



# Cloud Manager 和 Cloud Volumes ONTAP 文档

## Cloud Manager 3.7

NetApp  
March 25, 2024

# 目录

Cloud Manager 和 Cloud Volumes ONTAP 文档	1
BlueXP	1
了解新增功能	1
入门	1
通过 API 实现自动化	1
与同行建立联系、获得帮助并查找更多信息	1
发行说明	2
云管理器	2
概念	11
Cloud Manager 和 Cloud Volumes ONTAP 概述	11
NetApp Cloud Central	12
Cloud Central 帐户	13
云提供商帐户	18
存储	23
高可用性对	31
评估	39
许可	39
安全性	40
性能	42
入门	43
部署概述	43
AWS 中的 Cloud Volumes ONTAP 入门	44
开始在 Azure 中使用 Cloud Volumes ONTAP	46
在 Google 云平台中开始使用 Cloud Volumes ONTAP	47
设置 Cloud Manager	49
网络要求	69
其他部署选项	85
保持 Cloud Manager 正常运行	98
部署 Cloud Volumes ONTAP	99
在创建 Cloud Volumes ONTAP 系统之前	99
登录到 Cloud Manager	99
规划 Cloud Volumes ONTAP 配置	100
正在查找 Cloud Manager 系统 ID	106
在 Cloud Volumes ONTAP 上启用 Flash Cache	106
在 AWS 中启动 Cloud Volumes ONTAP	107
在 Azure 中启动 Cloud Volumes ONTAP	117
在 GCP 中启动 Cloud Volumes ONTAP	121
注册按需购买的系统	124
设置 Cloud Volumes ONTAP	125

配置存储	127
配置存储	127
将非活动数据分层到低成本对象存储	131
使用 ONTAP 作为 Kubernetes 的永久性存储	135
使用 NetApp 卷加密对卷进行加密	137
管理现有存储	138
复制和保护数据	145
发现和管理 ONTAP 集群	145
在系统之间复制数据	146
将数据备份到 Amazon S3	153
正在将数据同步到 Amazon S3	162
深入了解数据隐私	165
了解云合规性	165
Cloud Volumes ONTAP 云合规性入门	168
获得私有数据的可见性和控制权	173
查看隐私风险评估报告	180
响应数据主体访问请求	182
禁用 Cloud Compliance	183
有关云合规性的常见问题解答	184
管理 Cloud Volumes ONTAP	188
连接到 Cloud Volumes ONTAP	188
更新 Cloud Volumes ONTAP 软件	189
修改 Cloud Volumes ONTAP 系统	194
管理 Cloud Volumes ONTAP 的状态	200
监控 AWS 资源成本	201
提高防范勒索软件的能力	202
将现有 Cloud Volumes ONTAP 系统添加到 Cloud Manager	203
删除 Cloud Volumes ONTAP 工作环境	203
管理 Cloud Manager	205
更新 Cloud Manager	205
在 Cloud Central 帐户中管理工作空间和用户	206
删除 Cloud Volumes ONTAP 工作环境	209
配置 Cloud Manager 以使用代理服务器	210
续订 Cloud Manager HTTPS 证书	210
正在还原 Cloud Manager	211
卸载 Cloud Manager	211
为文件服务配置卷	212
管理 Azure NetApp Files 的卷	212
管理适用于 AWS 的 Cloud Volumes Service	216
API 和自动化	221
基础架构即代码自动化示例	221

- 参考 ..... 222
  - 常见问题：将 Cloud Manager 与 NetApp Cloud Central 集成 ..... 222
  - AWS 的安全组规则 ..... 223
  - Azure 的安全组规则 ..... 229
  - GCP 的防火墙规则 ..... 235
  - 适用于 Cloud Manager 和 Cloud Volumes ONTAP 的 AWS Marketplace 页面 ..... 240
  - Cloud Manager 如何使用云提供商权限 ..... 241
  - 默认配置 ..... 246
  - 角色 ..... 250
  - 从何处获取帮助和查找更多信息 ..... 250
- 早期版本的 Cloud Manager 文档 ..... 253
- 法律声明 ..... 254
  - 版权 ..... 254
  - 商标 ..... 254
  - 专利 ..... 254
  - 隐私政策 ..... 254
  - 开放源代码 ..... 254

