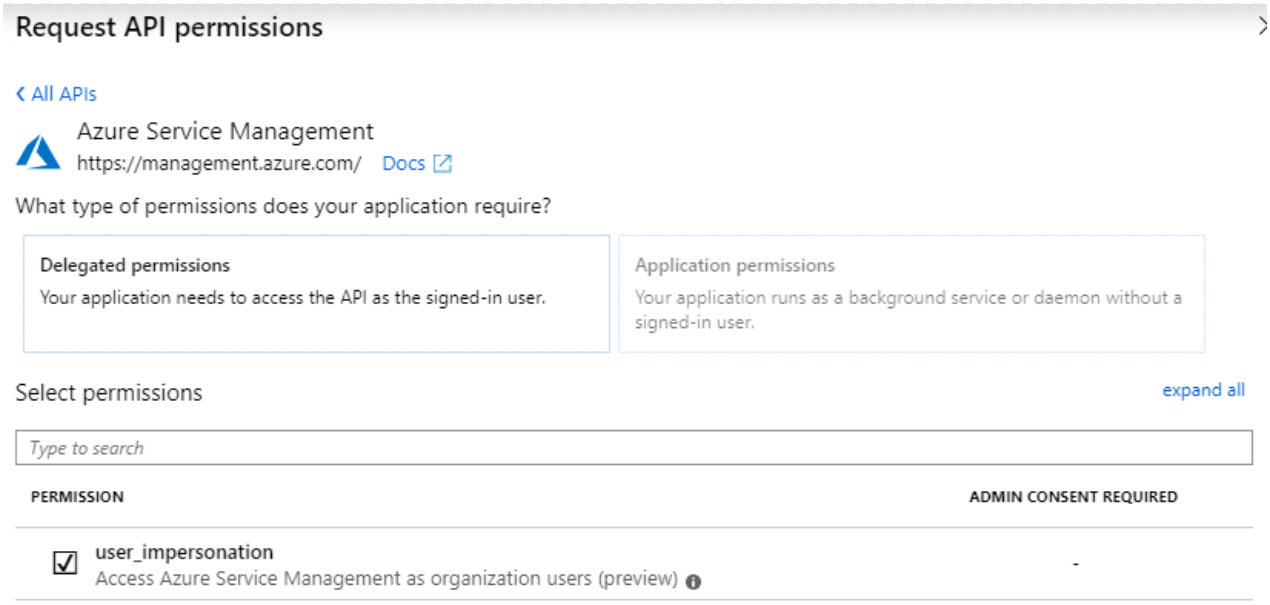
如果您想从多个 Azure 订阅部署Cloud Volumes ONTAP ，则必须将服务主体绑定到每个订阅。在NetApp控制台中，您可以选择部署Cloud Volumes ONTAP时要使用的订阅。

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”。

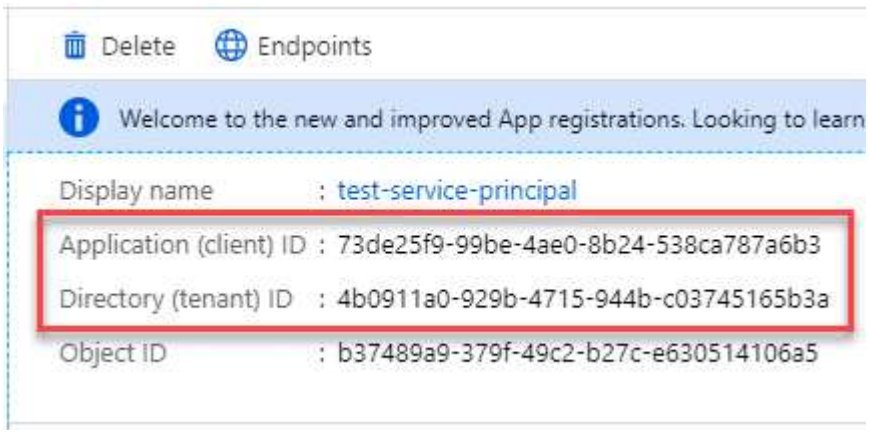


4. 选择*以组织用户身份访问 Azure 服务管理*，然后选择*添加权限*。



获取应用程序的应用程序**ID**和目录**ID**

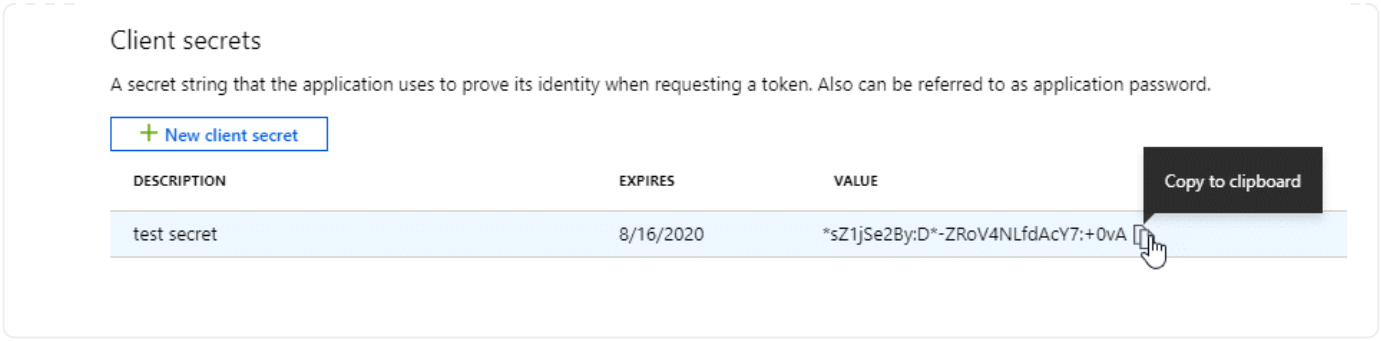
1. 在*Microsoft Entra ID*服务中，选择*App Registrations*并选择应用程序。
2. 复制*应用程序（客户端）ID*和*目录（租户）ID*。



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控制台下载文件或部署 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控制台下载 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**控制台注册控制台代理

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控制台"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
      - 客户端机密
   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控制台"开始使用控制台代理。

订阅NetApp智能服务（标准模式）

从云提供商的市场订阅NetApp智能服务，以按小时费率（PAYGO）或通过年度合同支付数据服务费用。如果您从NetApp （BYOL）购买了许可证，您还需要订阅市场产品。您的

许可证始终会先被收费，但如果您超出许可容量或许可证期限到期，则会按小时费率向您收费。

通过市场订阅可以对以下NetApp数据服务收费：

- NetApp备份和恢复
- Cloud Volumes ONTAP
- NetApp云分层
- NetApp勒索软件抵御能力
- NetApp灾难恢复

NetApp数据分类可通过您的订阅启用，但使用分类是免费的。

开始之前

您必须已经部署控制台代理才能订阅数据服务。您需要将市场订阅与连接到控制台代理的云凭据关联起来。

AWS

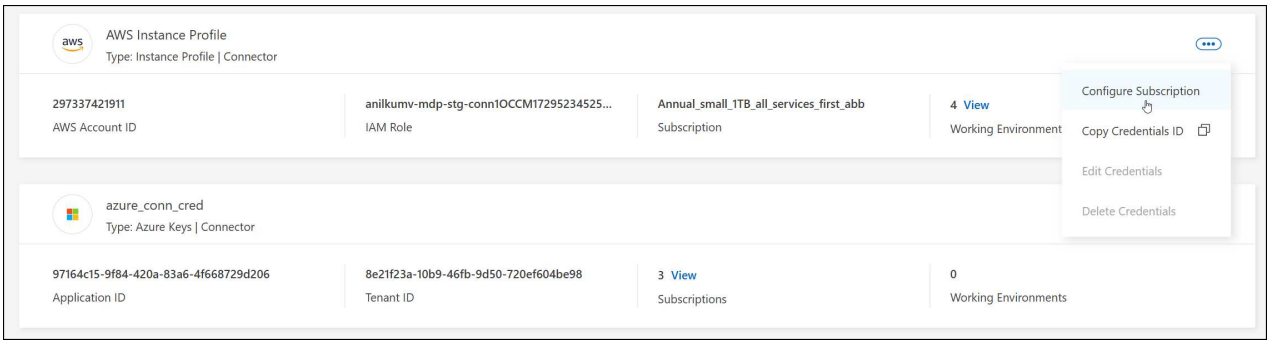
以下视频展示了从 AWS Marketplace 订阅NetApp智能服务的步骤：

从 AWS Marketplace 订阅NetApp智能服务

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控制台关联的凭据关联。



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控制台。

   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*。

Azure

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控制台关联的凭据关联。

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控制台。

   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*。

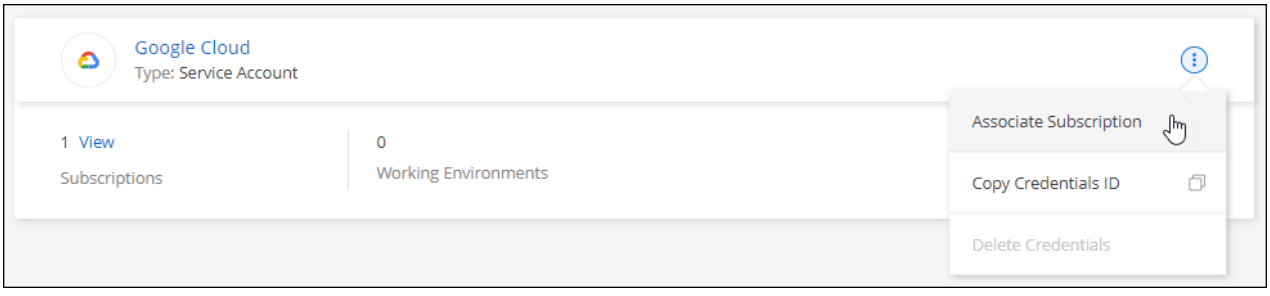
        以下视频展示了从 Azure 市场订阅的步骤：

[从 Azure 市场订阅NetApp智能服务]

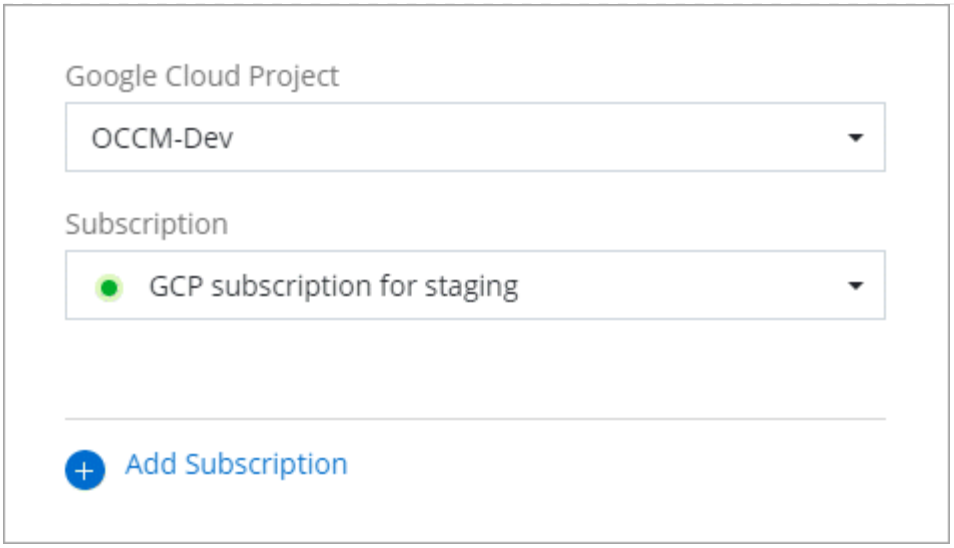
Google Cloud

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*。 +需要新的屏幕截图（TS）



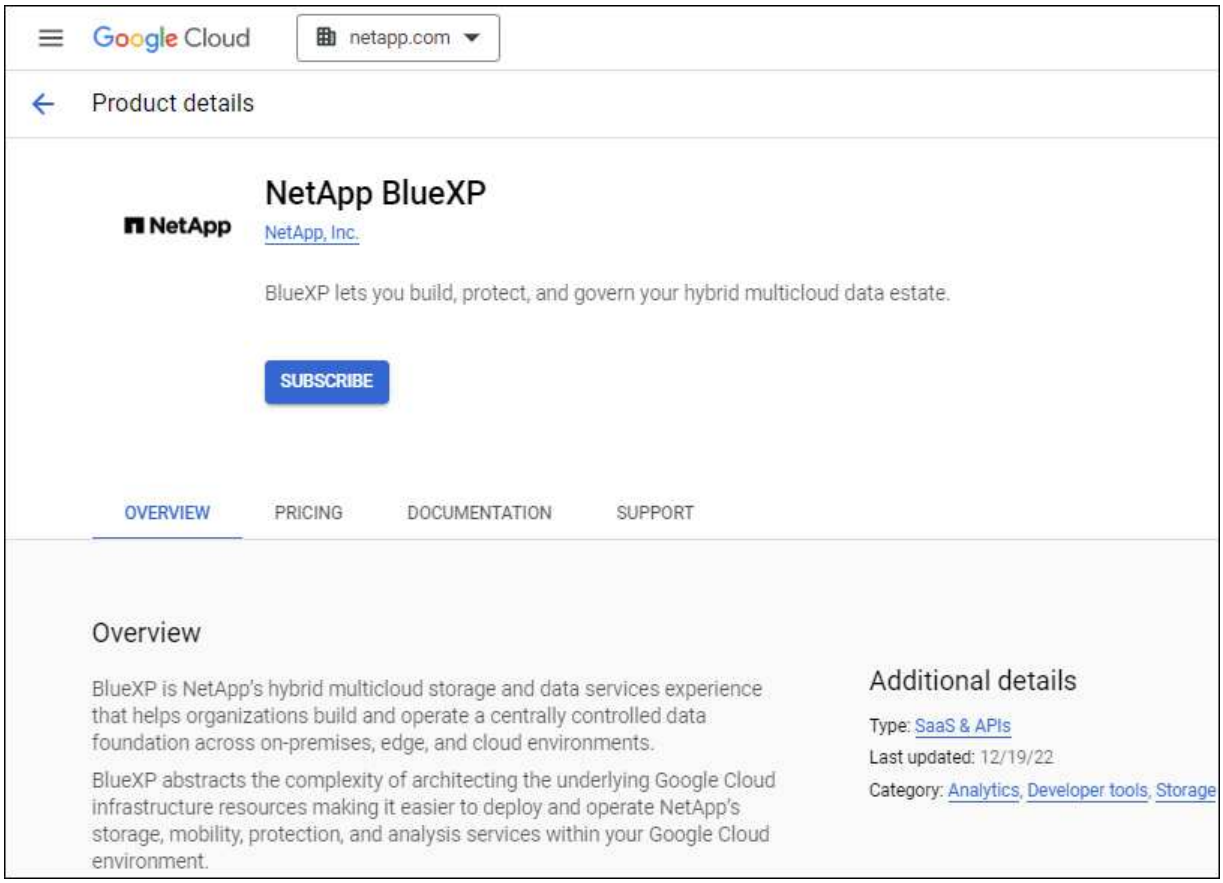
4. 要使用选定的凭据配置现有订阅，请从下拉列表中选择一个 Google Cloud 项目和订阅，然后选择*配置*。



5. 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智能服务页面"，确保在顶部导航菜单中选择了正确的项目。



   b. 选择*订阅*。

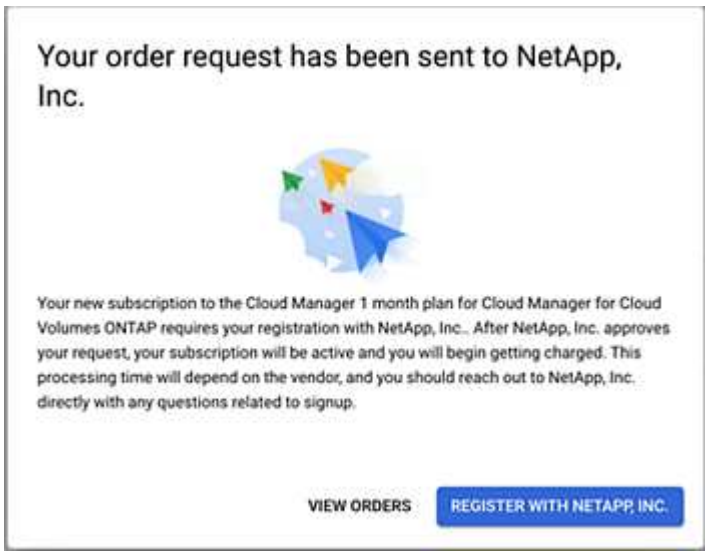
   c. 选择适当的结算账户并同意条款和条件。

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控制台中的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。

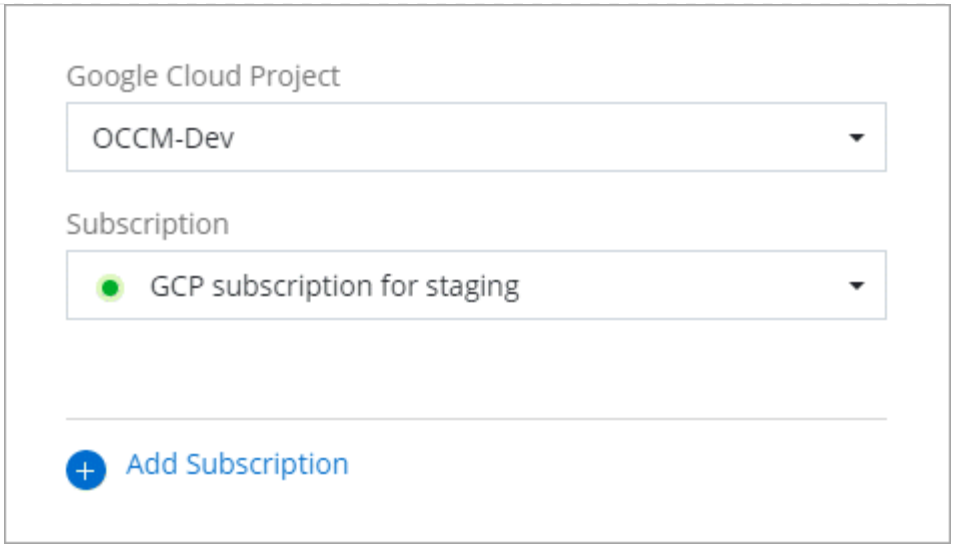
对于所有其他组织或帐户，您需要重复这些步骤来手动关联订阅。

- 选择*保存*。

以下视频展示了从 Google Cloud Marketplace 订阅的步骤：

从 Google Cloud Marketplace 订阅

a. 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。



相关信息

- "管理Cloud Volumes ONTAP 的BYOL 基于容量的许可证"
- "管理数据服务的 BYOL 许可证"
- "管理 AWS 凭证和订阅"
- "管理 Azure 凭据和订阅"
- "管理 Google Cloud 凭据和订阅"

接下来可以做什么（标准模式）

现在您已登录并以标准模式设置NetApp控制台，用户可以创建和发现存储系统并使用NetApp数据服务。

如果您在 AWS、Microsoft Azure 或 Google Cloud 中安装了控制台代理，则控制台会自动发现有关安装代理的位置中的 Amazon S3 存储桶、Azure Blob 存储或 Google Cloud Storage 存储桶的信息。这些系统会自动添加到*系统*页面。

如需帮助，请访问 "NetApp控制台文档主页"查看NetApp控制台文档。

相关信息

"NetApp控制台部署模式"

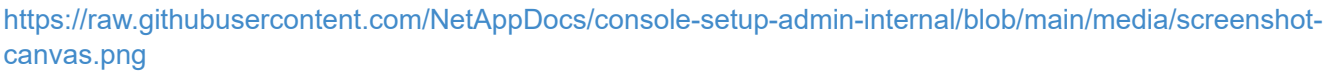
开始使用受限模式

入门工作流程（受限模式）

通过准备环境和部署控制台代理，开始以受限模式使用NetApp控制台。

受限模式通常由州和地方政府以及受监管的公司使用，包括在 AWS GovCloud 和 Azure Government 区域中的部署。在开始之前，请确保您了解"控制台代理"和"部署模式"。

1 "准备部署"



1. 准备一个满足 CPU、RAM、磁盘空间、容器编排工具等要求的专用 Linux 主机。
2. 设置提供对目标网络的访问、用于手动安装的出站互联网访问以及用于日常访问的出站互联网的网络。
3. 在您的云提供商中设置权限，以便您可以在部署控制台代理实例后将这些权限与控制台代理实例关联。

2 "部署控制台代理"

1. 从云提供商的市场安装控制台代理，或者在您自己的 Linux 主机上手动安装该软件。
2. 通过打开 Web 浏览器并输入 Linux 主机的 IP 地址来设置NetApp控制台。
3. 向控制台代理提供您之前设置的权限。

3 "订阅NetApp智能服务（可选）"

可选：从云提供商的市场订阅NetApp智能服务，以按小时费率（PAYGO）或通过年度合同支付数据服务费用。NetApp智能服务包括NetApp备份和恢复、 Cloud Volumes ONTAP、 NetApp云分层、 NetApp勒索软件恢复和NetApp灾难恢复。 NetApp数据分类包含在您的订阅中，无需额外付费。

准备在受限模式下部署

在受限模式下部署NetApp控制台之前，请准备好您的环境。您需要查看主机要求、准备网络、设置权限等。

步骤 **1**：了解受限模式的工作原理

在开始之前了解NetApp控制台在受限模式下的工作方式。

使用已安装的NetApp控制台代理本地提供的基于浏览器的界面。您无法从通过 SaaS 层提供的基于 Web 的控制台访问NetApp控制台。

此外，并非所有控制台功能和NetApp数据服务都可用。

"了解限制模式的工作原理" 。

第 **2** 步：查看安装选项

在受限模式下，您只能在云中安装控制台代理。有以下安装选项可用：

- 来自 AWS Marketplace
- 来自 Azure 市场
- 在 AWS、Azure 或 Google Cloud 中运行的 Linux 主机上手动安装控制台代理

步骤 **3**：查看主机要求

主机必须满足特定的操作系统、RAM 和端口要求才能运行控制台代理。

当您从 AWS 或 Azure 市场部署控制台代理时，映像包含所需的操作系统和软件组件。您只需选择满足 CPU 和 RAM 要求的实例类型。

专用主机

与其他应用程序共享的主机不支持控制台代理。该主机必须是专用主机。主机可以是满足以下大小要求的任何架构：

- 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 Docker 或 Podman 的设计目的是在此目录中创建容器。具体来说，他们将在 `/var/lib/containers/storage`目录。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	9.1 至 9.4 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 查看 Podman 配置要求 。	在强制模式或宽容模式下受支持 • 操作系统上启用了 SELinux 的代理不支持对Cloud Volumes ONTAP系统的管理。

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
Ubuntu	24.04 LTS	3.9.45 或更高版本，NetApp控制台处于标准模式或受限模式	Docker Engine 23.06 至 28.0.0。	不支持

AWS EC2 实例类型

满足上述 CPU 和 RAM 要求的实例类型。我们推荐 t3.2xlarge。

Azure VM 大小

满足上述 CPU 和 RAM 要求的实例类型。我们推荐 Standard_D8s_v3。

Google Cloud 机器类型

满足上述 CPU 和 RAM 要求的实例类型。我们推荐 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"

/opt 中的磁盘空间

必须有 100 GiB 可用空间

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

/var 中的磁盘空间

必须有 20 GiB 可用空间

控制台代理需要此空间 `/var`因为 Docker 或 Podman 的设计目的是在此目录中创建容器。具体来说，他们将在 `/var/lib/containers/storage`目录。外部安装或符号链接不适用于此空间。

步骤 **4**：安装 **Podman** 或 **Docker Engine**

要手动安装控制台代理，请通过安装 Podman 或 Docker Engine 来准备主机。

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 **5.** 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 软件包版本 1.0.6
- 将 podman-compose 添加到 PATH 环境变量
- 如果使用 Red Hat Enterprise Linux 8，请验证您的 Podman 版本使用的是 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。

   对于 Red Hat Enterprise Linux 9：

```
sudo dnf install podman-2:<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 。

   对于 Red Hat Enterprise Linux 8：

```
sudo dnf install podman-3:<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。
6. 如果使用 Red Hat Enterprise：

   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。

   对于 Red Hat Enterprise Linux 9：

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

   对于 Red Hat Enterprise Linux 8：

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

7. 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。

8. 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。

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

      ```
      podman info | grep networkBackend
      ```

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

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

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

   d. 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。

9. 重新启动 podman。

```
systemctl restart podman
```

10. 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 **5**：准备网络访问

设置网络访问，以便控制台代理可以管理公共云中的资源。除了为控制台代理提供虚拟网络和子网之外，您还需要确保满足以下要求。

连接到目标网络

确保控制台代理与存储位置有网络连接。例如，您计划部署Cloud Volumes ONTAP 的VPC 或 VNet，或者您的本地ONTAP集群所在的数据中心。

准备网络以供用户访问**NetApp**控制台

在受限模式下，用户从控制台代理 VM 访问控制台。控制台代理联系几个端点来完成数据管理任务。当从控制台完成特定操作时，将从用户的计算机联系这些端点。

4.0.0 版本之前的控制台代理需要额外的端点。如果您升级到 4.0.0 或更高版本，则可以从允许列表中删除旧端点。"了解有关 4.0.0 之前版本所需的网络访问的更多信息。"

+

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控制台中提供功能和服务。
\ https://cdn.auth0.com \ https://services.cloud.netapp.com	您的 Web 浏览器通过NetApp控制台连接到这些端点以进行集中用户身份验证。

用于日常运营的出站互联网访问

控制台代理的网络位置必须具有出站互联网访问权限。它需要能够访问NetApp控制台的 SaaS 服务以及各自公共云环境中的端点。

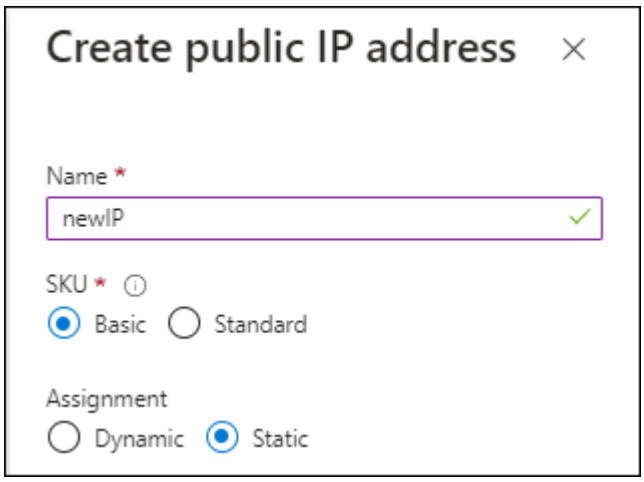
端点	目的
AWS 环境	AWS 服务（amazonaws.com）： • 云形成 • 弹性计算云（EC2） • 身份和访问管理 (IAM) • 密钥管理服务（KMS） • 安全令牌服务 (STS) • 简单存储服务（S3）
管理 AWS 资源。端点取决于您的 AWS 区域。 "有关详细信息，请参阅 AWS 文档"	Azure 环境
\ https://management.azure.com \ https://login.microsoftonline.com \ https://blob.core.windows.net \ https://core.windows.net	管理 Azure 公共区域中的资源。
\ https://management.usgovcloudapi.net \ https://login.microsoftonline.us \ https://blob.core.usgovcloudapi.net \ https://core.usgovcloudapi.net	管理 Azure 政府区域中的资源。
\ 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
Google Cloud 环境	\ 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://www.googleapis.com/deploymentmanager/v2/projects
管理 Google Cloud 中的资源。	• NetApp控制台端点*
\ https://mysupport.netapp.com	获取许可信息并向NetApp支持发送AutoSupport消息。
\ https://support.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控制台。
\ 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控制台中提供功能和服务。

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 中的公共 **IP** 地址

如果要在 Azure 中将公共 IP 地址与控制台代理 VM 一起使用，则该 IP 地址必须使用基本 SKU 以确保控制台使用此公共 IP 地址。



如果您使用标准 SKU IP 地址，则控制台将使用控制台代理的_私有_ IP 地址，而不是公共 IP。如果您用于访问控制台的机器无法访问该私有 IP 地址，则控制台中的操作将会失败。

"Azure 文档：公共 IP SKU"

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数据分类来扫描公司数据源，则应在控制台代理和NetApp数据分类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"

如果您计划从云提供商的市场创建控制台代理，请在创建控制台代理后实现此网络要求。

步骤 **6**：准备云权限

控制台代理需要云提供商的权限才能在虚拟网络中部署Cloud Volumes ONTAP并使用NetApp数据服务。您需要在云提供商中设置权限，然后将这些权限与控制台代理关联。

要查看所需的步骤，请选择用于云提供商的身份验证选项。

AWS IAM 角色

使用 IAM 角色为控制台代理提供权限。

如果您从 AWS Marketplace 创建控制台代理，则在启动 EC2 实例时系统会提示您选择该 IAM 角色。

如果您在自己的 Linux 主机上手动安装控制台代理，请将角色附加到 EC2 实例。

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。
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

您现在拥有控制台代理 EC2 实例的 IAM 角色。

AWS 访问密钥

为 IAM 用户设置权限和访问密钥。安装控制台代理并设置控制台后，您需要向控制台提供 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控制台。

Azure 角色

创建具有所需权限的 Azure 自定义角色。您将把此角色分配给控制台代理 VM。

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控制台一起使用的每个 Azure 订阅添加 ID。

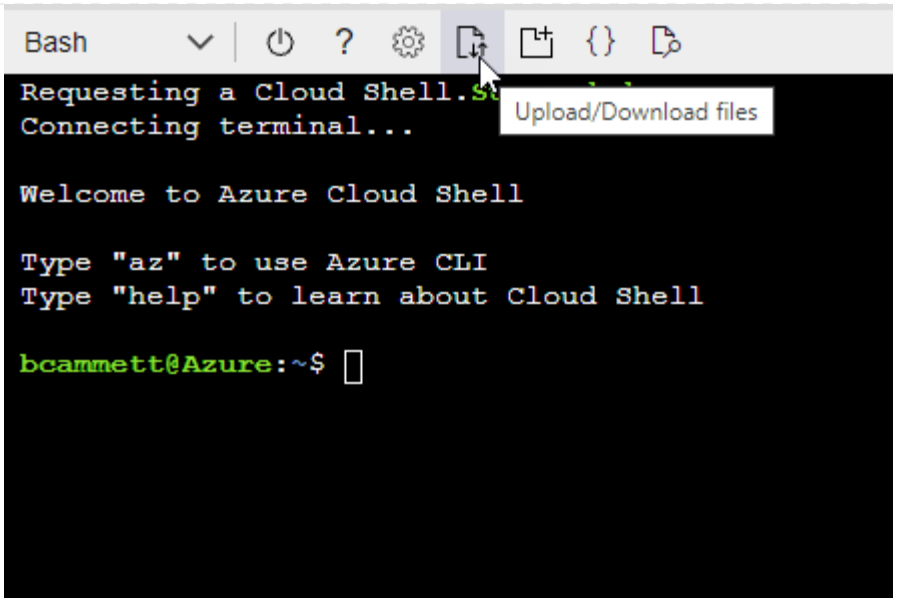
   例子

   ```
   "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 Connector_Policy.json
```

Azure 服务主体

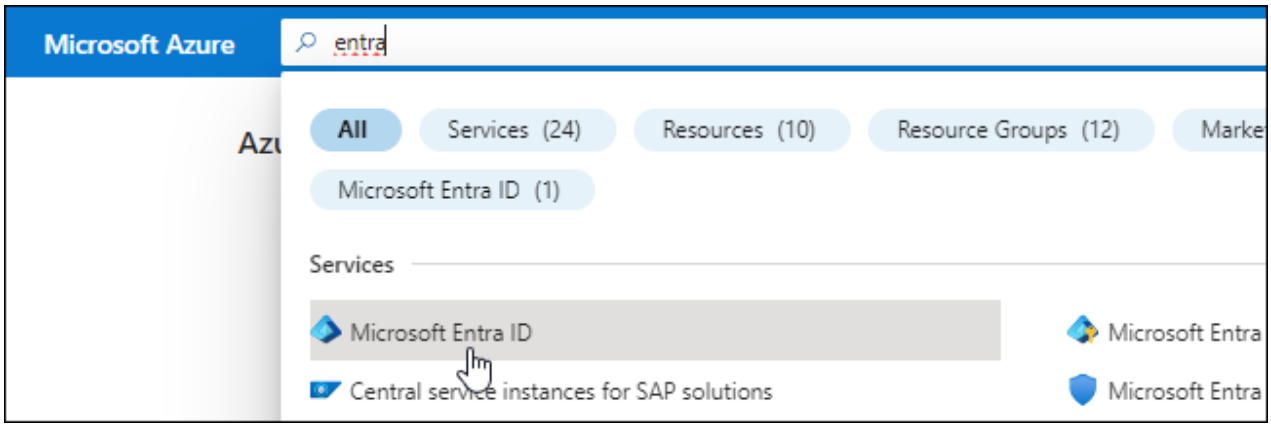
在 Microsoft Entra ID 中创建并设置服务主体，并获取控制台所需的 Azure 凭据。安装控制台代理后，您需要向控制台提供这些凭据。

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控制台一起使用）。
- 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。

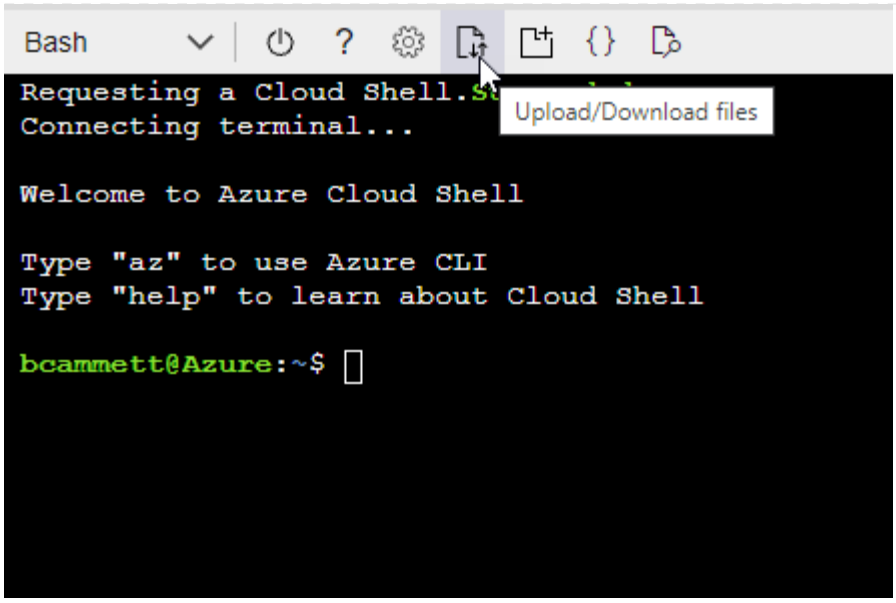
例子

```
"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
Connector_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。

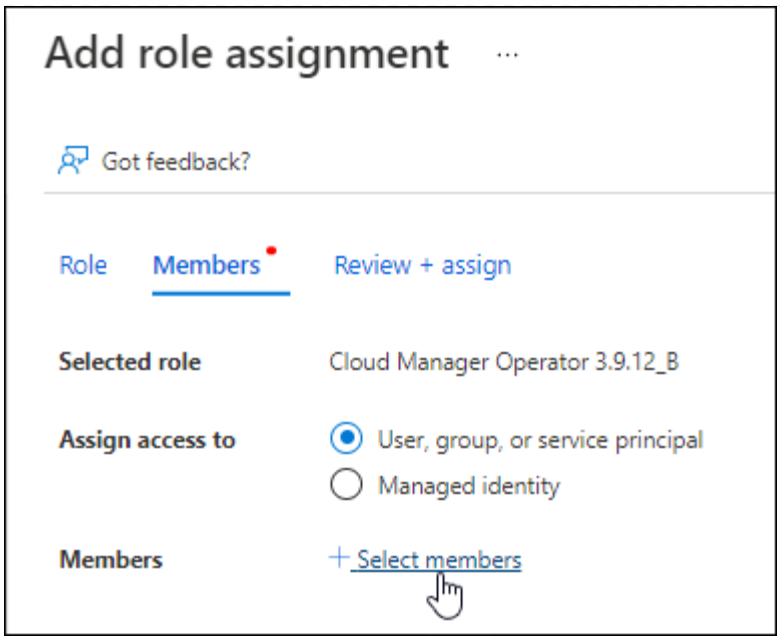
b. 选择订阅。

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*。

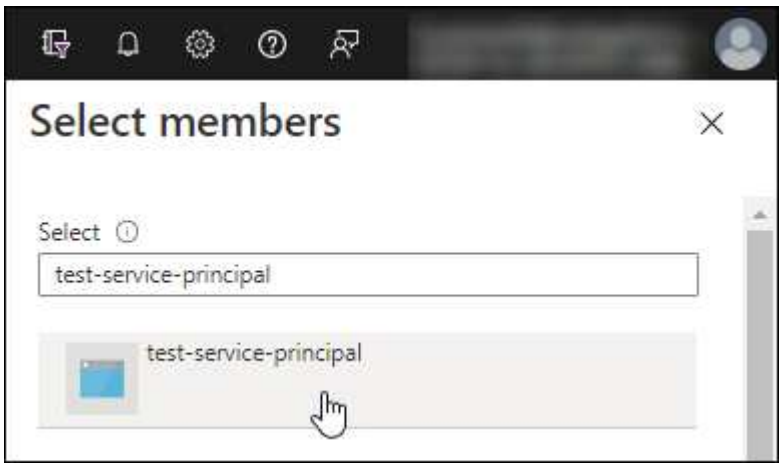
e. 在“成员”选项卡中，完成以下步骤：

- 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”。

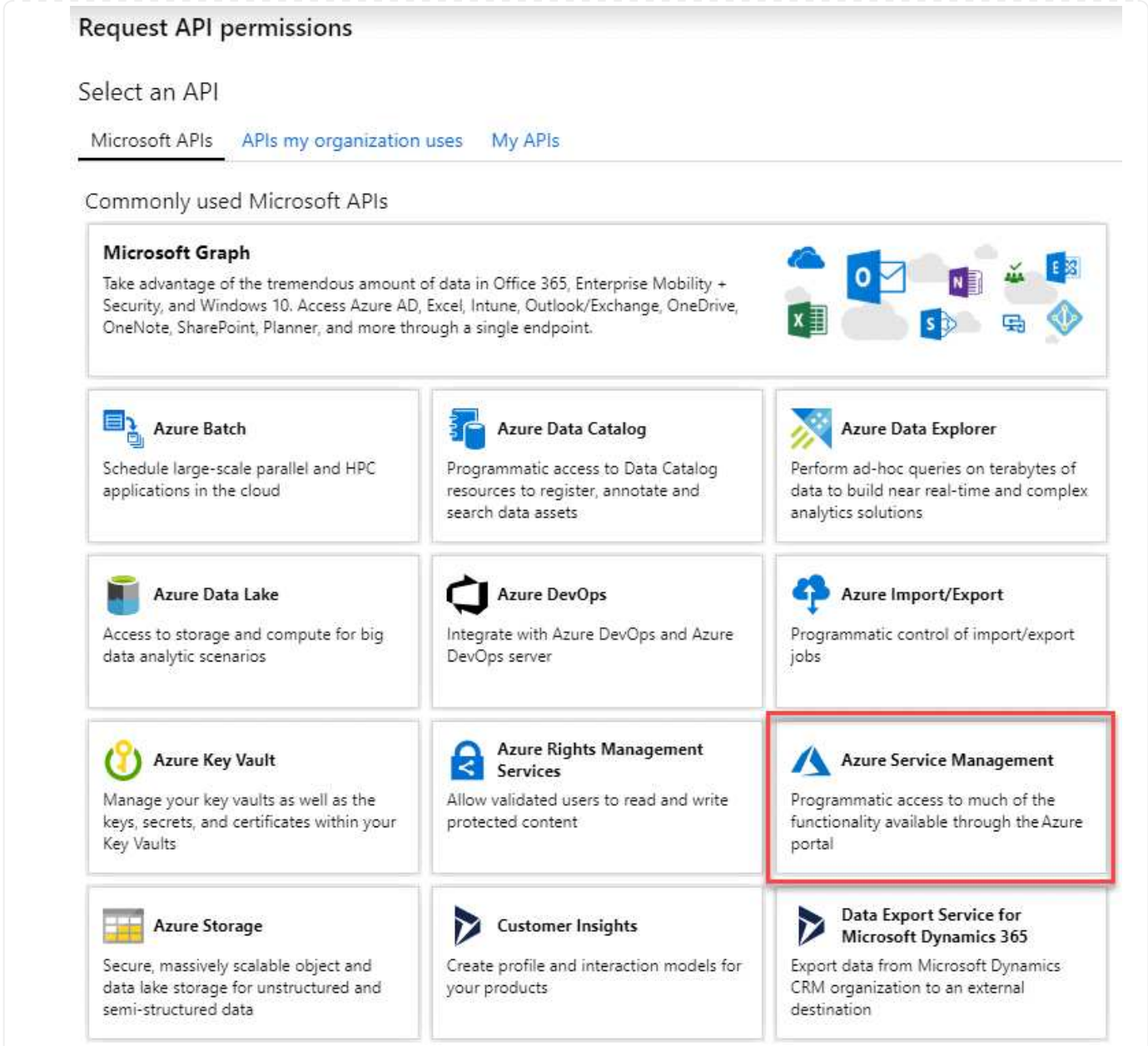
f. 选择*审阅+分配*。

服务主体现在具有部署控制台代理所需的 Azure 权限。

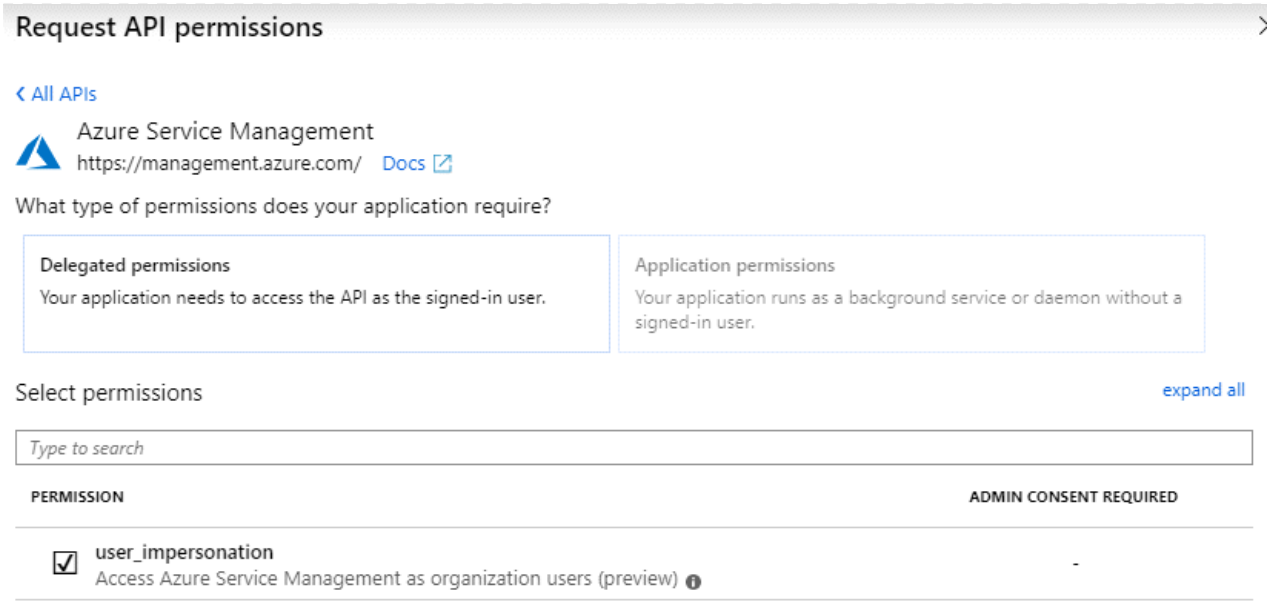
如果您想从多个 Azure 订阅部署Cloud Volumes ONTAP ，则必须将服务主体绑定到每个订阅。在NetApp控制台中，您可以选择部署Cloud Volumes ONTAP时要使用的订阅。

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”。

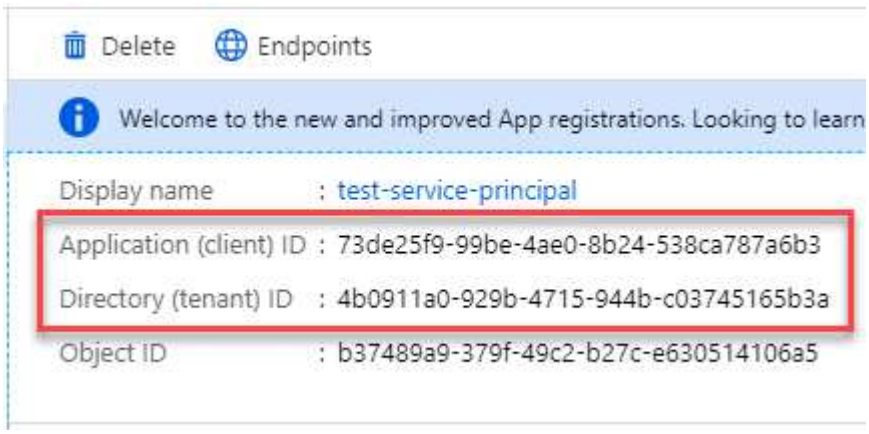


4. 选择*以组织用户身份访问 Azure 服务管理*，然后选择*添加权限*。



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完毕，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。

Google Cloud 服务帐号

创建一个角色并将其应用于您将用于控制台代理 VM 实例的服务帐户。

步骤

1. 在 Google Cloud 中创建自定义角色：

   a. 创建一个 YAML 文件，其中包含在"Google Cloud 的控制台代理政策"。

   b. 从 Google Cloud 激活云壳。

   c. 上传包含控制台代理所需权限的 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“connector”的角色：

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

   +
   "Google Cloud 文档：创建和管理自定义角色"

2. 在 Google Cloud 中创建服务帐号：

   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"

结果

您现在拥有一个可以分配给控制台代理 VM 实例的服务帐户。

步骤 **7**：启用 **Google Cloud API**

在 Google Cloud 中部署Cloud Volumes ONTAP需要多个 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
   - 云日志 API
   - 云资源管理器 API
   - 计算引擎 API
   - 身份和访问管理 (IAM) API
   - 云密钥管理服务 (KMS) API

     （仅当您计划将NetApp Backup and Recovery 与客户管理加密密钥 (CMEK) 结合使用时才需要）

在限制模式下部署控制台代理

以受限模式部署控制台代理，以便您可以在有限的出站连接下使用NetApp控制台。首先，安装控制台代理，通过访问控制台代理上运行的用户界面来设置控制台，然后提供您之前设置的云权限。

步骤 **1**：安装控制台代理

从云提供商的市场安装控制台代理或在 Linux 主机上手动安装。

AWS 商业市场

开始之前

您应该具有以下内容：

- 满足组网需求的VPC及子网。

  "了解网络要求"

- 具有附加策略的 IAM 角色，其中包含控制台代理所需的权限。

  "了解如何设置 AWS 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。

  "审查实例要求" 。

- EC2 实例的密钥对。

步骤

1. 前往 "AWS Marketplace 上的NetApp控制台代理列表"
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*。

结果

AWS 使用指定的设置启动软件。控制台代理实例和软件运行大约需要五分钟。

下一步是什么?

设置NetApp控制台。

AWS 政府市场

开始之前

您应该具有以下内容：

- 满足组网需求的VPC及子网。

  "了解网络要求"

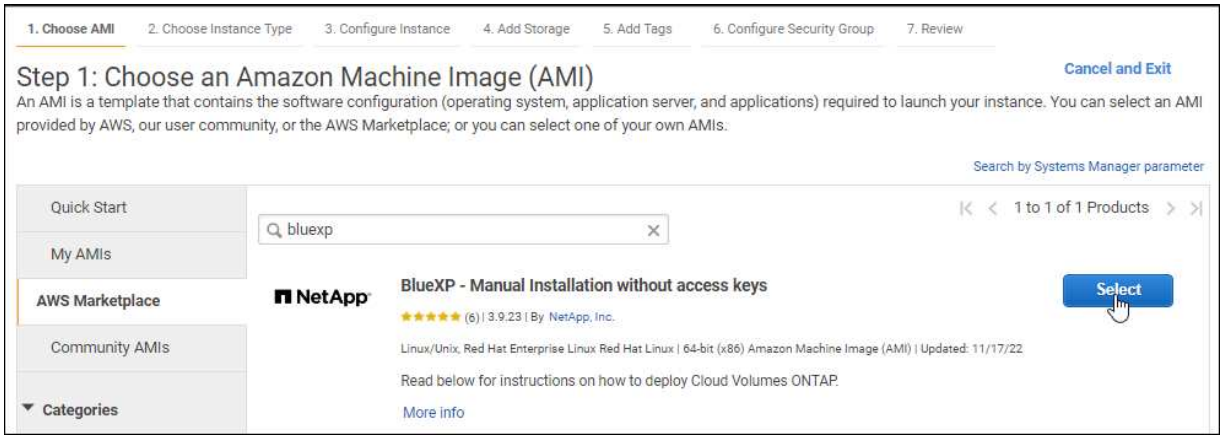
- 具有附加策略的 IAM 角色，其中包含控制台代理所需的权限。

  "了解如何设置 AWS 权限"

- 您的 IAM 用户订阅和取消订阅 AWS Marketplace 的权限。
- EC2 实例的密钥对。

步骤

1. 转到 AWS Marketplace 中提供的NetApp控制台代理。
   a. 打开 EC2 服务并选择 启动实例。
   b. 选择 **AWS Marketplace**。
   c. 搜索NetApp Console 并选择产品。



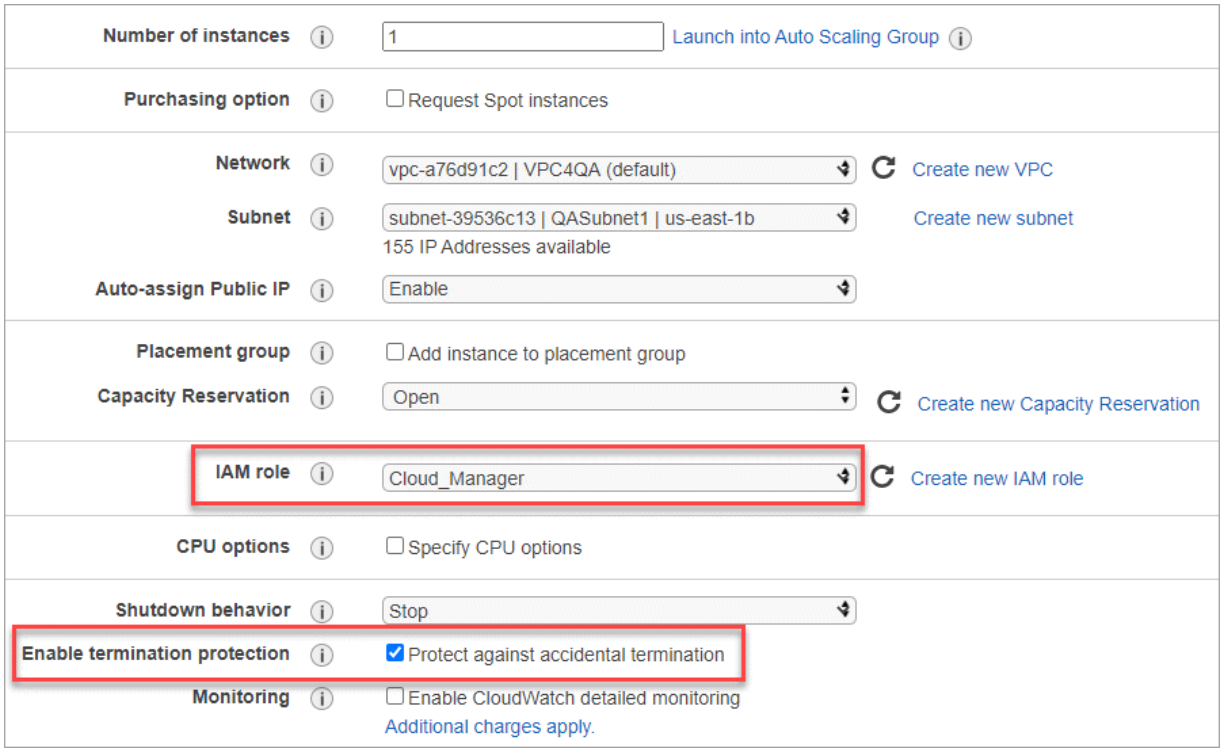
d. 选择*继续*。

2. 按照提示配置并部署实例：

   - 选择实例类型：根据区域可用性，选择一种受支持的实例类型（建议使用 t3.2xlarge）。

     "查看实例要求" 。

   - 配置实例详细信息：选择 VPC 和子网，选择您在步骤 1 中创建的 IAM 角色，启用终止保护（推荐），并选择任何其他符合您要求的配置选项。



   - 添加存储：保留默认存储选项。
   - 添加标签：如果需要，输入实例的标签。
   - 配置安全组：指定控制台代理实例所需的连接方法：SSH、HTTP 和 HTTPS。
   - 审查：审查您的选择并选择*启动*。

结果

AWS 使用指定的设置启动软件。控制台代理实例和软件运行大约需要五分钟。

下一步是什么？

设置控制台。

Azure 政府市场

开始之前

您应该具有以下内容：

- 满足网络要求的 VNet 和子网。

  "了解网络要求"

- 包含控制台代理所需权限的 Azure 自定义角色。

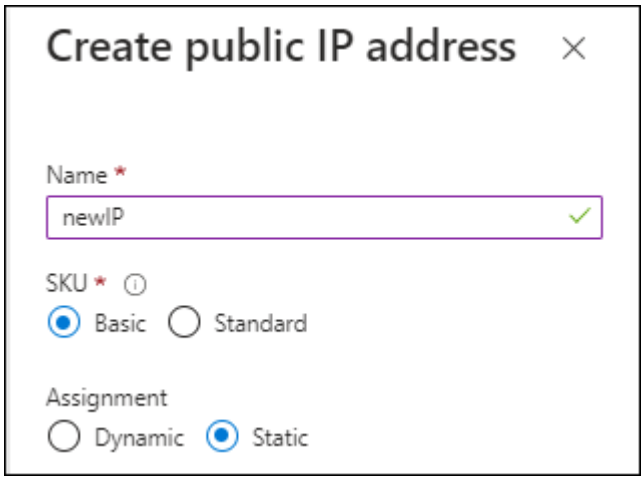
  "了解如何设置 Azure 权限"

步骤

1. 转到 Azure 市场中的NetApp控制台代理 VM 页面。
   - "商业区域的 Azure 市场页面"
   - "Azure 政府区域的 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。
   - 公共 **IP**：如果您想将公共 IP 地址与控制台代理 VM 一起使用，则该 IP 地址必须使用基本 SKU 以确保控制台使用此公共 IP 地址。



   如果您使用标准 SKU IP 地址，则控制台将使用控制台代理的_私有_ IP 地址，而不是公共 IP。如果您用于访问控制台的机器无法访问该私有 IP 地址，则控制台中的操作将会失败。

   "Azure 文档：公共 IP SKU"

   - 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。

结果

Azure 使用指定的设置部署虚拟机。虚拟机和控制台代理软件应在大约五分钟内运行。

下一步是什么?

设置NetApp控制台。

手动安装

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"。

- 您需要禁用安装期间验证出站连接的配置检查。如果未禁用此检查，手动安装将失败。"了解如何禁用手动安装的配置检查。"
- 根据您的操作系统，在安装控制台代理之前需要 Podman 或 Docker Engine。

关于此任务

NetApp支持站点上提供的安装程序可能是早期版本。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. 从下载控制台代理软件 "NetApp 支持站点"，然后将其复制到Linux主机上。

   您应该下载适用于您的网络或云中的“在线”代理安装程序。

3. 分配运行脚本的权限。

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

   其中 <version> 是您下载的控制台代理的版本。

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

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

如果您的网络需要代理来访问互联网，则需要添加代理信息。您可以添加透明或显式代理。 --proxy 和 --cacert 参数是可选的，系统不会提示您添加它们。如果您有代理服务器，则需要输入所示的参数。

以下是使用 CA 签名证书配置显式代理服务器的示例：

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

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

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

  请注意以下事项：

  - 用户可以是本地用户或域用户。
  - 对于域用户，您必须使用 \ 的 ASCII 代码，如上所示。
  - 控制台代理不支持包含 @ 字符的用户名或密码。
  - 如果密码包含以下任何特殊字符，则必须在该特殊字符前面加上反斜杠来转义该特殊字符：& 或 !

    例如：

http://bxpproxyuser:netapp1\!@地址:3128

`--cacert`指定用于控制台代理和代理服务器之间的 HTTPS 访问的 CA 签名证书。 HTTPS代理服务器、拦截代理服务器、透明代理服务器都需要此参数。

+ 下面是配置透明代理服务器的示例。配置透明代理时，不需要定义代理服务器。您只需将 CA 签名的证书添加到控制台代理主机：

