开始使用

NetApp Console setup and administration

NetApp
January 27, 2026

目录

开始使用

学习基础知识

了解NetApp Console

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。

它既可以作为软件即服务 (SaaS) 平台使用，也可以作为自托管选项安装在您自己的主权云中。它提供存储管理、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。

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

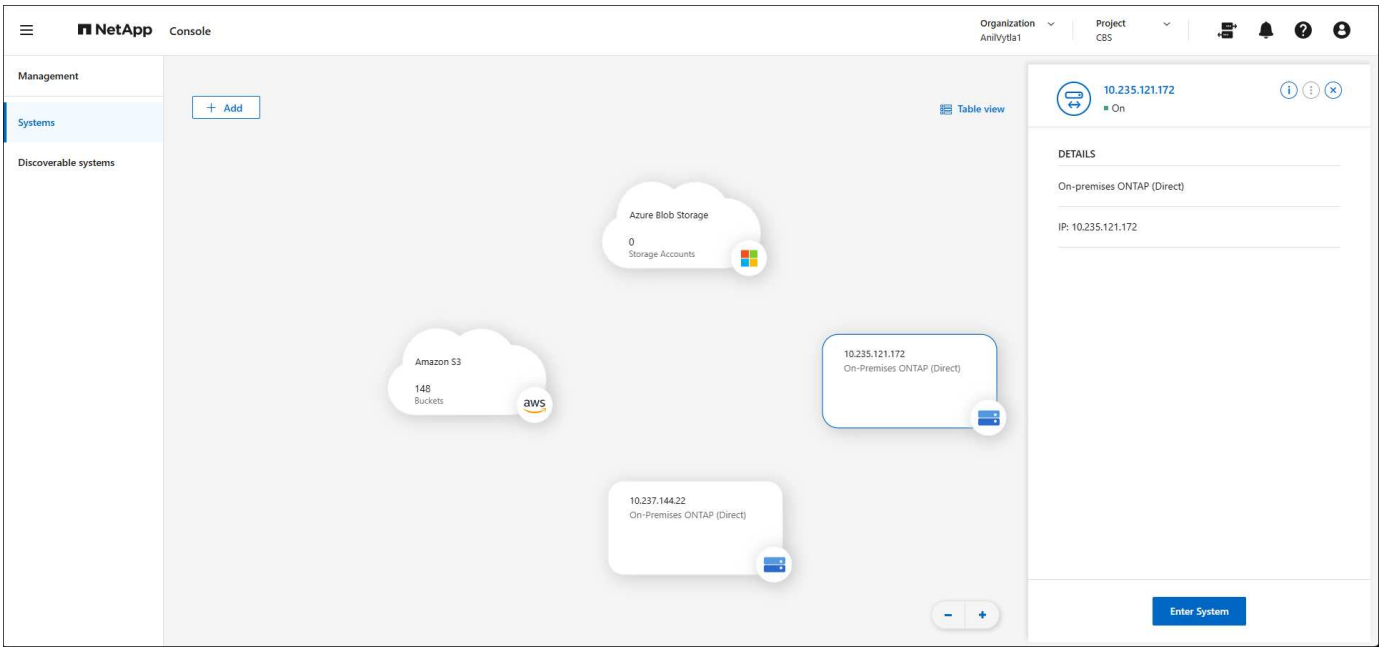
- E系列系统
- ONTAP集群
- StorageGRID系统

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 Backup and Recovery
: 备份和恢复云和本地数据。

NetApp Data Classification
: 让您的应用程序数据和云环境隐私做好准备。

NetApp Copy and Sync
: 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。

Licenses and subscriptions
: 管理和监控您的许可证和订阅。

NetApp Disaster Recovery
: 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 Ransomware Resilience

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 Replication

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 Cloud Tiering

将您的本地ONTAP存储扩展到云端。

NetApp Volume Caching

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 Console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 Console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 Console的工作原理

NetApp Console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
- 资源管理使您能够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 Console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" 。

SaaS 与主权云部署

您可以通过注册 SaaS 服务或将其部署在您的主权云中来开始使用NetApp Console 。在主权云中部署NetApp Console时， NetApp会限制出站连接，以满足您组织的安全性和合规性要求。当控制台部署在主权云中时，并非所有功能和服务都可用。

NetApp继续为不需要出站连接的站点提供BlueXP 。BlueXP可以安装在您的网络上，无需任何出站连接。 "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 Console**部署模式

NetApp Console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 Console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 ConsoleSaaS 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"

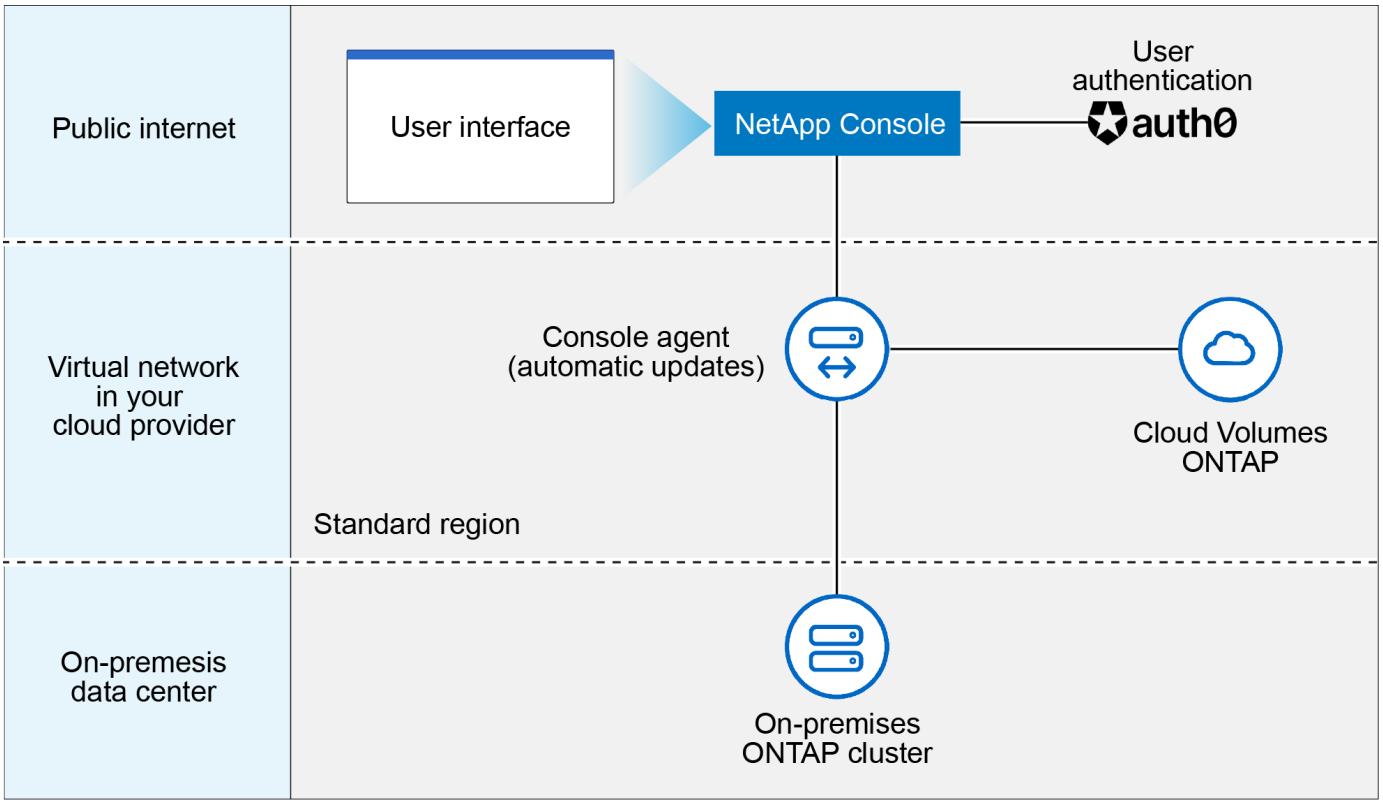
下表提供了NetApp控制台的比较。

	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
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 Console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。

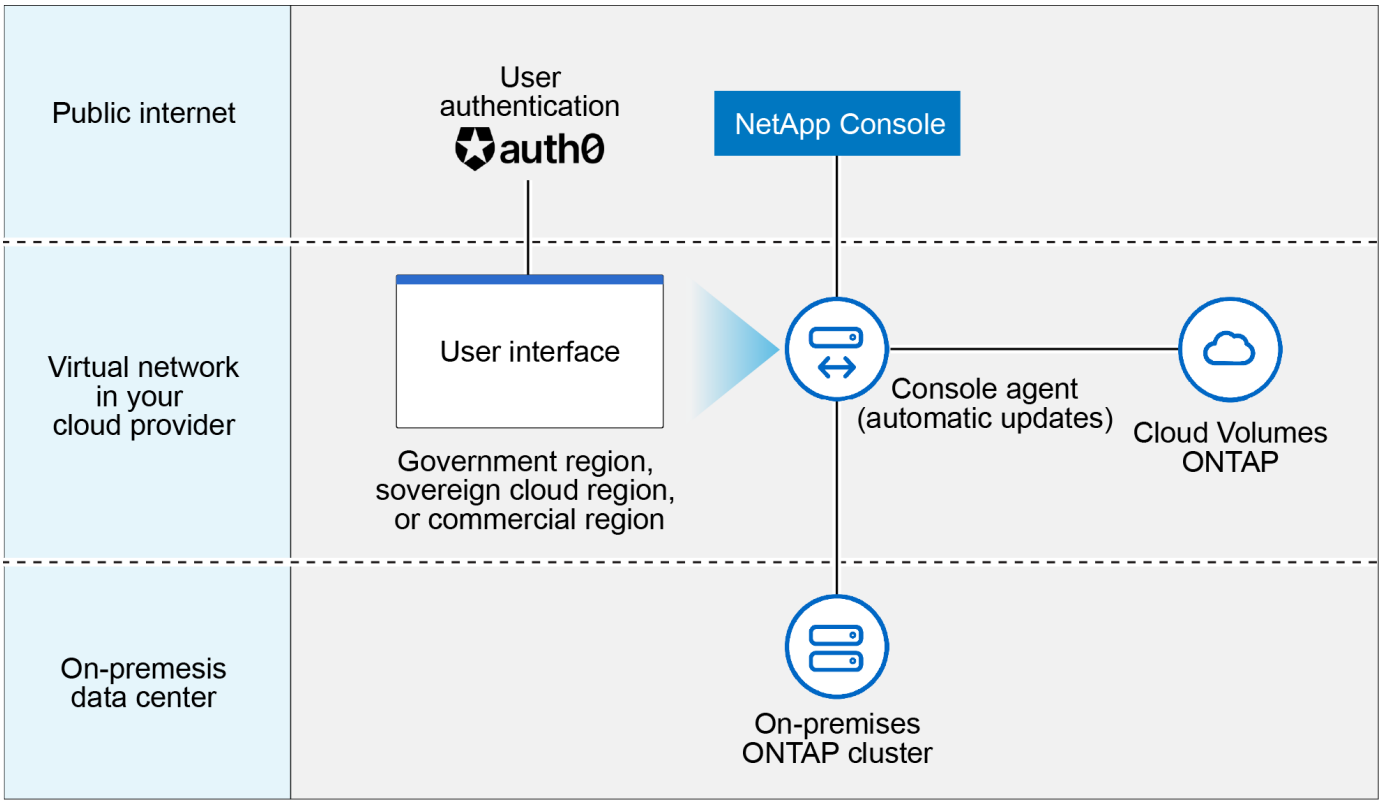
如何开始使用标准模式

前往 "NetApp Console"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 Data Classification	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
Licenses and subscriptions	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。