# Cloud Manager 和 Cloud Volumes ONTAP 文档

您可以通过 Cloud Manager 部署和管理 NetApp Cloud Volumes ONTAP，NetApp 解决方案是一种数据管理，可为基于云的工作负载提供保护，可见性和控制。

## BlueXP

NetApp BlueXP 扩展并增强了 Cloud Manager 提供的功能。

["转到 BlueXP 文档"](#)

## 了解新增功能

- ["Cloud Manager 中的新增功能"](#)
- ["Cloud Volumes ONTAP 中的新增功能"](#)

## 入门

- ["在 AWS 中入门"](#)
- ["在 Azure 开始"](#)
- ["开始使用 Google Cloud Platform"](#)
- ["查找支持的 Cloud Volumes ONTAP 配置"](#)
- ["查看 Cloud Manager 的网络要求"](#)
- ["查看 Cloud Volumes ONTAP for AWS 的网络要求"](#)
- ["查看 Cloud Volumes ONTAP for Azure 的网络要求"](#)
- ["查看适用于 GCP 的 Cloud Volumes ONTAP 的网络要求"](#)
- ["规划您的 Cloud Volumes ONTAP 配置"](#)

## 通过 API 实现自动化

- ["API 开发人员指南"](#)
- ["自动化示例"](#)

## 与同行建立联系、获得帮助并查找更多信息

- ["NetApp 社区：云数据服务"](#)
- ["NetApp Cloud Volumes ONTAP 支持"](#)
- ["从何处获取帮助和查找更多信息"](#)

# 发行说明

## 云管理器

### Cloud Manager 3.7 中的新增功能

Cloud Manager 通常会每月推出一个新版本，为您提供新功能，增强功能和错误修复。



正在查找先前版本？["3.6 中的新增功能"](#)  
["3.5 中的新增功能"](#)  
["3.4 中的新增功能"](#)

### Cloud Manager 3.7.5 更新（2019 年 12 月 16 日）

此更新包括以下增强功能：

- [Cloud Volumes ONTAP 9.7](#)
- [适用于 Cloud Volumes ONTAP 的云合规性](#)

#### Cloud Volumes ONTAP 9.7

Cloud Volumes ONTAP 9.7 现已在 AWS，Azure 和 Google 云平台中推出。

["了解 Cloud Volumes ONTAP 9.7 中的新增功能"](#)。

适用于 **Cloud Volumes ONTAP** 的云合规性

云合规性是一项适用于 AWS 和 Azure 中 Cloud Volumes ONTAP 的数据隐私和合规服务。借助人工智能（AI）驱动的技术，云合规性可帮助企业了解数据环境并识别 Cloud Volumes ONTAP 系统中的敏感数据。

Cloud Compliance 目前作为受控可用性版本提供。

["了解有关云合规性的更多信息"](#)。

### Cloud Manager 3.7.5（2019 年 12 月 3 日）

Cloud Manager 3.7.5 包括以下增强功能。

- [GCP 中的 Cloud Volumes ONTAP 写入速度较快](#)
- [将内部 ONTAP 集群作为 Kubernetes 的永久性存储](#)
- [适用于 Kubernetes 的最新 Trident 版本](#)
- [支持 Azure 通用 v2 存储帐户](#)
- [使用 API 的 Azure 存储帐户名称中的前缀](#)

