



# 设置和管理 **Cloud Manager**

## Set up and administration

NetApp  
July 13, 2022

# 目录

设置和管理 Cloud Manager .....	1
发行说明 .....	2
新增功能 .....	2
已知限制 .....	10
入门 .....	12
了解 Cloud Manager .....	12
入门检查清单 .....	13
注册到 NetApp Cloud Central .....	16
登录到 Cloud Manager .....	17
设置 NetApp 帐户 .....	18
设置连接器 .....	26
下一步行动 .....	63
管理 Cloud Manager .....	64
NetApp 帐户 .....	64
连接器 .....	79
AWS 凭据 .....	105
Azure credentials .....	113
Google Cloud 凭据 .....	127
在 Cloud Manager 中添加和管理 NetApp 支持站点帐户 .....	134
参考 .....	141
Cloud Manager 权限摘要 .....	141
Connector 的 AWS 权限 .....	142
Connector 的 Azure 权限 .....	166
适用于 Connector 的 Google Cloud 权限 .....	173
知识和支持 .....	178
注册以获得支持 .....	178
获取帮助 .....	179
法律声明 .....	181
版权 .....	181
商标 .....	181
专利 .....	181
隐私政策 .....	181
开放源代码 .....	181

# 设置和管理 **Cloud Manager**

# 发行说明

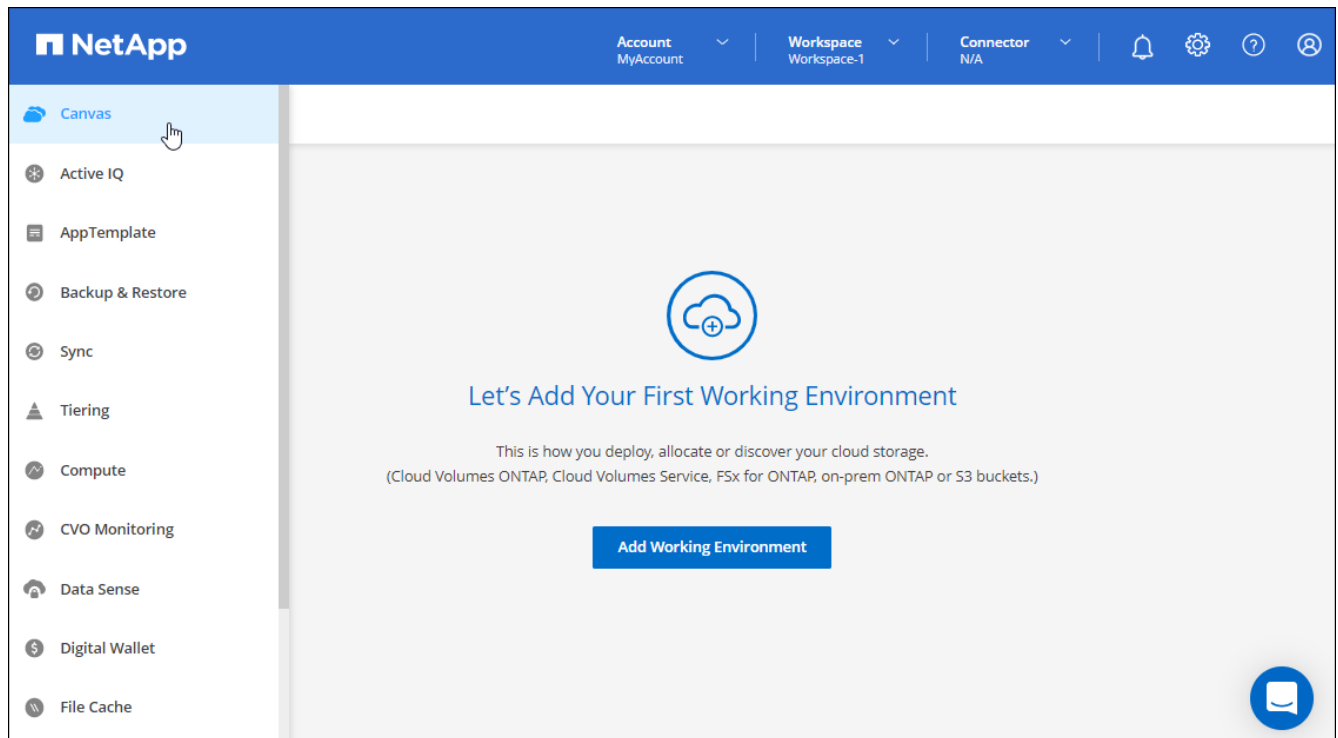
## 新增功能

了解 Cloud Manager 管理功能的新增功能： NetApp 帐户，连接器，云提供商凭据等。

**2022年7月3日**

### 连接器3.9.20

- 我们引入了一种新方法来自导航到Cloud Manager界面中不断增长的功能列表。现在、将鼠标悬停在左侧面板上即可轻松找到所有熟悉的Cloud Manager功能。



- 现在、您可以将Cloud Manager配置为通过电子邮件发送通知、这样、即使您未登录到系统、您也可以了解重要的系统活动。


["了解有关监控帐户中操作的更多信息"](#)。

- Cloud Manager现在支持Azure Blob存储和Google Cloud Storage作为工作环境、类似于Amazon S3支持。


在Azure或Google Cloud中安装Connector后、Cloud Manager现在会自动发现您的Azure订阅中的Azure Blob存储或安装了Connector的项目中的Google Cloud Storage的相关信息。Cloud Manager将对象存储显示为一个工作环境、您可以打开该环境以查看更多详细信息。

下面是Azure Blob工作环境的示例：


Overview



283  
Total Storage Accounts



2.26 TiB  
Total Capacity



7  
Total Locations

283 Storage Accounts

Storage Account Name	Subscription	Location	Creation Date	Resource Group	Blob Capacity
fqlcxn3ciw6dtim	OCCM Dev	West Europe	June 28, 2022	KobiAzureCvoSpillover2-rg	618.75 KiB
qniz6nq8x0yakb6	OCCM Dev	West Europe	June 28, 2022	KobiAzureCvoSpillover2-rg	170 B
8mqefjrtjco24lp	OCCM Dev	West Europe	June 28, 2022	KobiAzureCvoSpillover-rg	170 B
8tqosluboxoedvk	OCCM Dev	West Europe	June 28, 2022	KobiAzureCvoSpillover-rg	618.75 KiB

- 我们重新设计了Amazon S3工作环境的资源页面、提供了有关S3存储分段的更多详细信息、例如容量、加密详细信息等。
- 现在、以下Google Cloud地区支持Connector：
  - 马德里(欧洲-西南1)
  - 巴黎(欧洲-西部9)
  - 华沙(欧洲中部2)
- 现在、Azure West US 3区域支持Connector。

["查看支持的区域的完整列表"](#)

- 此版本的连接器还包括Cloud Volumes ONTAP 增强功能。

["了解Cloud Volumes ONTAP 增强功能"](#)

## 2022年6月28日

### 使用NetApp凭据登录

当新用户注册到Cloud Central时、他们现在可以选择\*使用NetApp\*登录选项以使用其NetApp支持站点凭据登录。这是输入电子邮件地址和密码的替代方法。



使用电子邮件地址和密码的现有登录需要继续使用该方法。注册的新用户可以使用"Log in with NetApp"选项。

## 2022年6月7日

### 连接器3.9.19

- 现在、AWS雅加达地区(亚太地区东南部3)支持Connector。
- 现在、Azure巴西东南部地区支持Connector。

["查看支持的区域的完整列表"](#)

- 此版本的Connector还包括Cloud Volumes ONTAP 增强功能和内部ONTAP 集群增强功能。
  - ["了解Cloud Volumes ONTAP 增强功能"](#)
  - ["了解ONTAP 内部集群增强功能"](#)

## 2022年5月12日

### 连接器3.9.18修补程序

我们更新了Connector以引入错误修复。最值得注意的修复方法是、当问题描述 位于共享VPC中时、它会影响Google Cloud中的Cloud Volumes ONTAP 部署。

## 2022年5月2日

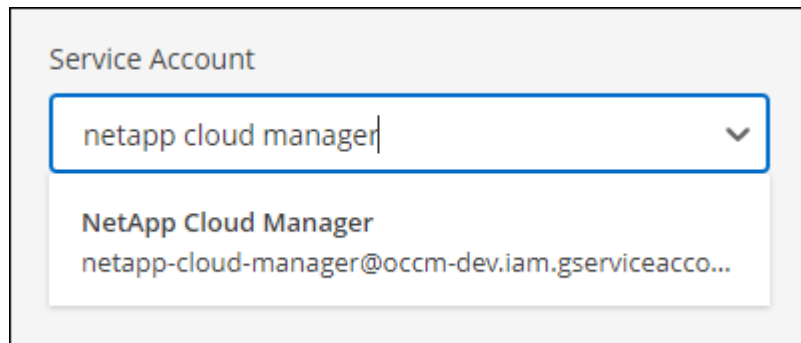
### 连接器3.9.18

- 现在、以下Google Cloud地区支持Connector：

- 新德里(亚洲-南2)
- 墨尔本(澳大利亚南部2)
- 米兰(欧洲-西部8)
- 圣地亚哥(南美洲-西维1)

["查看支持的区域的完整列表"](#)

- 当您选择要与Connector结合使用的Google Cloud服务帐户时、Cloud Manager现在会显示与每个服务帐户关联的电子邮件地址。通过查看电子邮件地址、可以更轻松地地区分同名服务帐户。



- 我们已在具有支持的操作系统的VM实例上对Google Cloud中的Connector进行了认证 ["屏蔽VM功能"](#)
- 此版本的连接器还包括Cloud Volumes ONTAP 增强功能。 ["了解这些增强功能"](#)
- 要使Connector能够部署Cloud Volumes ONTAP 、需要新的AWS权限。

现在、在单个可用性区域(AZ)中部署HA对时、创建AWS分布放置组需要以下权限：

```
"ec2:DescribePlacementGroups",
"iam:GetRolePolicy"
```

现在、要优化Cloud Manager创建布局组的方式、需要这些权限。

请务必为您添加到Cloud Manager的每组AWS凭据提供这些权限。 ["查看Connector的最新IAM策略"](#)。

## 2022 年 4 月 3 日

### 连接器3.9.17

- 现在，您可以通过让 Cloud Manager 承担您在环境中设置的 IAM 角色来创建 Connector 。此身份验证方法比共享 AWS 访问密钥和机密密钥更安全。

["了解如何使用 IAM 角色创建连接器"](#)。

- 此版本的连接器还包括Cloud Volumes ONTAP 增强功能。 ["了解这些增强功能"](#)

## 2022 年 2 月 27 日

### 连接器3.9.16

- 在 Google Cloud 中创建新的 Connector 时， Cloud Manager 现在将显示所有现有防火墙策略。以前，Cloud Manager 不会显示任何没有目标标记的策略。
- 此版本的连接器还包括Cloud Volumes ONTAP 增强功能。 ["了解这些增强功能"](#)

## 2022 年 1 月 30 日

### 连接器3.9.15

此版本的连接器包含Cloud Volumes ONTAP 增强功能。 ["了解这些增强功能"](#)

## 2022 年 1 月 2 日

### 减少了连接器的端点

我们减少了 Connector 为管理公有云环境中的资源和流程而需要联系的端点数量。

["查看所需端点的列表"](#)。

### 用于 Connector 的 EBS 磁盘加密

现在，当您从 Cloud Manager 在 AWS 中部署新的 Connector 时，您可以选择使用默认主密钥或托管密钥对 Connector 的 EBS 磁盘进行加密。

✓ Get Ready

✓ AWS Credentials

3 Details

4 Network

5 Security Group

6 Review

## Details

Connector Instance Name

Connector1

Connector Role

☒ Create Role ☐ Select an existing Role

Role Name

Cloud-Manager-Operator-9yils3K

+ Add Tags to Connector Instance

☒ AWS Managed Encryption

Master Key: aws/ebs (default) [Change Key](#)

**NSS** 帐户的电子邮件地址

Cloud Manager 现在可以显示与 NetApp 支持站点帐户关联的电子邮件地址。





2021 年 11 月 28 日

### NetApp 支持站点帐户需要更新

从 2021 年 12 月开始，NetApp 现在使用 Microsoft Azure Active Directory 作为身份提供程序来提供特定于支持和许可的身份验证服务。执行此更新后，Cloud Manager 将提示您更新先前添加的任何现有 NetApp 支持站点帐户的凭据。

如果您尚未将 NSS 帐户迁移到 IDaaS，则首先需要迁移此帐户，然后在 Cloud Manager 中更新凭据。

- ["了解如何将 NSS 帐户更新为新的身份验证方法"](#)。
- ["了解有关 NetApp 使用 Microsoft Azure AD 进行身份管理的更多信息"](#)

### 更改 Cloud Volumes ONTAP 的 NSS 帐户

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

["了解如何将工作环境附加到其他 NSS 帐户"](#)。

## 2021 年 11 月 4 日

### SOC 2 类型 2 认证

一家独立的认证公有会计师事务所和服务审计师对 Cloud Manager ， Cloud Sync ， Cloud Tiering ， Cloud Data sense 和 Cloud Backup （ Cloud Manager 平台）进行了检查，并确认他们已根据适用的信任服务标准获得 SOC 2 类型 2 报告。

["查看 NetApp 的 SOC 2 报告"](#)。

### 不再支持将连接器用作代理

您不能再使用 Cloud Manager Connector 作为代理服务器从 Cloud Volumes ONTAP 发送 AutoSupport 消息。此功能已被删除，不再受支持。您需要通过 NAT 实例或环境的代理服务提供 AutoSupport 连接。

["了解有关使用 Cloud Volumes ONTAP 验证 AutoSupport 的更多信息"](#)

## 2021 年 10 月 31 日

### 使用服务主体进行身份验证

在 Microsoft Azure 中创建新的 Connector 时，您现在可以使用 Azure 服务主体进行身份验证，而不是使用 Azure 帐户凭据进行身份验证。

["了解如何使用 Azure 服务主体进行身份验证"](#)。

### 凭据增强功能

我们重新设计了 "凭据" 页面，以便于使用，并与 Cloud Manager 界面的当前外观一致。

## 2021 年 9 月 2 日

### 已添加新的通知服务

通知服务已推出，因此您可以查看在当前登录会话期间启动的 Cloud Manager 操作的状态。您可以验证操作是否成功或失败。 ["了解如何监控帐户中的操作"](#)。

## 2021 年 8 月 1 日

### Connector 支持 RHEL 7.9

现在，运行 Red Hat Enterprise Linux 7.9 的主机支持 Connector 。

["查看 Connector 的系统要求"](#)。

## 2021 年 7 月 7 日

### 添加连接器向导的增强功能

我们重新设计了 \* 添加连接器 \* 向导，以添加新选项并使其更易于使用。现在，您可以添加标记，指定角色（对

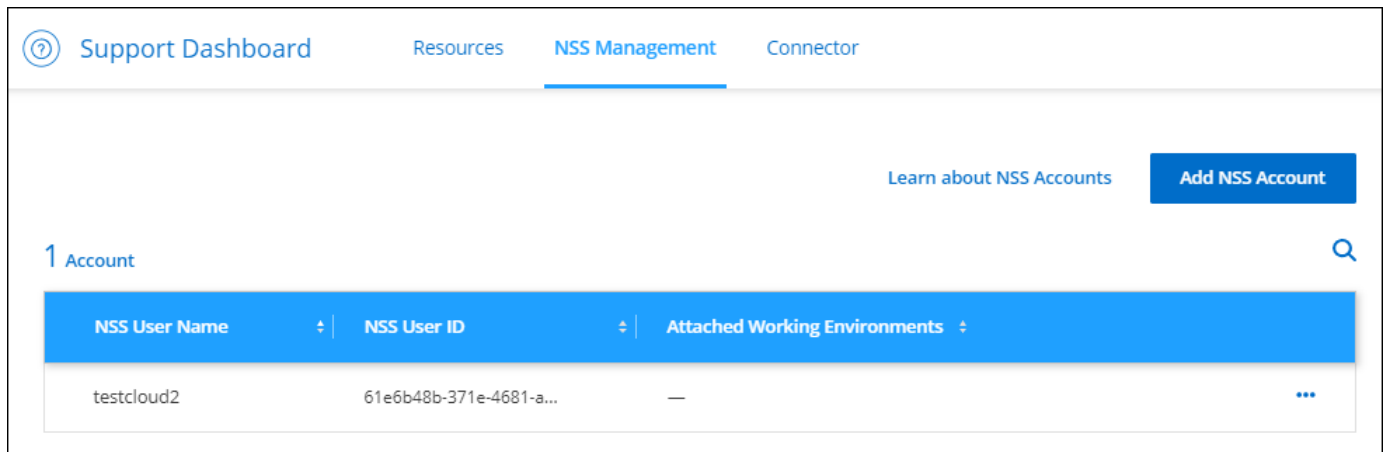
于 AWS 或 Azure），上传代理服务器的根证书，查看 Terraform 自动化的代码，查看进度详细信息等。

- ["在 AWS 中创建连接器"](#)
- ["在 Azure 中创建连接器"](#)
- ["在 GCP 中创建连接器"](#)

通过支持信息板管理 **NSS** 帐户

现在，NetApp 支持站点（NSS）帐户可通过支持信息板进行管理，而不是从设置菜单进行管理。通过此更改，可以更轻松地从一个位置查找和管理所有与支持相关的信息。

["了解如何管理 NSS 帐户"](#)。



## 2021 年 5 月 5 日

时间线中的帐户

Cloud Manager 中的时间线现在显示与帐户管理相关的操作和事件。这些操作包括关联用户，创建工作空间和创建连接器等。如果您需要确定执行特定操作的人员，或者需要确定操作的状态，则检查时间线会很有帮助。

["了解如何筛选租户服务的时间线"](#)。

## 2021 年 4 月 11 日

**API 直接调用 Cloud Manager**

如果您配置了代理服务器，则现在可以启用一个选项，在不通过代理的情况下直接向 Cloud Manager 发送 API 调用。在 AWS 或 Google Cloud 中运行的 Connectors 支持此选项。

["了解有关此设置的更多信息"](#)。

服务帐户用户

现在，您可以创建服务帐户用户。

服务帐户充当 "用户"，可以通过授权 API 调用 Cloud Manager 来实现自动化。这样可以更轻松地管理自动化，因为您不需要基于可以随时离开公司的真实用户帐户构建自动化脚本。如果您使用的是联合，则可以创建令牌

，而无需从云生成刷新令牌。

["了解有关使用服务帐户的更多信息"](#)。

## 私有预览

现在，您可以在帐户中允许进行私有预览，以便访问新的 NetApp 云服务，因为这些服务在 Cloud Manager 中作为预览版提供。

["了解有关此选项的更多信息"](#)。

## 第三方服务

您还可以允许帐户中的第三方服务访问 Cloud Manager 中提供的第三方服务。

["了解有关此选项的更多信息"](#)。

## 2021 年 2 月 9 日

### 支持信息板改进

我们更新了支持信息板，允许您添加 NetApp 支持站点凭据，以便为您注册支持。您也可以直接从信息板启动 NetApp 支持案例。只需单击帮助图标，然后单击 \* 支持 \*。

## 已知限制

已知限制确定了本产品版本不支持的平台、设备或功能、或者这些平台、设备或功能无法与产品正确交互操作。仔细审查这些限制。

这些限制特定于 Cloud Manager 的设置和管理：Connector，SaaS 平台等。

### 连接器限制

可能与 **172** 范围内的 **IP** 地址冲突

Cloud Manager 使用 IP 地址位于 172.17.0.0/16 和 172.18.0.0/16 范围的两个接口部署 Connector。

如果您的网络配置了其中任一范围的子网，则可能会在 Cloud Manager 中遇到连接失败。例如，在 Cloud Manager 中发现内部 ONTAP 集群可能会失败。

请参见知识库文章 ["Cloud Manager Connector IP 与现有网络冲突"](#) 有关如何更改连接器接口的 IP 地址的说明。

### 仅支持 HTTP 代理服务器

如果您的公司策略要求您使用代理服务器与 Internet 进行所有 HTTP 通信，则必须将您的连接器配置为使用该 HTTP 代理服务器。代理服务器可以位于云中或网络中。

Cloud Manager 不支持在 Connector 中使用 HTTPS 代理。

## 不支持 SSL 解密

Cloud Manager 不支持启用了 SSL 解密的防火墙配置。如果启用了 SSL 解密，则 Cloud Manager 中会显示错误消息，并且 Connector 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 时显示空白页面

如果加载 Connector 的本地用户界面，则 UI 有时可能无法显示，您只会看到一个空白页面。

此问题描述与缓存问题相关。临时解决策将使用匿名或专用 Web 浏览器会话。

## 不支持共享 Linux 主机

与其他应用程序共享的 VM 不支持此连接器。虚拟机必须专用于 Connector 软件。

## 第三方代理和扩展

Connector VM 不支持第三方代理或 VM 扩展。

## SaaS 限制

对于政府区域，**SaaS** 平台已禁用

如果您在 AWS GovCloud 区域，Azure Gov 区域或 Azure DoD 区域部署 Connector，则只能通过 Connector 的主机 IP 地址访问 Cloud Manager。对整个帐户禁用对 SaaS 平台的访问。

这意味着，只有能够访问最终用户内部 VPC-vNet 的有权限用户才能使用 Cloud Manager 的 UI 或 API。

请注意、这些地区仅支持Cloud Volumes ONTAP、云备份、云数据感知和复制服务。政府地区不支持任何其他NetApp服务。

["了解如何在Connector上访问本地UI"](#)。

## 市场限制

### Azure 和 Google Cloud 合作伙伴不支持按需购买

如果您是 Microsoft Cloud 解决方案提供商（CSP）合作伙伴或 Google Cloud 合作伙伴，则不提供 NetApp 按需购买订阅。您必须购买许可证并使用 BYOL 许可证部署 NetApp 云解决方案。

以下 NetApp 云服务不支持按需购买订阅：

- Cloud Volumes ONTAP
- 云分层
- 云备份
- 云数据感知

# 入门

## 了解 Cloud Manager

借助 Cloud Manager，IT 专家和云架构师可以使用 NetApp 的云解决方案集中管理其混合多云基础架构。

### 功能

Cloud Manager 是一款基于 SaaS 的企业级管理平台，无论数据位于何处，都能让您始终掌控数据。

- 设置和使用 ["Cloud Volumes ONTAP"](#) 跨云实现高效的多协议数据管理。
- 设置和使用文件存储服务：
  - ["Azure NetApp Files"](#)
  - ["适用于 ONTAP 的 Amazon FSX"](#)
  - ["适用于 AWS 的 Cloud Volumes Service"](#)
  - ["适用于 Google Cloud 的 Cloud Volumes Service"](#)
- 通过创建卷，备份到云，跨混合云复制数据以及将冷数据分层到云，发现和管理内部 ONTAP 集群。
- 启用集成云服务，例如：
  - ["云数据感知"](#)
  - ["Cloud Insights"](#)
  - ["云备份"](#)

["了解有关 Cloud Manager 的更多信息"](#)。

### 支持的对象存储提供程序

Cloud Manager 支持您在 Amazon Web Services，Microsoft Azure 和 Google Cloud 中管理云存储并使用云服务。

### 成本

NetApp 免费提供 Cloud Manager 软件。

对于大多数任务，Cloud Manager 会提示您在云网络中部署 Connector，这会导致云提供商为计算实例和关联存储收取费用。您可以选择在内部运行 Connector 软件。

["了解Connector的默认配置"](#)。

### Cloud Manager 的工作原理

Cloud Manager 包括一个与 NetApp Cloud Central 集成的基于 SaaS 的界面，以及用于管理 Cloud Volumes ONTAP 和其他云服务的 Connectors。

软件即服务

Cloud Manager 可通过访问 ["基于 SaaS 的用户界面"](#) 和 API。通过这种 SaaS 体验，您可以在最新功能发布后自动访问这些功能，并轻松在 NetApp 客户和连接器之间切换。

NetApp Cloud Central

["NetApp Cloud Central"](#) 提供一个用于访问和管理的集中位置 ["NetApp 云服务"](#)。通过集中式用户身份验证，您可以使用同一组凭据来访问 Cloud Manager 以及 Cloud Insights 等其他云服务。

NetApp 帐户

首次登录到 Cloud Manager 时，系统会提示您创建 `_NetApp 帐户 _`。此帐户可提供多租户，并可用于在隔离的 `_workworkworkspace _` 中组织用户和资源。

连接器

大多数情况下，客户管理员需要在云或内部网络中部署 *Connector*。借助此连接器， Cloud Manager 可以管理公有云环境中的资源和流程。

连接器应始终保持运行状态。对于您启用的服务的持续运行状况和运行来说，这一点非常重要。

例如、连接器是Cloud Volumes ONTAP 运行状况和运行的关键组件。如果某个连接器已关闭、则使用基于节点的许可的Cloud Volumes ONTAP PAYGO系统将在与某个连接器失去通信超过14天之后关闭。

["详细了解何时需要连接器及其工作原理"](#)。

SOC 2 类型 2 认证

一家独立的认证公有会计师事务所和服务审计师对 Cloud Manager ， Cloud Sync ， Cloud Tiering ， Cloud Data sense 和 Cloud Backup （ Cloud Manager 平台）进行了检查，并确认他们已根据适用的信任服务标准获得 SOC 2 类型 2 报告。

["查看 NetApp 的 SOC 2 报告"](#)

入门检查清单

使用此检查清单可了解在 Connector 具有出站 Internet 访问权限的典型部署中启动和运行 Cloud Manager 所需的资源。

NetApp Cloud Central 登录

您需要注册到 ["NetApp Cloud Central"](#) 以便您可以访问 Cloud Manager 和其他云服务。

从 Web 浏览器到多个端点的网络访问

可以从 Web 浏览器访问 Cloud Manager 用户界面。使用 Cloud Manager 用户界面时，它会联系多个端点来完成数据管理任务。运行 Web 浏览器的计算机必须连接到以下端点：

端点	目的
<a href="http://cloudmanager.netapp.com">http://cloudmanager.netapp.com</a>	使用 SaaS UI 时，您的 Web 浏览器会联系此 URL。

端点	目的
AWS 服务（AmazonAWS.com）： <ul style="list-style-type: none"> <li>• 云形成</li> <li>• Cognito</li> <li>• 弹性计算云（EC2）</li> <li>• 密钥管理服务（KMS）</li> <li>• 安全令牌服务（STS）</li> <li>• 简单存储服务 (S3)</li> </ul>	在 AWS 中部署 Cloud Manager 中的 Connector 时需要使用。确切的端点取决于部署 Connector 的区域。 <a href="#">"有关详细信息，请参阅 AWS 文档。"</a>
<a href="https://management.azure.com">https://management.azure.com</a> <a href="https://login.microsoftonline.com">https://login.microsoftonline.com</a>	在大多数 Azure 地区部署 Cloud Manager 中的 Connector 时需要此功能。
<a href="https://management.microsoftazure.de">https://management.microsoftazure.de</a> <a href="https://login.microsoftonline.de">https://login.microsoftonline.de</a>	在 Azure 德国地区部署 Cloud Manager 中的 Connector 时需要此许可证。
<a href="https://management.usgovcloudapi.net">https://management.usgovcloudapi.net</a> <a href="https://login.microsoftonline.com">https://login.microsoftonline.com</a>	在 Azure US Gov 地区部署 Cloud Manager 中的 Connector 时需要此许可证。
<a href="https://www.googleapis.com">https://www.googleapis.com</a>	在 Google Cloud 中部署 Cloud Manager 中的 Connector 时需要使用。
<a href="https://signin.b2c.netapp.com">https://signin.b2c.netapp.com</a>	更新 NetApp 支持站点（NSS）凭据或向 Cloud Manager 添加新的 NSS 凭据时需要此功能。
<a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a> <a href="https://cdn.auth0.com">https://cdn.auth0.com</a> <a href="https://services.cloud.netapp.com">https://services.cloud.netapp.com</a>	您的 Web 浏览器连接到这些端点、以便通过 NetApp Cloud Central 进行集中式用户身份验证。
<a href="https://widget.intercom.io">https://widget.intercom.io</a>	用于与 NetApp 云专家交流的产品内聊天。
连接器的 IP 地址	<p>在大多数情况下，您应该从 SaaS UI 使用 Cloud Manager，但是 <a href="#">"使用本地 UI 时"</a>，然后必须从 Web 浏览器输入主机的 IP 地址。</p> <p>根据与云提供商的连接，使用分配给主机的专用 IP 或公有 IP：</p> <ul style="list-style-type: none"> <li>• 如果您拥有 VPN 并直接访问虚拟网络，则专用 IP 可以正常工作</li> <li>• 公有 IP 可用于任何网络连接情形</li> </ul> <p>无论哪种情况，都可以通过确保安全组规则仅允许从授权的 IP 或子网进行访问来确保网络访问的安全。</p>

## Connector 的出站网络连接

登录到 Cloud Manager 后，客户管理员需要在云提供商或内部网络中部署 *Connector*。借助此连接器，Cloud Manager 可以管理公有云环境中的资源和流程。Azure NetApp Files，Cloud Volumes Service 或 Cloud Sync 不需要连接器，但 Cloud Manager 中的所有其他服务和功能都需要连接器。 ["了解有关连接器及其工作原理的更多信息"](#)。



- 部署 Connector 的网络位置必须具有出站 Internet 连接。

连接器需要通过出站 Internet 访问来联系以下端点，以便管理公有云环境中的资源和流程。

端点	目的
<a href="https://support.netapp.com">https://support.netapp.com</a>	获取许可信息并向 NetApp 支持部门发送 AutoSupport 消息。
<a href="https://*.cloudmanager.cloud.netapp.com">https://*.cloudmanager.cloud.netapp.com</a>	在 Cloud Manager 中提供 SaaS 功能和服务。
<a href="https://cloudmanagerinfraprod.azurecr.io">https://cloudmanagerinfraprod.azurecr.io</a> <a href="https://*.blob.core.windows.net">https://*.blob.core.windows.net</a>	升级 Connector 及其 Docker 组件。

- 如果您选择在自己的 Linux 主机上手动安装 Connector（而不是直接从 Cloud Manager 界面安装），则 Connector 的安装程序需要在安装过程中访问以下端点：
  - <https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm>
  - <https://s3.amazonaws.com/aws-cli/awscli-bundle.zip>
  - [https://\\*.blob.core.windows.net](https://*.blob.core.windows.net) 或 <https://hub.docker.com>

主机可能会在安装期间尝试更新操作系统软件包。主机可以联系这些操作系统软件包的不同镜像站点。

- 除非您启动 Connector，否则不会向其传入流量。

通过 HTTP（80）和 HTTPS（443），您可以访问本地 UI，在极少数情况下，您可以使用此界面。只有在需要连接到主机进行故障排除时，才需要使用 SSH（22）。

## 云提供商权限

您需要一个有权直接从 Cloud Manager 在云提供商中部署 Connector 的帐户。



可通过其他方法创建连接器：您可以从创建连接器 ["AWS Marketplace"](#)，["Azure Marketplace"](#)也可以 ["手动安装软件"](#)。

位置	高级步骤	详细步骤
AWS	<ol style="list-style-type: none"> <li>1. 使用包含所需权限的 JSON 文件在 AWS 中创建 IAM 策略。</li> <li>2. 将策略附加到 IAM 角色或 IAM 用户。</li> <li>3. 创建 Connector 时，请为 Cloud Manager 提供 IAM 角色的 ARN 或 IAM 用户的 AWS 访问密钥和机密密钥。</li> </ol>	<a href="#">"单击此处可查看详细步骤"</a> 。
Azure 酒店	<ol style="list-style-type: none"> <li>1. 使用包含所需权限的 JSON 文件在 Azure 中创建自定义角色。</li> <li>2. 将此角色分配给要从 Cloud Manager 创建 Connector 的用户。</li> <li>3. 创建 Connector 时，请使用具有所需权限的 Microsoft 帐户（由 Microsoft 拥有和托管的登录提示符）登录。</li> </ol>	<a href="#">"单击此处可查看详细步骤"</a> 。

位置	高级步骤	详细步骤
Google Cloud	<ol style="list-style-type: none"> <li>1. 使用包含所需权限的 YAML 文件在 Google Cloud 中创建自定义角色。</li> <li>2. 将此角色附加到将从 Cloud Manager 创建 Connector 的用户。</li> <li>3. 如果您计划使用 Cloud Volumes ONTAP，请设置具有所需权限的服务帐户。</li> <li>4. 启用 Google Cloud API。</li> <li>5. 创建 Connector 时，请使用具有所需权限的 Google 帐户登录（登录提示由 Google 拥有并托管）。</li> </ol>	"单击此处可查看详细步骤"。

### 为单个服务建立网络

设置完成后，您便可开始使用 Cloud Manager 提供的服务了。请注意，每个服务都有自己的网络要求。有关详细信息，请参见以下页面。

- "适用于 AWS 的 Cloud Volumes ONTAP"
- "适用于 Azure 的 Cloud Volumes ONTAP"
- "适用于 GCP 的 Cloud Volumes ONTAP"
- "在 ONTAP 系统之间进行数据复制"
- "部署 Cloud Data sense"
- "内部 ONTAP 集群"
- "云分层"
- "云备份"

## 注册到 NetApp Cloud Central

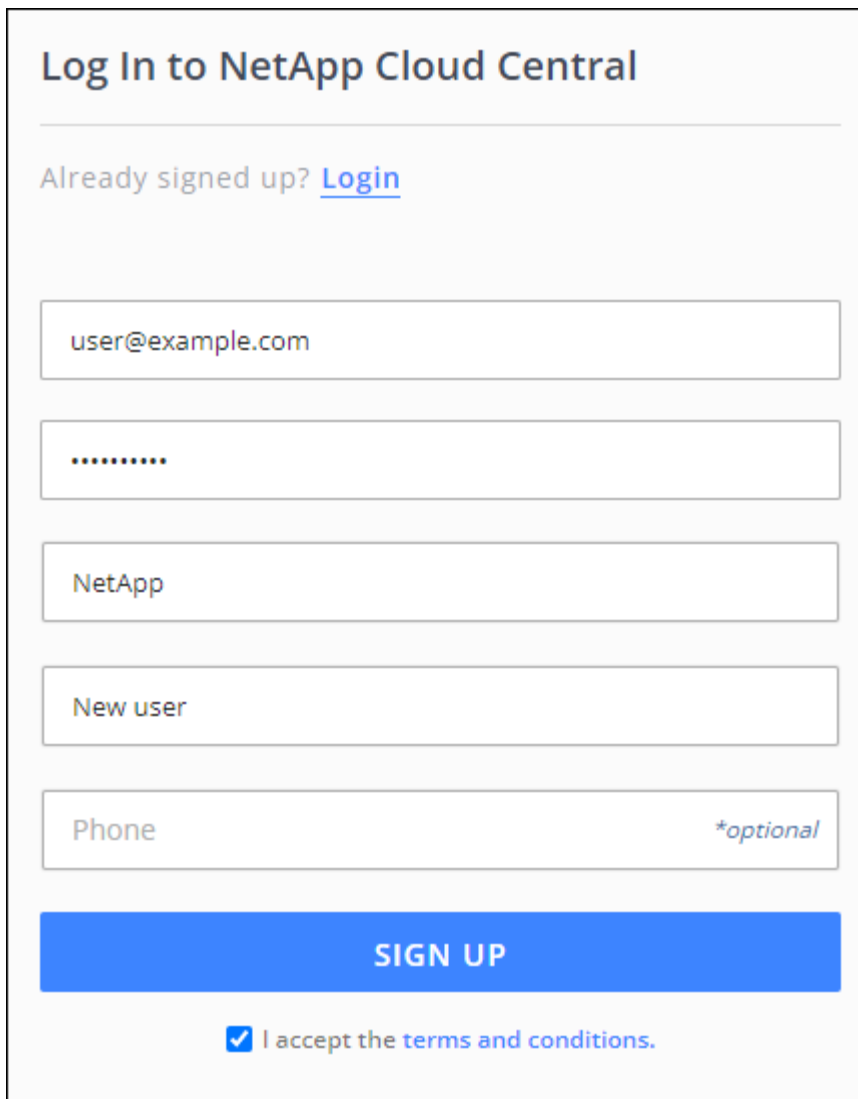
注册到 NetApp Cloud Central，以便您可以访问 NetApp 的云服务。



您可以使用单点登录使用公司目录中的凭据（联合身份）登录。要了解更多信息，请转到 "[Cloud Central 帮助中心](#)" 然后单击 \* Cloud Central 登录选项 \*。

### 步骤

1. 打开 Web 浏览器并转到 "[NetApp Cloud Central](#)"。
2. 单击 \* 注册 \*。
3. 您有两种选择：
  - a. 填写表单并单击 \* 注册 \*。



The image shows a web form titled "Log In to NetApp Cloud Central". Below the title is a link "Already signed up? [Login](#)". The form contains several input fields: an email field with "user@example.com", a password field with masked characters, a dropdown menu with "NetApp" selected, a "New user" button, a "Phone" field with a "\*optional" label, and a large blue "SIGN UP" button. At the bottom, there is a checkbox labeled "I accept the terms and conditions." which is checked.

- b. 如果您已注册NetApp支持站点帐户、请单击\*使用NetApp\*登录、然后输入您的NetApp支持站点凭据。
- 每次登录时、您都需要使用在此注册过程中选择的选项。



使用NetApp登录时、您的NetApp支持站点凭据不会添加到支持信息板中的Cloud Manager中。

4. 等待收到 NetApp Cloud Central 发送的电子邮件。
5. 单击电子邮件中的链接以验证您的电子邮件地址。

现在，您已有活动的 Cloud Central 用户登录。

## 登录到 Cloud Manager

Cloud Manager 界面可通过基于 SaaS 的用户界面访问，请访问 <https://cloudmanager.netapp.com>。

如果您要从无法访问出站Internet的政府区域或站点访问Cloud Manager、则需要登录到在Connector上运行的本地用户界面。"了解如何在Connector上访问本地UI"。



您可以使用单点登录使用公司目录中的凭据（联合身份）登录。要了解更多信息，请转到 "[Cloud Central 帮助中心](#)" 然后单击 \* Cloud Central 登录选项 \*。

#### 步骤

1. 打开 Web 浏览器并转到 <https://cloudmanager.netapp.com>。
2. 输入NetApp Cloud Central凭据或单击\*使用NetApp\*登录并输入NetApp支持站点凭据、即可登录。

您需要选择在注册到Cloud Central时使用的选项。

- 如果您通过输入电子邮件和密码进行注册、则每次登录时都需要输入这些凭据。
- 如果您通过使用NetApp支持站点凭据登录进行注册、则每次都需要使用该登录选项。

## Log In to NetApp Cloud Central

Don't have an account yet? [Sign Up](#)

LOG IN

[Forgot password?](#)

Or

Have a registered NetApp Support Site account?