+

```
 ./NetApp_Console_Agent_Cloud_v4.0.0 --cacert
/tmp/cacert/certificate.cer
```

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
      ...
      # 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
      ...
      Esc:wq
      ```

   c. 重新启动控制台代理虚拟机。

结果

控制台代理现已安装。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。

下一步是什么?

设置NetApp控制台。

第 2 步：设置NetApp控制台

首次访问控制台时，系统会提示您为控制台代理选择一个组织，并需要启用受限模式。

开始之前

设置控制台代理的人员必须使用尚不属于控制台组织的登录名登录控制台。

如果您的登录信息与其他组织相关联，则您需要使用新的登录信息进行注册。否则，您将不会在设置屏幕上看到启用受限模式的选项。

步骤

1. 从与控制台代理实例有连接的主机打开 Web 浏览器，然后输入您安装的控制台代理的以下 URL。
2. 注册或登录NetApp控制台。
3. 登录后，设置控制台：

a. 输入控制台代理的名称。
b. 输入新控制台组织的名称。
c. 选择*您是否在安全环境中运行？*
d. 选择*在此帐户上启用受限模式*。

请注意，帐户创建后您无法更改此设置。您以后无法启用受限模式，也无法禁用它。

如果您在政府区域部署了控制台代理，则该复选框已启用且无法更改。这是因为限制模式是政府区域唯一支持的模式。

a. 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。所有用户都需要使用控制台代理实例的 IP 地址访问控制台。

下一步是什么？

向控制台提供您之前设置的权限。

步骤 3：提供对NetApp控制台的权限

如果您从 Azure 市场部署了控制台代理，或者手动安装了控制台代理软件，则需要提供之前设置的权限。

如果您从 AWS Marketplace 部署了控制台代理，则这些步骤不适用，因为您在部署期间选择了所需的 IAM 角色。

"了解如何准备云权限" 。

AWS IAM 角色

将您之前创建的 IAM 角色附加到安装了控制台代理的 EC2 实例。

仅当您在 AWS 中手动安装了控制台代理时，这些步骤才适用。对于 AWS Marketplace 部署，您已将控制台代理实例与包含所需权限的 IAM 角色关联。

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。

AWS 访问密钥

向NetApp控制台提供具有所需权限的 IAM 用户的 AWS 访问密钥。

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*。

Azure 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控制台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。

Azure 服务主体

向NetApp控制台提供您之前设置的 Azure 服务主体的凭据。

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
        - 客户端机密
    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

NetApp控制台现在具有代表您在 Azure 中执行操作所需的权限。

Google Cloud 服务帐号

将服务帐户与控制台代理 VM 关联。

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. 如果您想管理其他项目中的资源，请通过将具有控制台代理角色的服务帐户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。

订阅**NetApp**智能服务（受限模式）

从云提供商的市场订阅NetApp智能服务，以按小时费率（PAYGO）或通过年度合同支付数据服务费用。如果您从NetApp （BYOL）购买了许可证，您还需要订阅市场产品。您的许可证始终会先被收费，但如果您超出许可容量或许可证期限到期，则会按小时费率向您

收费。

市场订阅支持以受限模式对以下数据服务收费：

- NetApp备份和恢复
- Cloud Volumes ONTAP
- NetApp云分层
- NetApp勒索软件抵御能力
- NetApp灾难恢复

NetApp数据分类可通过您的订阅启用，但使用分类是免费的。

开始之前

您必须已经部署控制台代理才能订阅数据服务。您需要将市场订阅与连接到控制台代理的云凭据关联起来。

AWS

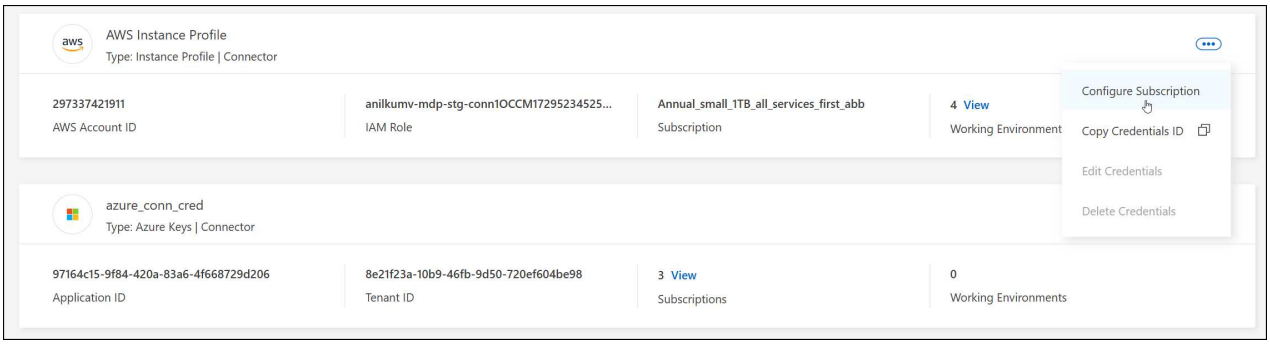
以下视频展示了从 AWS Marketplace 订阅NetApp智能服务的步骤：

从 AWS Marketplace 订阅NetApp智能服务

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控制台关联的凭据关联。



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控制台。

   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*。

Azure

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控制台关联的凭据关联。

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控制台。

   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*。

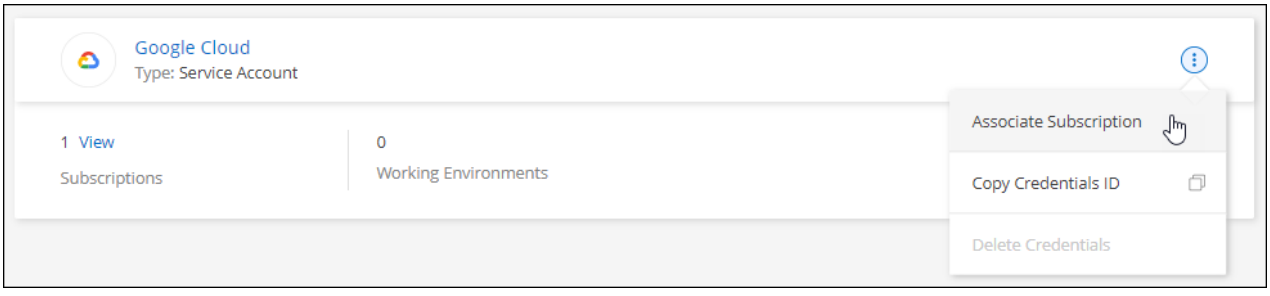
        以下视频展示了从 Azure 市场订阅的步骤：

[从 Azure 市场订阅NetApp智能服务]

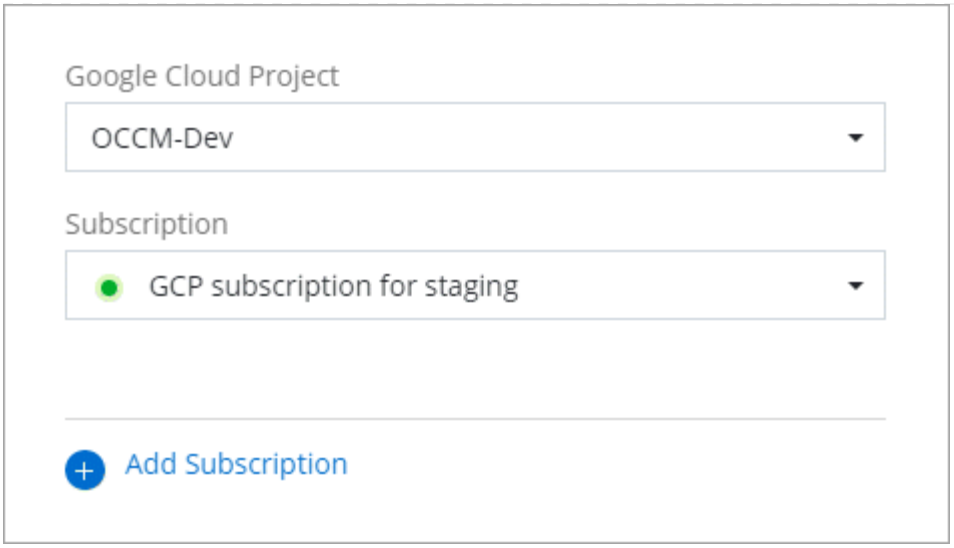
Google Cloud

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*。 +需要新的屏幕截图（TS）



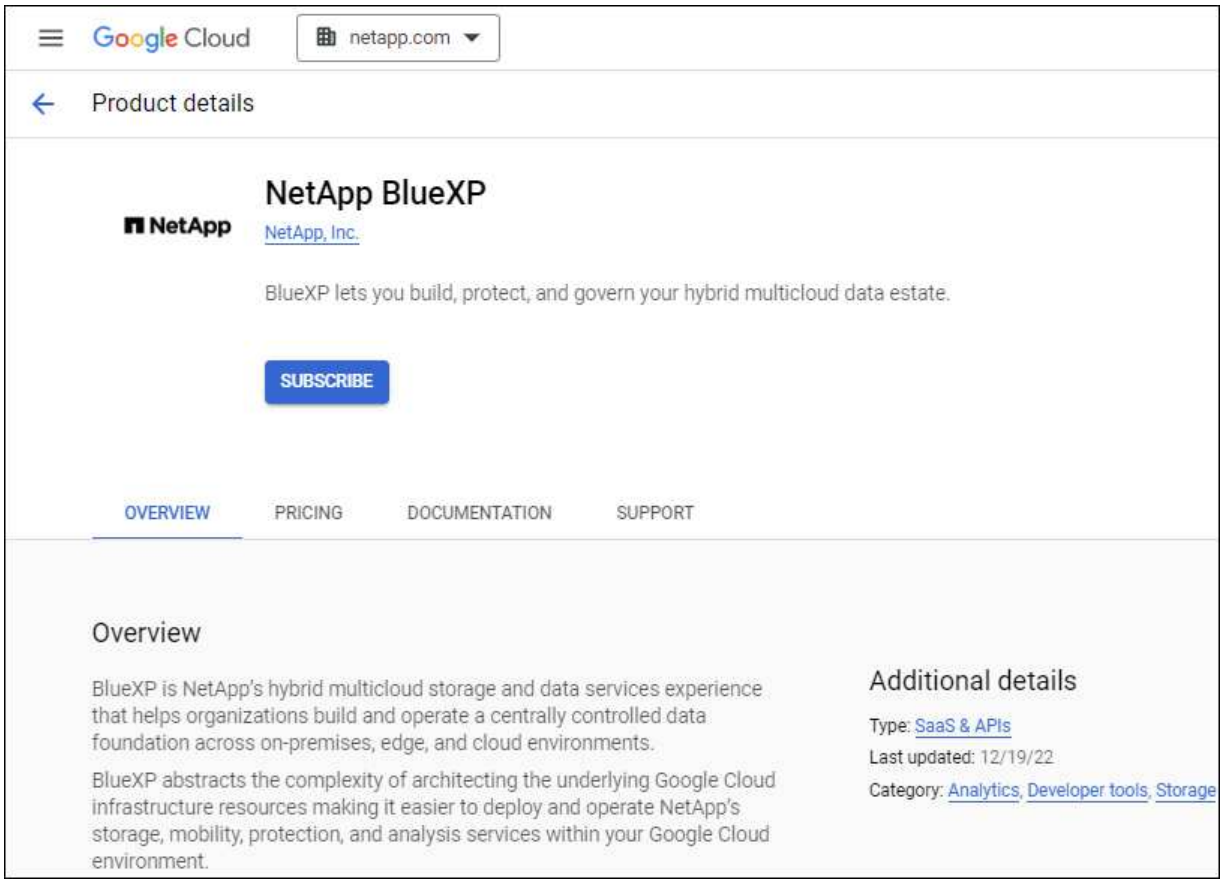
4. 要使用选定的凭据配置现有订阅，请从下拉列表中选择一个 Google Cloud 项目和订阅，然后选择*配置*。



5. 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智能服务页面"，确保在顶部导航菜单中选择了正确的项目。



   b. 选择*订阅*。

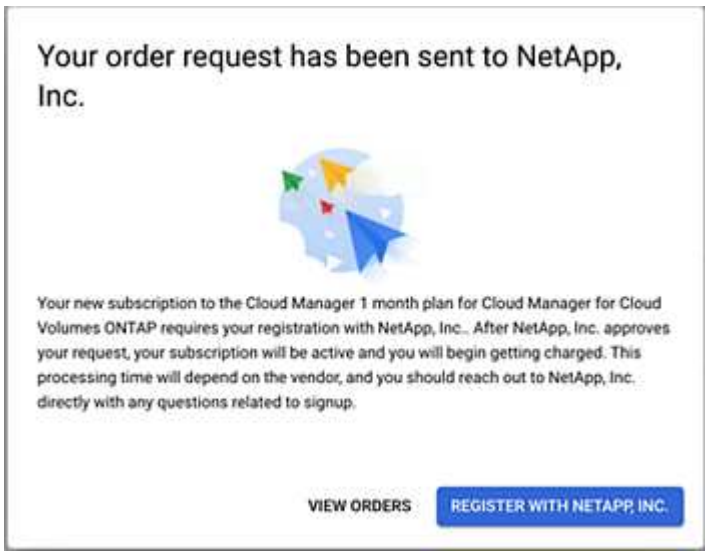
   c. 选择适当的结算账户并同意条款和条件。

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控制台中的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。

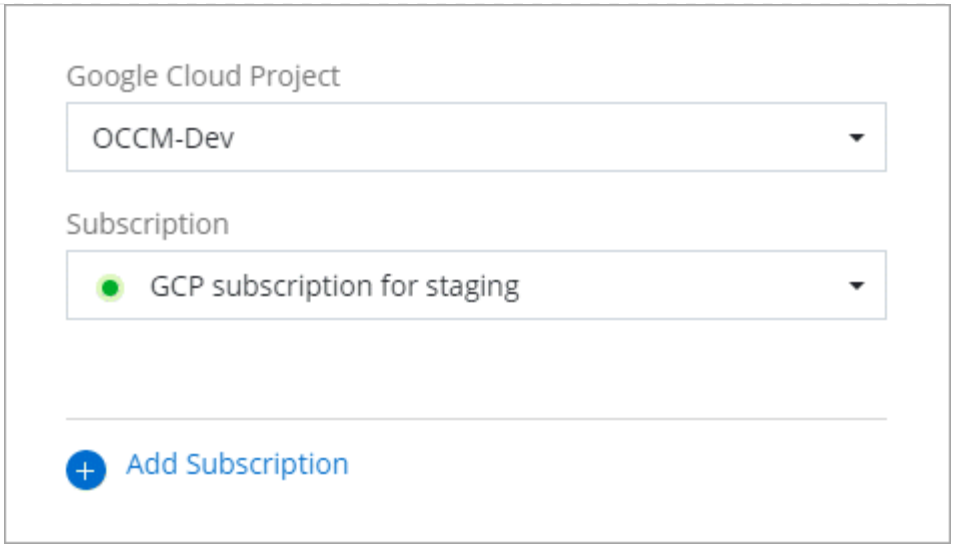
对于所有其他组织或帐户，您需要重复这些步骤来手动关联订阅。

- 选择*保存*。

以下视频展示了从 Google Cloud Marketplace 订阅的步骤：

从 Google Cloud Marketplace 订阅

a. 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。



相关信息

- "管理Cloud Volumes ONTAP 的BYOL 基于容量的许可证"
- "管理数据服务的 BYOL 许可证"
- "管理 AWS 凭证和订阅"
- "管理 Azure 凭据和订阅"
- "管理 Google Cloud 凭据和订阅"

接下来可以做什么（受限模式）

在限制模式下启动并运行NetApp控制台后，您可以开始使用限制模式支持的服务。

如需帮助，请参阅以下服务的文档：

- "Azure NetApp Files文档"
- "备份和恢复文档"
- "分类文档"
- "Cloud Volumes ONTAP文档"
- "数字钱包文档"
- "本地ONTAP集群文档"
- "复制文档"

相关信息

"NetApp控制台部署模式"

开始使用BlueXP旧版界面（私人模式）

入门工作流程（**BlueXP**私人模式）

BlueXP私有模式（传统BlueXP接口）通常用于没有互联网连接的本地环境和安全云区域，其中包括 AWS Secret Cloud、AWS Top Secret Cloud 和 Azure IL6。 NetApp继续通过传统的BlueXP界面支持这些环境。

"BlueXP私人模式的 PDF 文档"

私有模式支持的功能和数据服务

下表可以帮助您快速识别哪些BlueXP服务和功能支持私人模式。

请注意，某些服务可能会受到限制。

产品领域	**BlueXP**服务或功能	私人模式
工作环境 表格的这一部分列出了对BlueXP画布的工作环境管理的支持。它没有指出BlueXP backup and recovery所支持的备份目的地。	适用于ONTAP 的Amazon FSx	否
	Amazon S3	否
	Azure Blob	否
	Azure NetApp Files	否
	Cloud Volumes ONTAP	是
	Google Cloud NetApp Volumes	否
	Google Cloud Storage	否
	本地ONTAP集群	是
	E 系列	否
	StorageGRID	否

产品领域	**BlueXP**服务或功能	私人模式
服务	警报	否
	备份和恢复	是的https://docs.netapp.com/us-en/bluexp-backup-recovery/prev-ontap-protect-journey.html#support-for-sites-with-no-internet-connectivity["查看ONTAP卷数据支持的备份目标列表"^]
	分类	是
	复制和同步	否
	数字顾问	否
	数字钱包	是
	灾难恢复	否
	经济效益	否
	勒索软件防护	否
	复制	是
	软件更新	否
	可持续性	否
	分层	否
	卷缓存	否
	工作负载工厂	否
特征	身份和访问管理	是
	凭据	是
	联邦	否
	多因素身份验证	否
	NSS 账户	否
	通知	否
	搜索	否
	时间表	是

使用NetApp控制台

登录NetApp控制台

如何登录NetApp控制台取决于您使用的部署模式。

24 小时后或关闭浏览器后，您将自动退出。

"了解控制台部署模式" 。

标准模式

注册NetApp控制台后，您可以从基于 Web 的控制台登录，开始管理您的数据和存储基础架构。

关于此任务

您可以使用以下选项之一登录NetApp控制台：

- 您现有的NetApp支持站点 (NSS) 凭证
- 使用您的电子邮件地址和密码的NetApp控制台帐户
- 联合连接

  您可以使用单点登录，使用公司目录（联合身份）中的凭据登录。"了解如何设置身份联合" 。

步骤

1. 打开 Web 浏览器并转到 "NetApp控制台"
2. 在*登录*页面上，输入与您的登录关联的电子邮件地址。
3. 根据与您的登录相关的身份验证方法，系统将提示您输入您的凭据：
   - NetApp云凭证：输入您的密码
   - 联合用户：输入您的联合身份凭证
   - NetApp支持站点帐户：输入您的NetApp支持站点凭据

结果

您现在已登录并可以开始使用它来管理您的混合多云基础设施。

限制模式

在受限模式下使用控制台时，您需要从代理上本地运行的用户界面登录到控制台。

关于此任务

在受限模式下，控制台支持使用以下选项之一登录：

- 使用您的电子邮件地址和密码登录NetApp控制台
- 联合连接

  您可以使用单点登录，使用公司目录（联合身份）中的凭据登录。"了解如何使用身份联合" 。

步骤

1. 打开 Web 浏览器并输入安装代理的 IP 地址。
2. 输入您的用户名和密码登录。

查看NetApp控制台主页上的指标

监控存储资产的健康状况可确保您了解存储保护问题并采取措施解决这些问题。使用NetApp控制台主页，查看NetApp Backup and Recovery 的备份和恢复状态，以及面临

勒索软件攻击风险或受到NetApp Ransomware Resilience 保护的工作负载数量。您可以查看单个集群和Cloud Volumes ONTAP的存储容量、 ONTAP警报、每个集群或Cloud Volumes ONTAP系统的存储性能容量、您拥有的不同类型的许可证等等。

主页上的所有窗格均显示组织级别的数据。存储容量和存储性能窗格显示用户可以根据 IAM 权限访问的与项目相关的系统。

系统每五分钟刷新一次主页上的数据。缓存可能会导致此页面上的数据与实际值相差长达 15 分钟。

主页上的准确指标需要适当大小和配置的控制台代理。

所需的NetApp控制台角色

主页中的每个窗格都需要不同的用户角色：

- 存储容量窗格：能够查看NetApp控制台系统页面
- * ONTAP警报窗格*：文件夹或项目管理员、运营支持分析师、组织管理员、组织查看器、超级管理员、超级查看器
- 存储性能容量窗格：能够查看NetApp控制台系统页面
- 许可证和订阅窗格：文件夹或项目管理员、组织管理员、组织查看者、超级管理员、超级查看者
- 勒索软件弹性窗格：文件夹或项目管理员、组织管理员、勒索软件保护管理员、勒索软件保护查看器、超级管理员、超级查看器
- 备份和恢复窗格：备份和恢复备份管理员、备份和恢复超级管理员、备份和恢复备份查看器、备份和恢复克隆管理员、文件夹或项目管理员、组织管理员、备份和恢复恢复管理员、超级管理员、超级查看器

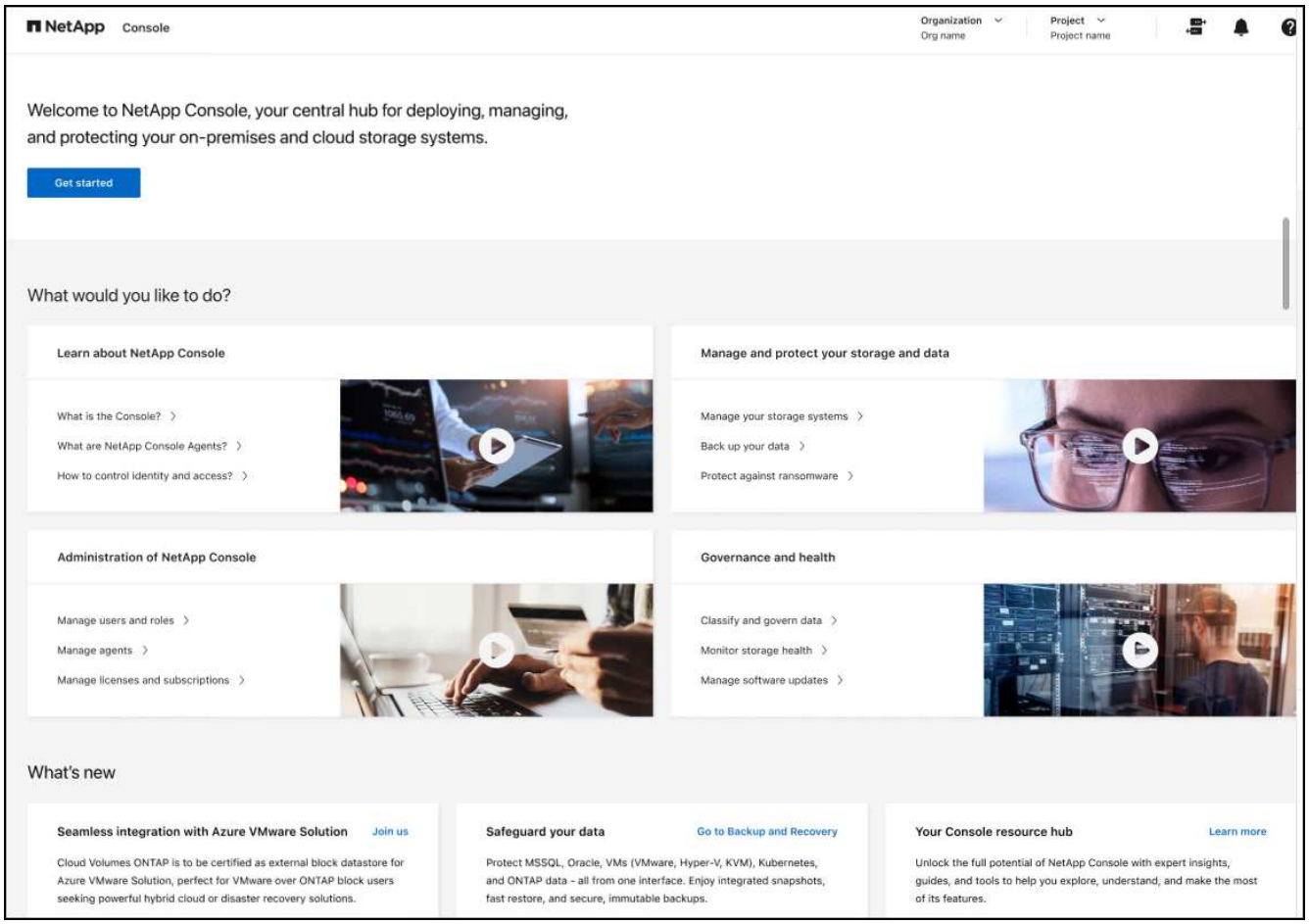
如果您没有访问窗格的权限，该窗格会显示一条消息，表明您没有使用该窗格的权限。

"了解NetApp控制台访问角色。" 。

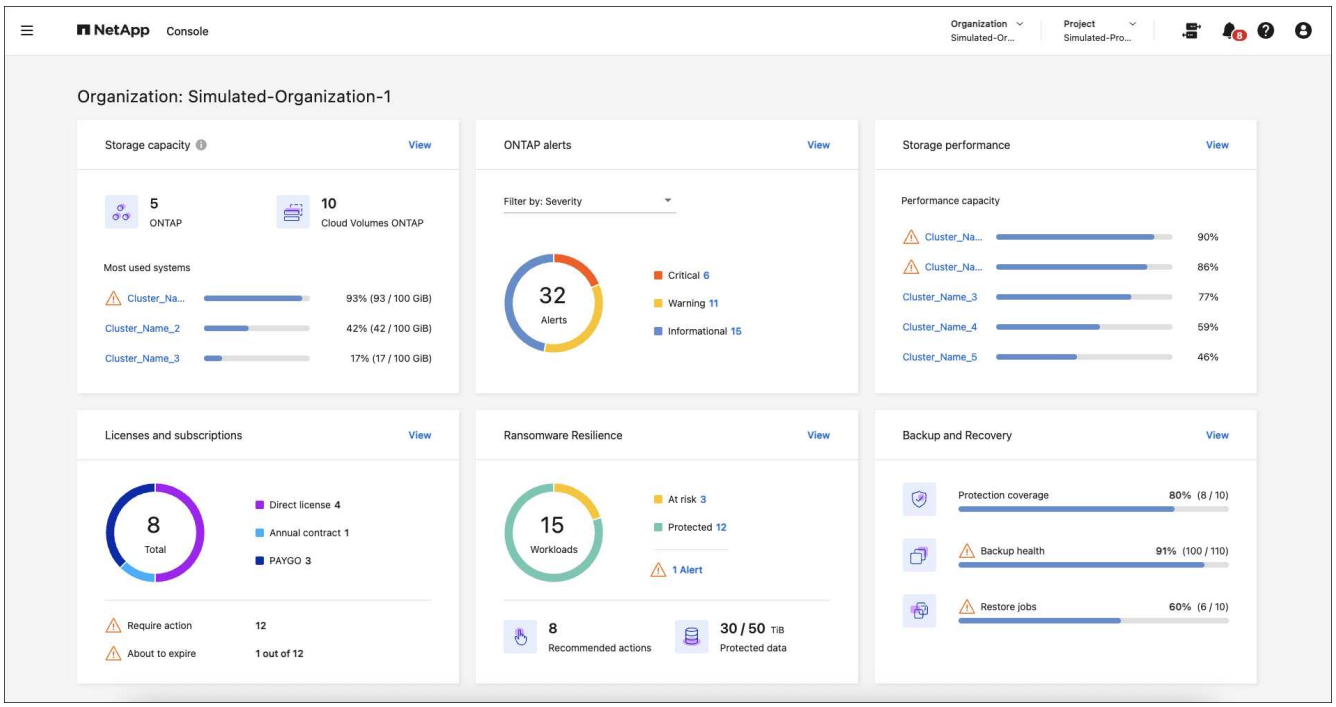
步骤

1. 从NetApp控制台菜单中，选择 主页。

   如果您具有组织管理员角色并且未设置代理或存储系统，则主页将显示入门信息。



如果您已设置NetApp控制台，至少启用了一个控制台代理，并且在该代理上添加了至少一个集群或Cloud Volumes ONTAP系统，则主页将显示有关您的存储环境的指标。



启用指标以显示在主页上

当满足以下条件时，您可以在主页上看到指标：

- 您已登录到NetApp控制台的 SaaS 实例。
- 您属于具有现有存储资源（代理和集群或Cloud Volumes ONTAP系统）的组织。
- 至少启用了一个控制台代理。
- 该代理上至少添加了一个集群或Cloud Volumes ONTAP系统。

要使指标显示在主页上，请完成以下任务：

- 启用至少一个控制台代理。
- 使用该代理添加至少一个集群或一个Cloud Volumes ONTAP 。

查看整体存储容量

存储容量窗格提供跨ONTAP集群和Cloud Volumes ONTAP系统的以下信息：

- 控制台中发现的ONTAP系统数量
- 控制台中发现的Cloud Volumes ONTAP系统数量
- 每个集群的容量使用情况

集群或Cloud Volumes ONTAP系统的顺序基于所使用的容量。容量最高的集群或系统会首先出现，以便于识别。

警告指示器显示集群容量为 80%，数据每五分钟更新一次。

如果您有多个项目，您可能会在“存储容量”窗格中看到与“系统”页面不同的数据。这是因为“系统”页面显示基于项目级别的信息，而“存储容量”窗格显示组织级别的信息。此外，此窗格上的数据可能与实际值最多相差 15 分钟，因为数据会在此期间被缓存以优化性能。

步骤

1. 从NetApp控制台菜单中，查看存储容量窗格。
2. 在存储容量窗格中，选择“查看”转到“控制台系统”页面。
3. 在系统页面上，选择包含要查看的集群的项目。
4. 在系统页面上，选择一个集群以查看有关该集群的更多详细信息。

查看ONTAP警报

查看NetApp本地ONTAP环境中的问题或潜在风险。您可以看到一些非 EMS 警报和一些 EMS 警报。

数据每 5 分钟更新一次。

您可以看到具有以下严重程度的ONTAP警报：

- 批判的

- 警告
- 信息

您可以看到针对以下影响区域的ONTAP警报：

- 容量
- 性能
- 保护
- 可用性
- 安全性

缓存可优化性能，但可能会导致此窗格上的数据与实际值相差长达 15 分钟。

支持的系统

- 支持本地ONTAP NAS 或 SAN 系统。
- 不支持Cloud Volumes ONTAP系统。

支持的数据源

查看有关ONTAP中发生的某些事件的警报。它们是 EMS 和基于指标的警报的组合。

有关ONTAP警报的详细信息，请参阅 "关于ONTAP警报"。

有关您可能会看到的警报列表，请参阅 "查看ONTAP存储中的潜在风险"。

步骤

1. 从NetApp控制台菜单中，查看ONTAP警报窗格。
2. 或者，通过选择严重性级别来过滤警报，或者更改过滤器以根据影响区域显示警报。
3. 在ONTAP警报窗格中，选择“查看”以转到“控制台警报”页面。

查看存储性能容量

检查每个集群或Cloud Volumes ONTAP系统使用的存储性能容量，以确定性能容量、延迟和 IOPS 如何影响您的工作负载。例如，您可能会发现需要转移工作负载以最大限度地减少延迟并最大限度地提高关键工作负载的 IOPS 和吞吐量。

系统按性能容量排列集群和系统，首先列出最高容量，以便于识别。

缓存可优化性能，但可能会导致此窗格上的数据与实际值相差长达 15 分钟。

步骤

1. 从NetApp控制台菜单中，查看存储性能窗格。
2. 在存储性能窗格中，选择“查看”转到“性能”页面，该页面列出了所有集群和Cloud Volumes ONTAP系统的性能容量、IOPS 和延迟数据。

3. 选择一个集群以在系统管理器中查看其详细信息。

查看您拥有的许可证和订阅

查看许可证和订阅窗格中的以下信息：

- 您拥有的许可证和订阅的总数。
- 您拥有的每种许可证和订阅的数量（直接许可证、年度合同或 PAYGO）。
- 处于活动状态、需要操作或即将到期的许可证和订阅的数量。
- 系统会在需要采取行动或即将到期的许可证类型旁边显示指示符。

数据每 5 分钟刷新一次。

缓存可优化性能，但可能会导致此窗格上的数据与实际值相差长达 15 分钟。

步骤

1. 从NetApp控制台菜单中，查看许可证和订阅窗格。
2. 在许可证和订阅窗格中，选择“查看”以转到控制台许可证和订阅页面。

查看勒索软件抵御能力状态

了解工作负载是否面临勒索软件攻击的风险或是否受到NetApp勒索软件恢复数据服务的保护。您可以查看受保护的数据总量、查看建议的操作数量以及查看与勒索软件防护相关的警报数量。

数据每 5 分钟刷新一次，并与NetApp勒索软件恢复力仪表板中显示的数据相匹配。

"了解NetApp勒索软件恢复能力" 。

步骤

1. 从NetApp控制台菜单中，查看“勒索软件恢复力”窗格。
2. 在“勒索软件恢复”窗格中执行以下操作之一：
   - 选择“查看”转到NetApp勒索软件恢复力仪表板。有关详细信息，请参阅 "使用NetApp勒索软件恢复力仪表板监控工作负载健康状况"。
   - 查看NetApp勒索软件恢复力仪表板中的“推荐操作”。有关详细信息，请参阅 "查看NetApp勒索软件恢复力仪表板上的保护建议"。
   - 选择警报链接以查看NetApp勒索软件恢复警报页面中的警报。有关详细信息，请参阅 "使用NetApp勒索软件恢复功能处理检测到的勒索软件警报"。

查看备份和恢复状态

查看NetApp Backup and Recovery 的备份和恢复的总体状态。您可以看到受保护和不受保护的资源的数量。您还可以查看备份和恢复操作的百分比，以保护您的工作负载。百分比越高，表示数据保护越好。

数据每 5 分钟刷新一次。

缓存可优化性能，但可能会导致此窗格上的数据与实际值相差长达 15 分钟。

步骤

1. 从NetApp控制台菜单中，查看“备份和恢复”窗格。
2. 选择“查看”转到NetApp备份和恢复仪表板。有关详细信息，请参阅 "NetApp备份和恢复文档"。

管理您的NetApp控制台用户设置

您可以修改您的控制台配置文件，包括更改您的密码、启用多重身份验证 (MFA) 以及查看您的控制台管理员是谁。

在控制台中，每个用户都有一个配置文件，其中包含有关用户及其设置的信息。您可以查看和编辑您的个人资料设置。

更改您的显示名称

您可以更改用于识别您并且其他用户可见的控制台显示名称。您的显示名称与您的用户名或电子邮件地址不同，并且无法更改。

步骤

1. 选择控制台右上角的配置文件图标以查看用户设置面板。
2. 选择您姓名旁边的“编辑”图标。
3. 在“名称”字段中输入您的新显示名称。

配置多重身份验证

配置多重身份验证 (MFA)，通过要求第二种验证方法来提高安全性。

使用外部身份提供商或NetApp支持站点进行单点登录的用户无法启用 MFA。如果您遇到上述任一情况，您将不会在个人资料设置中看到启用 MFA 的选项。

如果您的用户帐户用于 API 访问，请不要启用 MFA。当为用户帐户启用多因素身份验证时，它会停止 API 访问。使用服务帐户进行所有 API 访问。

开始之前

- 您必须已将身份验证应用程序（例如 Google Authenticator 或 Microsoft Authenticator）下载到您的设备。
- 您需要密码来设置 MFA。

如果您无法访问身份验证应用程序或丢失恢复代码，请联系控制台管理员寻求帮助。

步骤

1. 选择控制台右上角的配置文件图标以查看用户设置面板。
2. 选择“多重身份验证”标题旁边的“配置”。
3. 按照提示为您的帐户设置 MFA。

4. 完成后，系统将提示您保存恢复代码。选择复制代码或下载包含代码的文本文件。请将此代码保存在安全的地方。如果您无法访问身份验证应用程序，则需要恢复代码。

   设置 MFA 后，控制台会在您每次登录时提示您输入来自身份验证应用程序的一次性代码。

重新生成您的 MFA 恢复代码

您只能使用一次恢复代码。如果您使用或丢失了您的，请创建一个新的。

步骤

1. 选择控制台右上角的配置文件图标以查看用户设置面板。
2. 选择 ••• 在“多重身份验证”标题旁边。
3. 选择*重新生成恢复代码*。
4. 复制生成的恢复代码并将其保存在安全的位置。

删除您的 MFA 配置

要停止使用多重身份验证 (MFA) 进行登录，请删除您的 MFA 配置。这样，您在登录时就无需输入身份验证应用程序中的一次性代码。

如果您无法访问您的身份验证应用程序或恢复代码，您将需要联系您的组织管理员来重置您的 MFA 配置。

步骤

1. 选择控制台右上角的配置文件图标以查看用户设置面板。
2. 选择 ••• 在“多重身份验证”标题旁边。
3. 选择*删除*。

联系您的组织管理员

如果您需要联系您的组织管理员，您可以直接从控制台向他们发送电子邮件。管理员管理组织内的用户帐户和权限。

您必须为浏览器配置默认电子邮件应用程序才能使用“联系管理员”功能。

步骤

1. 选择控制台右上角的配置文件图标以查看用户设置面板。
2. 选择“联系管理员”向您的组织管理员发送电子邮件。
3. 选择要使用的电子邮件应用程序。
4. 完成电子邮件并选择*发送*。

配置暗黑模式（暗黑主题）

您可以将控制台设置为以暗模式显示。

步骤

1. 选择控制台右上角的配置文件图标以查看用户设置面板。
2. 移动*黑暗主题*滑块以启用它。

管理NetApp控制台

身份和访问管理

了解NetApp控制台身份和访问管理

NetApp控制台中的身份和访问管理 (IAM) 使您能够组织和控制对NetApp资源的访问。您可以根据组织的层次结构来组织资源。例如，您可以按地理位置、站点或业务部门组织资源。然后，您可以将 IAM 角色分配给层次结构特定部分的成员，从而阻止访问层次结构其他部分的资源。

- "了解控制台部署模式"

IAM 的工作原理

IAM 允许您通过将用户访问角色分配给层次结构的特定部分来授予资源访问权限。例如，可以为成员分配具有五种资源的项目的文件夹或项目管理员角色。

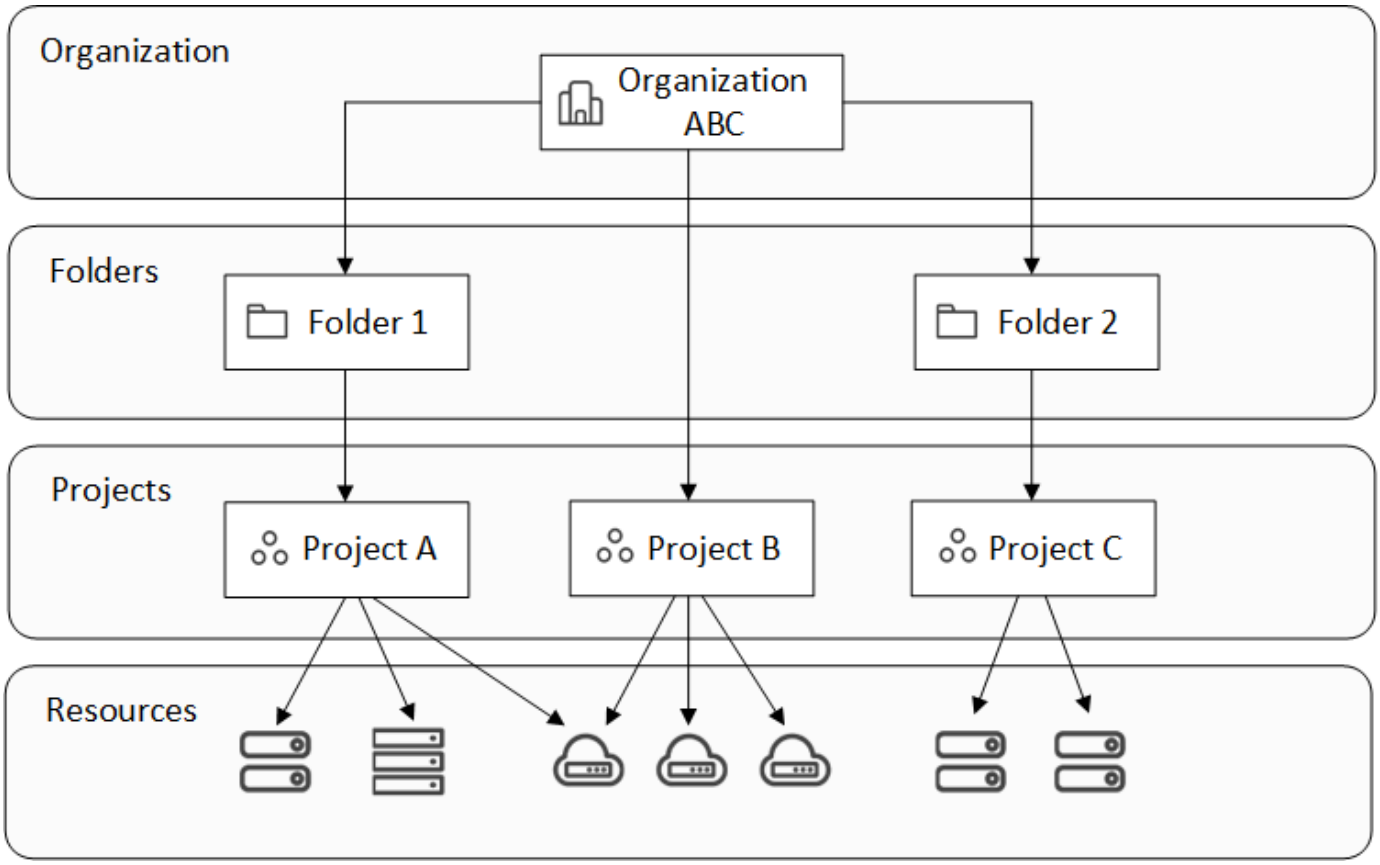
使用 IAM 时，您可以管理以下组件：

- 该组织
- 文件夹
- 项目
- 资源
- 成员
- 角色和权限
- 控制台代理

资源按层次结构组织：

- 该组织处于层级结构的顶端。
- 文件夹是组织或其他文件夹的子文件夹。
- 项目是组织或文件夹的子项。
- 资源与一个或多个文件夹或项目相关联。

下图从基本层面说明了这一层次结构。



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。

文件夹

_文件夹_使您能够将相关项目分组在一起，并将它们与组织中的其他项目分开。例如，文件夹可能代表地理位置（欧盟或美国东部）、站点（伦敦或多伦多）或业务部门（工程或营销）。

您可以组织文件夹以包含项目、其他文件夹或两者。它们是可选的。

项目

_项目_代表控制台中的一个工作区，组织成员可以从*系统*页面访问该工作区以管理资源。例如，一个项目可以包括一个Cloud Volumes ONTAP系统、一个本地ONTAP集群或一个 FSx for ONTAP文件系统。

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或文件夹内。

资源

_资源_是您在控制台中创建或发现的系统。

当您创建或发现资源时，该资源将与当前选定的项目相关联。这可能是您想要与该资源关联的唯一项目。但您可以选择将该资源与您组织中的其他项目相关联。

例如，您可以将Cloud Volumes ONTAP系统与另一个项目或组织中的所有项目关联。如何关联资源取决于您组织的需求。

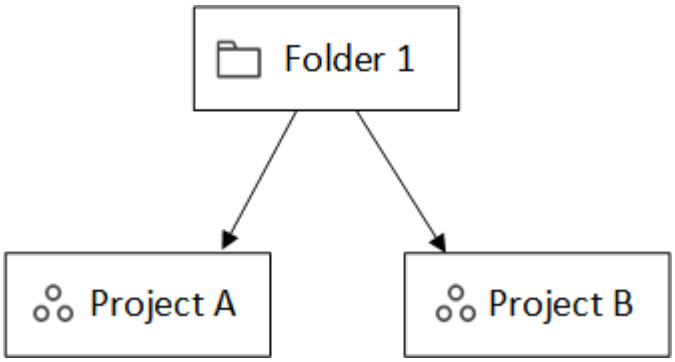
代理还可以与多个项目相关联。[了解有关使用代理与 IAM 的更多信息]。

何时将资源与文件夹关联

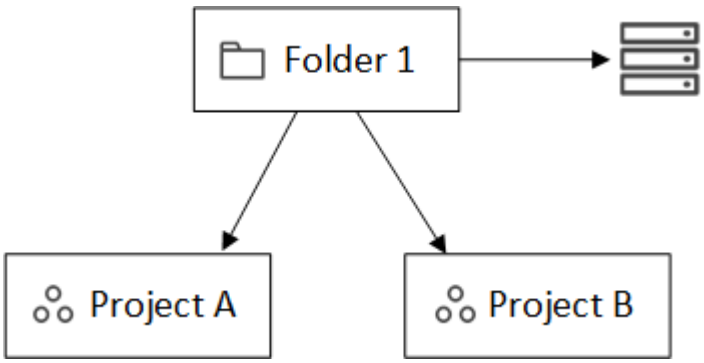
您还可以选择将资源与文件夹关联，但这是可选的，并且可以满足特定用例的需求。

_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：

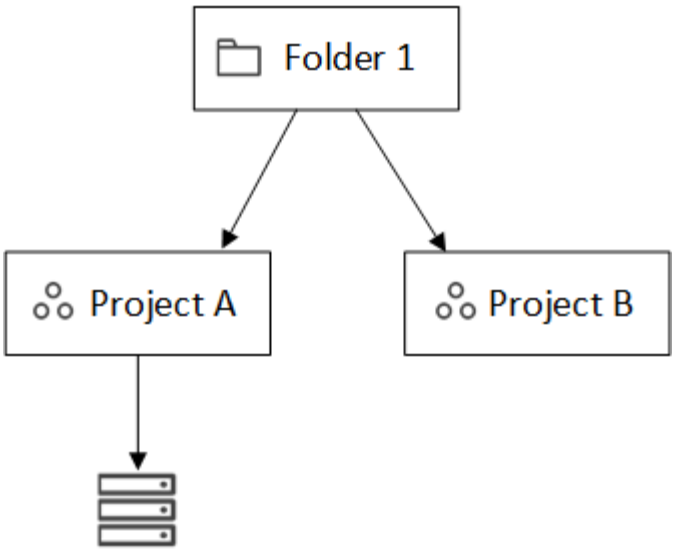


_组织管理员_可以将资源与文件夹关联：



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。

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。

每个组织至少包含一个具有“组织管理员”角色的用户（控制台会自动将此角色分配给创建该组织的用户）。您可以将其他成员添加到组织，并在资源层次结构的不同级别分配不同的权限。

角色和权限

您不能直接向组织成员授予权限。相反，您授予每个成员一个角色。角色包含一组权限，使成员能够在资源层次结构的特定级别执行特定操作。

在层次结构级别授予角色会限制成员对所需资源和服务的访问。

您可以在层次结构中分配角色

当您将成员与角色关联时，您需要选择整个组织、特定文件夹或特定项目。您选择的角色将授予成员对层次结构中选定部分中的资源的权限。

角色继承

当您分配角色时，该角色将在组织层次结构中继承：

组织

在组织级别授予成员访问角色将赋予他们访问所有文件夹、项目和资源的权限。

文件夹

当您在文件夹级别授予访问角色时，文件夹中的所有文件夹、项目和资源都会继承该角色。

例如，如果您在文件夹级别分配角色，并且该文件夹有三个项目，则该成员将对这三个项目和任何相关资源拥有权限。

项目

当您在项目级别授予访问角色时，与该项目相关的所有资源都会继承该角色。

多重角色

您可以为每个组织成员分配组织层次结构不同级别的角色。可以是相同的角色，也可以是不同的角色。例如，您可以为项目 1 和项目 2 分配成员角色 A。或者您可以为项目 1 分配成员角色 A，为项目 2 分配角色 B。

访问角色

控制台提供您可以分配给组织成员的访问角色。

"了解访问角色" 。

控制台代理

当“组织管理员”创建控制台代理时，控制台会自动将该代理与组织和当前选定的项目关联。 _组织管理员_可以从组织中的任何位置自动访问该代理。但是，如果您的组织中有具有不同角色的其他成员，则这些成员只能从创建该代理的项目访问该代理，除非您将该代理与其他项目关联。

在以下情况下，您可以为另一个项目提供控制台代理：

- 您希望允许组织中的成员使用现有代理来创建或发现另一个项目中的其他系统
- 您将现有资源与另一个项目关联，并且该资源由控制台代理管理

  如果使用控制台代理发现与其他项目关联的资源，那么您还需要将该代理与该资源现在关联的项目关联。否则，没有“组织管理员”角色的成员将无法从“系统”页面访问该代理及其关联资源。

您可以从控制台 IAM 中的“代理”页面创建关联：

- 将控制台代理与项目关联

  当您将控制台代理与项目关联时，可以在查看项目时从*系统*页面访问该代理。

- 将控制台代理与文件夹关联

  将控制台代理与文件夹关联并不会自动使文件夹中的所有项目都可以访问该代理。组织成员无法从项目访问控制台代理，除非您将代理与特定项目关联。

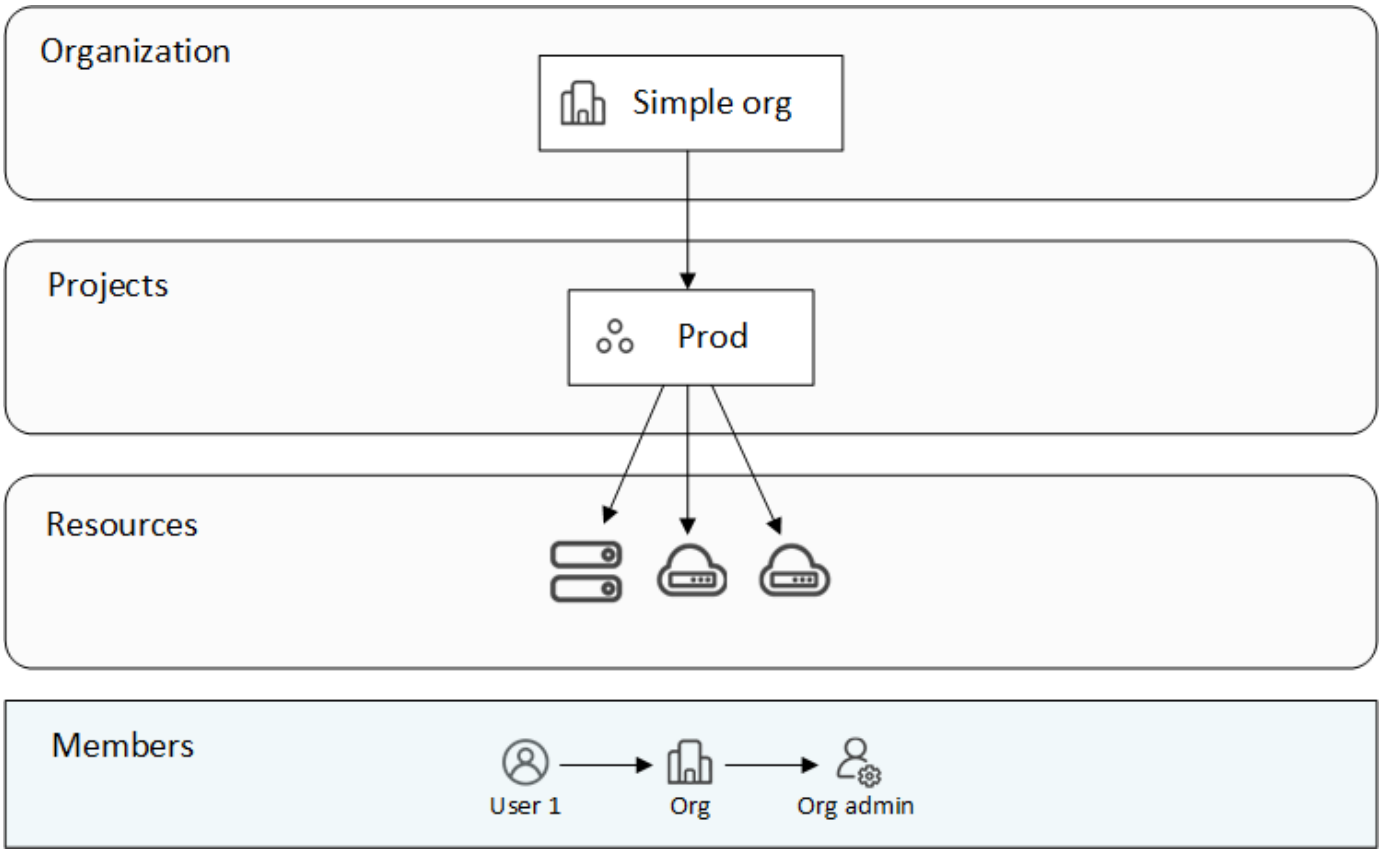
  _组织管理员_可能会将控制台代理与文件夹关联，以便_文件夹或项目管理员_可以决定将该代理与文件夹中的相应项目关联。

IAM 示例

这些示例演示了如何建立您的组织。

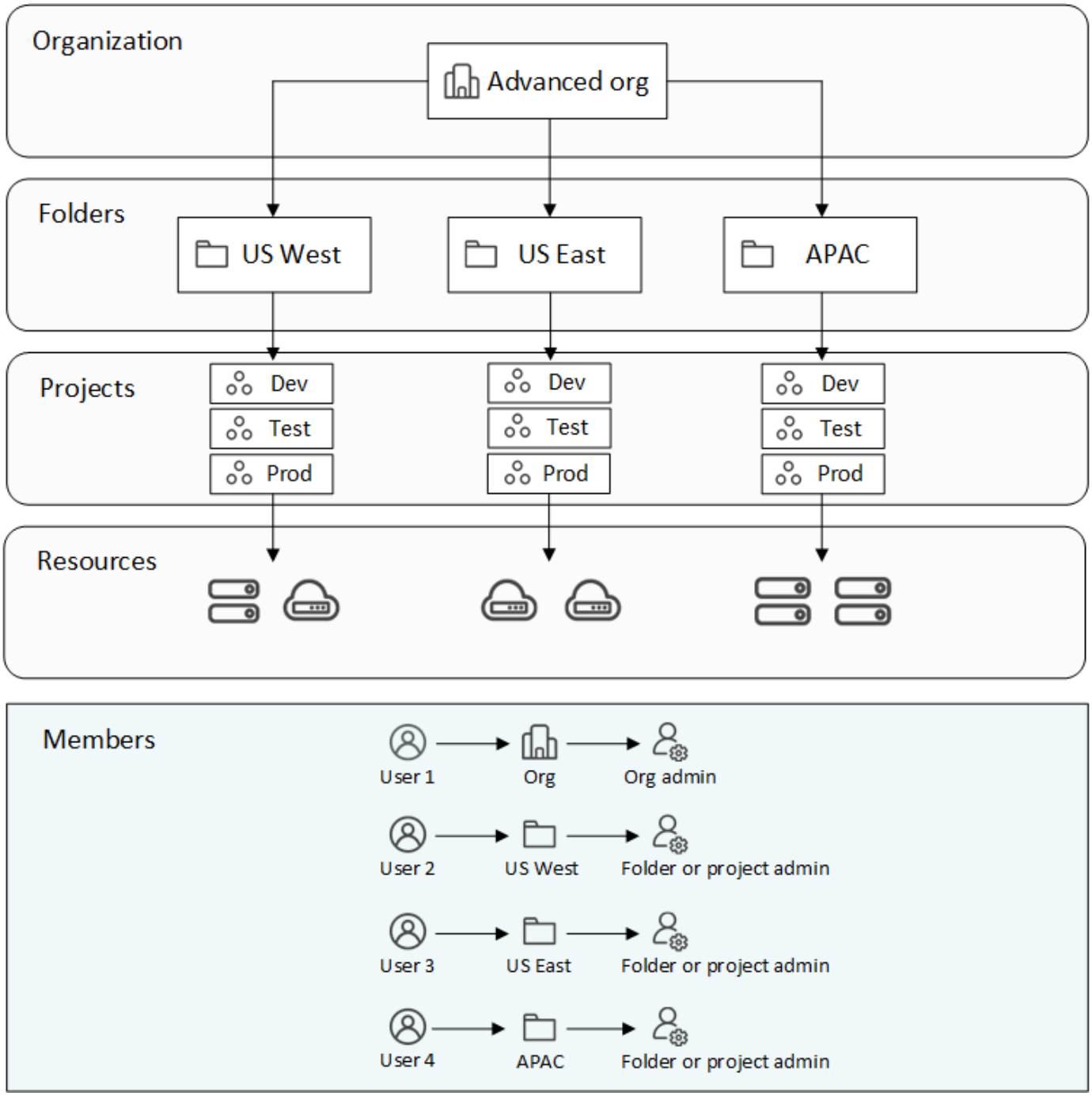
简单的组织

下图显示了使用默认项目且没有文件夹的组织的简单示例。一名成员管理整个组织。



先进组织

下图显示了一个组织使用文件夹来组织业务中每个地理位置的项目。每个项目都有自己的一套相关资源。成员包括组织管理员和组织中每个文件夹的管理员。



IAM 的功能

以下示例描述了如何使用 IAM 来管理控制台组织：

- 授予特定成员特定角色，以便他们只能完成所需的任务。
- 由于成员调动部门或承担额外责任而修改成员权限。
- 删除已离开公司的用户。
- 将文件夹或项目添加到您的层次结构中，因为新的业务部门已添加NetApp存储。
- 将资源与另一个项目关联起来，因为该资源具有另一个团队可以利用的能力。
- 查看成员可以访问的资源。

- 查看与特定项目相关的成员和资源。

下一步

- "开始使用NetApp控制台中的 IAM"
- "使用文件夹和项目在NetApp控制台中组织您的资源"
- "管理NetApp控制台成员及其权限"
- "管理NetApp控制台组织中的资源层次结构"
- "将代理与文件夹和项目关联"
- "在NetApp控制台项目和组织之间切换"
- "重命名您的NetApp控制台组织"
- "监控或审计 IAM 活动"
- "NetApp控制台访问角色"
- "了解NetApp Console IAM 的 API"

开始在**NetApp**控制台中使用身份和访问权限

当您注册NetApp控制台时，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。

您必须拥有*组织管理员*权限才能管理整个组织的身份和访问权限。如果您具有*文件夹或项目管理员*权限，则您只能管理您有权限的文件夹和项目。

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" 。


将成员与您的组织关联

将用户帐户链接到您的组织并分配权限。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" 。


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控制台中的身份和访问管理"
- "了解身份和访问 API"

使用文件夹和项目组织您的NetApp控制台资源

在NetApp控制台中，您可以使用项目和文件夹来组织您的NetApp资源。 项目_代表控制台中的一个工作区，组织成员可以访问该工作区来管理_资源（例如， Cloud Volumes ONTAP系统）。 _文件夹_将相关项目分组在一起。将资源组织到文件夹和项目中后，您可以通过向组织成员提供特定文件夹和项目的权限来授予对资源的细粒度访问权限。

添加文件夹或项目

当您创建组织时，它包含一个项目。添加项目来管理资源和文件夹来对相关项目进行分组。

您的组织的资源层次结构最多可以有七个级别，其中文件夹嵌套六级，项目位于第七级。

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. 提供有关文件夹或项目的详细信息：
    - 名称和位置：输入名称并选择文件夹或项目的层次结构中的位置。文件夹或项目可以直接位于组织下或文件夹内。
    - 资源：选择您想要与此文件夹或项目关联的资源。

      您可以选择与父文件夹或项目相关的资源。

"了解何时将资源与文件夹关联" 。

- 访问：根据资源层次结构中已定义的现有权限，查看有权访问文件夹或项目的成员。

  选择*添加成员*为其他成员分配访问权限和角色。角色定义成员对文件夹或项目的权限。

"了解访问角色" 。

6. 选择“添加”。