**GCP 中的 Cloud Volumes ONTAP 写入速度较快**

现在，您可以在 Google 云平台中对新的和现有的 Cloud Volumes ONTAP 系统启用高写入速度。如果工作负载

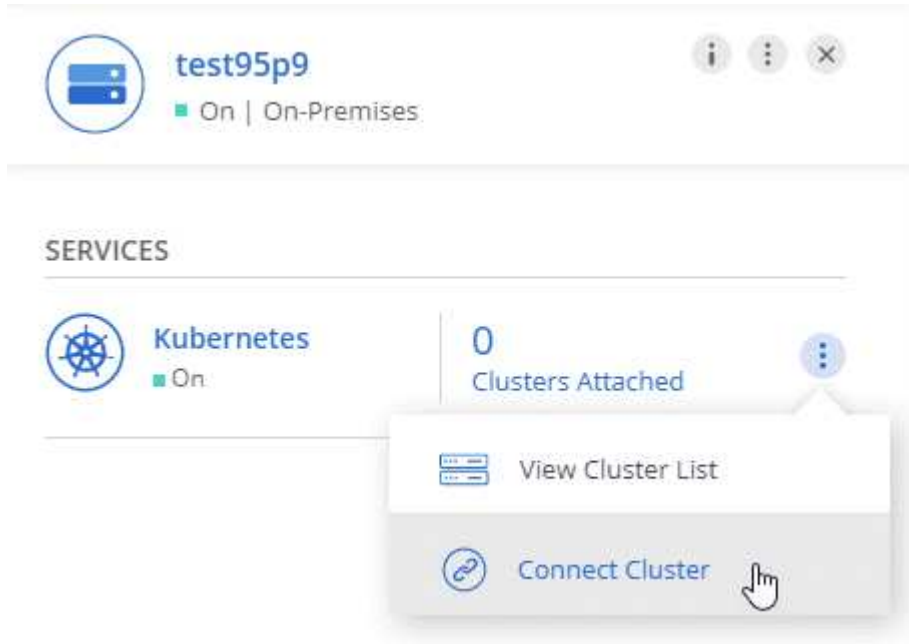
需要快速写入性能，则高写入速度是一个不错的选择。

- ["了解如何选择写入速度"](#)
- ["了解如何更改现有系统上的写入速度"](#)

将内部 **ONTAP** 集群作为 **Kubernetes** 的永久性存储

现在，您可以使用 Cloud Manager 将内部 ONTAP 集群用作容器的永久性存储。与 Cloud Volumes ONTAP 类似，Cloud Manager 可自动部署 NetApp Trident，并将 ONTAP 连接到 Kubernetes 集群。

将 Kubernetes 集群添加到 Cloud Manager 后，您可以从 "工作环境" 页面将其连接到内部 ONTAP 集群：



["了解如何开始使用"](#)。

适用于 **Kubernetes** 的最新 **Trident** 版本

现在，当您在工作环境连接到 Kubernetes 集群时，Cloud Manager 将安装最新版本的 Trident（版本 19.07.1）。

支持 **Azure** 通用 **v2** 存储帐户

在 Azure 中部署新的 Cloud Volumes ONTAP 系统时，Cloud Manager 为诊断和数据分层创建的存储帐户现已成为通用 v2 存储帐户。

使用 **API** 的 **Azure** 存储帐户名称中的前缀

现在，您可以为 Cloud Manager 为 Cloud Volumes ONTAP 创建的 Azure 存储帐户的名称添加前缀。在 Azure 中部署新 Cloud Volumes ONTAP 系统时，只需使用 `storageAccountPrefix` 参数即可。

["有关使用 API 的详细信息，请参见 API 开发人员指南"](#)。

## Cloud Manager 3.7.4 (2019 年 10 月 6 日)

Cloud Manager 3.7.4 包括以下增强功能。

- [支持 Azure NetApp Files](#)
- [适用于 GCP 的 Cloud Volumes ONTAP 增强功能](#)
- [备份到 S3 增强功能](#)
- [AWS 中的启动和根磁盘加密](#)
- [支持 AWS 巴林地区](#)
- [支持 Azure UAE 北部地区](#)

### 支持 Azure NetApp Files

现在，您可以直接从 Cloud Manager 查看和创建 Azure NetApp Files 的 NFS 卷。这一增强功能延续了我们的目标，即帮助您从一个界面管理云存储。

["了解如何开始使用"](#)。

此功能需要新的权限，如最新所示 ["适用于 Azure 的 Cloud Manager 策略"](#)。

```
"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"
```

### 适用于 GCP 的 Cloud Volumes ONTAP 增强功能

Cloud Manager 3.7.4 为 Cloud Volumes ONTAP for Google 云平台提供了以下增强功能：

#### GCP Marketplace 中的按需购买订阅

现在，您可以通过在 Google 云平台市场中订阅 Cloud Volumes ONTAP，随时为 Cloud Volumes ONTAP 付费。

["Google 云平台市场：适用于 Cloud Volumes ONTAP 的 Cloud Manager"](#)