Log In with NetApp

您现在已登录，可以开始使用 Cloud Manager 管理混合多云基础架构。

## 设置 NetApp 帐户

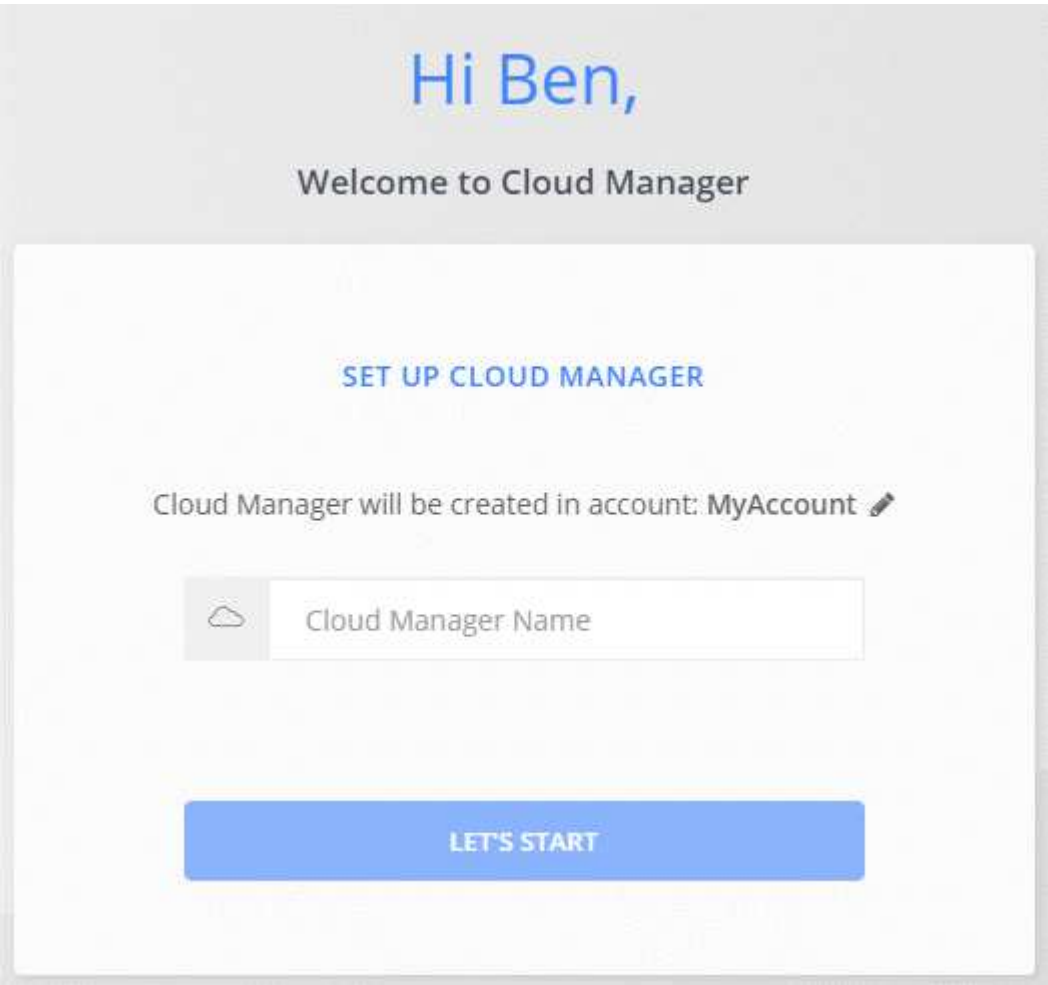
### 了解 NetApp 客户

\_NetApp 帐户\_ 提供多租户功能，可用于在 Cloud Manager 中将用户和资源组织在隔离

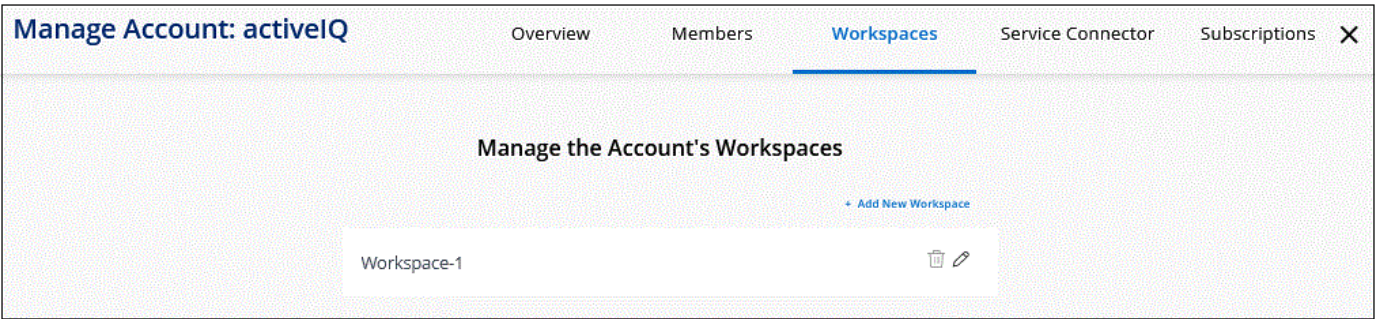
的工作空间中。

例如，多个用户可以在称为 `_workworkspace` 的隔离环境中部署和管理 Cloud Volumes ONTAP 系统。除非共享这些工作空间，否则其他用户不会看到这些工作空间。

首次访问 Cloud Manager 时，系统会提示您选择或创建 NetApp 帐户：



然后，帐户管理员可以通过管理用户（成员），工作空间，连接器和订阅来修改此帐户的设置：



有关分步说明，请参见 "设置 NetApp 帐户"。

帐户设置

通过 Cloud Manager 中的 Manage Account 小工具，客户管理员可以管理 NetApp 帐户。如果您刚刚创建了帐

户，则从头开始。但是，如果您已设置帐户，则会看到与该帐户关联的用户，工作空间，连接器和订阅。

## 概述

"概述" 页面将显示 "帐户名称" 和 "帐户 ID"。注册某些服务时，您可能需要提供帐户 ID。此页面还包括一些 Cloud Manager 配置选项。

## 成员

成员是您与 NetApp 帐户关联的 NetApp Cloud Central 用户。通过将用户与某个帐户以及该帐户中的一个或多个工作空间相关联，这些用户可以在 Cloud Manager 中创建和管理工作环境。

关联用户时，您会为其分配一个角色：

- *Account Admin*：可以在 Cloud Manager 中执行任何操作。
- *Workspace Admin*：可以在分配的工作空间中创建和管理资源。
- *Compliance Viewer*：只能查看 Cloud Data 感知合规性信息，并为其有权访问的系统生成报告。
- *SnapCenter Admin*：可以使用 SnapCenter 服务创建应用程序一致的备份并使用这些备份还原数据。\_ 此服务当前处于测试阶段。 \_

["详细了解这些角色"](#)。

## 工作空间

在 Cloud Manager 中，工作空间会将任意数量的 *work2* 环境与其他工作环境隔离。除非帐户管理员将管理员与工作空间关联，否则 Workspace 管理员无法访问工作空间中的工作环境。

工作环境代表存储系统：

- 单节点 Cloud Volumes ONTAP 系统或 HA 对
- 网络中的内部 ONTAP 集群
- NetApp 私有存储配置中的 ONTAP 集群

["了解如何添加工作空间"](#)。

## 连接器

借助连接器，Cloud Manager 可以管理公有云环境中的资源和流程。连接器在云提供商中部署的虚拟机实例上运行，或者在您配置的内部主机上运行。

您可以将 Connector 与多个 NetApp 云数据服务结合使用。例如，如果您已经有适用于 Cloud Manager 的 Connector，则可以在设置 Cloud Tiering 服务时选择它。

["了解有关连接器的更多信息"](#)。

## 订阅

这些是与选定帐户关联的 NetApp 订阅。

当您从云提供商的市场订阅 Cloud Manager 时，系统会将您重定向到 Cloud Central，您需要在其中保存订阅并

将其与特定帐户关联。

订阅后，每个订阅均可从 " 管理帐户 " 小工具中获取。您将只看到与当前正在查看的帐户关联的订阅。

您可以选择重命名订阅并取消订阅与一个或多个帐户的关联。

例如，假设您有两个帐户，每个帐户都通过单独的订阅付费。您可能会解除某个订阅与某个帐户的关联，以便该帐户中的用户在创建 Cloud Volume ONTAP 工作环境时不会意外选择错误的订阅。

["了解如何管理订阅"](#)。

示例

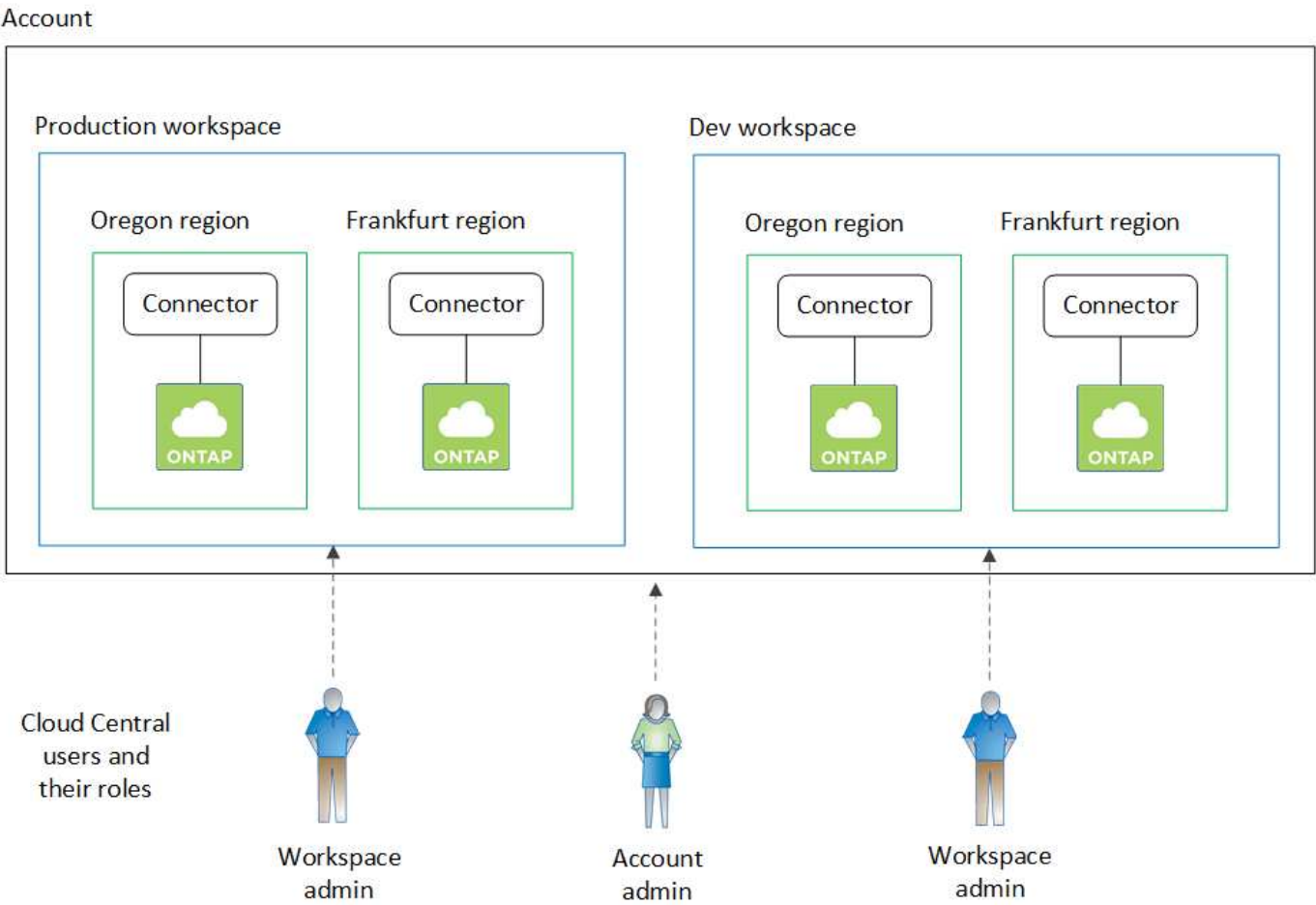
以下示例说明了如何设置帐户。



在后面的两个示例映像中， Connector 和 Cloud Volumes ONTAP 系统实际上并不驻留在 NetApp 帐户中—它们运行在云提供商中。这是每个组件之间关系的概念表示。

示例 1

以下示例显示了一个使用两个工作空间创建隔离环境的帐户。第一个工作空间用于生产环境，第二个工作空间用于开发环境。

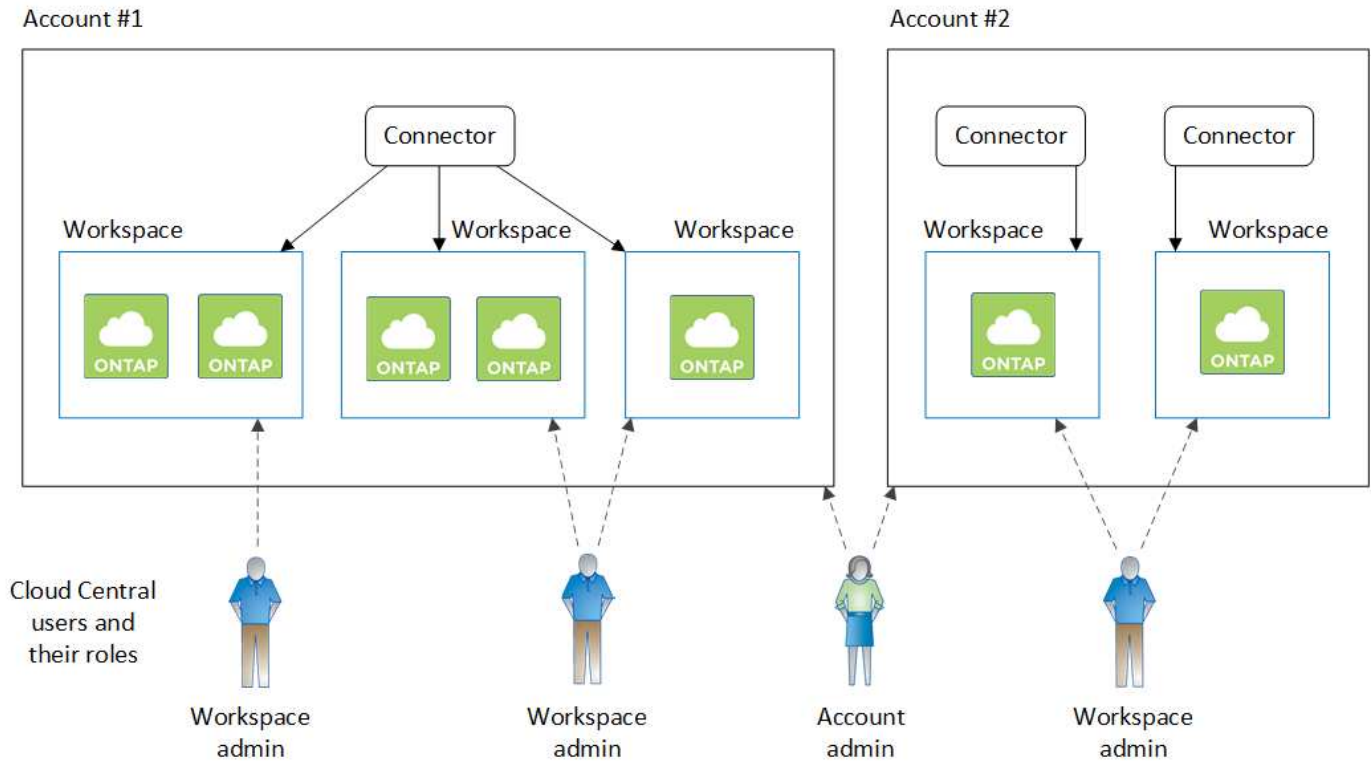




## 示例 2.

下面是另一个示例，通过使用两个单独的 NetApp 帐户显示了最高的多租户级别。例如，服务提供商可能会在一个帐户中使用 Cloud Manager 为其客户提供服务，而使用另一个帐户为其业务部门之一提供灾难恢复。

请注意，帐户 2 包含两个单独的连接器。如果您的系统位于不同的区域或不同的云提供商中，则可能会发生这种情况。



## 在 NetApp 帐户中设置工作空间和用户

首次登录到 Cloud Manager 时，系统会提示您创建 `_NetApp 帐户_`。此帐户可提供多租户，并可用于在隔离的 `_workworkworkspace_` 中组织用户和资源。

["详细了解 NetApp 客户的工作原理"](#)。

设置您的 NetApp 帐户，以便用户可以访问 Cloud Manager 并访问工作空间中的工作环境。只需添加一个用户或添加多个用户和工作空间即可。

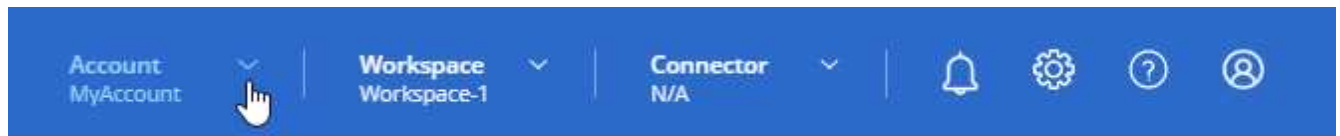
### 添加工作空间

在 Cloud Manager 中，您可以通过工作空间将一组工作环境与其他工作环境和其他用户隔离。例如，您可以创建两个工作空间，并将不同的用户与每个工作空间相关联。

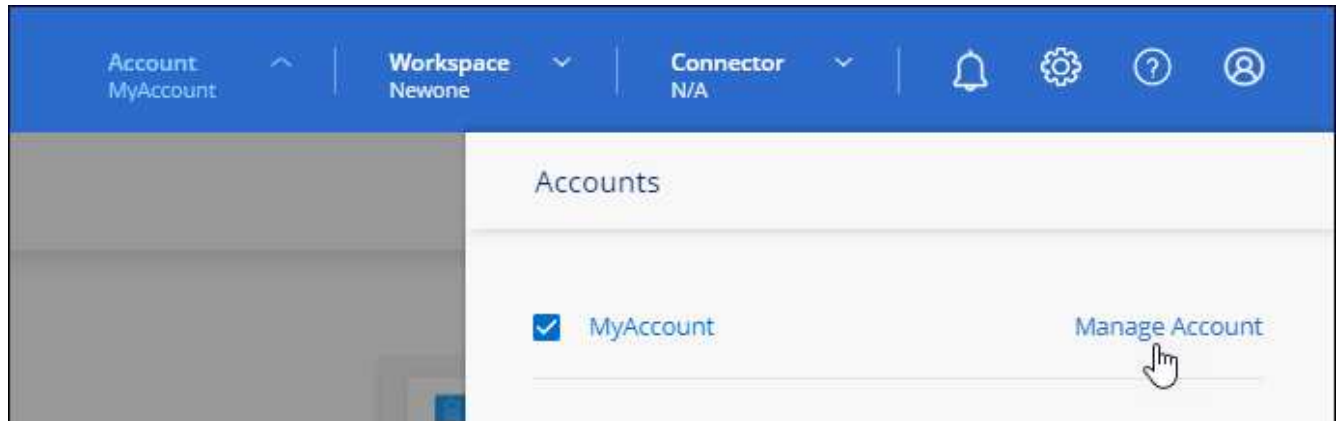
### 步骤

1. 从顶部 ["云管理器"](#)下，单击 \* 帐户 \* 下拉列表。





2. 单击当前选定帐户旁边的 \* 管理帐户 \*。



3. 单击 \* 工作空间 \*。
4. 单击 \* 添加新工作空间 \*。
5. 输入工作空间的名称，然后单击 \* 添加 \*。

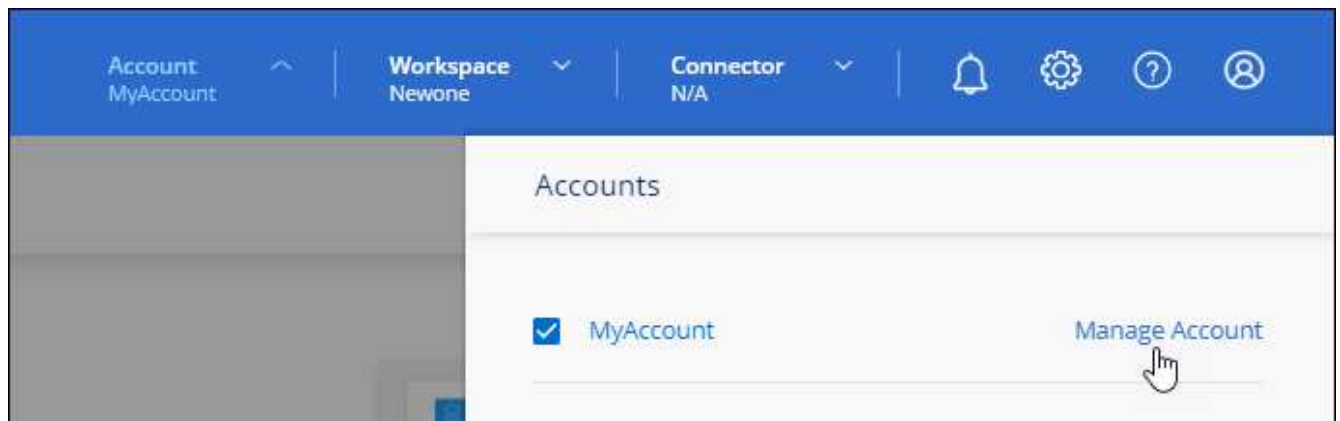
如果 Workspace Admin 需要访问此工作空间，则需要关联此用户。您还需要将 Connectors 与工作空间相关联，以便 Workspace 管理员可以使用这些 Connectors。

### 添加用户

将 Cloud Central 用户与 NetApp 帐户关联，以便这些用户可以在 Cloud Manager 中创建和管理工作环境。

### 步骤

1. 如果用户尚未执行此操作，请让用户转到 "NetApp Cloud Central" 并注册。
2. 从顶部 "云管理器"，单击 \* 帐户 \* 下拉列表，然后单击 \* 管理帐户 \*。

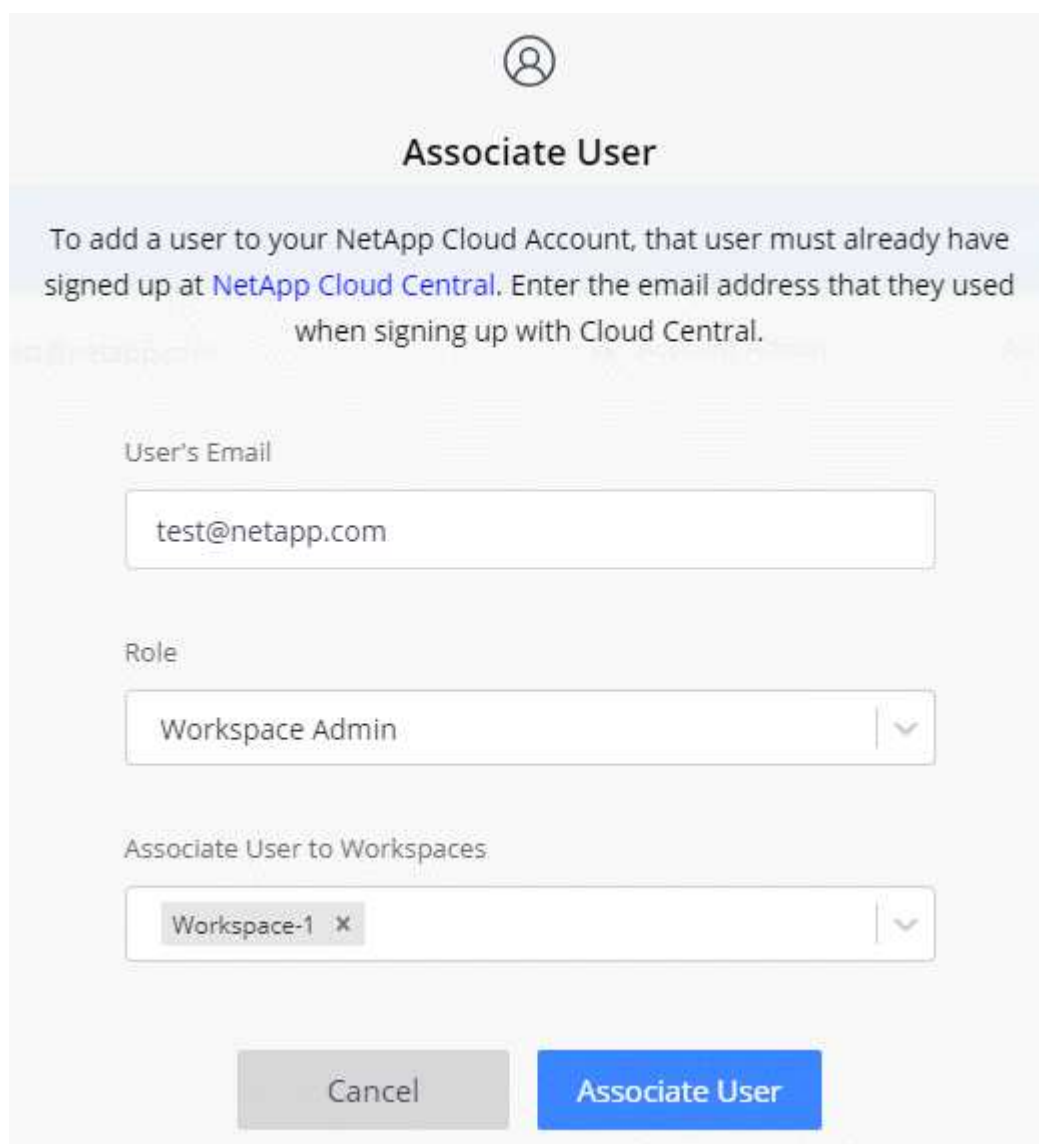


3. 在成员选项卡中，单击 \* 关联用户 \*。

4. 输入用户的电子邮件地址并为用户选择一个角色：

- \* 帐户管理员 \*：可以在 Cloud Manager 中执行任何操作。
- \* 工作空间管理员 \*：可以在分配的工作空间中创建和管理资源。
- \* 合规性查看器 \*：只能查看 Cloud Data sense 监管和合规性信息，并为其有权访问的工作空间生成报告。
- \* SnapCenter Admin\*：可以使用 SnapCenter 服务创建应用程序一致的备份并使用这些备份还原数据。此服务当前处于测试阶段。

5. 如果您选择的帐户不是帐户管理员，请选择一个或多个要与该用户关联的工作空间。



The image shows a dialog box titled "Associate User" with a user icon at the top. Below the title, there is a light blue banner with the text: "To add a user to your NetApp Cloud Account, that user must already have signed up at [NetApp Cloud Central](#). Enter the email address that they used when signing up with Cloud Central." Below this banner, there are three input fields: "User's Email" containing "test@netapp.com", "Role" with a dropdown menu showing "Workspace Admin", and "Associate User to Workspaces" with a dropdown menu showing "Workspace-1" and a close button (X). At the bottom, there are two buttons: a grey "Cancel" button and a blue "Associate User" button.

6. 单击 \* 关联 \*。

用户应从 NetApp Cloud Central 收到一封标题为 " 客户关联 " 的电子邮件。此电子邮件包含访问 Cloud Manager 所需的信息。

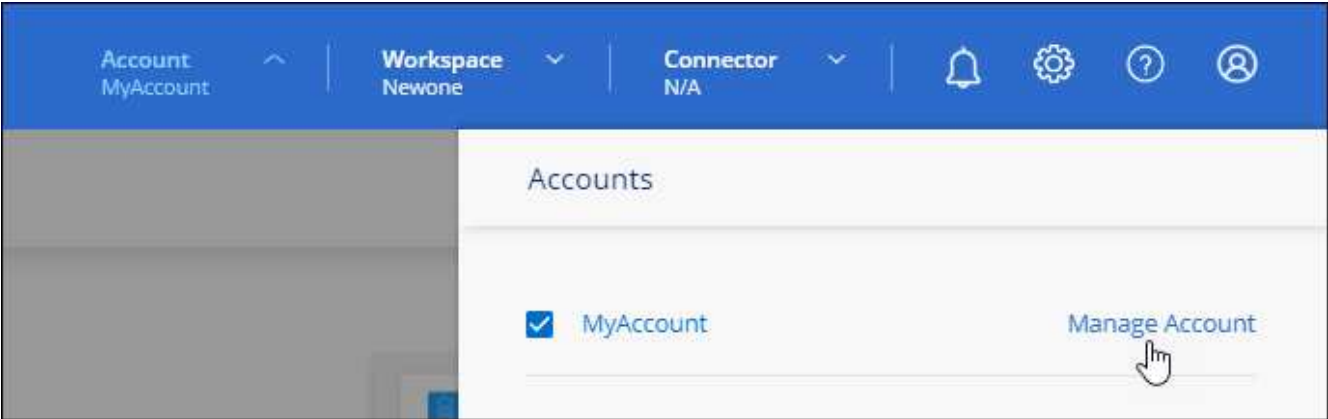
将 **Workspace Admins** 与工作空间相关联

您可以随时将 Workspace Admins 与其他工作空间相关联。通过关联用户，用户可以在该工作空间中创建和查

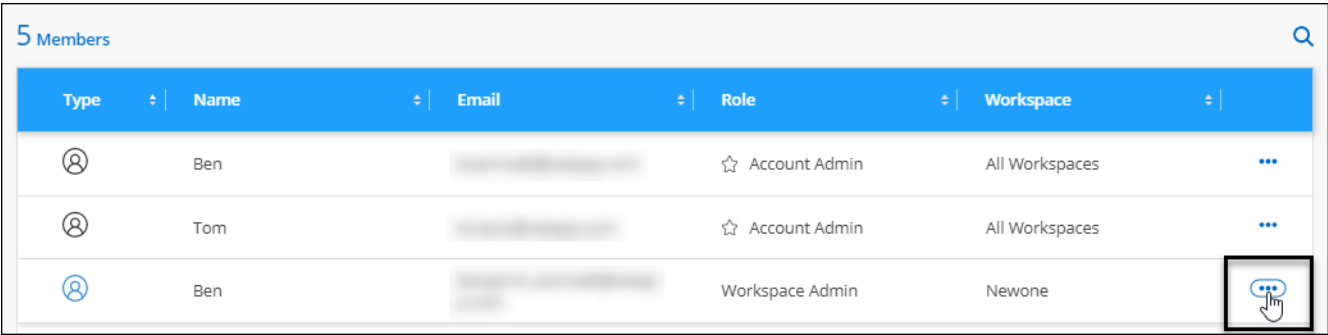
看工作环境。

步骤

- 1. 从 Cloud Manager 顶部，单击 \* 帐户 \* 下拉列表，然后单击 \* 管理帐户 \*。



- 2. 在成员选项卡中，单击与用户对应的行中的操作菜单。



- 3. 单击 \* 管理工作空间 \*。
- 4. 选择一个或多个工作空间，然后单击 \* 应用 \*。

现在，只要 Connector 还与这些工作空间关联，用户就可以从 Cloud Manager 访问这些工作空间。

将 **Connectors** 与工作空间关联

您需要将连接器与工作空间关联，以便 Workspace 管理员可以使用这些连接器创建 Cloud Volumes ONTAP 系统。

如果您只有帐户管理员，则不需要将 Connector 与工作空间相关联。默认情况下，帐户管理员可以访问 Cloud Manager 中的所有工作空间。

["详细了解用户，工作空间和连接器"。](#)

步骤

- 1. 从 Cloud Manager 顶部，单击 \* 帐户 \* 下拉列表，然后单击 \* 管理帐户 \*。



2. 单击 \* 连接器 \*。
3. 单击要关联的 Connector 的 \* 管理工作空间 \*。
4. 选择一个或多个工作空间，然后单击 \* 应用 \*。

Workspace 管理员现在可以使用这些连接器创建 Cloud Volumes ONTAP 系统。

下一步是什么？

现在，您已经设置了帐户，您可以随时通过删除用户，管理工作空间，连接器和订阅来对其进行管理。"[了解如何管理您的帐户](#)"。

## 设置连接器

### 了解连接器

大多数情况下，客户管理员需要在云或内部网络中部署 *Connector*。连接器是 Cloud Manager 日常使用的关键组件。借助此连接器，Cloud Manager 可以管理公有云环境中的资源和流程。

需要连接器时

要使用 Cloud Manager 中的许多功能和服务，需要使用 Connector。

服务

- 适用于 ONTAP 的 Amazon FSX 管理功能
- Amazon S3发现
- Azure Blob发现
- 云备份
- 云数据感知
- 云分层
- Cloud Volumes ONTAP
- 全局文件缓存

- Google Cloud Storage发现
- Kubernetes 集群
- 监控
- 内部 ONTAP 集群

以下服务需要使用连接器 \*。not\_\*：

- Active IQ 数字顾问
- 创建适用于 ONTAP 的 Amazon FSx 工作环境虽然创建工作环境不需要使用 Connector，但需要使用它来创建和管理卷，复制数据以及将适用于 ONTAP 的 FSx 与 Data sense 和 Cloud Sync 等 NetApp 云服务集成。
- Azure NetApp Files

虽然设置和管理 Azure NetApp Files 不需要连接器，但如果要使用云数据感知扫描 Azure NetApp Files 数据，则需要连接器。

- 适用于 Google Cloud 的 Cloud Volumes Service
- Cloud Sync

#### 数字电子钱包

在几乎所有情况下，您都可以在没有连接器的情况下向数字电子钱包添加许可证。

只有在使用 Cloud Volumes ONTAP \_node-based\_ 许可证时，才需要使用 Connector 向数字电子钱包添加许可证。在这种情况下，需要使用连接器，因为数据是从 Cloud Volumes ONTAP 系统上安装的许可证中获取的。

#### 支持的位置

以下位置支持连接器：

- Amazon Web Services
- Microsoft Azure
- Google Cloud
- 在您的内部环境中
- 在您的内部环境中，无法访问 Internet

#### 请注意 **Azure** 部署

如果在 Azure 中部署连接器，则应将其部署在与所管理的 Cloud Volumes ONTAP 系统相同的 Azure 区域中，或者部署在中 ["Azure 区域对"](#) 对于 Cloud Volumes ONTAP 系统。此要求可确保在 Cloud Volumes ONTAP 与其关联存储帐户之间使用 Azure 专用链路连接。 ["了解 Cloud Volumes ONTAP 如何使用 Azure 专用链路"](#)。

#### 有关 **Google Cloud** 部署的注意事项

如果要在 Google Cloud 中创建 Cloud Volumes ONTAP 系统，则必须同时在 Google Cloud 中运行 Connector。您不能使用在 AWS，Azure 或内部运行的 Connector。

连接器应保持运行状态

连接器应始终保持运行状态。对于您启用的服务的持续运行状况和运行来说，这一点非常重要。

例如，连接器是Cloud Volumes ONTAP 运行状况和运行的关键组件。如果某个连接器已关闭、则使用基于节点的许可的Cloud Volumes ONTAP PAYGO系统将在与某个连接器失去通信超过14天之后关闭。

## 如何创建 **Connector**

在工作空间管理员创建 Cloud Volumes ONTAP 工作环境并使用上述任何其他服务之前，客户管理员需要先创建连接器。管理员可以通过多种方式创建Connector：

- 直接从 Cloud Manager （建议）
  - ["在 AWS 中创建"](#)
  - ["在 Azure 中创建"](#)
  - ["在 GCP 中创建"](#)
- 在您自己的 Linux 主机上手动安装软件
  - ["在可访问 Internet 的主机上"](#)
  - ["在无法访问 Internet 的内部主机上"](#)
- 来自云提供商的市场
  - ["AWS Marketplace"](#)
  - ["Azure Marketplace"](#)

如果需要创建一个 Connector 来完成操作， Cloud Manager 将提示您创建一个连接器。

## 权限

创建 Connector 需要特定权限，而 Connector 实例本身也需要另一组权限。

### 创建 **Connector** 的权限

从 Cloud Manager 创建 Connector 的用户需要特定权限才能在您选择的云提供商中部署此实例。Cloud Manager 将在您创建 Connector 时提醒您权限要求。

- ["查看所需的AWS权限"](#)
- ["查看所需的Azure权限"](#)
- ["查看所需的Google Cloud权限"](#)

### **Connector** 实例的权限

Connector 需要特定的云提供商权限才能代表您执行操作。例如，部署和管理 Cloud Volumes ONTAP 。

直接从 Cloud Manager 创建 Connector 时， Cloud Manager 会使用所需权限创建 Connector 。您无需执行任何操作。

如果您自己从 AWS Marketplace ， Azure Marketplace 或通过手动安装软件来创建 Connector ，则需要确保已设置正确的权限。

- ["了解Connector如何使用AWS权限"](#)
- ["了解Connector如何使用Azure权限"](#)
- ["了解Connector如何使用Google Cloud权限"](#)

## 连接器升级

我们通常每月更新一次 Connector 软件，以引入新功能并提高稳定性。虽然 Cloud Manager 平台中的大多数服务和功能均通过基于 SaaS 的软件提供，但有几项特性和功能取决于 Connector 的版本。其中包括 Cloud Volumes ONTAP 管理，内部 ONTAP 集群管理，设置和帮助。

只要有最新版本，Connector 就会自动将其软件更新到最新版本 ["出站 Internet 访问"](#) 以获取软件更新。

## 每个连接器的工作环境数量

Connector 可以在 Cloud Manager 中管理多个工作环境。一个 Connector 应管理的最大工作环境数因情况而异。具体取决于工作环境的类型，卷数量，要管理的容量以及用户数量。

如果您要进行大规模部署，请与 NetApp 代表合作来估算您的环境规模。如果您在此过程中遇到任何问题，请通过产品内聊天联系我们。

## 何时使用多个连接器

在某些情况下，您可能只需要一个连接器，但可能需要两个或更多连接器。

以下是几个示例：

- 您正在使用多云环境（AWS 和 Azure），因此在 AWS 中有一个连接器，在 Azure 中有另一个连接器。每个都管理在这些环境中运行的 Cloud Volumes ONTAP 系统。
- 服务提供商可能会使用一个 NetApp 帐户为其客户提供服务，而使用另一个帐户为其某个业务部门提供灾难恢复。每个帐户都有单独的 Connectors。

## 在相同的工作环境中使用多个连接器

您可以同时管理具有多个连接器的工作环境，以实现灾难恢复。如果一个连接器发生故障，您可以切换到另一个连接器以立即管理工作环境。

要设置此配置，请执行以下操作：

1. ["切换到另一个连接器"](#)
2. 发现现有工作环境。
  - ["将现有 Cloud Volumes ONTAP 系统添加到 Cloud Manager"](#)
  - ["发现 ONTAP 集群"](#)
3. 设置 ["容量管理模式"](#)

只能将主连接器设置为 \* 自动模式 \*。如果出于灾难恢复目的而切换到另一个连接器，则可以根据需要更改容量管理模式。

## 何时在连接器之间切换

创建首个 Connector 时，Cloud Manager 会自动对您创建的每个附加工作环境使用此 Connector。创建额外的 Connector 后，您需要在它们之间切换，以查看每个 Connector 特有的工作环境。

["了解如何在连接器之间切换"](#)。

## 本地用户界面

而您应从执行几乎所有任务 ["SaaS 用户界面"](#)，连接器上仍提供本地用户界面。如果您在无法访问 Internet 的环境中安装 Connector，并且需要从 Connector 本身执行一些任务，而不是从 SaaS 界面执行这些任务，则需要使用此接口：

- ["设置代理服务器"](#)
- 安装修补程序（您通常与 NetApp 人员一起安装修补程序）
- 下载 AutoSupport 消息（通常在遇到问题时由 NetApp 人员指导）

["了解如何访问本地 UI"](#)。

## 为连接器设置网络连接

设置您的网络，以便 Connector 可以管理公有云环境中的资源和流程。最重要的步骤是确保对各种端点的出站 Internet 访问。

此页面上的信息适用于 Connector 具有出站 Internet 访问权限的典型部署。



如果您的网络使用代理服务器与 Internet 进行所有通信，则可以从设置页面指定代理服务器。请参见 ["将 Connector 配置为使用代理服务器"](#)。

## 连接到目标网络

连接器要求与您要创建的工作环境类型以及计划启用的服务建立网络连接。

例如，如果您在公司网络中安装了连接器，则必须设置与启动 Cloud Volumes ONTAP 的 VPC 或 vNet 的 VPN 连接。

## 可能与 172 范围内的 IP 地址冲突

Cloud Manager 使用 IP 地址位于 172.17.0.0/16 和 172.18.0.0/16 范围的两个接口部署 Connector。

如果您的网络配置了其中任一范围的子网，则可能会在 Cloud Manager 中遇到连接失败。例如，在 Cloud Manager 中发现内部 ONTAP 集群可能会失败。

请参见知识库文章 ["Cloud Manager Connector IP与现有网络冲突"](#) 有关如何更改连接器接口的IP地址的说明。

## 出站 Internet 访问

需要从 Connector 进行出站 Internet 访问。



用于管理公有云环境中资源的端点

连接器需要通过出站 Internet 访问来管理公有云环境中的资源和流程。

端点	目的
<a href="https://support.netapp.com">https://support.netapp.com</a>	获取许可信息并向 NetApp 支持部门发送 AutoSupport 消息。
<a href="https://*.cloudmanager.cloud.netapp.com">https://*.cloudmanager.cloud.netapp.com</a>	在 Cloud Manager 中提供 SaaS 功能和服务。
<a href="https://cloudmanagerinfraprod.azurecr.io">https://cloudmanagerinfraprod.azurecr.io</a> <a href="https://*.blob.core.windows.net">https://*.blob.core.windows.net</a>	升级 Connector 及其 Docker 组件。

用于在 Linux 主机上安装 Connector 的端点

您可以选择在自己的 Linux 主机上手动安装 Connector 软件。否则，Connector 的安装程序必须在安装过程中访问以下 URL：

- <https://dl.fedoraProject.org/pub/epel/epel-release-latest-7.noarch.rpm>
- <https://s3.amazonaws.com/aws-cli/awscri-bundle.zip>
- [https://\\*.blob.core.windows.net](https://*.blob.core.windows.net) 或 <https://hub.docker.com>

主机可能会在安装期间尝试更新操作系统软件包。主机可以联系这些操作系统软件包的不同镜像站点。

## 端口和安全组

除非您启动 Connector，否则不会向其传入流量。HTTP 和 HTTPS 可用于访问 "本地 UI"，在极少数情况下使用。只有在需要连接到主机进行故障排除时，才需要使用 SSH。

### AWS 中连接器的规则

Connector 的安全组需要入站和出站规则。

#### 入站规则

协议	Port	目的
SSH	22.	提供对 Connector 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
HTTPS	443.	提供从客户端 Web 浏览器到本地用户界面的 HTTPS 访问，以及从 Cloud Data sense 实例建立的连接
TCP	3128	如果您的 AWS 网络不使用 NAT 或代理，则可为云数据感知实例提供 Internet 访问
TCP	9060	支持启用和使用 Cloud Data sense （仅适用于 GovCloud 部署）

#### 出站规则

连接器的预定义安全组将打开所有出站流量。如果可以接受，请遵循基本出站规则。如果您需要更严格的规则、请使用高级出站规则。

基本外向规则

Connector 的预定义安全组包括以下出站规则。

协议	Port	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设置严格的规则，则可以使用以下信息仅打开 Connector 进行出站通信所需的端口。



源 IP 地址是 Connector 主机。

服务	协议	Port	目标	目的
API 调用和 AutoSupport	HTTPS	443.	出站 Internet 和 ONTAP 集群管理 LIF	API 调用 AWS 和 ONTAP ，云数据感知，勒索软件服务以及向 NetApp 发送 AutoSupport 消息
API 调用	TCP	3000	ONTAP HA 调解器	与 ONTAP HA 调解器通信
	TCP	8088	备份到 S3	对备份到 S3 进行 API 调用
DNS	UDP	53.	DNS	用于云管理器进行 DNS 解析

Azure 中连接器的规则

Connector 的安全组需要入站和出站规则。

入站规则

协议	Port	目的
SSH	22.	提供对 Connector 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
HTTPS	443.	提供从客户端 Web 浏览器到本地用户界面的 HTTPS 访问，以及从 Cloud Data sense 实例建立的连接
TCP	9060	支持启用和使用 Cloud Data Asense（仅适用于政府云部署）

## 出站规则

连接器的预定义安全组将打开所有出站流量。如果可以接受，请遵循基本出站规则。如果您需要更严格的规则、请使用高级出站规则。

### 基本外向规则

Connector 的预定义安全组包括以下出站规则。

协议	Port	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设置严格的规则，则可以使用以下信息仅打开 Connector 进行出站通信所需的端口。



源 IP 地址是 Connector 主机。

服务	协议	Port	目标	目的
API 调用和 AutoSupport	HTTPS	443.	出站 Internet 和 ONTAP 集群管理 LIF	API 调用 AWS 和 ONTAP，云数据感知，勒索软件服务以及向 NetApp 发送 AutoSupport 消息
DNS	UDP	53.	DNS	用于云管理器进行 DNS 解析

### GCP 中连接器的规则

Connector 的防火墙规则需要入站和出站规则。

#### 入站规则

协议	Port	目的
SSH	22.	提供对 Connector 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
HTTPS	443.	提供从客户端 Web 浏览器到本地用户界面的 HTTPS 访问

#### 出站规则

连接器的预定义防火墙规则会打开所有出站流量。如果可以接受，请遵循基本出站规则。如果您需要更严格的规则、请使用高级出站规则。

基本外向规则

Connector 的预定义防火墙规则包括以下出站规则。

协议	Port	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设置严格的规则，则可以使用以下信息仅打开 Connector 进行出站通信所需的端口。



源 IP 地址是 Connector 主机。

服务	协议	Port	目标	目的
API 调用和 AutoSupport	HTTPS	443.	出站 Internet 和 ONTAP 集群管理 LIF	API 调用 GCP 和 ONTAP ，云数据感知，勒索软件服务以及向 NetApp 发送 AutoSupport 消息
DNS	UDP	53.	DNS	用于云管理器进行 DNS 解析

内部连接器的端口

在内部 Linux 主机上手动安装时， Connector 会使用以下 *inbound* 端口。

这些入站规则适用于以下两种部署模式：通过 Internet 访问或不通过 Internet 访问安装的内部连接器。

协议	Port	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
HTTPS	443.	提供从客户端 Web 浏览器到本地用户界面的 HTTPS 访问

从 Cloud Manager 在 AWS 中创建连接器

客户管理员需要先部署 *Connector* ，然后才能使用大多数 Cloud Manager 功能。借助此连接器， Cloud Manager 可以管理公有云环境中的资源和流程。 ["了解何时需要连接器"](#)。