重命名文件夹或项目

如果需要，您可以更改文件夹和项目的名称。

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。

开始之前

- 确保文件夹或项目没有关联资源。了解如何解除资源关联 。
- 确保文件夹或项目没有关联资源。

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。

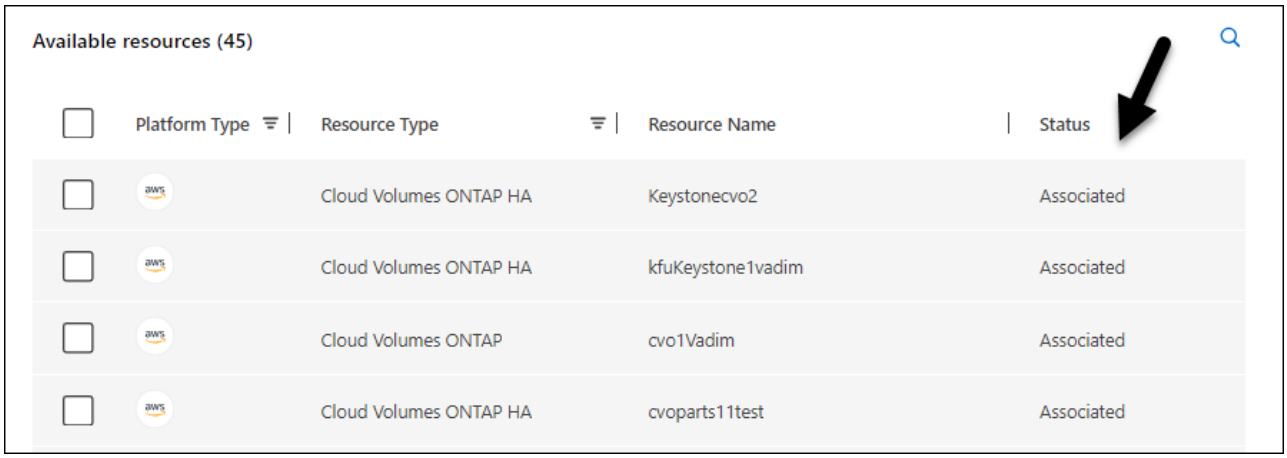
查看与文件夹或项目关联的资源

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。



修改与文件夹或项目关联的资源

拥有文件夹或项目权限的成员可以访问其相关资源。

开始之前

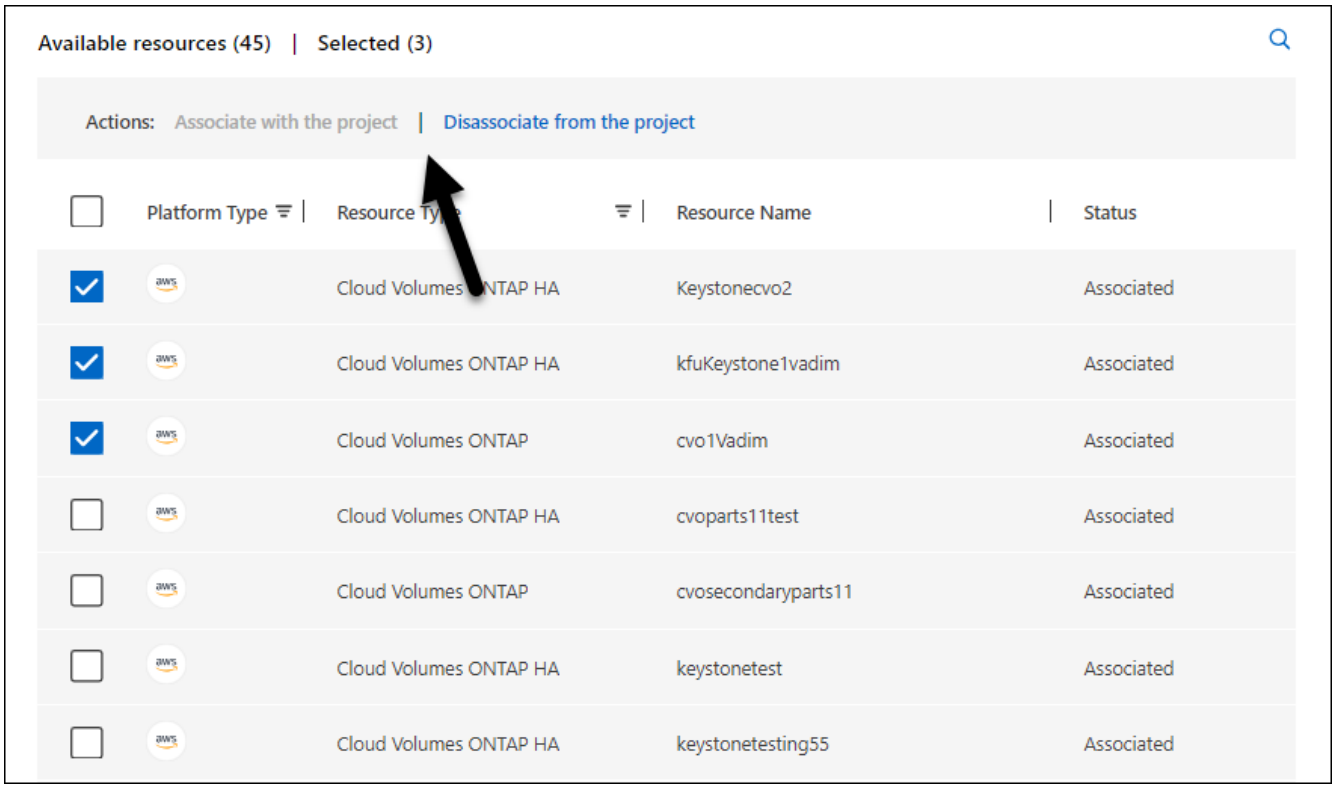
"了解何时将资源与文件夹关联" 。

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，选择*资源*。

   在表中，“状态”列标识与文件夹或项目相关的资源。

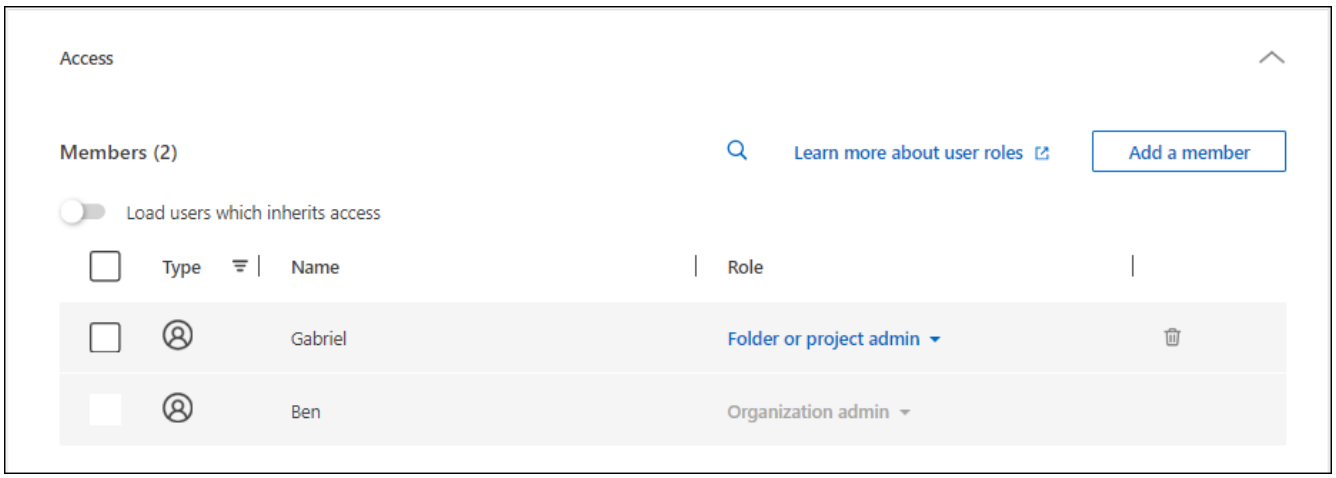
3. 选择您想要关联或取消关联的资源。
4. 根据您选择的资源，选择*与项目关联*或*与项目取消关联*。



5. 选择“应用”

查看与文件夹或项目关联的成员

- 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确保正确的成员可以访问相关资源。

较高层次结构级别提供的成员访问权限不能在较低级别更改。更新更高层次结构级别的成员权限以更改访问权限。或者，您可以"从“会员”页面管理权限"。

"了解有关角色继承的详细信息" 。

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控制台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"

将成员和服务帐户添加到NetApp控制台

在控制台中，您可以将用户和服务帐户添加到您的组织，并在资源层次结构中为他们分配一个或多个角色。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特定级别执行特定操作。

您需要以下角色之一来管理用户和权限：

- 组织管理员

  具有此角色的用户可以管理所有成员

- 文件夹或项目管理员

  具有此角色的用户只能管理指定文件夹或项目的成员

  _文件夹或项目管理员_可以在*成员*页面上查看所有成员，但只能管理他们有权访问的文件夹和项目的权限。"详细了解文件夹或项目管理员可以完成的操作" 。

向您的组织添加成员

您可以向您的组织添加两种类型的成员：用户帐户和服务帐户。应用程序使用服务帐户来执行 API 任务，无需人工干预。人们通常使用用户帐户来登录和管理资源。

用户必须先注册NetApp控制台，然后您才能将他们添加到组织或为他们分配角色。您可以直接从控制台创建服务帐户。

要管理用户及其权限，您必须具有*组织管理员*角色或*文件夹或项目管理员*角色。请记住，具有“文件夹或项目管理员”角色的用户只能管理他们具有管理员权限的文件夹或项目的成员。

添加用户帐户

尽管用户可以自行注册NetApp控制台，但他们需要明确添加到组织或特定文件夹或项目才能访问控制台中的资源。

步骤

1. 引导用户访问 "NetApp控制台"进行注册。

   用户注册后，他们会完成*注册*页面，检查电子邮件并登录。如果控制台提示用户创建组织，他们会关闭它并通知您他们的帐户已创建。然后，您可以将该用户添加到您现有的组织。

   "了解如何注册NetApp控制台" 。

2. 选择*管理>身份和访问*。
3. 选择*成员*。
4. 选择*添加成员*。
5. 对于*会员类型*，保持选择*用户*。
6. 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。
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*，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" 。

9. 可选：选择其他角色或项目。如果您想提供对组织内其他文件夹或项目的访问权限，或授予用户在所选区域中的其他角色，请选择*添加角色*，指定另一个文件夹或项目或其他角色类别，然后选择一个角色。
10. 选择“添加”。

    控制台向用户发送一封包含说明的电子邮件。

添加服务帐户

您可以使用服务帐户自动执行任务并与控制台 API 安全地集成。创建服务帐户时，请在两种身份验证方法之间进行选择：使用客户端 ID 和密钥，或使用 JWT（JSON Web 令牌）身份验证。客户端 ID 和秘密方法适合简单设置，而 JWT 身份验证为自动化或云原生环境提供更强的安全性。选择最适合您的安全需求以及您计划如何使用控制台的选项。

如果您想使用 JWT 身份验证，请准备好您的公钥或证书。

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. 如果您想使用 JWT 身份验证，请选择 使用私钥 **JWT** 身份验证 并上传您的公共 RSA 密钥或证书。如果您想使用客户端 ID 和密钥，请跳过此步骤。

   您的 X.509 证书。它必须是 PEM、CRT 或 CER 格式。

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*，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" 。

9. 可选：选择其他角色或项目。如果您想提供对组织内其他文件夹或项目的访问权限，或授予用户在所选区域中的其他角色，请选择*添加角色*，指定另一个文件夹或项目或其他角色类别，然后选择一个角色。
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。 + 控制台仅显示一次客户端密钥。安全地复制它；如果需要，您可以稍后重新创建它。
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。此信息仅显示一次，之后无法检索。
12. 选择*关闭*。

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。"

您可以从“成员”页面查看用户帐户和服务帐户。

您还可以查看与特定文件夹或项目相关的所有成员。"了解更多" 。

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*。

从您的组织中移除成员

您可能需要从您的组织中删除某个成员 - 例如，如果他们离开了您的公司。

系统将删除该成员的权限，但保留其控制台和NetApp支持站点帐户。

步骤

1. 从“成员”页面，导航到表中的成员，选择 ••• 然后选择*删除用户*。
2. 确认您要从组织中删除该成员。

重新创建服务帐户的凭据

如果您丢失了凭证或需要更新凭证，请创建新的凭证。

重新创建凭据时，您将删除服务帐户的现有凭据并创建新的凭据。您不能使用以前的凭据。

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。 + 客户端密钥仅显示一次。复制或下载并安全存储。

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。

删除后，用户必须在登录时重新配置 MFA。如果用户只是暂时无法访问其 MFA 设备，他们可以使用设置 MFA 时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。

使用角色管理用户对**NetApp**控制台资源的访问

在控制台中，您可以根据用户需要做什么以及在哪里为用户分配角色。

具有*组织管理员*或*文件夹或项目管理员*角色的用户有责任将角色分配给其他用户。您可以根据项目或文件夹分配访问角色。例如，您可以为用户分配一个项目的勒索软件保护管理员角色，并为另一个项目分配SnapCenter管理员角色。或者，如果用户需要特定文件夹内所有项目的分类管理员角色，您可以在文件夹级别授予他们此角色。

使用访问角色根据用户需要执行的特定任务分配对存储资源的访问权限。例如，如果用户需要与勒索软件保护服务进行交互，则必须为他们授予访问角色，该角色包括对授予该访问角色的项目的勒索软件保护服务的查看或管理权限。

根据您的 IAM 策略为用户分配角色以增强安全性。 IAM 角色确保用户只拥有他们需要的访问权限。

请记住，您不能直接授予对资源的访问权限。首先将资源分配给项目。在分配用户访问权限之前，请考虑设置资源层次结构。"了解如何使用文件夹和项目来组织您的资源。"

查看分配给成员的角色

当您向组织添加成员时，系统会提示您为其分配角色。您可以向成员验证他们当前分配了哪些角色。

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. 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*。
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”。

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以及不同的项目中拥有多个角色。例如，较小的组织可能会将所有可用的访问角色分配给同一个用户，而较大的组织可能会让用户执行更专业的任务。或者，您也可以为一个用户分配组织的勒索软件保护管理员角色。在该示例中，用户将能够对组织内的所有项目执行勒索软件保护任务。

您的访问角色策略应与您组织NetApp资源的方式保持一致。

被分配了组织管理员角色的成员不能被分配任何其他角色。他们已经拥有整个组织的权限。具有文件夹或项目角色的成员不能被分配文件夹或项目中他们已经具有该角色的任何其他角色。这两个角色都提供对其被分配范围内的所有服务的访问权限。

步骤

1. 选择*管理>身份和访问*。
2. 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”。
3. 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。

4. 选择*添加新角色*。

更改成员的指定角色

如果您需要调整用户的访问权限，您可以更改成员分配的角色。

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. 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*。
3. 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。
4. 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 取消为该成员分配相应的角色。系统会要求您确认删除。

管理NetApp控制台组织中的资源层次结构

当您将成员与您的组织关联时，您会在组织、文件夹或项目级别提供权限。为了确保这些成员有权访问正确的资源，您需要通过将资源与特定项目和文件夹关联来管理组织的资源层次结构。 _资源_是控制台已经管理或知道的存储系统或控制台代理。

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。未发现的资源是已识别但尚未添加到控制台的存储资源。

注意：资源页面不包括Amazon FSx for NetApp ONTAP资源，因为用户无法将它们与角色关联。在系统页面或工作负载中查看它们。

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. 使用任何可用选项来查找您正在寻找的资源：
   - 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

将资源与文件夹或项目关联以使其可用。

开始之前

您应该了解资源关联是如何工作的。"了解资源，包括何时将资源与文件夹关联" 。

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

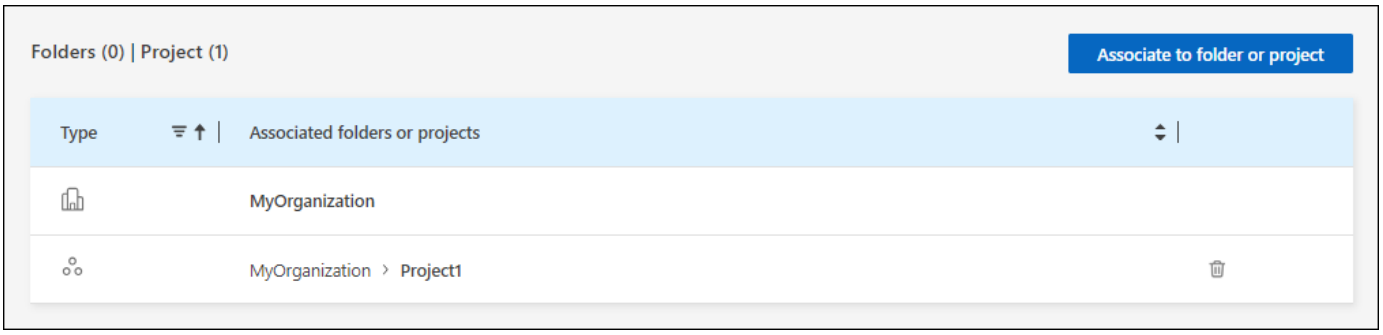
您可以查看与特定资源关联的文件夹和项目。

> 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。



如果您需要确定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"。

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，您需要删除文件夹或项目与资源之间的关联。当您删除关联时，它会阻止成员管理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，请从“系统”页面中删除该系统。

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. 对于要删除资源的文件夹或项目，选择 🗑
3. 通过选择“删除”确认您要删除关联。

相关信息

- "了解NetApp控制台中的身份和访问权限"
- "开始在NetApp控制台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

当“组织管理员”创建控制台代理时，该控制台代理会自动与组织内当前选定的项目相关联。尽管具有“组织管理员”角色的人可以从组织中的任何地方访问该控制台代理。除非您将该控制台代理与其他项目关联，否则您组织中的其他成员只能从创建该控制台代理的项目访问该控制台代理。

开始之前

回顾控制台代理关联的工作原理。"了解如何将控制台代理与身份和访问结合使用" 。

关于此任务

文件夹或项目管理员可以在代理页面上查看所有控制台代理，但只能将控制台代理与他们有权限的文件夹和项目关联。"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控制台代理"
- "了解NetApp控制台身份和访问管理"
- "开始使用身份和访问权限"
- "了解身份和访问管理的 API"

在控制台组织、项目和代理之间切换

您可能属于多个控制台组织，或者有权访问组织内的多个项目或代理。需要时，您可以轻松地在组织、项目和控制台代理之间切换，以访问与该组织、项目或代理相关的资源。

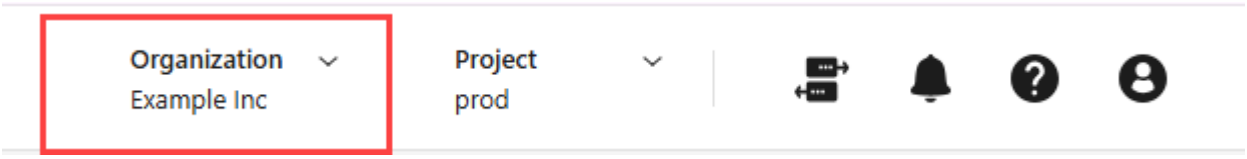
如果其他组织邀请您加入或者您自己创建一个组织，那么您可能属于多个组织。您可以使用 API 创建其他组织。 "了解如何创建新组织"

在组织之间切换

如果您是多个组织的成员，您可以随时在它们之间切换。

步骤

1. 在控制台的顶部标题中，选择*组织*。



2. 如果您有任何合作组织，请选择“合作伙伴关系”选项卡来查看可用的合作伙伴组织。

+ 如果您没有任何合作伙伴组织，则不会显示“合作伙伴关系”选项卡。

1. 选择另一个组织，然后选择*切换*。

+ 如果您有任何合作组织，请选择“合作伙伴关系”选项卡来查看可用的合作伙伴组织。

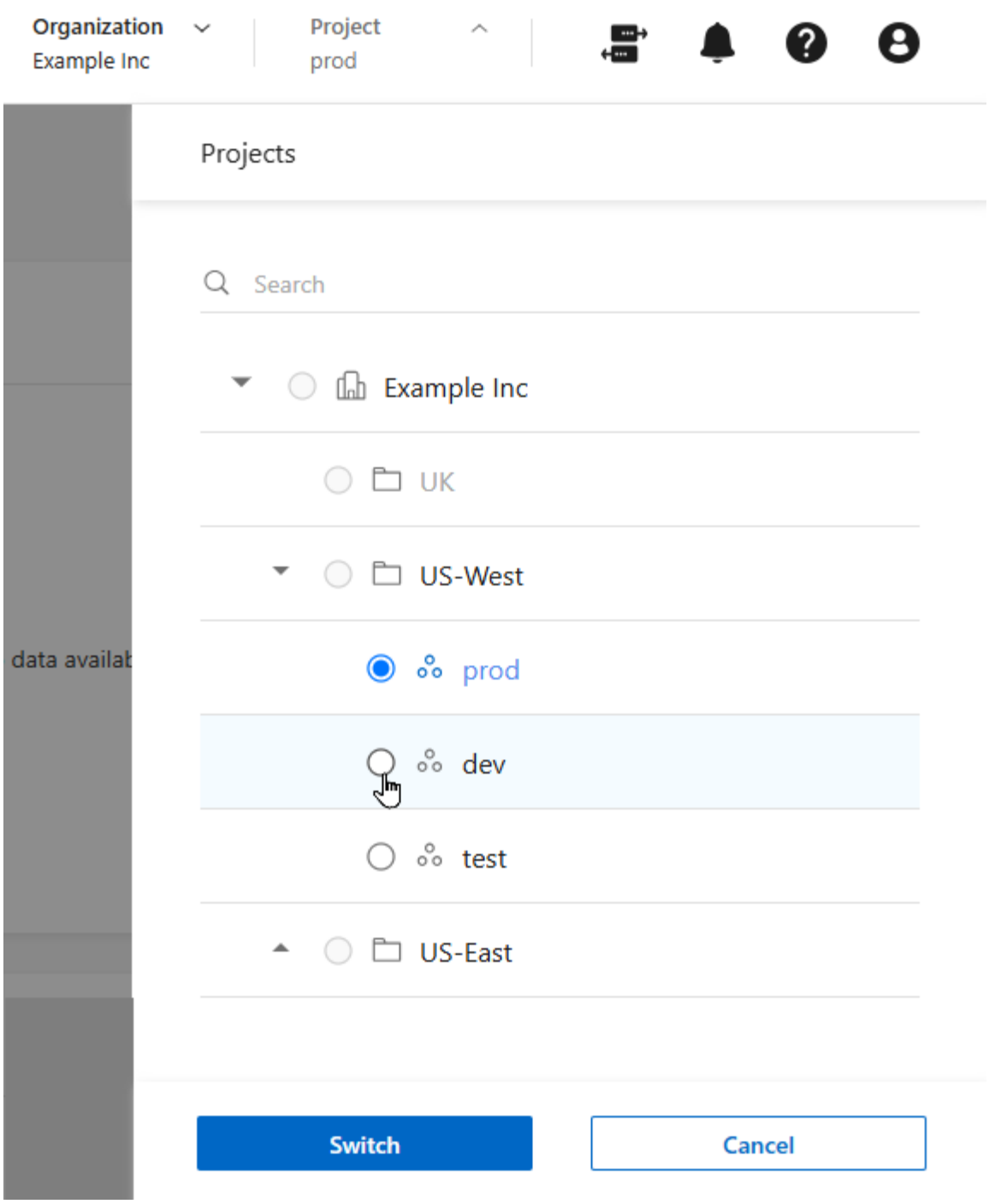
在项目之间切换

如果您的组织包含多个项目并且您有权访问这些项目，则您可以随时在它们之间切换。

在查看任何*身份和访问*页面时，您无法切换到另一个项目。

步骤

1. 在控制台的顶部标题中，选择*项目*。
2. 浏览您组织中的文件夹和项目，选择您想要的项目，然后选择*切换*。



在控制台代理之间切换

如果您有多个控制台代理，您可以在它们之间切换以查看与特定代理关联的系统。

步骤

1. 在控制台的顶部标题中，选择代理图标。
2. 选择另一个代理，然后选择*切换*。

相关信息

"将代理与文件夹和项目关联" 。

相关信息

- "了解NetApp控制台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"

组织和项目 ID

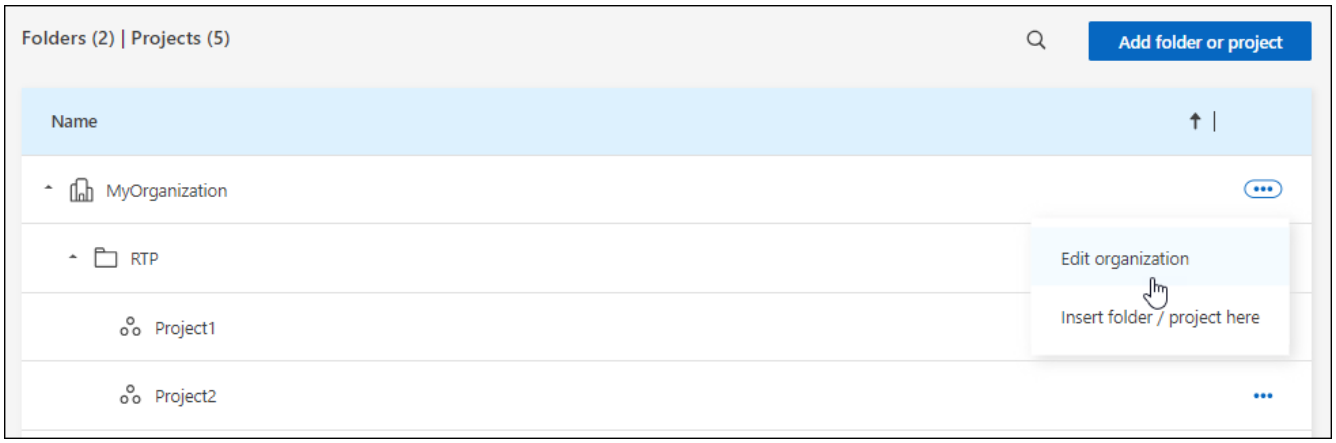
您的NetApp控制台组织有一个名称和一个 ID。您可以为您的组织选择一个名称以帮助识别它。您可能还需要检索某些集成的组织 ID。

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

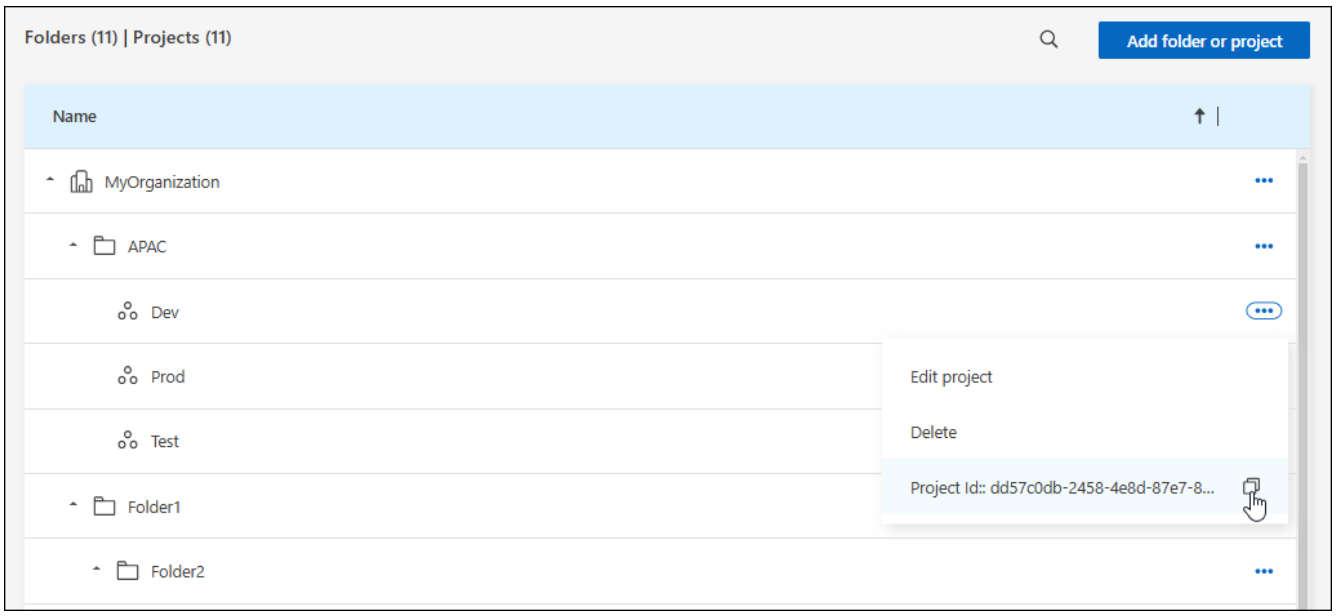
如果您使用 API，则需要获取项目的 ID。例如，创建Cloud Volumes ONTAP系统时。

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"

监控或审计 IAM 活动

如果您需要监控或审计与身份和访问相关的已完成的操作，您可以从审计页面查看详细信息。例如，您可能想要验证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. 在*审计*页面上，使用过滤器缩小结果范围。选择*服务*，然后选择*租赁*。
3. 使用任何其他过滤器来更改表中显示的操作。

   例如，您可以使用*用户*过滤器来显示与特定用户帐户相关的操作。

NetApp控制台访问角色

了解NetApp控制台访问角色

NetApp控制台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控制台管理权限，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。
"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"。

应用程序角色	职责
"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。
"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灾难恢复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数据分类扫描结果。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。分类没有查看者角色。
"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控制台服务SnapCenter没有查看者角色。

相关链接

- "了解NetApp控制台身份和访问管理"
- "开始使用NetApp Console IAM"

- "管理NetApp控制台成员及其权限"
- "了解NetApp Console IAM 的 API"

NetApp控制台平台访问角色

为用户分配平台角色，以授予管理NetApp控制台、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
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控制台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控制台中的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控制台中的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 。

NetApp控制台中的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控制台中的**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	否
管理警报	是	否
为自己创建提醒	是	是
许可证和订阅：		
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控制台的运营支持分析师访问角色

您可以为用户分配以下角色，以便他们访问警报和监控。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
是	查看审核页面和通知
是	查看、下载和配置警报

NetApp控制台的存储访问角色

您可以为用户分配以下角色，以便他们访问NetApp控制台中的存储管理功能。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控制台合作伙伴 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控制台中的存储角色示例

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
许可证和订阅			
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控制台中的**NetApp**备份和恢复角色

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备份和恢复中执行任何操作。
- 备份和恢复备份管理员：在NetApp备份和恢复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备份和恢复恢复工作负载。
- 备份和恢复克隆管理：使用NetApp备份和恢复克隆应用程序和数据。
- 备份和恢复查看器：查看NetApp备份和恢复中的信息，但不执行任何操作。

有关所有NetApp控制台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备份和恢复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备份和恢复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备份和恢复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控制台中的**NetApp**灾难恢复角色

您可以为用户分配以下角色，以便他们访问控制台内的NetApp灾难恢复。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控制台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勒索软件恢复的访问权限。这两个角色分别是勒索软件保护管理员和勒索软件保护查看者。这两个角色的主要区别在于他们在勒索软件恢复中可以采取的行动。

下表显示了每个角色可以执行的操作。

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	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
查看仪表板和所有选项卡	是	是	否	否
在仪表板上更新推荐状态	是	否	否	否
开始免费试用	是	否	否	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	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
启动工作负载发现	是	否	否	否
启动工作负载的重新发现	是	否	否	否
在“保护”选项卡上：				
添加、修改或删除保护计划	是	否	否	否
保护工作负载	是	否	否	否
识别敏感数据的暴露	是	否	否	否
列出保护计划和细节	是	是	否	否
列出保护组	是	是	否	否
查看保护组详细信息	是	是	否	否
创建、编辑或删除保护组	是	否	否	否
下载数据	是	是	否	否
在“警报”选项卡上：				
查看警报和警报详细信息	是	是	否	否
编辑事件状态	是	否	否	否
标记恢复警报	是	否	否	否
查看事件详细信息	是	是	否	否
解除或解决事件	是	否	否	否
阻止用户	是	否	否	否
获取受影响文件的完整列表	是	否	否	否
下载警报数据	是	是	否	否
查看可疑用户活动	否	否	是	是

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	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“恢复”选项卡上：				
下载受影响的文件	是	否	否	否
恢复工作负载	是	否	否	否
下载恢复数据	是	是	否	否
下载报告	是	是	否	否
在“设置”选项卡上：				
添加或修改备份目标	是	否	否	否
列出备份目的地	是	是	否	否
查看已连接的 SIEM 目标	是	是	否	否
添加或修改 SIEM 目标	是	否	否	否
配置准备演练	是	否	否	否
开始准备演习	是	否	否	否
重置准备演习	是	否	否	否
编辑准备演习	是	否	否	否
审查准备演习状态	是	是	否	否
更新发现配置	是	否	否	否
查看发现配置	是	是	否	否
配置可疑用户行为设置	否	否	是	否
在“报告”选项卡上：				
下载报告	是	是	否	否

合作组织

NetApp控制台中的合作伙伴关系

通过在组织之间建立合作伙伴关系， NetApp控制台可让合作伙伴跨组织边界安全地管理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。

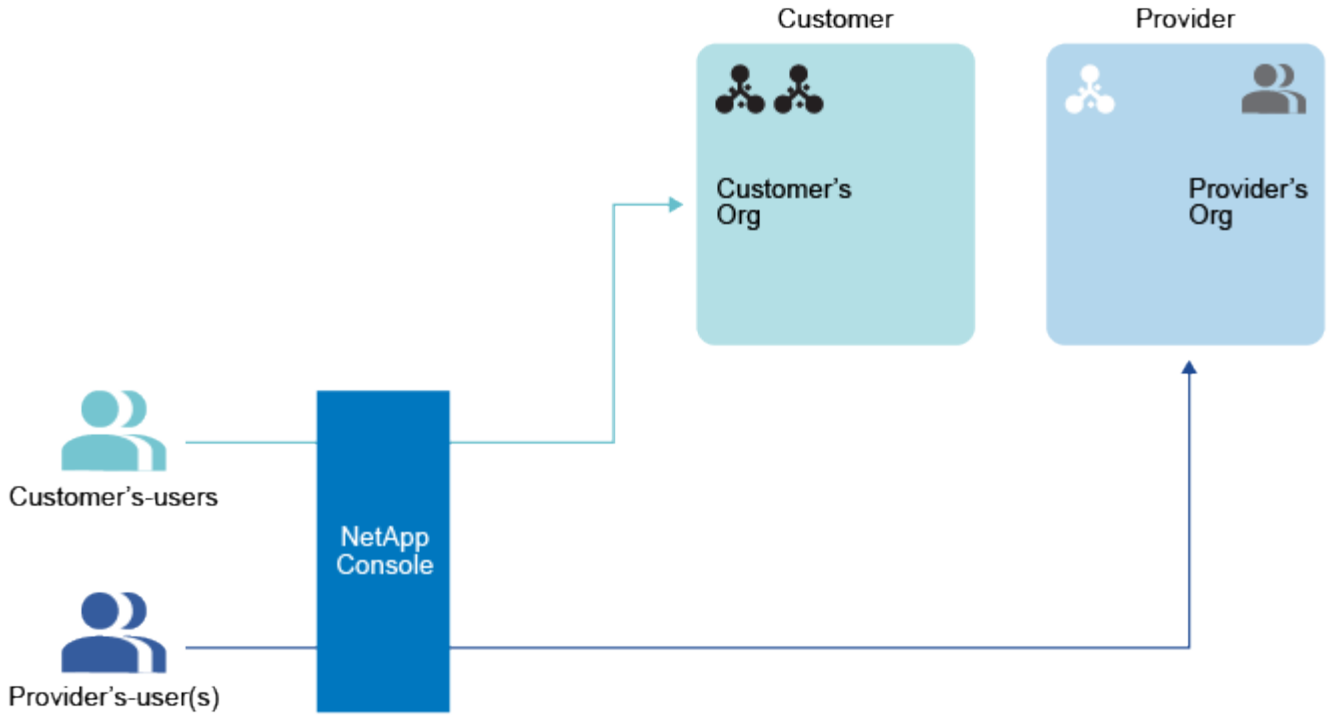
1. 为一个或多个用户分配合作伙伴管理员角色

为发起组织和接收组织中的一个或多个用户分配合作伙伴管理员角色来创建和管理合作伙伴关系。您可以将合作伙伴查看器角色分配给只需要查看合作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**

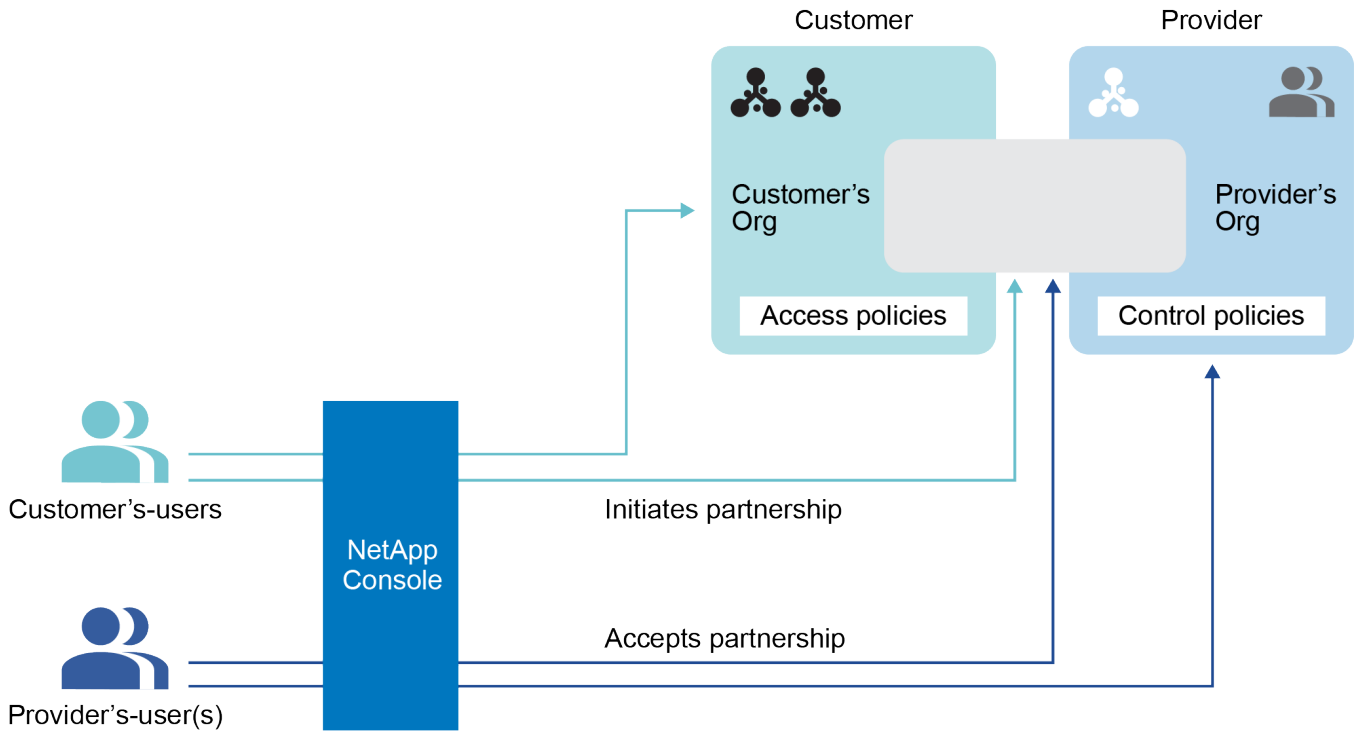
要发起合作关系，发起者必须知道目标组织的组织 ID。只有相应的组织可以访问此组织 ID。通过电子邮件或其他方式直接与NetApp控制台之外的发起组织共享。

发起组织是授予其资源访问权限的组织。



3 在**NetApp**控制台内建立合作关系

发起合作关系的组织通过从NetApp控制台发送合作关系请求来发起合作关系。



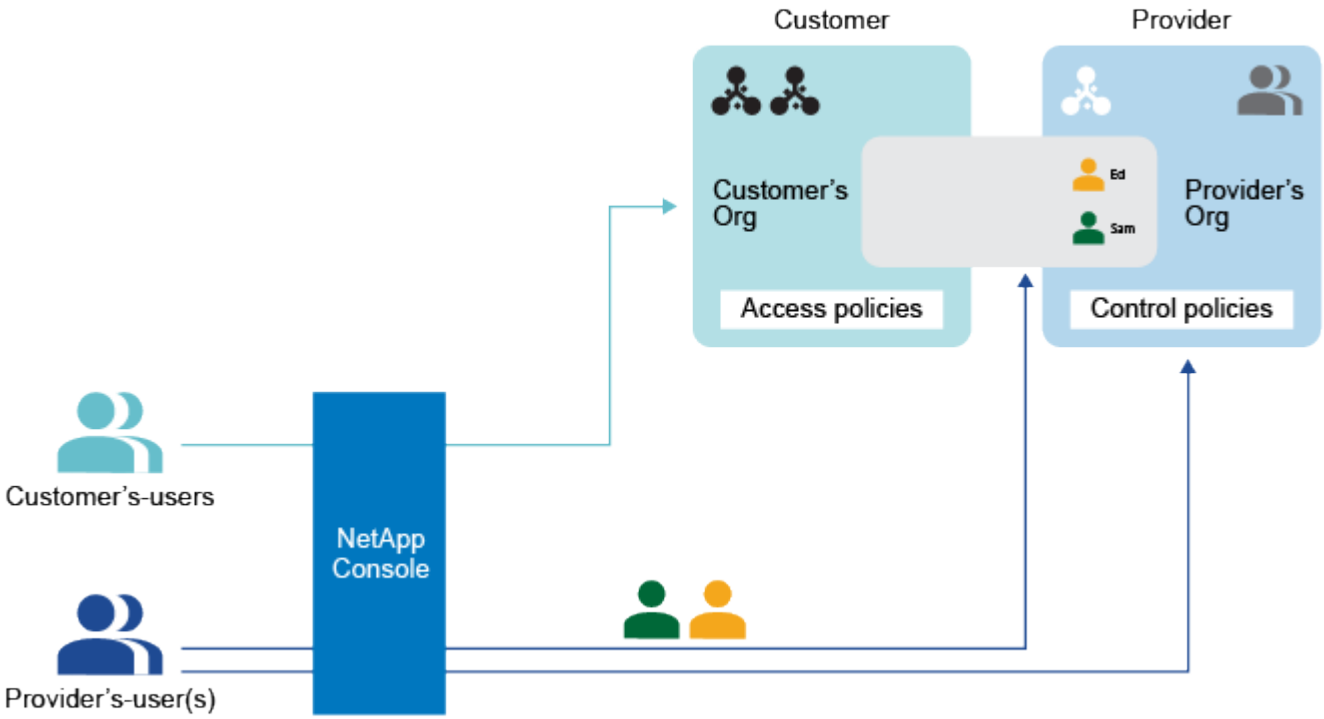
4 批准合作

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

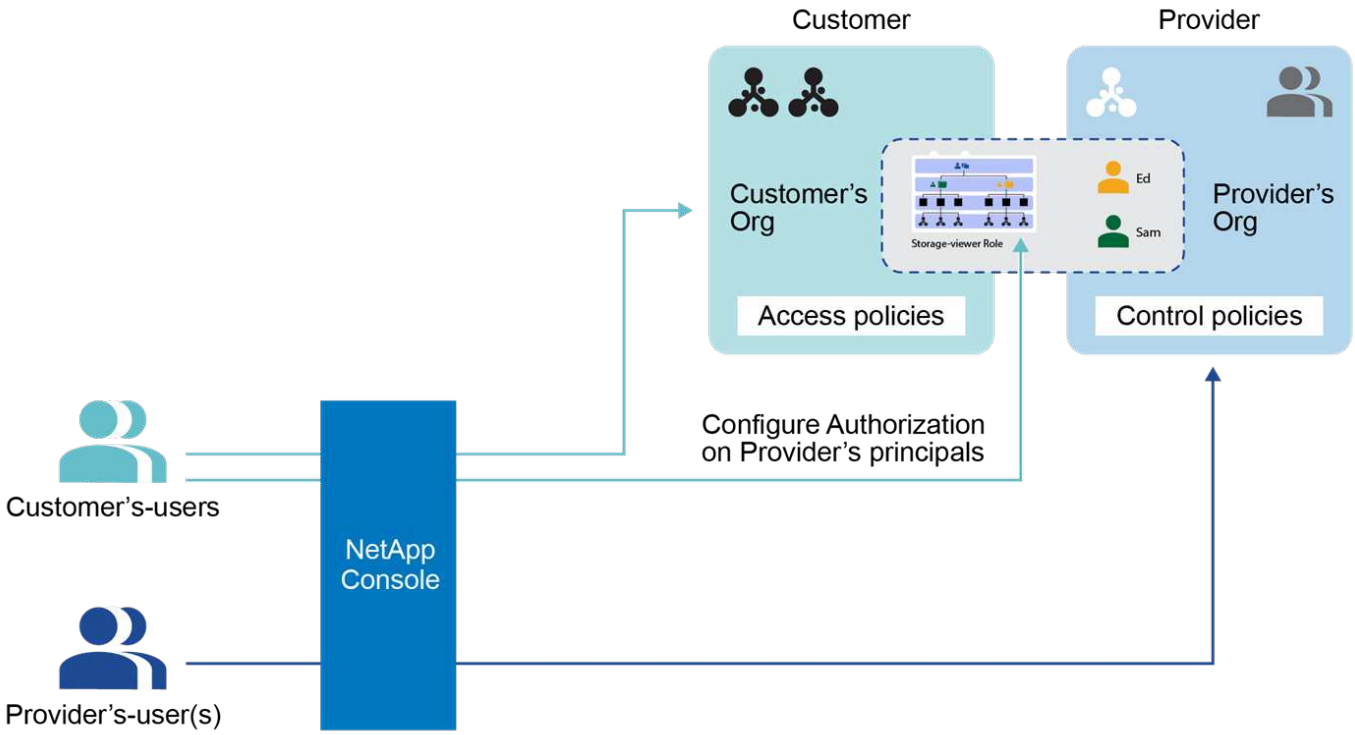
接收组织将您组织中的特定用户或服务帐户分配给合作伙伴关系。发起组织为这些用户分配角色。



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控制台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 🗑 取消为该成员分配相应的角色。系统会要求您确认删除。

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。

身份联合

使用NetApp控制台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控制台，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。"

与NetApp支持站点的身份联合

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。

与您的身份提供商建立联合连接

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**控制台联合工作流程

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。

1 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。

2 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。

3 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。

4 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。

5 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控制台信任该域进行联合。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**控制台与 **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控制台联合起来，以便为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控制台作为服务提供者。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控制台的单点登录 (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控制台中创建连接。

开始之前

- 需要具有管理权限的 IdP 帐户。与您的 IdP 管理员协调以完成这些步骤。
- 确定要用于联合的域。您可以使用您的电子邮件域名或您拥有的其他域名。如果您想使用电子邮件域以外的域，则必须首先在控制台中验证该域。您可以按照以下步骤操作"在NetApp控制台中验证您的域"话题。

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控制台值：
      - 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控制台自动检索最新的 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控制台中手动更新它。

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 IdP 凭据登录以完成测试并返回控制台以启用连接。
14. 选择“下一步”。
15. 在“启用联合”页面上，查看联合详细信息，然后选择“启用联合”。
16. 选择“完成”以完成该过程。

启用联合后，用户可以使用其公司凭据登录NetApp控制台。

将**NetApp**控制台与 **Microsoft Entra ID** 联合起来

与您的 Microsoft Entra ID 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。

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。

开始之前

- 需要具有管理权限的 IdP 帐户。与您的 IdP 管理员协调以完成这些步骤。
- 确定要用于联合的域。您可以使用您的电子邮件域名或您拥有的其他域名。如果您想使用电子邮件域以外的域，则必须首先在控制台中验证该域。您可以按照以下步骤操作"在NetApp控制台中验证您的域"话题。

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 IdP 凭据登录以完成测试并返回控制台以启用连接。
3. 选择“下一步”。
4. 在“启用联合”页面上，查看联合详细信息，然后选择“启用联合”。
5. 选择“完成”以完成该过程。

启用联合后，用户可以使用其公司凭据登录NetApp控制台。

使用 **PingFederate** 联合**NetApp**控制台

与您的 PingFederate 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。

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。

开始之前

- 需要具有管理权限的 IdP 帐户。与您的 IdP 管理员协调以完成这些步骤。
- 确定要用于联合的域。您可以使用您的电子邮件域名或您拥有的其他域名。如果您想使用电子邮件域以外的域，则必须首先在控制台中验证该域。您可以按照以下步骤操作"在NetApp控制台中验证您的域"话题。

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控制台时，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 IdP 凭据登录以完成测试并返回控制台以启用连接。
14. 选择“下一步”。
15. 在“启用联合”页面上，查看联合详细信息，然后选择“启用联合”。
16. 选择“完成”以完成该过程。

启用联合后，用户可以使用其公司凭据登录NetApp控制台。

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。

开始之前

- 需要具有管理权限的 IdP 帐户。与您的 IdP 管理员协调以完成这些步骤。
- 确定要用于联合的域。您可以使用您的电子邮件域名或您拥有的其他域名。如果您想使用电子邮件域以外的域，则必须首先在控制台中验证该域。您可以按照以下步骤操作"在NetApp控制台中验证您的域"话题。

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>
```