支持的服务	笔记
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 Console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。它没有指明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/data-services-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 Data Classification	是
	NetApp Copy and Sync	否
	NetApp Disaster Recovery	否
	NetApp Ransomware Resilience	否
	NetApp Replication	是
	NetApp Cloud Tiering	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

管理与NetApp Console关联的 NSS 凭据

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

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

概述

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

- 自带许可证 (BYOL) 时部署Cloud Volumes ONTAP

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

- 注册即用即付Cloud Volumes ONTAP系统

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

- 将Cloud Volumes ONTAP软件升级到最新版本

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

添加 NSS 帐户

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

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

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

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

步骤

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

   成功登录后， NetApp将存储 NSS 用户名。

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

   - 如果您需要刷新登录凭证令牌，还有一个*更新凭证*选项 ••• 菜单。

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

下一步是什么?

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

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

更新 **NSS** 凭证

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

过期的凭证可能会影响以下情况，但不限于：

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

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

步骤

1. 在*管理 > 支持*中。
2. 选择*NSS 管理*。

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

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

5. 在登录页面，提供您的NetApp支持站点注册的电子邮件地址和密码。

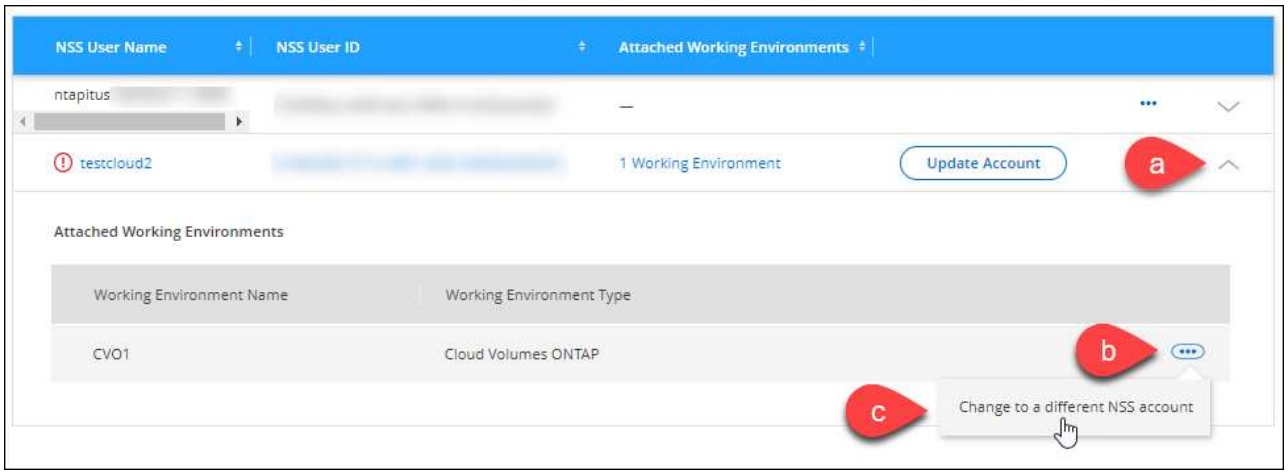
将系统附加到不同的 **NSS** 帐户

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

您必须首先将帐户与控制台关联。

步骤

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



   d. 选择帐户，然后选择*保存*。

显示 **NSS** 帐户的电子邮件地址

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

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

步骤

1. 在*管理 > 支持*中。

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

删除 **NSS** 帐户

删除不再想在控制台中使用的所有 NSS 帐户。

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

步骤

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

了解NetApp Console代理

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

控制台代理使您能够：

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

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

下表显示了您可以使用和不使用控制台代理时可以使用的功能和服务。

	可联系经纪人获取信息	无需代理即可购买
支持的存储系统：		
适用于ONTAP 的Amazon FSx	是的（发现和管理功能）	是的（仅限探索）
Amazon S3 存储	是	否
Azure Blob 存储	是	是
Azure NetApp Files	是	是

	可联系经纪人获取信息	无需代理即可购买
Cloud Volumes ONTAP	是	否
E系列系统	是	否
Google Cloud NetApp Volumes	是	是
Google Cloud 存储桶	是	否
StorageGRID系统	是	否
本地部署ONTAP集群（高级管理和发现）	是的（高级管理和发现）	否（仅限基本发现）
可用的存储管理服务：		
警报	是	否
自动化中心	是	是
Digital Advisor（Active IQ）	是	否
许可证和订阅管理	是	否
经济效益	是	否
首页仪表盘指标	是的[2]	否
生命周期规划	是	1号
可持续性	是	否
软件更新	是	是
NetApp工作负载	是	是
可用数据服务：		
NetApp Backup and Recovery	是	否
数据分类	是	否
NetApp Cloud Tiering	是	否

	可联系经纪人获取信息	无需代理即可购买
NetApp Copy and Sync	是	否
NetApp Disaster Recovery	是	否
NetApp Ransomware Resilience	是	否
NetApp Volume Caching	是	否

[1] 无需控制台代理即可查看生命周期规划，但需要控制台代理才能启动操作。

[2] 主页上的准确指标需要大小合适且配置正确的控制台代理。

控制台代理必须始终处于运行状态

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

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

支持的位置

您可以在以下位置安装代理：

- Amazon Web Services
- Microsoft Azure

  在 Azure 中与其管理的Cloud Volumes ONTAP系统位于同一区域的控制台代理。或者，将其部署在 "Azure 区域对"。这可确保Cloud Volumes ONTAP及其关联的存储帐户之间使用 Azure Private Link 连接。 "了解Cloud Volumes ONTAP如何使用 Azure Private Link"

- Google Cloud

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

- 在您的场所

与云提供商的沟通

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

限制模式

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

"了解NetApp Console部署模式" 。

如何安装控制台代理

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

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

云提供商权限

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

在标准模式下使用控制台时，如何提供权限取决于您计划如何创建控制台代理。

要了解如何设置权限，请参阅以下内容：

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

要查看控制台代理日常操作所需的确切权限，请参阅以下页面：

- "了解控制台代理如何使用 AWS 权限"
- "了解控制台代理如何使用 Azure 权限"
- "了解控制台代理如何使用 Google Cloud 权限"

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

代理升级

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

当您在云端安装代理时，如果控制台代理可以访问互联网，则会自动更新。

操作系统和虚拟机维护

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

请注意，您（客户）在应用次要安全更新时不需要停止控制台主机上的任何服务。

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

执行此操作。

控制台代理必须始终处于运行状态 。

多系统和代理

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

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

以下是代理部署的一些示例：

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

了解NetApp Console身份和访问管理

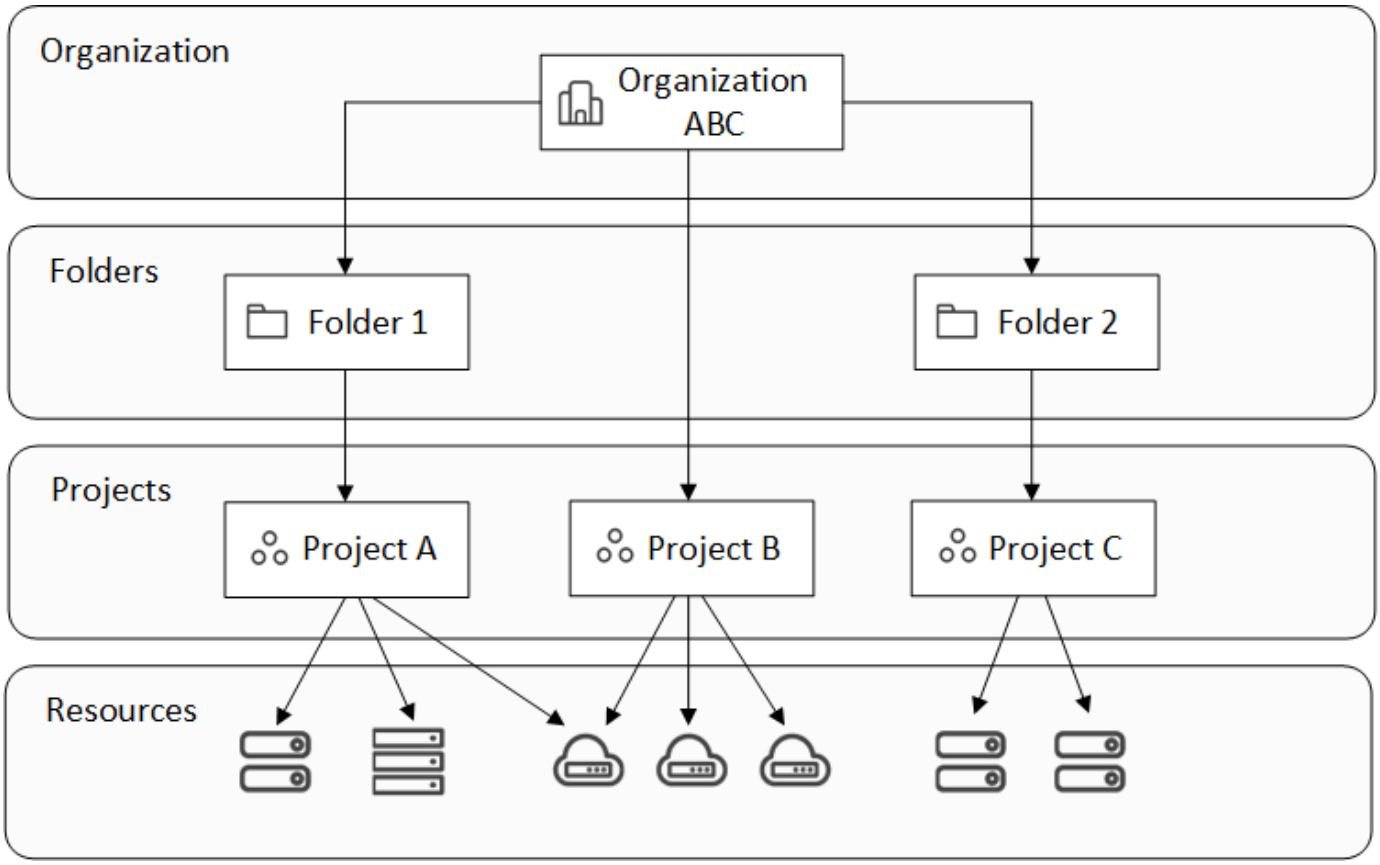
使用NetApp控制台的身份和访问管理 (IAM) 来组织您的NetApp资源，并根据您的业务结构（按位置、部门或项目）控制访问权限。