此页面介绍如何直接从 Cloud Manager 在 AWS 中创建 Connector 。 ["了解部署 Connector 的其他方法"](#)。

这些步骤必须由具有帐户管理员角色的用户完成。Workspace 管理员无法创建 Connector 。

设置 AWS 身份验证

Cloud Manager 需要先向 AWS 进行身份验证，然后才能在 VPC 中部署 Connector 实例。您可以选择以下身份验证方法之一：

- 让Cloud Manager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访问密钥和机密密钥

无论选择哪一种方式、您都需要首先创建一个包含所需权限的IAM策略。

#### 创建IAM策略

此策略仅包含从Cloud Manager在AWS中启动Connector实例所需的权限。请勿在其他情况下使用此策略。

在Cloud Manager创建Connector时、它会将一组新的权限应用于Connector实例、从而使Connector能够管理公有云环境中的资源。

#### 步骤

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

```
{
  "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",
      "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",
        "cloudformation:CreateStack",
        "cloudformation>DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:ValidateTemplate",
        "ec2:AssociateIamInstanceProfile",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DisassociateIamInstanceProfile",
        "iam:GetRole",
        "iam:TagRole",
        "iam:ListRoles",
        "kms:ListAliases"
    ],
    "Resource": "*"
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:TerminateInstances"
    ],
    "Condition": {
        "StringLike": {
            "ec2:ResourceTag/OCCMInstance": "*"
        }
    },
    "Resource": [
        "arn:aws:ec2:*:*:instance/*"
    ]
}
]
}

```

5. 单击\*下一步\*并根据需要添加标记。
6. 单击\*下一步\*并输入名称和问题描述。
7. 单击\*创建策略\*。

将此策略附加到Cloud Manager可以承担的IAM角色或IAM用户。

## 设置 IAM 角色

设置一个 IAM 角色，Cloud Manager 可以承担此角色，以便在 AWS 中部署 Connector。

### 步骤

1. 转到目标帐户中的 AWS IAM 控制台。
2. 在访问管理下，单击 \* 角色 > 创建角色 \*，然后按照步骤创建角色。

请务必执行以下操作：

- 在 \* 可信实体类型 \* 下，选择 \* AWS 帐户 \*。
- 选择 \* 其他 AWS 帐户 \*，然后输入 Cloud Manager SaaS 帐户的 ID：952013314444
- 选择在上一节中创建的策略。

3. 创建角色后、复制角色ARN、以便您可以在创建Connector时将其粘贴到Cloud Manager中。

IAM 角色现在具有所需的权限。

## 为 IAM 用户设置权限

创建 Connector 时，您可以为拥有部署 Connector 实例所需权限的 IAM 用户提供 AWS 访问密钥和机密密钥。

### 步骤

1. 在AWS IAM控制台中、单击\*用户\*、然后选择用户名。
2. 单击\*添加权限>直接附加现有策略\*。
3. 选择创建的策略。
4. 单击\*下一步\*、然后单击\*添加权限\*。
5. 确保您有权访问 IAM 用户的访问密钥和机密密钥。

AWS 用户现在具有从 Cloud Manager 创建 Connector 所需的权限。在 Cloud Manager 提示时，您需要为此用户指定 AWS 访问密钥。

## 创建连接器

您可以通过 Cloud Manager 直接从其用户界面在 AWS 中创建 Connector。

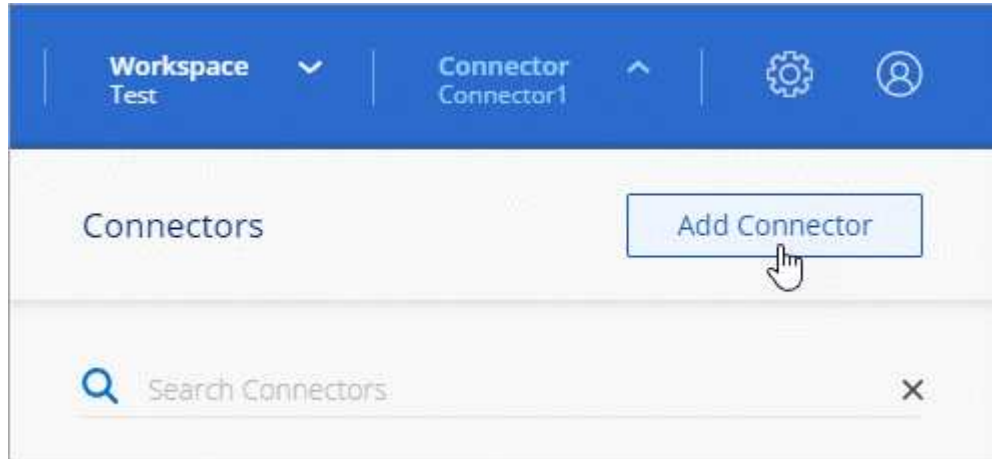
您需要什么？ #8217 ；将需要什么

- AWS 身份验证方法：Cloud Manager 可承担的 IAM 角色的 ARN，或者 IAM 用户的 AWS 访问密钥和机密密钥。
- 您选择的 AWS 区域中的 VPC，子网和密钥对。
- 如果您不希望 Cloud Manager 自动为 Connector 创建 IAM 角色，则需要创建您自己的角色 ["使用此页面上的策略"](#)。

这些权限是 Connector 在公有云环境中管理资源所需的权限。它与您为创建 Connector 实例提供的权限集不同。

### 步骤

1. 如果要创建首个工作环境，请单击 \* 添加工作环境 \* 并按照提示进行操作。否则，请单击 \* 连接器 \* 下拉列表并选择 \* 添加连接器 \*。



2. 选择 \* Amazon Web Services \* 作为您的云提供商，然后单击 \* 继续 \*。

请记住，Connector 必须与您要创建的工作环境类型以及您计划启用的服务建立网络连接。

["详细了解 Connector 的网络要求"](#)。

3. 按照向导中的步骤创建 Connector：

- \* 准备就绪 \*：查看您需要的内容。
- \* AWS Credentials\*：指定您的 AWS 区域，然后选择身份验证方法，即 Cloud Manager 可以承担的 IAM 角色或 AWS 访问密钥和机密密钥。



如果选择 \* 承担角色 \*，则可以从 Connector 部署向导创建第一组凭据。必须从 "凭据" 页面创建任何其他凭据集。然后，这些文件将从向导的下拉列表中显示。 ["了解如何添加其他凭据"](#)。

- \* 详细信息 \*：提供有关连接器的详细信息。
  - 输入实例的名称。
  - 向实例添加自定义标记（元数据）。
  - 选择是希望 Cloud Manager 创建具有所需权限的新角色，还是要选择使用设置的现有角色 ["所需权限"](#)。
  - 选择是否要对 Connector 的 EBS 磁盘进行加密。您可以选择使用默认加密密钥或自定义密钥。
- \* 网络 \*：指定实例的 VPC，子网和密钥对，选择是否启用公有 IP 地址，并可选择指定代理配置。
- \* 安全组 \*：选择是创建新的安全组，还是选择允许入站 HTTP，HTTPS 和 SSH 访问的现有安全组。



除非您启动 Connector，否则不会向其传入流量。HTTP 和 HTTPS 可用于访问 ["本地 UI"](#)，在极少数情况下使用。只有在需要连接到主机进行故障排除时，才需要使用 SSH。

- \* 审核 \*：查看您选择的内容，确认您的设置正确无误。

4. 单击 \* 添加 \*。



此实例应在大约 7 分钟后准备就绪。您应停留在页面上，直到此过程完成。

您需要将连接器与工作空间关联，以便 Workspace 管理员可以使用这些连接器创建 Cloud Volumes ONTAP 系统。如果您只有帐户管理员，则不需要将 Connector 与工作空间相关联。默认情况下，帐户管理员可以访问 Cloud Manager 中的所有工作空间。"[了解更多信息](#)"。

## 从 Cloud Manager 在 Azure 中创建 Connector

客户管理员需要先部署 *Connector*，然后才能使用大多数 Cloud Manager 功能。借助此连接器，Cloud Manager 可以管理公有云环境中的资源和流程。"[了解何时需要连接器](#)"。

此页面介绍如何直接从 Cloud Manager 在 Azure 中创建 Connector。"[了解部署 Connector 的其他方法](#)"。

这些步骤必须由具有帐户管理员角色的用户完成。Workspace 管理员无法创建 Connector。

### 概述

要部署 Connector，您需要为 Cloud Manager 提供一个登录名，该登录名必须具有在 Azure 中创建 Connector VM 所需的权限。

您有两种选择：

1. 出现提示时，使用 Microsoft 帐户登录。此帐户必须具有特定的 Azure 权限。这是默认选项。

[请按照以下步骤开始操作](#)。

2. 提供有关 Azure AD 服务主体的详细信息。此服务主体还需要特定权限。

[请按照以下步骤开始操作](#)。

### 有关 Azure 地区的说明

此连接器应部署在与其管理的 Cloud Volumes ONTAP 系统所在的同一 Azure 区域或中 "[Azure 区域对](#)" 对于 Cloud Volumes ONTAP 系统。此要求可确保在 Cloud Volumes ONTAP 与其关联存储帐户之间使用 Azure 专用链路连接。"[了解 Cloud Volumes ONTAP 如何使用 Azure 专用链路](#)"。

### 使用 Azure 帐户创建 Connector

在 Azure 中创建 Connector 的默认方法是，在出现提示时使用 Azure 帐户登录。此登录表由 Microsoft 拥有和托管。您的凭据不会提供给 NetApp。

为 Azure 帐户设置权限

在从 Cloud Manager 部署 Connector 之前，您需要确保 Azure 帐户具有正确的权限。

### 步骤

1. 在 Azure 中复制新自定义角色所需的权限、并将其保存在 JSON 文件中。



此策略仅包含从Cloud Manager在Azure中启动Connector VM所需的权限。请勿在其他情况下使用此策略。在Cloud Manager创建Connector时、它会将一组新的权限应用于Connector VM、从而使Connector能够管理公有云环境中的资源。

```
{
  "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。

◦ 示例 \*

```

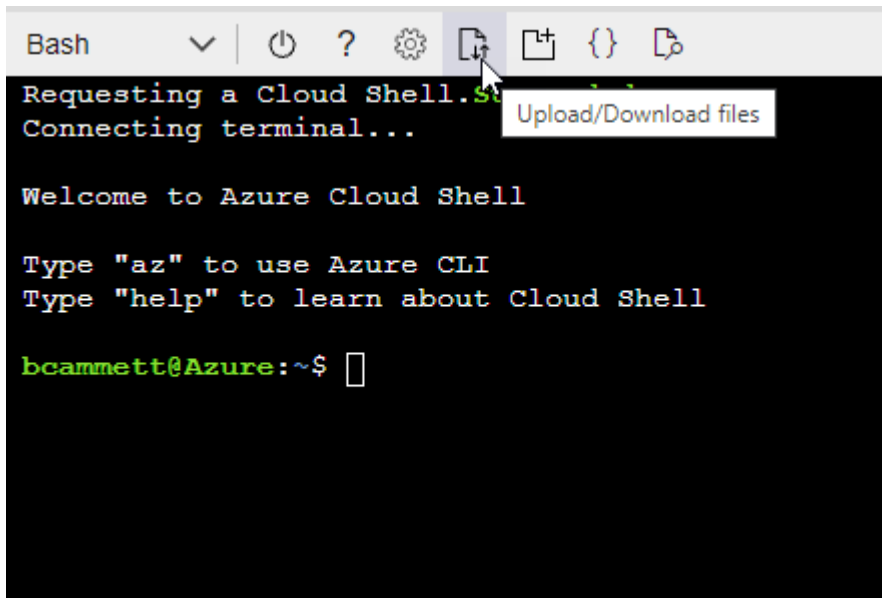
"AssignableScopes": [
    "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz"
],

```

## 3. 使用 JSON 文件在 Azure 中创建自定义角色。

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

- a. start "Azure Cloud Shell" 并选择 Bash 环境。
- b. 上传 JSON 文件。



- c. 输入以下 Azure 命令行界面命令：

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

现在，您应具有一个名为 *Azure SetupAsService* 的自定义角色。

4. 将角色分配给要从 Cloud Manager 部署 Connector 的用户：

- a. 打开 \* 订阅 \* 服务并选择用户的订阅。
- b. 单击 \* 访问控制（IAM） \*。
- c. 单击 \* 添加 \* > \* 添加角色分配 \*，然后添加权限：
  - 选择 \* Azure SetupAsService \* 角色，然后单击 \* 下一步 \*。



Azure SetupAsService 是 Azure 的 Connector 部署策略中提供的默认名称。如果您为角色选择了其他名称，请选择该名称。

- 保持选中 \* 用户，组或服务主体 \*。
- 单击 \* 选择成员 \*，选择您的用户帐户，然后单击 \* 选择 \*。
- 单击 \* 下一步 \*。
- 单击 \* 审核 + 分配 \*。

Azure 用户现在具有从 Cloud Manager 部署 Connector 所需的权限。

## 使用 Azure 帐户登录以创建 Connector

您可以通过 Cloud Manager 直接从其用户界面在 Azure 中创建 Connector。

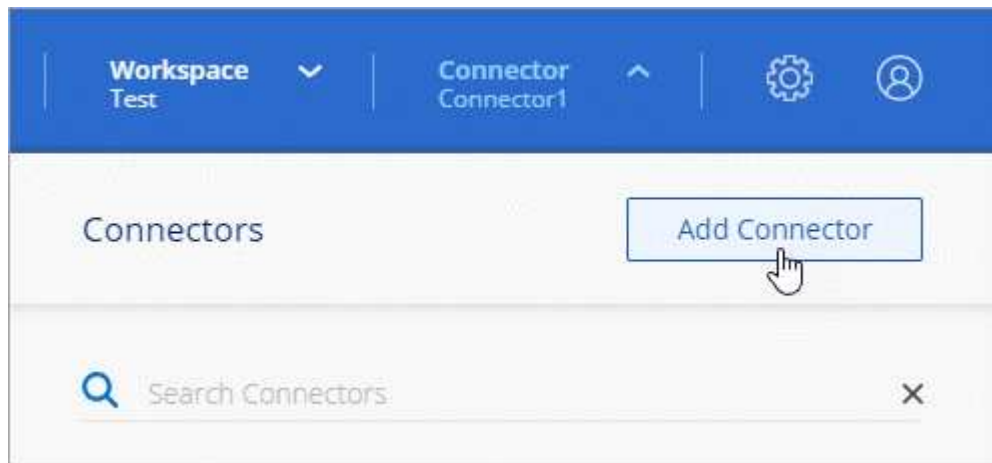
您需要什么？ #8217 ；将需要什么

- Azure 订阅。
- 您选择的 Azure 区域中的 vNet 和子网。
- 如果您不希望 Cloud Manager 自动为 Connector 创建 Azure 角色，则需要创建您自己的角色 ["使用此页面上的策略"](#)。

这些权限适用于 Connector 实例本身。它是一组与您先前设置的权限不同的权限，只需部署 Connector 即可。

### 步骤

1. 如果要创建首个工作环境，请单击 \* 添加工作环境 \* 并按照提示进行操作。否则，请单击 \* 连接器 \* 下拉列表并选择 \* 添加连接器 \*。



2. 选择 \* Microsoft Azure\* 作为云提供商。

请记住，Connector 必须与您要创建的工作环境类型以及您计划启用的服务建立网络连接。

["详细了解 Connector 的网络要求"](#)。

3. 按照向导中的步骤创建 Connector：

- \* 准备就绪 \*：查看您需要的内容，然后单击 \* 下一步 \*。
- 如果出现提示，请登录到您的 Microsoft 帐户，该帐户应具有创建虚拟机所需的权限。

此表由 Microsoft 拥有和托管。您的凭据不会提供给 NetApp。



如果您已登录到 Azure 帐户，则 Cloud Manager 将自动使用该帐户。如果您有多个帐户，则可能需要先注销，以确保您使用的是正确的帐户。

- \* 虚拟机身份验证 \*：选择 Azure 订阅，位置，新资源组或现有资源组，然后选择身份验证方法。
- \* 详细信息 \*：输入实例的名称，指定标记，然后选择是希望 Cloud Manager 创建具有所需权限的新角

色，还是要选择使用设置的现有角色 ["所需权限"](#)。

请注意，您可以选择与此角色关联的订阅。您选择的每个订阅都为 Connector 提供了在这些订阅中部署 Cloud Volumes ONTAP 的权限。

- \* 网络 \*：选择 vNet 和子网，是否启用公有 IP 地址，并可选择指定代理配置。
- \* 安全组 \*：选择是创建新的安全组，还是选择允许入站 HTTP，HTTPS 和 SSH 访问的现有安全组。



除非您启动 Connector，否则不会向其传入流量。HTTP 和 HTTPS 可用于访问 ["本地 UI"](#)，在极少数情况下使用。只有在需要连接到主机进行故障排除时，才需要使用 SSH。

- \* 审核 \*：查看您选择的内容，确认您的设置正确无误。

#### 4. 单击 \* 添加 \*。

虚拟机应在大约 7 分钟内准备就绪。您应停留在页面上，直到此过程完成。

您需要将连接器与工作空间关联，以便 Workspace 管理员可以使用这些连接器创建 Cloud Volumes ONTAP 系统。如果您只有帐户管理员，则不需要将 Connector 与工作空间相关联。默认情况下，帐户管理员可以访问 Cloud Manager 中的所有工作空间。["了解更多信息。"](#)

### 使用服务主体创建连接器

您还可以选择为 Cloud Manager 提供具有所需权限的 Azure 服务主体的凭据，而不是使用 Azure 帐户登录。

#### 使用服务主体授予 **Azure** 权限

通过在 Azure Active Directory 中创建和设置服务主体并获取 Cloud Manager 所需的 Azure 凭据，授予在 Azure 中部署 Connector 所需的权限。

#### 步骤

1. [\[Create an Azure Active Directory application\]](#)。
2. [\[Assign the application to a role\]](#)。
3. [\[Add Windows Azure Service Management API permissions\]](#)。
4. [\[Get the application ID and directory ID\]](#)。
5. [\[Create a client secret\]](#)。

### 创建 **Azure Active Directory** 应用程序

创建一个 Azure Active Directory（AD）应用程序和服务主体，Cloud Manager 可使用此主体部署 Connector。

要创建 Active Directory 应用程序并将此应用程序分配给角色，您必须在 Azure 中拥有适当的权限。有关详细信息，请参见 ["Microsoft Azure 文档：所需权限"](#)。

#### 步骤

1. 从 Azure 门户中，打开 \* Azure Active Directory\* 服务。



2. 在菜单中，单击 \* 应用程序注册 \*。
3. 单击 \* 新建注册 \*。
4. 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（任何将适用于 Cloud Manager）。
  - \* 重定向 URI\*：可以将此字段留空。
5. 单击 \* 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计划部署 Connector 的 Azure 订阅，并为其分配自定义 "Azure SetupAsService" 角色。

步骤

1. 在 Azure 中复制新自定义角色所需的权限、并将其保存在 JSON 文件中。



此策略仅包含从 Cloud Manager 在 Azure 中启动 Connector VM 所需的权限。请勿在其他情况下使用此策略。在 Cloud Manager 创建 Connector 时、它会将一组新的权限应用于 Connector VM、从而使 Connector 能够管理公有云环境中的资源。

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

```

"Microsoft.Compute/virtualMachines/extensions/write",
"Microsoft.Compute/virtualMachines/extensions/read",
"Microsoft.Compute/availabilitySets/read",
"Microsoft.Network/locations/operationResults/read",
"Microsoft.Network/locations/operations/read",
"Microsoft.Network/networkInterfaces/join/action",
"Microsoft.Network/networkInterfaces/read",
"Microsoft.Network/networkInterfaces/write",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkSecurityGroups/join/action",
"Microsoft.Network/networkSecurityGroups/read",
"Microsoft.Network/networkSecurityGroups/write",

"Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read",
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/virtualNetworks/subnets/join/action",
"Microsoft.Network/virtualNetworks/subnets/read",

"Microsoft.Network/virtualNetworks/subnets/virtualMachines/read",
"Microsoft.Network/virtualNetworks/virtualMachines/read",
"Microsoft.Network/publicIPAddresses/write",
"Microsoft.Network/publicIPAddresses/read",
"Microsoft.Network/publicIPAddresses/delete",
"Microsoft.Network/networkSecurityGroups/securityRules/read",
"Microsoft.Network/networkSecurityGroups/securityRules/write",
"Microsoft.Network/networkSecurityGroups/securityRules/delete",
"Microsoft.Network/publicIPAddresses/join/action",

"Microsoft.Network/locations/virtualNetworkAvailableEndpointServices/read",

"Microsoft.Network/networkInterfaces/ipConfigurations/read",
"Microsoft.Resources/deployments/operations/read",
"Microsoft.Resources/deployments/read",
"Microsoft.Resources/deployments/delete",
"Microsoft.Resources/deployments/cancel/action",
"Microsoft.Resources/deployments/validate/action",
"Microsoft.Resources/resources/read",
"Microsoft.Resources/subscriptions/operationresults/read",
"Microsoft.Resources/subscriptions/resourceGroups/delete",
"Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Resources/subscriptions/resourcegroups/resources/read",
"Microsoft.Resources/subscriptions/resourceGroups/write",
"Microsoft.Authorization/roleDefinitions/write",
"Microsoft.Authorization/roleAssignments/write",

```



```

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

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

```

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

◦ 示例 \*

```

"AssignableScopes": [
    "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
]

```

3. 使用 JSON 文件在 Azure 中创建自定义角色。

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

- a. start "Azure Cloud Shell" 并选择 Bash 环境。
- b. 上传 JSON 文件。



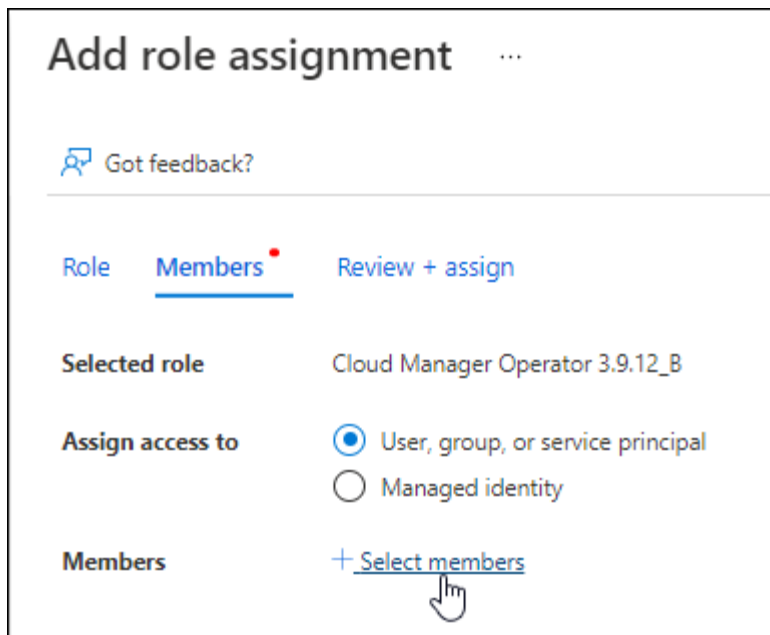
c. 输入以下 Azure 命令行界面命令：

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

现在，您应具有一个名为 *Azure SetupAsService* 的自定义角色。

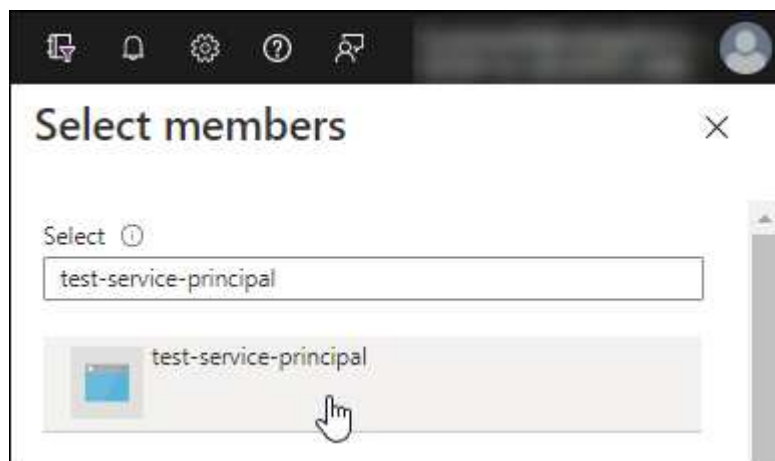
4. 将应用程序分配给角色：

- a. 从 Azure 门户中，打开 \* 订阅 \* 服务。
- b. 选择订阅。
- c. 单击 \* 访问控制（IAM） > 添加 > 添加角色分配 \*。
- d. 在 \* 角色 \* 选项卡中，选择 \* Azure SetupAsService \* 角色，然后单击 \* 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 \*。
  - 单击 \* 选择成员 \*。



- 搜索应用程序的名称。

以下是一个示例：



- 选择应用程序并单击 \* 选择 \*。
- 单击 \* 下一步 \*。
- a. 单击 \* 审核 + 分配 \*。

现在，服务主体具有部署 Connector 所需的 Azure 权限。

## 添加 **Windows Azure** 服务管理 **API** 权限

服务主体必须具有 "Windows Azure 服务管理 API" 权限。

### 步骤

1. 在 \* Azure Active Directory\* 服务中，单击 \* 应用程序注册 \* 并选择应用程序。
2. 单击 \* API 权限 > 添加权限 \*。


3. 在 \* Microsoft APIs\* 下, 选择 \* Azure Service Management\* 。













## Request API permissions

### Select an API

Microsoft APIs   APIs my organization uses   My APIs

#### Commonly used Microsoft APIs

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

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

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

## Request API permissions

< All APIs



Azure Service Management

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

What type of permissions does your application require?

### Delegated permissions

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

### Application permissions

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

Select permissions

[expand all](#)

Type to search

PERMISSION

ADMIN CONSENT REQUIRED



user\_impersonation

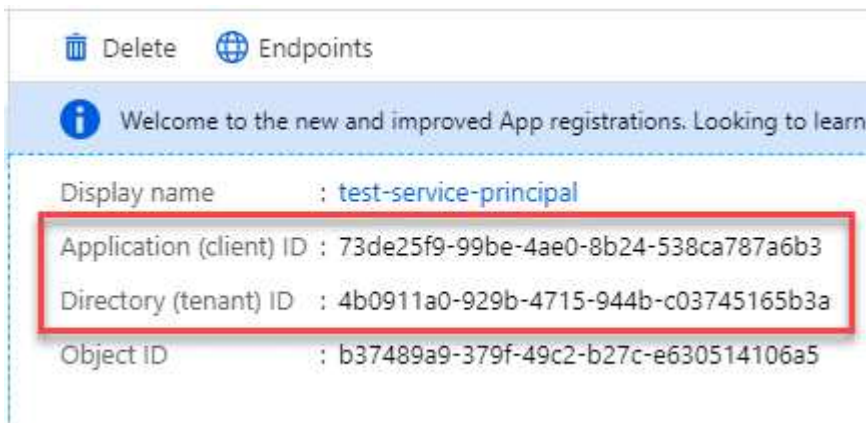
Access Azure Service Management as organization users (preview) ⓘ

## 获取应用程序 ID 和目录 ID

从 Cloud Manager 创建 Connector 时，您需要提供应用程序（客户端）ID 和目录（租户）ID。Cloud Manager 使用 ID 以编程方式登录。

### 步骤

1. 在 \* Azure Active Directory\* 服务中，单击 \* 应用程序注册 \* 并选择应用程序。
2. 复制 \* 应用程序（客户端）ID\* 和 \* 目录（租户）ID\*。



## 创建客户端密钥

您需要创建客户端密钥，然后向 Cloud Manager 提供该密钥的值，以便 Cloud Manager 可以使用它向 Azure AD 进行身份验证。

### 步骤

1. 打开 \* Azure Active Directory\* 服务。
2. 单击 \* 应用程序注册 \* 并选择您的应用程序。

3. 单击 \* 证书和密码 > 新客户端密钥 \*。
4. 提供密钥和持续时间的问题描述。
5. 单击 \* 添加 \*。
6. 复制客户端密钥的值。

### Client secrets

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

+ New client secret		
DESCRIPTION	EXPIRES	VALUE
test secret	8/16/2020	*sZ1jSe2By:D*-ZRov4NLfdAcY7:+0vA

Copy to clipboard

此时，您的服务主体已设置完毕，您应已复制应用程序（客户端）ID，目录（租户）ID 和客户端密钥值。创建 Connector 时，您需要在 Cloud Manager 中输入此信息。

### 使用服务主体登录以创建 Connector

您可以通过 Cloud Manager 直接从其用户界面在 Azure 中创建 Connector。

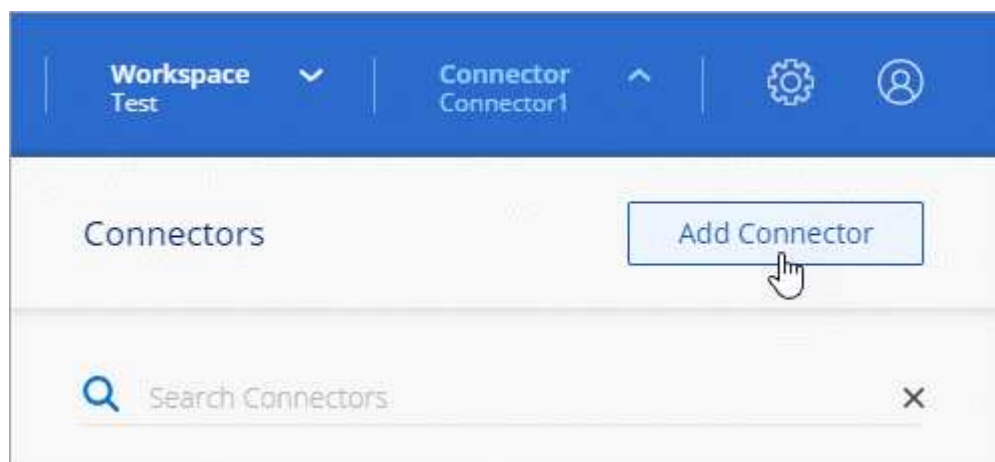
您需要什么？ #8217 ；将需要什么

- Azure 订阅。
- 您选择的 Azure 区域中的 vNet 和子网。
- 如果您不希望 Cloud Manager 自动为 Connector 创建 Azure 角色，则需要创建您自己的角色 "使用此页面上的策略"。

这些权限适用于 Connector 实例本身。它是一组与您先前设置的权限不同的权限，只需部署 Connector 即可。

### 步骤

1. 如果要创建首个工作环境，请单击 \* 添加工作环境 \* 并按照提示进行操作。否则，请单击 \* 连接器 \* 下拉列表并选择 \* 添加连接器 \*。



## 2. 选择 \* Microsoft Azure\* 作为云提供商。

请记住，Connector 必须与您要创建的工作环境类型以及您计划启用的服务建立网络连接。

["详细了解 Connector 的网络要求"](#)。

## 3. 按照向导中的步骤创建 Connector：

- \* 准备就绪 \*：单击 \* Azure AD 服务主体 \* 并输入有关 Azure Active Directory 服务主体的信息，该服务主体授予所需权限：
  - 应用程序（客户端）ID：请参见 [\[Get the application ID and directory ID\]](#)。
  - 目录（租户）ID：请参见 [\[Get the application ID and directory ID\]](#)。
  - 客户端密钥：请参见 [\[Create a client secret\]](#)。
- \* 虚拟机身份验证 \*：选择 Azure 订阅，位置，新资源组或现有资源组，然后选择身份验证方法。
- \* 详细信息 \*：输入实例的名称，指定标记，然后选择是希望 Cloud Manager 创建具有所需权限的新角色，还是要选择使用设置的现有角色 ["所需权限"](#)。

请注意，您可以选择与此角色关联的订阅。您选择的每个订阅都为 Connector 提供了在这些订阅中部署 Cloud Volumes ONTAP 的权限。

- \* 网络 \*：选择 vNet 和子网，是否启用公有 IP 地址，并可选择指定代理配置。
- \* 安全组 \*：选择是创建新的安全组，还是选择允许入站 HTTP，HTTPS 和 SSH 访问的现有安全组。



除非您启动 Connector，否则不会向其传入流量。HTTP 和 HTTPS 可用于访问 ["本地 UI"](#)，在极少数情况下使用。只有在需要连接到主机进行故障排除时，才需要使用 SSH。

- \* 审核 \*：查看您选择的内容，确认您的设置正确无误。

## 4. 单击 \* 添加 \*。

虚拟机应在大约 7 分钟内准备就绪。您应停留在页面上，直到此过程完成。

您需要将连接器与工作空间关联，以便 Workspace 管理员可以使用这些连接器创建 Cloud Volumes ONTAP 系统。如果您只有帐户管理员，则不需要将 Connector 与工作空间相关联。默认情况下，帐户管理员可以访问 Cloud Manager 中的所有工作空间。 ["了解更多信息"](#)。

## 从 Cloud Manager 在 Google Cloud 中创建 Connector

客户管理员需要先部署 *Connector*，然后才能使用大多数 Cloud Manager 功能。 ["了解何时需要连接器"](#)。借助此连接器，Cloud Manager 可以管理公有云环境中的资源和流程。

此页面介绍如何直接从 Cloud Manager 在 Google Cloud 中创建 Connector。 ["了解部署 Connector 的其他方法"](#)。

这些步骤必须由具有帐户管理员角色的用户完成。Workspace 管理员无法创建 Connector。



在创建首个 Cloud Volumes ONTAP 工作环境时，如果您还没有连接器，Cloud Manager 将提示您创建一个连接器。

## 设置部署Connector的权限

在部署Connector之前、您需要确保Google Cloud帐户具有正确的权限。

### 步骤

1. "创建自定义角色" 其中包括以下权限：

```
title: Connector deployment policy
description: Permissions for the user who deploys the Connector from
Cloud Manager
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
```

2. 将自定义角色附加到要从Cloud Manager部署Connector的用户。

Google Cloud用户现在具有创建Connector所需的权限。

为**Connector**设置服务帐户

需要使用服务帐户为Connector提供在Google Cloud中管理资源所需的权限。创建此服务帐户时，您需要将其与Connector VM 关联。

此服务帐户的权限与您在上一节中设置的权限不同。

步骤

1. "创建自定义角色" 其中包括以下权限：

```
title: NetApp Cloud Manager
description: Permissions for the service account associated with the
Connector 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.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
```

2. "创建Google Cloud服务帐户并应用您刚刚创建的自定义角色"。
3. 如果要在其他项目中部署 Cloud Volumes ONTAP ， "通过向该项目添加具有 Cloud Manager 角色的服务帐户来授予访问权限"。您需要对每个项目重复此步骤。

已设置Connector VM的服务帐户。

## 共享 VPC 权限

如果您使用共享 VPC 将资源部署到服务项目中，则需要以下权限。此表仅供参考，您的环境应在 IAM 配置完成后反映权限表。

身份	创建者	托管在中	服务项目权限	托管项目权限	目的
用于部署Connector的Google帐户	自定义	服务项目	<ul style="list-style-type: none"> <li>"以上部分中的权限"</li> </ul>	<ul style="list-style-type: none"> <li>compute.networkUser</li> </ul>	在服务项目中部署Connector
连接器服务帐户	自定义	服务项目	<ul style="list-style-type: none"> <li>"以上部分中的权限"</li> </ul>	<ul style="list-style-type: none"> <li>compute.networkUser</li> <li>deploymentmanager.editor</li> </ul>	在服务项目中部署和维护 Cloud Volumes ONTAP 和服务
Cloud Volumes ONTAP 服务帐户	自定义	服务项目	<ul style="list-style-type: none"> <li>storage.admin</li> <li>成员： Cloud Manager 服务帐户为 serviceAccount.user</li> </ul>	不适用	(可选) 适用于数据分层和 Cloud Backup
Google API 服务代理	Google Cloud	服务项目	<ul style="list-style-type: none"> <li>(默认) 编辑器</li> </ul>	<ul style="list-style-type: none"> <li>compute.networkUser</li> </ul>	代表部署与Google Cloud API进行交互。允许 Cloud Manager 使用共享网络。
Google Compute Engine 默认服务帐户	Google Cloud	服务项目	<ul style="list-style-type: none"> <li>(默认) 编辑器</li> </ul>	<ul style="list-style-type: none"> <li>compute.networkUser</li> </ul>	代表部署部署部署部署Google Cloud实例和计算基础架构。允许 Cloud Manager 使用共享网络。

注释：

1. 只有在未向部署传递防火墙规则并选择让 Cloud Manager 为您创建这些规则的情况下，主机项目才需要使用 deploymentManager.editor。如果未指定任何规则， Cloud Manager 将在包含 VPC0 防火墙规则的主机项目中创建部署。
2. 只有当您不向部署传递防火墙规则并选择让 Cloud Manager 为您创建这些规则时，才需要 firewall.create 和 firewall.delete。这些权限位于 Cloud Manager 服务帐户 .yaml 文件中。如果要使用共享 VPC 部署 HA 对，则会使用这些权限为 VC1， 2 和 3 创建防火墙规则。对于所有其他部署，这些权限还将用于为 VPC0 创建规则。
3. 对于数据分层，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，则在使用 getIAMPolicy 查询服务帐户时不会显示权限。

## 启用 Google Cloud API

部署连接器和 Cloud Volumes ONTAP 需要多个 API。

### 步骤

1. "在项目中启用以下 Google Cloud API"。

- Cloud Deployment Manager V2 API
- 云日志记录 API
- Cloud Resource Manager API
- 计算引擎 API
- 身份和访问管理（IAM）API

## 在Google Cloud中创建连接器

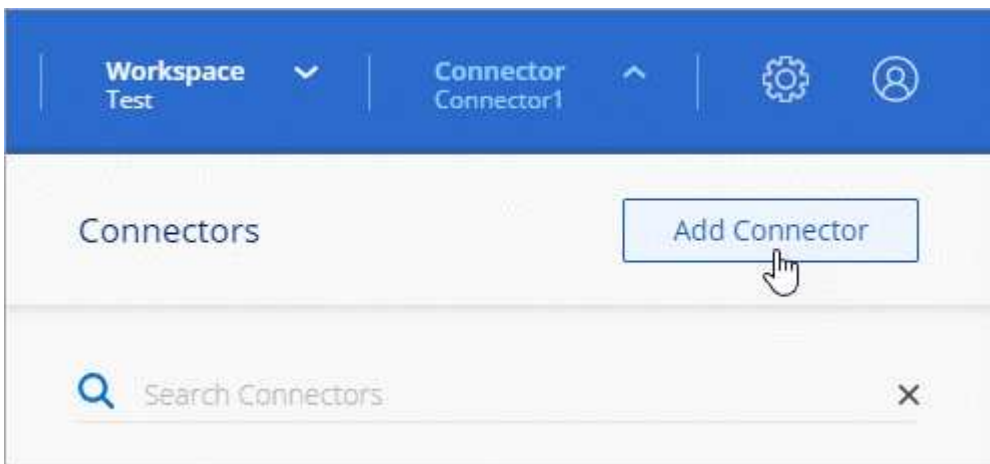
直接从 Cloud Manager 用户界面或使用 gcloud 在 Google Cloud 中创建 Connector。

您需要什么？ #8217 ；将需要什么

- 您的Google Cloud帐户所需的权限、如本页面第一部分所述。
- Google Cloud 项目。
- 一种具有创建和管理 Cloud Volumes ONTAP 所需权限的服务帐户，如本页面第一部分所述。
- 您选择的 Google Cloud 区域中的 VPC 和子网。

## 云管理器

1. 如果要创建首个工作环境，请单击 \* 添加工作环境 \* 并按照提示进行操作。否则，请单击 \* 连接器 \* 下拉列表并选择 \* 添加连接器 \*。



2. 选择 \* Google Cloud Platform\* 作为云提供商。

请记住，Connector 必须与您要创建的工作环境类型以及您计划启用的服务建立网络连接。

["详细了解 Connector 的网络要求"](#)。

3. 按照向导中的步骤创建 Connector：

- \* 准备就绪 \*：查看您需要的内容。
- 如果出现提示，请登录到您的 Google 帐户，该帐户应具有创建虚拟机实例所需的权限。

此表由 Google 拥有和托管。您的凭据不会提供给 NetApp。

- \* 基本设置 \*：输入虚拟机实例的名称，指定标记，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，请参见上述部分）。
- \* 位置 \*：指定实例的区域，分区，VPC 和子网。
- \* 网络 \*：选择是否启用公有 IP 地址，并可选择指定代理配置。
- \* 防火墙策略 \*：选择是创建新的防火墙策略，还是选择允许入站 HTTP，HTTPS 和 SSH 访问的现有防火墙策略。



除非您启动 Connector，否则不会向其传入流量。HTTP 和 HTTPS 可用于访问 ["本地 UI"](#)，在极少数情况下使用。只有在需要连接到主机进行故障排除时，才需要使用 SSH。

- \* 审核 \*：查看您选择的内容，确认您的设置正确无误。

4. 单击 \* 添加 \*。

此实例应在大约 7 分钟后准备就绪。您应停留在页面上，直到此过程完成。

## 云

1. 使用您首选的方法登录到 gcloud SDK。

在我们的示例中、我们将使用安装了gcloud SDK的本地Shell、但您可以在Google云控制台中使用原生Google Cloud Shell。

有关 Google Cloud SDK 的详细信息，请访问 ["Google Cloud SDK 文档页面"](#)。

2. 验证您是否以具有上一节中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 \* 用户帐户是要以身份登录的所需用户帐户：

```
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=n1-standard-4
  --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) 要部署 VM 的项目。

## 服务帐户

步骤 2 输出中指定的服务帐户。

## 分区

要部署 VM 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有 Internet)

## 网络标记

(可选) 添加网络标记以使用标记将防火墙规则链接到 Connector 实例

## 网络路径

(可选) 添加要将 Connector 部署到的网络的名称 (对于共享 VPC, 您需要完整路径)

## 子网路径

(可选) 添加要将 Connector 部署到的子网的名称 (对于共享 VPC, 您需要完整路径)

## kms-key-path

(可选) 添加 KMS 密钥以加密连接器的磁盘 (还需要应用 IAM 权限)

有关这些标志的详细信息, 请访问 ["Google Cloud 计算 SDK 文档"](#)。

+

运行命令可使用 NetApp 黄金映像部署 Connector。Connector 实例和软件应在大约五分钟内运行。

1. 从已连接到 Connector 实例的主机打开 Web 浏览器, 然后输入以下 URL:

`http://ipaddress:80[]`

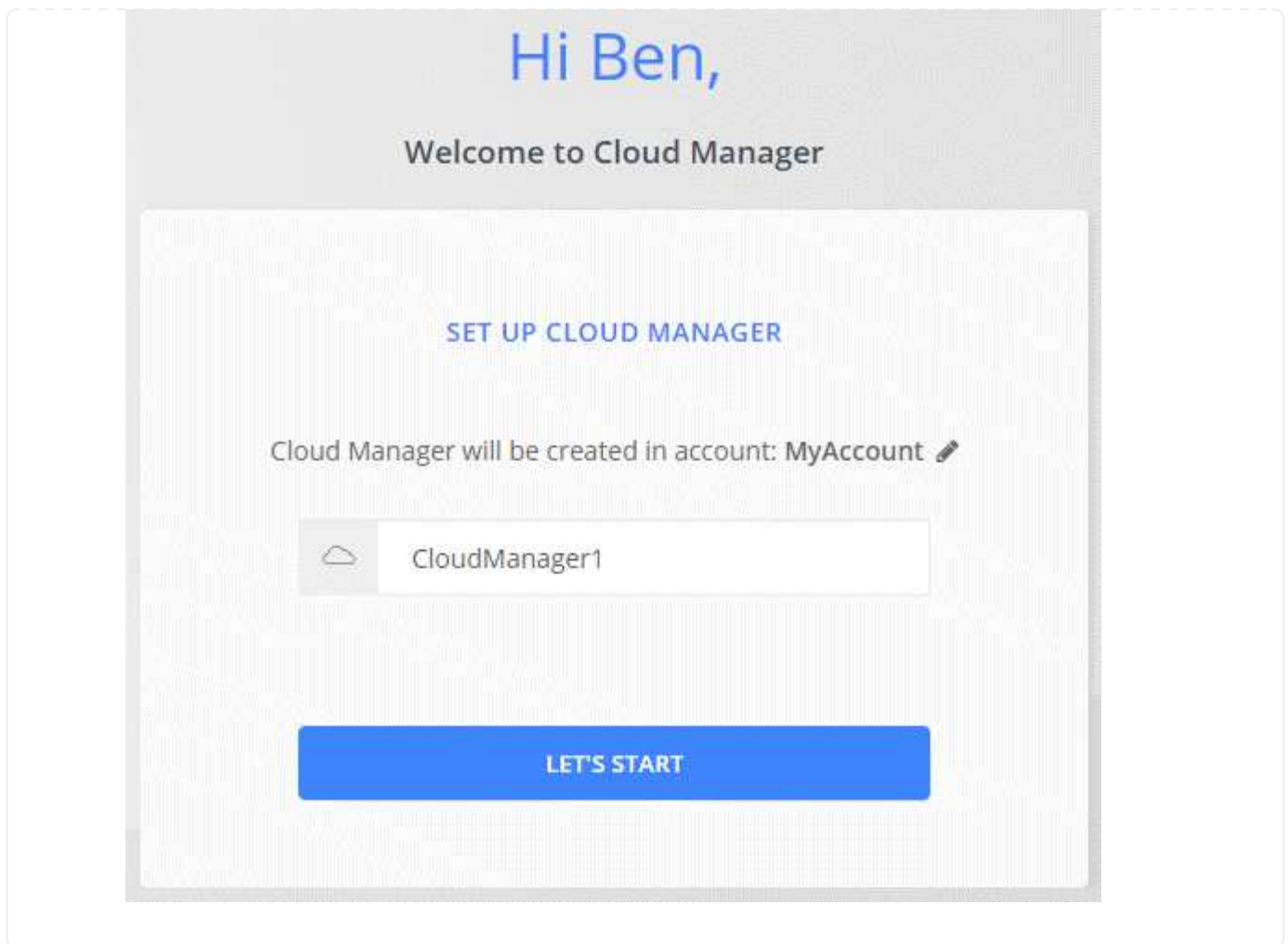
2. 登录后, 设置 Connector:

- a. 指定要与 Connector 关联的 NetApp 帐户。

["了解 NetApp 客户"](#)。

- b. 输入系统名称。





现在，您可以使用 NetApp 帐户安装并设置 Connector。Cloud Manager 将在您创建新的工作环境时自动使用此 Connector。但是，如果您有多个 Connector，则需要 [在它们之间切换](#)。

## 下一步行动

登录并设置 Cloud Manager 后，用户便可开始创建和发现工作环境。

- ["开始使用适用于 AWS 的 Cloud Volumes ONTAP"](#)
- ["开始使用适用于 Azure 的 Cloud Volumes ONTAP"](#)
- ["开始使用适用于 Google Cloud 的 Cloud Volumes ONTAP"](#)
- ["设置 Azure NetApp Files"](#)
- ["设置适用于 ONTAP 的 Amazon FSX"](#)
- ["为 AWS 设置 Cloud Volumes Service"](#)
- ["发现内部 ONTAP 集群"](#)
- ["发现您的 Amazon S3 存储分段"](#)

# 管理 Cloud Manager

## NetApp 帐户

管理您的 **NetApp** 帐户

"[执行初始设置后](#)"，您可以稍后通过管理用户，服务帐户，工作空间，连接器和订阅来管理帐户设置。

"[详细了解 NetApp 客户的工作原理](#)"。

使用租户 **API** 管理您的帐户

如果要通过发送 API 请求来管理帐户设置，则需要使用 `_租户` API。此 API 与用于创建和管理 Cloud Volumes ONTAP 工作环境的 Cloud Manager API 不同。

"[查看租户 API 的端点](#)"

创建和管理用户

您帐户中的用户可以访问管理帐户工作空间中的资源。

添加用户

将 Cloud Central 用户与 NetApp 帐户关联，以便这些用户可以在 Cloud Manager 中创建和管理工作环境。

步骤

1. 如果用户尚未执行此操作，请让用户转到 "[NetApp Cloud Central](#)" 并注册。
2. 从 Cloud Manager 顶部，单击 \* 帐户 \* 下拉列表。



3. 单击当前选定帐户旁边的 \* 管理帐户 \*。



4. 在成员选项卡中，单击 \* 关联用户 \*。
5. 输入用户的电子邮件地址并为用户选择一个角色：
  - \* 帐户管理员 \*：可以在 Cloud Manager 中执行任何操作。
  - \* 工作空间管理员 \*：可以在分配的工作空间中创建和管理资源。
  - \* 合规性查看器 \*：只能查看 Cloud Data sense 合规性信息，并为其有权访问的工作空间生成报告。
  - \* SnapCenter Admin\*：可以使用 SnapCenter 服务创建应用程序一致的备份并使用这些备份还原数据。\_ 此服务当前处于测试阶段。 \_
6. 如果选择了 Workspace Admin 或 Compliance Viewer，请选择一个或多个要与该用户关联的工作空间。



The image shows a web-based dialog box titled "Associate User". At the top, there is a user icon. Below the title, a light blue banner contains the text: "To add a user to your NetApp Cloud Account, that user must already have signed up at [NetApp Cloud Central](#). Enter the email address that they used when signing up with Cloud Central." The main form area has three sections: "User's Email" with a text input field containing "test@netapp.com"; "Role" with a dropdown menu showing "Workspace Admin"; and "Associate User to Workspaces" with a dropdown menu showing "Workspace-1" and a close icon. At the bottom, there are two buttons: a grey "Cancel" button and a blue "Associate User" button.



### Associate User

To add a user to your NetApp Cloud Account, that user must already have signed up at [NetApp Cloud Central](#). Enter the email address that they used when signing up with Cloud Central.

User's Email

test@netapp.com

Role

Workspace Admin

Associate User to Workspaces

Workspace-1

Cancel Associate User

7. 单击 \* 关联 \*。

用户应从 NetApp Cloud Central 收到一封标题为 " 客户关联 " 的电子邮件。此电子邮件包含访问 Cloud Manager 所需的信息。

#### 删除用户

解除用户关联后，用户将无法再访问 NetApp 帐户中的资源。

#### 步骤

1. 从 Cloud Manager 顶部，单击 \* 帐户 \* 下拉列表，然后单击 \* 管理帐户 \*。



2. 在成员选项卡中，单击与用户对应的行中的操作菜单。



3. 单击 \* 解除关联用户 \*，然后单击 \* 解除关联 \* 进行确认。

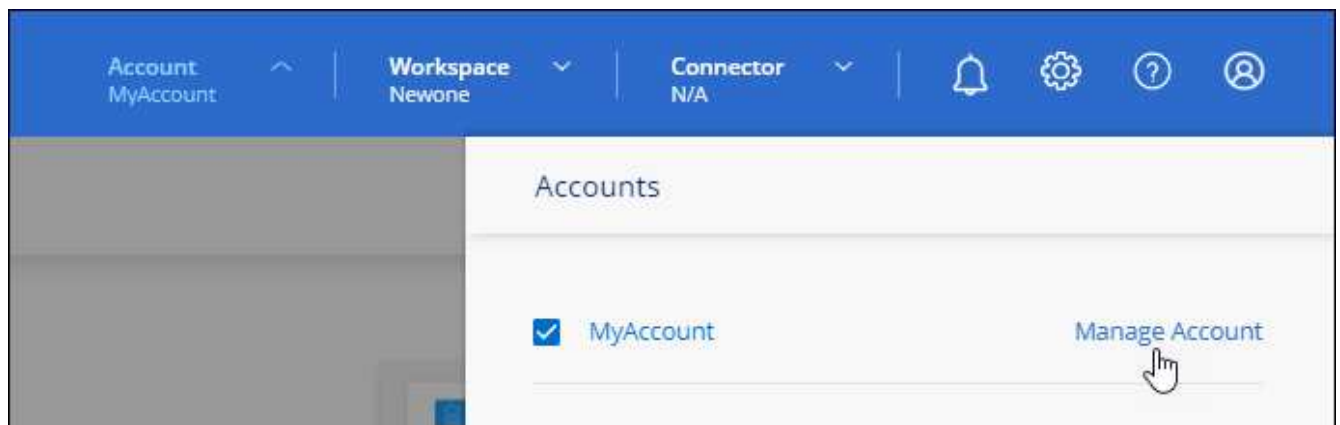
用户无法再访问此 NetApp 帐户中的资源。

管理 **Workspace Admin** 的工作空间

您可以随时将 Workspace Admins 与工作空间关联和解除关联。通过关联用户，用户可以在该工作空间中创建和查看工作环境。

步骤

1. 从 Cloud Manager 顶部，单击 \* 帐户 \* 下拉列表，然后单击 \* 管理帐户 \*。



2. 在成员选项卡中，单击与用户对应的行中的操作菜单。

5 Members						
Type	Name	Email	Role	Workspace		
	Ben		☆ Account Admin	All Workspaces	...	
	Tom		☆ Account Admin	All Workspaces	...	
	Ben		Workspace Admin	Newone		

3. 单击 \* 管理工作空间 \*。

4. 选择要与用户关联的工作空间，然后单击 \* 应用 \*。

现在，只要 Connector 还与这些工作空间关联，用户就可以从 Cloud Manager 访问这些工作空间。

### 创建和管理服务帐户

服务帐户充当 "用户"，可以通过授权 API 调用 Cloud Manager 来实现自动化。这样可以更轻松的管理自动化，因为您不需要基于可以随时离开公司的真实用户帐户构建自动化脚本。如果您使用的是联合，则可以创建令牌，而无需从云生成刷新令牌。

您可以通过为服务帐户分配角色来为其授予权限，就像任何其他 Cloud Manager 用户一样。您还可以将服务帐户与特定工作空间相关联，以控制服务可以访问的工作环境（资源）。

创建服务帐户时，您可以通过 Cloud Manager 复制或下载此服务帐户的客户端 ID 和客户端密钥。此密钥对用于通过 Cloud Manager 进行身份验证。

### 创建服务帐户

根据需要创建尽可能多的服务帐户来管理工作环境中的资源。

### 步骤

1. 从 Cloud Manager 顶部，单击 \* 帐户 \* 下拉列表。



2. 单击当前选定帐户旁边的 \* 管理帐户 \*。



3. 在成员选项卡中，单击 \* 创建服务帐户 \*。
4. 输入名称并选择角色。如果您选择的角色不是帐户管理员，请选择要与此服务帐户关联的工作空间。
5. 单击 \* 创建 \*。
6. 复制或下载客户端 ID 和客户端密钥。

此客户端密钥只能显示一次，不会由 Cloud Manager 存储在任何位置。复制或下载密钥并将其安全存储。

7. 单击 \* 关闭 \*。

获取服务帐户的令牌

以便对进行 API 调用 **"租户 API"**，您需要为服务帐户获取一个不带标志。

```
curl --location --request POST 'https://netapp-cloud-account.auth0.com/oauth/token' \
--header 'Content-Type: application/json' \
--data-raw '{
  "grant_type": "client_credentials",
  "client_secret": "<client secret>",
  "audience": "https://api.cloud.netapp.com",
  "client_id": "<client id>"
}'
```

正在复制客户端 ID

您可以随时复制服务帐户的客户端 ID。

步骤

1. 在成员选项卡中，单击与服务帐户对应的行中的操作菜单。



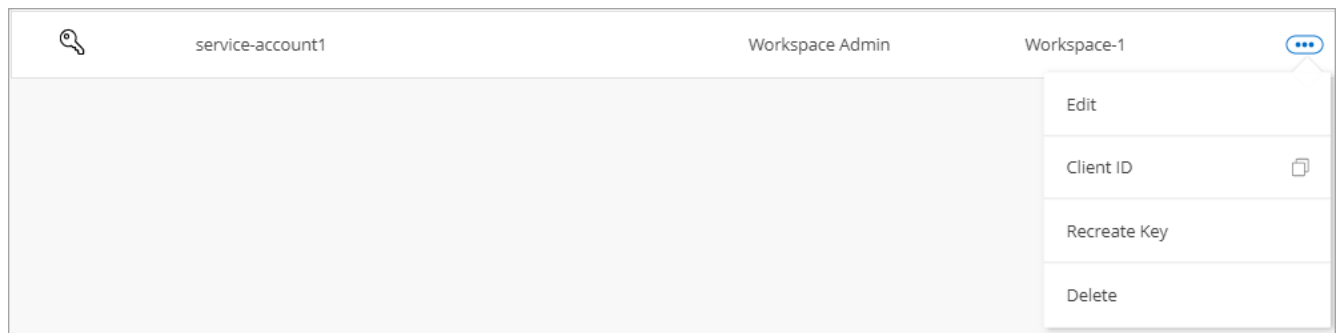
2. 单击 \* 客户端 ID\* 。
3. 此 ID 将复制到剪贴板。

正在重新创建密钥

重新创建此密钥将删除此服务帐户的现有密钥，然后创建新密钥。您将无法使用上一个密钥。

步骤

1. 在成员选项卡中，单击与服务帐户对应的行中的操作菜单。



2. 单击 \* 重新创建密钥\* 。
3. 单击 \* 重新创建\* 进行确认。
4. 复制或下载客户端 ID 和客户端密钥。

此客户端密钥只能显示一次，不会由 Cloud Manager 存储在任何位置。复制或下载密钥并将其安全存储。

5. 单击 \* 关闭\* 。

删除服务帐户

如果不再需要使用某个服务帐户，请将其删除。

步骤

1. 在成员选项卡中，单击与服务帐户对应的行中的操作菜单。





2. 单击 \* 删除 \*。
3. 再次单击 \* 删除 \* 进行确认。

## 管理工作空间

通过创建，重命名和删除工作空间来管理工作空间。请注意，如果某个工作空间包含任何资源，则无法将其删除。必须为空。

### 步骤

1. 从 Cloud Manager 顶部，单击 \* 帐户 \* 下拉列表，然后单击 \* 管理帐户 \*。
2. 单击 \* 工作空间 \*。
3. 选择以下选项之一：
  - 单击 \* 添加新工作空间 \* 以创建新工作空间。
  - 单击 \* 重命名 \* 以重命名工作空间。
  - 单击 \* 删除 \* 以删除此工作空间。

## 管理 **Connector** 的工作空间

您需要将 Connector 与工作空间关联，以便 Workspace 管理员可以从 Cloud Manager 访问这些工作空间。

如果您只有帐户管理员，则不需要将 Connector 与工作空间相关联。默认情况下，帐户管理员可以访问 Cloud Manager 中的所有工作空间。

["详细了解用户，工作空间和连接器"。](#)

### 步骤

1. 从 Cloud Manager 顶部，单击 \* 帐户 \* 下拉列表，然后单击 \* 管理帐户 \*。
2. 单击 \* 连接器 \*。
3. 单击要关联的 Connector 的 \* 管理工作空间 \*。
4. 选择要与 Connector 关联的工作空间，然后单击 \* 应用 \*。

## 管理订阅

从云提供商的市场订阅后，每个订阅均可从 Account Settings 小工具中获取。您可以选择重命名订阅并取消订阅与一个或多个帐户的关联。

例如，假设您有两个帐户，每个帐户都通过单独的订阅付费。您可能会解除某个订阅与某个帐户的关联，以便该

帐户中的用户在创建 Cloud Volume ONTAP 工作环境时不会意外选择错误的订阅。

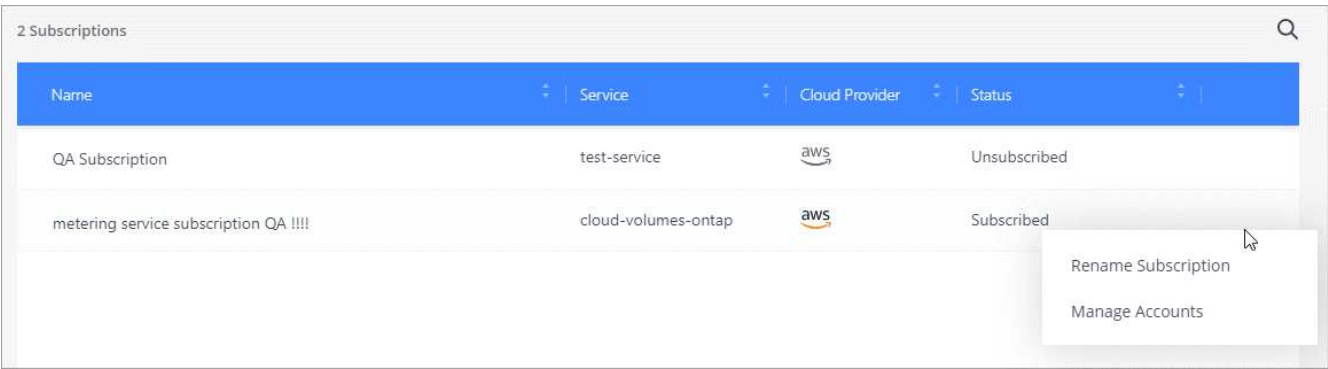
["了解有关订阅的更多信息"](#)。

步骤

- 1. 从 Cloud Manager 顶部，单击 \* 帐户 \* 下拉列表，然后单击 \* 管理帐户 \*。
- 2. 单击 \* 订阅 \*。

您将只看到与当前正在查看的帐户关联的订阅。

- 3. 单击与要管理的订阅对应的行中的操作菜单。



- 4. 选择重命名订阅或管理与订阅关联的帐户。

更改帐户名称

随时更改您的帐户名称，将其更改为对您有意义的名称。

步骤

- 1. 从 Cloud Manager 顶部，单击 \* 帐户 \* 下拉列表，然后单击 \* 管理帐户 \*。
- 2. 在 \* 概述 \* 选项卡中，单击帐户名称旁边的编辑图标。
- 3. 键入新帐户名称并单击 \* 保存 \*。

允许私有预览

允许在您的帐户中进行私有预览，以访问在 Cloud Manager 中预览的新 NetApp 云服务。

私有预览中的服务无法保证按预期运行，并且可能会持续中断并缺少功能。

步骤

- 1. 从 Cloud Manager 顶部，单击 \* 帐户 \* 下拉列表，然后单击 \* 管理帐户 \*。
- 2. 在 \* 概述 \* 选项卡中，启用 \* 允许私有预览 \* 设置。

允许第三方服务

允许您帐户中的第三方服务访问 Cloud Manager 中提供的第三方服务。第三方服务是指与 NetApp 提供的服务类似的云服务，但它们由第三方公司管理和支持。

步骤

1. 从 Cloud Manager 顶部，单击 \* 帐户 \* 下拉列表，然后单击 \* 管理帐户 \*。
2. 在 \* 概述 \* 选项卡中，启用 \* 允许第三方服务 \* 设置。


禁用 SaaS 平台

除非您需要遵守公司的安全策略，否则我们不建议禁用 SaaS 平台。禁用 SaaS 平台会限制您使用 NetApp 集成云服务的能力。

如果禁用 SaaS 平台，则无法从 Cloud Manager 获得以下服务：

- 云数据感知
- Kubernetes
- 云分层
- 全局文件缓存

如果禁用 SaaS 平台，则需要从执行所有任务 ["Connector 上提供的本地用户界面"](#)。



此操作不可逆，将阻止您使用 Cloud Manager SaaS 平台。您需要从本地连接器执行操作。您将无法使用 NetApp 的许多集成云服务，重新启用 SaaS 平台需要 NetApp 支持的帮助。

步骤

1. 从 Cloud Manager 顶部，单击 \* 帐户 \* 下拉列表，然后单击 \* 管理帐户 \*。
2. 在概述选项卡中，切换选项以禁用 SaaS 平台。

监控帐户中的操作


您可以监控 Cloud Manager 正在执行的操作的状态，以查看是否存在需要解决的任何问题。您可以在通知中心、时间线中查看状态、也可以向您的电子邮件发送通知。

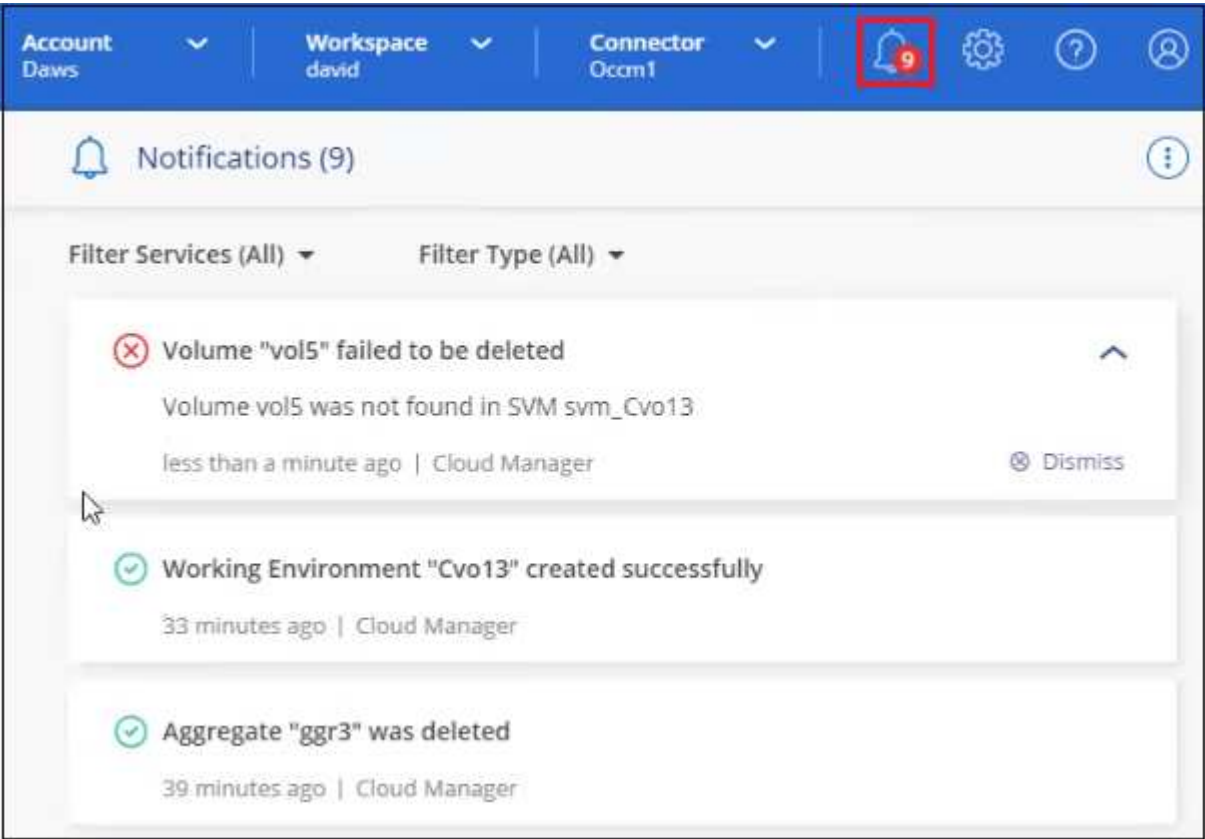
此表对通知中心和时间线进行了比较，以便您了解每个通知中心的功能。

通知中心	时间线
显示事件和操作的高级状态	提供每个事件或操作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，此信息不会显示在通知中心中	保留上个月的状态
仅显示在用户界面中启动的操作	显示 UI 或 API 中的所有操作
显示用户启动的操作	显示所有操作，无论是用户启动的操作还是系统启动的操作
按重要性筛选结果	按服务，操作，用户，状态等进行筛选
可以通过电子邮件向帐户用户和其他人发送通知	无电子邮件功能

使用通知中心监控活动

通知可跟踪您在Cloud Manager中启动的操作的进度、以便您验证操作是否成功。您可以通过它们查看当前登录会话期间启动的许多Cloud Manager操作的状态。目前、并非所有服务都会将信息报告到通知中心。

您可以通过单击通知铃。铃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，则表示您应查看一条重要通知。



此外、您还可以将Cloud Manager配置为通过电子邮件发送通知、以便即使未登录到系统、您也能了解重要的系统活动。您可以将电子邮件发送给您的NetApp云帐户中的任何Cloud Central用户、也可以发送给需要了解某些类型的系统活动的任何其他收件人。请参见 [设置电子邮件通知设置](#)。

通知类型

通知分为以下几类：

通知类型	Description
严重	发生的问题可能会导致服务中断，如果不立即采取更正操作。
error	以失败结束的操作或过程、或者如果不采取更正操作、可能导致失败。
警告	为确保问题描述 不会达到严重级别而应注意的。此严重性的通知不会中断发生原因 服务、可能不需要立即采取更正操作。
建议	系统建议您采取措施来改进系统或特定服务；例如：节省成本、建议新服务、建议安全配置等
信息	向追加信息 提供有关操作或进程的消息。

通知类型	Description
success	操作或进程已成功完成。

#### 筛选通知

默认情况下，您将看到所有通知。您可以筛选通知中心中显示的通知，以便仅显示对您重要的通知。您可以按 Cloud Manager " 服务 " 和通知 " 类型 " 进行筛选。

例如，如果您只想查看 Cloud Manager 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。

#### 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、以便即使未登录到Cloud Manager、您也可以了解重要的系统活动。您可以向NetApp帐户中的任何用户或需要了解某些类型的系统活动的任何其他收件人发送电子邮件。

**\*注意：** \*如果Connector安装在无法访问Internet的站点上、则不支持发送电子邮件通知。

默认情况下、客户管理员将收到所有"严重"和"建议"通知的电子邮件。默认情况下、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。

您必须是帐户管理员才能自定义通知设置。

#### 步骤

1. 在Cloud Manager菜单栏中、单击\*设置>警报和通知设置\*。



2. 从 \_Account Users\_ 选项卡或 \_Additional Recipients\_ 选项卡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、请单击该用户的Notifications列中的菜单、检查要发送的通知类型、然后单击\*应用\*。
- 要对多个用户进行更改、请选中每个用户对应的框、单击\*管理电子邮件通知\*、检查要发送的通知类型、然后单击\*应用\*。

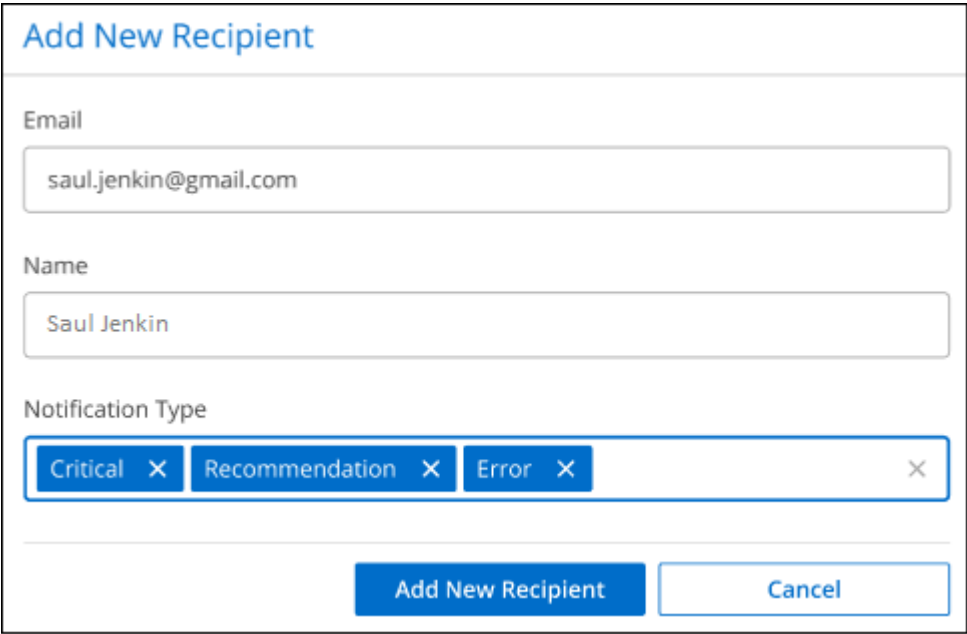


添加其他电子邮件收件人

"Account Users"选项卡中显示的用户将自动从NetApp帐户中的用户(从 "管理帐户页面")。您可以在 \_Additional recipients\_ 选项卡中为无权访问Cloud Manager但需要获得特定类型警报和通知通知的其他人员或组添加电子邮件地址。

步骤

1. 在警报和通知设置页面中、单击\*添加新收件人\*。

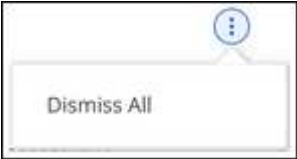



The image shows a form titled "Add New Recipient". It contains three input fields: "Email" with the value "saul.jenkin@gmail.com", "Name" with the value "Saul Jenkin", and "Notification Type" which is a multi-select dropdown menu. The menu is open, showing three selected options: "Critical", "Recommendation", and "Error". At the bottom of the form are two buttons: "Add New Recipient" and "Cancel".

2. 输入姓名、电子邮件地址、选择收件人将收到的通知类型、然后单击\*添加新收件人\*。

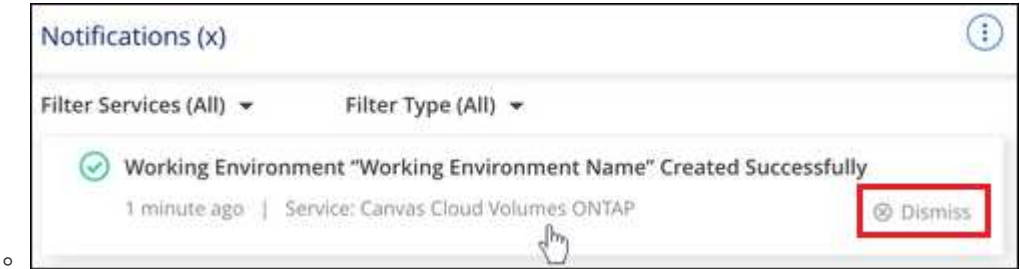
取消通知

如果您不再需要查看通知，可以从页面中删除这些通知。您可以一次性取消所有通知，也可以取消单个通知。



要取消所有通知，请在通知中心中单击  并选择 \* 全部取消 \*。

要取消单个通知，请将光标悬停在通知上方，然后单击 \* 取消 \*



审核帐户中的用户活动

Cloud Manager 中的时间线显示了用户为管理您的帐户而完成的操作。其中包括关联用户，创建工作空间，创建连接器等管理操作。

如果您需要确定执行特定操作的人员，或者需要确定操作的状态，则检查时间线会很有帮助。

步骤

1. 在Cloud Manager菜单栏中、单击\*设置>时间线\*。

2. 在筛选器下，单击 \* 服务 \*，启用 \* 租户 \*，然后单击 \* 应用 \*。

时间线将更新以显示帐户管理操作。

## 角色

帐户管理员，工作空间管理员，合规性查看器和 SnapCenter 管理员角色可为用户提供特定权限。

合规性查看器角色用于只读云数据感知访问。

任务	帐户管理员	工作空间管理员	合规性查看器	SnapCenter 管理员
管理工作环境	是的。	是的。	否	否
在工作环境中启用服务	是的。	是的。	否	否
查看数据复制状态	是的。	是的。	否	否
查看时间表	是的。	是的。	否	否
在工作空间之间切换	是的。	是的。	是的。	否
查看数据感知扫描结果	是的。	是的。	是的。	否
删除工作环境	是的。	否	否	否
将 Kubernetes 集群连接到工作环境	是的。	否	否	否
接收 Cloud Volumes ONTAP 报告	是的。	否	否	否
创建连接器	是的。	否	否	否
管理 NetApp 帐户	是的。	否	否	否
管理凭据	是的。	否	否	否
修改 Cloud Manager 设置	是的。	否	否	否
查看和管理支持仪表板	是的。	否	否	否
从 Cloud Manager 中删除工作环境	是的。	否	否	否
安装 HTTPS 证书	是的。	否	否	否
使用 SnapCenter 服务	是的。	是的。	否	是的。

## 相关链接

- ["在 NetApp 帐户中设置工作空间和用户"](#)
- ["管理 NetApp 帐户中的工作空间和用户"](#)



# 连接器

## 高级部署

### 从 AWS Marketplace 创建 Connector

最好直接从 Cloud Manager 创建 Connector，但如果您不想指定 AWS 访问密钥，则可以从 AWS Marketplace 启动 Connector。创建并设置 Connector 后，Cloud Manager 将在您创建新的工作环境时自动使用它。

#### 步骤

1. 在AWS中设置权限：
  - a. 在IAM控制台中、通过复制和粘贴内容来创建您自己的策略 "[Connector的IAM策略](#)"。
  - b. 创建角色类型为 Amazon EC2 的 IAM 角色，并将您在上一步骤中创建的策略附加到该角色。
2. 现在转到 "[AWS Marketplace 上的 Cloud Manager 页面](#)" 从 AMI 部署 Cloud Manager。

IAM 用户必须具有 AWS Marketplace 权限才能订阅和取消订阅。

3. 在 Marketplace 页面上，单击 \* 继续订阅 \*，然后单击 \* 继续配置 \*。

**a**

Cloud Manager - Manual Installation without access keys

By: [NetApp, Inc.](#) Latest Version: 3.8.4

Read below for instructions on how to deploy Cloud Volumes ONTAP.

Linux/Unix ★★★★★ 6 AWS reviews

Typical Total Price  
**\$0.226/hr**  
Total pricing per instance for services hosted on t3.xlarge in US East (N. Virginia). [View Details](#)

Continue to Subscribe

Save to List

Overview Pricing Usage Support Reviews

### Product Overview

Do NOT subscribe on this page unless instructed by NetApp or redirected here from the NetApp website.

This listing lets you manually launch a Cloud Manager instance without providing your AWS credentials. After launching the Cloud Manager software in AWS, you can access it by entering the instance's IP address in a web browser. If you subscribe here, you still need to subscribe on the listing below for PAYGO charges.

### Highlights

- See Product Overview for instructions on how to deploy NetApp Cloud Manager.

**b**

Cloud Manager - Manual Installation without access keys

Continue to Configuration

< Product Detail Subscribe

### Subscribe to this software

You're subscribed to this software. Please see the terms and pricing details below or click the button above to configure your software.

### Terms and Conditions

#### NetApp, Inc. Offer

You have subscribed to this software and agreed that your use of this software is subject to the pricing terms and the seller's [End User License Agreement \(EULA\)](#). You agreed that AWS may share information about this transaction (including your payment terms) with the respective seller, reseller or underlying provider, as applicable, in accordance with the [AWS Privacy Notice](#). Your use of AWS services remains subject to the [AWS Customer Agreement](#) or other agreement with AWS governing your use of such services.

4. 更改任何默认选项，然后单击 \* 继续启动 \*。

5. 在 \* 选择操作 \* 下，选择 \* 通过 EC2 启动 \*，然后单击 \* 启动 \*。

以下步骤介绍了如何从 EC2 控制台启动实例，因为控制台允许您将 IAM 角色附加到 Cloud Manager 实例。使用 \* 从网站启动 \* 操作无法实现这一点。

6. 按照提示配置和部署实例：

- \* 选择实例类型 \*：根据区域可用性，选择支持的实例类型之一（建议使用 T3.xlarge）。

["查看实例要求"](#)。

- \* 配置实例 \*：选择一个 VPC 和子网，选择您在第 1 步中创建的 IAM 角色，启用终止保护（建议），然后选择符合您要求的任何其他配置选项。

Number of instances	1	<a href="#">Launch into Auto Scaling Group</a>
Purchasing option	<input type="checkbox"/> Request Spot instances	
Network	vpc-a76d91c2   VPC4QA (default)	<a href="#">Create new VPC</a>
Subnet	subnet-39536c13   QASubnet1   us-east-1b 155 IP Addresses available	<a href="#">Create new subnet</a>
Auto-assign Public IP	Enable	
Placement group	<input type="checkbox"/> Add instance to placement group	
Capacity Reservation	Open	<a href="#">Create new Capacity Reservation</a>
IAM role	Cloud_Manager	<a href="#">Create new IAM role</a>
CPU options	<input type="checkbox"/> Specify CPU options	
Shutdown behavior	Stop	
Enable termination protection	<input checked="" type="checkbox"/> Protect against accidental termination	
Monitoring	<input type="checkbox"/> Enable CloudWatch detailed monitoring <a href="#">Additional charges apply.</a>	

- \* 添加存储 \*：保留默认存储选项。
- \* 添加标记 \*：根据需输入实例的标记。
- \* 配置安全组 \*：指定 Connector 实例所需的连接方法：SSH，HTTP 和 HTTPS。
- \* 审阅 \*：查看您选择的内容，然后单击 \* 启动 \*。

AWS 使用指定的设置启动软件。Connector 实例和软件应在大约五分钟内运行。

7. 从已连接到 Connector 实例的主机打开 Web 浏览器，然后输入以下 URL：

`http://ipaddress:80[]`

8. 登录后，设置 Connector：

- a. 指定要与 Connector 关联的 NetApp 帐户。

["了解 NetApp 客户"](#)。

- b. 输入系统名称。



现在，您可以使用 NetApp 帐户安装并设置 Connector。Cloud Manager 将在您创建新的工作环境时自动使用此 Connector。但是，如果您有多个 Connector，则需要 ["在它们之间切换"](#)。

### 从 **Azure Marketplace** 创建 **Connector**

最好直接从 Cloud Manager 创建 Connector，但如果愿意，您可以从 Azure Marketplace 启动 Connector。创建并设置 Connector 后，Cloud Manager 将在您创建新的工作环境时自动使用它。

#### 在 **Azure** 中创建连接器

使用 Azure Marketplace 中的映像部署 Connector，然后登录到 Connector 以指定您的 NetApp 帐户。

#### 步骤

1. 转到 Azure Marketplace 中的 NetApp Connector VM 页面。
  - ["适用于商业区域的 Azure Marketplace 页面"](#)
  - ["Azure 政府区域的 Azure Marketplace 页面"](#)
2. 单击 \* 立即获取 \*，然后单击 \* 继续 \*。
3. 在 Azure 门户中，单击 \* 创建 \*，然后按照步骤配置虚拟机。

配置虚拟机时，请注意以下事项：

- 借助 HDD 或 SSD 磁盘、Cloud Manager 可以实现最佳性能。
- 选择满足 CPU 和 RAM 要求的 VM 大小。我们建议使用 DS3 v2 。

["查看虚拟机要求"](#)。

- 对于网络安全组，Connector 需要使用 SSH，HTTP 和 HTTPS 进行入站连接。

["详细了解 Connector 的安全组规则"](#)。

- 在 \* 管理 \* 下，通过选择 \* 启用 \* 系统分配的托管身份 \* 来为连接器启用。

此设置非常重要，因为托管身份允许 Connector 虚拟机在不提供任何凭据的情况下向 Azure Active Directory 标识自己。 ["详细了解 Azure 资源的托管身份"](#)。

4. 在 \* 查看 + 创建 \* 页面上，查看所做的选择并单击 \* 创建 \* 以开始部署。

Azure 使用指定的设置部署虚拟机。虚拟机和 Connector 软件应在大约五分钟内运行。

5. 从已连接到 Connector 虚拟机的主机打开 Web 浏览器，然后输入以下 URL：

`http://ipaddress:80[]`

6. 登录后，设置 Connector：

- a. 指定要与 Connector 关联的 NetApp 帐户。

["了解 NetApp 客户"](#)。

- b. 输入系统名称。



现在，已安装并设置 Connector。您必须先授予 Azure 权限，然后用户才能在 Azure 中部署 Cloud Volumes ONTAP。

正在授予 **Azure** 权限

在 Azure 中部署 Connector 时，您应已启用 ["系统分配的受管身份"](#)。现在，您必须先创建一个自定义角色，然后为一个或多个订阅的 Connector 虚拟机分配此角色，从而授予所需的 Azure 权限。

步骤

1. 创建自定义角色：
  - a. 复制的内容 ["Connector的自定义角色权限"](#) 并将其保存在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。