   b. 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`。
   c. 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）
   d. 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。
9. 返回控制台，然后选择“下一步”来创建连接。
10. 使用 SAML 创建连接。
    a. 输入您的 SAML 服务器的 登录 **URL**。
    b. 上传从 SAML 提供商服务器下载的 X.509 证书。
    c. 或者，输入您的 SAML 服务器的 退出 **URL**。

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 IdP 凭据登录以完成测试并返回控制台以启用连接。
14. 选择“下一步”。
15. 在“启用联合”页面上，查看联合详细信息，然后选择“启用联合”。
16. 选择“完成”以完成该过程。

启用联合后，用户可以使用其公司凭据登录NetApp控制台。

在NetApp控制台中管理联合

您可以在NetApp控制台中管理您的联合。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。

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"

您还可以将已验证的域添加到现有联合中，这允许您使用多个域进行联合连接。

联合管理事件（例如启用、禁用和更新联合）显示在时间轴中。"了解有关在NetApp控制台中监控操作的更多信息。"

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。"

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，如果证书或客户端密钥等凭证过期，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控制台。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**控制台

如果您之前已通过NetApp Cloud Central（ NetApp控制台的外部应用程序）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*。

控制台代理

维护控制台代理虚拟机和操作系统

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代理主机上的操作系统应用安全更新。

如果您有现成的代理，您应该注意"受支持的 Linux 操作系统的变更"。

操作系统补丁和代理

无需停止代理主机服务即可应用操作系统安全补丁。

VM 或实例类型

如果您从控制台创建控制台代理，它会使用默认配置在您的云提供商中部署 VM 实例。创建代理后，不要切换到具有较少 CPU 或 RAM 的较小 VM 实例。

下表列出了 CPU 和 RAM 要求：

CPU

8 个核心或 8 个 vCPU

RAM

32 GB

"了解代理的默认配置" 。

监控代理

当代理虚拟机不健康时，控制台会通知您，包括磁盘空间、RAM 和 CPU 问题。在控制台内的通知中心监控这些通知或配置电子邮件通知。磁盘空间、内存或 CPU 使用率偶尔增加是正常现象，但如果经常发生，则应采取措施解决。

例如，当代理资源（CPU、RAM 或磁盘空间）连续 30 分钟超过其总容量的 90% 时，控制台会通知您。之后，如果资源使用率低于该阈值，则通知中心将显示通知已解决（绿色）。

如果您对修改代理 VM 有任何疑问，请联系NetApp支持。

"了解更多信息。"

通知	需要采取行动
磁盘空间过高	"查看NetApp知识库文章" 。
CPU 使用率过高	根据安装位置，增加云提供商或本地代理 VM 的 CPU 大小。或者，创建额外的代理并将工作负载分配给多个代理。 RAM 利用率可能因您的环境、 ONTAP工作负载、 Cloud Volumes ONTAP系统的数量以及您正在使用的数据服务而异。
RAM 使用率过高	根据安装位置，增加云提供商或本地代理虚拟机的 RAM。或者，创建额外的代理并将工作负载分配给多个代理。 RAM 利用率可能因您的环境、 ONTAP工作负载、 Cloud Volumes ONTAP系统的数量以及您正在使用的数据服务而异。

停止和启动代理虚拟机

如果需要，请使用云提供商的控制台或标准内部部署程序停止并启动代理虚拟机。

"请注意，控制台代理必须始终处于运行状态" 。

连接到 **Linux VM**

如果您需要连接到代理运行的 Linux VM，请使用云提供商提供的连接选项。

AWS

在 AWS 中创建代理实例时，请提供 AWS 访问密钥和密钥。您可以使用此密钥对通过 SSH 连接到实例。对 EC2 Linux 实例使用用户名“ubuntu”。对于 2023 年 5 月之前创建的代理，请使用用户名“ec2-user”。

"AWS 文档：连接到您的 Linux 实例"

Azure

在 Azure 中创建代理 VM 时，您可以指定用户名并选择使用密码或 SSH 公钥进行身份验证。使用您选择的身份验证方法连接到虚拟机。

"Azure 文档：通过 SSH 进入您的 VM"

Google Cloud

在 Google Cloud 中创建代理时，您无法指定身份验证方法。但是，您可以使用 Google Cloud Console 或 Google Cloud CLI (gcloud) 连接到 Linux VM 实例。

"Google Cloud Docs：连接到 Linux 虚拟机"

更改代理的 IP 地址

如果需要，您可以更改云提供商分配的代理实例的内部和公共 IP 地址。

步骤

1. 按照云提供商的说明更改代理实例的本地 IP 地址或公共 IP 地址（或两者）。
2. 重新启动代理实例以向控制台注册新的公共 IP 地址。
3. 如果您更改了私有 IP 地址，请更新Cloud Volumes ONTAP配置文件的备份位置，以便将备份发送到代理上的新私有 IP 地址。

   更新每个Cloud Volumes ONTAP系统的备份位置。

   a. 从Cloud Volumes ONTAP CLI，将权限级别设置为高级：

   ```
   set -privilege advanced
   ```

   b. 运行以下命令显示当前备份目标：

   ```
   system configuration backup settings show
   ```

   c. 运行以下命令来更新备份目标的 IP 地址：

   ```
   system configuration backup settings modify -destination <target-
   location>
   ```

编辑代理的 **URI**

您可以添加和删除代理的统一资源标识符 (URI)。

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*代理 URI* 栏以查看代理 URI。
4. 添加和删除 URI，然后选择*应用*。

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 之间的数字以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控制台时，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*。

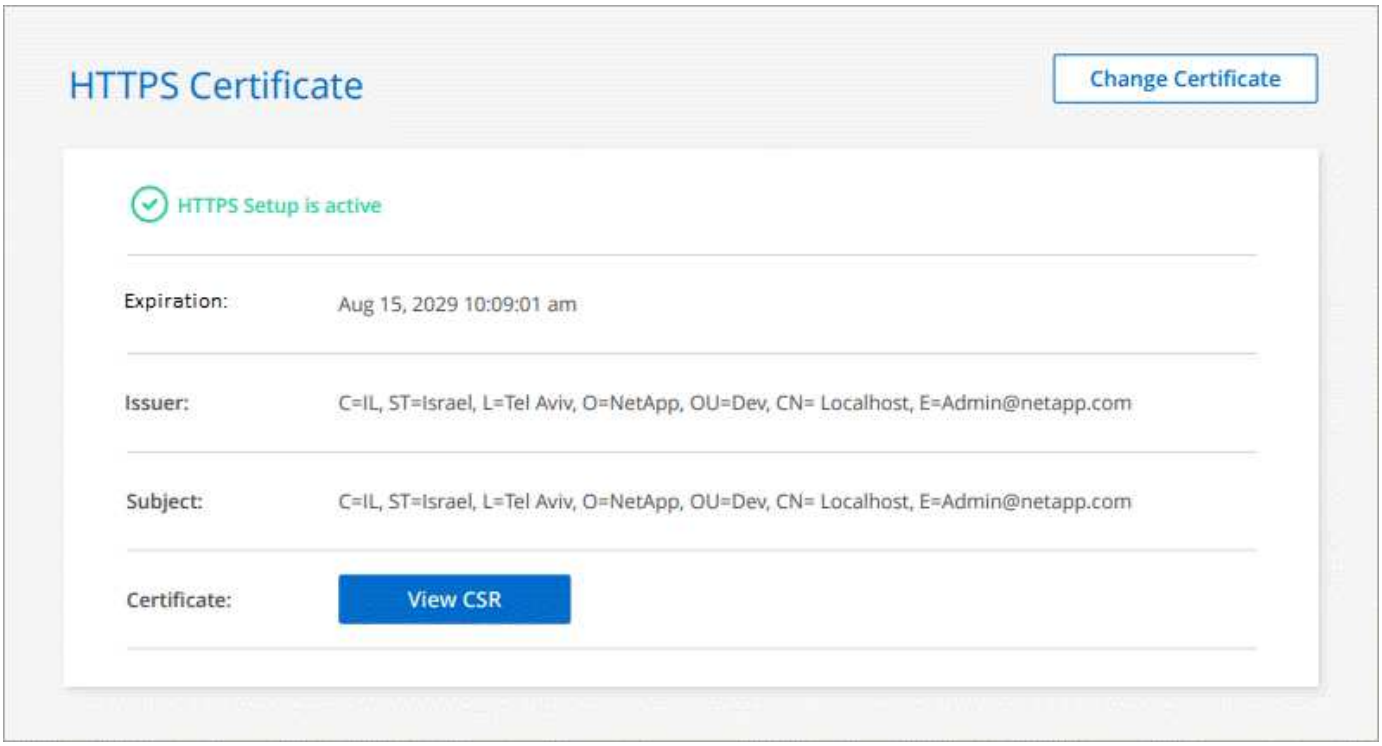
   控制台代理必须处于活动状态才能对其进行编辑。

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。

要将现有代理配置为使用透明代理服务器，请使用可通过控制台代理主机上的命令行获取的控制台代理维护工具。

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 `proxy update`命令或使用 `proxy remove`命令。有关详细信息，请参阅"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，以便将 API 调用直接发送到云提供商服务，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*。

要求在 **Amazon EC2** 实例上使用 **IMDSv2**

NetApp控制台通过控制台代理和Cloud Volumes ONTAP （包括 HA 部署的中介）支持 Amazon EC2 实例元数据服务版本 2 (IMDSv2)。大多数情况下，IMDSv2 会在新的 EC2 实例上自动配置。 IMDSv1 于 2024 年 3 月之前启用。如果您的安全策略需要，您可能需要在 EC2 实例上手动配置 IMDSv2。

开始之前

- 控制台代理版本必须为 3.9.38 或更高版本。
- Cloud Volumes ONTAP必须运行以下版本之一：
  - 9.12.1 P2（或任何后续补丁）
  - 9.13.0 P4（或任何后续补丁）
  - 9.13.1 或此版本之后的任何版本
- 此更改要求您重新启动Cloud Volumes ONTAP实例。
- 这些步骤需要使用 AWS CLI，因为您必须将响应跳数限制更改为 3。

关于此任务

IMDSv2 提供了增强的针对漏洞的保护。 "从 AWS 安全博客了解有关 IMDSv2 的更多信息"

实例元数据服务 (IMDS) 在 EC2 实例上启用如下：

- 对于从控制台或使用 "Terraform 脚本"，IMDSv2 在 EC2 实例上默认启用。
- 如果您在 AWS 中启动新的 EC2 实例，然后手动安装控制台代理软件，则 IMDSv2 也会默认启用。
- 如果您从 AWS Marketplace 启动控制台代理，则默认启用 IMDSv1。您可以在 EC2 实例上手动配置 IMDSv2。
- 对于现有的控制台代理，仍然支持 IMDSv1，但如果您愿意，可以在 EC2 实例上手动配置 IMDSv2。
- 对于Cloud Volumes ONTAP，IMDSv1 在新实例和现有实例上默认启用。如果愿意，您可以在 EC2 实例上手动配置 IMDSv2。

步骤

1. 要求在控制台代理实例上使用 IMDSv2：

   a. 连接到控制台代理的 Linux VM。

      当您在 AWS 中创建控制台代理实例时，您提供了 AWS 访问密钥和密钥。您可以使用此密钥对通过 SSH 连接到实例。 EC2 Linux 实例的用户名是 ubuntu（对于 2023 年 5 月之前创建的控制台代理，用户名是 ec2-user）。

      "AWS 文档：连接到您的 Linux 实例"

   b. 安装 AWS CLI。

      "AWS 文档：安装或更新到最新版本的 AWS CLI"

   c. 使用 `aws ec2 modify-instance-metadata-options`命令要求使用 IMDSv2 并将 PUT 响应跳数限制更改为 3。

      例子

      ```
      aws ec2 modify-instance-metadata-options \
          --instance-id <instance-id> \
          --http-put-response-hop-limit 3 \
          --http-tokens required \
          --http-endpoint enabled
      ```

      这 `http-tokens`参数将 IMDSv2 设置为必需。什么时候 `http-tokens`是必需的，您还必须设置 `http-endpoint`启用。

2. 要求在Cloud Volumes ONTAP实例上使用 IMDSv2：

   a. 前往 "Amazon EC2 控制台"

   b. 从导航窗格中，选择*实例*。

   c. 选择一个Cloud Volumes ONTAP实例。

   d. 选择*操作>实例设置>修改实例元数据选项*。

   e. 在“修改实例元数据选项”对话框中，选择以下内容：

      - 对于*实例元数据服务*，选择*启用*。
      - 对于 **IMDSv2**，选择 必需。
      - 选择*保存*。

   f. 对其他Cloud Volumes ONTAP实例（包括 HA 中介）重复这些步骤。

   g. "停止并启动Cloud Volumes ONTAP实例"

结果

控制台代理实例和Cloud Volumes ONTAP实例现已配置为使用 IMDSv2。

管理控制台代理升级

当您使用标准模式或受限模式时，只要控制台代理具有出站互联网访问权限以获取软件更新， NetApp控制台就会自动将您的控制台代理升级到最新版本。

如果您需要手动管理控制台代理的升级时间，您可以禁用标准模式或受限模式的自动升级。

禁用自动升级

禁用控制台代理的自动升级包括两个步骤。首先，您需要确保您的控制台代理健康且是最新的。然后编辑配置文件以关闭自动升级。

仅当您拥有控制台代理版本 3.9.48 或更高版本时，您才可以禁用自动升级。

验证代理的健康状况

您应该验证您的代理是否稳定，以及代理虚拟机上运行的所有容器是否健康且正在运行。禁用自动升级后，代理虚拟机将停止检查新服务或升级包。

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，请在禁用自动升级之前联系NetApp支持。

Docker（用于 **Ubuntu** 和 **VCenter** 部署）

```
docker ps -a
```

Podman

```
podman ps -a
```

禁用代理的自动升级

您可以通过在 *com/opt/application/netapp/service-manager-2/config.json* 文件中设置 *isUpgradeDisabled* 标志来禁用自动升级。默认情况下，此标志设置为 false，并且您的代理会自动升级。您可以将此标志设置为 true 以禁用自动升级。在完成此步骤之前，您应该熟悉 JSON 语法。

要重新启用自动升级，请使用以下步骤并将 *isUpgradeDisabled* 标志设置为 false。

步骤

1. 确保您已验证您的代理是最新的并且健康。
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. 编辑 */opt/application/netapp/service-manager-2/config.json* 文件并将 *isUpgradeDisabled* 标志的值更改为 true。

```
  "isUpgradeDisabled": true,
```

4. 保存您的文件。
5. 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
```

6. 运行以下命令并验证代理的状态是否显示为_active(running)：

```
systemctl status netapp-service-manager.service
—
```

升级控制台代理

控制台代理需要在升级过程中重新启动，因此NetApp控制台在升级期间将不可用。

步骤

1. 从下载控制台代理软件 "NetApp 支持站点"。
2. 将安装程序复制到 Linux 主机。
3. 分配运行脚本的权限。

```
chmod +x /path/NetApp-Console-Agent-Offline-<version>
```

其中 <version> 是您下载的控制台代理的版本。

4. 运行安装脚本：

```
sudo /path/NetApp-Console-Agent-Offline-<version>
```

其中 <version> 是您下载的代理的版本。

5. 升级完成后，您可以前往*管理>支持>代理*来验证代理的版本。

使用多个控制台代理

如果您使用多个控制台代理，则可以直接从控制台在这些控制台代理之间切换以查看相关系统。

在控制台代理之间切换

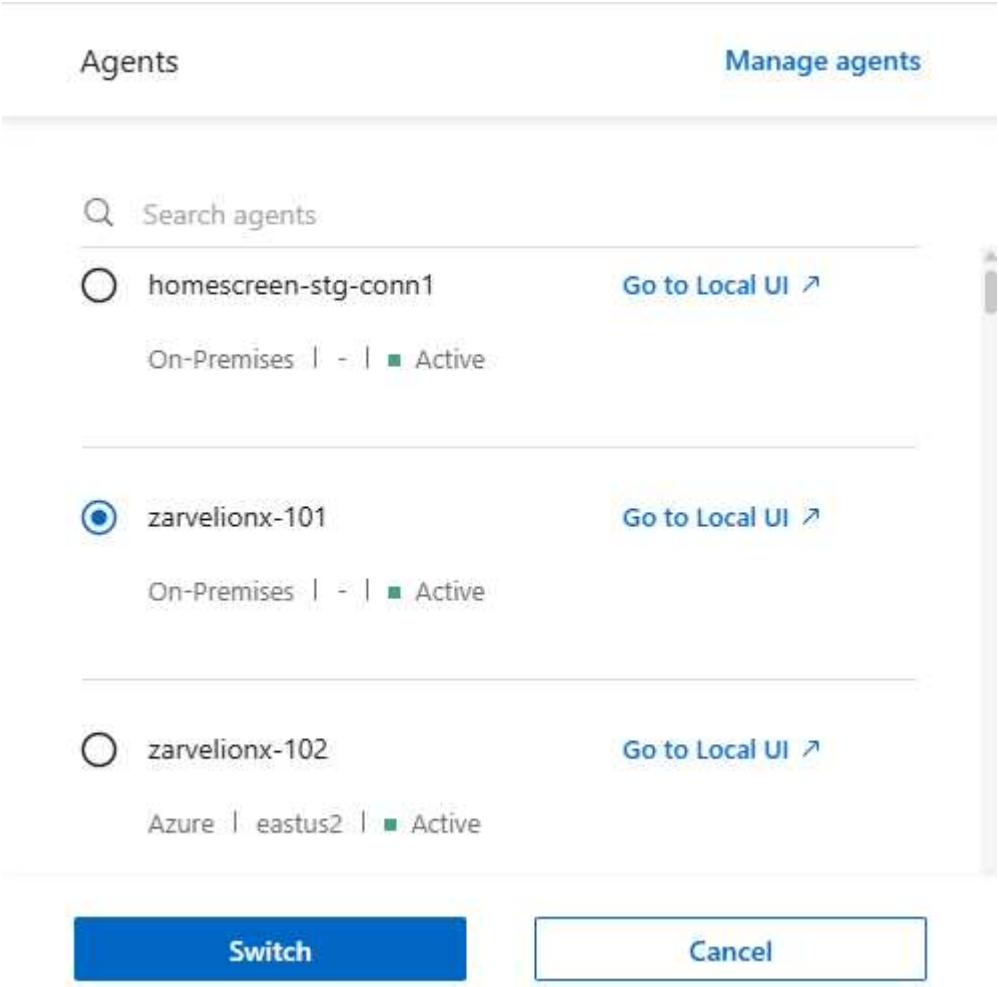
如果您有多个控制台代理，您可以在它们之间切换以查看与特定代理关联的系统。

例如，在多云环境中，您可能在 AWS 中有一个代理，在 Google Cloud 中有一个代理。在这些代理之间切换以管理各自云环境中的Cloud Volumes ONTAP系统。

从代理的本地 UI 查看NetApp控制台时，此选项不可用

步骤

1. 选择控制台代理图标 ( ) 查看可用代理的列表。



结果

控制台刷新并显示与所选代理关联的系统。

设置灾难恢复配置

您可以同时使用多个控制台代理来管理系统，以实现灾难恢复。如果一个控制台代理出现故障，您可以切换到另一个代理来立即管理系统。

步骤

1. 切换到您想要使用控制台代理管理的其他控制台代理。
2. 发现现有系统。
   - "将现有的Cloud Volumes ONTAP系统添加到控制台"
   - "发现ONTAP集群"

3. 如果您正在管理Cloud Volumes ONTAP系统，请将容量管理模式调整为*手动模式*。

   为了避免争用问题，只有主控制台代理应设置为*自动模式*。

   "了解有关容量管理模式的更多信息"

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

下表列出了常见的错误信息及其解决建议：

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。 • 如果问题仍然存在，请联系支持人员。
无法访问NetApp代理 UI	尝试访问代理的 IP 地址时会出现此消息。如果代理没有正确的网络访问权限或不稳定，则代理可能无法初始化。	• 连接到控制台代理。 • 验证 Service Manager 服务 • 验证代理是否具有所需的网络访问权限。"了解有关所需网络访问端点的更多信息。"
无法加载代理设置	当您尝试访问代理设置页面时，控制台会显示此消息。	• 检查 OCCM 容器是否正在运行并正常工作。 • 如果问题仍然存在，请联系支持人员。
无法加载代理的支持信息。	如果代理无法访问您的支持帐户，则会显示此消息。	• *。

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。"

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，您需要禁用配置检查，否则安装将失败。
- 如果您继续使用以前的端点列表进行代理升级，您可能还需要禁用这些检查。

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，您应该熟悉 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
```