资源按层级排列：组织位于顶层，其次是文件夹（可以包含其他文件夹或项目），然后是项目，项目包含存储系统、工作负载和代理。

在组织、文件夹或项目级别为成员分配基于角色的访问控制 (RBAC) 权限，以确保用户拥有对资源的适当访问权限。

您必须拥有_超级管理员_、_组织管理员_或_文件夹或项目管理员_角色才能在NetApp Console中管理 IAM。

下图从基本层面说明了这一层次结构。



]

身份和访问管理组件

在NetApp Console中，您可以使用三个主要组件来组织存储资源：组织组件、资源组件和用户访问组件。

组织内的项目和文件夹

在您的 IAM 结构中，您使用三个组织组件：组织、项目和文件夹。您可以通过为用户分配以下任何级别的角色来授予他们访问权限。

组织

_组织_是控制台 IAM 系统的顶层，通常代表您的公司。您的组织由文件夹、项目、成员、角色和资源组成。代理与组织内的特定项目相关联。

项目

项目用于提供对存储资源的访问。必须先将资源分配给项目，其他人才能访问这些资源。您可以将多个资源分配给一个项目，也可以创建多个项目。然后，您可以为用户分配项目权限，使他们能够访问项目中的资源。

例如，您可以根据需要，将本地ONTAP系统与单个项目或组织中的所有项目关联起来。

"了解如何向您的组织添加项目。"

文件夹

将相关项目分组到_文件夹_中，以便按位置、站点或业务部门进行组织。您无法直接将资源与文件夹关联，但将用户分配到文件夹级别的角色，即可使其访问该文件夹中的所有项目。

"了解如何向您的组织添加文件夹。"

资源

资源包括存储系统、 Keystone订阅以及控制台代理。

+ 必须先将资源与项目关联，其他人才能访问该资源。

+

例如，您可以将Cloud Volumes ONTAP系统与一个项目或组织中的所有项目关联起来。资源的分配方式取决于贵组织的需求。

+

"了解如何将资源关联到项目。"

存储系统和**Keystone**订阅

存储系统是您在NetApp Console中管理的主要资源。NetApp Console支持对本地和云存储系统的管理。必须先在项目中添加存储系统，其他人才能访问该项目。

存储系统会自动与添加它们的项目关联，但您也可以从“资源”页面将它们与其他项目或文件夹关联。

Keystone订阅也是您可以与项目关联的资源，以便授予用户在NetApp Console中访问订阅的权限。

控制台代理

组织管理员创建控制台代理来管理存储系统并启用NetApp数据服务。代理最初与创建它们的项目关联，但管理员可以从“代理”页面将它们添加到其他项目或文件夹。

将代理与项目关联起来，可以管理该项目中的资源；而将代理与文件夹关联起来，可以让文件夹或项目管理员决定哪些项目应该使用该代理。代理人必须与特定项目关联才能提供管理能力。

"了解如何将代理商与项目关联起来。"

成员及角色

成员

您的组织的成员是用户帐户或服务帐户。应用程序通常使用服务帐户来完成指定的任务，而无需人工干预。

成员注册NetApp Console后，您需要将他们添加到您的组织中。添加完成后，您可以为他们分配角色，以便授予他们访问资源的权限。您可以手动从控制台添加服务帐户，也可以通过NetApp ConsoleIAM API 自动创建和管理服务帐户。

"了解如何向您的组织添加成员。"

访问角色

控制台提供您可以分配给组织成员的访问角色。

将成员与角色关联时，您可以为整个组织、特定文件夹或特定项目授予该角色。您选择的角色赋予成员对层次结构中选定部分的资源的权限。

NetApp Console提供细粒度的角色控制，遵循“最小权限”原则，这意味着访问角色旨在仅向用户授予其所需

的权限。

这意味着随着用户职责的增加，他们可能会被分配多个角色。

"了解访问角色" 。

IAM 策略示例

小型组织战略

对于用户少于 50 人且采用集中式存储管理的组织，可以考虑使用超级管理员和超级查看者角色的简化方法。

示例：**ABC**公司（**5**人团队）

- 组织结构： 单一组织，下设 3 个项目（生产、开发、备份）
- 角色：
  - 2 位高级成员：拥有*超级管理员*角色，可获得完整的管理权限
  - 3 名团队成员：*超级查看者*角色，拥有监控权限但无修改权限
- 代理策略：所有项目都关联一个代理，以实现资源共享访问。
- 优势：简化管理，降低角色复杂性，适合需要广泛访问权限的团队

多区域企业战略

对于拥有区域运营和专业团队的大型组织，应采用层级式方法，用文件夹表示地理或业务单元边界。

例如：**XYZ**公司（跨国公司）

- 结构： 组织结构 > 区域文件夹（北美、欧洲、亚太） > 每个区域的项目文件夹
- 平台角色：
  - 1 组织管理：全球监督和政策管理
  - 3 文件夹或项目管理员：区域控制（每个区域一个）
  - 1 联盟管理员：企业身份提供商集成
- 按区域划分的存储角色：
  - 9 存储管理员：发现和管理指定区域中的存储系统
  - 2 存储查看器：监控跨区域的存储资源
  - 1 系统健康专家：无需修改系统即可管理存储健康状况
- 数据服务角色：
  - 备份和恢复管理员：按项目根据备份职责而定
  - 勒索软件恢复管理员：负责跨项目的安全团队监控
- 代理策略：与相应地理项目相关的区域代理
- 优势： 通过角色分离、区域自主权和遵守当地法规来增强安全性

对于拥有需要特定数据服务访问权限的专业团队的组织，应根据职能职责进行有针对性的角色分配。

例如：**TechCorp**（一家中型科技公司）

- 结构： 组织 > 部门文件夹（IT、安全、开发） > 项目特定资源
- 专业岗位：
  - 安全团队：*勒索软件恢复管理员*和*分类查看器*角色
  - 备份团队：备份和恢复超级管理员，负责全面的备份操作
  - 开发团队：测试环境管理存储管理员
  - 合规团队：运营支持分析师，负责监控和支持案例管理
- 代理策略： 根据资源所有权将代理与部门项目关联起来
- 优势： 可定制的访问控制、更高的运营效率以及明确的专项任务责任划分

NetApp Console中 IAM 的后续步骤

- "开始使用NetApp Console中的 IAM"
- "监控或审计 IAM 活动"
- "了解NetApp Console IAM 的 API"

NetApp Console (SaaS) 入门

入门工作流程（SaaS）

要开始使用NetApp Console(SaaS)，请先准备控制台的网络，注册并创建帐户，然后使用控制台助手设置初始功能。

您可以访问由NetApp提供的基于 Web 的控制台，该控制台是软件即服务 (SaaS) 产品。您可以使用控制台管理混合云存储环境并使用NetApp数据服务。

1 "准备使用**NetApp**控制台的网络"

确保访问NetApp控制台的计算机能够通过网络访问所需的端点。

"了解如何为NetApp控制台配置网络。"

2 "注册并创建组织"

前往 "NetApp控制台" 并注册。如果系统提示您创建组织，而您认为您的公司已经存在组织，请关闭对话框并告知您的组织管理员。如果贵公司目前没有组织管理员，您可以认领此角色。 "了解如何联系组织管理员。"

此时，您已登录，可以使用NetApp助手开始配置控制台。首先，请将您的NetApp支持帐户与控制台代理关联，以启用全部功能。

如果您选择不使用NetApp助手或安装控制台代理，您可以开始管理存储并使用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 关联您的**NetApp**支持站点 **(NSS)** 帐户

将您的NetApp支持站点 (NSS) 帐户与控制台关联，可以更轻松地管理您的许可证和订阅，并直接从控制台访问支持资源。

4 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"

5 为主机添加存储系统

在NetApp Console中，您可以添加或发现存储系统来管理您的混合云存储环境。使用NetApp助手添加您的第一个存储系统。

如果在 AWS、Microsoft Azure 或 Google Cloud 中安装控制台代理，则控制台会自动发现代理安装位置的 Amazon S3 存储桶、Azure Blob 存储或 Google Cloud Storage 存储桶的相关信息。这些系统会自动添加到“系统”页面。

- "了解如何发现ONTAP系统"
- "了解如何发现StorageGRID系统"
- "了解如何发现 E 系列系统"

6 "订阅**NetApp Intelligent Services**（可选）"

通过您的云提供商注册NetApp Intelligent Services ，即可按小时（按需付费）或按年计费。订阅包含NetApp Backup and Recovery、 Cloud Volumes ONTAP、 NetApp Cloud Tiering、 NetApp Ransomware Resilience、NetApp Disaster Recovery和NetApp Data Classification。