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

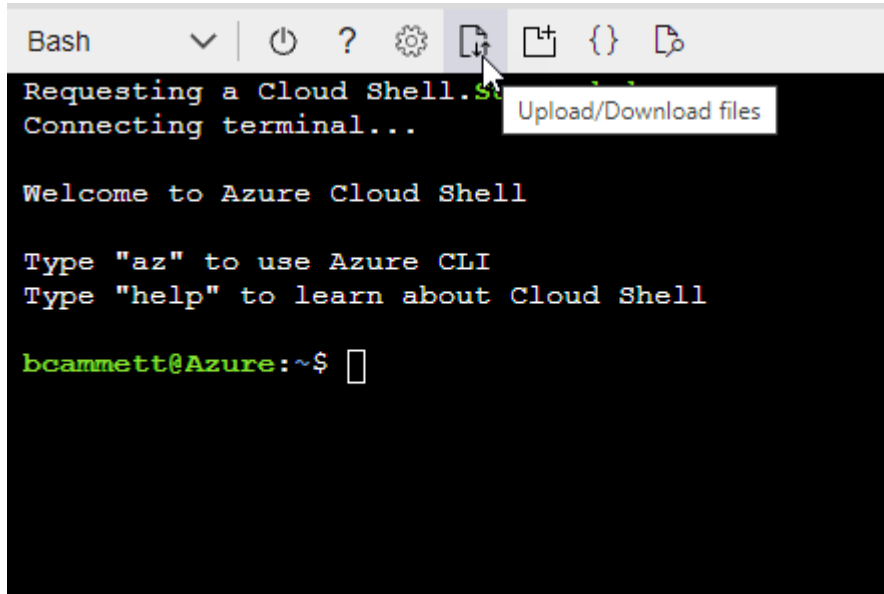
▪ 示例 \*

```
"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。

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

- start "Azure Cloud Shell" 并选择 Bash 环境。
- 上传 JSON 文件。



- 输入以下 Azure 命令行界面命令：

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

现在，您应该拥有一个名为 Cloud Manager Operator 的自定义角色，可以将该角色分配给 Connector 虚拟机。

2. 为一个或多个订阅向 Connector 虚拟机分配角色：

- a. 打开 \* 订阅 \* 服务，然后选择要部署 Cloud Volumes ONTAP 系统的订阅。
- b. 单击 \* 访问控制（IAM） \* > \* 添加 \* > \* 添加角色分配 \*。
- c. 在 \* 角色 \* 选项卡中，选择 \* Cloud Manager 操作员 \* 角色，然后单击 \* 下一步 \*。



Cloud Manager Operator 是 Cloud Manager 策略中提供的默认名称。如果您为角色选择了其他名称，请选择该名称。

- d. 在 \* 成员 \* 选项卡中，完成以下步骤：

- 为 \* 受管身份 \* 分配访问权限。
- 单击 \* 选择成员 \*，选择创建 Connector 虚拟机的订阅，选择 \* 虚拟机 \*，然后选择 Connector 虚拟机。
- 单击 \* 选择 \*。

- 单击 \* 下一步 \*。
- e. 单击 \* 审核 + 分配 \*。
- f. 如果要从其他订阅部署 Cloud Volumes ONTAP、请切换到该订阅，然后重复这些步骤。

现在，Connector 拥有管理公有云环境中的资源和流程所需的权限。Cloud Manager 将在您创建新的工作环境时自动使用此 Connector。但是，如果您有多个 Connector，则需要 ["在它们之间切换"](#)。

在可访问 **Internet** 的现有 **Linux** 主机上安装 **Connector**

创建 Connector 的最常见方法是直接从 Cloud Manager 或云提供商的市场创建。但是，您可以选择在网络或云中的现有 Linux 主机上下载并安装 Connector 软件。这些步骤特定于可访问 Internet 的主机。

["了解部署 Connector 的其他方法"](#)。



如果要在 Google Cloud 中创建 Cloud Volumes ONTAP 系统，则必须同时在 Google Cloud 中运行 Connector。您不能使用在 AWS，Azure 或内部运行的 Connector。

验证主机要求

连接器软件必须在满足特定操作系统要求，RAM 要求，端口要求等要求的主机上运行。

需要一个专用主机

与其他应用程序共享的主机不支持此连接器。主机必须是专用主机。

## CPU

4 个核心或 4 个 vCPU

## RAM

16 GB

## AWS EC2 实例类型

满足上述 CPU 和 RAM 要求的实例类型。我们建议使用 T3.xlarge。

## Azure 虚拟机大小

满足上述 CPU 和 RAM 要求的实例类型。我们建议使用 DS3 v2。

## GCP 计算机类型

满足上述 CPU 和 RAM 要求的实例类型。我们建议使用 n1-standard-4。

在具有支持的操作系统的 VM 实例上、Google Cloud 支持 Connector ["屏蔽 VM 功能"](#)

支持的操作系统

- CentOS 7.6
- CentOS 7.7
- CentOS 7.8
- CentOS 7.9



- Red Hat Enterprise Linux 7.6
- Red Hat Enterprise Linux 7.7
- Red Hat Enterprise Linux 7.8
- Red Hat Enterprise Linux 7.9

Red Hat Enterprise Linux 系统必须在 Red Hat 订购管理中注册。如果未注册，则在安装 Connector 期间，系统无法访问存储库来更新所需的第三方软件。

这些操作系统的英语版本支持 Connector。

## 虚拟机管理程序

经过认证可运行 CentOS 或 Red Hat Enterprise Linux 的裸机或托管虚拟机管理程序<https://access.redhat.com/certified-hypervisors>["Red Hat 解决方案：哪些虚拟机管理程序已通过认证，可以运行 Red Hat Enterprise Linux ? "]

## /opt 中的磁盘空间

必须有 100 GiB 的可用空间

## /var 中的磁盘空间

必须有 20 GiB 的可用空间

## 出站 Internet 访问

要安装 Connector，需要进行出站 Internet 访问，而要使 Connector 能够管理公有云环境中的资源和流程，则需要出站 Internet 访问。有关端点列表，请参见 ["连接器的网络连接要求"](#)。

## 安装连接器

确认您拥有受支持的 Linux 主机后，您可以获取 Connector 软件并进行安装。

安装连接器需要 root 权限。

## 关于此任务

- 此安装将安装 AWS 命令行工具（awscli），以便从 NetApp 支持部门执行恢复过程。

如果您收到安装 AWSCLI 失败的消息，则可以安全地忽略该消息。如果没有工具，连接器可以成功运行。

- 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，Connector 会自动进行更新。

## 步骤

1. 从下载 Cloud Manager 软件 ["NetApp 支持站点"](#)，然后将其复制到 Linux 主机。

有关在 AWS 中将文件连接和复制到 EC2 实例的帮助，请参见 ["AWS 文档：使用 SSH 连接到 Linux 实例"](#)。

2. 分配运行脚本的权限。

```
chmod +x OnCommandCloudManager-V3.9.19.sh
```

### 3. 运行安装脚本。

如果您有代理服务器，则需要输入命令参数，如下所示。安装程序不会提示您提供有关代理的信息。

```
./OnCommandCloudManager-V3.9.19.sh [silent] [proxy=ipaddress]  
[proxyport=port] [proxyuser=user_name] [proxypwd=password]
```

*silent* 运行安装时不提示您提供信息。

如果主机位于代理服务器后端，则需要 *proxy*。

*proxyport* 是代理服务器的端口。

*proxyuser* 是代理服务器的用户名，前提是需要进行基本身份验证。

*proxypwd* 是您指定的用户名的密码。

### 4. 除非指定了 *silent* 参数，否则请输入 \*。Y\* 以继续安装。

现已安装 Cloud Manager。在安装结束时、如果指定了代理服务器、则 Cloud Manager Service (OCCM) 会重新启动两次。

### 5. 打开 Web 浏览器并输入以下 URL：

<https://ipaddress/>

*ipaddress* 可以是 localhost，专用 IP 地址或公有 IP 地址，具体取决于主机的配置。例如，如果连接器位于公有云中且没有公有 IP 地址，则必须输入与连接器主机连接的主机的专用 IP 地址。

### 6. 请在 NetApp Cloud Central 上注册或登录。

### 7. 如果您在 Google Cloud 中安装了 Connector，请设置一个服务帐户，该帐户具有 Cloud Manager 在项目中创建和管理 Cloud Volumes ONTAP 系统所需的权限。

- "[在 GCP 中创建角色](#)" 其中包括定义的权限 "[GCP 的连接策略](#)"。
- "[创建 GCP 服务帐户并应用刚刚创建的自定义角色](#)"。
- "[将此服务帐户与 Connector VM 关联](#)"。
- 如果要在其他项目中部署 Cloud Volumes ONTAP，"[通过向该项目添加具有 Cloud Manager 角色的服务帐户来授予访问权限](#)"。您需要对每个项目重复此步骤。

### 8. 登录后，设置 Cloud Manager：

- 指定要与 Connector 关联的 NetApp 帐户。

"[了解 NetApp 客户](#)"。

- 输入系统名称。



现在，您可以使用 NetApp 帐户安装并设置 Connector。Cloud Manager 将在您创建新的工作环境时自动使用此 Connector。

设置权限，以便 Cloud Manager 可以管理公有云环境中的资源和流程：

- AWS "设置 AWS 帐户，然后将其添加到 Cloud Manager"
- Azure 酒店 "设置 Azure 帐户，然后将其添加到 Cloud Manager"
- Google Cloud：请参见上文第 7 步

在不访问 **Internet** 的情况下在内部安装 **Connector**

您可以在无法访问 Internet 的内部 Linux 主机上安装 Connector。然后、您可以发现内部 ONTAP 集群、在它们之间复制数据、使用 Cloud Backup 备份卷、并使用 Cloud Data sense 对其进行扫描。

这些安装说明专门针对上述使用情形。"了解部署 Connector 的其他方法"。

验证主机要求

连接器软件必须在满足特定操作系统要求，RAM 要求，端口要求等要求的主机上运行。

需要一个专用主机

与其他应用程序共享的主机不支持此连接器。主机必须是专用主机。

## CPU

4 个核心或 4 个 vCPU

## RAM

16 GB

支持的操作系统

- CentOS 7.6
- CentOS 7.7
- CentOS 7.8
- CentOS 7.9
- Red Hat Enterprise Linux 7.6
- Red Hat Enterprise Linux 7.7
- Red Hat Enterprise Linux 7.8
- Red Hat Enterprise Linux 7.9

Red Hat Enterprise Linux 系统必须在 Red Hat 订购管理中注册。如果未注册，则在安装 Connector 期间，系统无法访问存储库来更新所需的第三方软件。

这些操作系统的英语版本支持 Connector。

虚拟机管理程序

经过认证可运行 CentOS 或 Red Hat Enterprise Linux 的裸机或托管虚拟机管理程序<https://access.redhat.com/certified-hypervisors>["Red Hat 解决方案：哪些虚拟机管理程序已通过认证，可以运行 Red Hat Enterprise Linux ? "]

## Disk type

SSD 为必填项

**/opt** 中的磁盘空间

必须有 100 GiB 的可用空间

**/var** 中的磁盘空间

必须有 20 GiB 的可用空间

## Docker 引擎

在安装 Connector 之前，主机上需要安装 Docker 引擎版本 19 或更高版本。 ["查看安装说明"](#)。

安装连接器

确认您拥有受支持的 Linux 主机后，您可以获取 Connector 软件并进行安装。

安装连接器需要 root 权限。

## 步骤

1. 验证 Docker 是否已启用且正在运行。

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

2. 从下载 Cloud Manager 软件 "[NetApp 支持站点](#)"。
3. 将安装程序复制到 Linux 主机。
4. 分配运行脚本的权限。

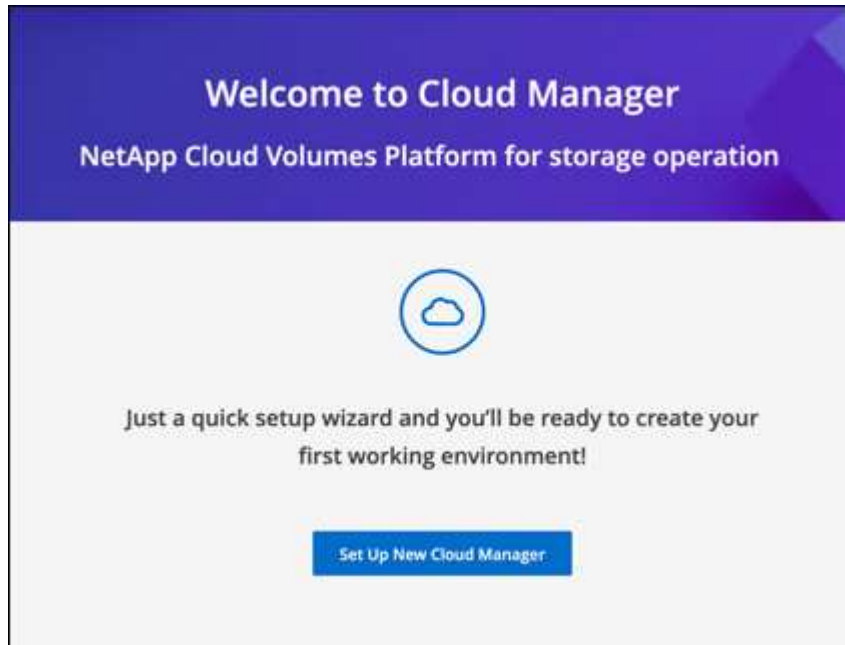
```
chmod +x /path/cloud-manager-connector-offline-v3.9.19
```

5. 运行安装脚本：

```
sudo /path/cloud-manager-connector-offline-v3.9.19
```

6. 打开 Web 浏览器并输入 `https://ipaddress[]` 其中 `ipaddress` 是 Linux 主机的 IP 地址。

您应看到以下屏幕。



7. 单击 \* 设置新的 Cloud Manager\* ，然后按照提示设置系统。
  - \* 系统详细信息 \* ：输入 Cloud Manager 系统的名称和您的公司名称。



- \* 创建管理员用户 \*：为系统创建管理员用户。

此用户帐户在系统本地运行。无法连接到 NetApp Cloud Central。

- \* 审阅 \*：查看详细信息，接受许可协议，然后单击 \* 设置 \*。

8. 使用刚刚创建的管理员用户登录到 Cloud Manager。

现在已安装 Connector，您可以开始使用非公开站点部署中提供的 Cloud Manager 功能。

接下来是什么？

- "发现内部 ONTAP 集群"
- "在内部 ONTAP 集群之间复制数据"
- "使用云备份将内部 ONTAP 卷数据备份到 StorageGRID"
- "使用云数据感知扫描内部 ONTAP 卷数据"

如果有新版本的 Connector 软件可用，则这些软件将发布到 NetApp 支持站点。"[了解如何升级 Connector](#)"。

## 查找连接器的系统 ID

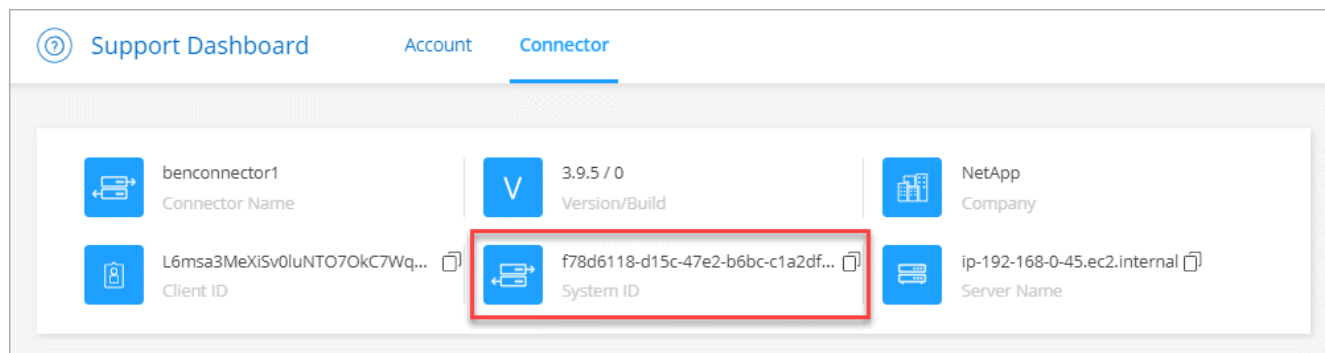
为了帮助您入门，NetApp 代表可能会要求您提供 Connector 的系统 ID。此 ID 通常用于许可和故障排除目的。

### 步骤

1. 在 Cloud Manager 控制台右上角，单击帮助图标。
2. 单击 \* 支持 > 连接器 \*。

系统 ID 显示在顶部。

- 示例 \*



## 管理现有连接器

创建一个或多个连接器后，您可以通过在连接器之间切换，连接到在连接器上运行的本地用户界面等方式来管理这些连接器。

### 在连接器之间切换

如果您有多个连接器，则可以在它们之间切换，以查看与特定连接器关联的工作环境。

例如，假设您正在多云环境中工作。您可能在 AWS 中有一个连接器，在 Google Cloud 中有另一个连接器。您需要在这些连接器之间进行切换，以管理在这些云中运行的 Cloud Volumes ONTAP 系统。

### 步骤

1. 单击 \* 连接器 \* 下拉列表，选择另一个连接器，然后单击 \* 交换机 \*。



Cloud Manager 将刷新并显示与选定 Connector 关联的工作环境。

## 访问本地 UI

虽然您应该从 SaaS 用户界面执行几乎所有任务，但连接器上仍提供本地用户界面。如果您要从无法访问出站Internet的政府区域或站点访问Cloud Manager、则需要使用在Connector上运行的本地用户界面。

### 步骤

1. 打开 Web 浏览器并输入以下 URL：

`https://ipaddress[]`

*ipaddress* 可以是 localhost，专用 IP 地址或公有 IP 地址，具体取决于主机的配置。例如，如果连接器位于公有云中且没有公有 IP 地址，则必须输入与连接器主机连接的主机的专用 IP 地址。

2. 输入您的用户名和密码以登录。

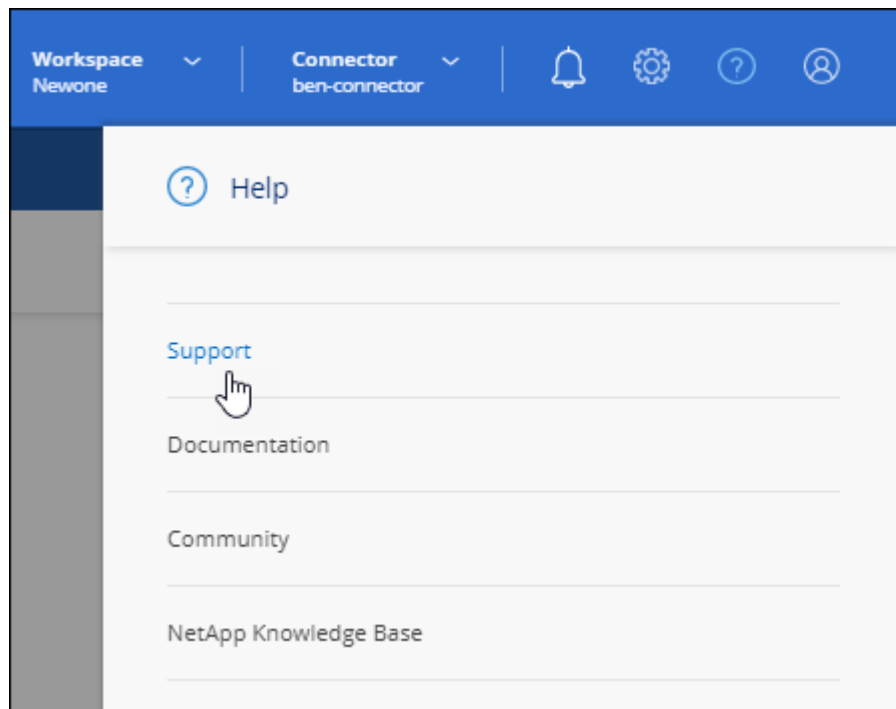
## 下载或发送 **AutoSupport** 消息

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

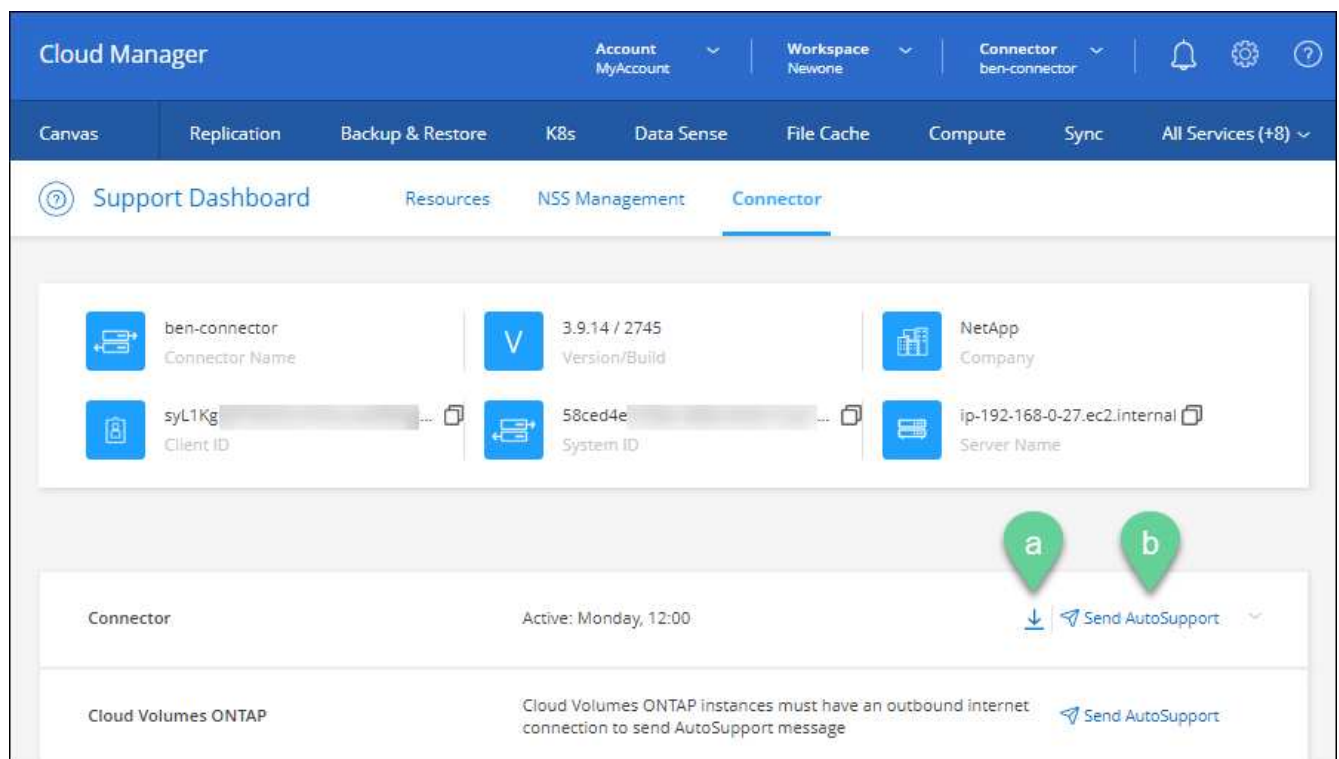
### 步骤

1. 连接到连接器本地 UI，如上一节所述。
2. 在 Cloud Manager 控制台右上角，单击帮助图标，然后选择 \* 支持 \*。





3. 单击 \* 连接器 \*。
4. 根据向 NetApp 支持部门发送信息的方式，选择以下选项之一：
  - a. 选择选项以将 AutoSupport 消息下载到本地计算机。然后，您可以使用首选方法将其发送给 NetApp 支持部门。
  - b. 单击 \* 发送 NetApp\* 以直接将消息发送给 AutoSupport 支持。



## 连接到 Linux VM

如果您需要连接到运行 Connector 的 Linux VM，可以使用云提供商提供的连接选项来执行此操作。

### AWS

在 AWS 中创建 Connector 实例时，您提供了 AWS 访问密钥和机密密钥。您可以使用此密钥对通过 SSH 连接到实例。

["AWS 文档：连接到 Linux 实例"](#)

### Azure 酒店

在 Azure 中创建 Connector VM 时，您选择使用密码或 SSH 公有 密钥进行身份验证。使用您选择的身份验证方法连接到虚拟机。

["Azure 文档：通过 SSH 连接到虚拟机"](#)

### Google Cloud

在 Google Cloud 中创建 Connector 时，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 VM"](#)

## 应用安全更新

在 Connector 上更新操作系统，以确保使用最新的安全更新对其进行修补。

### 步骤

1. 访问 Connector 主机上的命令行界面 Shell。
2. 使用提升的权限运行以下命令：

```
sudo -s
service service-manager stop
yum -y update --security
service service-manager start
```

## 更改连接器的 IP 地址

如果您的业务需要，您可以更改云提供商自动分配的 Connector 实例的内部 IP 地址和公有 IP 地址。

### 步骤

1. 按照云提供商的说明更改连接器实例的本地 IP 地址或公有 IP 地址（或两者）。
2. 如果您更改了公有 IP 地址，并且需要连接到在 Connector 上运行的本地用户界面，请重新启动 Connector 实例以向 Cloud Manager 注册新的 IP 地址。
3. 如果更改了专用 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 Connector 上的新专用 IP 地址。

- a. 从 Cloud Volumes ONTAP 命令行界面运行以下命令以删除当前备份目标：

```
system configuration backup settings modify -destination ""
```

- b. 转到 Cloud Manager 并打开工作环境。
- c. 单击菜单并选择 \* 高级 > 配置备份 \*。
- d. 单击 \* 设置备份目标 \*。

## 编辑 Connector 的 URI

添加并删除 Connector 的 URI。

### 步骤

1. 单击 Cloud Manager 标题中的 \* 连接器 \* 下拉列表。
2. 单击 \* 管理连接器 \*。
3. 单击 Connector 的操作菜单，然后单击 \* 编辑 URIs\*。
4. 添加并删除 URI，然后单击 \* 应用 \*。

## 修复使用 Google Cloud NAT 网关时的下载失败问题

连接器会自动下载 Cloud Volumes ONTAP 的软件更新。如果您的配置使用 Google Cloud NAT 网关，则下载可能会失败。您可以通过限制软件映像划分到的部件数来更正此问题描述。必须使用 Cloud Manager API 完成此步骤。

### 步骤

1. 使用以下 JSON 正文向 /occm/config 提交 PUT 请求：

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

maxDownloadSessions\_ 的值可以是 1 或大于 1 的任意整数。如果值为 1，则下载的映像不会被拆分。

请注意，32 是一个示例值。应使用的值取决于 NAT 配置以及可以同时拥有的会话数。

["了解有关 /ocem/config API 调用的更多信息"](#)。

## 在不访问 Internet 的情况下升级内部连接器

如果您 ["已在无法访问 Internet 的内部主机上安装 Connector"](#)，您可以在 NetApp 支持站点上提供较新版本时升级 Connector。

在升级过程中，Connector 需要重新启动，因此用户界面在升级期间将不可用。

### 步骤

1. 从下载 Cloud Manager 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/cloud-manager-connector-offline-v3.9.14
```

4. 运行安装脚本：

```
sudo /path/cloud-manager-connector-offline-v3.9.14
```

5. 升级完成后，您可以转到 \* 帮助 > 支持 > 连接器 \* 来验证连接器的版本。

### 可以访问 Internet 的主机上的软件升级又如何？

只要有最新版本，Connector 就会自动将其软件更新到最新版本 "[出站 Internet 访问](#)" 以获取软件更新。

## 从 Cloud Manager 中删除 Connectors

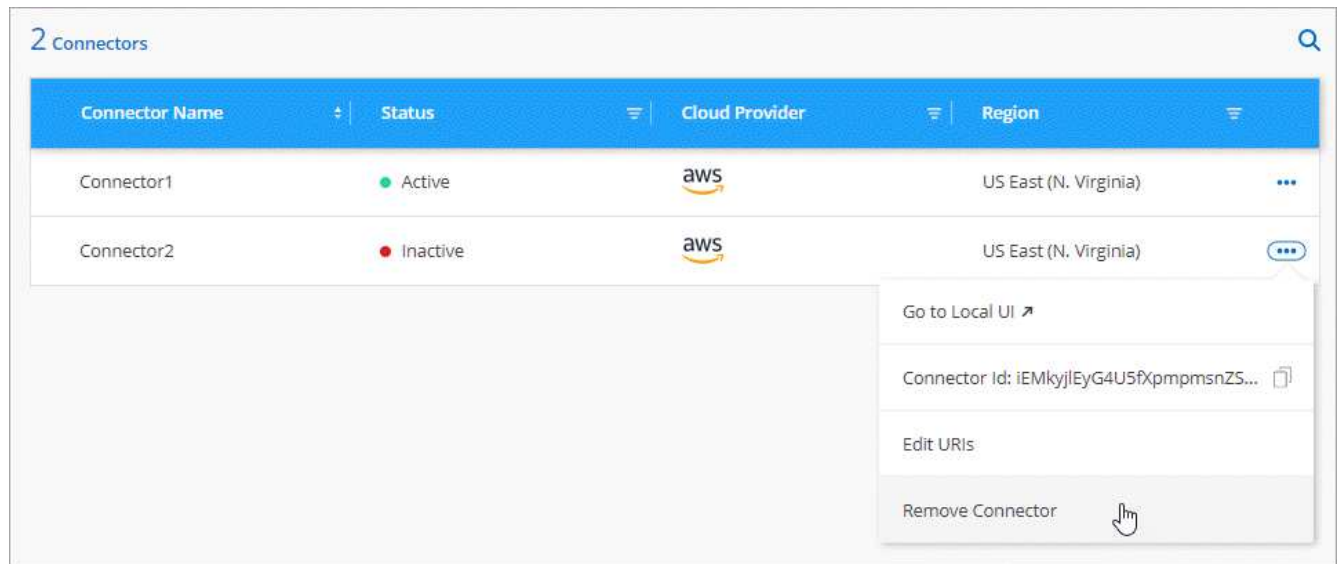
如果某个 Connector 处于非活动状态，您可以将其从 Cloud Manager 中的 Connectors 列表中删除。如果删除了 Connector 虚拟机或卸载了 Connector 软件，则可以执行此操作。

有关删除连接器，请注意以下事项：

- 此操作不会删除虚拟机。
- 无法还原此操作—从 Cloud Manager 中删除 Connector 后，便无法将其重新添加到 Cloud Manager 中。

### 步骤

1. 单击 Cloud Manager 标题中的 \* 连接器 \* 下拉列表。
2. 单击 \* 管理连接器 \*。
3. 单击非活动连接器的操作菜单，然后单击 \* 删除连接器 \*。



4. 输入 Connector 的名称进行确认，然后单击删除。

Cloud Manager 将从其记录中删除 Connector。

### 卸载 **Connector** 软件

卸载 Connector 软件以解决问题或从主机中永久删除此软件。您需要使用的步骤取决于您是将 Connector 安装在可访问 Internet 的主机上，还是安装在无法访问 Internet 的受限网络中的主机上。

#### 从可访问 **Internet** 的主机卸载

联机连接器包含一个卸载脚本，您可以使用此脚本卸载软件。

#### 步骤

1. 在 Linux 主机上运行卸载脚本：
  - `/opt/application/netapp/cloudmanager/bin/uninstall.sh [silent]*`  
*silent* 运行此脚本，而不提示您进行确认。

#### 从无法访问 **Internet** 的主机卸载

如果您从 NetApp 支持站点下载了 Connector 软件并将其安装在无法访问 Internet 的受限网络中，请使用以下命令。

#### 步骤

1. 在 Linux 主机中，运行以下命令：

```
docker-compose -f /opt/application/netapp/ds/docker-compose.yml down -v  
rm -rf /opt/application/netapp/ds
```

管理 HTTPS 证书以实现安全访问

默认情况下， Cloud Manager 使用自签名证书对 Web 控制台进行 HTTPS 访问。您可以安装由证书颁发机构（ CA ）签名的证书、该证书提供比自签名证书更好的安全保护。

开始之前

您需要先创建 Connector ，然后才能更改 Cloud Manager 设置。 ["了解如何操作"](#)。

安装 HTTPS 证书

安装由 CA 签名的证书以确保安全访问。

步骤

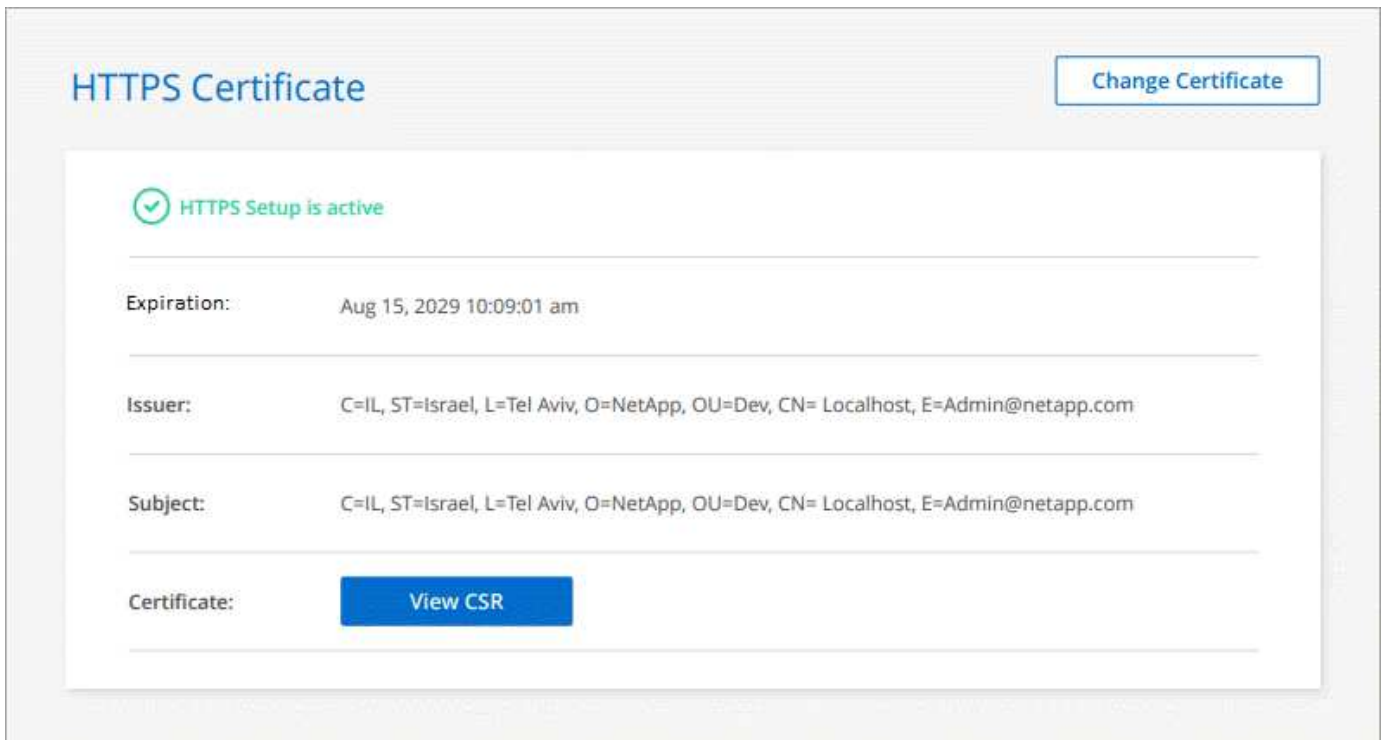
- 1. 在 Cloud Manager 控制台的右上角，单击设置图标，然后选择 \* HTTPS 设置 \* 。



- 2. 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	Description
生成 CSR	<div>a. 输入 Connector 主机的主机名或 DNS （其公用名），然后单击 * 生成 CSR* 。</div> <div>Cloud Manager 将显示证书签名请求。</div> <div>b. 使用 CSR 向 CA 提交 SSL 证书请求。</div> <div>证书必须使用 Privacy Enhanced Mail （ PEM ） Base — 64 编码的 X.509 格式。</div> <div>c. 上传证书文件，然后单击 * 安装 * 。</div>
安装您自己的 CA 签名证书	<div>a. 选择 * 安装 CA 签名证书 * 。</div> <div>b. 加载证书文件和私钥，然后单击 * 安装 * 。</div> <div>证书必须使用 Privacy Enhanced Mail （ PEM ） Base — 64 编码的 X.509 格式。</div>

Cloud Manager 现在使用 CA 签名的证书提供安全 HTTPS 访问。下图显示了为安全访问配置的 Cloud Manager 系统：



## 续订 Cloud Manager HTTPS 证书

您应该在云管理器 HTTPS 证书过期之前续订该证书，以确保对云管理器 Web 控制台的安全访问。如果在证书过期前未续订证书、则当用户使用 HTTPS 访问 Web 控制台时会显示警告。

### 步骤

1. 在 Cloud Manager 控制台的右上角，单击设置图标，然后选择 \* HTTPS 设置 \*。

此时将显示有关 Cloud Manager 证书的详细信息、包括到期日期。

2. 单击 \* 更改证书 \*，然后按照以下步骤生成 CSR 或安装您自己的 CA 签名证书。

Cloud Manager 使用新的 CA 签名证书提供安全 HTTPS 访问。

## 配置 Connector 以使用 HTTP 代理服务器

如果您的公司策略要求您使用代理服务器与 Internet 进行所有 HTTP 通信，则必须将您的连接器配置为使用该 HTTP 代理服务器。代理服务器可以位于云中或网络中。

Cloud Manager 不支持在 Connector 中使用 HTTPS 代理。

### 在 Connector 上启用代理

在将 Connector 配置为使用代理服务器时，该连接器及其管理的 Cloud Volumes ONTAP 系统（包括任何 HA 调解器）都会使用代理服务器。

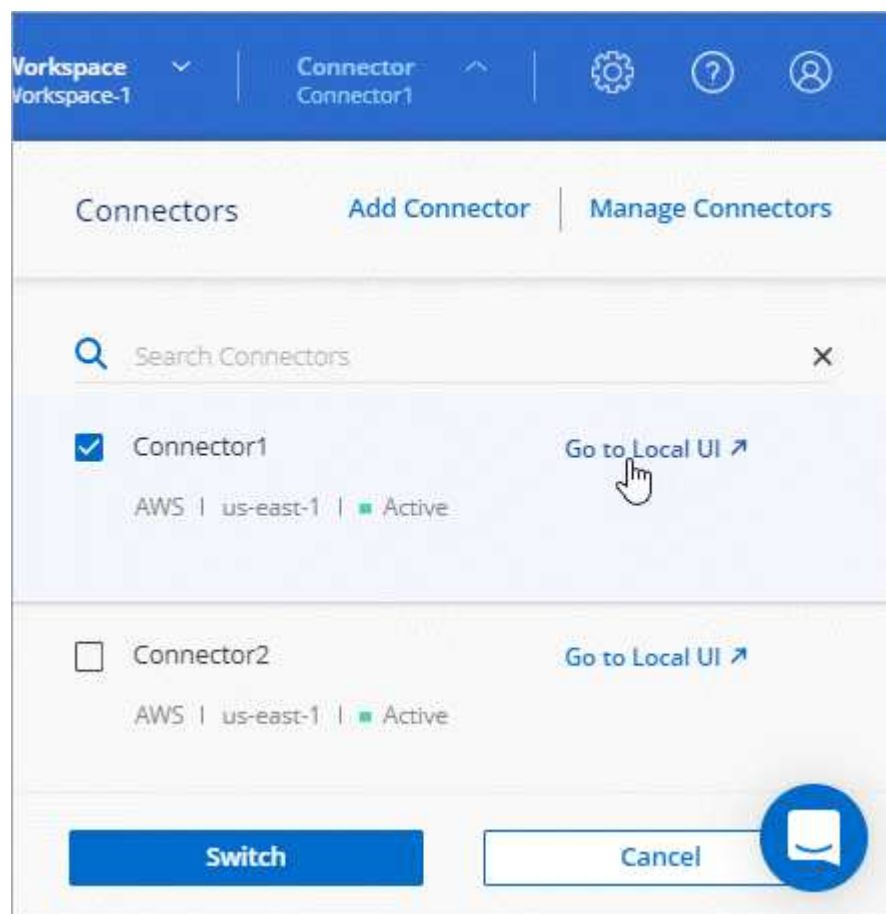
请注意，此操作将重新启动 Connector。继续操作前，请确保 Connector 未执行任何操作。

### 步骤

1. "登录到 Cloud Manager SaaS 界面" 从已通过网络连接到 Connector 实例的计算机。

如果此连接器没有公有 IP 地址，您需要 VPN 连接，或者您需要从与此连接器位于同一网络的跳转主机进行连接。

2. 单击 \* 连接器 \* 下拉列表，然后单击 \* 转到特定连接器的本地 UID\* 。



在 Connector 上运行的 Cloud Manager 界面将加载到新的浏览器选项卡中。

3. 在 Cloud Manager 控制台的右上角，单击设置图标，然后选择 \* 连接器设置 \* 。



4. 在 \* 常规 \* 下，单击 \* HTTP 代理配置 \* 。
5. 设置代理：
  - a. 单击 \* 启用代理 \* 。
  - b. 使用语法指定服务器 `http://address:port[]`
  - c. 如果服务器需要基本身份验证，请指定用户名和密码
  - d. 单击 \* 保存 \* 。





Cloud Manager 不支持包含 @ 字符的密码。

指定代理服务器后、新的 Cloud Volumes ONTAP 系统会自动配置为在发送 AutoSupport 消息时使用代理服务器。如果在用户创建 Cloud Volumes ONTAP 系统之前未指定代理服务器，则用户必须使用 System Manager 在每个系统的 AutoSupport 选项中手动设置代理服务器。

## 启用直接 API 流量

如果您配置了代理服务器，则无需通过代理即可将 API 调用直接发送到 Cloud Manager。在 AWS，Azure 或 Google Cloud 中运行的 Connectors 支持此选项。

### 步骤

1. 在 Cloud Manager 控制台的右上角，单击设置图标，然后选择 \* 连接器设置 \*。



2. 在 \* 常规 \* 下，单击 \* 支持直接 API 流量 \*。
3. 单击复选框以启用此选项，然后单击 \* 保存 \*。

## Connector 的默认配置

您可能希望在部署连接器之前或需要对任何问题进行故障排除时了解有关连接器的更多信息。

### 具有 Internet 访问权限的默认配置

如果您从 Cloud Manager、云提供商的市场部署了 Connector、或者在可访问 Internet 的内部 Linux 主机上手动安装了 Connector、则以下配置详细信息适用。

#### AWS 详细信息

如果您从 Cloud Manager 或云提供商的市场部署了 Connector、请注意以下事项：

- EC2 实例类型为 T3.xlarge。
- 此映像的操作系统为 Red Hat Enterprise Linux 7.6 (HVM)。

操作系统不包含 GUI。您必须使用终端访问系统。

- EC2 Linux 实例的用户名为 EC2-user。
- 默认系统磁盘为 50 GiB GP2 磁盘。

#### Azure 详细信息

如果您从 Cloud Manager 或云提供商的市场部署了 Connector、请注意以下事项：

- VM 类型为 DS3 v2。

- 映像的操作系统为CentOS 7.6。

操作系统不包含 GUI 。您必须使用终端访问系统。

- 默认系统磁盘为100 GiB高级SSD磁盘。

#### Google Cloud详细信息

如果您从Cloud Manager或云提供商的市场部署了Connector、请注意以下事项：

- VM实例为n1-standard-4。
- 映像的操作系统为CentOS 7.9。

操作系统不包含 GUI 。您必须使用终端访问系统。

- 默认系统磁盘为100 GiB SSD永久性磁盘。

#### 安装文件夹

Connector 安装文件夹位于以下位置：

/opt/application/netapp/cloudmanager

#### 日志文件

日志文件包含在以下文件夹中：

- /opt/application/netapp/cloudmanager/log

此文件夹中的日志提供了有关连接器和 Docker 映像的详细信息。

- /opt/application/netapp/cloudmanager/docker\_occm/data/log

此文件夹中的日志提供了有关云服务以及在 Connector 上运行的 Cloud Manager 服务的详细信息。

#### 连接器服务

- 云管理器服务的名称是 OCCM 。
- OCUM 服务依赖于 MySQL 服务。

如果 MySQL 服务已关闭，则 OCCM 服务也将关闭。

#### 软件包

如果尚未安装下列软件包，则 Cloud Manager 会在 Linux 主机上安装这些软件包：

- 7 邮政编码
- AWSCLI
- Docker
- Java

- Kubectl
- MySQL
- Tridentctl
- 拉拔
- wget

端口

Connector 在 Linux 主机上使用以下端口：

- 80 用于 HTTP 访问
- 443 用于 HTTPS 访问
- 3306 表示云管理器数据库
- 8080 用于云管理器 API 代理
- 8666 用于 Service Manager API
- 8777 ，用于运行状况检查程序容器服务 API