用于升级的端点安装失败

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。为避免这种情况，请在安装到 VCenter 时取消选中 验证代理配置 复选框或跳过配置检查。

NetApp建议更新防火墙规则以允许访问"当前端点"尽早。"了解如何更新您的端点" 。

请务必验证唯一的错误是否与前面的端点有关：

- \ https://bluexpinfraprod.eastus2.data.azurecr.io
- \ https://bluexpinfraprod.azurecr.io

如果存在其他错误，您需要先解决它们，然后才能继续。

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

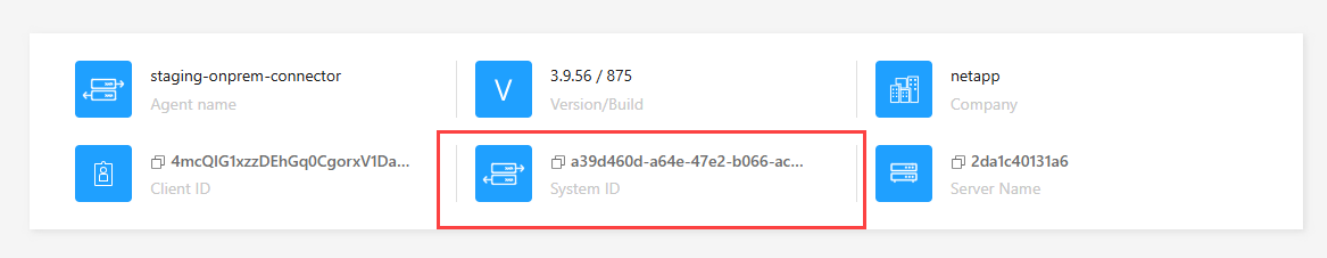
为了帮助您入门，您可能需要控制台代理的系统 ID。该 ID 通常用于许可和故障排除目的。

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控制台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控制台部署模式" 。

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

如果控制台代理处于非活动状态，您可以将其从代理列表中删除。如果您删除代理虚拟机或卸载代理软件，则可能会执行此操作。

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，选择非活动代理的操作菜单，然后选择*删除代理*。
3. 输入代理人的姓名进行确认，然后选择*删除*。

控制台代理的默认配置

在部署控制台代理之前，请了解有关其配置的更多信息。

可访问互联网的默认配置

如果您从NetApp控制台、云提供商的市场部署了控制台代理，或者在具有 Internet 访问权限的本地 Linux 主机上手动安装了控制台代理，则以下配置详细信息适用。

AWS 详细信息

如果您从控制台或云提供商的市场部署了控制台代理，请注意以下事项：

- EC2 实例类型为 t3.2xlarge。
- 该图像的操作系统是 Ubuntu 22.04 LTS。

  该操作系统不包含 GUI。您必须使用终端来访问系统。

- 安装包括 Docker Engine，它是必需的容器编排工具。
- EC2 Linux 实例的用户名是 ubuntu（对于 2023 年 5 月之前创建的代理，用户名是 ec2-user）。
- 默认系统磁盘是 100 GiB gp2 磁盘。

Azure 详细信息

如果您从控制台或云提供商的市场部署了控制台代理，请注意以下事项：

- VM 类型为 Standard_D8s_v3。
- 该图像的操作系统是 Ubuntu 22.04 LTS。

  该操作系统不包含 GUI。您必须使用终端来访问系统。

- 安装包括 Docker Engine，它是必需的容器编排工具。
- 默认系统盘为100GiB高级SSD盘。

Google Cloud 详细信息

如果您从控制台部署了控制台代理，请注意以下事项：

- VM 实例是 n2-standard-8。
- 该图像的操作系统是 Ubuntu 22.04 LTS。

  该操作系统不包含 GUI。您必须使用终端来访问系统。

- 安装包括 Docker Engine，它是必需的容器编排工具。

- 默认系统磁盘是 100 GiB SSD 持久磁盘。

安装文件夹

代理安装文件夹位于以下位置：

/opt/应用程序/netapp/cloudmanager

日志文件

日志文件包含在以下文件夹中：

- /opt/application/netapp/cloudmanager/log 或
- /opt/application/netapp/service-manager-2/logs（从新的 3.9.23 安装开始）

  这些文件夹中的日志提供了有关控制台代理的详细信息。

- /opt/应用程序/netapp/cloudmanager/docker_occm/数据/日志

  此文件夹中的日志提供有关云服务和在控制台代理上运行的控制台服务的详细信息。

控制台代理服务

- 控制台代理服务名为 occm。
- occm 服务依赖于 MySQL 服务。

  如果 MySQL 服务关闭，那么 occm 服务也会关闭。

端口

代理在 Linux 主机上使用以下端口：

- 80 用于 HTTP 访问
- 443 用于 HTTPS 访问

无需互联网访问的默认配置

如果您在没有互联网访问权限的本地 Linux 主机上手动安装了控制台代理，则适用以下配置。"了解有关此安装选项的更多信息" 。

- 代理安装文件夹位于以下位置：

  /opt/应用程序/netapp/ds

- 日志文件包含在以下文件夹中：

  /var/lib/docker/volumes/ds_occmdata/_data/log

  此文件夹中的日志提供有关控制台代理和 Docker 映像的详细信息。

- 所有服务都在docker容器内运行

  这些服务依赖于docker运行时服务的运行

- 代理在 Linux 主机上使用以下端口：
  - 80 用于 HTTP 访问
  - 443 用于 HTTPS 访问

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。

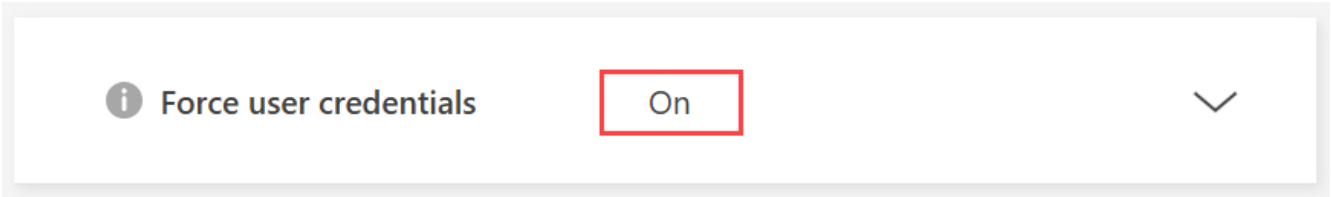
您必须具有组织管理员角色才能编辑控制台代理设置。

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。



凭证和订阅

AWS

了解**NetApp**控制台中的 **AWS** 凭证和权限

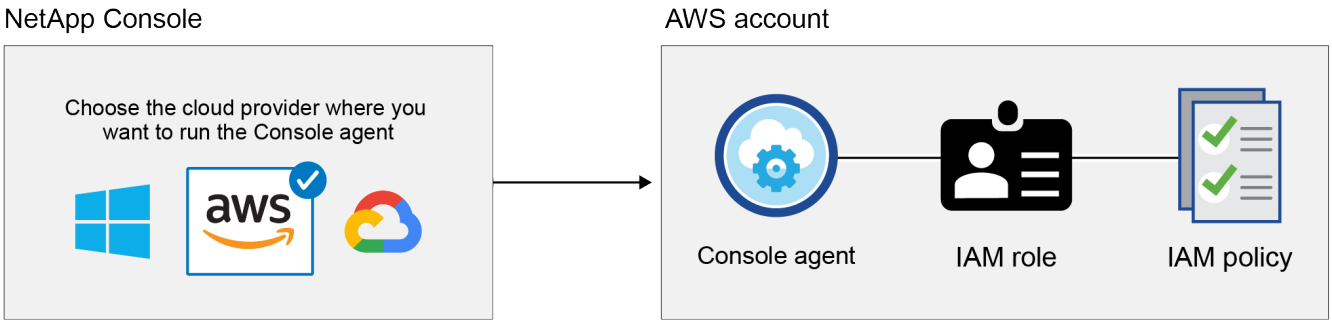
了解NetApp控制台如何使用 AWS 凭证代表您执行操作以及这些凭证如何与市场订阅相关联。了解这些详细信息有助于您在NetApp控制台中管理一个或多个 AWS 帐户的凭据。例如，您可能想了解何时添加额外的 AWS 凭证。

初始 **AWS** 凭证

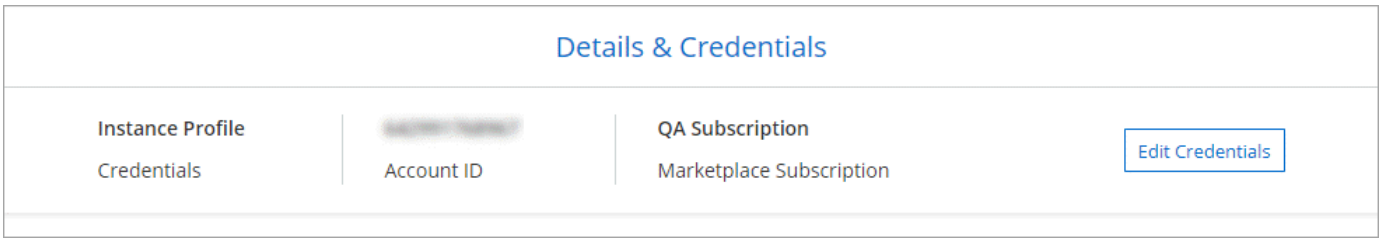
从控制台部署控制台代理时，您需要提供 IAM 角色的 ARN 或 IAM 用户的访问密钥。身份验证方法必须具有在

AWS 中部署控制台的权限。所需的权限列在链接中：task-install-connector-aws-the Console.html#console-permissions-aws[AWS 的代理部署策略]。

当控制台在 AWS 中启动控制台代理实例时，它会为该实例创建一个 IAM 角色和一个实例配置文件。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。"查看控制台如何使用权限" 。



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

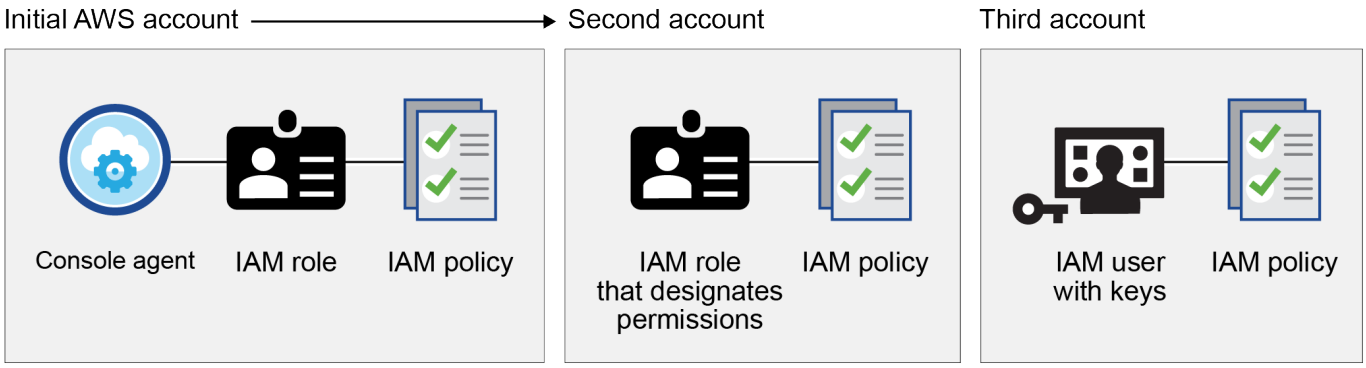
在以下情况下，您可能会向控制台添加其他 AWS 凭证：

- 将现有的控制台代理与其他 AWS 账户一起使用
- 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。

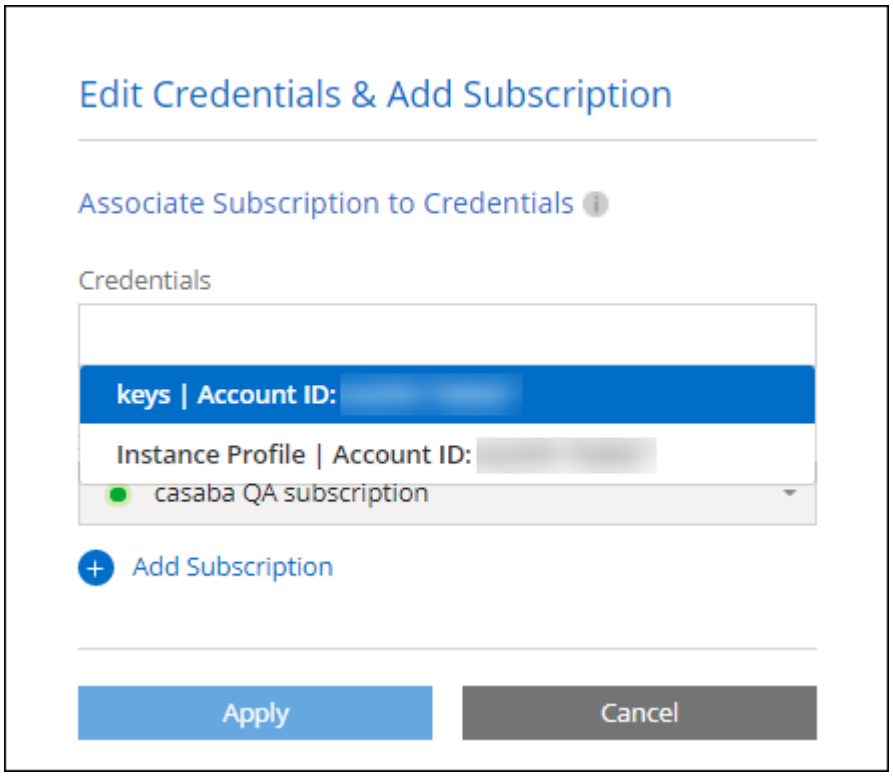
添加 **AWS** 凭证以将控制台代理与另一个 **AWS** 账户一起使用

如果您想将控制台与其他 AWS 账户一起使用，则可以为 IAM 用户提供 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：



然后，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

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

您添加到控制台代理的凭证必须与 AWS Marketplace 订阅相关联，以便您可以按小时费率 (PAYGO) 和其他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 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：与控制台代理实例关联的 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。这个过程是最佳实践——它是自动的并且是安全的。

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，并且可以在自己的 Linux 主机上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**控制台的 **AWS** 凭证和市场订阅

添加和管理 AWS 凭证，以便您从NetApp控制台部署和管理 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控制台 。

- 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控制台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。

如果您刚刚开始使用控制台，"了解NetApp控制台如何使用 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。"了解 AWS 凭证和权限" 。

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实例的源 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"

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 。

添加凭据

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。

```
 New credentials in your cloud provider may take a few minutes to become
available. Then, add the credentials.
```

.步骤

. 使用顶部导航栏选择要添加凭据的控制台代理。
. 在左侧导航栏中，选择"管理"＞"凭据"。
. 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。

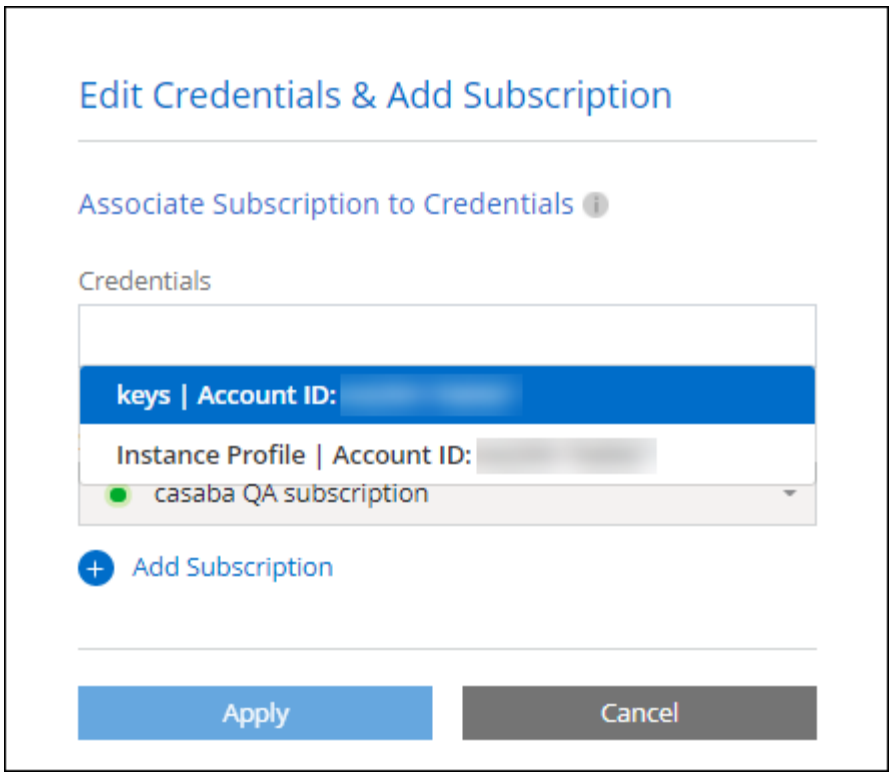
+
.. 凭证位置：选择*Amazon Web Services > 代理*。
.. 定义凭证：提供受信任的 IAM 角色的 ARN（Amazon 资源名称），或输入 AWS 访问密钥和密钥。
.. 市场订阅：通过立即订阅或选择现有订阅将市场订阅与这些凭证关联。

+
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。

a. 审核：确认有关新凭证的详细信息并选择*添加*。

结果

现在，在将系统添加到控制台时，您可以从“详细信息和凭据”页面切换到另一组凭据



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控制台软件即服务 (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

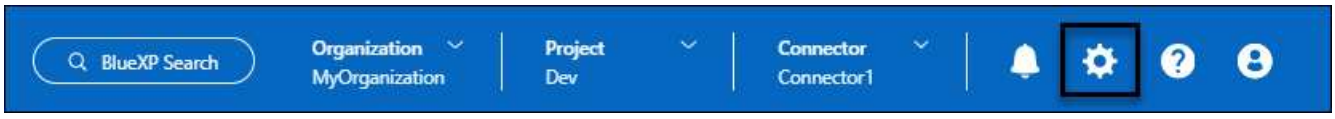
为 IAM 角色提供所需的权限后，将角色 ARN 添加到控制台。

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*或*帐户凭据*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 > NetApp Console*。
   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Cloud Volumes ONTAP费用，并支付其他数据服务费用。

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" 。

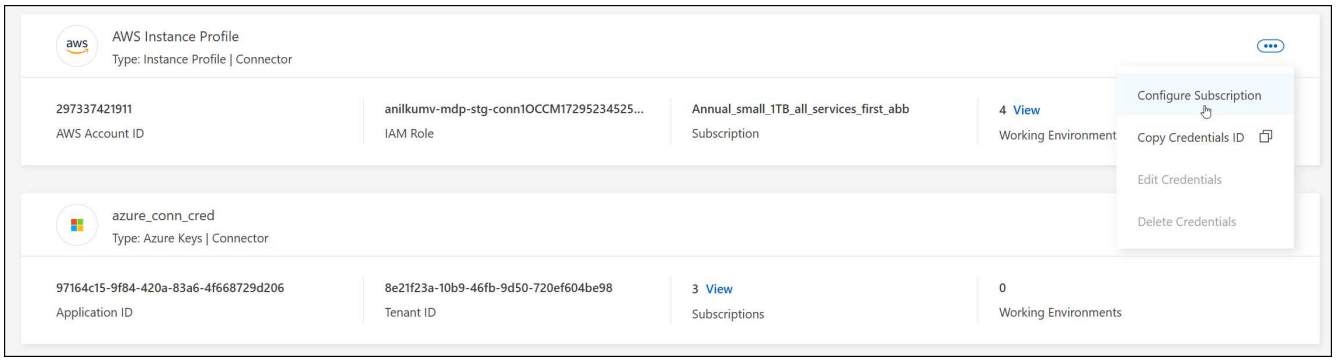
以下视频展示了从 AWS Marketplace 订阅NetApp智能服务的步骤：

从 AWS Marketplace 订阅NetApp智能服务

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控制台关联的凭据关联。



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控制台。

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或帐户关联

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或帐户中使用该订阅。

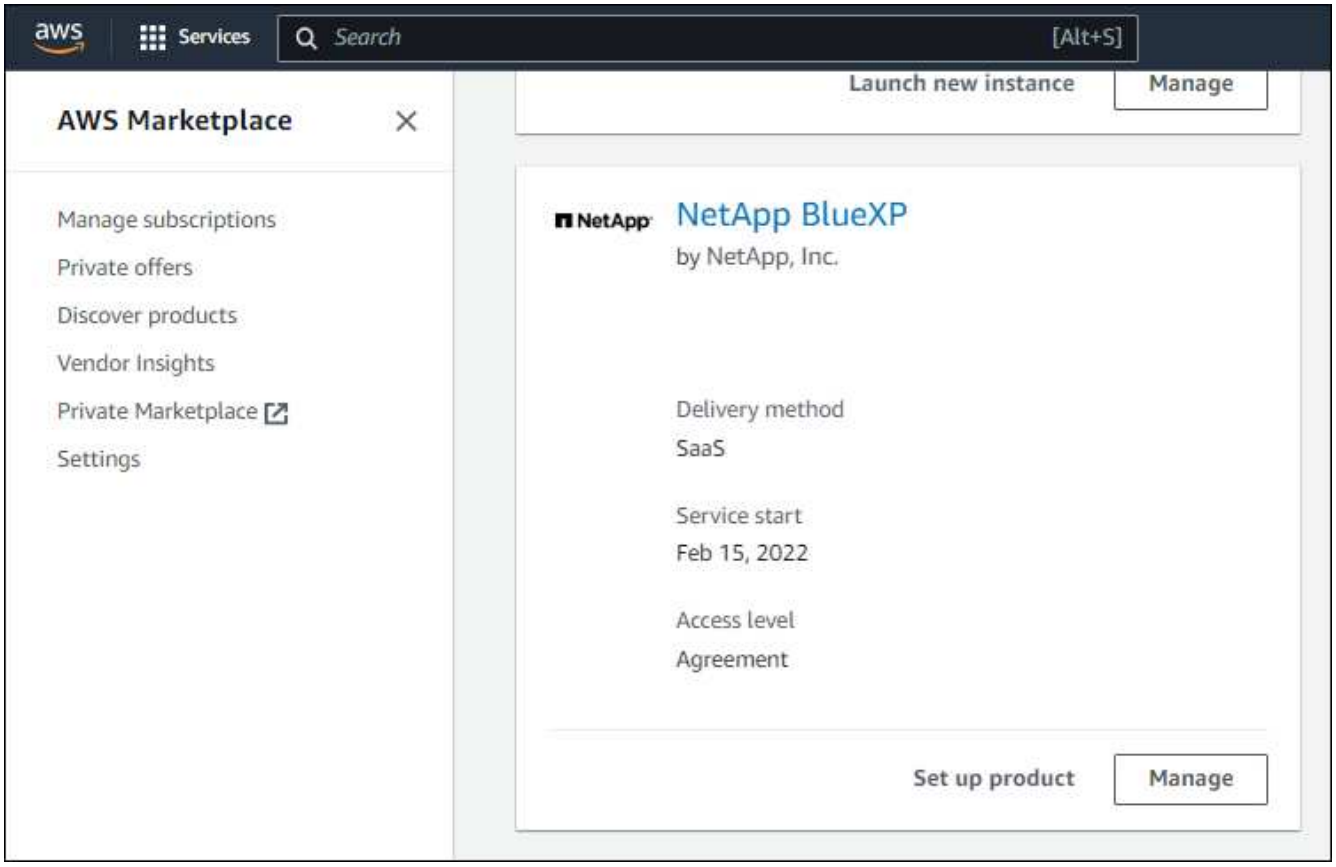
- "了解控制台部署模式"
- "了解控制台身份和访问管理"

如果您从 AWS Marketplace 订阅了NetApp智能数据服务，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或帐户关联。
   a. 从导航菜单中，选择*管理>许可证和订阅*。
   b. 选择*订阅*。
   c. 确认您的订阅没有出现。

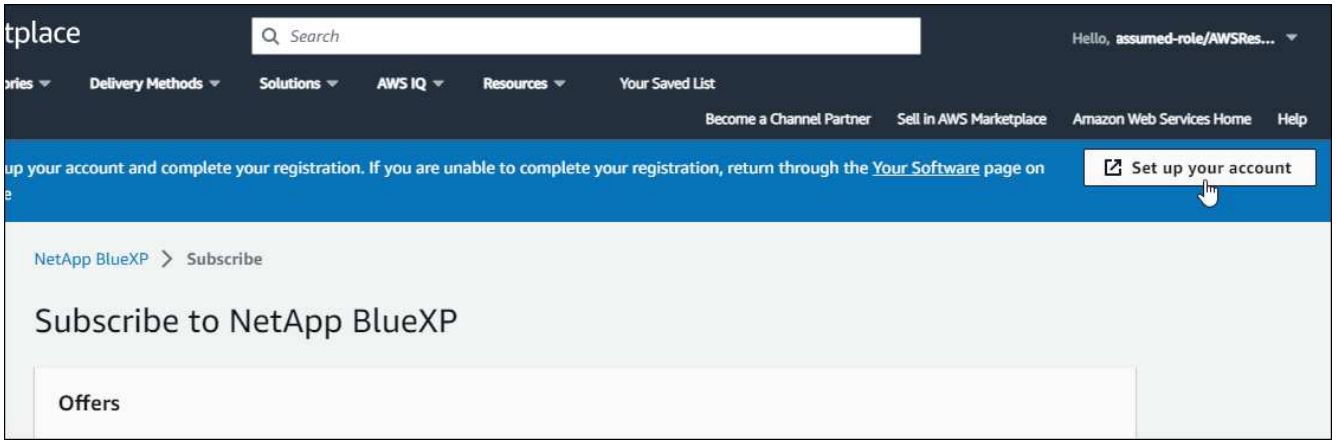
      您只会看到与您当前正在查看的组织或帐户相关的订阅。如果您没有看到您的订阅，请继续执行以下步骤。
2. 登录 AWS 控制台并导航到 **AWS Marketplace** 订阅。
3. 查找订阅。



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。

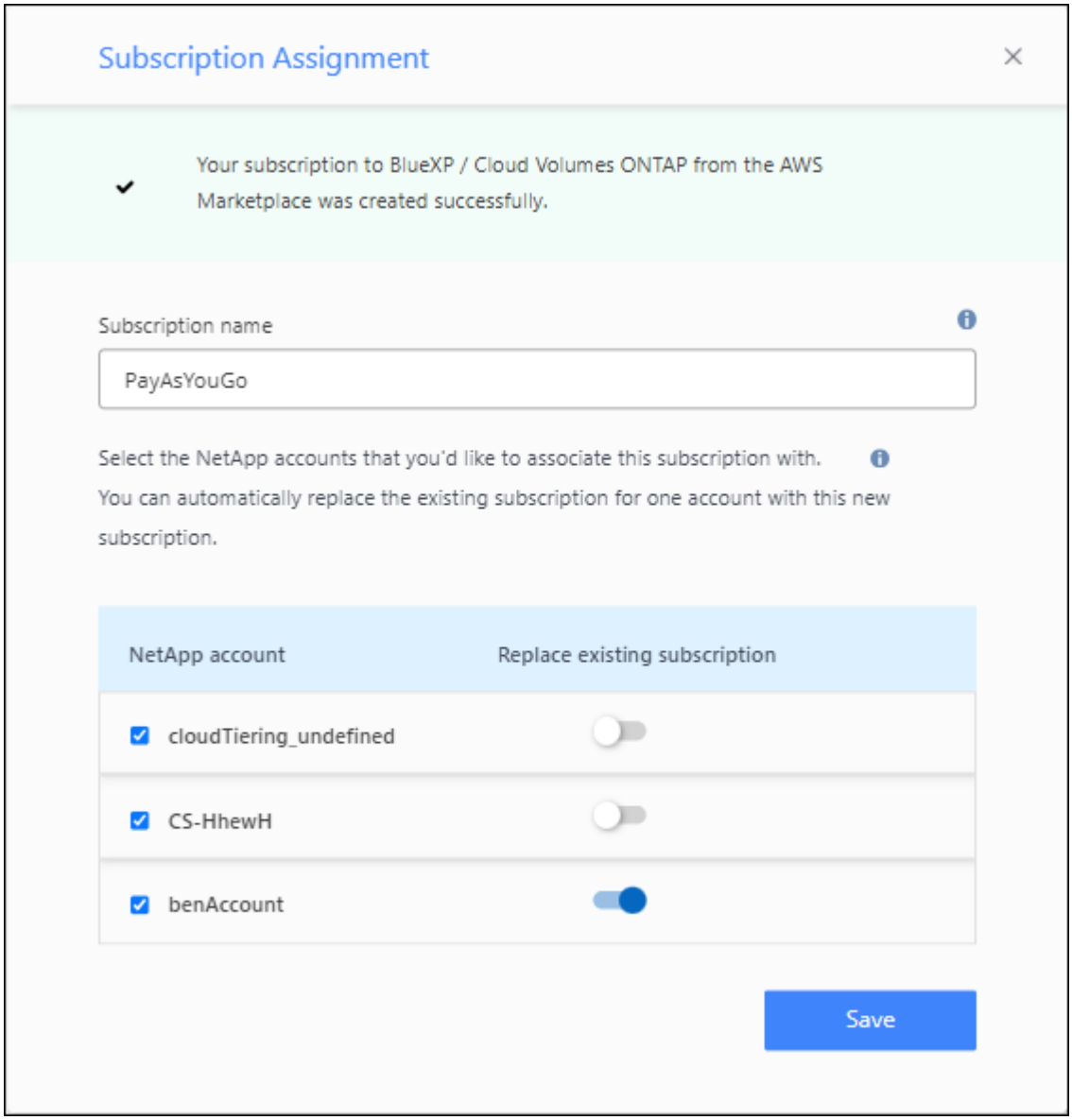
6. 从“订阅分配”页面：

   ◦ 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。

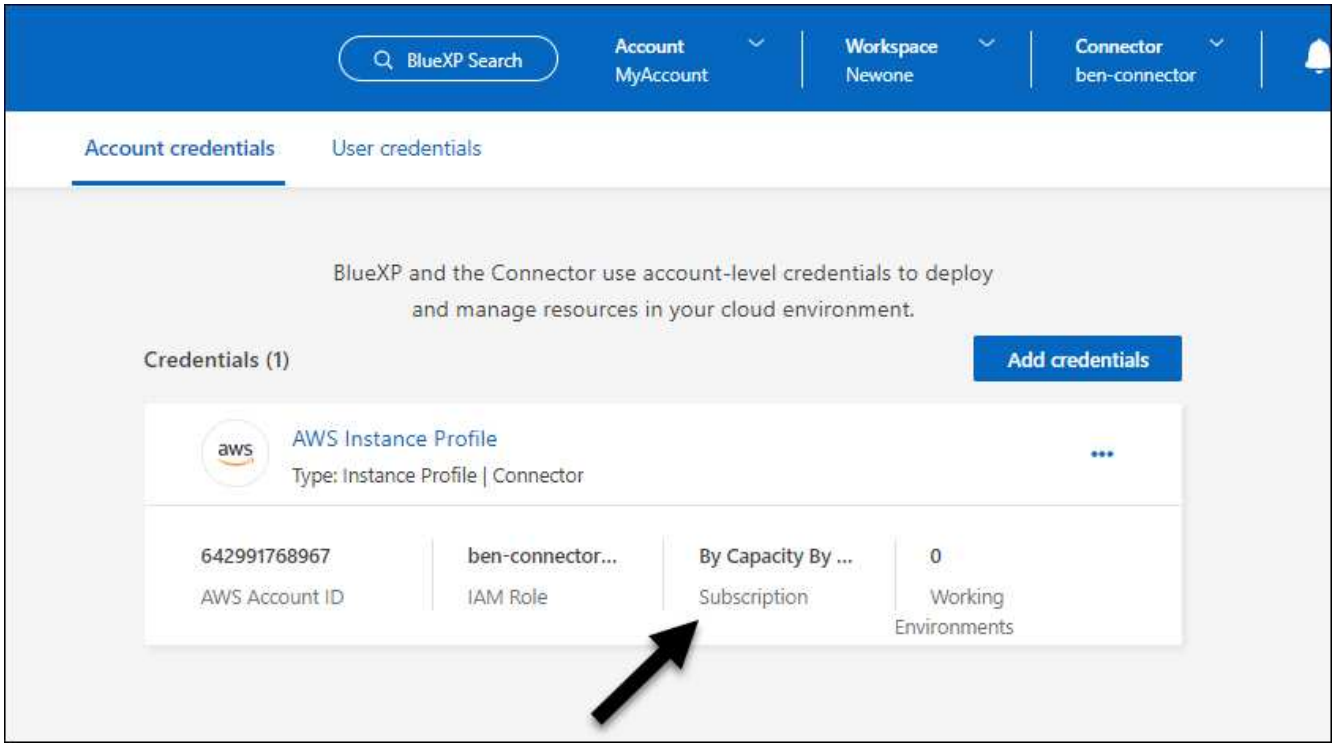
  控制台将用这个新订阅替换组织或帐户中所有凭据的现有订阅。如果一组凭证从未与订阅关联，那么这个新订阅将不会与这些凭证关联。

  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或帐户相关联。
   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. 在控制台的右上角，选择“设置”图标，然后选择“凭据”。
   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*组织凭据*或*帐户凭据*页面上，选择一组凭据的操作菜单，然后选择*编辑凭据*。
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实例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

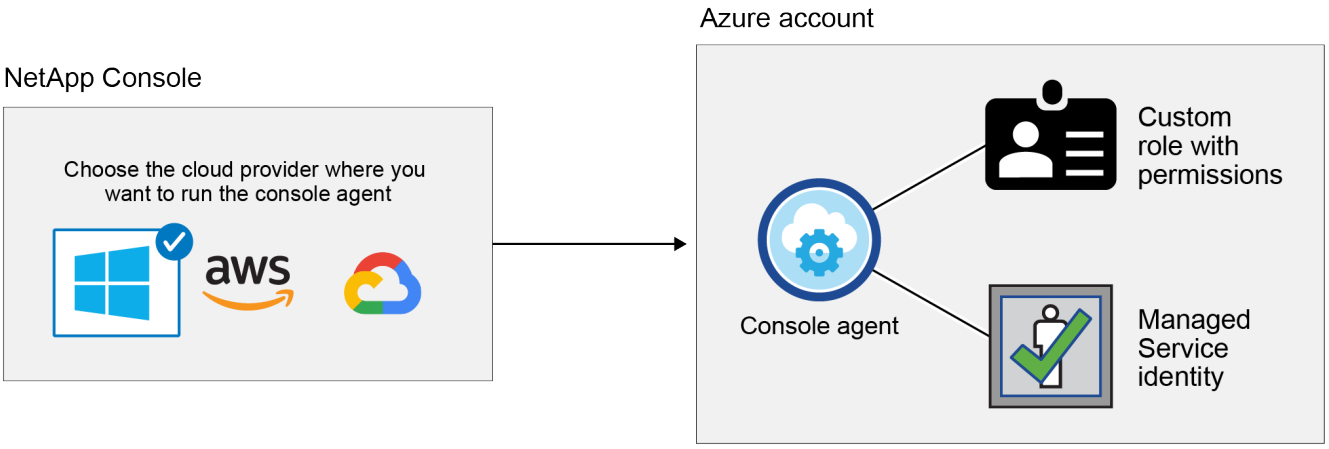
了解NetApp控制台中的 Azure 凭据和权限

了解NetApp控制台如何使用 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。

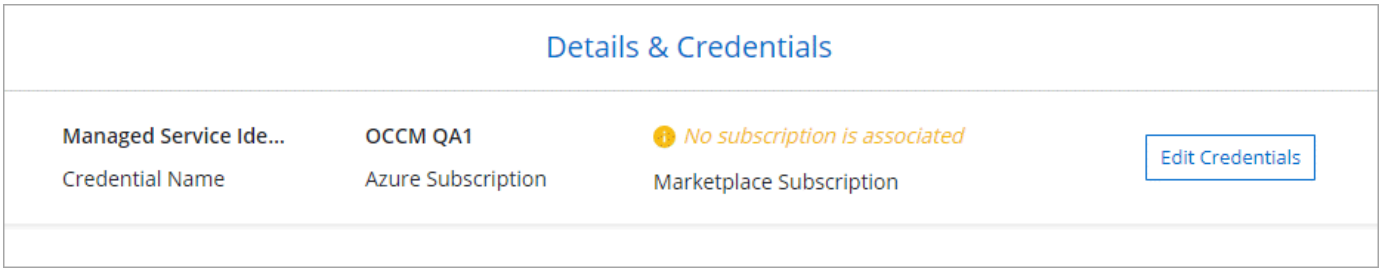
初始 Azure 凭据

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。

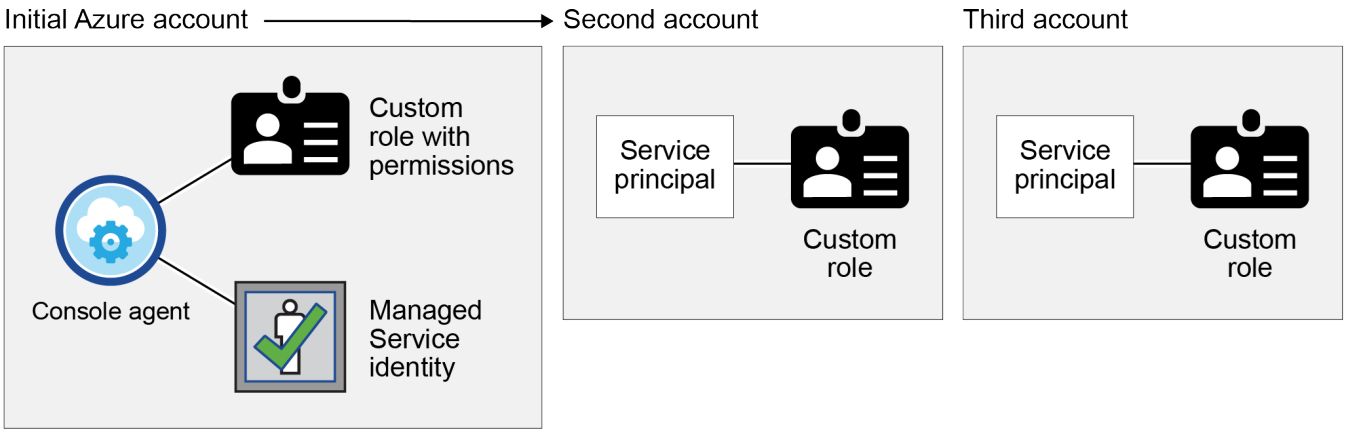
托管标识的其他 Azure 订阅

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

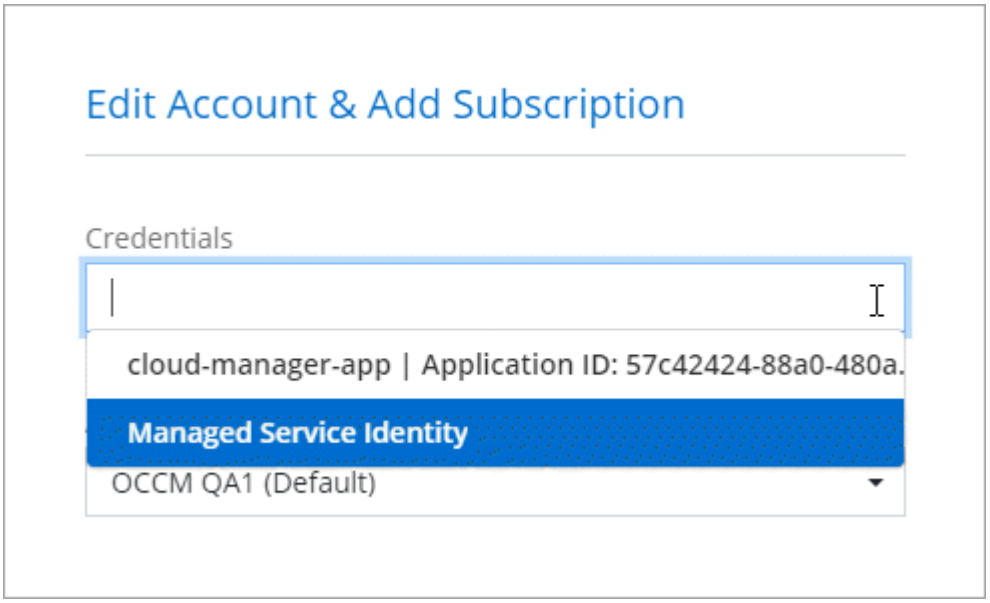
如果要在控制台中使用不同的 Azure 凭据，则必须通过以下方式授予所需的权限"在 Microsoft Entra ID 中创建和

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**控制台的 **Azure** 凭据和市场订阅

添加和管理 Azure 凭据，以便NetApp控制台具有在 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

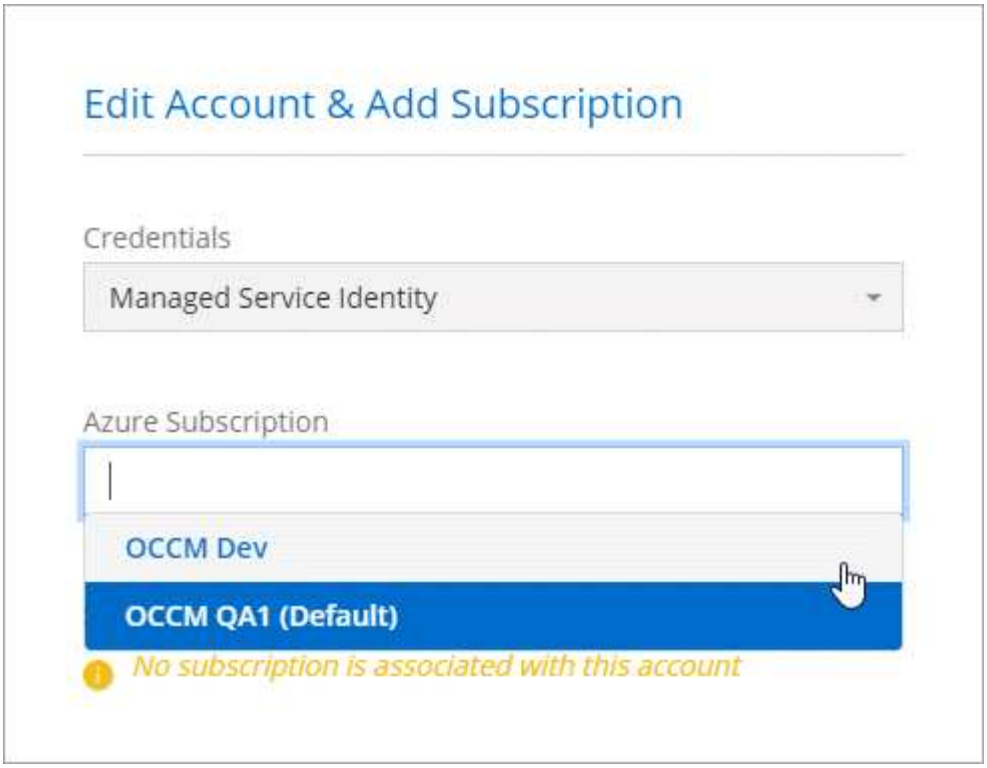
1. 登录 Azure 门户。
2. 打开*订阅*服务，然后选择要部署Cloud Volumes ONTAP 的订阅。
3. 选择*访问控制 (IAM)*。
   a. 选择 添加 > 添加角色分配，然后添加权限：
      - 选择*控制台操作员*角色。

        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**控制台添加其他 **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" 。