准备**NetApp Console**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 Console的计算机
- 您在本地或云端安装的控制台代理。控制台代理。

> 在 4.0.0 中， 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 Console和控制台代理联系的端点

您部署的每个代理和访问NetApp Console的每台计算机都必须连接到下面列出的端点。

部署在您的云提供商中的控制台代理需要访问该云提供商各自的端点。

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

云提供商端点联系了控制台代理

如果控制台代理部署在您的云提供商中，则它们必须能够访问其他端点。

在安装控制台代理之前设置云提供商网络端点访问。

- "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"

控制台代理联系的数据服务端点

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"

工作负载端点

控制台代理必须能够访问以下NetApp工作负载端点。

端点	目的
https://api.workloads.netapp.com	基于 Web 的控制台通过与 Workload Factory API 交互来管理和操作基于ONTAP 的FSx 工作负载。

注册或登录**NetApp Console**

要使用控制台，请注册或使用您的NetApp支持站点凭据登录，或者创建NetApp Console登录。如果您是公司第一个注册的人，您将创建一个新的组织并担任管理员。如果贵公司已有组织，请使用您现有的NetApp支持站点凭据或公司单点登录 (SSO) 注册或登录。

以初始组织管理员身份注册**NetApp Console**

如果贵公司还没有NetApp Console组织，请注册创建一个。第一个用户将成为组织管理员，并管理用户帐户和权限。您可以稍后更新角色并添加更多管理员。

步骤

1. 打开 Web 浏览器并转到 "NetApp Console"
2. 如果您拥有NetApp支持站点帐户，请直接在“登录”页面上输入与您的帐户关联的电子邮件地址。

   控制台会在您首次登录时使用您的NetApp支持站点凭据进行注册。

3. 如果您想通过创建控制台登录来注册，请选择*注册*。
   a. 在*注册*页面上，输入所需信息并选择*下一步*。

      注册表格中只允许使用英文字符。

   b. 检查您的收件箱，查找来自NetApp的电子邮件，其中包含验证您的电子邮件地址的说明。

      请验证您的电子邮件地址以完成注册。

4. 登录后，请阅读并接受最终用户许可协议。
5. 在“欢迎”页面上，创建一个组织。
6. 选择*让我们开始吧*。

+ 作为首次用户和组织管理员，您可以按照引导流程添加存储资源、创建控制台代理等等。 "了解如何使用控制台助手。"

下一步

作为管理员，在完成控制台助手中包含的步骤后，您应该规划身份和访问策略，将用户添加到您的组织，并分配角色。 "了解NetApp Console的身份和访问管理"

如果组织已存在，请注册或登录**NetApp Console**。

如果贵公司已有NetApp Console组织，请注册或登录以访问它。您的注册或登录方式取决于您的公司是否使用身份联合或拥有NetApp支持站点凭据。如果还没有，请创建NetApp Console登录帐户。

步骤

1. 打开 Web 浏览器并转到 "NetApp Console"
2. 如果您拥有NetApp支持站点帐户，或者您的公司已设置单点登录 (SSO)，请在“登录”页面上输入您关联的电子邮件地址或 SSO 凭据。按照提示完成登录。

   在这两种情况下，您都会在初始登录时注册控制台。

3. 如果您想通过创建控制台登录来注册，请选择*注册*。
   a. 在*注册*页面上，输入所需信息并选择*下一步*。

      注册表格中只允许使用英文字符。

   b. 检查您的收件箱，查找来自NetApp的电子邮件，其中包含验证您的电子邮件地址的说明。

      请验证您的电子邮件地址以完成注册。

4. 登录后，请阅读并接受最终用户许可协议。
5. 如果系统提示您创建组织，请关闭对话框并告知控制台管理员，以便他们可以将您添加到控制台组织并授予您访问权限。 "了解如何联系组织管理员。"

下一步

获得组织访问权限后，即可开始管理存储和使用分配给您的数据服务。

开始使用**NetApp Console**助手

如果您是首次使用NetApp Console(SaaS) 并拥有组织管理员角色的用户，则可以使用控制台助手来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您的数据。

访问控制台助手所需的角色

控制台助手仅对具有组织管理员角色的用户可用。

默认情况下，对于具有组织管理员角色的首次用户， NetApp Console会在主页上显示控制台助手。在您完成创建控制台代理和添加系统的必要任务之前，它将一直可用。

使用助手完成以下任务，这些任务将为您的NetApp Console环境提供最基本的设置：

- 添加NetApp支持站点 (NSS) 帐户。

  "了解如何添加 NSS 帐户"。

- 通过部署控制台代理连接到您的存储环境。

  "了解如何在本地安装控制台代理。"

- 通过添加或发现集群来管理存储系统
- 添加市场订阅或 PAYGO 许可证。

  "了解如何添加许可证和订阅"。

- 查看数据服务信息。

NetApp Console入门（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 Console。

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"。

"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。

"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 Console。
3. 向控制台代理提供您之前设置的权限。

"订阅NetApp Intelligent Services（可选）"

可选：从云提供商的市场订阅NetApp Intelligent Services，以按小时费率（PAYGO）或通过年度合同支付数据服务费用。 NetApp Intelligent Services包括NetApp Backup and Recovery、 Cloud Volumes ONTAP、 NetApp Cloud Tiering、 NetApp Ransomware Resilience和NetApp Disaster Recovery。 NetApp Data Classification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 Console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**：了解限制模式的工作原理

在开始之前了解NetApp Console在受限模式下的工作方式。

使用已安装的NetApp Console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 Console。

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

第 **3** 步：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

控制台代理需要专用主机。只要满足以下尺寸要求，任何架构都受支持：

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

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

  - `/var`：必须有 40 GiB 可用空间

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

AWS EC2 实例类型

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

Azure VM 大小

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

Google Cloud 机器类型

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

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

虚拟机管理程序

需要经过认证可运行受支持的操作系统的裸机或托管虚拟机管理程序。

操作系统和容器要求

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

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

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

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 **1.** 步骤

Podman

按照以下步骤安装和配置 Podman：

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

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

步骤

1. 如果主机上安装了 podman-docker 包，请将其删除。

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

2. 安装 Podman。

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

   a. 对于 Red Hat Enterprise Linux 9.6：

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

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

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

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

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

   c. 对于 Red Hat Enterprise Linux 8：

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

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

3. 启用并启动 podman.socket 服务。

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

4. 安装 python3。

```
sudo dnf install python3
```

5. 如果您的系统上还没有 EPEL 存储库包，请安装它。

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

6. 如果使用 Red Hat Enterprise 9：

   a. 安装EPEL存储库软件包。

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

   +

   a. 安装 podman-compose 包 1.5.0。

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

7. 如果使用的是 Red Hat Enterprise Linux 8：

   a. 安装EPEL存储库软件包。

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

   b. 安装 podman-compose 包 1.0.6。

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

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

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

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

```
podman info | grep networkBackend
```

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

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

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

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

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

v. 重新启动 podman。

```
systemctl restart podman
```

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

```
podman info | grep networkBackend
```

Docker 引擎

按照 Docker 的文档安装 Docker Engine。

步骤

1. "查看 Docker 的安装说明"

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

2. 验证 Docker 是否已启用并正在运行。

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

步骤 **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 Console**

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 Console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 Console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 Console的 SaaS 服务以及各自公共云环境中的端点。

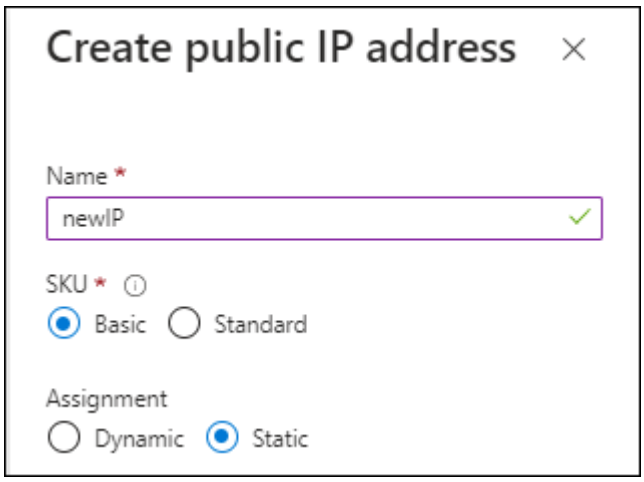
端点	目的
AWS 环境	AWS 服务（amazonaws.com）： • 云形成 • 弹性计算云（EC2） • 身份和访问管理 (IAM) • 密钥管理服务（KMS） • 安全令牌服务 (STS) • 简单存储服务（S3）
管理 AWS 资源。端点取决于您的 AWS 区域。 "有关详细信息，请参阅 AWS 文档"	Amazon FsX for NetApp ONTAP： • api.workloads.netapp.com
基于 Web 的控制台通过与 Workload Factory API 交互来管理和操作基于ONTAP 的FSx 工作负载。	Azure 环境

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

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

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

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 Console。

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 Console一起使用的每个 Azure 订阅添加 ID。