无 **Internet** 访问的默认配置

如果您在无法访问 Internet 的内部 Linux 主机上手动安装了 Connector ，则以下配置适用。 ["了解有关此安装选项的更多信息"](#)。

- Connector 安装文件夹位于以下位置：

`/opt/application/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了有关连接器和 Docker 映像的详细信息。

- 所有服务均在 Docker 容器中运行

这些服务取决于运行的 Docker 运行时服务

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

## AWS 凭据

### AWS 凭据和权限

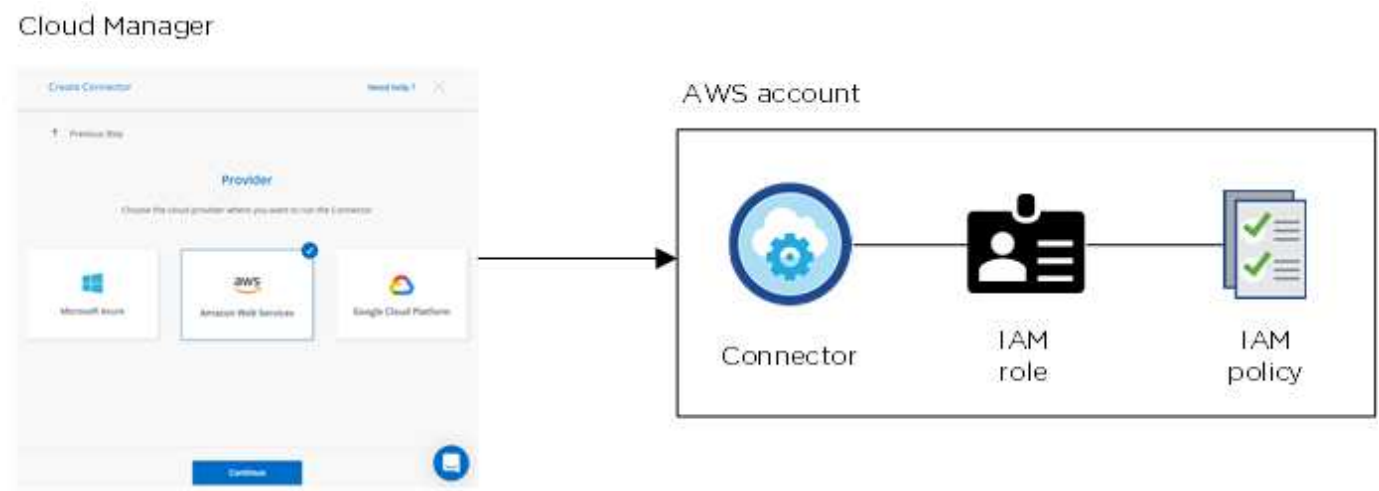
通过 Cloud Manager ，您可以选择部署 Cloud Volumes ONTAP 时要使用的 AWS 凭据。您可以使用初始 AWS 凭据部署所有 Cloud Volumes ONTAP 系统，也可以添加其他凭

据。

初始 **AWS** 凭据

从 Cloud Manager 部署 Connector 时，您需要为 IAM 用户提供 IAM 角色的 ARN 或访问密钥。您使用的身份验证方法必须具有在 AWS 中部署 Connector 实例所需的权限。中列出了所需的权限 ["AWS 的连接部署策略"](#)。

当 Cloud Manager 在 AWS 中启动 Connector 实例时，它会为此实例创建 IAM 角色和实例配置文件。此外，它还会附加一个策略，为 Connector 提供管理该 AWS 帐户中资源和进程的权限。 ["查看 Cloud Manager 如何使用权限"](#)。



在为 Cloud Volumes ONTAP 创建新工作环境时， Cloud Manager 会默认选择以下 AWS 凭据：

Details & Credentials			
Instance Profile		QA Subscription	<a href="#">Edit Credentials</a>
Credentials	Account ID	Marketplace Subscription	

其他 **AWS** 凭据

可以通过两种方式添加其他 AWS 凭据。

将 **AWS** 凭据添加到现有 **Connector**

如果您要在不同的 AWS 帐户中启动 Cloud Volumes ONTAP ，则可以选择一种 ["为 IAM 用户或受信任帐户中某个角色的 ARN 提供 AWS 密钥"](#)。下图显示了另外两个帐户，一个通过可信帐户中的 IAM 角色提供权限，另一个通过 IAM 用户的 AWS 密钥提供权限：



您可以这样做 "将帐户凭据添加到 [Cloud Manager](#)" 指定 IAM 角色的 Amazon 资源名称（ARN）或 IAM 用户的 AWS 密钥。

添加另一组凭据后，您可以在创建新的工作环境时切换到这些凭据：

**Edit Credentials & Add Subscription**

Associate Subscription to Credentials ⓘ

Credentials

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

+ Add Subscription

Apply Cancel

将 **AWS** 凭据直接添加到 **Cloud Manager**

向 Cloud Manager 添加新的 AWS 凭据可为 Cloud Manager 提供创建和管理适用于 ONTAP 的 FSX 工作环境或创建 Connector 所需的权限。

市场部署和内部部署如何？

以上各节介绍了 Cloud Manager 中建议的 Connector 部署方法。您也可以从在 AWS 中部署连接器 "[AWS Marketplace](#)" 您可以做到 "[在内部安装 Connector](#)"。

如果您使用 Marketplace，则会以相同方式提供权限。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即可。

对于内部部署，您不能为 Cloud Manager 系统设置 IAM 角色，但可以像为其他 AWS 帐户提供权限一样提供权限。

## 如何安全地轮换 **AWS** 凭据？

如上所述，Cloud Manager 支持您通过以下几种方式提供 AWS 凭据：与 Connector 实例关联的 IAM 角色，在可信帐户中承担 IAM 角色或提供 AWS 访问密钥。

对于前两个选项，Cloud Manager 使用 AWS 安全令牌服务获取持续轮换的临时凭据。这是最佳实践——它是自动的，安全的。

如果您为 Cloud Manager 提供了 AWS 访问密钥，则应定期在 Cloud Manager 中更新这些密钥以轮换使用。这是一个完全手动过程。

## 管理 **Cloud Manager** 的 **AWS** 凭据和订阅

添加和管理 AWS 凭据，以便 Cloud Manager 拥有在 AWS 帐户中部署和管理云资源所需的权限。如果您管理多个 AWS 订阅，则可以从凭据页面将其中每个订阅分配给不同的 AWS 凭据。

### 概述

您可以将 AWS 凭据添加到现有 Connector 或直接添加到 Cloud Manager：

- 向现有 Connector 添加其他 AWS 凭据

通过向现有连接器添加新的 AWS 凭据，您可以使用同一连接器在另一个 AWS 帐户中部署 Cloud Volumes ONTAP。[了解如何将 AWS 凭据添加到 Connector。](#)

- 将 AWS 凭据添加到 Cloud Manager 以创建 Connector

向 Cloud Manager 添加新的 AWS 凭据可为 Cloud Manager 提供创建 Connector 所需的权限。[了解如何向 Cloud Manager 添加 AWS 凭据。](#)

- 将 AWS 凭据添加到 Cloud Manager for FSX for ONTAP

向 Cloud Manager 添加新的 AWS 凭据可为 Cloud Manager 提供创建和管理适用于 ONTAP 的 FSX 所需的权限。["了解如何为适用于 ONTAP 的 FSX 设置权限"](#)

### 如何轮换凭据

您可以通过 Cloud Manager 通过以下几种方式提供 AWS 凭据：与 Connector 实例关联的 IAM 角色，在可信帐户中担任 IAM 角色或提供 AWS 访问密钥。["详细了解 AWS 凭据和权限"](#)。

对于前两个选项，Cloud Manager 使用 AWS 安全令牌服务获取持续轮换的临时凭据。此过程是最佳实践，因为它是自动的，并且安全。

如果您为 Cloud Manager 提供了 AWS 访问密钥，则应定期在 Cloud Manager 中更新这些密钥以轮换使用。这是一个完全手动过程。

### 向 **Connector** 添加其他凭据

将 AWS 凭据添加到 Connector，以便它可以在其他 AWS 帐户中部署和管理 Cloud Volumes ONTAP。您可以在其他帐户中提供 IAM 角色的 ARN，也可以提供 AWS 访问密钥。

## 授予权限

在将其他 AWS 凭据添加到 Connector 之前，您需要提供所需的权限。通过这些权限，Cloud Manager 可以管理该 AWS 帐户中的资源和进程。如何提供权限取决于您是要为 Cloud Manager 提供受信任帐户或 AWS 密钥中某个角色的 ARN。



从 Cloud Manager 部署 Connector 时，Cloud Manager 会自动为部署此 Connector 的帐户添加 AWS 凭据。如果您在现有系统上手动安装了 Connector 软件，则不会添加此初始帐户。["了解 AWS 凭据和权限"](#)。

- 选项 \*
- [\[Grant permissions by assuming an IAM role in another account\]](#)
- [\[Grant permissions by providing AWS keys\]](#)

在另一个帐户中担任 **IAM** 角色以授予权限

您可以使用 IAM 角色在部署 Connector 实例的源 AWS 帐户与其他 AWS 帐户之间设置信任关系。然后，您可以为 Cloud Manager 提供可信帐户中 IAM 角色的 ARN。

### 步骤

1. 转到要部署 Cloud Volumes ONTAP 的目标帐户中的 IAM 控制台。
2. 在访问管理下，单击 \* 角色 > 创建角色 \*，然后按照步骤创建角色。

请务必执行以下操作：

- 在 \* 可信实体类型 \* 下，选择 \* AWS 帐户 \*。
  - 选择 \* 其他 AWS 帐户 \*，然后输入 Connector 实例所在帐户的 ID。
  - 通过复制和粘贴内容来创建策略 "[Connector的IAM策略](#)"。
3. 复制 IAM 角色的角色 ARN，以便稍后将其粘贴到 Cloud Manager 中。

现在，此帐户具有所需权限。 [现在，您可以将凭据添加到 Connector。](#)

### 通过提供 **AWS** 密钥授予权限

如果要为 IAM 用户提供 Cloud Manager 的 AWS 密钥，则需要向该用户授予所需的权限。Cloud Manager IAM 策略定义了允许云管理器使用的 AWS 操作和资源。

### 步骤

1. 在 IAM 控制台中，通过复制和粘贴内容来创建策略 "[Connector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"](#)

现在，此帐户具有所需权限。 [现在，您可以将凭据添加到 Connector。](#)

## 添加凭据

在为 AWS 帐户提供所需权限后，您可以将该帐户的凭据添加到现有 Connector。这样，您就可以使用同一个连接器在该帐户中启动 Cloud Volumes ONTAP 系统了。

如果您刚刚在云提供商中创建了这些凭据，则可能需要几分钟的时间才能使用这些凭据。请等待几分钟，然后再将凭据添加到 Cloud Manager。

### 步骤

1. 确保当前已在 Cloud Manager 中选择正确的 Connector。
2. 在 Cloud Manager 控制台的右上角，单击设置图标，然后选择 \* 凭据 \*。



3. 单击 \* 添加凭据 \*，然后按照向导中的步骤进行操作。
  - a. \* 凭据位置 \*：选择 \* Amazon Web Services > Connector\*。
  - b. \* 定义凭据 \*：提供可信 IAM 角色的 ARN（Amazon 资源名称），或者输入 AWS 访问密钥和机密密钥。
  - 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据相关联。

要按每小时费率（PAYGO）或按年度合同支付 Cloud Volumes ONTAP 费用，AWS 凭据必须与 AWS Marketplace 中的 Cloud Volumes ONTAP 订阅相关联。

- d. \* 查看 \*：确认有关新凭据的详细信息，然后单击 \* 添加 \*。

现在，在创建新的工作环境时，您可以从 " 详细信息和凭据 " 页面切换到另一组凭据：



**Edit Credentials & Add Subscription**

---

Associate Subscription to Credentials ⓘ

Credentials

keys   Account ID:
Instance Profile   Account ID:

casaba QA subscription

+ Add Subscription

Apply Cancel

向**Cloud Manager**添加用于创建**Connector**的凭据

通过提供IAM角色的ARN为Cloud Manager提供创建Connector所需的权限、将AWS凭据添加到Cloud Manager。您可以在创建新的Connector时选择这些凭据。

设置 **IAM** 角色

设置一个 IAM 角色，使 Cloud Manager SaaS 能够承担此角色。

步骤

1. 转到目标帐户中的 IAM 控制台。
2. 在访问管理下，单击 \* 角色 > 创建角色 \*，然后按照步骤创建角色。

请务必执行以下操作：

- 在 \* 可信实体类型 \* 下，选择 \* AWS 帐户 \*。
- 选择 \* 其他 AWS 帐户 \* 并输入 Cloud Manager SaaS 的 ID：952013314444
- 创建包含创建Connector所需权限的策略。
  - "查看适用于 ONTAP 的 FSX 所需的权限"
  - "查看连接器部署策略"

3. 复制 IAM 角色的角色 ARN，以便您可以在下一步将其粘贴到 Cloud Manager 中。

IAM 角色现在具有所需的权限。现在，您可以将其添加到 [Cloud Manager](#) 中。

## 添加凭据

为 IAM 角色提供所需权限后，将角色 ARN 添加到 Cloud Manager 中。

如果您刚刚创建了 IAM 角色，则可能需要几分钟的时间，直到这些角色可用为止。请等待几分钟，然后再将凭据添加到 Cloud Manager。

### 步骤

1. 在 Cloud Manager 控制台的右上角，单击设置图标，然后选择 \* 凭据 \*。



2. 单击 \* 添加凭据 \*，然后按照向导中的步骤进行操作。
  - a. \* 凭据位置 \*：选择 \* Amazon Web Services > Cloud Manager\*。
  - b. \* 定义凭据 \*：提供 IAM 角色的 ARN（Amazon 资源名称）。
  - c. \* 查看 \*：确认有关新凭据的详细信息，然后单击 \* 添加 \*。

现在、您可以在创建新Connector时使用这些凭据。

## 关联 AWS 订阅

将 AWS 凭据添加到 Cloud Manager 后，您可以将 AWS Marketplace 订阅与这些凭据相关联。通过订阅，您可以按每小时费率（PAYGO）或使用年度合同为 Cloud Volumes ONTAP 付费，并使用其他 NetApp 云服务。

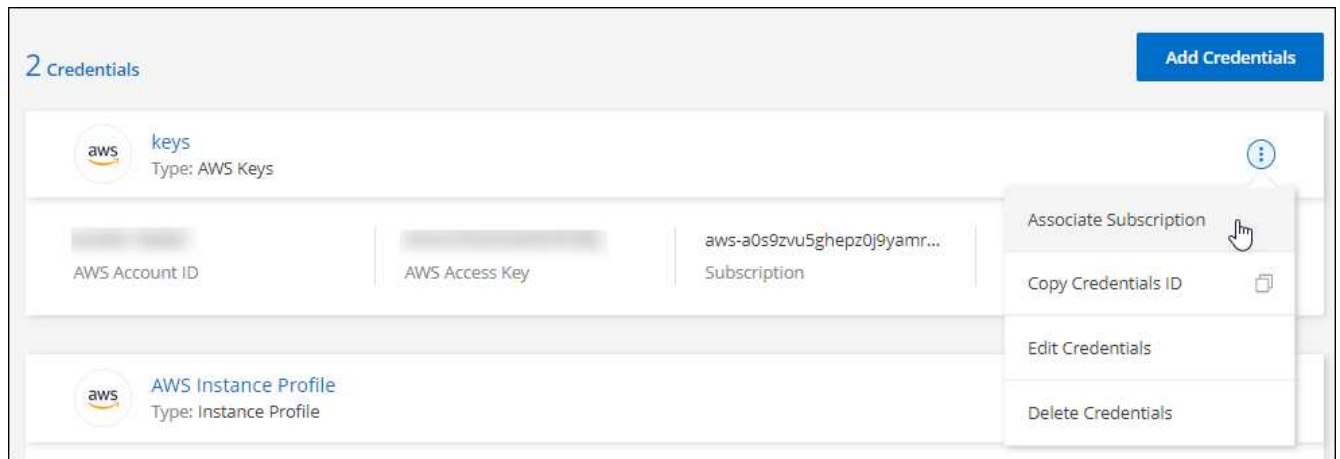
在以下两种情况下，您可能会在将凭据添加到 Cloud Manager 后关联 AWS Marketplace 订阅：

- 最初将凭据添加到 Cloud Manager 时，您未关联订阅。
- 您希望将现有 AWS Marketplace 订阅替换为新订阅。

您需要先创建 Connector，然后才能更改 Cloud Manager 设置。 ["了解如何创建 Connector"](#)。

### 步骤

1. 在 Cloud Manager 控制台的右上角，单击设置图标，然后选择 \* 凭据 \*。
2. 单击一组凭据的操作菜单，然后选择 \* 关联订阅 \*。



3. 从下拉列表中选择现有订阅或单击 \* 添加订阅 \*，然后按照步骤创建新订阅。

► [https://docs.netapp.com/zh-cn/cloud-manager-setup-admin//media/video\\_subscribing\\_aws.mp4](https://docs.netapp.com/zh-cn/cloud-manager-setup-admin//media/video_subscribing_aws.mp4) (video)

## 编辑凭据

通过更改帐户类型（AWS 密钥或承担角色），编辑名称或更新凭据本身（密钥或角色 ARN），在 Cloud Manager 中编辑 AWS 凭据。



您不能编辑与 Connector 实例关联的实例配置文件的凭据。

## 步骤

1. 在 Cloud Manager 控制台的右上角，单击设置图标，然后选择 \* 凭据 \*。
2. 单击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，然后单击 \* 应用 \*。

## 正在删除凭据

如果您不再需要一组凭据，可以从 Cloud Manager 中删除这些凭据。您只能删除与工作环境无关的凭据。



您不能删除与 Connector 实例关联的实例配置文件的凭据。

## 步骤

1. 在 Cloud Manager 控制台的右上角，单击设置图标，然后选择 \* 凭据 \*。
2. 单击一组凭据的操作菜单，然后选择 \* 删除凭据 \*。
3. 单击 \* 删除 \* 进行确认。

# Azure credentials

## Azure 凭据和权限

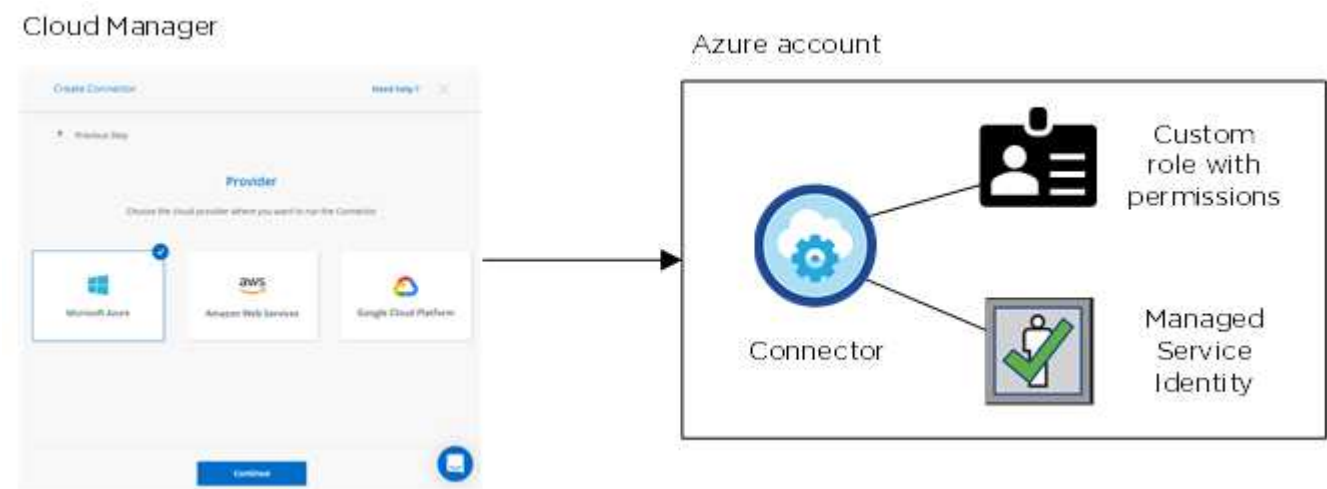
通过 Cloud Manager，您可以选择部署 Cloud Volumes ONTAP 时要使用的 Azure 凭据。您可以使用初始 Azure 凭据部署所有 Cloud Volumes ONTAP 系统，也可以添加其他凭

据。

初始 **Azure** 凭据

从 Cloud Manager 部署 Connector 时，您需要使用有权部署 Connector 虚拟机的 Azure 帐户或服务主体。中列出了所需的权限 ["适用于 Azure 的连接部署策略"](#)。

当 Cloud Manager 在 Azure 中部署 Connector 虚拟机时，它会启用 ["系统分配的受管身份"](#) 在虚拟机上，创建自定义角色并将其分配给虚拟机。此角色为 Cloud Manager 提供了管理该 Azure 订阅中的资源和流程的权限。" [查看 Cloud Manager 如何使用权限](#)"。



在为 Cloud Volumes ONTAP 创建新工作环境时，Cloud Manager 会默认选择以下 Azure 凭据：

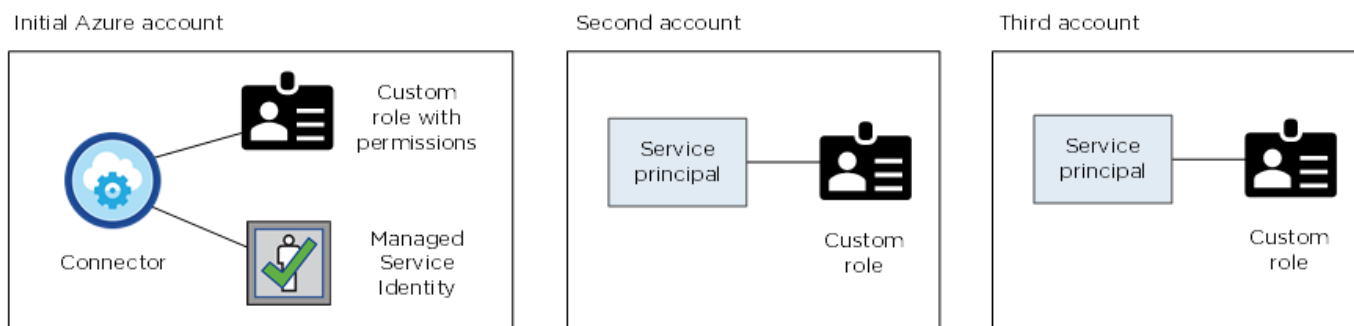
Details & Credentials			
Managed Service Ide...	OCCM QA1	<span>ⓘ</span> No subscription is associated	<a href="#">Edit Credentials</a>
Credential Name	Azure Subscription	Marketplace Subscription	

为受管身份订阅其他 **Azure**

托管身份与启动 Connector 的订阅相关联。如果要选择其他 Azure 订阅，则需要 ["将托管身份与这些订阅相关联"](#)。

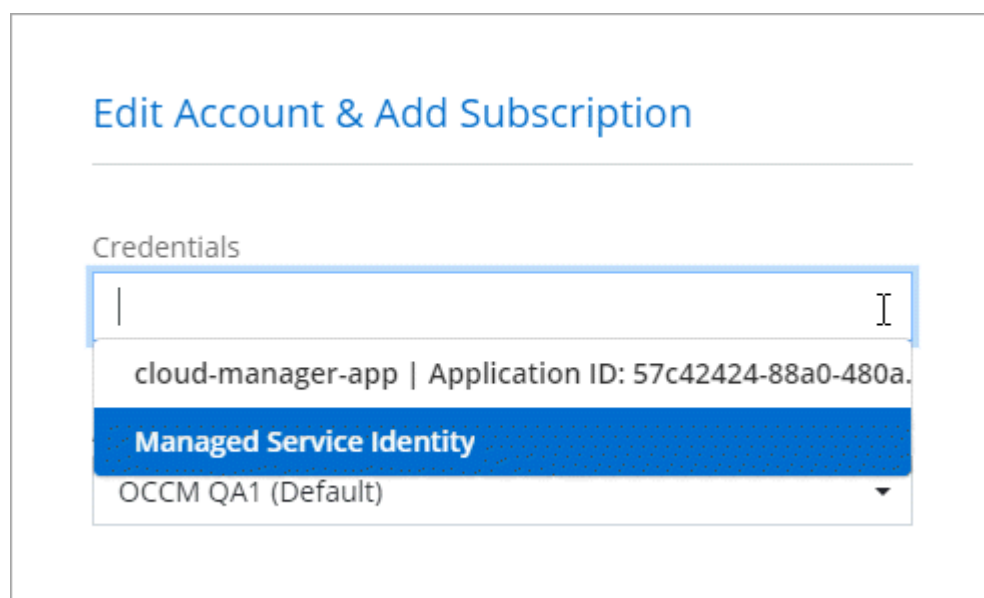
其他 **Azure** 凭据

如果要使用不同的 Azure 凭据部署 Cloud Volumes ONTAP，则必须通过授予所需权限 ["在 Azure Active Directory 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，每个帐户都设置有一个服务主体和一个提供权限的自定义角色：



您可以这样做 "将帐户凭据添加到 Cloud Manager" 提供有关 AD 服务主体的详细信息。

添加另一组凭据后，您可以在创建新的工作环境时切换到这些凭据：



### 市场部署和内部部署如何？

以上各节介绍了从 NetApp Cloud Central 为 Connector 推荐的部署方法。您也可以从在 Azure 中部署 Connector "Azure Marketplace"，您可以 "在内部安装 Connector"。

如果您使用 Marketplace，则会以相同方式提供权限。您只需手动创建并设置 Connector 的托管身份，然后为任何其他帐户提供权限即可。

对于内部部署，您不能为 Connector 设置托管身份，但可以像使用服务主体为其他帐户提供权限一样提供权限。

### 管理 Cloud Manager 的 Azure 凭据和订阅

创建 Cloud Volumes ONTAP 系统时，您需要选择要用于该系统的 Azure 凭据。如果您使用的是按需购买许可，则还需要选择 Marketplace 订阅。如果您需要使用多个 Azure 凭据或多个适用于 Cloud Volumes ONTAP 的 Azure Marketplace 订阅，请按照此页面上的步骤进行操作。

可以通过两种方式在 Cloud Manager 中添加其他 Azure 订阅和凭据。

1. 将其他 Azure 订阅与 Azure 托管身份关联。
2. 如果要使用不同的 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 Cloud Manager。

### 将其他 **Azure** 订阅与受管身份关联

通过 Cloud Manager，您可以选择要在其中部署 Cloud Volumes ONTAP 的 Azure 凭据和 Azure 订阅。除非关联，否则您无法为托管身份配置文件选择其他 Azure 订阅 **"托管身份"** 这些订阅。

托管身份为 **"初始 Azure 帐户"** 从 Cloud Manager 部署 Connector 时。部署 Connector 时，Cloud Manager 会创建 Cloud Manager 操作员角色并将其分配给 Connector 虚拟机。

### 步骤

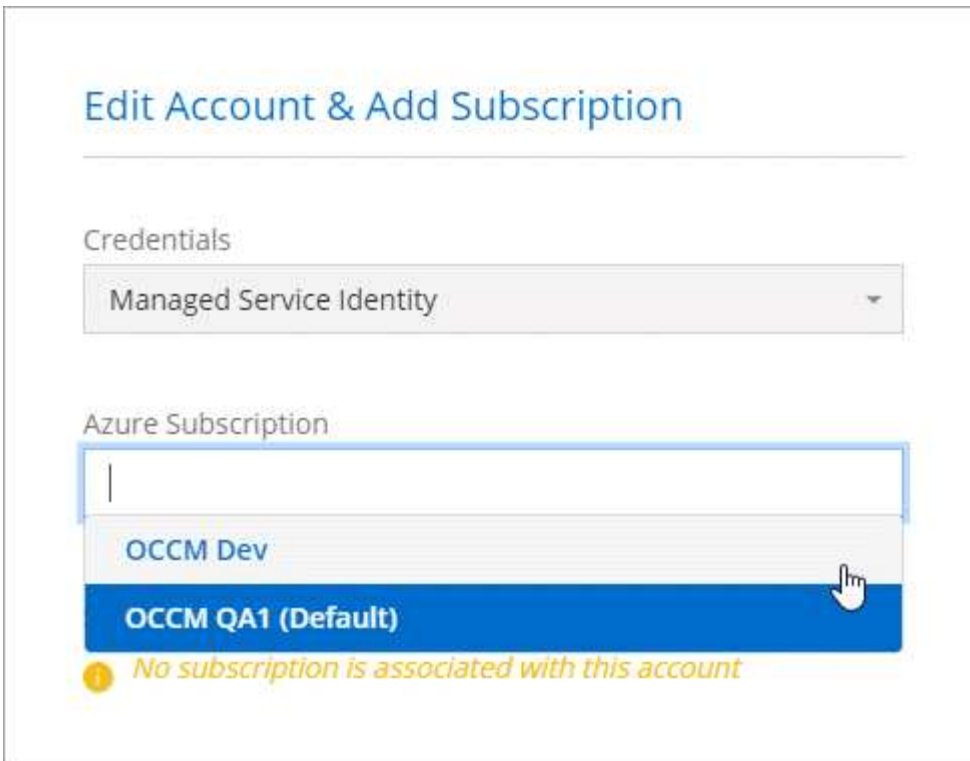
1. 登录 Azure 门户。
2. 打开 \* 订阅 \* 服务，然后选择要部署 Cloud Volumes ONTAP 的订阅。
3. 单击 \* 访问控制 (IAM) \*。
  - a. 单击 \* 添加 \* > \* 添加角色分配 \*，然后添加权限：
    - 选择 \* Cloud Manager Operator\* 角色。



Cloud Manager Operator是Connector策略中提供的默认名称。如果您为角色选择了其他名称，请选择该名称。

- 分配对 \* 虚拟机 \* 的访问权限。
  - 选择创建 Connector 虚拟机的订阅。
  - 选择 Connector 虚拟机。
  - 单击 \* 保存 \*。
4. 对其他订阅重复这些步骤。

创建新的工作环境时，您现在应该能够为托管身份配置文件从多个 Azure 订阅中进行选择。



**Edit Account & Add Subscription**

Credentials

Managed Service Identity

Azure Subscription

OCCM Dev

OCCM QA1 (Default)

*No subscription is associated with this account*

### 向 **Cloud Manager** 添加其他 **Azure** 凭据

从 Cloud Manager 部署 Connector 时，Cloud Manager 会在具有所需权限的虚拟机上启用系统分配的托管身份。在为 Cloud Volumes ONTAP 创建新工作环境时，Cloud Manager 会默认选择以下 Azure 凭据：



如果在现有系统上手动安装 Connector 软件，则不会添加一组初始凭据。"[了解 Azure 凭据和权限](#)"。

如果您要使用 *Different* Azure 凭据部署 Cloud Volumes ONTAP，则必须通过在 Azure Active Directory 中为每个 Azure 帐户创建和设置服务主体来授予所需权限。然后，您可以将新凭据添加到 Cloud Manager。

#### 使用服务主体授予 **Azure** 权限

Cloud Manager 需要权限才能在 Azure 中执行操作。您可以通过在 Azure Active Directory 中创建和设置服务主体以及获取 Cloud Manager 所需的 Azure 凭据来为 Azure 帐户授予所需权限。

下图描述了 Cloud Manager 如何获得在 Azure 中执行操作的权限。与一个或多个 Azure 订阅绑定的服务主体对象表示 Azure Active Directory 中的 Cloud Manager 并分配给允许所需权限的自定义角色。



#### 步骤

1. 创建 [Azure Active Directory 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. 创建客户端密钥。

#### 创建 **Azure Active Directory** 应用程序

创建一个 Azure Active Directory （AD）应用程序和服务主体，Cloud Manager 可使用该应用程序和服务主体进行基于角色的访问控制。

要创建 Active Directory 应用程序并将此应用程序分配给角色，您必须在 Azure 中拥有适当的权限。有关详细信息，请参见 "[Microsoft Azure 文档：所需权限](#)"。

#### 步骤

1. 从 Azure 门户中，打开 \* Azure Active Directory\* 服务。





2. 在菜单中，单击 \* 应用程序注册 \*。
3. 单击 \* 新建注册 \*。
4. 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（任何将适用于 Cloud Manager）。
  - \* 重定向 URI\*：可以将此字段留空。
5. 单击 \* 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 OnCommand 订阅，并为其分配自定义 "Cloud Manager 操作员" 角色，以便 管理器在 Azure 中具有权限。

#### 步骤

1. 创建自定义角色：
  - a. 复制的内容 "[Connector的自定义角色权限](#)" 并将其保存在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。

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

#### ▪ 示例 \*

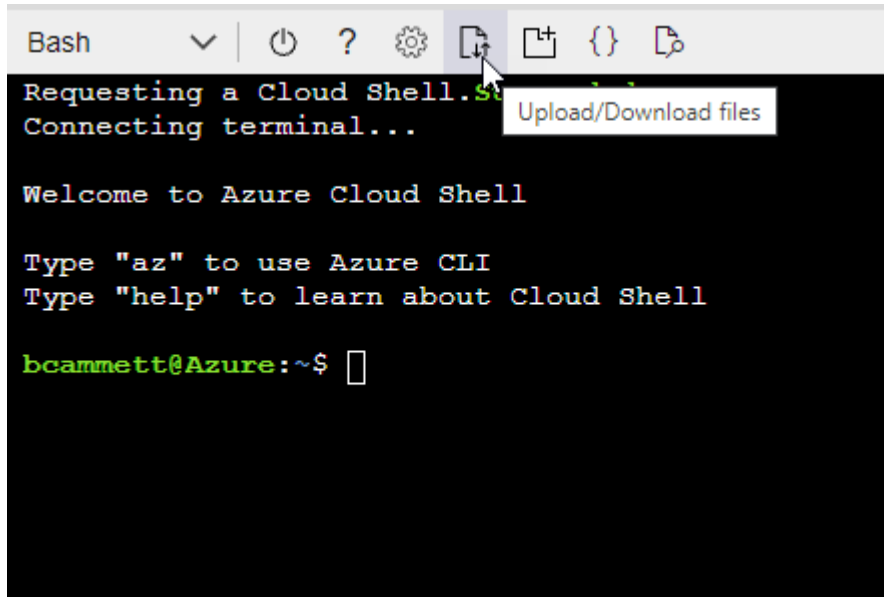
```
"AssignableScopes": [  
  "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",  
  "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",  
  "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
```

- c. 使用 JSON 文件在 Azure 中创建自定义角色。

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

- start "[Azure Cloud Shell](#)" 并选择 Bash 环境。

- 上传 JSON 文件。



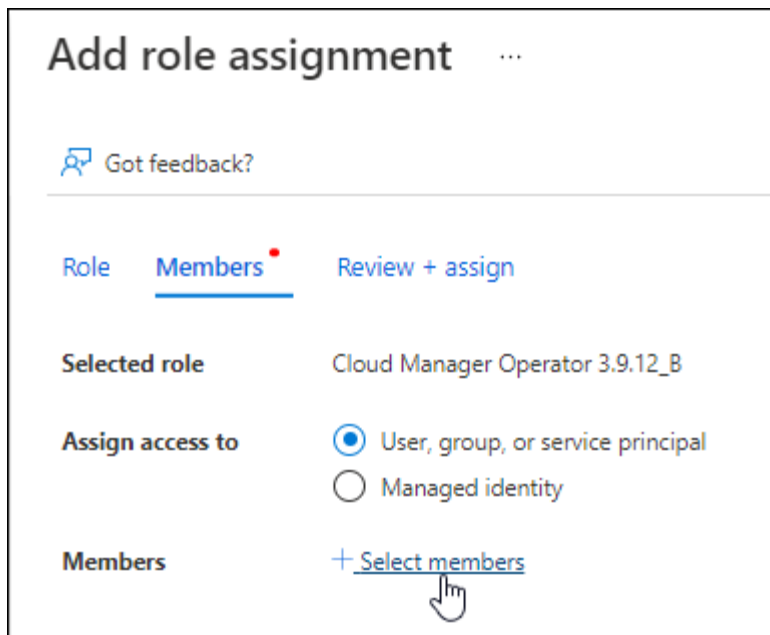
- 输入以下 Azure 命令行界面命令：

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

现在，您应该拥有一个名为 Cloud Manager Operator 的自定义角色，可以将该角色分配给 Connector 虚拟机。

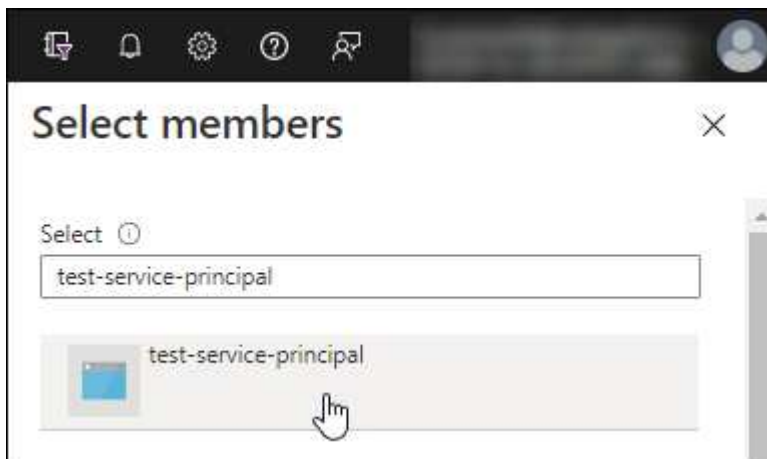
## 2. 将应用程序分配给角色：

- a. 从 Azure 门户中，打开 \* 订阅 \* 服务。
- b. 选择订阅。
- c. 单击 \* 访问控制（IAM） > 添加 > 添加角色分配 \*。
- d. 在 \* 角色 \* 选项卡中，选择 \* Cloud Manager 操作员 \* 角色，然后单击 \* 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 \*。
  - 单击 \* 选择成员 \*。



- 搜索应用程序的名称。

以下是一个示例：



- 选择应用程序并单击 \* 选择 \*。
  - 单击 \* 下一步 \*。
- f. 单击 \* 审核 + 分配 \*。

现在，服务主体具有部署 Connector 所需的 Azure 权限。

如果要从多个 Azure 订阅部署 Cloud Volumes ONTAP，则必须将服务主体绑定到每个订阅。使用 Cloud Manager，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

服务主体必须具有 "Windows Azure 服务管理 API" 权限。

步骤


1. 在 \* Azure Active Directory\* 服务中，单击 \* 应用程序注册 \* 并选择应用程序。
2. 单击 \* API 权限 > 添加权限 \*。
3. 在 \* Microsoft APIs\* 下，选择 \* Azure Service Management\*。













## Request API permissions

### Select an API

Microsoft APIs   APIs my organization uses   My APIs

#### Commonly used Microsoft APIs

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

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

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

## Request API permissions

[< All APIs](#)



Azure Service Management

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

What type of permissions does your application require?