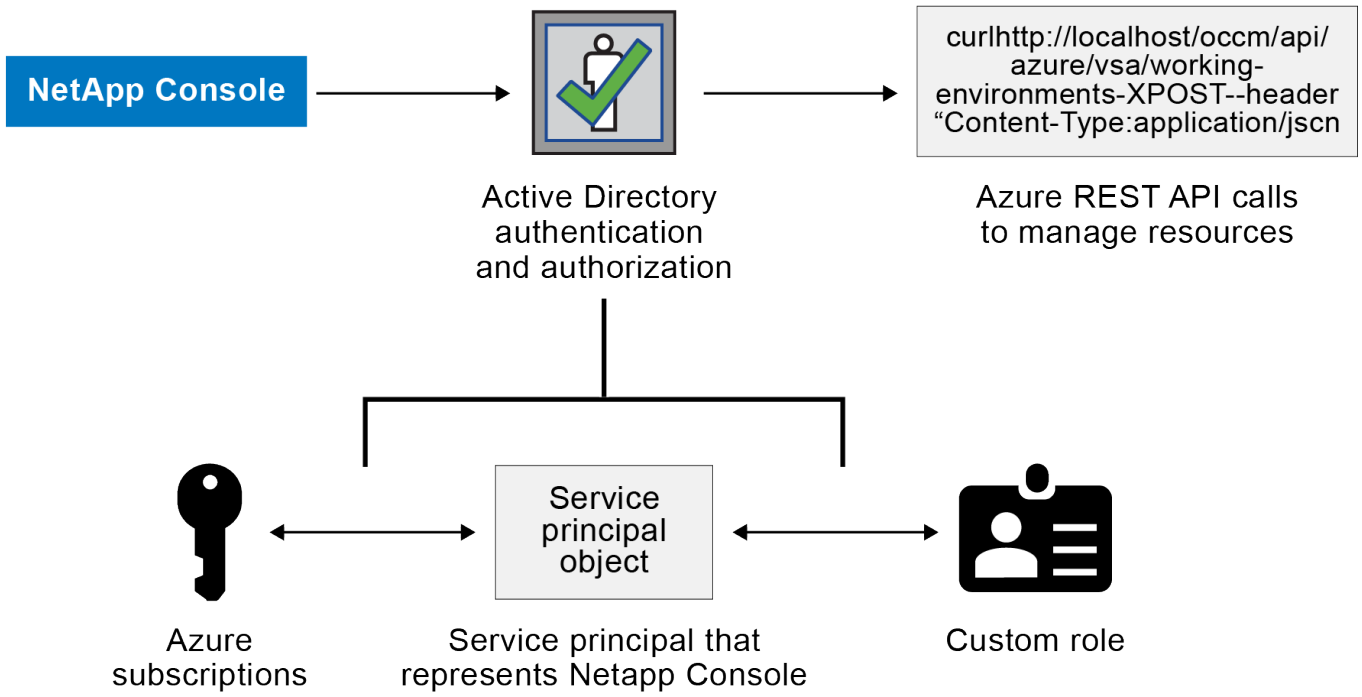
如果您想使用不同的 Azure 凭据部署Cloud Volumes ONTAP ，则必须通过在 Microsoft Entra ID 中为每个 Azure 帐户创建和设置服务主体来授予所需的权限。然后，您可以将新凭据添加到控制台。

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

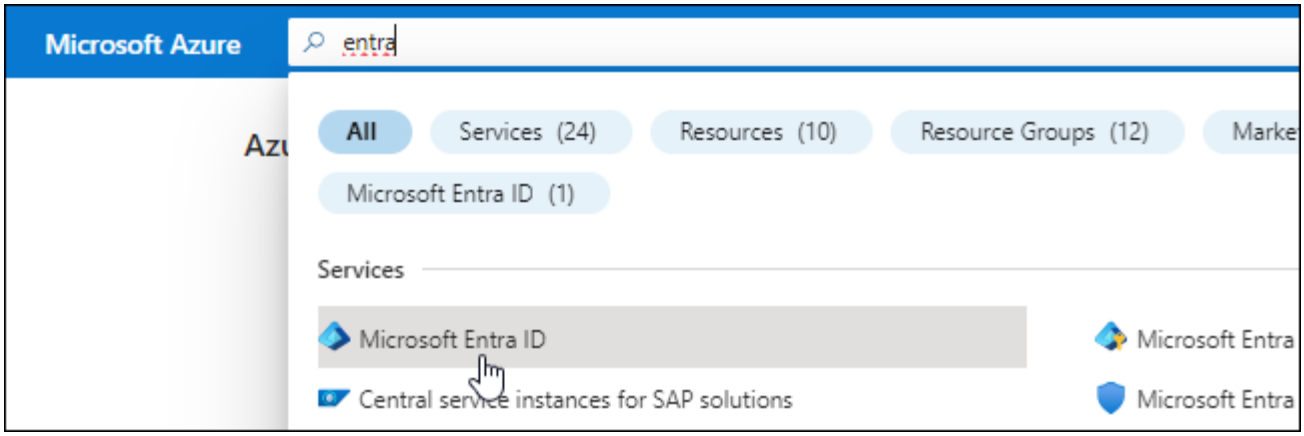
创建控制台可用于基于角色的访问控制的 Microsoft Entra 应用程序和服务主体。

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控制台一起使用）。
   - 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。

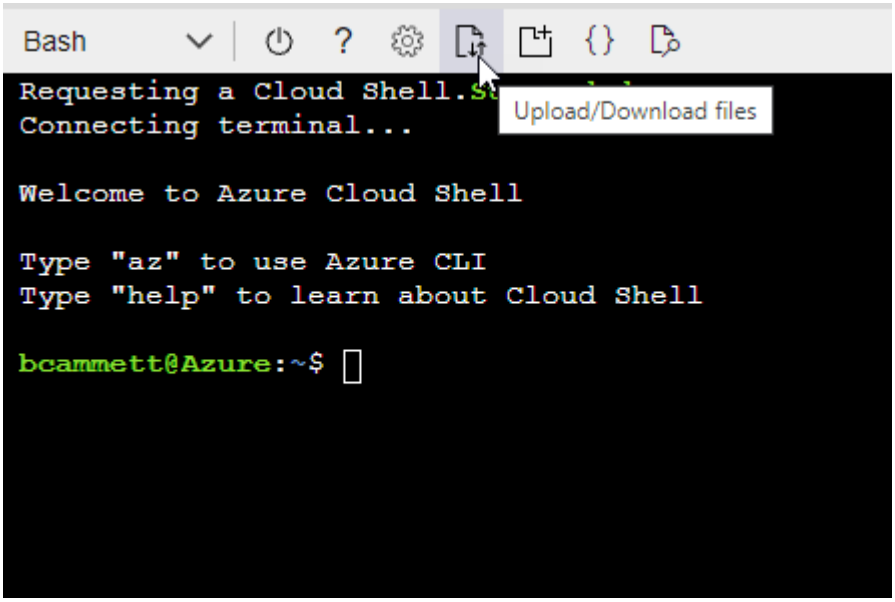
      例子

```
"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 Connector_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。

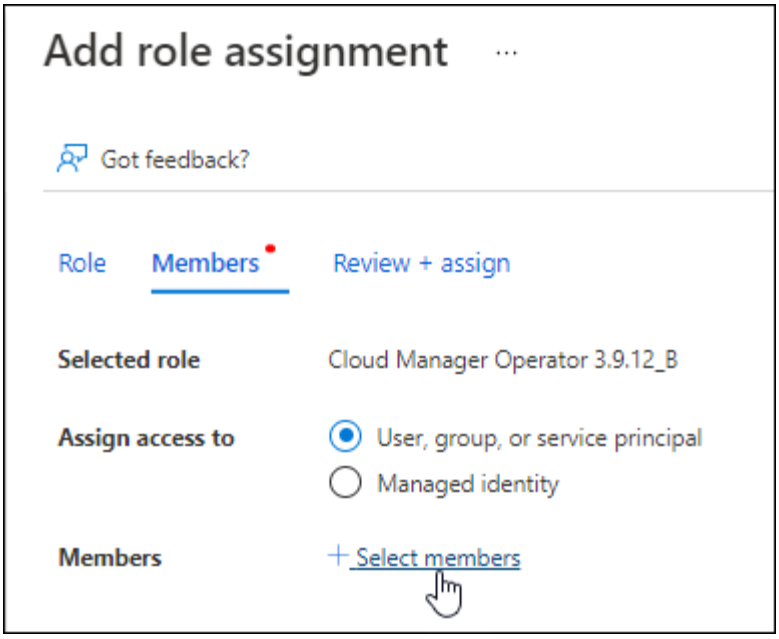
b. 选择订阅。

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*。

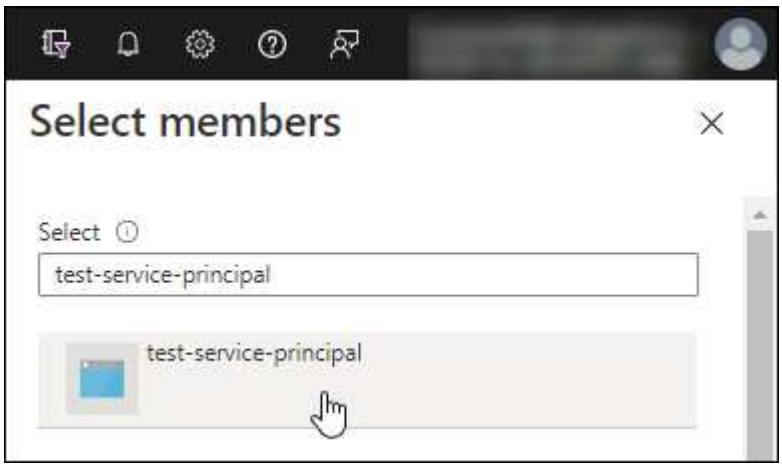
e. 在“成员”选项卡中，完成以下步骤：

- 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。

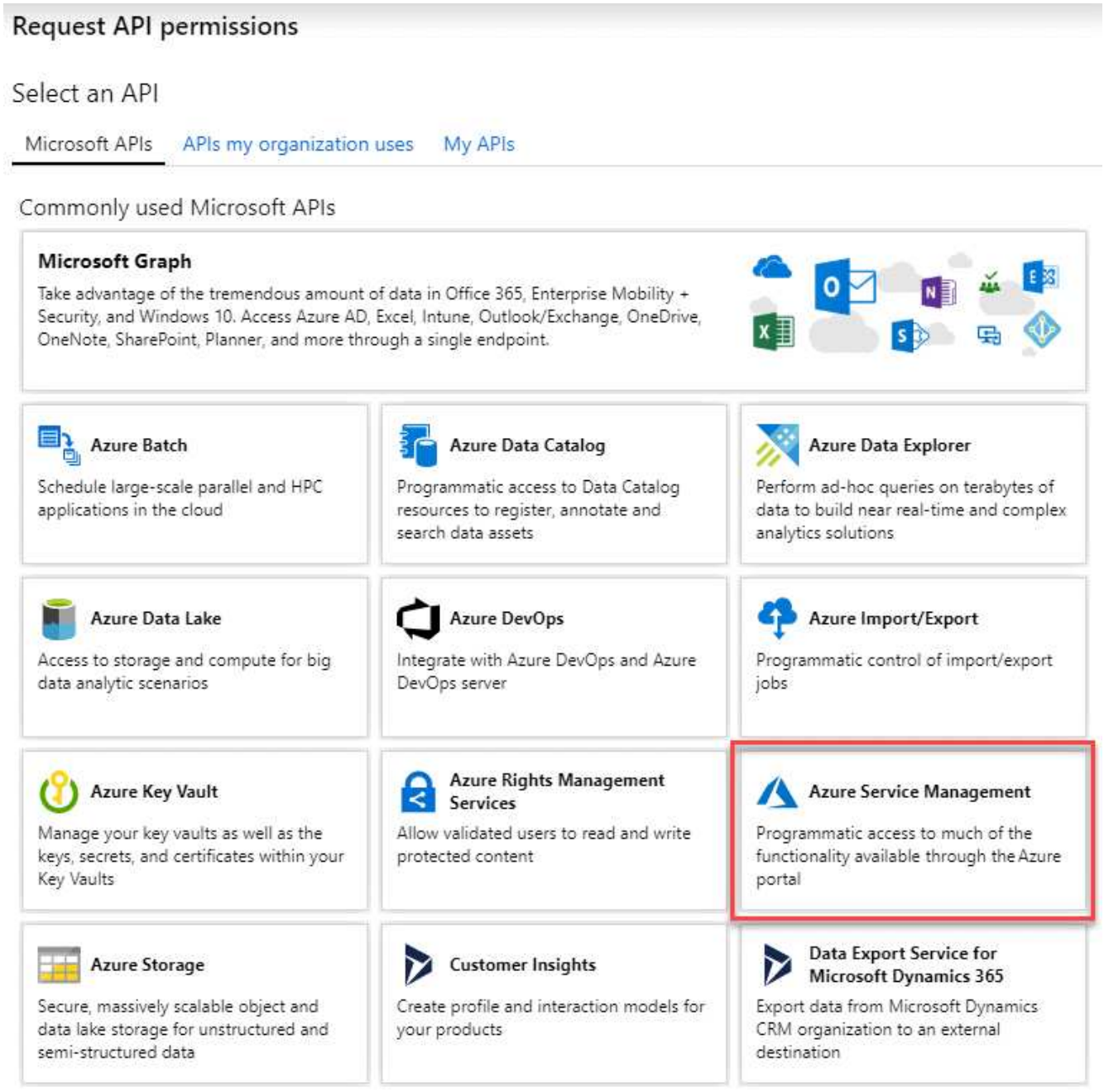
如果您想从多个 Azure 订阅部署Cloud Volumes ONTAP ，则必须将服务主体绑定到每个订阅。在NetApp控制台中，您可以选择部署Cloud Volumes ONTAP时要使用的订阅。

添加 **Windows Azure** 服务管理 **API** 权限

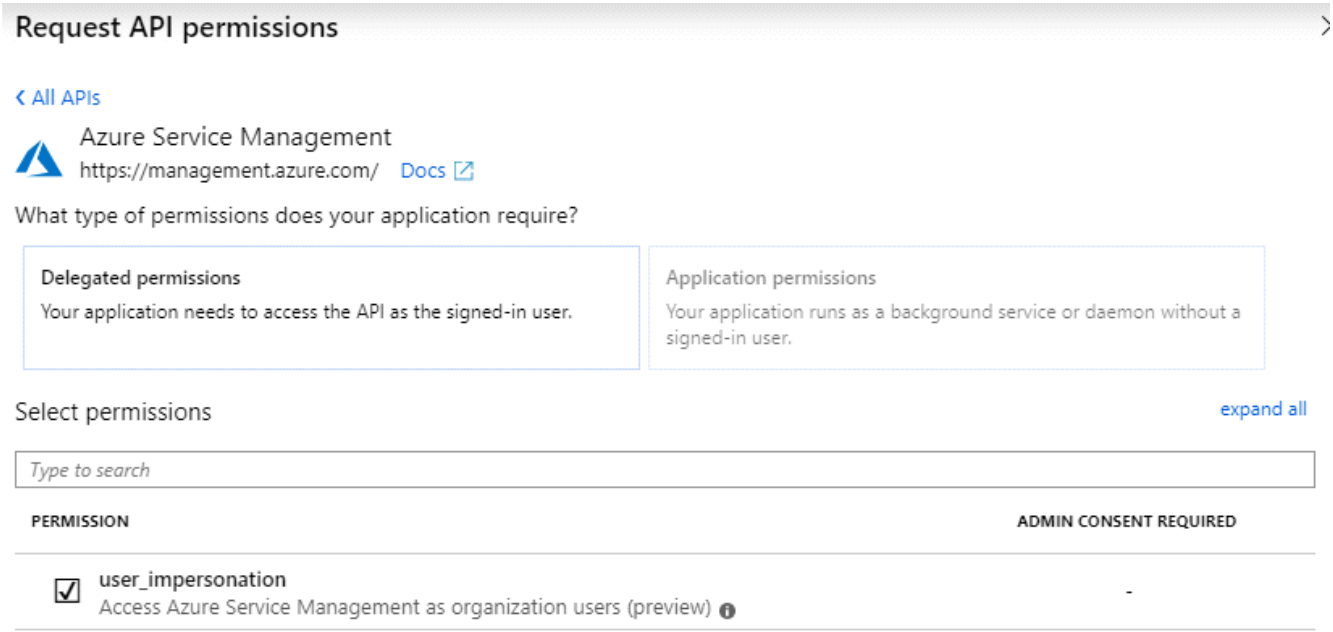
您必须为服务主体分配“Windows Azure 服务管理 API”权限。

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*。

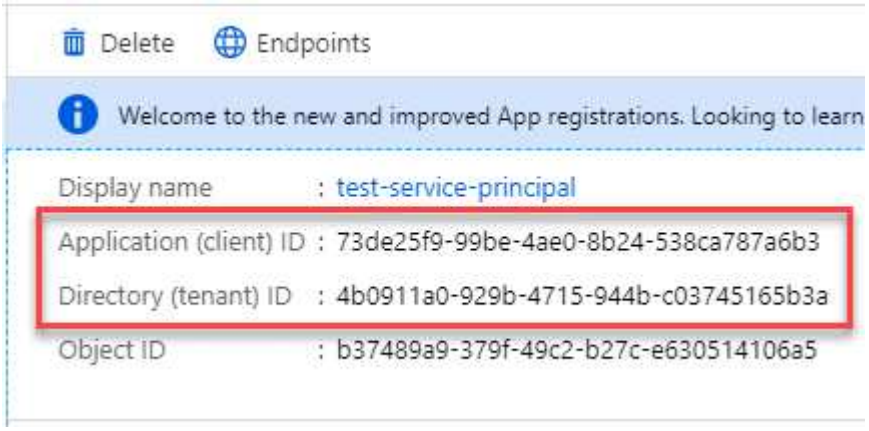


获取应用程序**ID**和目录**ID**

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

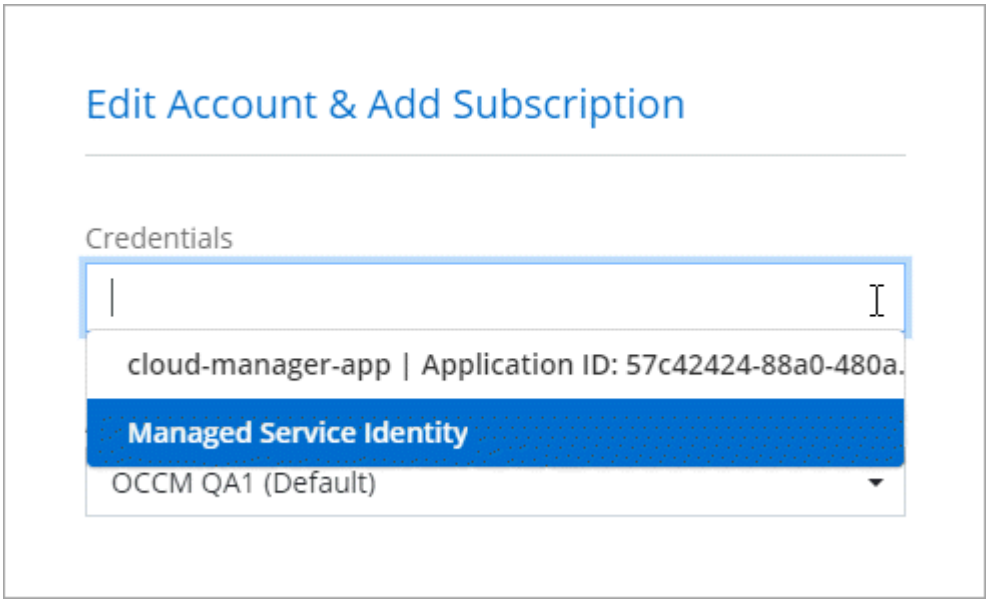
您需要先创建控制台代理，然后才能更改控制台设置。"了解如何创建控制台代理" 。

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
      - 客户端机密
   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控制台关联的凭据关联。
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控制台。

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*。

以下视频展示了从 Azure 市场订阅的步骤：

从 Azure 市场订阅NetApp智能服务

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控制台如何使用 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。

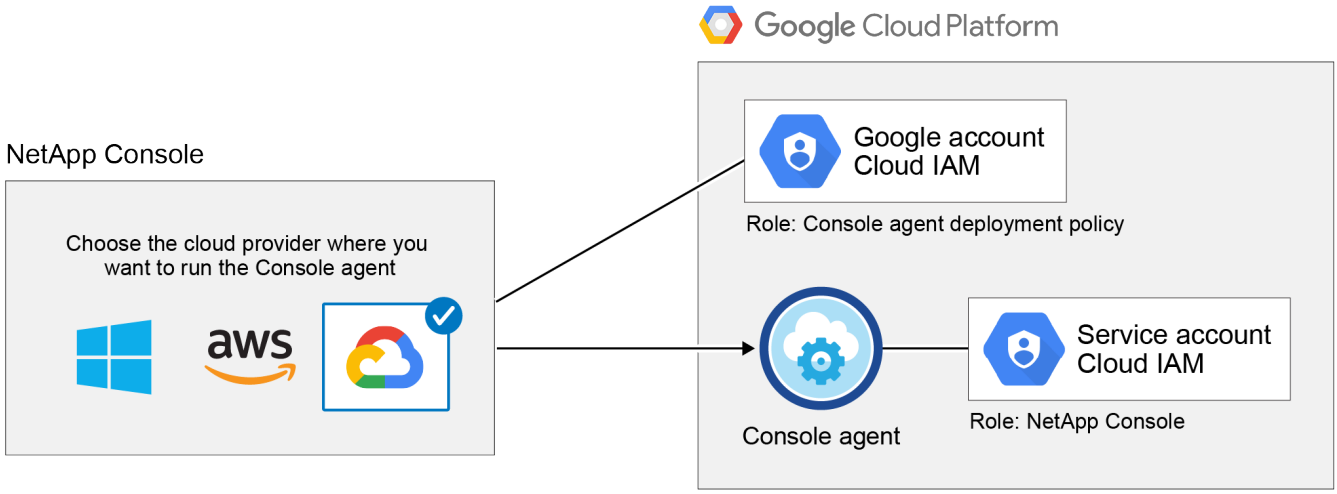
NetApp控制台的项目和权限

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 VM 实例权限的 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"用于虚拟机实例。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控制台的 Google Cloud 凭据和订阅

您可以通过关联市场订阅并对订阅过程进行故障排除来管理与控制台代理 VM 实例关联的 Google Cloud 凭据。这两项任务确保您可以使用市场订阅来支付数据服务。

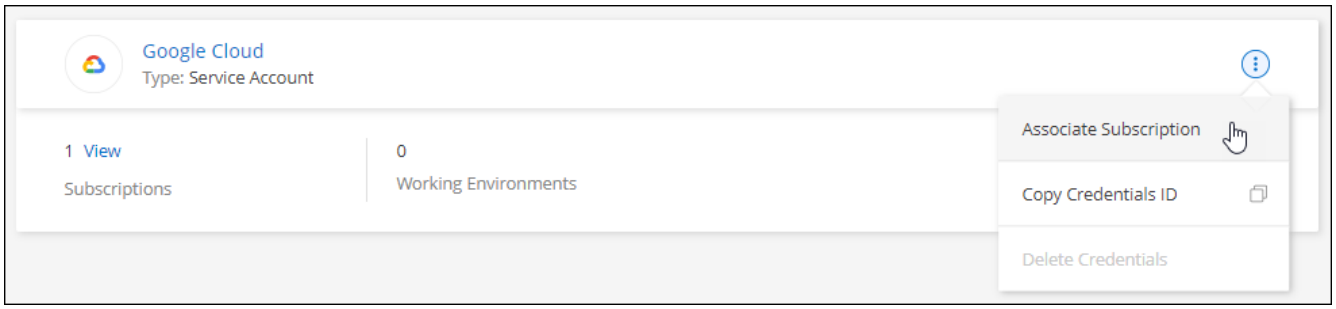
将 Marketplace 订阅与 Google Cloud 凭据关联

在 Google Cloud 中部署控制台代理时，控制台会创建一组与控制台代理虚拟机实例关联的默认凭据。您可以随时更改与这些凭据关联的 Google Cloud Marketplace 订阅。通过订阅，您可以创建按使用量付费的Cloud Volumes ONTAP系统，并使用其他数据服务。

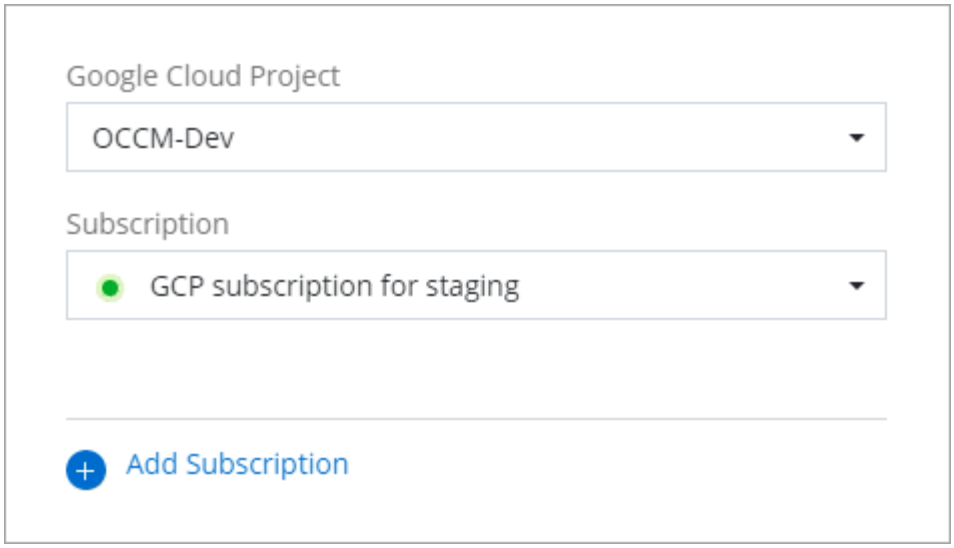
用新的订阅替换当前的市场订阅会更改任何现有Cloud Volumes ONTAP系统和所有新系统的市场订阅。

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*。 +需要新的屏幕截图（TS
)



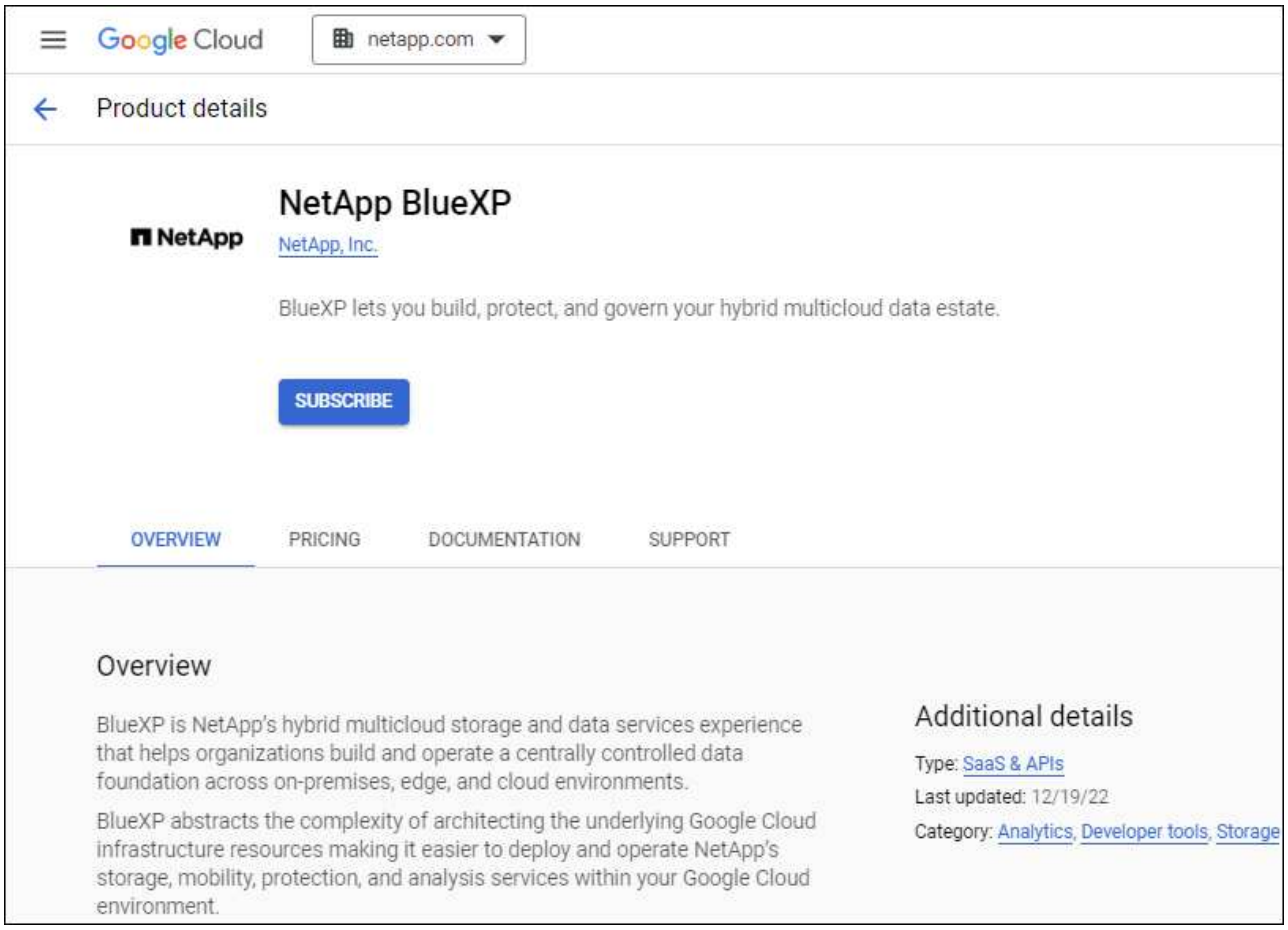
4. 要使用选定的凭据配置现有订阅，请从下拉列表中选择一个 Google Cloud 项目和订阅，然后选择*配置*。



5. 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智能服务页面"，确保在顶部导航菜单中选择了正确的项目。



b. 选择*订阅*。

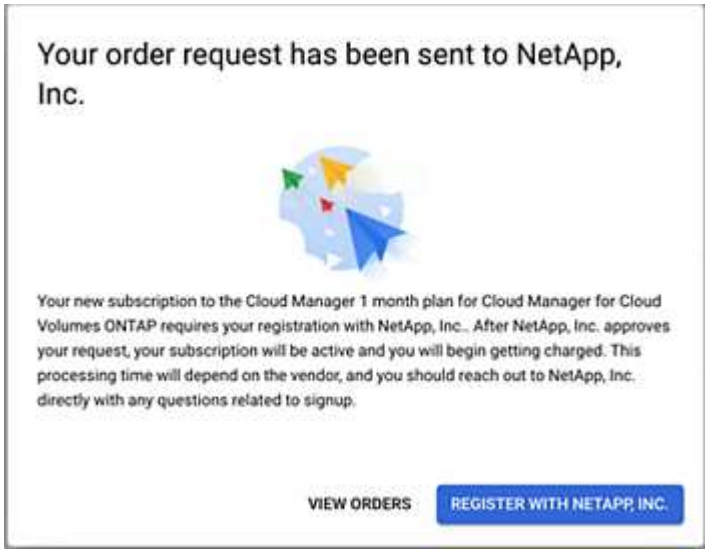
c. 选择适当的结算账户并同意条款和条件。

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控制台中的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。

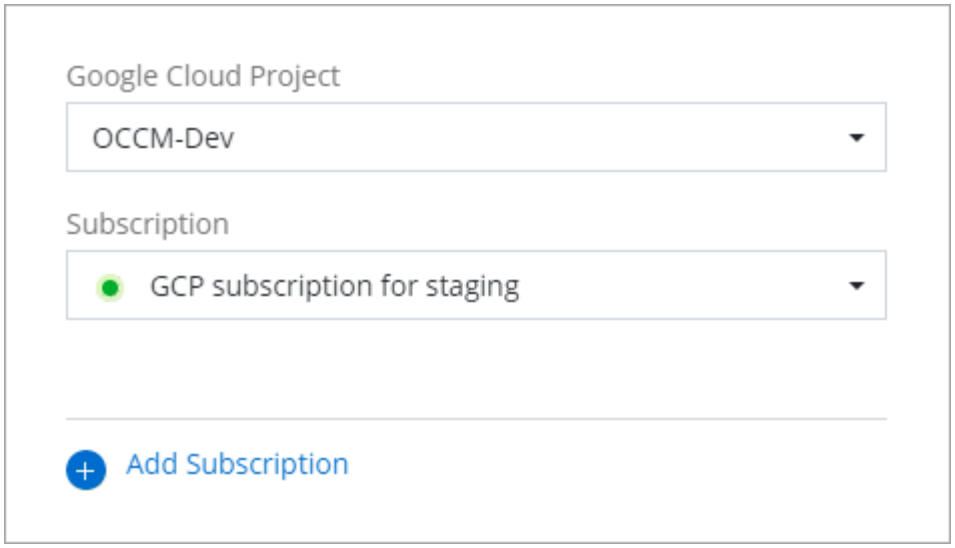
对于所有其他组织或帐户，您需要重复这些步骤来手动关联订阅。

- 选择*保存*。

以下视频展示了从 Google Cloud Marketplace 订阅的步骤：

从 Google Cloud Marketplace 订阅

a. 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。

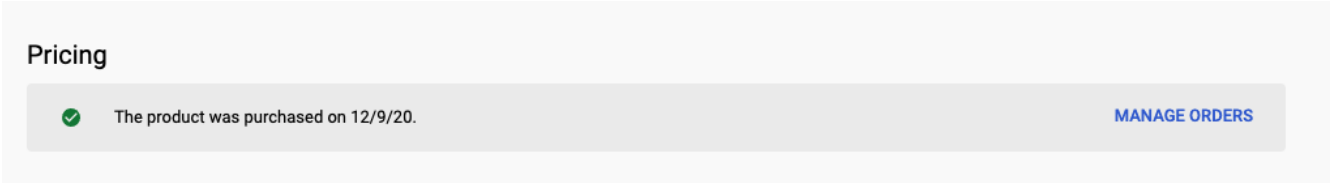


解决 **Marketplace** 订阅流程问题

有时，通过 Google Cloud Marketplace 订阅NetApp数据服务可能会由于权限不正确或意外未遵循重定向到控制台而变得碎片化。如果发生这种情况，请按照以下步骤完成订阅过程。

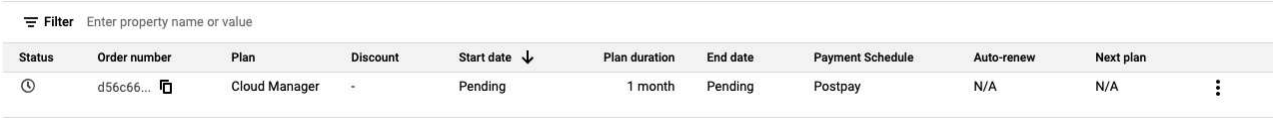
步骤

1. 导航至 "Google Cloud Marketplace 上的NetApp页面"检查订单状态。如果页面显示*在提供商处管理*，请向下滚动并选择*管理订单*。



   - 如果订单显示绿色复选标记并且这是意外情况，则该组织中使用相同计费帐户的其他人可能已经订阅。如果这是意外情况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*待定*状态，请返回市场页面并选择*在提供商处管理*以完成如上所述的流程。



管理与NetApp控制台关联的 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。

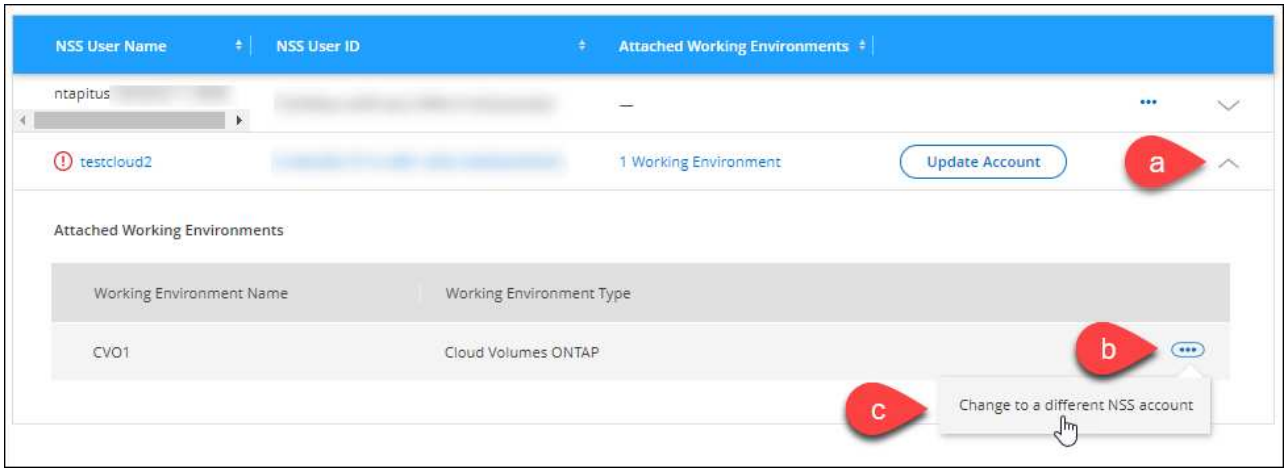
将系统附加到不同的 **NSS** 帐户

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**控制台登录关联的凭据

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控制台登录关联的 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控制台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。

监控NetApp控制台操作

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

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。

使用审计页面来识别谁执行了操作或其状态。

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控制台警报的更多信息"

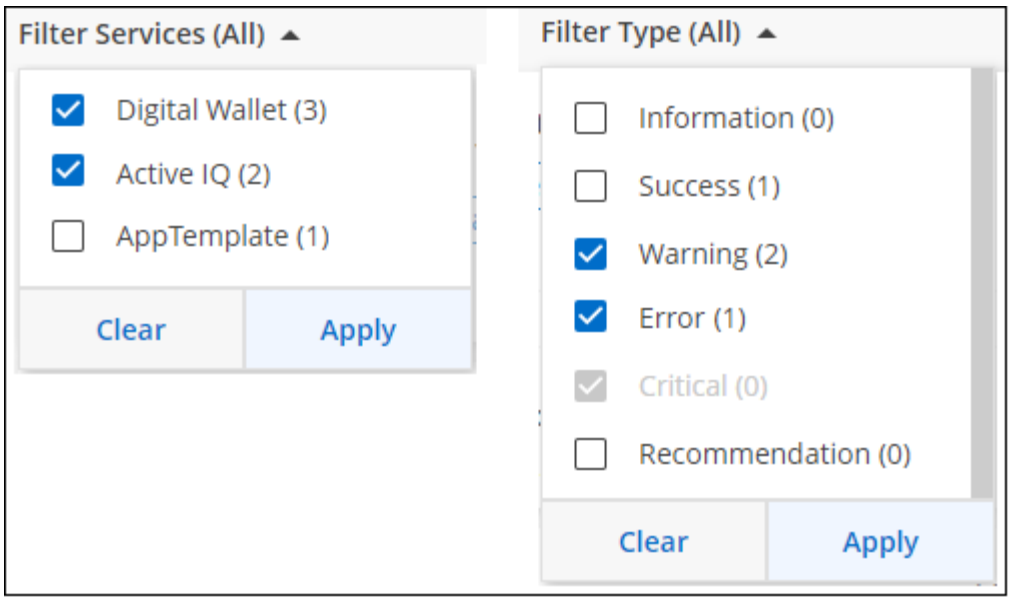
通知类型

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。

- 控制台会发送代理、许可证和订阅、 NetApp复制和同步以及NetApp备份和恢复的电子邮件通知。
- 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备份和恢复。

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。

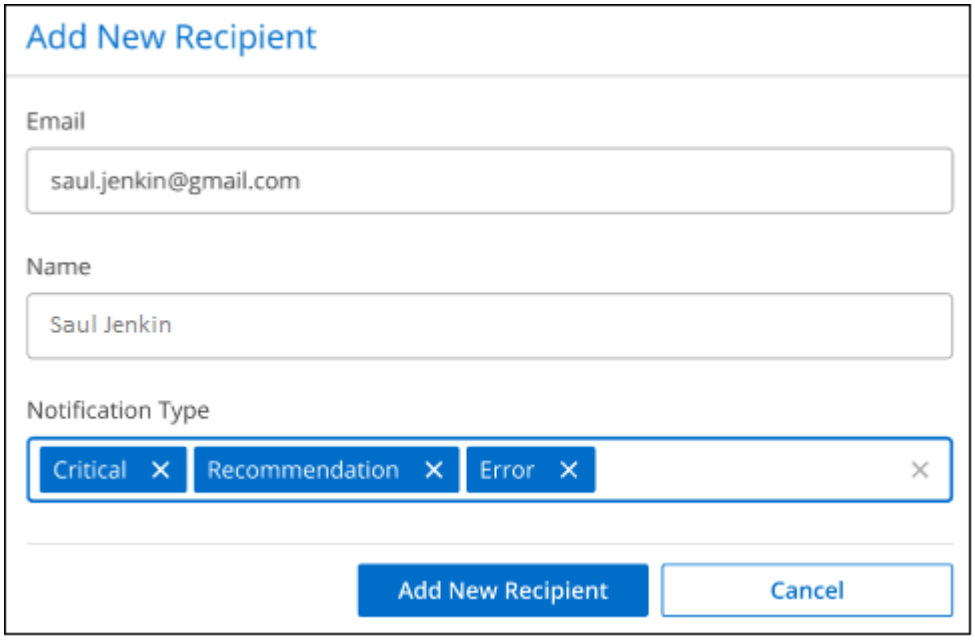
3. 从“组织用户”页面或“其他收件人”页面中选择一个或多个用户，然后选择要发送的通知类型：
   - 要对单个用户进行更改，请选择该用户的通知列中的菜单，检查要发送的通知类型，然后选择*应用*。
   - 要对多个用户进行更改，请选中每个用户的复选框，选择*管理电子邮件通知*，检查要发送的通知类型，然后选择*应用*。

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*。

参考

代理维护控制台

控制台代理维护控制台

您可以使用控制台代理维护控制台来配置控制台代理以使用透明代理服务器。

访问代理维护控制台

您可以从控制台代理主机访问维护控制台。导航到以下目录：

```
/opt/application/netapp/service-manager-2/agent-maint-console
```

透明代理命令

代理维护控制台提供命令来配置代理使用透明代理服务器。

查看当前透明代理配置

要查看当前的透明代理配置，请使用以下命令：

```
./agent-maint-console proxy get
```

添加透明代理服务器

要添加透明代理服务器，请使用以下命令，其中 `/home/ubuntu/myCA1.pem`是代理服务器证书文件的路径。证书文件必须为 PEM 格式：

```
./agent-maint-console proxy add -c /home/ubuntu/myCA1.pem
```

确保证书文件与命令位于同一目录中，或者指定证书文件的完整路径。

更新透明代理服务器的证书

要更新透明代理服务器的证书，请使用以下命令，其中 `/home/ubuntu/myCA1.pem`是代理服务器的新证书文件的路径。证书文件必须为 PEM 格式：

```
./agent-maint-console proxy update -c /home/ubuntu/myCA1.pem
```

确保证书文件与命令位于同一目录中，或者指定证书文件的完整路径。

删除透明代理服务器

要删除透明代理服务器，请使用以下命令：

```
./agent-maint-console proxy remove
```

查看任何命令的帮助

要查看任何命令的帮助，请附加 `--help`到命令。例如，要查看 `proxy add`命令，使用以下命令：