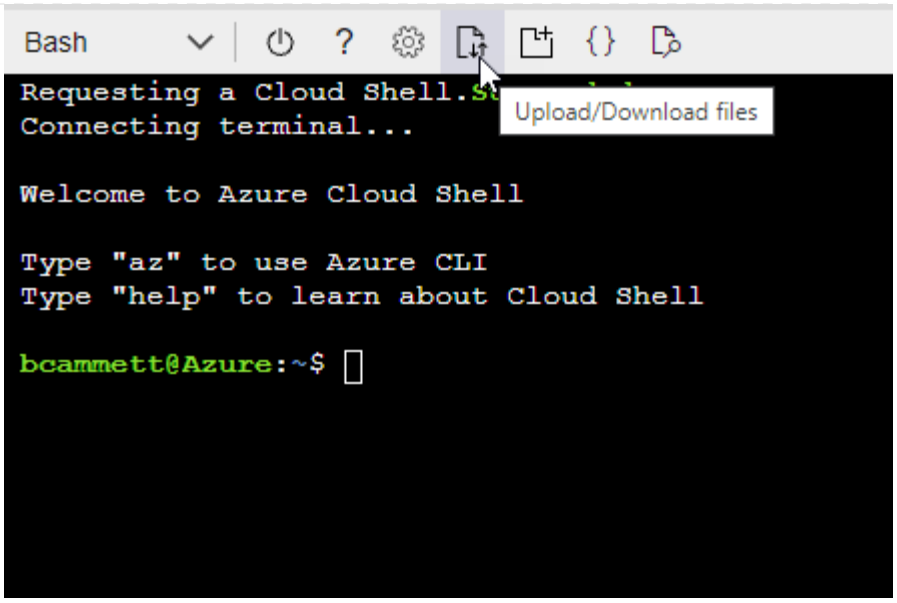
   例子

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

4. 使用 JSON 文件在 Azure 中创建自定义角色。

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

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



c. 使用 Azure CLI 创建自定义角色：

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

Azure 服务主体

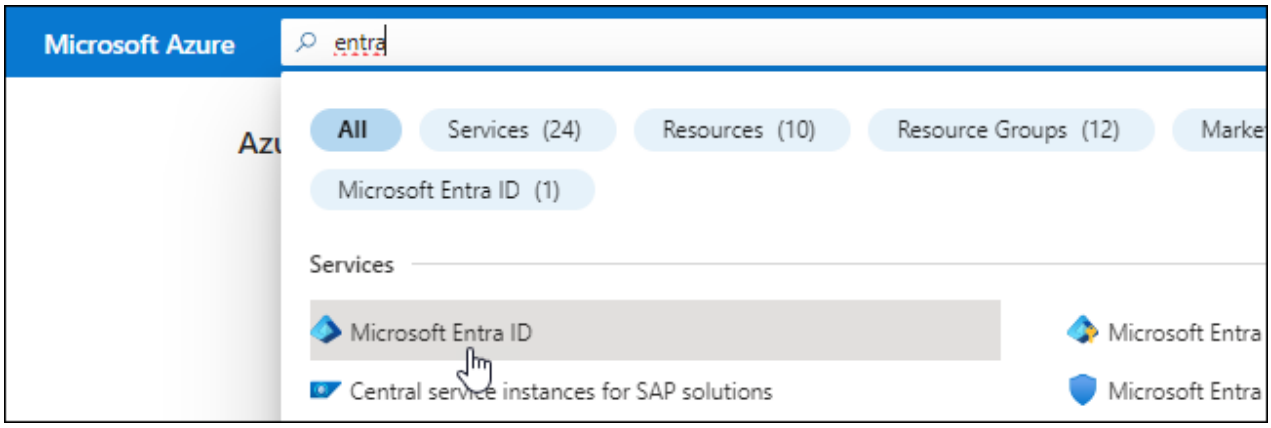
在 Microsoft Entra ID 中创建并设置服务主体，并获取控制台所需的 Azure 凭据。安装控制台代理后，您需要向控制台提供这些凭据。

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 Console一起使用）。
- 重定向 **URI**：您可以将此字段留空。