### Delegated permissions

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

### Application permissions

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

Select permissions

[expand all](#)

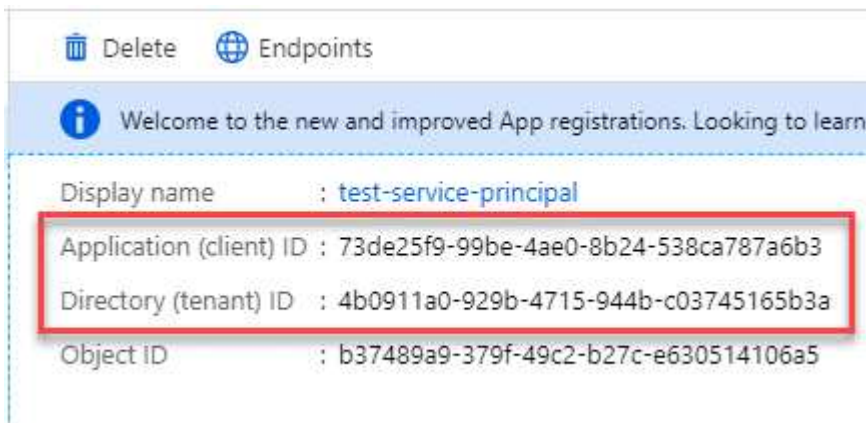
Type to search	
PERMISSION	ADMIN CONSENT REQUIRED
<input checked="" type="checkbox"/> <b>user_impersonation</b> Access Azure Service Management as organization users (preview) ⓘ	-

## 获取应用程序 ID 和目录 ID

将 Azure 帐户添加到 Cloud Manager 时，您需要提供应用程序（客户端）ID 和目录（租户）ID。Cloud Manager 使用 ID 以编程方式登录。

### 步骤

1. 在 \* Azure Active Directory\* 服务中，单击 \* 应用程序注册 \* 并选择应用程序。
2. 复制 \* 应用程序（客户端）ID\* 和 \* 目录（租户）ID\*。



## 创建客户端密钥

您需要创建客户端密钥，然后向 Cloud Manager 提供该密钥的值，以便 Cloud Manager 可以使用它向 Azure AD 进行身份验证。

### 步骤

1. 打开 \* Azure Active Directory\* 服务。
2. 单击 \* 应用程序注册 \* 并选择您的应用程序。

3. 单击 \* 证书和密码 > 新客户端密钥 \*。
4. 提供密钥和持续时间的问题描述。
5. 单击 \* 添加 \*。
6. 复制客户端密钥的值。

### Client secrets

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

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

Copy to clipboard

此时，您的服务主体已设置完毕，您应已复制应用程序（客户端） ID，目录（租户） ID 和客户端密钥值。添加 Azure 帐户时，您需要在 Cloud Manager 中输入此信息。

### 将凭据添加到 Cloud Manager

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

如果您刚刚在云提供商中创建了这些凭据，则可能需要几分钟的时间才能使用这些凭据。请等待几分钟，然后再将凭据添加到 Cloud Manager。

您需要先创建 Connector，然后才能更改 Cloud Manager 设置。"[了解如何操作](#)"。

### 步骤

1. 在 Cloud Manager 控制台的右上角，单击设置图标，然后选择 \* 凭据 \*。

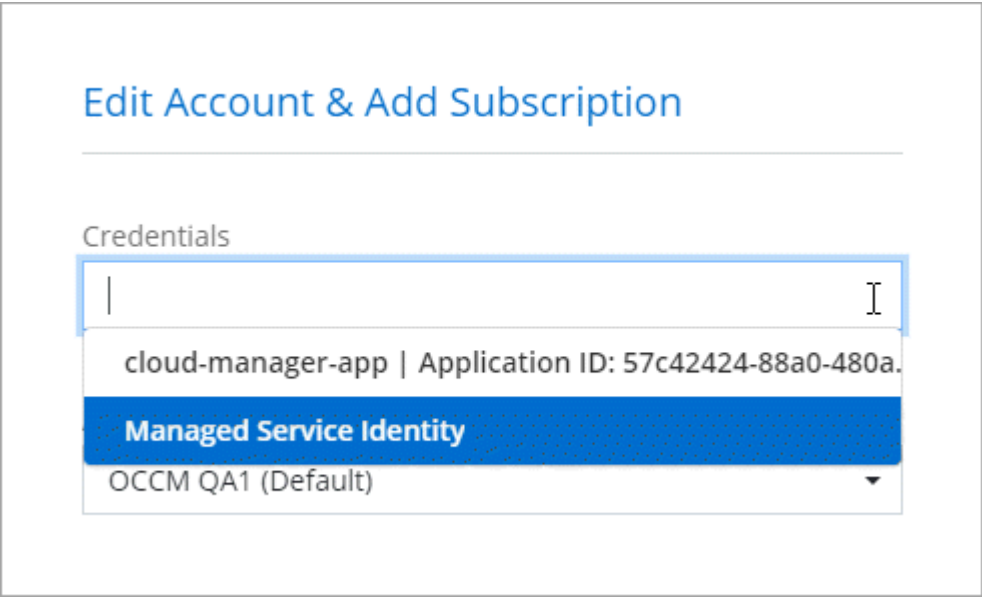


2. 单击 \* 添加凭据 \*，然后按照向导中的步骤进行操作。
  - a. \* 凭据位置 \*：选择 \* Microsoft Azure > Connector\*。
  - b. \* 定义凭据 \*：输入有关授予所需权限的 Azure Active Directory 服务主体的信息：
    - 应用程序（客户端） ID：请参见 [\[Getting the application ID and directory ID\]](#)。
    - 目录（租户） ID：请参见 [\[Getting the application ID and directory ID\]](#)。
    - 客户端密钥：请参见 [\[Creating a client secret\]](#)。
  - 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据相关联。

要按每小时费率（PAYGO）购买 Cloud Volumes ONTAP，这些 Azure 凭据必须与 Azure Marketplace 中的订阅相关联。

- d. \* 查看 \*：确认有关新凭据的详细信息，然后单击 \* 添加 \*。

现在，您可以从 " 详细信息和凭据 " 页面切换到不同的凭据集 "创建新的工作环境时"



管理现有凭据

通过关联 Marketplace 订阅，编辑凭据并将其删除，管理已添加到 Cloud Manager 的 Azure 凭据。

将 **Azure Marketplace** 订阅与凭据关联

将 Azure 凭据添加到 Cloud Manager 后，您可以将 Azure Marketplace 订阅与这些凭据相关联。通过订阅，您可以创建按需购买的 Cloud Volumes ONTAP 系统并使用其他 NetApp 云服务。

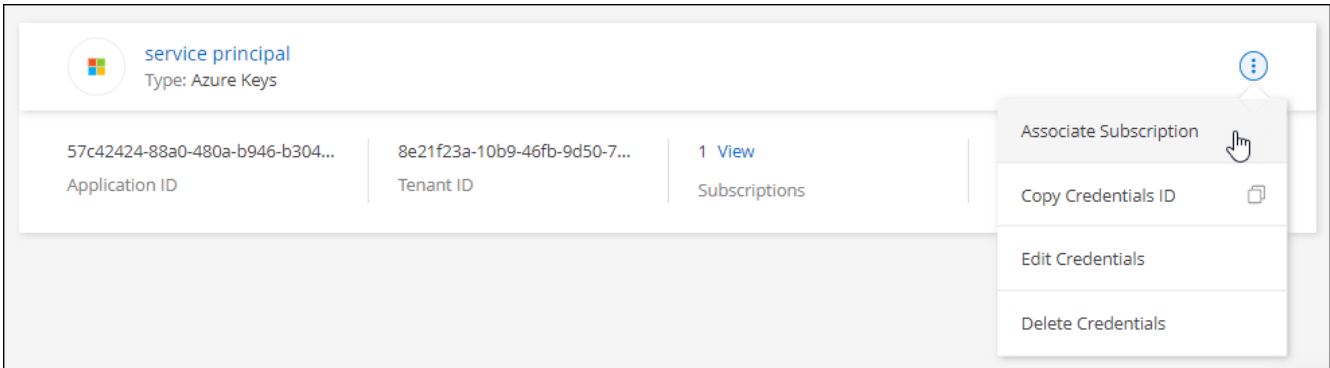
在以下两种情况下，您可能会在将凭据添加到 Cloud Manager 后关联 Azure Marketplace 订阅：

- 最初将凭据添加到 Cloud Manager 时，您未关联订阅。
- 您希望将现有 Azure Marketplace 订阅替换为新订阅。

您需要先创建 Connector ，然后才能更改 Cloud Manager 设置。 "[了解如何操作](#)"。

步骤

1. 在 Cloud Manager 控制台的右上角，单击设置图标，然后选择 \* 凭据 \* 。
2. 单击一组凭据的操作菜单，然后选择 \* 关联订阅 \* 。



3. 从下拉列表中选择订阅或单击 \* 添加订阅 \* ，然后按照步骤创建新订阅。

以下视频从工作环境向导的上下文中启动，但在您单击 \* 添加订阅 \* 后显示相同的工作流：

► [https://docs.netapp.com/zh-cn/cloud-manager-setup-admin//media/video\\_subscribing\\_azure.mp4](https://docs.netapp.com/zh-cn/cloud-manager-setup-admin//media/video_subscribing_azure.mp4)



(video)

### 编辑凭据

通过修改 Azure 服务凭据的详细信息，在 Cloud Manager 中编辑 Azure 凭据。例如，如果为服务主体应用程序创建了新密钥，则可能需要更新客户端密钥。

#### 步骤

1. 在 Cloud Manager 控制台的右上角，单击设置图标，然后选择 \* 凭据 \*。
2. 单击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，然后单击 \* 应用 \*。

### 正在删除凭据

如果您不再需要一组凭据，可以从 Cloud Manager 中删除这些凭据。您只能删除与工作环境无关的凭据。

#### 步骤

1. 在 Cloud Manager 控制台的右上角，单击设置图标，然后选择 \* 凭据 \*。
2. 单击一组凭据的操作菜单，然后选择 \* 删除凭据 \*。
3. 单击 \* 删除 \* 进行确认。

## Google Cloud 凭据

### Google Cloud 项目，权限和帐户

通过服务帐户，Cloud Manager 可以部署和管理与 Connector 位于同一项目或不同项目中的 Cloud Volumes ONTAP 系统。

#### Cloud Manager 的项目和权限

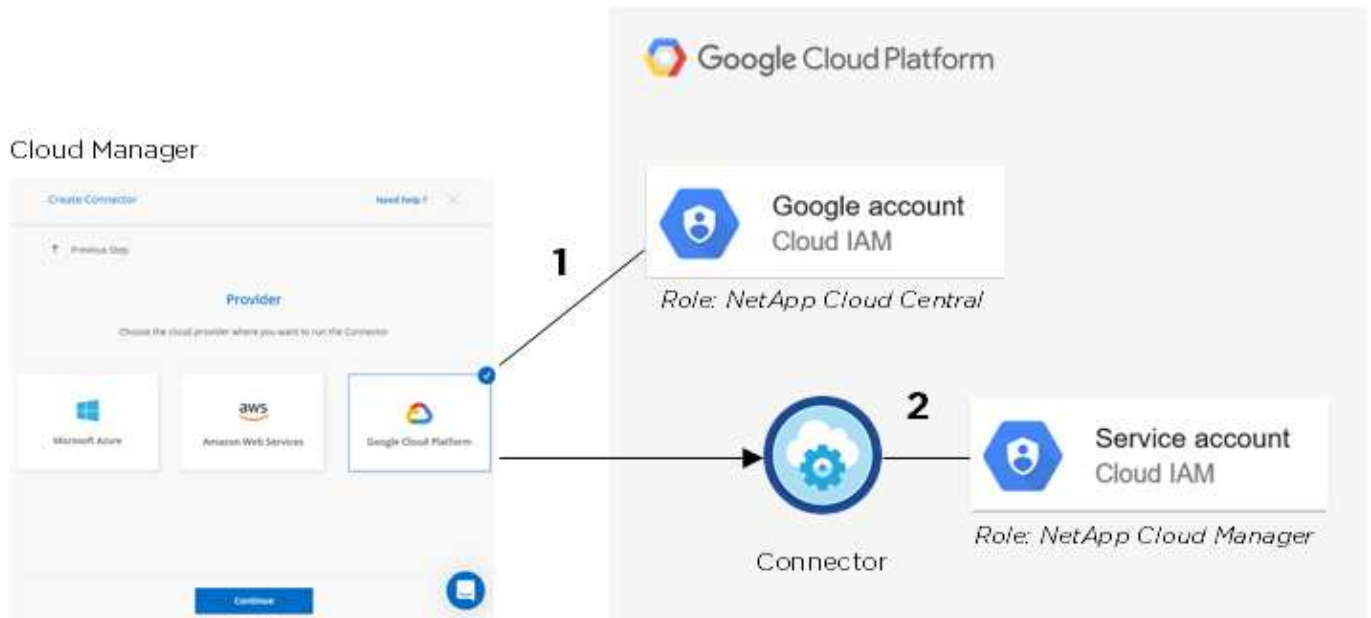
在 Google Cloud 中部署 Cloud Volumes ONTAP 之前，必须先在 Google Cloud 项目中部署 Connector。Connector 不能在您的内部环境或其他云提供商中运行。

在直接从 Cloud Manager 部署 Connector 之前，必须具有两组权限：

1. 您需要使用有权从 Cloud Manager 启动 Connector VM 实例的 Google 帐户部署 Connector。
2. 部署 Connector 时，系统会提示您选择 **"服务帐户"** VM 实例。Cloud Manager 可从服务帐户中获得代表您创建和管理 Cloud Volumes ONTAP 系统的权限。权限可通过将自定义角色附加到服务帐户来提供。

我们设置了两个 YAML 文件，其中包括用户和服务帐户所需的权限。["了解如何使用 YAML 文件设置权限"](#)。

下图显示了上面编号 1 和 2 中所述的权限要求：



## Cloud Volumes ONTAP 项目

Cloud Volumes ONTAP 可以与 Connector 位于同一项目中，也可以位于不同项目中。要在其他项目中部署 Cloud Volumes ONTAP，您需要先将 Connector 服务帐户和角色添加到该项目中。

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

## 管理 Cloud Manager 的 GCP 凭据和订阅

您可以管理与 Connector VM 实例关联的凭据。

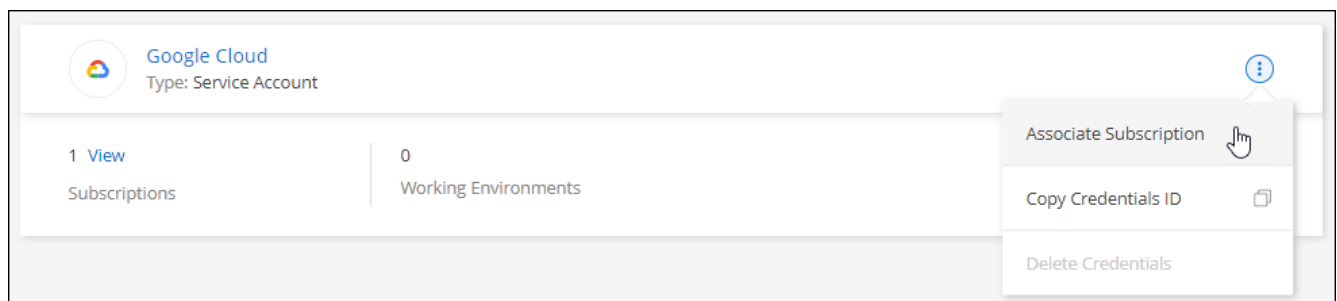
### 将 Marketplace 订阅与 GCP 凭据关联

在 GCP 中部署 Connector 时，Cloud Manager 会创建一组与 Connector VM 实例关联的默认凭据。这些凭据是 Cloud Manager 用于部署 Cloud Volumes ONTAP 的凭据。

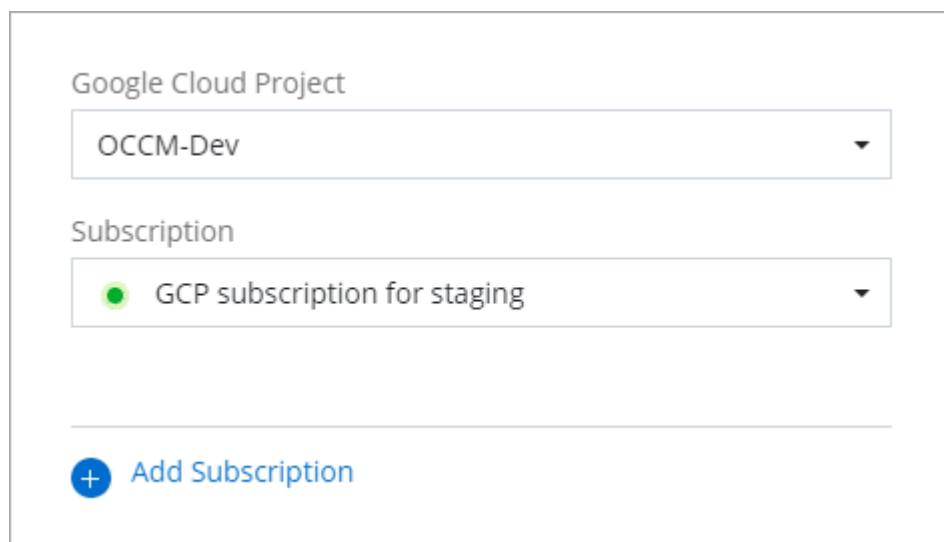
您可以随时更改与这些凭据关联的 Marketplace 订阅。通过订阅，您可以创建按需购买的 Cloud Volumes ONTAP 系统并使用其他 NetApp 云服务。

### 步骤

1. 在 Cloud Manager 控制台的右上角，单击设置图标，然后选择 \* 凭据 \*。
2. 单击一组凭据的操作菜单，然后选择 \* 关联订阅 \*。



3. 从下拉列表中选择 Google Cloud 项目和订阅。



The screenshot shows a web interface for selecting a Google Cloud Project and Subscription. It features two dropdown menus. The first dropdown, labeled "Google Cloud Project", has "OCCM-Dev" selected. The second dropdown, labeled "Subscription", has "GCP subscription for staging" selected, which is preceded by a green circular icon. Below these dropdowns is a horizontal line, and at the bottom is a blue button with a plus icon and the text "Add Subscription".

4. 单击 \* 关联 \*。
5. 如果您尚未订阅，请单击 \* 添加订阅 \*，然后按照以下步骤创建新订阅。



在完成以下步骤之前，请确保您在 Google Cloud 帐户中同时拥有计费管理员权限，并同时拥有 NetApp Cloud Central 登录权限。

6. 查看订阅步骤并单击 \* 继续 \*。

## Add Subscription

### Subscription Steps:

- 1 **Cloud Manager**  
Clicking **Continue** to create your subscription from the Google Cloud Marketplace.
  - 2 **Google Cloud Marketplace**  
Subscribe and then then click **Register With NetApp** to configure your account from Cloud Central.
  - 3 **Cloud Central**  
Save your subscription.
  - 4 **Cloud Manager**  
Associate the Marketplace subscription with your Google Cloud project.
-  View video instructions

Continue

Cancel

7. 重定向到后 "[Google Cloud Marketplace 上的 NetApp Cloud Manager 页面](#)", 确保在顶部导航菜单中选择了正确的项目。

 Google Cloud Platform 





## Cloud Manager for Cloud Volumes ONTAP

NetApp, Inc.

Enterprise-grade data management and protection

[SUBSCRIBE](#)

[OVERVIEW](#) [PRICING](#) [SUPPORT](#)

### Overview

Cloud Volumes ONTAP is a data-management layer that runs natively on Google Cloud infrastructure enabling enhanced control, data protection, mobility and agility for business application data. Get consistent enterprise-grade storage across your hybrid cloud platforms with built-in disaster recovery, backup and ransomware protection. Seamlessly migrate enterprise applications without reengineering. Create company-wide file shares with simultaneous NFS and CIFS/SMB access and iSCSI block storage for GCE instances with scalability up to 368TB. Automate persistent storage provisioning for your Kubernetes clusters. Accelerate CI/CD cycles with instant, zero-capacity data replication. Reduce storage costs by 70% with advanced storage efficiencies. Cloud Manager is the console used to deploy, manage and automate Cloud Volumes ONTAP instances across the hybrid multi-cloud.

[Learn more](#)

### Additional details

Type: [APIs & services](#)

Last updated: 3/26/21

Category: [Storage](#)

Runs on: NetApp, Inc. Cloud Servers

8. 单击 \* 订阅 \*。
9. 选择相应的计费帐户并同意条款和条件。

## 2. Purchase details

Select a billing account \*  
Secondary\_Billing\_Account

## 3. Terms

### Cancellation and change policy

- Usage fee is billed every month.
- You can cancel the service at any time and it will take effect immediately. You will be billed by the amount you used for that month.

### Additional terms

- ☒ I understand this subscription will be automatically renewed at the end of the current term.
- ☒ I authorize Google LLC and its affiliates ("Google") to share my purchase, usage, operational (e.g., project lifecycle events), support ticket, and account information with NetApp, Inc., its affiliates and subcontractors, for the purposes of providing the service, sales attribution, and technical support. I represent that I have the authority to bind my company.
- ☒ By deploying the software or accessing the service you are agreeing to comply with the [End User License Agreement](#), [GCP Marketplace Terms of Service](#), and the terms of applicable open source software licenses bundled with the software or service. Please review these terms and licenses carefully for details about any obligations you may have related to the software or service. To the limited extent an open source software license related to the software or service expressly supersedes the GCP Marketplace Terms of Service, that open source software license governs your use of that software or service.
- By using this product, you understand that certain account and usage information may be shared with NetApp, Inc. for the purposes of financial accounting, sales attribution, performance analysis, and support.
- Google is providing this software or service "as-is" and any support for this software or service will be provided by NetApp, Inc. under their terms of service.

SUBSCRIBE

10. 单击 \* 订阅 \*。

此步骤会将您的传输请求发送给 NetApp。

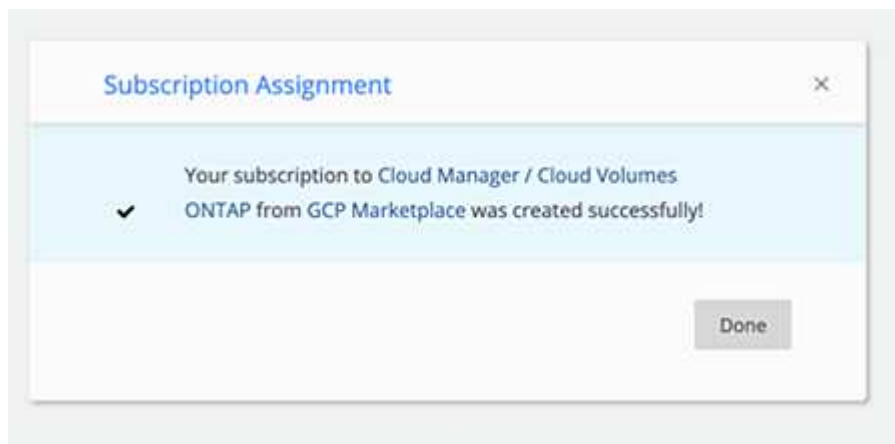
11. 在弹出对话框中，单击 \* 向 NetApp， Inc. 注册 \* 以重定向到 NetApp Cloud Central。



要将 GCP 订阅链接到您的 NetApp 帐户，必须完成此步骤。只有在从此页面重定向并登录到 NetApp Cloud Central 后，链接订阅的过程才会完成。

12. 重定向到 Cloud Central 后，登录到 NetApp Cloud Central 或注册，然后单击 \* 完成 \* 继续。

GCP 订阅将链接到与您的用户登录关联的所有 NetApp 帐户。



如果贵组织的某个用户已从您的计费帐户订阅 NetApp Cloud Manager 订阅，则您将重定向到 "NetApp Cloud Central 上的 Cloud Volumes ONTAP 页面" 而是。如果这是意外情况，请联系您的 NetApp 销售团队。Google 仅为每个 Google 计费帐户启用一个订阅。

13. 完成此过程后，导航回 Cloud Manager 中的凭据页面并选择此新订阅。

Google Cloud Project

OCCM-Dev

Subscription

GCP subscription for staging

Add Subscription

对 Marketplace 订阅过程进行故障排除

有时，通过 Google 云市场订阅 Cloud Volumes ONTAP 可能会由于权限不正确或在重定向到 NetApp Cloud Central 后意外地变得支离破碎。如果发生这种情况，请按照以下步骤完成订阅过程。

步骤

- 1. 导航到 "Google Cloud Marketplace 上的 NetApp Cloud Manager 页面" 以检查订单的状态。如果页面显示 \* 在提供商上管理 \* ，请向下滚动并单击 \* 管理订单 \* 。

Pricing

The product was purchased on 12/9/20.

MANAGE ORDERS

- a. 如果订单显示绿色复选标记，这是意外的，则使用同一计费帐户的组织中的其他人可能已订阅。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。

Filter Enter property name or value

Status	Order number	Plan	Discount	Start date ↓	Plan duration	End date	Payment Schedule	Auto-renew	Next plan	
<div></div>	2eebbc...	Cloud Manager	-	10/21/21	1 month	-	Postpay	N/A	N/A	⋮

- b. 如果订单显示时钟和 \* 待定 \* 状态，请返回到 Marketplace 页面并选择 \* 在提供商上管理 \* 以完成上述流程。

Filter Enter property name or value

Status	Order number	Plan	Discount	Start date ↓	Plan duration	End date	Payment Schedule	Auto-renew	Next plan	
<div></div>	d56c66...	Cloud Manager	-	Pending	1 month	Pending	Postpay	N/A	N/A	⋮

在 Cloud Manager 中添加和管理 NetApp 支持站点帐户

提供 NetApp 支持站点（NSS）帐户的凭据，以便为 Cloud Volumes ONTAP 启用关键工



作流，并通过 Active IQ 提供预测性分析和主动式支持。

## 概述

要启用以下任务，需要将 NetApp 支持站点帐户添加到 Cloud Manager：

- 自带许可证时部署 Cloud Volumes ONTAP （BYOL）

需要提供您的 NSS 帐户，以便 Cloud Manager 可以上传您的许可证密钥并为您购买的期限启用订阅。这包括自动更新期限续订。

- 注册按需购买 Cloud Volumes ONTAP 系统

要激活对系统的支持并访问 NetApp 技术支持资源，需要提供 NSS 帐户。

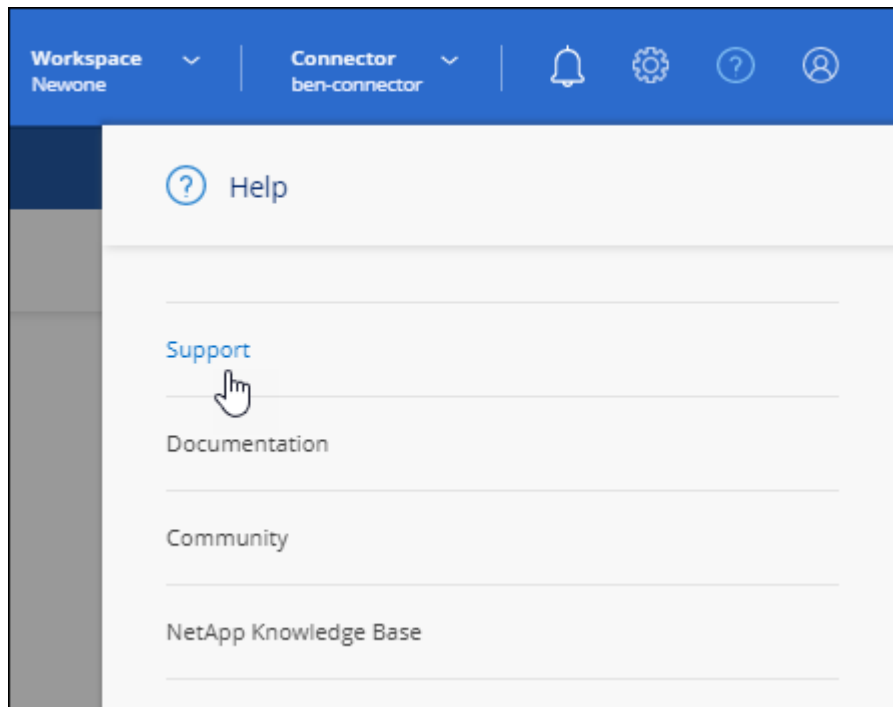
- 将 Cloud Volumes ONTAP 软件升级到最新版本
- 在 Cloud Manager 中使用 Active IQ 数字顾问

## 添加 NSS 帐户

通过支持信息板，您可以从一个位置添加和管理所有 NetApp 支持站点帐户。

### 步骤

1. 如果您还没有 NetApp 支持站点帐户，["注册一个"](#)。
2. 在 Cloud Manager 控制台右上角，单击帮助图标，然后选择 \* 支持 \*。



3. 单击 \* NSS 管理 > 添加 NSS 帐户 \*。
4. 出现提示时，单击 \* 继续 \* 以重定向到 Microsoft 登录页面。

NetApp 使用 Microsoft Azure Active Directory 作为身份提供程序来提供特定于支持和许可的身份验证服务。

5. 在登录页面上，提供 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。

此操作可使 Cloud Manager 使用您的 NSS 帐户。

请注意帐户的以下要求：

- 此帐户必须是客户级别的帐户（而不是来宾或临时帐户）。
- 如果您计划部署基于节点的 BYOL 系统：
  - 帐户必须获得访问 BYOL 系统序列号的授权。
  - 如果您购买了安全的 BYOL 订阅，则需要安全的 NSS 帐户。

现在，用户可以在创建新 Cloud Volumes ONTAP 系统，注册现有 Cloud Volumes ONTAP 系统以及在 Active IQ 中查看数据时选择帐户。

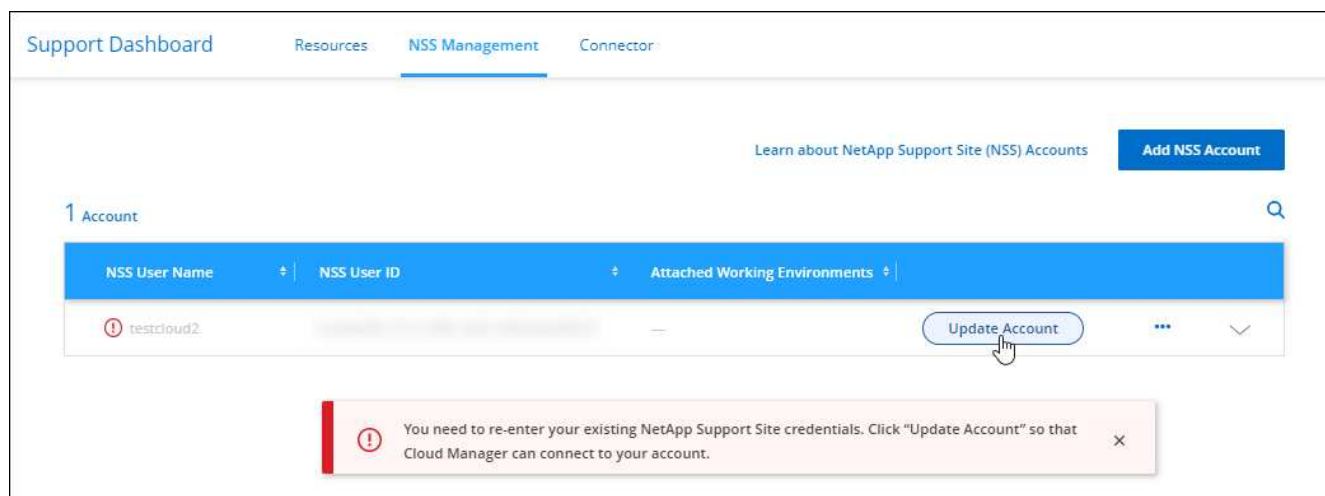
- ["在 AWS 中启动 Cloud Volumes ONTAP"](#)
- ["在 Azure 中启动 Cloud Volumes ONTAP"](#)
- ["在 GCP 中启动 Cloud Volumes ONTAP"](#)
- ["注册按需购买的系统"](#)

## 更新新身份验证方法的 NSS 帐户

从 2021 年 11 月开始，NetApp 现在使用 Microsoft Azure Active Directory 作为身份提供程序来提供特定于支持和许可的身份验证服务。由于此更新，Cloud Manager 将提示您更新先前添加的任何现有帐户的凭据。

### 步骤

1. 如果您尚未执行此操作，["创建一个 Microsoft Azure Active Directory B2C 帐户，此帐户将链接到您的当前 NetApp 帐户"](#)。
2. 在 Cloud Manager 控制台右上角，单击帮助图标，然后选择 \* 支持 \*。
3. 单击 \* NSS 管理 \*。
4. 对于要更新的 NSS 帐户，请单击 \* 更新帐户 \*。



5. 出现提示时，单击 \* 继续 \* 以重定向到 Microsoft 登录页面。

NetApp 使用 Microsoft Azure Active Directory 作为身份提供程序来提供特定于支持和许可的身份验证服务。

6. 在登录页面上，提供 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。

此过程完成后，您更新的帐户现在应在表中列为 *new* 帐户。此帐户的 *older* 版本以及任何现有的工作环境关联仍列在表中。

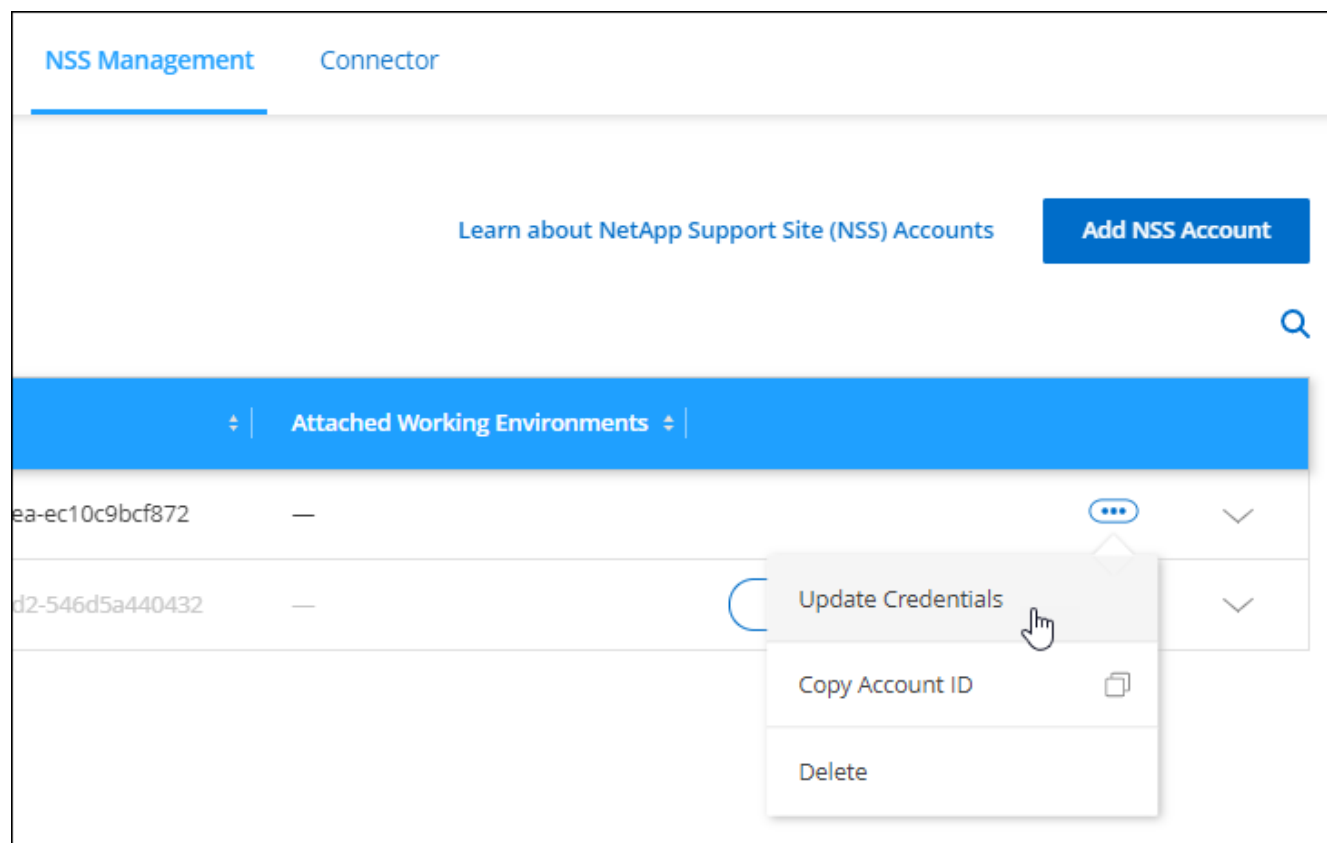
7. 如果现有 Cloud Volumes ONTAP 工作环境已附加到旧版本的帐户，请按照以下步骤进行操作 [将这些工作环境附加到其他 NSS 帐户](#)。
8. 转到旧版本的 NSS 帐户，然后单击 ... 然后选择 \* 删除 \*。

## 更新 NSS 凭据

每当更改 NSS 帐户的凭据时，您都需要在 Cloud Manager 中更新这些凭据。

### 步骤

1. 在 Cloud Manager 控制台右上角，单击帮助图标，然后选择 \* 支持 \*。
2. 单击 \* NSS 管理 \*。
3. 对于要更新的 NSS 帐户，请单击 ... 然后选择 \* 更新凭据 \*。



4. 出现提示时，单击 \* 继续 \* 以重定向到 Microsoft 登录页面。

NetApp 使用 Microsoft Azure Active Directory 作为身份提供程序来提供特定于支持和许可的身份验证服务。

5. 在登录页面上，提供 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。

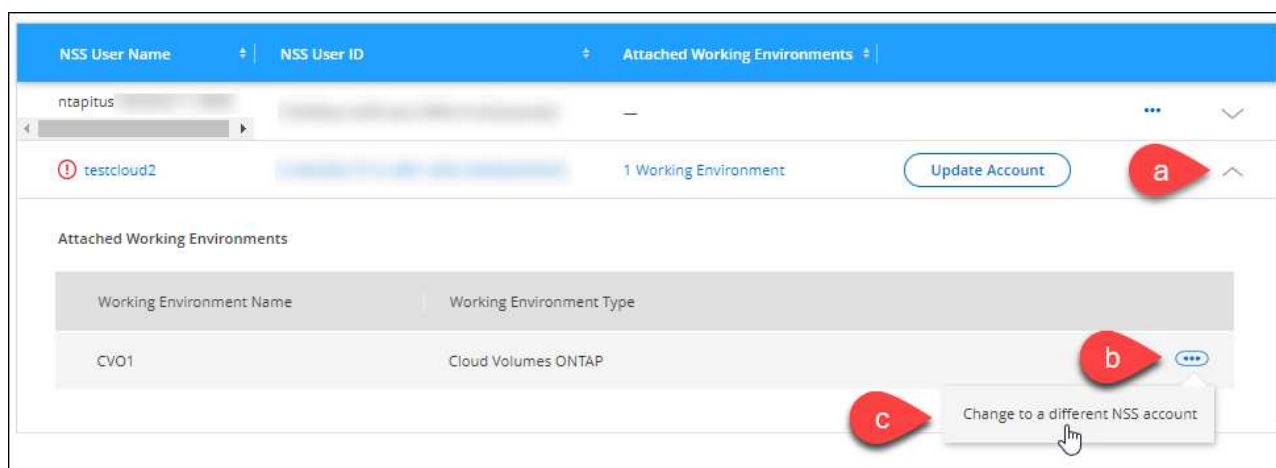
## 将工作环境附加到其他 NSS 帐户

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

只有配置为使用 NetApp 采用的 Microsoft Azure AD 进行身份管理的 NSS 帐户才支持此功能。在使用此功能之前，您需要单击 \* 添加 NSS 帐户 \* 或 \* 更新帐户 \*。

### 步骤

1. 在 Cloud Manager 控制台右上角，单击帮助图标，然后选择 \* 支持 \*。
2. 单击 \* NSS 管理 \*。
3. 完成以下步骤以更改 NSS 帐户：
  - a. 展开当前与工作环境关联的 NetApp 支持站点帐户对应的行。
  - b. 对于要更改关联的工作环境，请单击 ...
  - c. 选择 \* 更改为其他 NSS 帐户 \*。



- d. 选择帐户，然后单击 \* 保存 \*。

## 显示 NSS 帐户的电子邮件地址

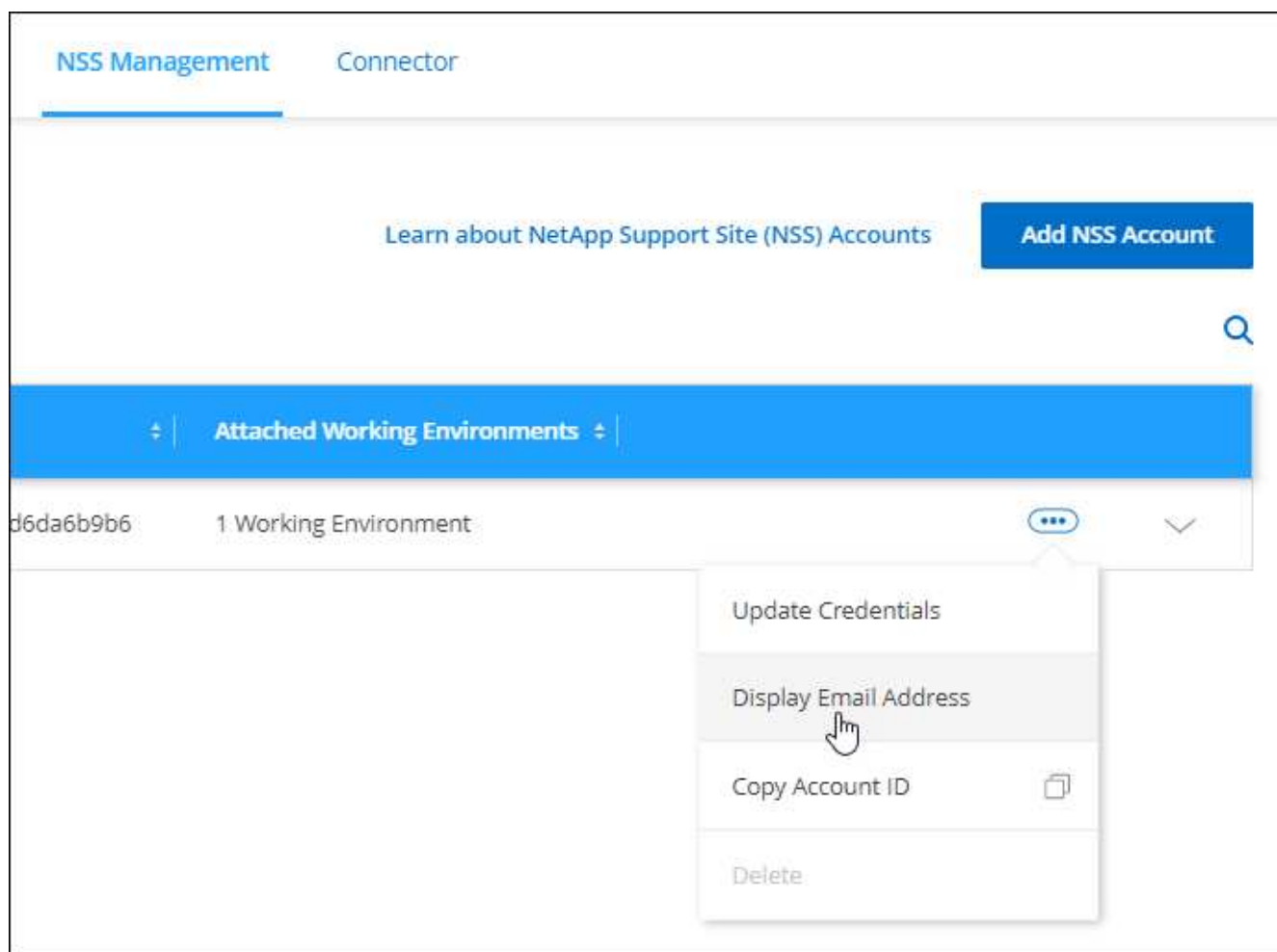
现在，NetApp 支持站点帐户使用 Microsoft Azure Active Directory 进行身份验证服务，Cloud Manager 中显示的 NSS 用户名通常是 Azure AD 生成的标识符。因此，您可能无法立即知道与该帐户关联的电子邮件地址。但 Cloud Manager 可以选择向您显示关联的电子邮件地址。



转到 "NSS 管理" 页面时，Cloud Manager 会为表中的每个帐户生成一个令牌。此令牌包含有关关联电子邮件地址的信息。退出此页面后，此令牌将被删除。此信息永远不会缓存，这有助于保护您的隐私。

### 步骤

1. 在 Cloud Manager 控制台右上角，单击帮助图标，然后选择 \* 支持 \*。
2. 单击 \* NSS 管理 \*。
3. 对于要更新的 NSS 帐户，请单击 ... 然后选择 \* 显示电子邮件地址 \*。