```
./agent-maint-console proxy add --help
```

权限

NetApp控制台的权限摘要

要使用NetApp控制台功能和服务，您需要提供权限，以便控制台可以在您的云环境中执行操作。使用此页面上的链接可以根据您的目标快速访问所需的权限。

AWS 权限

NetApp控制台需要控制台代理和各个服务的 AWS 权限。

控制台代理

目标	描述	链路
从控制台部署控制台代理	从控制台创建控制台代理的用户需要特定权限才能在 AWS 中部署实例。	"设置 AWS 权限"
为控制台代理提供权限	当控制台部署控制台代理时，它会将一个策略附加到实例，该实例提供管理 AWS 账户中的资源和流程所需的权限。如果您从 AWS Marketplace 部署控制台代理、手动安装控制台代理，或者"向控制台代理添加更多 AWS 凭证"。您还需要确保策略是最新的，因为后续版本中会添加新的权限。	"控制台代理的 AWS 权限"

NetApp备份和恢复

目标	描述	链路
使用NetApp备份和恢复将本地ONTAP集群备份到 Amazon S3	在ONTAP卷上激活备份时， NetApp Backup and Recovery 会提示您输入具有特定权限的 IAM 用户的访问密钥和密码。	"设置备份的 S3 权限"

Cloud Volumes ONTAP

目标	描述	链路
为Cloud Volumes ONTAP节点提供权限	必须将 IAM 角色附加到 AWS 中的每个Cloud Volumes ONTAP节点。对于 HA 调解员来说也是如此。默认选项是让控制台为您创建 IAM 角色，但您可以在控制台中创建系统时使用自己的角色。	"了解如何自行设置 IAM 角色"

NetApp复制和同步

目标	描述	链路
在 AWS 中部署数据代理	用于部署数据代理的 AWS 用户帐户必须具有特定权限。	"在 AWS 中部署数据代理所需的权限"
为数据经纪人提供权限	当NetApp Copy and Sync 部署数据代理时，它会为数据代理实例创建一个 IAM 角色。如果您愿意，您可以使用自己的 IAM 角色部署数据代理。	"使用您自己的 IAM 角色与 AWS 数据代理的要求"
为手动安装的数据代理启用 AWS 访问	如果您使用包含 S3 存储桶的同步关系的数据代理，那么您应该准备好 Linux 主机以供 AWS 访问。安装数据代理时，您需要为具有编程访问权限和特定权限的 IAM 用户提供 AWS 密钥。	"启用对 AWS 的访问"

适用于**ONTAP**的 **FSx**

目标	描述	链路
创建和管理 FSx for ONTAP	要创建或管理Amazon FSx for NetApp ONTAP系统，您需要通过提供 IAM 角色的 ARN（为控制台提供所需的权限）将 AWS 凭证添加到控制台。	"了解如何为 FSx 设置 AWS 凭证"

NetApp云分层

目标	描述	链路
将本地ONTAP集群分层到 Amazon S3	当您启用NetApp Cloud Tiering 到 AWS 时，向导会提示您输入访问密钥和密钥。这些凭证被传递到ONTAP集群，以便ONTAP可以将数据分层到 S3 存储桶。	"设置 S3 分层权限"

Azure 权限

控制台需要控制台代理和各个服务的 Azure 权限。

控制台代理

目标	描述	链路
从控制台部署控制台代理	从控制台部署控制台代理时，您需要使用具有在 Azure 中部署控制台代理 VM 的权限的 Azure 帐户或服务主体。	"设置 Azure 权限"

目标	描述	链路
为控制台代理提供权限	当控制台在 Azure 中部署控制台代理 VM 时，它会创建一个自定义角色，该角色提供管理该 Azure 订阅中的资源和流程所需的权限。 如果您从市场启动控制台代理，如果您手动安装控制台代理，或者如果您"向控制台代理添加更多 Azure 凭据"。 您还需要确保策略是最新的，因为后续版本中会添加新的权限。	"控制台代理的 Azure 权限"

NetApp备份和恢复

目标	描述	链路
将Cloud Volumes ONTAP备份到 Azure Blob 存储	使用NetApp Backup and Recovery 备份Cloud Volumes ONTAP 时，您需要在以下情况下向控制台代理添加权限： • 您想使用“搜索和恢复”功能 • 您想要使用客户管理的加密密钥 (CMEK)	• "使用备份和恢复将Cloud Volumes ONTAP 数据备份到 Azure Blob 存储"
将本地ONTAP集群备份到 Azure Blob 存储	使用NetApp Backup and Recovery 备份本地 ONTAP 集群时，您需要向控制台代理添加权限才能使用“搜索和恢复”功能。	"使用备份和恢复将本地ONTAP数据备份到 Azure Blob 存储"

NetApp复制和同步

目标	描述	链路
在 Azure 中部署数据代理	用于部署数据代理的 Azure 用户帐户必须具有所需的权限。	"在 Azure 中部署数据代理所需的权限"

Google Cloud 权限

控制台需要控制台代理和各个服务的 Google Cloud 权限。

控制台代理

目标	描述	链路
从控制台部署控制台代理	从控制台部署控制台代理的 Google Cloud 用户需要特定权限才能在 Google Cloud 中部署控制台代理。	"设置权限以创建控制台代理"
为控制台代理提供权限	控制台代理 VM 实例的服务帐户必须具有日常操作的特定权限。您需要在部署期间将服务帐户与控制台代理关联。您还需要确保策略是最新的，因为后续版本中会添加新的权限。	"设置控制台代理的权限"

NetApp备份和恢复

目标	描述	链路
将Cloud Volumes ONTAP备份到Google Cloud	使用NetApp Backup and Recovery 备份Cloud Volumes ONTAP时，您需要在以下情况下向控制台代理添加权限： • 您想使用“搜索和恢复”功能 • 您想要使用客户管理的加密密钥 (CMEK)	• "使用备份和恢复将Cloud Volumes ONTAP数据备份到Google Cloud Storage" • "CMEK 的权限"
将本地ONTAP集群备份到 Google Cloud	使用NetApp Backup and Recovery 备份本地 ONTAP 集群时，您需要向控制台代理添加权限才能使用“搜索和恢复”功能。	"使用备份和恢复将本地ONTAP数据备份到 Google Cloud Storage"

NetApp复制和同步

目标	描述	链路
在 Google Cloud 中部署数据代理	确保部署数据代理的 Google Cloud 用户具有所需的权限。	"在 Google Cloud 中部署数据代理所需的权限"
为手动安装的数据代理启用 Google Cloud 访问权限	如果您计划使用包含 Google Cloud Storage 存储桶的同步关系的数据代理，那么您应该准备 Linux 主机以供 Google Cloud 访问。安装数据代理时，您需要为具有特定权限的服务帐户提供密钥。	"启用对 Google Cloud 的访问"

StorageGRID权限

控制台需要两项服务的StorageGRID权限。

NetApp备份和恢复

目标	描述	链路
将本地ONTAP集群备份到StorageGRID	当您准备将StorageGRID作为ONTAP集群的备份目标时， NetApp Backup and Recovery 会提示您输入具有特定权限的 IAM 用户的访问密钥和密码。	"准备StorageGRID作为备份目标"

NetApp云分层

目标	描述	链路
将本地ONTAP集群分层到StorageGRID	当您将NetApp Cloud Tiering 设置为StorageGRID时，您需要向 Cloud Tiering 提供 S3 访问密钥和密钥。云分层使用密钥来访问您的存储桶。	"准备分层到StorageGRID"

控制台代理的 **AWS** 权限

当NetApp控制台在 AWS 中启动控制台代理实例时，它会将一个策略附加到该实例，该策略为代理提供管理该 AWS 帐户内的资源和流程的权限。代理使用权限对多个 AWS 服务进行 API 调用，包括 EC2、S3、CloudFormation、IAM、密钥管理服务 (KMS) 等。

IAM 策略

下面提供的 IAM 策略提供了控制台代理根据您的 AWS 区域管理公共云环境内的资源和流程所需的权限。

请注意以下事项：

- 如果您直接从控制台在标准 AWS 区域中创建控制台代理，则控制台会自动将策略应用于该代理。
- 如果您从 AWS Marketplace 部署代理、在 Linux 主机上手动安装代理或者想要向控制台添加其他 AWS 凭证，则需要自行设置策略。
- 无论哪种情况，您都需要确保策略是最新的，因为在后续版本中添加了新的权限。如果需要新的权限，它们将在发行说明中列出。
- 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"
- 要查看使用这些策略的分步说明，请参阅以下页面：
  - "设置 AWS Marketplace 部署的权限"
  - "设置本地部署的权限"
  - "设置限制模式的权限"

选择您所在的地区以查看所需的政策：

标准区域

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。

政策 **#1**

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:RunInstances",
                "ec2:ModifyInstanceAttribute",
                "ec2:DescribeInstanceAttribute",
                "ec2:DescribeRouteTables",
                "ec2:DescribeImages",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DescribeVolumes",
                "ec2:ModifyVolumeAttribute",
                "ec2:CreateSecurityGroup",
                "ec2:DescribeSecurityGroups",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:CreateNetworkInterface",
                "ec2:DescribeNetworkInterfaces",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeDhcpOptions",
                "ec2:CreateSnapshot",
                "ec2:DescribeSnapshots",
                "ec2:GetConsoleOutput",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeRegions",
                "ec2:DescribeTags",
                "ec2:AssociateIamInstanceProfile",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:CreatePlacementGroup",
                "ec2:DescribeReservedInstancesOfferings",
                "ec2:AssignPrivateIpAddresses",
                "ec2:CreateRoute",
                "ec2:DescribeVpcs",
```

```
                "ec2:ReplaceRoute",
                "ec2:UnassignPrivateIpAddresses",
                "ec2:DeleteSecurityGroup",
                "ec2:DeleteNetworkInterface",
                "ec2:DeleteSnapshot",
                "ec2:DeleteTags",
                "ec2:DeleteRoute",
                "ec2:DeletePlacementGroup",
                "ec2:DescribePlacementGroups",
                "ec2:DescribeVolumesModifications",
                "ec2:ModifyVolume",
                "cloudformation:CreateStack",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackEvents",
                "cloudformation:ValidateTemplate",
                "cloudformation:DeleteStack",
                "iam:PassRole",
                "iam:CreateRole",
                "iam:PutRolePolicy",
                "iam:CreateInstanceProfile",
                "iam:AddRoleToInstanceProfile",
                "iam:RemoveRoleFromInstanceProfile",
                "iam:ListInstanceProfiles",
                "iam:DeleteRole",
                "iam:DeleteRolePolicy",
                "iam:DeleteInstanceProfile",
                "iam:GetRolePolicy",
                "iam:GetRole",
                "sts:DecodeAuthorizationMessage",
                "sts:AssumeRole",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:ListBucket",
                "s3:CreateBucket",
                "s3:GetLifecycleConfiguration",
                "s3:ListBucketVersions",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetBucketPolicy",
                "s3:GetBucketAcl",
                "s3:PutObjectTagging",
                "s3:GetObjectTagging",
                "s3:DeleteObject",
                "s3:DeleteObjectVersion",
                "s3:PutObject",
                "s3:ListAllMyBuckets",
```

```
                "s3:GetObject",
                "s3:GetEncryptionConfiguration",
                "kms:List*",
                "kms:ReEncrypt*",
                "kms:Describe*",
                "kms:CreateGrant",
                "fsx:Describe*",
                "fsx:List*",
                "kms:GenerateDataKeyWithoutPlaintext"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "cvoServicePolicy"
        },
        {
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:RunInstances",
                "ec2:TerminateInstances",
                "ec2:DescribeInstanceAttribute",
                "ec2:DescribeImages",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:CreateSecurityGroup",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeRegions",
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStacks",
                "kms:List*",
                "kms:Describe*",
                "ec2:DescribeVpcEndpoints",
                "kms:ListAliases",
                "athena:StartQueryExecution",
                "athena:GetQueryResults",
                "athena:GetQueryExecution",
                "glue:GetDatabase",
                "glue:GetTable",
                "glue:CreateTable",
                "glue:CreateDatabase",
                "glue:GetPartitions",
                "glue:BatchCreatePartition",
```

```
                "glue:BatchDeletePartition"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "backupPolicy"
        },
        {
            "Action": [
                "s3:GetBucketLocation",
                "s3:ListAllMyBuckets",
                "s3:ListBucket",
                "s3:CreateBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions",
                "s3:GetBucketAcl",
                "s3:PutBucketPublicAccessBlock",
                "s3:GetObject",
                "s3:PutEncryptionConfiguration",
                "s3:DeleteObject",
                "s3:DeleteObjectVersion",
                "s3:ListBucketMultipartUploads",
                "s3:PutObject",
                "s3:PutBucketAcl",
                "s3:AbortMultipartUpload",
                "s3:ListMultipartUploadParts",
                "s3:DeleteBucket",
                "s3:GetObjectVersionTagging",
                "s3:GetObjectVersionAcl",
                "s3:GetObjectRetention",
                "s3:GetObjectTagging",
                "s3:GetObjectVersion",
                "s3:PutObjectVersionTagging",
                "s3:PutObjectRetention",
                "s3:DeleteObjectTagging",
                "s3:DeleteObjectVersionTagging",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetBucketVersioning",
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutBucketVersioning",
                "s3:BypassGovernanceRetention",
                "s3:PutBucketPolicy",
                "s3:PutBucketOwnershipControls"
            ],
            "Resource": [
```

```
                "arn:aws:s3:::netapp-backup-*"
            ],
            "Effect": "Allow",
            "Sid": "backupS3Policy"
        },
        {
            "Action": [
                "s3:CreateBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "s3:PutBucketPublicAccessBlock",
                "s3:DeleteBucket"
            ],
            "Resource": [
                "arn:aws:s3:::fabric-pool*"
            ],
            "Effect": "Allow",
            "Sid": "fabricPoolS3Policy"
        },
        {
            "Action": [
                "ec2:DescribeRegions"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "fabricPoolPolicy"
        },
        {
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/netapp-adc-manager": "*"
                }
            },
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:instance/*"
```

```
            ],
            "Effect": "Allow"
        },
        {
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/WorkingEnvironment": "*"
                }
            },
            "Action": [
                "ec2:StartInstances",
                "ec2:TerminateInstances",
                "ec2:AttachVolume",
                "ec2:DetachVolume",
                "ec2:StopInstances",
                "ec2:DeleteVolume"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:instance/*"
            ],
            "Effect": "Allow"
        },
        {
            "Action": [
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:volume/*"
            ],
            "Effect": "Allow"
        },
        {
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/WorkingEnvironment": "*"
                }
            },
            "Action": [
                "ec2:DeleteVolume"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:volume/*"
            ],
            "Effect": "Allow"
        }
```

```
    ]
}
```

政策 **#2**

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:CreateTags",
                "ec2:DeleteTags",
                "ec2:DescribeTags",
                "tag:getResources",
                "tag:getTagKeys",
                "tag:getTagValues",
                "tag:TagResources",
                "tag:UntagResources"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "tagServicePolicy"
        }
    ]
}
```

GovCloud（美国）区域

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iam:ListInstanceProfiles",
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:PutRolePolicy",
                "iam:CreateInstanceProfile",
                "iam:DeleteRolePolicy",
                "iam:AddRoleToInstanceProfile",
                "iam:RemoveRoleFromInstanceProfile",
                "iam:DeleteInstanceProfile",
                "ec2:ModifyVolumeAttribute",
                "sts:DecodeAuthorizationMessage",
                "ec2:DescribeImages",
                "ec2:DescribeRouteTables",
                "ec2:DescribeInstances",
                "iam:PassRole",
                "ec2:DescribeInstanceStatus",
                "ec2:RunInstances",
                "ec2:ModifyInstanceAttribute",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DescribeVolumes",
                "ec2:DeleteVolume",
                "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:CreateSnapshot",
```

```
                "ec2:DeleteSnapshot",
                "ec2:DescribeSnapshots",
                "ec2:StopInstances",
                "ec2:GetConsoleOutput",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeRegions",
                "ec2:DeleteTags",
                "ec2:DescribeTags",
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackEvents",
                "cloudformation:ValidateTemplate",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:ListAllMyBuckets",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:CreateBucket",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "kms:List*",
                "kms:ReEncrypt*",
                "kms:Describe*",
                "kms:CreateGrant",
                "ec2:AssociateIamInstanceProfile",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:DescribeInstanceAttribute",
                "ec2:CreatePlacementGroup",
                "ec2:DeletePlacementGroup"
            ],
            "Resource": "*"
        },
        {
            "Sid": "fabricPoolPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions",
                "s3:GetBucketPolicyStatus",
```

```
                "s3:GetBucketPublicAccessBlock",
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "s3:PutBucketPublicAccessBlock"
            ],
            "Resource": [
                "arn:aws-us-gov:s3:::fabric-pool*"
            ]
        },
        {
            "Sid": "backupPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:ListAllMyBuckets",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "s3:PutBucketPublicAccessBlock"
            ],
            "Resource": [
                "arn:aws-us-gov:s3:::netapp-backup-*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:TerminateInstances",
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/WorkingEnvironment": "*"
                }
            },
```

```
            "Resource": [
                "arn:aws-us-gov:ec2:*:*:instance/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws-us-gov:ec2:*:*:volume/*"
            ]
        }
    ]
}
```

秘密区域

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:RunInstances",
                "ec2:ModifyInstanceAttribute",
                "ec2:DescribeRouteTables",
                "ec2:DescribeImages",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DescribeVolumes",
                "ec2:ModifyVolumeAttribute",
                "ec2:DeleteVolume",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:DescribeSecurityGroups",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateNetworkInterface",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DeleteNetworkInterface",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeDhcpOptions",
                "ec2:CreateSnapshot",
                "ec2:DeleteSnapshot",
                "ec2:DescribeSnapshots",
                "ec2:GetConsoleOutput",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeRegions",
                "ec2:DeleteTags",
                "ec2:DescribeTags",
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackEvents",
                "cloudformation:ValidateTemplate",
```

```
                "iam:PassRole",
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:PutRolePolicy",
                "iam:CreateInstanceProfile",
                "iam:DeleteRolePolicy",
                "iam:AddRoleToInstanceProfile",
                "iam:RemoveRoleFromInstanceProfile",
                "iam:DeleteInstanceProfile",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:ListAllMyBuckets",
                "kms:List*",
                "kms:Describe*",
                "ec2:AssociateIamInstanceProfile",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:DescribeInstanceAttribute",
                "ec2:CreatePlacementGroup",
                "ec2:DeletePlacementGroup",
                "iam:ListinstanceProfiles"
            ],
            "Resource": "*"
        },
        {
            "Sid": "fabricPoolPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions"
            ],
            "Resource": [
                "arn:aws-iso-b:s3:::fabric-pool*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances",
```

```
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/WorkingEnvironment": "*"
                }
            },
            "Resource": [
                "arn:aws-iso-b:ec2:*:*:instance/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws-iso-b:ec2:*:*:volume/*"
            ]
        }
    ]
}
```

绝密地区

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:RunInstances",
                "ec2:ModifyInstanceAttribute",
                "ec2:DescribeRouteTables",
                "ec2:DescribeImages",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DescribeVolumes",
                "ec2:ModifyVolumeAttribute",
                "ec2:DeleteVolume",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:DescribeSecurityGroups",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateNetworkInterface",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DeleteNetworkInterface",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeDhcpOptions",
                "ec2:CreateSnapshot",
                "ec2:DeleteSnapshot",
                "ec2:DescribeSnapshots",
                "ec2:GetConsoleOutput",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeRegions",
                "ec2:DeleteTags",
                "ec2:DescribeTags",
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackEvents",
                "cloudformation:ValidateTemplate",
```

```
                "iam:PassRole",
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:PutRolePolicy",
                "iam:CreateInstanceProfile",
                "iam:DeleteRolePolicy",
                "iam:AddRoleToInstanceProfile",
                "iam:RemoveRoleFromInstanceProfile",
                "iam:DeleteInstanceProfile",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:ListAllMyBuckets",
                "kms:List*",
                "kms:Describe*",
                "ec2:AssociateIamInstanceProfile",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:DescribeInstanceAttribute",
                "ec2:CreatePlacementGroup",
                "ec2:DeletePlacementGroup",
                "iam:ListinstanceProfiles"
            ],
            "Resource": "*"
        },
        {
            "Sid": "fabricPoolPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions"
            ],
            "Resource": [
                "arn:aws-iso:s3:::fabric-pool*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances",
```

```
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/WorkingEnvironment": "*"
                }
            },
            "Resource": [
                "arn:aws-iso:ec2:*:*:instance/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws-iso:ec2:*:*:volume/*"
            ]
        }
    ]
}
```

如何使用 **AWS** 权限

以下部分介绍了如何使用每个NetApp控制台管理或数据服务的权限。如果您的公司政策规定仅在需要时提供权限，则此信息会很有帮助。

适用于**ONTAP** 的**Amazon FSx**

控制台代理发出以下 API 请求来管理Amazon FSx for ONTAP文件系统：

- ec2:描述实例
- ec2：描述实例状态
- ec2:描述实例属性
- ec2:描述路由表
- ec2:描述图像
- ec2:创建标签
- ec2:描述卷
- ec2:描述安全组
- ec2:描述网络接口

- ec2:描述子网
- ec2:描述Vpcs
- ec2:描述DHCP选项
- ec2:描述快照
- ec2:描述密钥对
- ec2:描述区域
- ec2:描述标签
- ec2：描述IamInstanceProfileAssociations
- ec2:描述预留实例产品
- ec2:描述Vpc端点
- ec2:描述Vpcs
- ec2：描述卷修改
- ec2:描述放置组
- kms:列表*
- kms:描述*
- kms:创建授权
- kms：列出别名
- fsx:描述*
- fsx:列表*

Amazon S3 存储桶发现

控制台代理发出以下 API 请求来发现 Amazon S3 存储桶：

s3:获取加密配置

NetApp备份和恢复

该代理发出以下 API 请求来管理 Amazon S3 中的备份：

- s3：获取存储桶位置
- s3：列出所有我的存储桶
- s3：列表桶
- s3：创建桶
- s3:获取生命周期配置
- s3：PutLifecycle配置
- s3：PutBucket标记
- s3：列出存储桶版本

- s3：获取存储桶Acl
- s3：PutBucket公共访问块
- kms:列表*
- kms:描述*
- s3：获取对象
- ec2:描述Vpc端点
- kms：列出别名
- s3：PutEncryption配置

当您使用搜索和还原方法还原卷和文件时，代理会发出以下 API 请求：

- s3：创建桶
- s3：删除对象
- s3：删除对象版本
- s3：获取存储桶Acl
- s3：列表桶
- s3：列出存储桶版本
- s3：列出桶多部分上传
- s3：Put对象
- s3:PutBucketAcl
- s3：PutLifecycle配置
- s3：PutBucket公共访问块
- s3：中止分段上传
- s3:列出多部分上传部分
- athena：开始查询执行
- 雅典娜：获取查询结果
- 雅典娜：获取查询执行
- athena：停止查询执行
- 胶水：创建数据库
- 胶水：创建表
- 胶水：批量删除分区

当您使用 DataLock 和NetApp Ransomware Resilience 进行卷备份时，代理会发出以下 API 请求：

- s3:获取对象版本标记
- s3：获取存储桶对象锁配置
- s3:获取对象版本Acl

- s3：PutObjectTagging
- s3：删除对象
- s3：删除对象标记
- s3：获取对象保留
- s3：删除对象版本标记
- s3：Put对象
- s3：获取对象
- s3:PutBucketObjectLock配置
- s3:获取生命周期配置
- s3：按标签列出存储桶
- s3：获取存储桶标记
- s3：删除对象版本
- s3：列出存储桶版本
- s3：列表桶
- s3：PutBucket标记
- s3:获取对象标记
- s3：PutBucket版本控制
- s3：PutObjectVersionTagging
- s3：获取存储桶版本
- s3：获取存储桶Acl
- s3：绕过治理保留
- s3：PutObjectRetention
- s3：获取存储桶位置
- s3：获取对象版本

如果您对Cloud Volumes ONTAP备份使用的 AWS 账户与对源卷使用的账户不同，则代理会发出以下 API 请求：

- s3：PutBucket策略
- s3：PutBucket所有权控制

分类

代理发出以下 API 请求来部署NetApp数据分类：

- ec2:描述实例
- ec2：描述实例状态
- ec2：运行实例

- ec2：终止实例
- ec2:创建标签
- ec2：创建卷
- ec2：附加卷
- ec2：创建安全组
- ec2：删除安全组
- ec2:描述安全组
- ec2:创建网络接口
- ec2:描述网络接口
- ec2:删除网络接口
- ec2:描述子网
- ec2:描述Vpcs
- ec2：创建快照
- ec2:描述区域
- cloudformation:创建堆栈
- cloudformation:删除堆栈
- cloudformation:描述堆栈
- cloudformation：描述堆栈事件
- iam:添加角色到实例配置文件
- ec2:AssociateIamInstanceProfile
- ec2：描述IamInstanceProfileAssociations

当您使用NetApp数据分类时，代理会发出以下 API 请求来扫描 S3 存储桶：

- iam:添加角色到实例配置文件
- ec2:AssociateIamInstanceProfile
- ec2：描述IamInstanceProfileAssociations
- s3：获取存储桶标记
- s3：获取存储桶位置
- s3：列出所有我的存储桶
- s3：列表桶
- s3：获取存储桶策略状态
- s3：获取存储桶策略
- s3：获取存储桶Acl
- s3：获取对象
- iam：获取角色

- s3：删除对象
- s3：删除对象版本
- s3：Put对象
- sts：AssumeRole

Cloud Volumes ONTAP

该代理发出以下 API 请求以在 AWS 中部署和管理Cloud Volumes ONTAP 。

目的	操作	用于部署?	用于日常运营?	用于删除?
为Cloud Volumes ONTAP实例创建和管理 IAM 角色和实例配置文件	iam:列出实例配置文件	是	是	否
	iam：创建角色	是	否	否
	iam：删除角色	否	是	是
	iam:PutRolePolicy	是	否	否
	iam:创建实例配置文件	是	否	否
	iam:删除角色策略	否	是	是
	iam:添加角色到实例配置文件	是	否	否
	iam:从实例配置文件中删除角色	否	是	是
	iam:删除实例配置文件	否	是	是
	iam：PassRole	是	否	否
	ec2:AssociateIamInstanceProfile	是	是	否
	ec2：描述IamInstanceProfileAssociations	是	是	否
	ec2：解除关联IamInstanceProfile	否	是	否
解码授权状态消息	sts：解码授权消息	是	是	否
描述账户可用的指定镜像（AMI）	ec2:描述图像	是	是	否
描述 VPC 中的路由表（仅 HA 对需要）	ec2:描述路由表	是	否	否

目的	操作	用于部署?	用于日常运营?	用于删除?
停止、启动和监控实例	ec2：启动实例	是	是	否
	ec2：停止实例	是	是	否
	ec2:描述实例	是	是	否
	ec2：描述实例状态	是	是	否
	ec2：运行实例	是	否	否
	ec2：终止实例	否	否	是
	ec2:修改实例属性	否	是	否
验证是否为受支持的实例类型启用了增强联网	ec2:描述实例属性	否	是	否
使用“WorkingEnvironment”和“WorkingEnvironmentId”标签标记资源，用于维护和成本分配	ec2:创建标签	是	是	否
管理Cloud Volumes ONTAP用作后端存储的 EBS 卷	ec2：创建卷	是	是	否
	ec2:描述卷	是	是	是
	ec2:修改卷属性	否	是	是
	ec2：附加卷	是	是	否
	ec2：删除卷	否	是	是
	ec2：分离卷	否	是	是
为Cloud Volumes ONTAP创建和管理安全组	ec2：创建安全组	是	否	否
	ec2：删除安全组	否	是	是
	ec2:描述安全组	是	是	是
	ec2：撤销安全组出口	是	否	否
	ec2：授权安全组出口	是	否	否
	ec2：授权安全组入口	是	否	否
	ec2：撤销安全组入口	是	是	否

目的	操作	用于部署?	用于日常运营?	用于删除?
在目标子网中创建和管理Cloud Volumes ONTAP的网络接口	ec2:创建网络接口	是	否	否
	ec2:描述网络接口	是	是	否
	ec2:删除网络接口	否	是	是
	ec2:修改网络接口属性	否	是	否
获取目标子网和安全组列表	ec2:描述子网	是	是	否
	ec2:描述Vpcs	是	是	否
获取Cloud Volumes ONTAP实例的 DNS 服务器和默认域名	ec2:描述DHCP选项	是	否	否
为Cloud Volumes ONTAP拍摄 EBS 卷快照	ec2：创建快照	是	是	否
	ec2：删除快照	否	是	是
	ec2:描述快照	否	是	否
捕获Cloud Volumes ONTAP控制台，该控制台附加到AutoSupport消息	ec2：获取控制台输出	是	是	否
获取可用密钥对列表	ec2:描述密钥对	是	否	否
获取可用 AWS 区域列表	ec2:描述区域	是	是	否
管理与Cloud Volumes ONTAP实例关联的资源的标签	ec2:删除标签	否	是	是
	ec2:描述标签	否	是	否
创建和管理 AWS CloudFormation 模板的堆栈	cloudformation:创建堆栈	是	否	否
	cloudformation:删除堆栈	是	否	否
	cloudformation:描述堆栈	是	是	否
	cloudformation：描述堆栈事件	是	否	否
	云信息：验证模板	是	否	否

目的	操作	用于部署?	用于日常运营?	用于删除?
创建和管理Cloud Volumes ONTAP系统用作数据分层容量层的 S3 存储桶	s3：创建桶	是	是	否
	s3：删除桶	否	是	是
	s3:获取生命周期配置	否	是	否
	s3：PutLifecycle配置	否	是	否
	s3：PutBucket标记	否	是	否
	s3：列出存储桶版本	否	是	否
	s3：获取存储桶策略状态	否	是	否
	s3：获取存储桶公共访问块	否	是	否
	s3：获取存储桶Acl	否	是	否
	s3：获取存储桶策略	否	是	否
	s3：PutBucket公共访问块	否	是	否
	s3：获取存储桶标记	否	是	否
	s3：获取存储桶位置	否	是	否
	s3：列出所有我的存储桶	否	否	否
	s3：列表桶	否	是	否
使用 AWS 密钥管理服务 (KMS) 启用Cloud Volumes ONTAP的数据加密	kms:列表*	是	是	否
	kms:重新加密*	是	否	否
	kms:描述*	是	是	否
	kms:创建授权	是	是	否
	kms:生成不带明文的数据密钥	是	是	否
在单个 AWS 可用区中为两个 HA 节点和中介器创建和管理 AWS 扩展置放群组	ec2:创建放置组	是	否	否
	ec2:删除放置组	否	是	是
创建报告	fsx:描述*	否	是	否
	fsx:列表*	否	是	否
创建和管理支持 Amazon EBS 弹性卷功能的聚合	ec2：描述卷修改	否	是	否
	ec2：修改卷	否	是	否

目的	操作	用于部署?	用于日常运营?	用于删除?
检查可用区是否为 AWS 本地区域，并验证所有部署参数是否兼容	ec2：描述可用区域	是	否	是

更改日志

当添加和删除权限时，我们会在下面的部分中注明。

2024年**9**月**9**日

由于NetApp控制台不再支持NetApp边缘缓存以及 Kubernetes 集群的发现和管理，因此从标准区域的策略 #2 中删除了权限。

查看从策略中删除的权限

```
        {
            "Action": [
                "ec2:DescribeRegions",
                "eks:ListClusters",
                "eks:DescribeCluster",
                "iam:GetInstanceProfile"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "K8sServicePolicy"
        },
        {
            "Action": [
                "cloudformation:DescribeStacks",
                "cloudwatch:GetMetricStatistics",
                "cloudformation:ListStacks"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "GFCservicePolicy"
        },
        {
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/GFCInstance": "*"
                }
            },
            "Action": [
                "ec2:StartInstances",
                "ec2:TerminateInstances",
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:instance/*"
            ],
            "Effect": "Allow"
        },
```

2024年5月9日

Cloud Volumes ONTAP现在需要以下权限：

ec2：描述可用区域

2023年6月6日

Cloud Volumes ONTAP现在需要以下权限：

kms:生成不带明文的数据密钥

2023年2月14日

NetApp Cloud Tiering 现在需要以下权限：

ec2:描述Vpc端点

控制台代理的 **Azure** 权限

当NetApp控制台在 Azure 中启动控制台代理时，它会将一个自定义角色附加到 VM，该 VM 为代理提供管理该 Azure 订阅中的资源和流程的权限。代理使用权限对多个 Azure 服务进行 API 调用。

是否需要为代理创建此自定义角色取决于您如何部署它。

从**NetApp**控制台部署

当您使用控制台在 Azure 中部署代理虚拟机时，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。当代理升级时，角色的权限保持最新。您不需要为代理创建此角色或管理更新。

手动部署或从 **Azure** 市场部署

当您从 Azure 市场部署代理或在 Linux 主机上手动安装代理时，您需要自行设置自定义角色并在任何更改时维护其权限。

您需要确保角色是最新的，因为后续版本中会添加新的权限。如果需要新的权限，它们将在发行说明中列出。

- 要查看使用这些策略的分步说明，请参阅以下页面：
  - "设置 Azure 市场部署的权限"
  - "设置本地部署的权限"
  - "设置限制模式的权限"

```
{
    "Name": "Console Operator",
    "Actions": [
                    "Microsoft.Compute/disks/delete",
                    "Microsoft.Compute/disks/read",
                    "Microsoft.Compute/disks/write",
                    "Microsoft.Compute/locations/operations/read",
                    "Microsoft.Compute/locations/vmSizes/read",
                    "Microsoft.Resources/subscriptions/locations/read",
                    "Microsoft.Compute/operations/read",
```

```
                    "Microsoft.Compute/virtualMachines/instanceView/read",
                    "Microsoft.Compute/virtualMachines/powerOff/action",
                    "Microsoft.Compute/virtualMachines/read",
                    "Microsoft.Compute/virtualMachines/restart/action",
                    "Microsoft.Compute/virtualMachines/deallocate/action",
                    "Microsoft.Compute/virtualMachines/start/action",
                    "Microsoft.Compute/virtualMachines/vmSizes/read",
                    "Microsoft.Compute/virtualMachines/write",
                    "Microsoft.Compute/images/read",
                    "Microsoft.Network/locations/operationResults/read",
                    "Microsoft.Network/locations/operations/read",
                    "Microsoft.Network/networkInterfaces/read",
                    "Microsoft.Network/networkInterfaces/write",
                    "Microsoft.Network/networkInterfaces/join/action",
                    "Microsoft.Network/networkSecurityGroups/read",
                    "Microsoft.Network/networkSecurityGroups/write",
                    "Microsoft.Network/networkSecurityGroups/join/action",
                    "Microsoft.Network/virtualNetworks/read",

"Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read",
                    "Microsoft.Network/virtualNetworks/subnets/read",
                    "Microsoft.Network/virtualNetworks/subnets/write",

"Microsoft.Network/virtualNetworks/subnets/virtualMachines/read",

"Microsoft.Network/virtualNetworks/virtualMachines/read",

"Microsoft.Network/virtualNetworks/subnets/join/action",
                    "Microsoft.Resources/deployments/operations/read",
                    "Microsoft.Resources/deployments/read",
                    "Microsoft.Resources/deployments/write",
                    "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.Storage/checknameavailability/read",
                    "Microsoft.Storage/operations/read",
                    "Microsoft.Storage/storageAccounts/listkeys/action",
                    "Microsoft.Storage/storageAccounts/read",
```

```
                    "Microsoft.Storage/storageAccounts/delete",
                    "Microsoft.Storage/storageAccounts/write",

"Microsoft.Storage/storageAccounts/blobServices/containers/read",

"Microsoft.Storage/storageAccounts/listAccountSas/action",
                    "Microsoft.Storage/usages/read",
                    "Microsoft.Compute/snapshots/write",
                    "Microsoft.Compute/snapshots/read",
                    "Microsoft.Compute/availabilitySets/write",
                    "Microsoft.Compute/availabilitySets/read",
                    "Microsoft.Compute/disks/beginGetAccess/action",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreemen
ts/read",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreemen
ts/write",
                    "Microsoft.Network/loadBalancers/read",
                    "Microsoft.Network/loadBalancers/write",
                    "Microsoft.Network/loadBalancers/delete",

"Microsoft.Network/loadBalancers/backendAddressPools/read",

"Microsoft.Network/loadBalancers/backendAddressPools/join/action",

"Microsoft.Network/loadBalancers/loadBalancingRules/read",
                    "Microsoft.Network/loadBalancers/probes/read",
                    "Microsoft.Network/loadBalancers/probes/join/action",
                    "Microsoft.Authorization/locks/*",
                    "Microsoft.Network/routeTables/join/action",
                    "Microsoft.NetApp/netAppAccounts/read",
                    "Microsoft.NetApp/netAppAccounts/capacityPools/read",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/write",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/read",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/delete",
                    "Microsoft.Network/privateEndpoints/write",

"Microsoft.Storage/storageAccounts/PrivateEndpointConnectionsApproval/acti
on",

"Microsoft.Storage/storageAccounts/privateEndpointConnections/read",
```

```
"Microsoft.Storage/storageAccounts/managementPolicies/read",

"Microsoft.Storage/storageAccounts/managementPolicies/write",
                    "Microsoft.Network/privateEndpoints/read",
                    "Microsoft.Network/privateDnsZones/write",

"Microsoft.Network/privateDnsZones/virtualNetworkLinks/write",
                    "Microsoft.Network/virtualNetworks/join/action",
                    "Microsoft.Network/privateDnsZones/A/write",
                    "Microsoft.Network/privateDnsZones/read",

"Microsoft.Network/privateDnsZones/virtualNetworkLinks/read",

"Microsoft.Resources/deployments/operationStatuses/read",
                    "Microsoft.Insights/Metrics/Read",
                    "Microsoft.Compute/virtualMachines/extensions/write",
                    "Microsoft.Compute/virtualMachines/extensions/delete",
                    "Microsoft.Compute/virtualMachines/extensions/read",
                    "Microsoft.Compute/virtualMachines/delete",
                    "Microsoft.Network/networkInterfaces/delete",
                    "Microsoft.Network/networkSecurityGroups/delete",
                    "Microsoft.Resources/deployments/delete",
                    "Microsoft.Compute/diskEncryptionSets/read",
                    "Microsoft.Compute/snapshots/delete",
                    "Microsoft.Network/privateEndpoints/delete",
                    "Microsoft.Compute/availabilitySets/delete",
                    "Microsoft.KeyVault/vaults/read",
                    "Microsoft.KeyVault/vaults/accessPolicies/write",
                    "Microsoft.Compute/diskEncryptionSets/write",
                    "Microsoft.KeyVault/vaults/deploy/action",
                    "Microsoft.Compute/diskEncryptionSets/delete",
                    "Microsoft.Resources/tags/read",
                    "Microsoft.Resources/tags/write",
                    "Microsoft.Resources/tags/delete",
                    "Microsoft.Network/applicationSecurityGroups/write",
                    "Microsoft.Network/applicationSecurityGroups/read",

"Microsoft.Network/applicationSecurityGroups/joinIpConfiguration/action",

"Microsoft.Network/networkSecurityGroups/securityRules/write",
                    "Microsoft.Network/applicationSecurityGroups/delete",

"Microsoft.Network/networkSecurityGroups/securityRules/delete",
                    "Microsoft.Synapse/workspaces/write",
                    "Microsoft.Synapse/workspaces/read",
                    "Microsoft.Synapse/workspaces/delete",
```

```
                    "Microsoft.Synapse/register/action",
                    "Microsoft.Synapse/checkNameAvailability/action",
                    "Microsoft.Synapse/workspaces/operationStatuses/read",
                    "Microsoft.Synapse/workspaces/firewallRules/read",

"Microsoft.Synapse/workspaces/replaceAllIpFirewallRules/action",
                    "Microsoft.Synapse/workspaces/operationResults/read",

"Microsoft.Synapse/workspaces/privateEndpointConnectionsApproval/action",

"Microsoft.ManagedIdentity/userAssignedIdentities/assign/action",
                    "Microsoft.Compute/images/write",

"Microsoft.Network/loadBalancers/frontendIPConfigurations/read",
                    "Microsoft.Compute/virtualMachineScaleSets/write",
                    "Microsoft.Compute/virtualMachineScaleSets/read",
                    "Microsoft.Compute/virtualMachineScaleSets/delete"
    ],
    "NotActions": [],
    "AssignableScopes": [],
    "Description": "Console Permissions",
    "IsCustom": "true"
}
```

如何使用 **Azure** 权限

以下部分介绍了如何对每个NetApp存储系统和数据服务使用权限。如果您的公司政策规定仅在需要时提供权限，则此信息会很有帮助。

Azure NetApp Files

当您使用NetApp数据分类扫描Azure NetApp Files数据时，代理会发出以下 API 请求：

- NetApp。NetApp /netAppAccounts/read
- NetApp。NetApp /netAppAccounts/capacityPools/read
- NetApp/netAppAccounts/capacityPools/volumes/write
- NetApp/netAppAccounts/capacityPools/volumes/read
- NetApp/netAppAccounts/capacityPools/volumes/delete

NetApp备份和恢复

控制台代理对NetApp备份和恢复发出以下 API 请求：

- Microsoft.Storage/storageAccounts/listkeys/action
- Microsoft.Storage/storageAccounts/读取
- Microsoft.Storage/storageAccounts/write

- Microsoft.Storage/storageAccounts/blobServices/containers/read
- Microsoft.Storage/storageAccounts/listAccountSas/action
- Microsoft.KeyVault/保管库/读取
- Microsoft.KeyVault/保管库/访问策略/写入
- Microsoft.Network/网络接口/读取
- Microsoft.Resources/订阅/位置/读取
- Microsoft.Network/virtualNetworks/读取
- Microsoft.Network/virtualNetworks/子网/读取
- Microsoft.Resources/订阅/资源组/读取
- Microsoft.Resources/订阅/资源组/资源/读取
- Microsoft.Resources/订阅/资源组/写入
- Microsoft.授权/锁/*
- Microsoft.Network/privateEndpoints/写入
- Microsoft.Network/privateEndpoints/读取
- Microsoft.Network/privateDnsZones/virtualNetworkLinks/写入
- Microsoft.Network/virtualNetworks/join/action
- Microsoft.Network/privateDnsZones/A/写入
- Microsoft.Network/privateDnsZones/读取
- Microsoft.Network/privateDnsZones/virtualNetworkLinks/读取
- Microsoft.Network/networkInterfaces/删除
- Microsoft.Network/networkSecurityGroups/删除
- Microsoft.Resources/部署/删除
- Microsoft.ManagedIdentity/userAssignedIdentities/分配/操作

当您使用搜索和恢复功能时，代理会发出以下 API 请求：

- Microsoft.Synapse/工作区/写入
- Microsoft.Synapse/工作区/读取
- Microsoft.Synapse/工作区/删除
- Microsoft.Synapse/注册/操作
- Microsoft.Synapse/checkNameAvailability/操作
- Microsoft.Synapse/工作区/operationStatuses/读取
- Microsoft.Synapse/工作区/防火墙规则/读取
- Microsoft.Synapse/工作区/replaceAllIpFirewallRules/操作
- Microsoft.Synapse/工作区/操作结果/读取
- Microsoft.Synapse/工作区/privateEndpointConnectionsApproval/操作

当您使用数据分类时，代理会发出以下 API 请求。

操作	用于设置吗?	用于日常运营?
Microsoft.Compute/位置/操作/读取	是	是
Microsoft.Compute/位置/vmSizes/读取	是	是
Microsoft.Compute/操作/读取	是	是
Microsoft.Compute/virtualMachines/instanceView/读取	是	是
Microsoft.Compute/virtualMachines/powerOff/action	是	否
Microsoft.Compute/虚拟机/读取	是	是
Microsoft.Compute/virtualMachines/重启/操作	是	否
Microsoft.Compute/virtualMachines/启动/操作	是	否
Microsoft.Compute/virtualMachines/vmSizes/读取	否	是
Microsoft.Compute/虚拟机/写入	是	否
Microsoft.Compute/图像/读取	是	是
Microsoft.Compute/磁盘/删除	是	否
Microsoft.Compute/磁盘/读取	是	是
Microsoft.Compute/磁盘/写入	是	否
Microsoft.Storage/checknameavailability/读取	是	是
Microsoft.Storage/操作/读取	是	是
Microsoft.Storage/storageAccounts/listkeys/action	是	否
Microsoft.Storage/storageAccounts/读取	是	是
Microsoft.Storage/storageAccounts/write	是	否
Microsoft.Storage/storageAccounts/blobServices/containers/read	是	是
Microsoft.Network/网络接口/读取	是	是
Microsoft.Network/networkInterfaces/写入	是	否
Microsoft.Network/networkInterfaces/join/action	是	否

操作	用于设置吗?	用于日常运营?
Microsoft.Network/networkSecurityGroups/读取	是	是
Microsoft.Network/networkSecurityGroups/写入	是	否
Microsoft.Resources/订阅/位置/读取	是	是
Microsoft.Network/locations/operationResults/read	是	是
Microsoft.Network/位置/操作/读取	是	是
Microsoft.Network/virtualNetworks/读取	是	是
Microsoft.Network/virtualNetworks/checkIpAddressAvailability/读取	是	是
Microsoft.Network/virtualNetworks/子网/读取	是	是
Microsoft.Network/virtualNetworks/子网/virtualMachines/读取	是	是
Microsoft.Network/virtualNetworks/virtualMachines/读取	是	是
Microsoft.Network/virtualNetworks/子网/加入/操作	是	否
Microsoft.Network/virtualNetworks/子网/写入	是	否
Microsoft.Network/routeTables/join/action	是	否
Microsoft.Resources/部署/操作/读取	是	是
Microsoft.Resources/部署/读取	是	是
Microsoft.Resources/部署/写入	是	否
Microsoft.Resources/资源/读取	是	是
Microsoft.Resources/subscriptions/operationresults/read	是	是
Microsoft.Resources/subscriptions/resourceGroups/delete	是	否
Microsoft.Resources/订阅/资源组/读取	是	是
Microsoft.Resources/订阅/资源组/资源/读取	是	是
Microsoft.Resources/订阅/资源组/写入	是	否

Cloud Volumes ONTAP

该代理发出以下 API 请求以在 Azure 中部署和管理Cloud Volumes ONTAP 。

目的	操作	用于部署?	用于日常运营?	用于删除?
创建和管理虚拟机	Microsoft.Compute/位置/操作/读取	是	是	否
	Microsoft.Compute/位置/vmSizes/读取	是	是	否
	Microsoft.Resources/订阅/位置/读取	是	否	否
	Microsoft.Compute/操作/读取	是	是	否
	Microsoft.Compute/virtualMachines/instanceView/读取	是	是	否
	Microsoft.Compute/virtualMachines/powerOff/action	是	是	否
	Microsoft.Compute/虚拟机/读取	是	是	否
	Microsoft.Compute/virtualMachines/重启/操作	是	是	否
	Microsoft.Compute/virtualMachines/启动/操作	是	是	否
	Microsoft.Compute/virtualMachines/解除分配/操作	否	是	是
	Microsoft.Compute/virtualMachines/vmSizes/读取	否	是	否
	Microsoft.Compute/虚拟机/写入	是	是	否
	Microsoft.Compute/virtualMachines/删除	是	是	是
	Microsoft.Resources/部署/删除	是	否	否
启用从 VHD 部署	Microsoft.Compute/图像/读取	是	否	否
	Microsoft.Compute/图像/写入	是	否	否

目的	操作	用于部署?	用于日常运营?	用于删除?
在目标子网中创建和管理网络接口	Microsoft.Network/网络接口/读取	是	是	否
	Microsoft.Network/networkInterfaces/写入	是	是	否
	Microsoft.Network/networkInterfaces/join/action	是	是	否
	Microsoft.Network/networkInterfaces/删除	是	是	否
创建和管理网络安全组	Microsoft.Network/networkSecurityGroups/读取	是	是	否
	Microsoft.Network/networkSecurityGroups/写入	是	是	否
	Microsoft.Network/networkSecurityGroups/加入/操作	是	否	否
	Microsoft.Network/networkSecurityGroups/删除	否	是	是

目的	操作	用于部署?	用于日常运营?	用于删除?
获取有关区域、目标 VNet 和子网的网络信息，并将 VM 添加到 VNet	Microsoft.Network/locations/operationResults/read	是	是	否
	Microsoft.Network/位置/操作/读取	是	是	否
	Microsoft.Network/virtualNetworks/读取	是	否	否
	Microsoft.Network/virtualNetworks/checkIpAddressAvailability/读取	是	否	否
	Microsoft.Network/virtualNetworks/子网/读取	是	是	否
	Microsoft.Network/virtualNetworks/子网/virtualMachines/读取	是	是	否
	Microsoft.Network/virtualNetworks/virtualMachines/读取	是	是	否
	Microsoft.Network/virtualNetworks/子网/加入/操作	是	是	否
创建和管理资源组	Microsoft.Resources/部署/操作/读取	是	是	否
	Microsoft.Resources/部署/读取	是	是	否
	Microsoft.Resources/部署/写入	是	是	否
	Microsoft.Resources/资源/读取	是	是	否
	Microsoft.Resources/subscriptions/operationresults/read	是	是	否
	Microsoft.Resources/subscriptions/resourceGroups/delete	是	是	是
	Microsoft.Resources/订阅/资源组/读取	否	是	否
	Microsoft.Resources/订阅/资源组/资源/读取	是	是	否
	Microsoft.Resources/订阅/资源组/写入	是	是	否

目的	操作	用于部署?	用于日常运营?	用于删除?
管理 Azure 存储帐户和磁盘	Microsoft.Compute/磁盘/读取	是	是	是
	Microsoft.Compute/磁盘/写入	是	是	否
	Microsoft.Compute/磁盘/删除	是	是	是
	Microsoft.Storage/checknameavailability/读取	是	是	否
	Microsoft.Storage/操作/读取	是	是	否
	Microsoft.Storage/storageAccounts/listkeys/action	是	是	否
	Microsoft.Storage/storageAccounts/读取	是	是	否
	Microsoft.Storage/storageAccounts/删除	否	是	是
	Microsoft.Storage/storageAccounts/write	是	是	否
	Microsoft.Storage/使用情况/读取	否	是	否
启用 Blob 存储备份和存储帐户加密	Microsoft.Storage/storageAccounts/blobServices/containers/read	是	是	否
	Microsoft.KeyVault/保管库/读取	是	是	否
	Microsoft.KeyVault/保管库/访问策略/写入	是	是	否
启用 VNet 服务终结点以进行数据分层	Microsoft.Network/virtualNetworks/子网/写入	是	是	否
	Microsoft.Network/routeTables/join/action	是	是	否