6. 选择*注册*。

您已创建 AD 应用程序和服务主体。

将应用程序分配给角色

1. 创建自定义角色：

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

a. 复制"控制台代理的自定义角色权限"并将它们保存在 JSON 文件中。

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

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

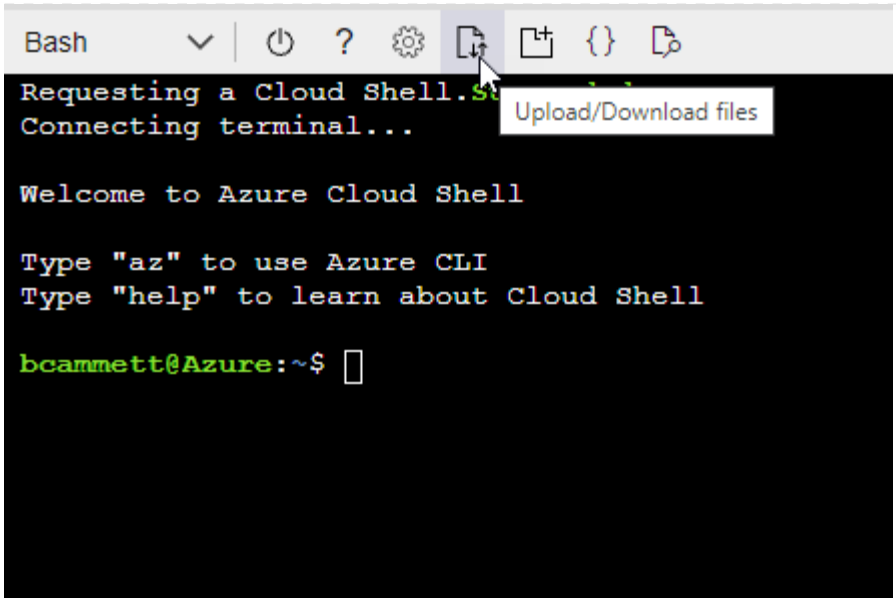
例子

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

c. 使用 JSON 文件在 Azure 中创建自定义角色。

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

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



- 使用 Azure CLI 创建自定义角色：

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

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

2. 将应用程序分配给角色：

a. 从 Azure 门户打开 **Subscriptions** 服务。

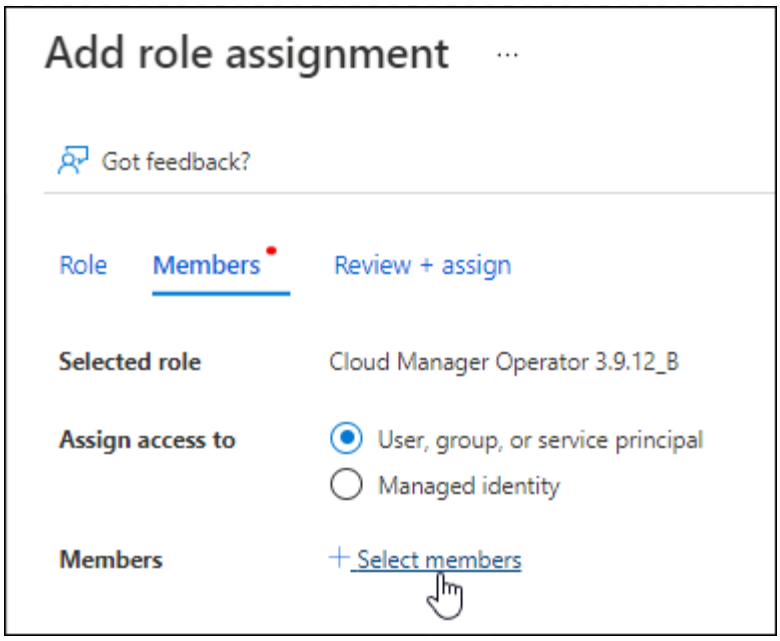
b. 选择订阅。

c. 选择“访问控制 (IAM)”>“添加”>“添加角色分配”。

d. 在*角色*选项卡中，选择*控制台操作员*角色并选择*下一步*。

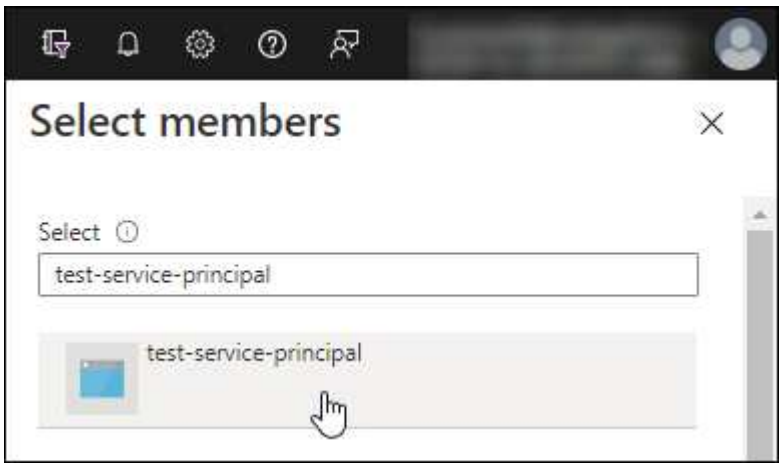
e. 在“成员”选项卡中，完成以下步骤：

- 保持选中“用户、组或服务主体”。
- 选择*选择成员*。



- 搜索应用程序的名称。

  以下是一个例子：



- 选择应用程序并选择*选择*。
- 选择“下一步”。

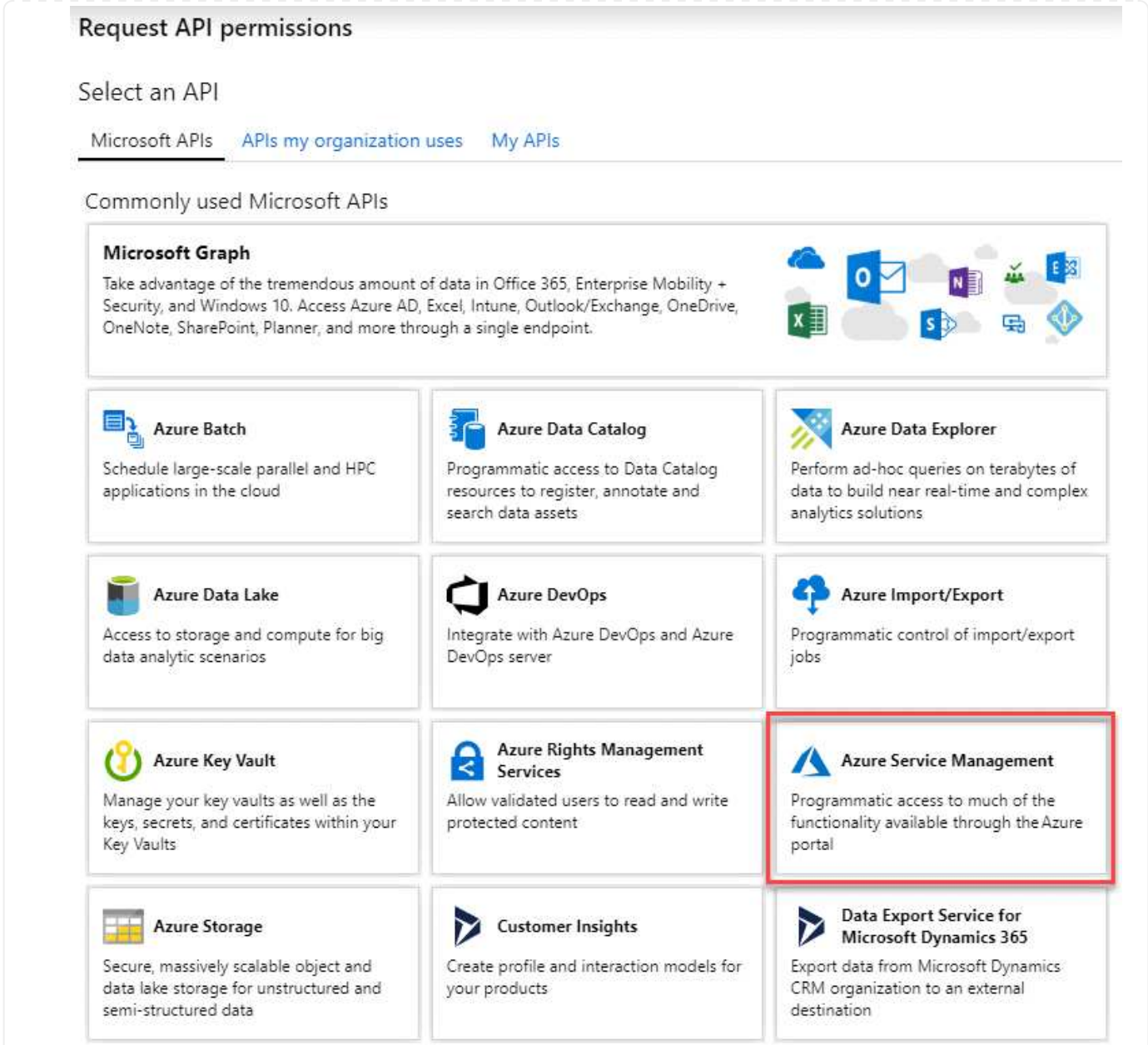
f. 选择*审阅+分配*。

服务主体现在具有部署控制台代理所需的 Azure 权限。

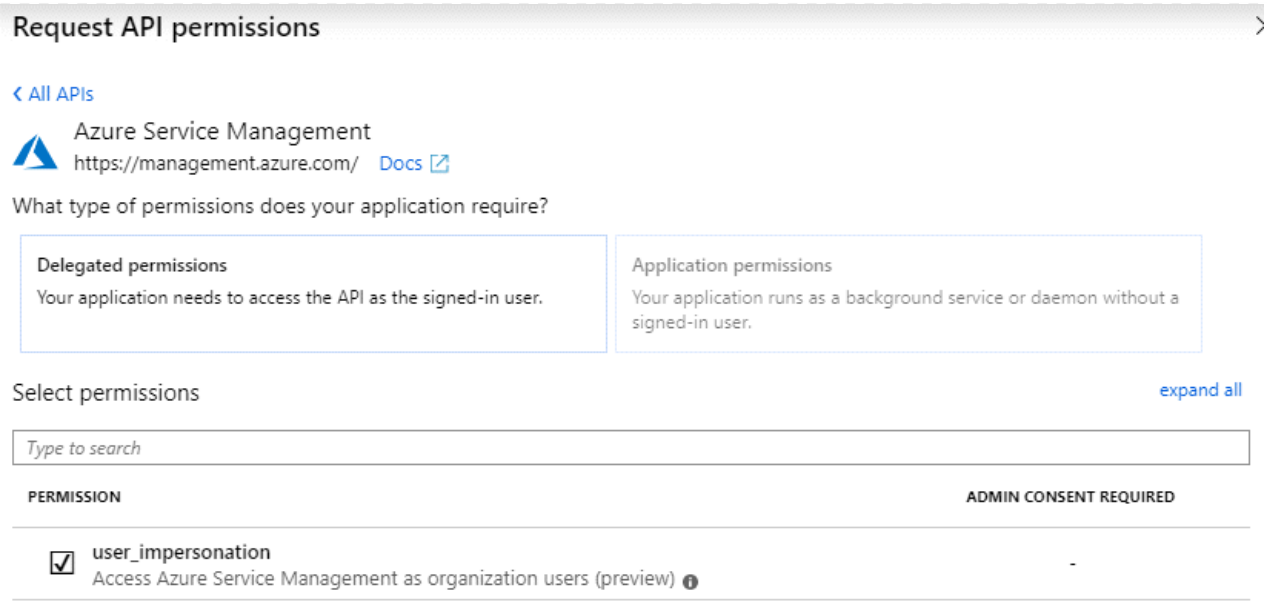
如果您想从多个 Azure 订阅部署Cloud Volumes ONTAP ，则必须将服务主体绑定到每个订阅。在NetApp Console中，您可以选择部署Cloud Volumes ONTAP时要使用的订阅。

添加 **Windows Azure** 服务管理 **API** 权限

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

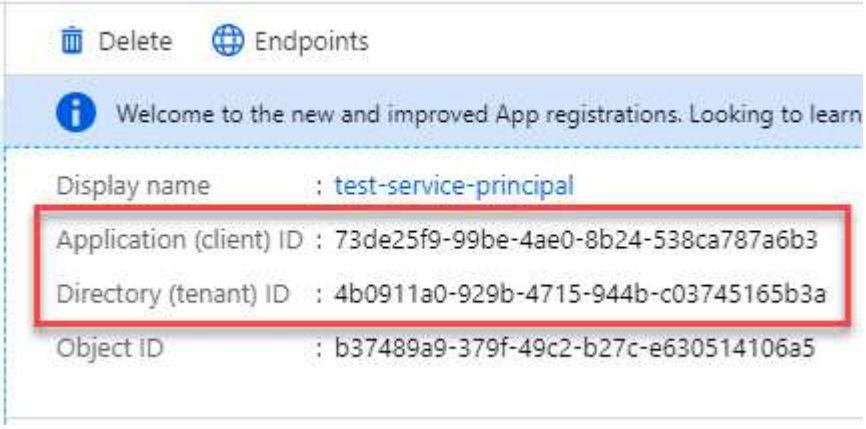


4. 选择*以组织用户身份访问 Azure 服务管理*，然后选择*添加权限*。



获取应用程序的应用程序**ID**和目录**ID**

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



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

创建客户端机密

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

结果

您的服务主体现已设置完毕，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“agent”的角色：

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

   +
   "Google Cloud 文档：创建和管理自定义角色"

2. 在 Google Cloud 中创建服务帐号：

   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"

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"
    - 云基础设施管理器 API
    - 云部署管理器 V2 API
    - 云日志 API
    - 云资源管理器 API
    - 计算引擎 API
    - 身份和访问管理 (IAM) API
    - 云密钥管理服务 (KMS) API

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

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 Console。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。

安装控制台代理之前，您需要先准备好环境。您可以从 AWS Marketplace、Azure Marketplace 安装，也可以在您自己的运行于 AWS、Azure 或 Google Cloud 中的 Linux 主机上手动安装。

AWS 商业市场

开始之前

需要以下物品：

- 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。
- 了解代理的 CPU 和 RAM 要求。

  "审查代理要求"。

- EC2 实例的密钥对。

步骤

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

   订阅过程可能需要几分钟。

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

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

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

       "查看 AWS 的安全组规则" 。

- 配置存储：保留根卷的默认大小和磁盘类型。

  如果要在根卷上启用 Amazon EBS 加密，请选择 高级，展开 卷 **1**，选择 加密，然后选择一个 KMS 密钥。

- 高级详细信息：在 **IAM** 实例配置文件 下，选择包含控制台代理所需权限的 IAM 角色。
- 摘要：查看摘要并选择*启动实例*。

结果

AWS 使用指定的设置启动软件。控制台代理大约需要五分钟即可部署。

下一步是什么?

设置NetApp Console。

AWS 政府市场

开始之前

需要以下物品：

- 满足组网需求的VPC及子网。

  "了解网络要求"

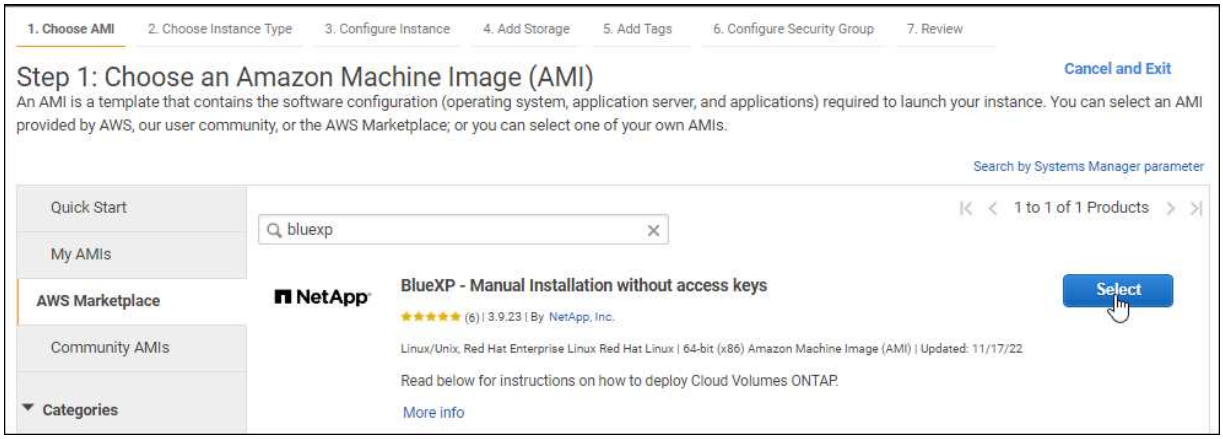
- 具有附加策略的 IAM 角色，其中包含控制台代理所需的权限。

  "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 Console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。