Cloud Manager 将显示 NetApp 支持站点的用户名以及关联的电子邮件地址。您可以使用复制按钮复制电子邮件地址。

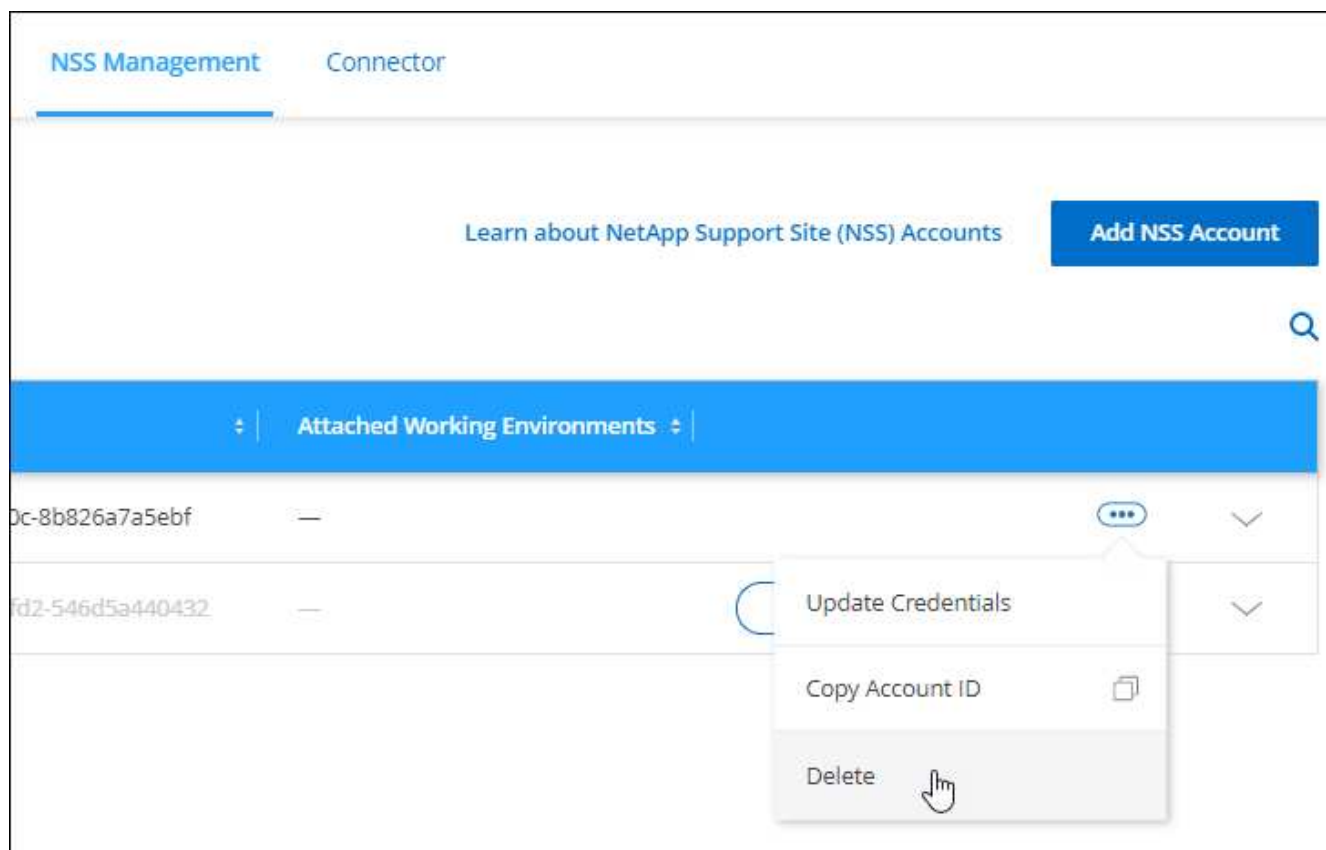
## 删除 NSS 帐户

删除您不想再与 Cloud Manager 结合使用的任何 NSS 帐户。

请注意，您不能删除当前与 Cloud Volumes ONTAP 工作环境关联的帐户。您首先需要 [将这些工作环境附加到其他 NSS 帐户](#)。

### 步骤

1. 在 Cloud Manager 控制台右上角，单击帮助图标，然后选择 \* 支持 \*。
2. 单击 \* NSS 管理 \*。
3. 对于要删除的 NSS 帐户，请单击 ... 然后选择 \* 删除 \*。



4. 单击 \* 删除 \* 进行确认。

# 参考

## Cloud Manager权限摘要

要使用Cloud Manager中的功能和服务、您需要提供权限、以便Cloud Manager可以在您的云环境中执行操作。使用此页面上的链接可根据您的目标快速访问所需的权限。

### AWS权限

目的	Description	链接。
连接器部署	从Cloud Manager创建Connector的用户需要特定权限才能在AWS中部署实例。	<a href="#">"从 Cloud Manager 在 AWS 中创建连接器"</a>
连接器操作	Cloud Manager启动Connector时、它会将一个策略附加到实例、该实例提供管理AWS帐户中资源和进程所需的权限。如果需要、您需要自行设置策略 <a href="#">"从市场启动Connector"</a> 或者 <a href="#">"向Connector添加更多AWS凭据"</a> 。此外、您还需要确保在后续版本中添加新权限时策略是最新的。	<a href="#">"Connector 的 AWS 权限"</a>
Cloud Volumes ONTAP 操作	必须将IAM角色附加到AWS中的每个Cloud Volumes ONTAP 节点。HA调解器也是如此。默认选项是让Cloud Manager为您创建IAM角色、但您可以使用自己的角色。	<a href="#">"了解如何自己设置IAM角色"</a>

### Azure权限

目的	Description	链接。
连接器部署	从Cloud Manager部署Connector时、您需要使用有权在Azure中部署Connector VM的Azure帐户或服务主体。	<a href="#">"从 Cloud Manager 在 Azure 中创建 Connector"</a>
连接器操作	当Cloud Manager在Azure中部署Connector VM时、它会创建一个自定义角色、此角色可提供在该Azure订阅中管理资源和进程所需的权限。  如果需要、您需要自己设置自定义角色 <a href="#">"从市场启动Connector"</a> 或者 <a href="#">"向Connector添加更多Azure凭据"</a> 。  此外、您还需要确保在后续版本中添加新权限时策略是最新的。	<a href="#">"Connector 的 Azure 权限"</a>

### Google Cloud权限

目的	Description	链接。
连接器部署	从Cloud Manager部署Connector的Google Cloud用户需要特定权限才能在Google Cloud中部署Connector。	<a href="#">"设置部署Connector的权限"</a>
连接器操作	Connector VM实例的服务帐户必须具有执行日常操作的特定权限。在从Cloud Manager部署服务帐户时、您需要将其与Connector相关联。此外、您还需要确保在后续版本中添加新权限时策略是最新的。	<a href="#">"为Connector设置服务帐户"</a>

## Connector 的 AWS 权限

当Cloud Manager在AWS中启动Connector实例时、它会向此实例附加一个策略、此策略可为Connector提供管理该AWS帐户中资源和进程的权限。Connector使用这些权限对多个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

下面显示的IAM策略提供了Connector根据您的AWS区域管理公有云环境中的资源和流程所需的权限。

直接从Cloud Manager创建Connector时、Cloud Manager会自动将此策略应用于Connector。

如果您从AWS Marketplace部署Connector、或者在Linux主机上手动安装Connector、则需要自己设置策略。

此外、您还需要确保在后续版本中添加新权限时策略是最新的。



```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "cvoServicePolicy",
      "Effect": "Allow",
      "Action": [
        "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",
        "cloudformation:CreateStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:ValidateTemplate",
        "iam:PassRole",
        "iam:CreateRole",
        "iam:PutRolePolicy",
```

```
"iam:CreateInstanceProfile",
"iam:AddRoleToInstanceProfile",
"iam:RemoveRoleFromInstanceProfile",
"iam:ListInstanceProfiles",
"sts:DecodeAuthorizationMessage",
"ec2:AssociateIamInstanceProfile",
"ec2:DescribeIamInstanceProfileAssociations",
"ec2:DisassociateIamInstanceProfile",
"s3:GetBucketTagging",
"s3:GetBucketLocation",
"s3:ListBucket",
"s3:CreateBucket",
"s3:GetLifecycleConfiguration",
"s3:ListBucketVersions",
"s3:GetBucketPolicyStatus",
"s3:GetBucketPublicAccessBlock",
"s3:GetBucketPolicy",
"s3:GetBucketAcl",
"kms:List*",
"kms:ReEncrypt*",
"kms:Describe*",
"kms:CreateGrant",
"ce:GetReservationUtilization",
"ce:GetDimensionValues",
"ce:GetCostAndUsage",
"ce:GetTags",
"ec2:CreatePlacementGroup",
"ec2:DescribeReservedInstancesOfferings",
"sts:AssumeRole",
"ec2:AssignPrivateIpAddresses",
"ec2:CreateRoute",
"ec2:DescribeVpcs",
"ec2:ReplaceRoute",
"ec2:UnassignPrivateIpAddresses",
"s3:PutObjectTagging",
"s3:GetObjectTagging",
"fsx:Describe*",
"fsx:List*",
"ec2:DeleteSecurityGroup",
"ec2:DeleteNetworkInterface",
"ec2:DeleteSnapshot",
"ec2:DeleteTags",
"ec2:DeleteRoute",
"ec2:DeletePlacementGroup",
"iam:DeleteRole",
"iam:DeleteRolePolicy",
```

```

        "iam:DeleteInstanceProfile",
        "cloudformation:DeleteStack",
        "ec2:DescribePlacementGroups",
        "iam:GetRolePolicy",
        "s3:ListAllMyBuckets",
        "s3:GetObject",
        "iam:GetRole",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:PutObject",
        "ec2:ModifyVolume",
        "ec2:DescribeVolumesModifications"
    ],
    "Resource": "*"
},
{
    "Sid": "backupPolicy",
    "Effect": "Allow",
    "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",
        "athena:StopQueryExecution",
        "glue:CreateDatabase",
        "glue:CreateTable",
    ]
}

```

```

        "glue:BatchDeletePartition"
    ],
    "Resource": "*"
},
{
    "Sid": "backupS3Policy",
    "Effect": "Allow",
    "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"
    ],
    "Resource": [
        "arn:aws:s3:::netapp-backup-*"
    ]
},
{
    "Sid": "tagServicePolicy",
    "Effect": "Allow",
    "Action": [
        "ec2:CreateTags",
        "ec2:DeleteTags",
        "ec2:DescribeTags",
        "tag:getResources",
        "tag:getTagKeys",
        "tag:getTagValues",
        "tag:TagResources",
        "tag:UntagResources"
    ],

```

```

    "Resource": "*"
  },
  {
    "Sid": "fabricPoolS3Policy",
    "Effect": "Allow",
    "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*"
    ]
  },
  {
    "Sid": "fabricPoolPolicy",
    "Effect": "Allow",
    "Action": [
      "ec2:DescribeRegions"
    ],
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "ec2:StartInstances",
      "ec2:StopInstances",
      "ec2:TerminateInstances"
    ],
    "Condition": {
      "StringLike": {
        "ec2:ResourceTag/netapp-adc-manager": "*"
      }
    },
    "Resource": [
      "arn:aws:ec2:*:*:instance/*"
    ]
  },
},

```

```

{
  "Effect": "Allow",
  "Action": [
    "ec2:StartInstances",
    "ec2:TerminateInstances",
    "ec2:AttachVolume",
    "ec2:DetachVolume"
  ],
  "Condition": {
    "StringLike": {
      "ec2:ResourceTag/GFCInstance": "*"
    }
  },
  "Resource": [
    "arn:aws:ec2:*:*:instance/*"
  ]
},
{
  "Effect": "Allow",
  "Action": [
    "ec2:StartInstances",
    "ec2:TerminateInstances",
    "ec2:AttachVolume",
    "ec2:DetachVolume",
    "ec2:StopInstances",
    "ec2>DeleteVolume"
  ],
  "Condition": {
    "StringLike": {
      "ec2:ResourceTag/WorkingEnvironment": "*"
    }
  },
  "Resource": [
    "arn:aws:ec2:*:*:instance/*"
  ]
},
{
  "Effect": "Allow",
  "Action": [
    "ec2:AttachVolume",
    "ec2:DetachVolume"
  ],
  "Resource": [
    "arn:aws:ec2:*:*:volume/*"
  ]
},

```

```

{
  "Effect": "Allow",
  "Action": [
    "ec2:DeleteVolume"
  ],
  "Condition": {
    "StringLike": {
      "ec2:ResourceTag/WorkingEnvironment": "*"
    }
  },
  "Resource": [
    "arn:aws:ec2:*:*:volume/*"
  ]
},
{
  "Sid": "K8sServicePolicy",
  "Effect": "Allow",
  "Action": [
    "ec2:DescribeRegions",
    "iam:ListInstanceProfiles",
    "eks:ListClusters",
    "eks:DescribeCluster"
  ],
  "Resource": "*"
},
{
  "Sid": "GFCservicePolicy",
  "Effect": "Allow",
  "Action": [
    "cloudformation:DescribeStacks",
    "cloudwatch:GetMetricStatistics",
    "cloudformation:ListStacks"
  ],
  "Resource": "*"
}
]
}

```

### GovCloud (美国)地区

```

{
  "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",
        "ce:GetReservationUtilization",
        "ce:GetDimensionValues",
        "ce:GetCostAndUsage",
        "ce:GetTags",
        "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/*"
    ]
}
]
}

```

## C2S环境

```

{
    "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/*"
    ]
}
]
}

```

= AWS权限的使用方式

以下各节介绍了如何对每个NetApp云服务使用权限。如果您的公司策略规定仅在需要时提供权限、则此信息会很有用。

== AppTemplate标记

在使用AppTemplate标记服务时、Connector会发出以下API请求来管理AWS资源上的标记：

- EC2: CreateTags

- EC2: DeleteTags
- EC2: Describe标记
- 标记: getResources
- 标记: getTag密钥
- 标记: getTagValues
- 标记: 标记资源
- 标记: 未标记资源

==云备份

Connector会发出以下API请求来部署Cloud Backup的还原实例:

- EC2: StartInstances
- EC2: StopInstances
- EC2: Describe实例
- EC2: Describe实例状态
- EC2: RunInstances
- EC2: 终端状态
- EC2: Describe实例属性
- EC2: Describe
- EC2: CreateTags
- EC2: CreateVolume
- EC2: CreateSecurityGroup
- EC2: Describe子网
- EC2: Describe
- EC2: Describe注册
- CloudFormation: CreateStack
- CloudFormation: DeleteStack
- CloudFormation: Describe堆栈

Connector会发出以下API请求来管理Amazon S3中的备份:

- S3 : GetBucketLocation
- S3 : ListAllMy桶
- S3 : ListBucket
- S3 : CreateBucket
- S3 : GetLifecycleConfiguration
- S3 : PutLifecycleConfiguration

- S3 : PutBucketTagging
- S3 : ListBucketVersions
- S3 : GetBucketAcl
- S3: PutBucketPublicAccessBlock
- 公里: 列表\*
- 公里: 描述\*
- S3 : GetObject
- EC2: 介绍VpcEndpoints
- Kms: ListAliases
- S3 : PutEncryptionConfiguration

在使用搜索和还原方法还原卷和文件时、Connector会发出以下API请求:

- S3 : CreateBucket
- S3 : DeleteObject
- S3 : DeleteObjectVersion
- S3 : GetBucketAcl
- S3 : ListBucket
- S3 : ListBucketVersions
- S3 : ListBucketMultipartUploads
- S3 : PutObject
- S3: PutBucketAcl
- S3 : PutLifecycleConfiguration
- S3: PutBucketPublicAccessBlock
- S3 : AbortMultipartUpload
- S3 : ListMultipartUploadPart
- Athena: StartQueryExecutionc
- Athena: GetQueryResults
- Athena: GetQueryExecution
- Athena: StopQueryExecution
- 胶水: CreateDatabase
- 胶水: CreateTable
- 粘附: BatechDelete分区

==云数据感知

Connector发出以下API请求以部署Cloud Data sense实例:

- EC2: Describe实例
- EC2: Describe实例状态
- EC2: RunInstances
- EC2: 终端状态
- EC2: CreateTags
- EC2: CreateVolume
- EC2: Attach卷
- EC2: CreateSecurityGroup
- EC2: DeleteSecurityGroup
- EC2: Describe安全性组
- EC2: CreateNetworkInterface
- EC2: Describe网络接口
- EC2: DeleteNetworkInterface
- EC2: Describe子网
- EC2: Describe
- EC2: CreateSnapshot
- EC2: Describe注册
- CloudFormation: CreateStack
- CloudFormation: DeleteStack
- CloudFormation: Describe堆栈
- CloudFormation: Describe StackEvents
- IAM: AddRoleToInstanceProfile
- EC2: AssociateIamInstanceProfile
- EC2: Describe IamInstanceProfileAssociations

在使用Cloud Data sense时、Connector会发出以下API请求来扫描S3存储分段：

- IAM: AddRoleToInstanceProfile
- EC2: AssociateIamInstanceProfile
- EC2: Describe IamInstanceProfileAssociations
- S3 : GetBucketTagging
- S3 : GetBucketLocation
- S3 : ListAllMy桶
- S3 : ListBucket
- S3: GetBucketPolicyStatus
- S3 : GetBucketPolicy



- S3 : GetBucketAcl
- S3 : GetObject
- IAM: GetRole
- S3 : DeleteObject
- S3 : DeleteObjectVersion
- S3 : PutObject
- STS: AssumeRole

==云分层

在使用Cloud Tiering时、Connector会发出以下API请求、将数据分层到Amazon S3。

Action	用于设置?	用于日常操作?
S3 : CreateBucket	是的。	否
S3 : PutLifecycleConfiguration	是的。	否
S3 : GetLifecycleConfiguration	是的。	是的。
EC2: Describe注册	是的。	是的。

== Cloud Volumes ONTAP

Connector会发出以下API请求、以便在AWS中部署和管理Cloud Volumes ONTAP。

目的	Action	用于部署?	用于日常操作?	用于删除?
创建和管理Cloud Volumes ONTAP 实例的IAM角色和实例配置文件	IAM : ListInstanceProfile	是的。	是的。	否
	IAM: CreateRole	是的。	否	否
	IAM: DeleteRole	否	是的。	是的。
	IAM : PutRolePolicy	是的。	否	否
	IAM : CreateInstanceProfile	是的。	否	否
	IAM : DeleteRolePolicy	否	是的。	是的。
	IAM : AddRoleToInstanceProfile	是的。	否	否
	IAM : RemoveRoleFromInstanceProfile	否	是的。	是的。
	IAM : DeleteInstanceProfile	否	是的。	是的。
	IAM: PassRole	是的。	否	否
	EC2 : AssociateIamInstanceProfile	是的。	是的。	否
	EC2: DescribeIamInstanceProfileAssociations	是的。	是的。	否
	EC2 : DisassociateIamInstanceProfile	否	是的。	否
对授权状态消息进行解码	STS : DecodeAuthorizationMessage	是的。	是的。	否
描述可供帐户使用的指定映像(AMI)	EC2: Describe	是的。	是的。	否
描述VPC中的路由表(仅HA对需要)	EC2: Describe RouteTables	是的。	否	否

目的	Action	用于部署?	用于日常操作?	用于删除?
停止、启动和监控实例	EC2 : StartInstances	是的。	是的。	否
	EC2 : StopInstances	是的。	是的。	否
	EC2: Describe实例	是的。	是的。	否
	EC2: Describe实例状态	是的。	是的。	否
	EC2 : RunInstances	是的。	否	否
	EC2: 终端状态	否	否	是的。
	EC2 : ModifyInstance属性	否	是的。	否
验证是否已为支持的实例类型启用增强型网络连接	EC2: Describe实例属性	否	是的。	否
使用"WorkingEnvironment"和"WorkingEnvironmentId"标记标记资源、用于维护和成本分配	EC2: CreateTags	是的。	是的。	否
管理Cloud Volumes ONTAP 用作后端存储的EBS卷	EC2 : CreateVolume	是的。	是的。	否
	EC2: Describe卷	是的。	是的。	是的。
	EC2 : ModifyVolumeAttribute	否	是的。	是的。
	EC2: Attach卷	是的。	是的。	否
	EC2 : DeleteVolume	否	是的。	是的。
	EC2: 分离卷	否	是的。	是的。

目的	Action	用于部署?	用于日常操作?	用于删除?
创建和管理Cloud Volumes ONTAP 的安全组	EC2 : CreateSecurityGroup	是的。	否	否
	EC2 : DeleteSecurityGroup	否	是的。	是的。
	EC2: Describe安全性组	是的。	是的。	是的。
	EC2 : RevokeSecurityGroupEgress	是的。	否	否
	EC2 : AuthorizeSecurityGroupEgress	是的。	否	否
	EC2 : AuthorizeSecurityGroupIngress	是的。	否	否
	EC2 : RevokeSecurityGroupIngress	是的。	是的。	否
在目标子网中为Cloud Volumes ONTAP 创建和管理网络接口	EC2 : CreateNetworkInterface	是的。	否	否
	EC2: Describe网络接口	是的。	是的。	否
	EC2 : DeleteNetworkInterface	否	是的。	是的。
	EC2 : ModifyNetworkInterfaceAttribute	否	是的。	否
获取目标子网和安全组的列表	EC2: Describe子网	是的。	是的。	否
	EC2: Describe	是的。	是的。	否
获取DNS服务器和Cloud Volumes ONTAP 实例的默认域名	EC2: Describe DhcpOptions	是的。	否	否

目的	Action	用于部署?	用于日常操作?	用于删除?
为Cloud Volumes ONTAP 的EBS卷创建快照	EC2 : CreateSnapshot	是的。	是的。	否
	EC2 : DeleteSnapshot	否	是的。	是的。
	EC2: Describe Snapshot	否	是的。	否
捕获附加到AutoSupport 消息的Cloud Volumes ONTAP 控制台	EC2 : GetConsoleOutput	是的。	是的。	否
获取可用密钥对的列表	EC2: Describe KeyPairs	是的。	否	否
获取可用AWS区域的列表	EC2: Describe注册	是的。	是的。	否
管理与Cloud Volumes ONTAP 实例关联的资源的标记	EC2: DeleteTags	否	是的。	是的。
	EC2: Describe标记	否	是的。	否
为AWS CloudFormation模板创建和管理堆栈	CloudFormation : CreateStack	是的。	否	否
	CloudFormation : DeleteStack	是的。	否	否
	CloudFormation : Describe堆栈	是的。	是的。	否
	CloudFormation : Describe StackEvents	是的。	否	否
	CloudFormation: 验证模板	是的。	否	否

目的	Action	用于部署?	用于日常操作?	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存储分段	S3 : CreateBucket	是的。	是的。	否
	S3 : DeleteBucket	否	是的。	是的。
	S3 : GetLifecycleConfiguration	否	是的。	否
	S3 : PutLifecycleConfiguration	否	是的。	否
	S3 : PutBucketTagging	否	是的。	否
	S3 : ListBucketVersions	否	是的。	否
	S3 : GetBucketPolicy Status	否	是的。	否
	S3 : GetBucketPublic AccessBlock	否	是的。	否
	S3 : GetBucketAcl	否	是的。	否
	S3 : GetBucketPolicy	否	是的。	否
	S3 : PutBucketPublic AccessBlock	否	是的。	否
	S3 : GetBucketTagging	否	是的。	否
	S3 : GetBucketLocation	否	是的。	否
	S3 : ListAllMy桶	否	否	否
	S3 : ListBucket	否	是的。	否
使用AWS密钥管理服务(KMS)对Cloud Volumes ONTAP 启用数据加密	公里：列表*	是的。	是的。	否
	kms：重新加密*	是的。	否	否
	公里：描述*	是的。	是的。	否
	公里：CreateGrant	是的。	是的。	否

目的	Action	用于部署?	用于日常操作?	用于删除?
获取Cloud Volumes ONTAP 的AWS成本数据	CE : GetReservationUtilization	否	是的。	否
	CE : GetDimensionValues	否	是的。	否
	CE : GetCostAndUsage	否	是的。	否
	CE: GetTags	否	是的。	否
在一个AWS可用性区域中为两个HA节点和调解器创建和管理一个AWS分布式放置组	EC2 : CreatePlacementGroup	是的。	否	否
	EC2 : DeletePlacementGroup	否	是的。	是的。
创建报告	FSX: 描述*	否	是的。	否
	FSX: List*	否	是的。	否
创建和管理支持Amazon EBS弹性卷功能的聚合	EC2: Describe卷修改	否	是的。	否
	EC2 : ModifyVolume	否	是的。	否

## ==全局文件缓存

Connector会发出以下API请求、以便在部署期间部署全局文件缓存实例：

- CloudFormation: Describe堆栈
- CloudWatch: GetMetricStatistics
- CloudFormation: ListStack

## == Kubernetes

Connector会发出以下API请求来发现和管理Amazon EKS集群：

- EC2: Describe注册
- EKS: ListClusters
- EKS: Describe集群
- IAM: GetInstanceProfile

# Connector 的 Azure 权限

当Cloud Manager在Azure中启动Connector VM时、它会将一个自定义角色附加到该VM、从而使Connector能够管理该Azure订阅中的资源和进程。Connector使用权限对多个Azure服务进行API调用。

## 自定义角色权限

下面显示的自定义角色提供了Connector管理Azure网络中的资源和进程所需的权限。

直接从Cloud Manager创建Connector时、Cloud Manager会自动将此自定义角色应用于Connector。

如果您从Azure Marketplace部署Connector、或者在Linux主机上手动安装Connector、则需要您自己设置自定义角色。

您还需要确保角色是最新的、因为在后续版本中添加了新权限。

```
{
  "Name": "Cloud Manager 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/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/regeneratekey/action",
"Microsoft.Storage/storageAccounts/write",

"Microsoft.Storage/storageAccounts/blobServices/containers/read",
"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/agreements/read",

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

"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/action",

"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.Network/loadBalancers/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"
],
    "NotActions": [],

```

```

"AssignableScopes": [],
"Description": "Cloud Manager Permissions",
"IsCustom": "true"
}

```

## 如何使用Azure权限

操作	目的
Microsoft.Compute/locations/operations/read" , Microsoft.Compute/locations/vmSizes/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/start/action" , Microsoft.Compute/virtualMachines/deallocate/action" , Microsoft.Compute/virtualMachines/vmSizes/read" , " Microsoft.Compute/virtualMachines/write" ,	创建 Cloud Volumes ONTAP 并停止、启动、删除和获取系统状态。
"Microsoft.compute/images/write" 、 "Microsoft.compute/images/read" 、	支持从 VHD 部署 Cloud Volumes ONTAP 。
Microsoft.Compute/disks/delete" , Microsoft.Compute/disks/read" , Microsoft.Compute/disks/write" , "microsoft.Storage/SchecknameAvailability /Read" , "microsoft.Storage/operations/Read" , "microsoft.Storage/storageAccounts" , "microsoft.Storage/storageAccounts/Read" , "microsoft.Storage/storageAccounts" , "microsoft.Storage/storageAccounts" , "microsoft.Storage/storageAccounts" , "microsoft.Storage/storageAccounts" , "microsoft.Storage/Access/ Read" ,	管理 Azure 存储帐户和磁盘、并将磁盘连接到 Cloud Volumes ONTAP 。
"microsoft.Storage/storageAccounts/blobServices/containers/read" , "microsoft.KeyVault/vaults/read" , "microsoft.KeyVault/vaults/accessPolicies/write"	可备份到 Azure Blob 存储并对存储帐户进行加密
"microsoft.network/networkinterfaces/read" 、 "microsoft.network/networkinterfaces/write" 、 "microsoft.network/networkinterfaces/join/action" 、	在目标子网中为 Cloud Volumes ONTAP 创建和管理网络接口。
"microsoft.network/networksecuritygroups/read" 、 "microsoft.network/networksecuritygroups/write" 、 "microsoft.network/networksecuritygroups/join/action" 、	为 Cloud Volumes ONTAP 创建预定义的网络安全组。

操作	目的
"microsoft.resources/subscriptions/locations/read" , Microsoft.Network/locations/operationResults/read" , Microsoft.Network/locations/operations/read" , Microsoft.Network/virtualNetworks/read" , Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read" , Microsoft.Network/virtualNetworks/subnets/read" , Microsoft.Network/virtualNetworks/subnets/virtualMachines/read" , Microsoft.Network/virtualNetworks/virtualMachines/read" , Microsoft.Network/virtualNetworks/subnets/join/action" ,	获取有关区域、目标 VNet 和子网的网络信息、并将 Cloud Volumes ONTAP 添加到 VNETS 。
Microsoft.Network/virtualNetworks/subnets/write" , Microsoft.Network/routeTables/join/action" ,	启用 VNet 服务端点以进行数据分层。
"Microsoft.Resources/deployments/operations/read" 、 "Microsoft.Resources/deployments/read" 、 "Microsoft.Resources/deployments/write" 、	从模板部署 Cloud Volumes ONTAP 。
"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/write" ,	为 Cloud Volumes ONTAP 创建和管理资源组。
Microsoft.Compute/snapshots/write" , Microsoft.Compute/snapshots/read" , Microsoft.Compute/snapshots/delete" , Microsoft.Compute/disks/beginGetAccess/action" ,	创建和管理 Azure 管理的快照。
"microsoft.compute/availabilitysets/write" 、 "microsoft.compute/availabilitysets/read" 、	创建和管理 Cloud Volumes ONTAP 的可用性集。
"Microsoft.Marketplace/订购 / 服务类型 / 发布者 / 服务 / 计划 / 协议 / 读取 " 、 "Microsoft.Marketplace/订购 / 服务类型 / 发布者 / 服务 / 计划 / 协议 / 写入 "	支持从 Azure Marketplace 进行编程部署。

操作	目的
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/frontendIPConfigurations/read" , Microsoft.Network/loadBalancers/loadBalancingRules/read" , Microsoft.Network/loadBalancers/probes/read" , Microsoft.Network/loadBalancers/probes/join/action" , ,	管理 HA 对的 Azure 负载均衡器。
"Microsoft.Authorization/Locks/*"	支持管理 Azure 磁盘上的锁定。
"microsoft.Authorization/roleDefinitions/write" , "microsoft.Authorization/roleAssignments/write" , "microsoft.Web/sites/*"	管理 HA 对的故障转移。
Microsoft.Network/privateEndpoints/write" , "microsoft.Storage/storageAccounts/PrivateEndpointConnectionsApproval/Actions" , "microsoft.Storage/storageAccounts/privateEndpointConnections/Read" , 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" ,	用于管理私有端点。如果未向子网外部提供连接,则会使用私有端点。Cloud Manager 会为 HA 创建存储帐户,但子网中只有内部连接。
" Microsoft.NetApp/netAppAccounts/capacityPools/volumes/delete" ,	允许 Cloud Manager 删除 Azure NetApp Files 的卷。
"microsoft.resources/deployments/operationStatuss/Read"	Azure 在某些虚拟机部署中需要此权限(取决于部署期间使用的底层物理硬件)。
"microsoft.resources/deployments/operationStatuss/Read" , "microsoft.Insights / Metrics /Read" , Microsoft.Compute/virtualMachines/extensions/write" , , Microsoft.Compute/virtualMachines/extensions/read" , , Microsoft.Compute/virtualMachines/extensions/delete" , Microsoft.Compute/virtualMachines/delete" , Microsoft.Network/networkInterfaces/delete" , Microsoft.Network/networkSecurityGroups/delete" , "Microsoft 。 resources/deployments/delete" ,	用于使用全局文件缓存。

操作	目的
Microsoft.Network/privateEndpoints/delete" , Microsoft.Compute/availabilitySets/delete" ,	允许 Cloud Manager 在部署失败或删除时从属于 Cloud Volumes ONTAP 的资源组中删除资源。
Microsoft.Compute/diskEncryptionSets/read" Microsoft.Compute/diskEncryptionSets/write" , Microsoft.Compute/diskEncryptionSets/delete" "microsoft.KeyVault/vaults/deploy/action" , "microsoft.KeyVault/vaults/read" , "microsoft.KeyVault/vaults/accessPolicies/write" ,	支持将客户管理的加密密钥与 Cloud Volumes ONTAP 结合使用。使用 API 支持此功能。
"microsoft.resources/tags /read" , "microsoft.resources/tags /write" , "microsoft.resources/tags /delete"	用于使用 Cloud Manager 标记服务管理 Azure 资源上的标记。
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"	通过 Cloud Manager 可以为 HA 对配置应用程序安全组，从而隔离 HA 互连和集群网络 NIC 。

## 适用于 Connector 的 Google Cloud 权限

Cloud Manager需要在Google Cloud中执行操作的权限。这些权限包含在NetApp提供的自定义角色中。您可能希望了解 Cloud Manager 使用这些权限执行的操作。

### 服务帐户权限

下面显示的自定义角色提供了Connector在Google Cloud网络中管理资源和进程所需的权限。

您需要将此自定义角色应用于连接到Connector VM的服务帐户。"查看分步说明"。

您还需要确保角色是最新的、因为在后续版本中添加了新权限。

```

title: NetApp Cloud Manager
description: Permissions for the service account associated with the
Connector 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.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

## 如何使用Google Cloud权限

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.v防火墙 创建— compute.firewalls.delete — compute.v防火墙 .get — compute.v防火墙 列表	为 Cloud Volumes ONTAP 创建防火墙规则。
— compute.globalOperations.get	以获取操作状态。
— compute.images.get — compute.images.getFromFamily — compute.images.list — compute.images.useReadOnly	为 VM 实例获取映像。
— compute.instances.attachDisk — compute.instances.detachDisk	将磁盘连接和断开与 Cloud Volumes ONTAP 的连接。
— compute.instances.create — compute.instances.delete	创建和删除 Cloud Volumes ONTAP VM 实例。
— compute.instances.get	列出 VM 实例。
— compute.instances.getSerialPortOutput	以获取控制台日志。
— compute.instances.list	检索区域中实例的列表。
— compute.instances.setDeletionProtection	为实例设置删除保护。
— compute.instances.setLabels	以添加标签。
— compute.instances.setMachineType — compute.instances.setMinCpuPlatform	更改 Cloud Volumes ONTAP 的计算机类型。
— compute.instances.setMetadata	以添加元数据。
— compute.instances.setTags	为防火墙规则添加标记。
— compute.instances.start — compute.instances.stop — compute.instances.updateDisplayDevice	启动和停止 Cloud Volumes ONTAP 。
— compute.machineTypes.get	获取要检查 qoutas 的核心数。
— compute.projects.get	以支持多个项目。
— compute.snapshots.create — compute.snapshots.delete — compute.snapshots.get — compute.snapshots.list — compute.snapshots.setLabels	创建和管理永久性磁盘快照。
— compute.networks.get — compute.networks.list — compute.regions.get — compute.regions.list — compute.subnetworks.get — compute.subnetworks.list — compute.zoneOperations.get — compute.zones.get — compute.zones.list	获取创建新 Cloud Volumes ONTAP 虚拟机实例所需的网络信息。

操作	目的
- 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.resources.get - deploymentmanager.resources.list - deploymentmanager.typeProvider.get - deploymentmanager.typeProvider.get - deploymentmanager.typeProvider.list - get	使用 Google Cloud 部署管理器部署 Cloud Volumes ONTAP 虚拟机实例。
— logging.logEntries.list — logging.privateLogEntries.list	获取堆栈日志驱动器。
— resourceManager.projects.get	以支持多个项目。
— 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 存储分段。
— cloudkms.cryptoKeyVersions.useToEncrypt — cloudkms.encryptKeys.get — cloudkms.encryptKeys.list — cloudkms.keyrings.list	将云密钥管理服务中由客户管理的加密密钥与 Cloud Volumes ONTAP 结合使用。
— 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 存储分段的权限。
— compute.addresses ... list — compute.backendServices.create — compute.networks.updatePolicy — compute.regionBackendServices.create — compute.regionBackendServices.get — compute.regionBackendServices.list	部署 HA 对。
— compute.subnetworks.use — compute.subnetworks.useExternalIp — compute.instances.addAccessConfig	启用 Cloud Data sense 。
— container.clusters 。 get — container.clusters 。 list	发现在 Google Kubernetes Engine 中运行的 Kubernetes 集群。
—compute.instanceGroups.get—compute.addresses 。 get	在HA对上创建和管理Storage VM。

# 知识和支持

## 注册以获得支持

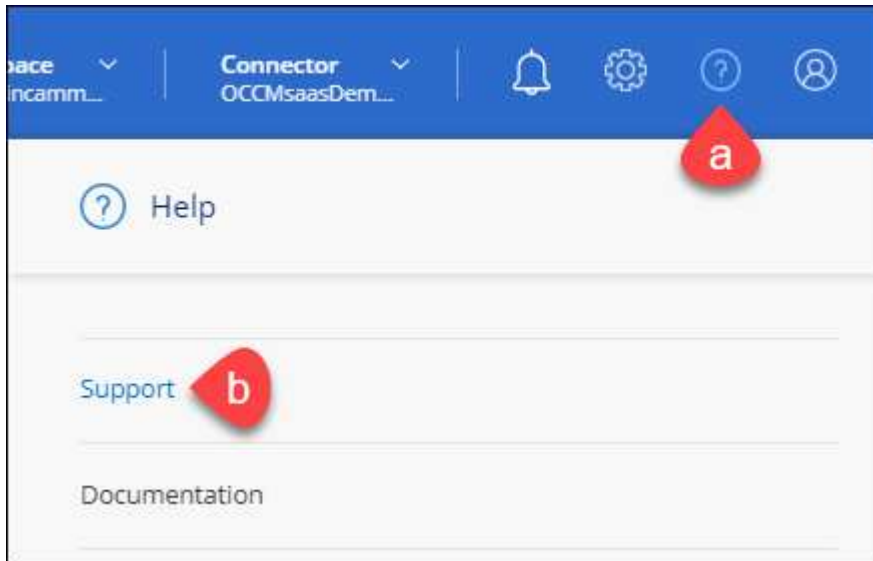
在向 NetApp 技术支持创建支持案例之前，您需要先将 NetApp 支持站点帐户添加到 Cloud Manager 中，然后注册获取支持。

### 添加 NSS 帐户

通过支持信息板，您可以从一个位置添加和管理所有 NetApp 支持站点帐户。

#### 步骤

1. 如果您还没有 NetApp 支持站点帐户，["注册一个"](#)。
2. 在 Cloud Manager 控制台右上角，单击帮助图标，然后选择 \* 支持 \*。



3. 单击 \* NSS 管理 > 添加 NSS 帐户 \*。
4. 出现提示时，单击 \* 继续 \* 以重定向到 Microsoft 登录页面。

NetApp 使用 Microsoft Azure Active Directory 作为身份提供程序来提供特定于支持和许可的身份验证服务。

5. 在登录页面上，提供 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。

此操作可使 Cloud Manager 使用您的 NSS 帐户。

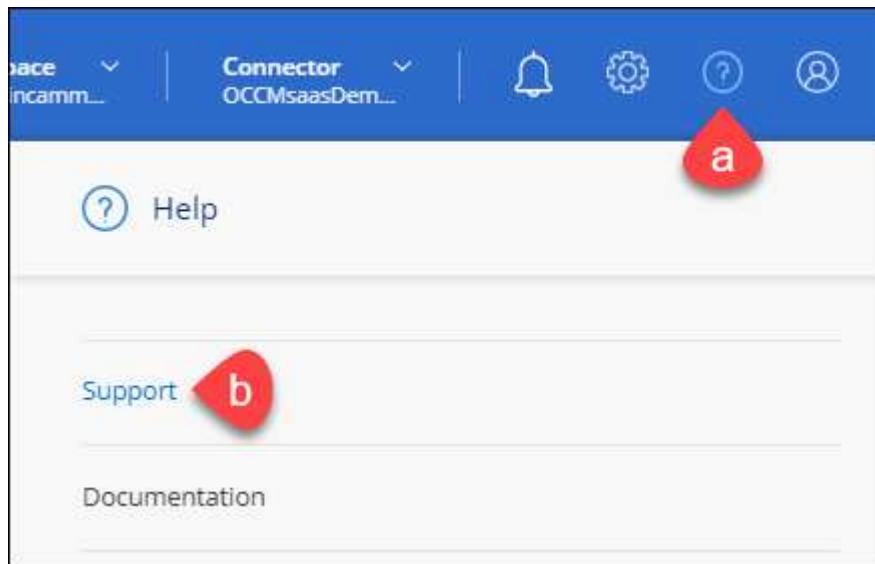
请注意，此帐户必须是客户级别的帐户（而不是来宾或临时帐户）。

### 注册您的帐户以获得支持

支持注册可从 Cloud Manager 的支持信息板中获取。

#### 步骤

1. 在 Cloud Manager 控制台右上角，单击帮助图标，然后选择 \* 支持 \*。



2. 在 \* 资源 \* 选项卡中，单击 \* 注册支持 \*。
3. 选择要注册的 NSS 凭据，然后单击 \* 注册 \*。

## 获取帮助

NetApp 通过多种方式为 Cloud Manager 及其云服务提供支持。全天候提供丰富的免费自助支持选项，例如知识库（KB）文章和社区论坛。您的支持注册包括通过 Web 服务单提供的远程技术支持。

### 自助支持

这些选项每周 7 天，每天 24 小时免费提供：

- ["知识库"](#)

通过 Cloud Manager 知识库搜索，查找有助于解决问题的文章。

- ["社区"](#)

加入 Cloud Manager 社区，关注正在进行的讨论或创建新的讨论。

- 文档。

您当前正在查看的 Cloud Manager 文档。

- [mailto: ng-cloudmanager-feedback@netapp.com](mailto:ng-cloudmanager-feedback@netapp.com)（反馈电子邮件）

我们非常重视您的反馈意见。提交反馈以帮助我们改进 Cloud Manager。

### NetApp 支持

除了上述自助支持选项之外，您还可以在激活支持后与 NetApp 支持工程师合作解决任何问题。

## 步骤

1. 在 Cloud Manager 中，单击 \* 帮助 > 支持 \*。
2. 在 "Technical Support" 下选择一个可用选项：
  - a. 单击 \* 致电我们 \* 可查找 NetApp 技术支持的电话号码。
  - b. 单击 \* 打开问题描述 \*，选择一个选项，然后单击 \* 发送 \*。

NetApp 代表将审核您的案例，并尽快与您联系。

# 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

<http://www.netapp.com/us/legal/copyright.aspx>

## 商标

NetApp、NetApp 徽标和 NetApp 商标页面上列出的标记是 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。

<http://www.netapp.com/us/legal/netapptmlist.aspx>

## 专利

有关 NetApp 拥有的专利的最新列表，请访问：

<https://www.netapp.com/us/media/patents-page.pdf>

## 隐私政策

<https://www.netapp.com/us/legal/privacypolicy/index.aspx>

## 开放源代码

通知文件提供有关 NetApp 软件中使用的第三方版权和许可证的信息。

- "有关 Cloud Manager 3.9 的注意事项"

## 版权信息

版权所有©2022 NetApp、Inc.。保留所有权利。Printed in the U.S.版权所涵盖的本文档的任何部分不得以任何形式或任何手段复制、包括影印、录制、磁带或存储在电子检索系统中—未经版权所有者事先书面许可。

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

本软件由NetApp按"原样"提供、不含任何明示或默示担保、包括但不限于适销性和特定用途适用性的默示担保、特此声明不承担任何任何责任。IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

## 商标信息

NetApp、NetApp标识和中列出的标记 <http://www.netapp.com/TM> 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。