目的	操作	用于部署?	用于日常运营?	用于删除?
创建和管理 Azure 托管快照	Microsoft.Compute/快照/写入	是	是	否
	Microsoft.Compute/快照/读取	是	是	否
	Microsoft.Compute/快照/删除	否	是	是
	Microsoft.Compute/磁盘/beginGetAccess/操作	否	是	否
创建和管理可用性集	Microsoft.Compute/可用性集/写入	是	否	否
	Microsoft.Compute/可用性集/读取	是	否	否
启用来自市场的程序化部署	Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/read	是	否	否
	Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/write	是	是	否

目的	操作	用于部署?	用于日常运营?	用于删除?
管理 HA 对的负载均衡器	Microsoft.Network/loadBalancers/读取	是	是	否
	Microsoft.Network/loadBalancers/写入	是	否	否
	Microsoft.Network/loadBalancers/删除	否	是	是
	Microsoft.Network/loadBalancers/backendAddressPools/读取	是	否	否
	Microsoft.Network/loadBalancers/backendAddressPools/join/action	是	否	否
	Microsoft.Network/loadBalancers/frontendIPConfigurations/读取	是	是	否
	Microsoft.Network/loadBalancers/loadBalancingRules/读取	是	否	否
	Microsoft.Network/loadBalancers/探测/读取	是	否	否
	Microsoft.Network/loadBalancers/探测/加入/操作	是	否	否
启用 Azure 磁盘上的锁管理	Microsoft.授权/锁/*	是	是	否

目的	操作	用于部署?	用于日常运营?	用于删除?
当子网外部没有连接时，为 HA 对启用专用端点	Microsoft.Network/privateEndpoints/写入	是	是	否
	Microsoft.Storage/storageAccounts/PrivateEndpointConnectionsApproval/action	是	否	否
	Microsoft.Storage/storageAccounts/privateEndpointConnections/读取	是	是	是
	Microsoft.Network/privateEndpoints/读取	是	是	是
	Microsoft.Network/privateDnsZones/写入	是	是	否
	Microsoft.Network/privateDnsZones/virtualNetworkLinks/写入	是	是	否
	Microsoft.Network/virtualNetworks/join/action	是	是	否
	Microsoft.Network/privateDnsZones/A/写入	是	是	否
	Microsoft.Network/privateDnsZones/读取	是	是	否
	Microsoft.Network/privateDnsZones/virtualNetworkLinks/读取	是	是	否
对于某些虚拟机部署是必需的，具体取决于底层物理硬件	Microsoft.Resources/deployments/operationStatuses/read	是	是	否
在部署失败或删除的情况下从资源组中删除资源	Microsoft.Network/privateEndpoints/删除	是	是	否
	Microsoft.Compute/可用性集/删除	是	是	否

目的	操作	用于部署?	用于日常运营?	用于删除?
使用 API 时启用客户管理的加密密钥	Microsoft.Compute/diskEncryptionSets/读取	是	是	是
	Microsoft.Compute/diskEncryptionSets/写入	是	是	否
	Microsoft.KeyVault/保管库/部署/操作	是	否	否
	Microsoft.Compute/diskEncryptionSets/删除	是	是	是
为 HA 对配置应用程序安全组，以隔离 HA 互连和集群网络 NIC	Microsoft.Network/applicationSecurityGroups/写入	否	是	否
	Microsoft.Network/applicationSecurityGroups/读取	否	是	否
	Microsoft.Network/applicationSecurityGroups/joinIpConfiguration/action	否	是	否
	Microsoft.Network/networkSecurityGroups/securityRules/写入	是	是	否
	Microsoft.Network/applicationSecurityGroups/删除	否	是	是
	Microsoft.Network/networkSecurityGroups/securityRules/删除	否	是	是
读取、写入和删除与Cloud Volumes ONTAP资源关联的标签	Microsoft.Resources/标签/阅读	否	是	否
	Microsoft.Resources/标签/写入	是	是	否
	Microsoft.Resources/标签/删除	是	否	否
在创建期间加密存储帐户	Microsoft.ManagedIdentity/userAssignedIdentities/分配/操作	是	是	否

目的	操作	用于部署?	用于日常运营?	用于删除?
在灵活编排模式下使用虚拟机规模集来为Cloud Volumes ONTAP指定特定区域	Microsoft.Compute/virtualMachineScaleSets/写入	是	否	否
	Microsoft.Compute/virtualMachineScaleSets/读取	是	否	否
	Microsoft.Compute/virtualMachineScaleSets/删除	否	否	是

分层

当您设置NetApp Cloud Tiering 时，代理会发出以下 API 请求。

- Microsoft.Storage/storageAccounts/listkeys/action
- Microsoft.Resources/订阅/资源组/读取
- Microsoft.Resources/订阅/位置/读取

控制台代理针对日常操作发出以下 API 请求。

- Microsoft.Storage/storageAccounts/blobServices/containers/read
- Microsoft.Storage/storageAccounts/managementPolicies/读取
- Microsoft.Storage/storageAccounts/managementPolicies/write
- Microsoft.Storage/storageAccounts/读取

更改日志

当添加和删除权限时，我们会在下面的部分中注明。

2024年9月9日

由于控制台不再支持发现和管理 Kubernetes 集群，因此从 JSON 策略中删除了以下权限：

- Microsoft.ContainerService/managedClusters/listClusterUserCredential/操作
- Microsoft.ContainerService/managedClusters/读取

2024年8月22日

以下权限已添加到 JSON 策略中，因为它们是Cloud Volumes ONTAP支持虚拟机规模集所必需的：

- Microsoft.Compute/virtualMachineScaleSets/写入
- Microsoft.Compute/virtualMachineScaleSets/读取
- Microsoft.Compute/virtualMachineScaleSets/删除

2023年12月5日

将卷数据备份到 Azure Blob 存储时， NetApp Backup and Recovery 不再需要以下权限：

- Microsoft.Compute/虚拟机/读取
- Microsoft.Compute/virtualMachines/启动/操作
- Microsoft.Compute/virtualMachines/解除分配/操作
- Microsoft.Compute/virtualMachines/扩展/删除
- Microsoft.Compute/virtualMachines/删除

其他控制台存储服务需要这些权限，因此如果您使用其他存储服务，它们仍将保留在代理的自定义角色中。

2023年5月12日

以下权限已添加到 JSON 策略，因为它们是Cloud Volumes ONTAP管理所必需的：

- Microsoft.Compute/图像/写入
- Microsoft.Network/loadBalancers/frontendIPConfigurations/读取

以下权限已从 JSON 策略中删除，因为不再需要它们：

- Microsoft.Storage/storageAccounts/blobServices/containers/write
- Microsoft.Network/publicIPAddresses/删除

2023年3月23日

数据分类不再需要“Microsoft.Storage/storageAccounts/delete”权限。

Cloud Volumes ONTAP仍然需要此权限。

2023年1月5日

以下权限已添加到 JSON 策略：

- Microsoft.Storage/storageAccounts/listAccountSas/action
- Microsoft.Synapse/工作区/privateEndpointConnectionsApproval/操作

  NetApp备份和恢复需要这些权限。

- Microsoft.Network/loadBalancers/backendAddressPools/join/action

  Cloud Volumes ONTAP部署需要此权限。

控制台代理的 **Google Cloud** 权限

NetApp控制台需要权限才能在 Google Cloud 中执行操作。这些权限包含在NetApp提供的自定义角色中。您应该了解代理使用这些权限做什么。

服务帐户权限

下面显示的自定义角色提供了控制台代理管理 Google Cloud 网络内的资源和流程所需的权限。

您需要将此自定义角色应用到附加到控制台代理 VM 的服务帐户。

- "设置标准模式的 Google Cloud 权限"
- "设置限制模式的权限"

您还需要确保角色是最新的，因为后续版本中会添加新的权限。如果需要新的权限，它们将在发行说明中列出。

```
title: NetApp Console agent
description: Permissions for the service account associated with the
Console agent instance.
stage: GA
includedPermissions:
- iam.serviceAccounts.actAs
- compute.regionBackendServices.create
- compute.regionBackendServices.get
- compute.regionBackendServices.list
- compute.networks.updatePolicy
- compute.backendServices.create
- compute.addresses.list
- compute.disks.create
- compute.disks.createSnapshot
- compute.disks.delete
- 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.addAccessConfig
- compute.instances.attachDisk
- compute.instances.create
- compute.instances.delete
- compute.instances.detachDisk
- compute.instances.get
- compute.instances.getSerialPortOutput
- compute.instances.list
```

```
- compute.instances.setDeletionProtection
- compute.instances.setLabels
- compute.instances.setMachineType
- compute.instances.setMetadata
- compute.instances.setTags
- compute.instances.start
- compute.instances.stop
- compute.instances.updateDisplayDevice
- compute.instanceGroups.get
- compute.addresses.get
- compute.instances.updateNetworkInterface
- compute.machineTypes.get
- compute.networks.get
- compute.networks.list
- compute.projects.get
- compute.regions.get
- compute.regions.list
- compute.snapshots.create
- compute.snapshots.delete
- compute.snapshots.get
- compute.snapshots.list
- compute.snapshots.setLabels
- compute.subnetworks.get
- compute.subnetworks.list
- compute.subnetworks.use
- compute.subnetworks.useExternalIp
- compute.zoneOperations.get
- compute.zones.get
- compute.zones.list
- compute.instances.setServiceAccount
- 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
```

```
- logging.logEntries.list
- logging.privateLogEntries.list
- resourcemanager.projects.get
- storage.buckets.create
- storage.buckets.delete
- storage.buckets.get
- storage.buckets.list
- cloudkms.cryptoKeyVersions.useToEncrypt
- cloudkms.cryptoKeys.get
- cloudkms.cryptoKeys.list
- cloudkms.keyRings.list
- storage.buckets.update
- iam.serviceAccounts.getIamPolicy
- iam.serviceAccounts.list
- storage.objects.get
- storage.objects.list
- monitoring.timeSeries.list
- storage.buckets.getIamPolicy
- cloudkms.cryptoKeys.getIamPolicy
- cloudkms.cryptoKeys.setIamPolicy
- cloudkms.keyRings.get
- cloudkms.keyRings.getIamPolicy
- cloudkms.keyRings.setIamPolicy
```

Google Cloud 权限的使用方式

操作	目的
- compute.disks.create - compute.disks.createSnapshot - compute.disks.delete - compute.disks.get - compute.disks.list - compute.disks.setLabels - compute.disks.use	为Cloud Volumes ONTAP创建和管理磁盘。
- compute.firewalls.创建 - compute.firewalls.删除 - compute.firewalls.获取 - compute.firewalls.列表	为Cloud Volumes ONTAP创建防火墙规则。
- 计算.全局操作.获取	获取操作状态。
- compute.images.get - compute.images.getFromFamily - compute.images.list - compute.images.useReadOnly	获取虚拟机实例的图像。
- 计算.实例.附加磁盘 - 计算.实例.分离磁盘	将磁盘附加到Cloud Volumes ONTAP中分离磁盘。
- 计算实例创建 - 计算实例删除	创建和删除Cloud Volumes ONTAP VM 实例。
- 计算.实例.获取	列出虚拟机实例。
- 计算.实例.获取串行端口输出	获取控制台日志。
- 计算.实例.列表	检索区域中的实例列表。
- compute.instances.setDeletionProtection	对实例设置删除保护。

操作	目的
- 计算.实例.设置标签	添加标签。
- compute.instances.setMachineType - compute.instances.setMinCpuPlatform	更改Cloud Volumes ONTAP的机器类型。
- 计算.实例.设置元数据	添加元数据。
- 计算.实例.设置标签	为防火墙规则添加标签。
- 计算实例.启动 - 计算实例.停止 - 计算实例.更新显示设备	启动和停止Cloud Volumes ONTAP。
- compute.machineTypes.get	获取核心数量来检查配额。
- 计算.项目.获取	支持多项目。
- compute.snapshots.create - compute.snapshots.delete - compute.snapshots.get - compute.snapshots.list - compute.snapshots.setLabels	创建和管理持久磁盘快照。
- 计算.网络.获取 - 计算.网络.列表 - 计算.区域.获取 - 计算.区域.列表 - 计算.子网络.获取 - 计算.子网络.列表 - 计算.区域操作.获取 - 计算.区域.获取 - 计算.区域.列表	获取创建新的Cloud Volumes ONTAP虚拟机实例所需的网络信息。
- 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	使用 Google Cloud Deployment Manager 部署Cloud Volumes ONTAP虚拟机实例。
- logging.logEntries.列表 - logging.privateLogEntries.列表	获取堆栈日志驱动器。
-资源管理器.项目.获取	支持多项目。
- storage.buckets.create - storage.buckets.delete - storage.buckets.get - storage.buckets.list - storage.buckets.update	创建和管理用于数据分层的 Google Cloud Storage 存储桶。
- cloudkms.cryptoKeyVersions.useToEncrypt - cloudkms.cryptoKeys.get - cloudkms.cryptoKeys.list - cloudkms.keyRings.list	将来自 Cloud Key Management Service 的客户管理加密密钥与Cloud Volumes ONTAP结合使用。

操作	目的
- compute.instances.setServiceAccount - iam.serviceAccounts.actAs - iam.serviceAccounts.getIamPolicy - iam.serviceAccounts.list - storage.objects.get - storage.objects.list	在Cloud Volumes ONTAP实例上设置服务帐户。此服务帐户提供将数据分层到 Google Cloud Storage 存储桶的权限。
- 计算.地址.列表	在部署 HA 对时检索区域中的地址。
- compute.backendServices.创建 - compute.regionBackendServices.创建 - compute.regionBackendServices.获取 - compute.regionBackendServices.列表	配置后端服务以在 HA 对中分配流量。
- 计算.网络.更新策略	在 HA 对的 VPC 和子网上应用防火墙规则。
- compute.subnetworks.use - compute.subnetworks.useExternalIp - compute.instances.addAccessConfig	启用NetApp数据分类。
- compute.instanceGroups.get - compute.addresses.get - compute.instances.updateNetworkInterface	在Cloud Volumes ONTAP HA 对上创建和管理存储虚拟机。
- 监控.时间序列.列表 - 存储.桶.获取IamPolicy	发现有关 Google Cloud Storage 存储桶的信息。
- cloudkms.cryptoKeys.get - cloudkms.cryptoKeys.getIamPolicy - cloudkms.cryptoKeys.list - cloudkms.cryptoKeys.setIamPolicy - cloudkms.keyRings.get - cloudkms.keyRings.getIamPolicy - cloudkms.keyRings.list - cloudkms.keyRings.setIamPolicy	在NetApp备份和恢复激活向导中选择您自己的客户管理密钥，而不是使用默认的 Google 管理加密密钥。

更改日志

当添加和删除权限时，我们会在下面的部分中注明。

2023年2月6日

此策略中添加了以下权限：

- 计算.实例.更新网络接口

Cloud Volumes ONTAP需要此权限。

2023年1月27日

已将以下权限添加到策略中：

- cloudkms.cryptoKeys.getIamPolicy
- cloudkms.cryptoKeys.setIamPolicy
- cloudkms.keyRings.get

- cloudkms.keyRings.getIamPolicy
- cloudkms.keyRings.setIamPolicy

NetApp备份和恢复需要这些权限。

端口

AWS 中的控制台代理安全组规则

代理的 AWS 安全组需要入站和出站规则。当您从控制台创建控制台代理时， NetApp控制台会自动创建此安全组。您需要为所有其他安装选项设置此安全组。

入站规则

协议	端口	目的
SSH	22	提供对代理主机的 SSH 访问
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	提供对本地用户界面的 HTTPS 访问以及来自NetApp数据分类实例的连接
TCP	3128	为Cloud Volumes ONTAP提供互联网访问。部署后您必须手动打开此端口。

出站规则

代理的预定义安全组打开所有出站流量。如果可以接受，请遵循基本的出站规则。如果您需要更严格的规则，请使用高级出站规则。

基本出站规则

代理的预定义安全组包括以下出站规则。

协议	端口	目的
所有 TCP	全部	所有出站流量
所有 UDP	全部	所有出站流量

高级出站规则

如果您需要对出站流量制定严格的规则，则可以使用以下信息仅打开代理出站通信所需的端口

源IP地址是代理主机。

服务	协议	端口	目标	目的
API 调用和AutoSupport	HTTPS	443	出站互联网和ONTAP集群管理LIF	对 AWS、 ONTAP、NetApp数据分类的 API 调用，以及向NetApp发送AutoSupport消息
API 调用	TCP	3000	ONTAP HA 调解器	与ONTAP HA 调解器的通信
	TCP	8080	数据分类	部署期间探测数据分类实例
DNS	UDP	53	DNS	用于控制台的 DNS 解析

Azure 中的控制台代理安全组规则

代理的 Azure 安全组需要入站和出站规则。当您从控制台创建控制台代理时， NetApp控制台会自动创建此安全组。对于其他安装选项，您需要手动设置此安全组。

入站规则

协议	端口	目的
SSH	22	提供对代理主机的 SSH 访问
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，以及来自NetApp数据分类实例的连接
TCP	3128	为Cloud Volumes ONTAP提供互联网访问权限，以便将AutoSupport消息发送给NetApp支持。部署后您必须手动打开此端口。 "了解如何将代理用作AutoSupport消息的代理"

出站规则

代理的预定义安全组打开所有出站流量。如果可以接受，请遵循基本的出站规则。如果您需要更严格的规则，请使用高级出站规则。

基本出站规则

代理的预定义安全组包括以下出站规则。

协议	端口	目的
所有 TCP	全部	所有出站流量
所有 UDP	全部	所有出站流量

高级出站规则

如果您需要对出站流量制定严格的规则，则可以使用以下信息仅打开代理出站通信所需的端口。

源IP地址是代理主机。

服务	协议	端口	目标	目的
API 调用和AutoSupport	HTTPS	443	出站互联网和ONTAP集群管理LIF	对 Azure、ONTAP、 NetApp数据分类的 API 调用，以及向NetApp发送AutoSupport消息
API 调用	TCP	8080	数据分类	部署期间探测数据分类实例
DNS	UDP	53	DNS	用于控制台的 DNS 解析

Google Cloud 中的代理防火墙规则

代理的 Google Cloud 防火墙规则需要入站和出站规则。当您从控制台创建控制台代理时， NetApp控制台会自动创建此安全组。对于其他安装选项，您需要手动设置此安全组。

入站规则

协议	端口	目的
SSH	22	提供对代理主机的 SSH 访问
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
TCP	3128	为Cloud Volumes ONTAP提供互联网访问。部署后您必须手动打开此端口。

出站规则

代理的预定义防火墙规则打开所有出站流量。如果可以接受，请遵循基本出站规则，或者使用高级出站规则来满足更严格的要求。

基本出站规则

代理的预定义防火墙规则包括以下出站规则。

协议	端口	目的
所有 TCP	全部	所有出站流量
所有 UDP	全部	所有出站流量

高级出站规则

如果您需要对出站流量制定严格的规则，则可以使用以下信息仅打开代理出站通信所需的端口。

源IP地址是代理主机。

服务	协议	端口	目标	目的
API 调用和AutoSupport	HTTPS	443	出站互联网和ONTAP集群管理LIF	对 Google Cloud、ONTAP、 NetApp数据分类的 API 调用，以及向NetApp发送AutoSupport消息
API 调用	TCP	8080	数据分类	部署期间探测数据分类实例
DNS	UDP	53	DNS	用于数据分类的 DNS 解析

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控制台部署模式。

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

3.9.55 及以下版本所需的网络接入点

本主题详细介绍了NetApp控制台 4.0.0 之前的版本标准模式所需的网络访问。NetAppNetApp、 NetApp控制台代理和NetApp数据服务出站互联网访问以及联系必要端点的能力。您需要确保控制台和您安装的任何代理都具有正确的网络访问权限以使用功能属性。

您需要为以软件即服务 (SaaS) 形式访问NetApp控制台的计算机以及您在本地或云中安装的任何控制台代理设置网络访问。您可能还需要某些NetApp数据服务（包括Cloud Volumes ONTAP）的额外端点。

将您的终端列表更新为 4.0.0 及更高版本的修订列表

从 4.0.0 版本开始，控制台代理需要的端点更少。 4.0.0 之前的现有部署仍然受支持。升级到 4.0.0 或更高版本后，您可以在方便时从允许列表中删除旧端点。

NetApp建议您更新防火墙规则以使用修订后的端点列表。修改后的列表更小，因此更安全且更易于管理。

审查"4.0.0 及更高版本支持的端点"

步骤

1. 将端点列入白名单"4.0.0 及更高版本支持的端点"。
2. 通过运行以下命令重新启动每个代理上的服务管理器 2 服务：

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

3. 运行以下命令并验证代理的状态是否显示为_active(running)：

```
systemctl status netapp-service-manager.service
```

4. 从允许列表中删除旧端点。

NetApp控制台联系的端点

访问NetApp控制台的每台计算机都必须连接到下面列出的端点。

系统在两种情况下联系这些端点：

- 从计算机访问 "NetApp控制台"作为软件即服务（SaaS）。
- 从直接访问代理主机的计算机，可以登录并进行设置，也可以从代理主机访问控制台。

端点	目的
\ https://support.netapp.com \ https://mysupport.netapp.com	获取许可信息并向NetApp支持发送AutoSupport消息。
https://*.api.bluexp.netapp.com \ https://api.bluexp.netapp.com https://*.cloudmanager.cloud.netapp.com \ https://cloudmanager.cloud.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com	在NetApp控制台中提供功能和服务。

端点	目的
在两组端点之间进行选择： • 选项 1（推荐） \ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://bluexpinfraprod.azurecr.io • 选项 2 https://*.blob.core.windows.net \ https://cloudmanagerinfraprod.azurecr.io	获取控制台代理升级的图像。 NetApp建议在防火墙中允许选项 1 端点，因为它们更安全，并禁止选项 2 端点，除非您使用勒索软件恢复或备份和恢复。请注意有关这些端点的以下事项： • 3.9.47 及更高版本支持选项 1 端点。 3.9.47 之前的版本不支持向后兼容。 • 控制台代理首先启动与选项 2 中的端点的联系。如果这些端点不可访问，它会自动联系选项 1 中的端点。 • 如果将控制台代理与NetApp Backup and Recovery 或 Ransomware Resilience 一起使用，则系统不支持选项 1 端点。允许选项 2 端点并不允许选项 1。

控制台代理联系的端点

您可以在本地或云中安装控制台代理，它会联系端点以完成控制台发起的操作。

控制台代理需要访问与NetApp控制台相同的端点，如果您在云提供商中部署代理，则还需要访问其他端点。

AWS 的代理端点

这些端点适用于 4.0.0 之前的控制台代理。

端点	目的
AWS 服务 (amazonaws.com)：CloudFormation 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 中的资源。确切的端点取决于您使用的 AWS 区域。有关详细信息，请参阅 AWS 文档以获取许可信息并向NetApp支持发送AutoSupport消息。
\ https://support.netapp.com \ https://mysupport.netapp.com	获取许可信息并向NetApp支持发送AutoSupport消息。

端点	目的
在两组端点之间进行选择： • 选项 1（推荐） \ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://bluexpinfraprod.azurecr.io • 选项 2 https://*.blob.core.windows.net \ https://cloudmanagerinfraprod.azurecr.io	获取控制台代理升级的图像。 NetApp建议在防火墙中允许选项 1 端点，因为它们更安全，并禁止选项 2 端点，除非您使用勒索软件恢复或备份和恢复。请注意有关这些端点的以下事项： • 3.9.47 及更高版本支持选项 1 端点。 3.9.47 之前的版本不支持向后兼容。 • 控制台代理首先启动与选项 2 中的端点的联系。如果这些端点不可访问，它会自动联系选项 1 中的端点。 • 如果将控制台代理与NetApp Backup and Recovery 或 Ransomware Resilience 一起使用，则系统不支持选项 1 端点。允许选项 2 端点并不允许选项 1。

Azure 的代理端点

这些端点适用于 4.0.0 之前的控制台代理。

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://support.netapp.com \ https://mysupport.netapp.com	获取许可信息并向NetApp支持发送AutoSupport消息。

端点	目的
在两组端点之间进行选择： • 选项 1（推荐） \ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://bluexpinfraprod.azurecr.io • 选项 2 https://*.blob.core.windows.net \ https://cloudmanagerinfraprod.azurecr.io	获取控制台代理升级的图像。 NetApp建议在防火墙中允许选项 1 端点，因为它们更安全，并禁止选项 2 端点，除非您使用勒索软件恢复或备份和恢复。请注意有关这些端点的以下事项： • 3.9.47 及更高版本支持选项 1 端点。 3.9.47 之前的版本不支持向后兼容。 • 控制台代理首先启动与选项 2 中的端点的联系。如果这些端点不可访问，它会自动联系选项 1 中的端点。 • 如果将控制台代理与NetApp Backup and Recovery 或 Ransomware Resilience 一起使用，则系统不支持选项 1 端点。允许选项 2 端点并不允许选项 1。

Google Cloud 的代理端点

这些端点适用于 4.0.0 之前的控制台代理。

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://www.googleapis.com/deploymentmanager/v2/project	管理 Google Cloud 中的资源。
\ https://support.netapp.com \ https://mysupport.netapp.com	获取许可信息并向NetApp支持发送AutoSupport消息。

端点	目的
在两组端点之间进行选择： • 选项 1（推荐） \ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://bluexpinfraprod.azurecr.io • 选项 2 https://*.blob.core.windows.net \ https://cloudmanagerinfraprod.azurecr.io	获取控制台代理升级的图像。 NetApp建议在防火墙中允许选项 1 端点，因为它们更安全，而不允许选项 2 端点。请注意有关这些端点的以下事项： • 从控制台代理 3.9.47 版本开始，系统支持选项 1 中列出的端点。控制台代理的先前版本不支持向后兼容。 • 控制台代理首先联系选项 2 中的端点。如果这些端点不可访问，它会自动联系选项 1 中的端点。 • 如果将控制台代理与NetApp Backup and Recovery 或 Ransomware Resilience 一起使用，则系统不支持选项 1 端点。允许选项 2 端点并不允许选项 1。

本地代理端点

知识和支持

注册以获得支持

需要注册支持才能获得针对BlueXP及其存储解决方案和服务的技术支持。还需要支持注册才能启用Cloud Volumes ONTAP系统的关键工作流程。

注册支持并不能使NetApp获得云提供商文件服务的支持。有关云提供商文件服务、其基础设施或使用该服务的任何解决方案的技术支持，请参阅该产品的BlueXP文档中的“获取帮助”。

- "适用于ONTAP 的Amazon FSx"
- "Azure NetApp Files"
- "Google Cloud NetApp Volumes"

支持注册概述

激活支持权利的注册方式有两种：

- 注册您的BlueXP帐户序列号（您的 20 位 960xxxxxxxx 序列号位于BlueXP中的支持资源页面上）。

  这是您在BlueXP内任何服务的单一支持订阅 ID。每个BlueXP帐户级支持订阅都必须注册。

- 在您的云提供商市场中注册与订阅相关的Cloud Volumes ONTAP序列号（这些是 20 位 909201xxxxxxxx 序列号）。

  这些序列号通常被称为_PAYGO 序列号_，由BlueXP在Cloud Volumes ONTAP部署时生成。

注册两种类型的序列号可以实现开立支持票和自动生成案例等功能。按照如下所述，通过将NetApp支持站点 (NSS) 帐户添加到BlueXP来完成注册。

注册**BlueXP**以获得**NetApp**支持

要注册支持并激活支持权利，您的BlueXP组织（或帐户）中的一名用户必须将NetApp支持站点帐户与其BlueXP登录名关联。如何注册NetApp支持取决于您是否已经拥有NetApp支持站点 (NSS) 帐户。

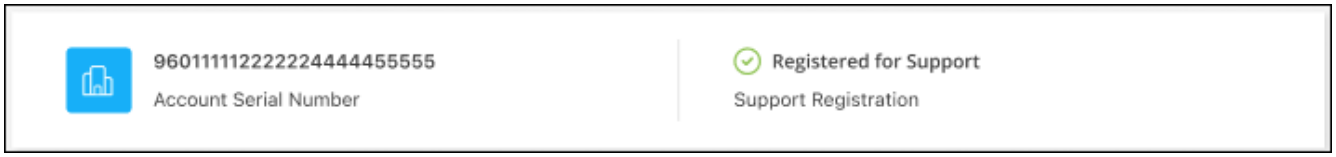
拥有 **NSS** 帐户的现有客户

如果您是拥有 NSS 帐户的NetApp客户，则只需通过BlueXP注册即可获得支持。

步骤

1. 在BlueXP控制台的右上角，选择“设置”图标，然后选择“凭据”。
2. 选择*用户凭证*。
3. 选择*添加 NSS 凭据*并按照NetApp支持站点 (NSS) 身份验证提示进行操作。
4. 要确认注册过程是否成功，请选择“帮助”图标，然后选择“支持”。

   *资源*页面应显示您的BlueXP组织已注册以获得支持。



请注意，如果其他BlueXP用户尚未将NetApp支持站点帐户与其BlueXP登录名关联，他们将看不到相同的支持注册状态。但是，这并不意味着您的BlueXP组织没有注册支持。只要组织中的一名用户遵循了这些步骤，那么您的组织就已注册。

现有客户但没有 **NSS** 账户

如果您是现有的NetApp客户，拥有现有许可证和序列号但没有 NSS 帐户，则需要创建一个 NSS 帐户并将其与您的BlueXP登录关联。

步骤

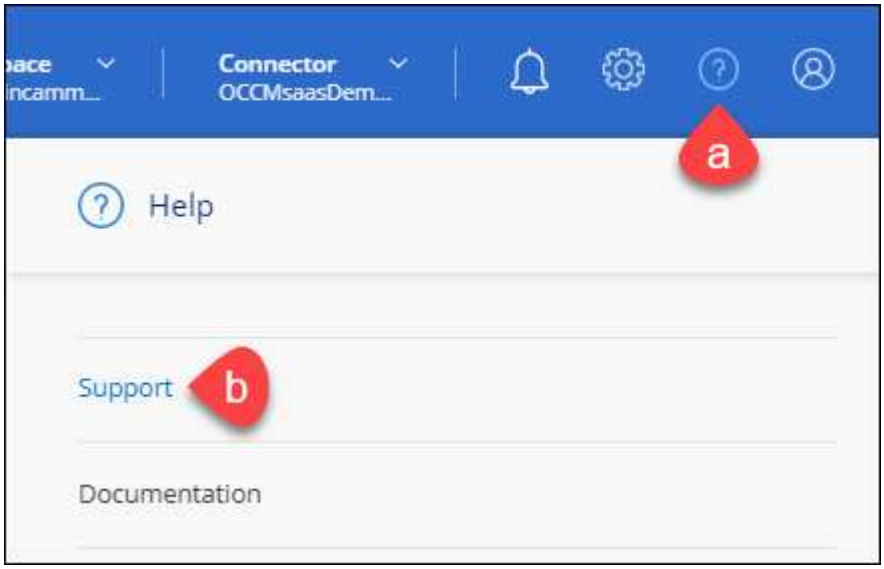
1. 通过完成以下操作创建NetApp支持站点帐户 "NetApp支持站点用户注册表"
   a. 请务必选择适当的用户级别，通常为* NetApp客户/最终用户*。
   b. 请务必复制上面用于序列号字段的BlueXP帐户序列号 (960xxxx)。这将加快账户处理速度。
2. 完成以下步骤，将您的新 NSS 帐户与您的BlueXP登录名关联拥有 NSS 帐户的现有客户。

NetApp全新产品

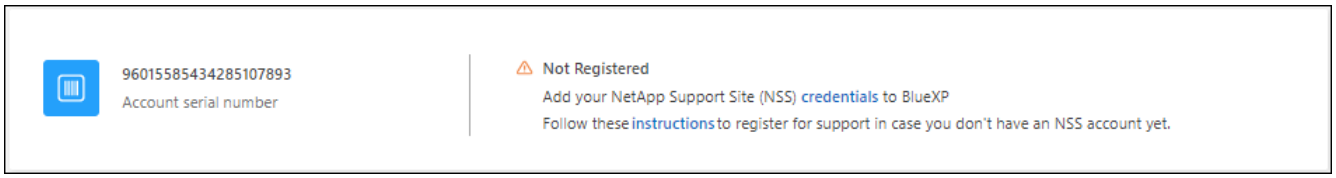
如果您是NetApp新用户并且没有 NSS 帐户，请按照以下步骤操作。

步骤

1. 在BlueXP控制台的右上角，选择“帮助”图标，然后选择“支持”。



2. 从支持注册页面找到您的帐户 ID 序列号。



3. 导航至 "NetApp 的支持注册网站"并选择*我不是注册的NetApp客户*。
4. 填写必填字段（带有红色星号的字段）。
5. 在*产品线*字段中，选择*云管理器*，然后选择适用的计费提供商。
6. 从上面的步骤 2 复制您的帐户序列号，完成安全检查，然后确认您已阅读 NetApp 的全球数据隐私政策。

   一封电子邮件会立即发送到提供的邮箱以完成此安全交易。如果几分钟内没有收到验证电子邮件，请务必检查您的垃圾邮件文件夹。

7. 从电子邮件中确认操作。

   确认向NetApp提交您的请求并建议您创建NetApp支持站点帐户。

8. 通过完成以下操作创建NetApp支持站点帐户 "NetApp支持站点用户注册表"
   a. 请务必选择适当的用户级别，通常为* NetApp客户/最终用户*。
   b. 请务必复制上面用于序列号字段的帐户序列号（960xxxx）。这将加快处理速度。

完成后

NetApp应该在此过程中与您联系。这是针对新用户的一次性入职培训。

拥有NetApp支持站点帐户后，请按照以下步骤将该帐户与您的BlueXP登录名关联拥有 NSS 帐户的现有客户。

关联 NSS 凭据以获得Cloud Volumes ONTAP支持

需要将NetApp支持站点凭据与您的BlueXP组织关联才能为Cloud Volumes ONTAP启用以下关键工作流程：

- 注册即用即付Cloud Volumes ONTAP系统以获得支持

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

- 自带许可证 (BYOL) 时部署Cloud Volumes ONTAP

  需要提供您的 NSS 帐户，以便BlueXP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。

- 将Cloud Volumes ONTAP软件升级到最新版本

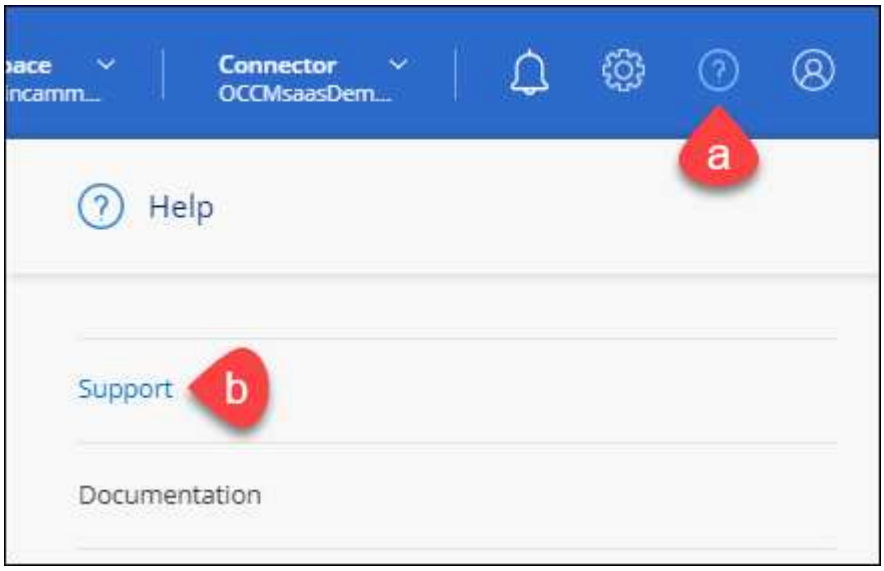
将 NSS 凭证与您的BlueXP组织关联与与BlueXP用户登录关联的 NSS 帐户不同。

这些 NSS 凭证与您的特定BlueXP组织 ID 相关联。属于BlueXP组织的用户可以从 支持 **> NSS** 管理 访问这些凭据。

- 如果您有客户级帐户，则可以添加一个或多个 NSS 帐户。
- 如果您有合作伙伴或经销商帐户，则可以添加一个或多个 NSS 帐户，但不能与客户级帐户一起添加。

步骤

1. 在BlueXP控制台的右上角，选择“帮助”图标，然后选择“支持”。



2. 选择*NSS 管理 > 添加 NSS 帐户*。
3. 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 作为特定于支持和许可的身份验证服务的身份提供者。

4. 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以执行身份验证过程。

   这些操作使BlueXP能够使用您的 NSS 帐户进行许可证下载、软件升级验证和未来支持注册等操作。

   请注意以下事项：

   - NSS 帐户必须是客户级帐户（不是访客或临时帐户）。您可以拥有多个客户级 NSS 帐户。
   - 如果该帐户是合作伙伴级别帐户，则只能有一个 NSS 帐户。如果您尝试添加客户级 NSS 帐户并且合作伙伴级帐户已存在，您将收到以下错误消息：

     “此帐户不允许使用 NSS 客户类型，因为已经存在不同类型的 NSS 用户。”

   如果您已有客户级 NSS 帐户并尝试添加合作伙伴级帐户，情况也是如此。

   - 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。

获取帮助

NetApp以多种方式为NetApp Console 及其云服务提供支持。全天候提供广泛的免费自助支持选项，例如知识库 (KB) 文章和社区论坛。您的支持注册包含通过网络工单获取的远程技术支持。

获取云提供商文件服务的支持

有关云提供商文件服务、其基础设施或使用该服务的任何解决方案的技术支持，请参阅该产品的文档。

- "适用于ONTAP 的Amazon FSx"
- "Azure NetApp Files"
- "Google Cloud NetApp Volumes"

要获得特定于NetApp及其存储解决方案和数据服务的技术支持，请使用下面描述的支持选项。

使用自助选项

这些选项每周 7 天、每天 24 小时免费提供：

- 文档

  您当前正在查看的NetApp控制台文档。

- "知识库"

  搜索NetApp知识库以查找有助于解决问题的文章。

- "社区"

  加入NetApp控制台社区，关注正在进行的讨论或创建新的讨论。

向**NetApp**支持创建案例

除了上述自助支持选项之外，您还可以在激活支持后与NetApp支持专家合作解决任何问题。

开始之前

- 要使用“创建案例”功能，您必须首先将您的NetApp支持站点凭据与您的控制台登录关联。 "了解如何管理与控制台登录相关的凭据" 。
- 如果您要为具有序列号的ONTAP系统打开案例，那么您的 NSS 帐户必须与该系统的序列号相关联。

步骤

1. 在NetApp控制台中，选择“帮助”>“支持”。
2. 在“资源”页面上，选择“技术支持”下的可用选项之一：

   a. 如果您想通过电话与某人交谈，请选择“致电我们”。您将被引导至 netapp.com 上的一个页面，其中列出了您可以拨打的电话号码。

b. 选择“创建案例”向NetApp支持专家开具一张票：

- 服务：选择与问题相关的服务。例如，* NetApp Console* 特定于控制台内的工作流或功能的技术支持问题。
- 系统：如果适用于存储，请选择* Cloud Volumes ONTAP* 或 **On-Prem**，然后选择相关的工作环境。

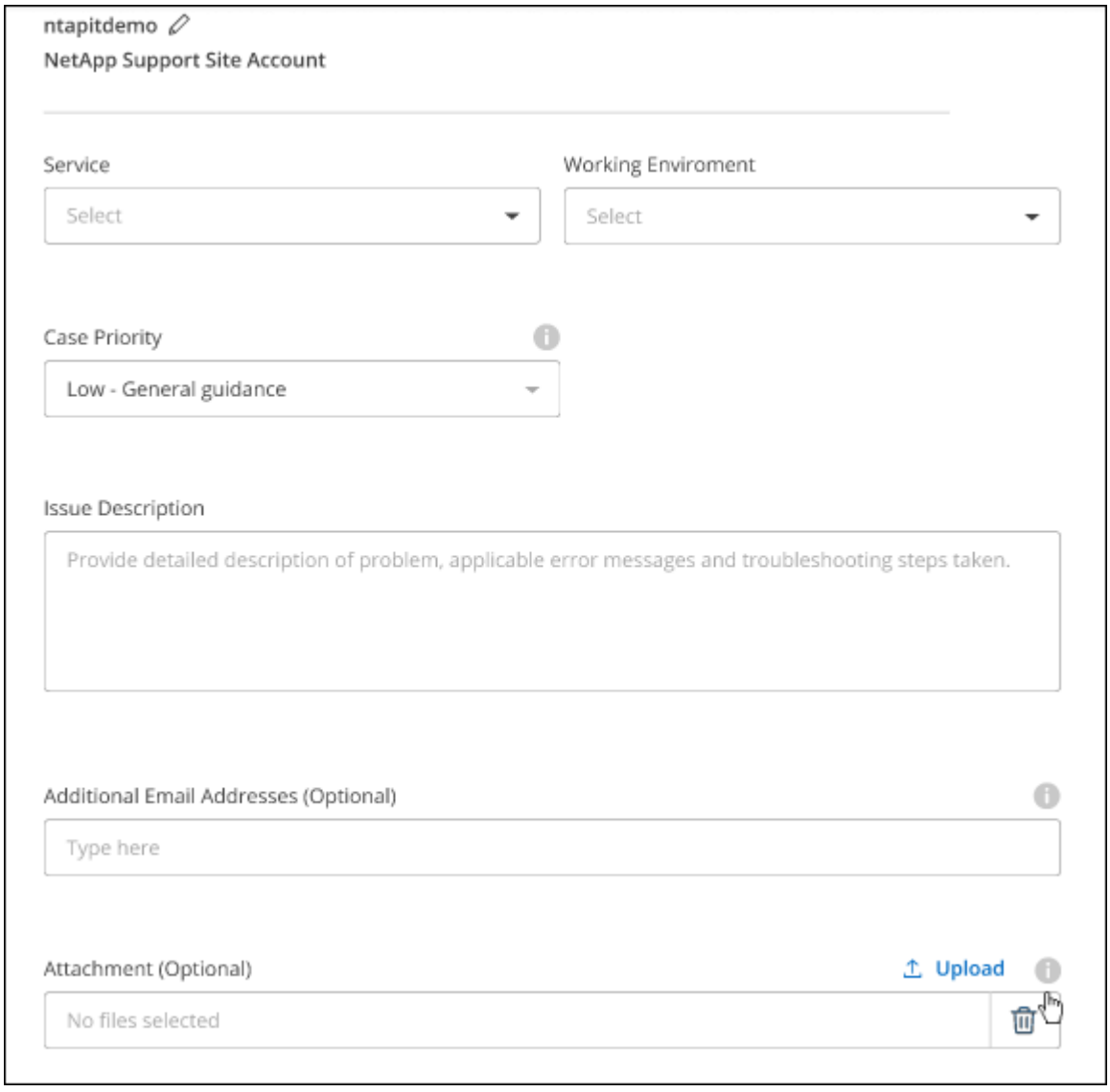
  系统列表位于控制台组织范围内，并且您在顶部横幅中选择了控制台代理。

- 案例优先级：选择案例的优先级，可以是低、中、高或严重。

  要了解有关这些优先事项的更多详细信息，请将鼠标悬停在字段名称旁边的信息图标上。

- 问题描述：提供问题的详细描述，包括任何适用的错误消息或您执行的故障排除步骤。
- 其他电子邮件地址：如果您想让其他人知道此问题，请输入其他电子邮件地址。
- 附件（可选）：一次最多上传五个附件。

  每个附件文件大小限制为 25 MB。支持以下文件扩展名：txt、log、pdf、jpg/jpeg、rtf、doc/docx、xls/xlsx 和 csv。



完成后

将会出现一个弹出窗口，其中显示您的支持案例编号。NetApp支持专家将审查您的案例并尽快回复您。

要查看支持案例的历史记录，您可以选择*设置>时间线*并查找名为“创建支持案例”的操作。最右边的按钮可让您展开操作以查看详细信息。

尝试创建案例时，您可能会遇到以下错误消息：

“您无权针对所选服务创建案例”

此错误可能意味着 NSS 帐户及其关联的记录公司与NetApp控制台帐户序列号的记录公司不同（即。960xxxx）或工作环境序列号。您可以使用以下选项之一寻求帮助：

- 提交非技术案例 https://mysupport.netapp.com/site/help

管理您的支持案例

您可以直接从控制台查看和管理活动和已解决的支持案例。您可以管理与您的 NSS 帐户和公司相关的案例。

请注意以下事项：

- 页面顶部的案例管理仪表板提供两种视图：
  - 左侧视图显示了您提供的用户 NSS 帐户在过去 3 个月内打开的案件总数。
  - 右侧的视图根据您的用户 NSS 帐户显示了过去 3 个月内贵公司级别开设的案件总数。

  表中的结果反映了与您选择的视图相关的案例。
- 您可以添加或删除感兴趣的列，并且可以过滤优先级和状态等列的内容。其他列仅提供排序功能。

  请查看以下步骤以了解更多详细信息。
- 在每个案件级别，我们提供更新案件记录或关闭尚未关闭或待关闭状态的案件的功能。

步骤

1. 在NetApp控制台中，选择“帮助”>“支持”。
2. 选择*案例管理*，如果出现提示，请将您的 NSS 帐户添加到控制台。

   案例管理*页面显示与您的控制台用户帐户关联的 **NSS** 帐户相关的未结案例。这与出现在 ***NSS** 管理 页面顶部的 NSS 帐户相同。
3. （可选）修改表中显示的信息：
   - 在“组织的案例”下，选择“查看”以查看与您的公司相关的所有案例。
   - 通过选择精确的日期范围或选择不同的时间范围来修改日期范围。
   - 过滤列的内容。
   - 通过选择  然后选择您想要显示的列。
4. 通过选择管理现有案例•••并选择其中一个可用选项：

- 查看案例：查看有关特定案例的完整详细信息。
- 更新案例说明：提供有关您的问题的更多详细信息，或选择*上传文件*以附加最多五个文件。

  每个附件文件大小限制为 25 MB。支持以下文件扩展名：txt、log、pdf、jpg/jpeg、rtf、doc/docx、xls/xlsx 和 csv。

- 结案：提供有关结案原因的详细信息，然后选择*结案*。

法律声明

法律声明提供对版权声明、商标、专利等的访问。

版权

"https://www.netapp.com/company/legal/copyright/"

商标

NETAPP、NETAPP 徽标和NetApp商标页面上列出的标志是NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。

"https://www.netapp.com/company/legal/trademarks/"

专利

NetApp拥有的专利的最新列表可以在以下位置找到：

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

隐私政策

"https://www.netapp.com/company/legal/privacy-policy/"

开源

通知文件提供有关NetApp软件中使用的第三方版权和许可的信息。

"NetApp控制台通知"