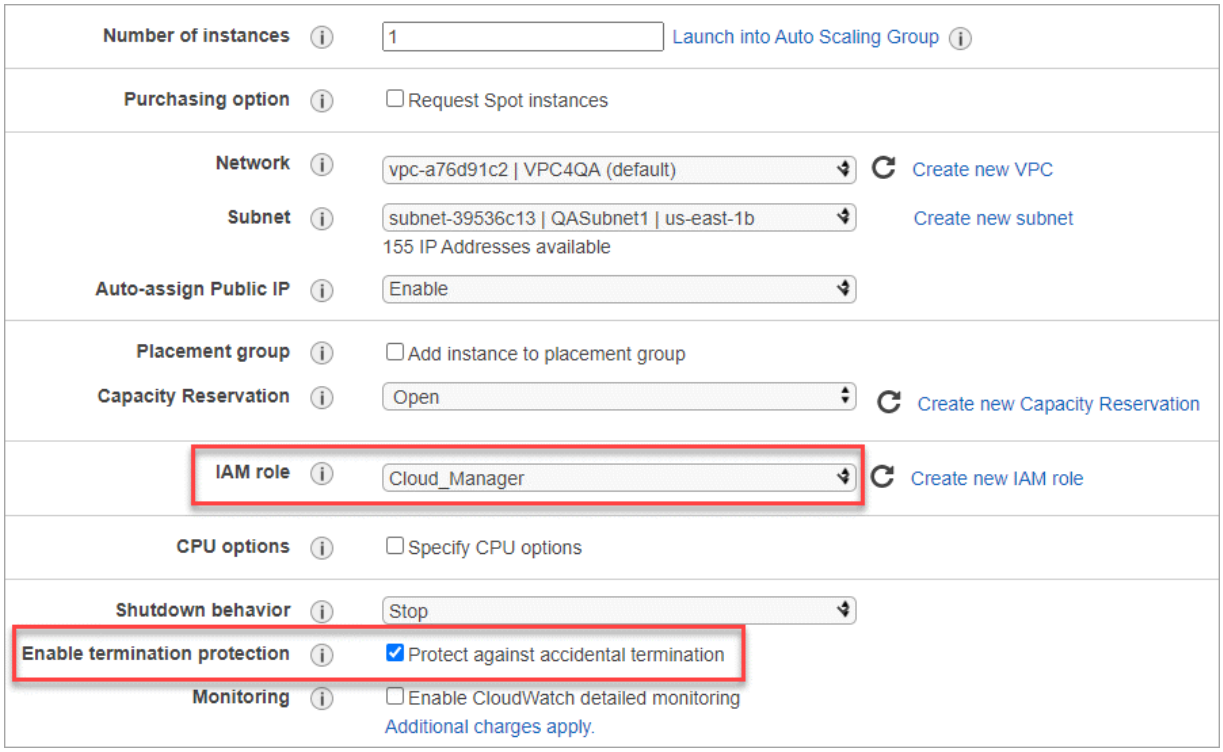
d. 选择*继续*。

2. 按照提示设置并启动实例：

   - 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。控制台代理大约需要五分钟即可部署。

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。

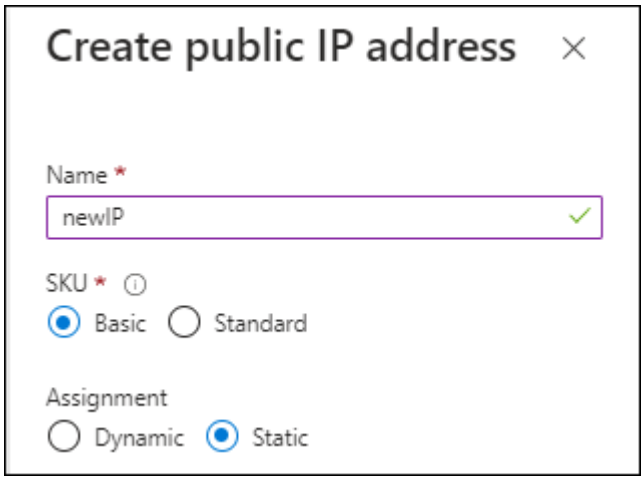
  "了解如何设置 Azure 权限"

步骤

1. 转到 Azure 市场中的NetApp Console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。
   - 公网 **IP**：要将公网 IP 地址与控制台代理 VM 一起使用，请选择基本 SKU。



   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。如果用于访问控制台的计算机无法访问私有 IP 地址，则控制台将无法工作。

   "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*。

     托管标识允许控制台代理虚拟机无需凭据即可向 Microsoft Entra ID 进行身份验证。 "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 Console。

手动安装（必须用于 **Google Cloud**）

您可以将控制台代理手动安装到运行在 AWS、Azure 或 Google Cloud 上的 Linux 主机上。

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

安装后，如果有新版本可用，控制台代理会自动更新。

步骤

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

```
unset http_proxy
unset https_proxy
```

   如果不删除这些系统变量，安装将失败。

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

     选择下载代理安装程序文件或文件的 URL。

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

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

其中 <version> 是您下载的控制台代理的版本。

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

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

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

如果要配置透明代理，可以在安装完成后进行配置。 "了解代理维护控制台"

+

以下是使用 CA 签名证书配置显式代理服务器的示例：

+

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

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

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

+ 注意以下事项：

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

+ 例如：

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

1. 如果您使用 Podman，则需要调整 aardvark-dns 端口。
   a. 通过 SSH 连接到控制台代理虚拟机。

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

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

例如：

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

a. 重新启动控制台代理虚拟机。

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 Console。

第 2 步：设置NetApp Console

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另一个组织关联，您需要注册一个新的登录信息。否则，您将在设置屏幕上看不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 Console。
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**：向控制台代理提供权限

如果您是从 Azure Marketplace 或手动安装的控制台代理，则需要授予您之前设置的权限。

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 Console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 Console内完成操作的能力将受到影响。

   "Microsoft Azure 文档：了解 Azure RBAC 的范围"

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

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

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

Azure 服务主体

向NetApp Console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
        - 客户端密钥
    c. 市场订阅：通过立即订阅或选择现有订阅将市场订阅与这些凭证关联。
    d. 审核：确认有关新凭证的详细信息并选择*添加*。

结果

NetApp Console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 Intelligent Services**（受限模式）

从云提供商的市场订阅NetApp Intelligent Services，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 Backup and Recovery
- Cloud Volumes ONTAP
- NetApp Cloud Tiering
- NetApp Ransomware Resilience
- NetApp Disaster Recovery

NetApp Data Classification可通过您的订阅启用，但使用分类是免费的。

开始之前

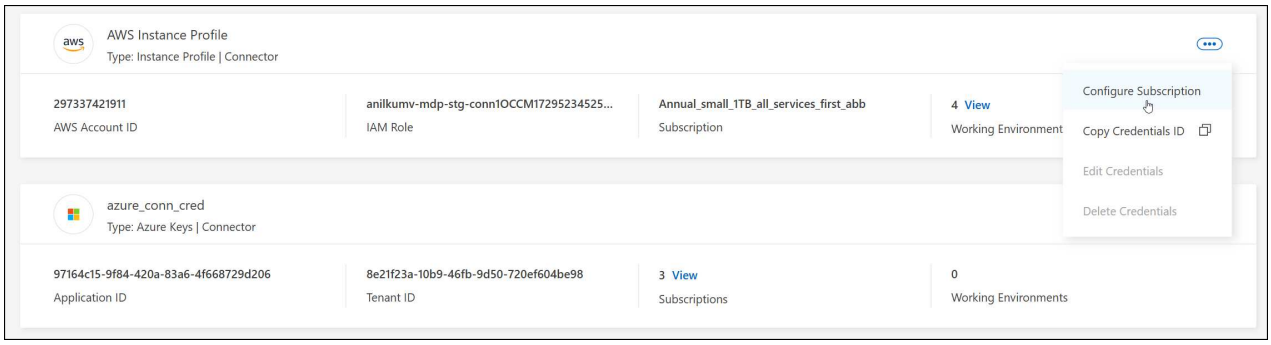
您必须已经部署控制台代理才能订阅数据服务。您需要将市场订阅与连接到控制台代理的云凭据关联起来。

AWS

步骤

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

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



4. 要将凭据与现有订阅关联，请从下拉列表中选择订阅并选择*配置*。
5. 要将凭证与新订阅关联，请选择“添加订阅”>“继续”*，然后按照 AWS Marketplace 中的步骤操作：

   a. 选择“查看购买选项”。

   b. 选择*订阅*。

   c. 选择*设置您的帐户*。

      您将被重定向到NetApp Console。

   d. 从“订阅分配”页面：

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

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

   对于所有其他组织或帐户，您需要重复这些步骤来手动关联订阅。

   ◦ 选择*保存*。

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 Console关联的凭据关联。

4. 要将凭据与现有订阅关联，请从下拉列表中选择订阅并选择*配置*。
5. 要将凭据与新订阅关联，请选择“添加订阅”>“继续”*，然后按照 Azure 市场中的步骤操作：

    a. 如果出现提示，请登录您的 Azure 帐户。

    b. 选择*订阅*。

    c. 填写表格并选择*订阅*。

    d. 订阅过程完成后，选择*立即配置帐户*。

    您将被重定向到NetApp Console。

    e. 从“订阅分配”页面：

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

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

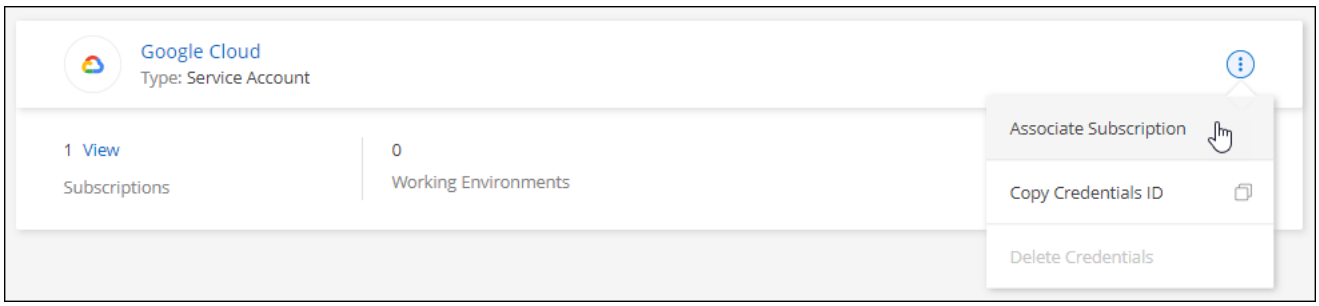
对于所有其他组织或帐户，您需要重复这些步骤来手动关联订阅。

- 选择*保存*。

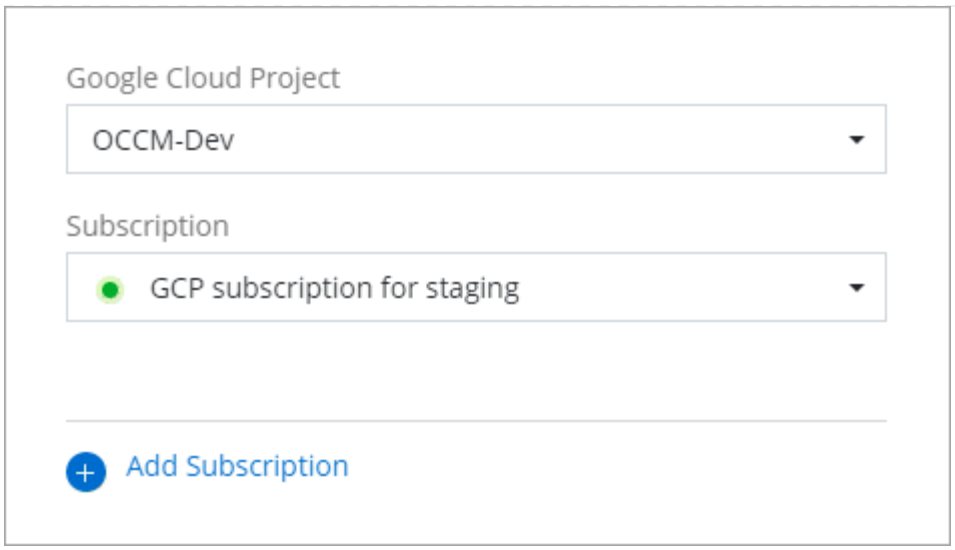
Google Cloud

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*。



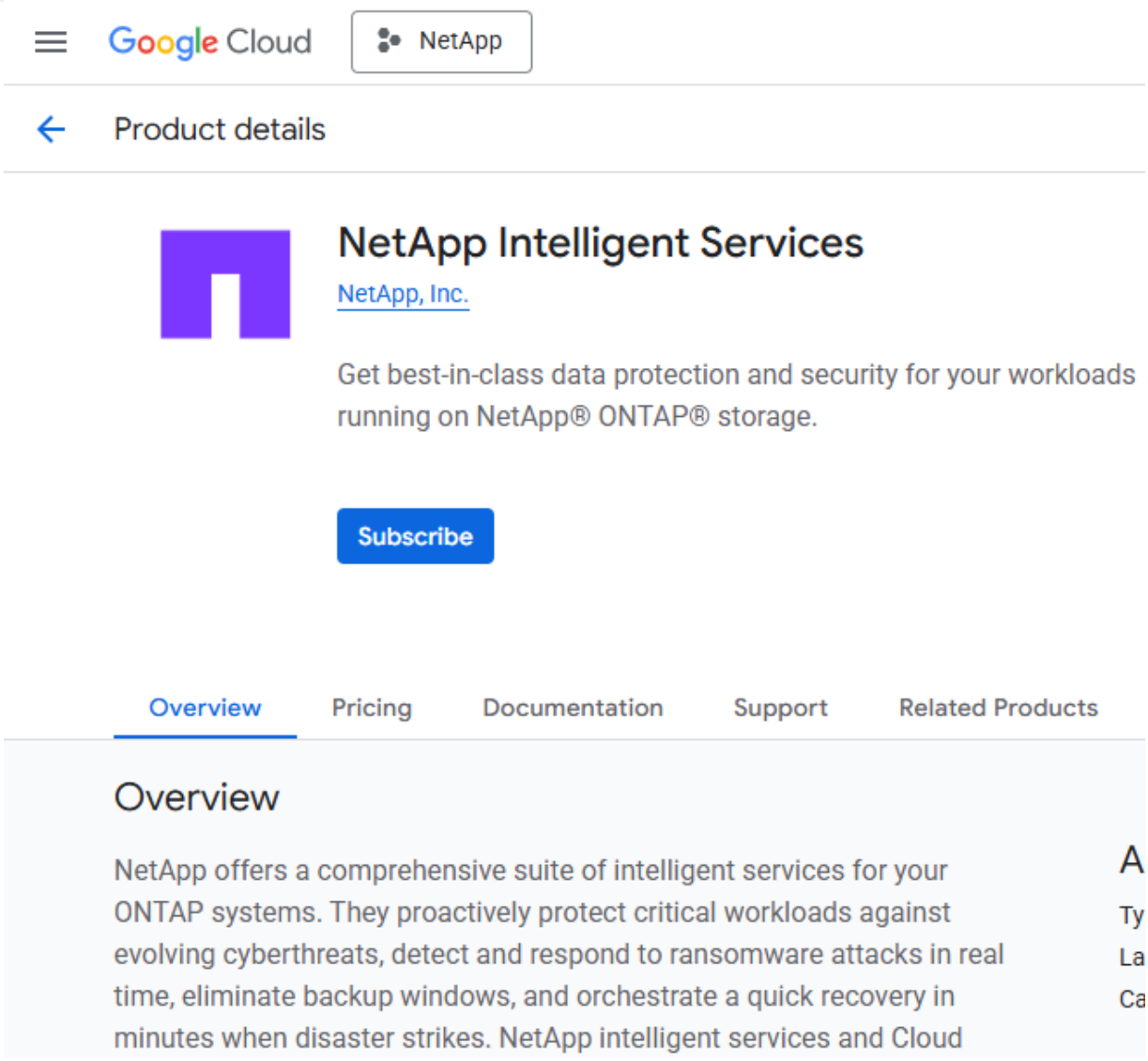
1. 要使用选定的凭据配置现有订阅，请从下拉列表中选择一个 Google Cloud 项目和订阅，然后选择*配置*。



2. 如果您还没有订阅，请选择*添加订阅>继续*并按照 Google Cloud Marketplace 中的步骤操作。

   在完成以下步骤之前，请确保您在 Google Cloud 帐户中同时拥有 Billing Admin 权限以及NetApp Console登录权限。

   a. 在您被重定向到 "Google Cloud Marketplace 上的NetApp Intelligent Services页面"，确保在顶部导航菜单中选择了正确的项目。



b. 选择*订阅*。

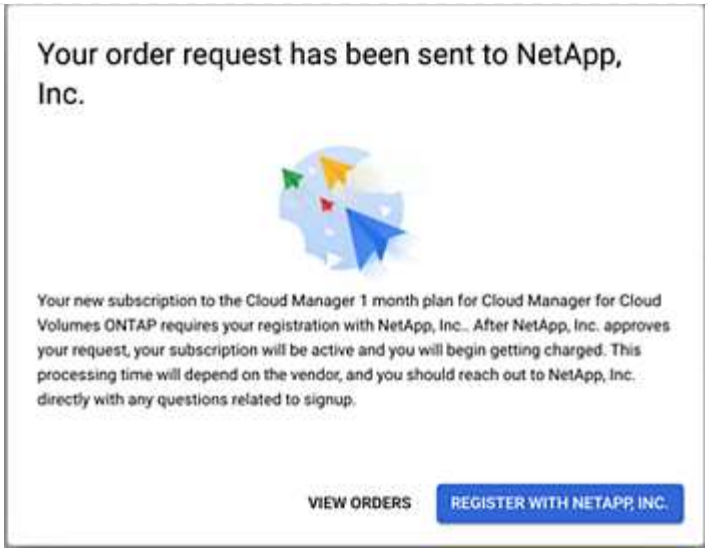
c. 选择适当的结算账户并同意条款和条件。

d. 选择*订阅*。

此步骤将您的转移请求发送给NetApp。

e. 在弹出的对话框中，选择*向NetApp, Inc. 注册*。

必须完成此步骤才能将 Google Cloud 订阅与您的控制台组织或帐户关联。直到您从此页面重定向并登录到控制台后，链接订阅的过程才完成。



f. 完成“订阅分配”页面上的步骤：

> 如果您组织中的某人已经从您的结算帐户中订阅了市场，那么您将被重定向到"NetApp Console中的Cloud Volumes ONTAP页面"反而。如果这是意外情况，请联系您的NetApp销售团队。 Google 为每个 Google 结算帐户仅启用一项订阅。

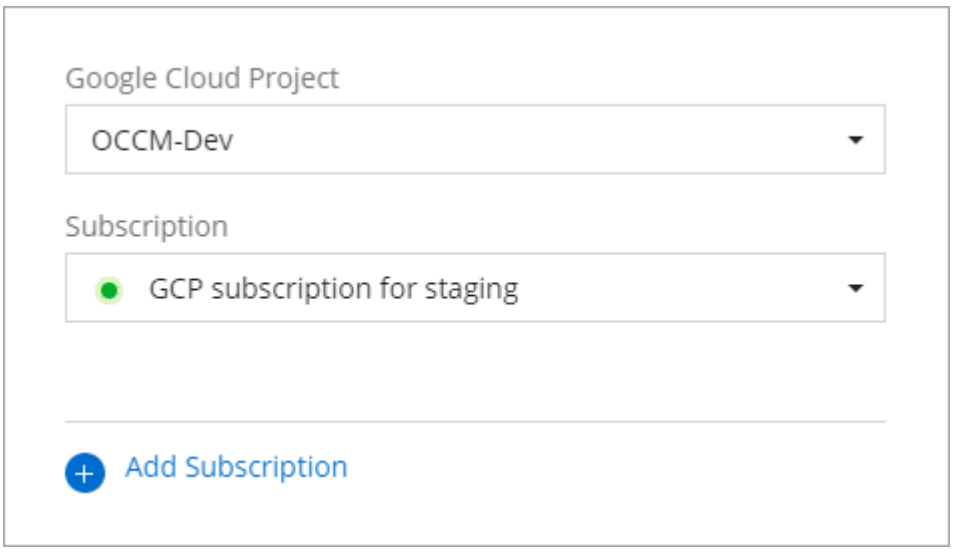
- 选择您想要与此订阅关联的控制台组织。
- 在“替换现有订阅”字段中，选择是否要用这个新订阅自动替换一个组织的现有订阅。

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

对于所有其他组织或帐户，您需要重复这些步骤来手动关联订阅。

◦ 选择*保存*。

3. 此过程完成后，导航回控制台中的“凭据”页面并选择此新订阅。



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 Console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 Console部署模式"

开始使用私人模式

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
服务	警报	否
	备份和恢复	是的https://docs.netapp.com/us-en/data-services-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
	勒索软件抵御能力	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

产品领域	**BlueXP**服务或功能	私人模式
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