#### 共享 VPC

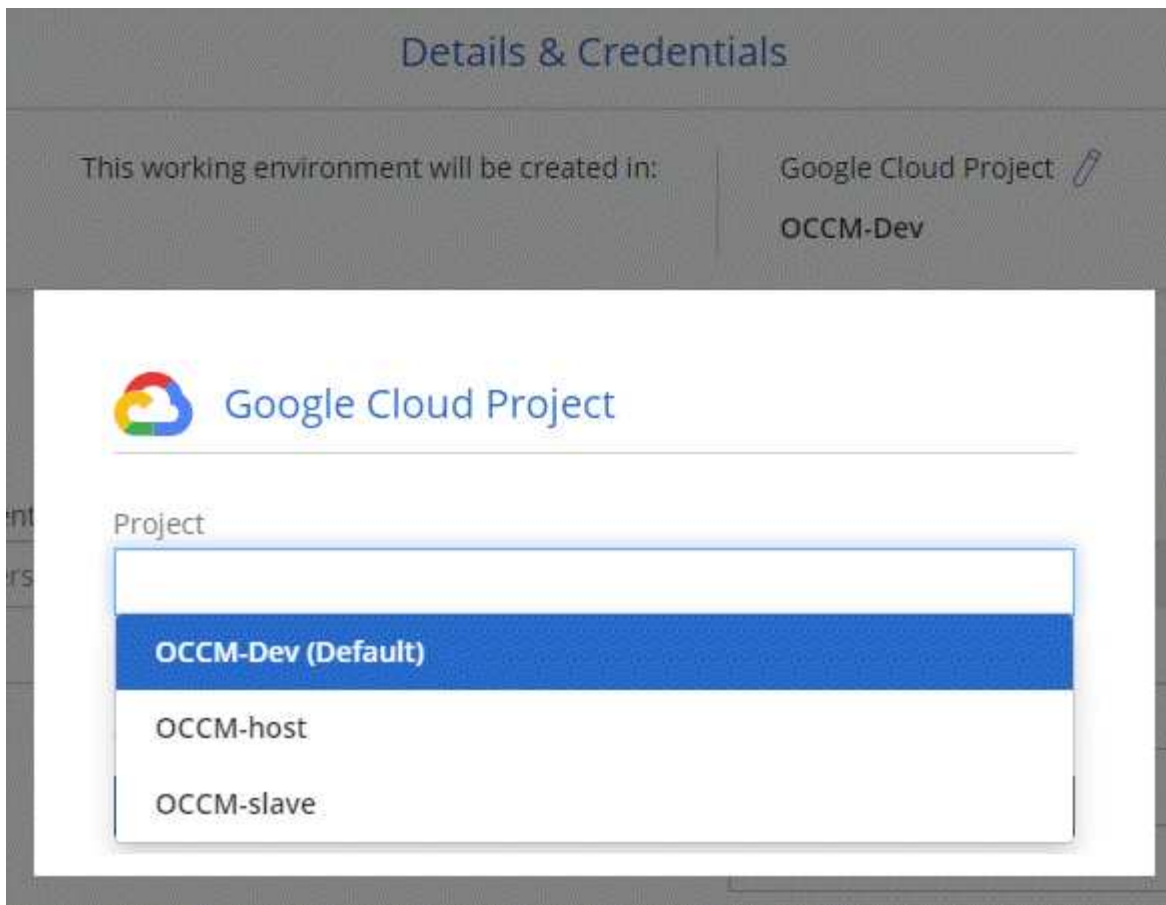
Cloud Manager 和 Cloud Volumes ONTAP 现在在 Google 云平台共享 VPC 中受支持。

通过共享 VPC，您可以跨多个项目配置和集中管理虚拟网络。您可以在 *host project* 中设置共享 VPC 网络，并在 *service project* 中部署 Cloud Manager 和 Cloud Volumes ONTAP 虚拟机实例。["Google Cloud 文档：共享 VPC 概述"](#)。

#### 多个 Google Cloud 项目

Cloud Volumes ONTAP 不再需要与 Cloud Manager 位于同一个项目中。将 Cloud Manager 服务帐户和角色添加到其他项目中，然后您可以从部署 Cloud Volumes ONTAP 的项目中进行选择。





有关设置 Cloud Manager 服务帐户的更多详细信息，["请参见此页面上的步骤 4b"](#)。

#### 使用 **Cloud Manager API** 时由客户管理的加密密钥

虽然 Google Cloud Storage 始终会在数据写入磁盘之前对数据进行加密，但您可以使用 Cloud Manager API 创建一个使用 *customer-managed encryption keys* 的新 Cloud Volumes ONTAP 系统。这些密钥可通过云密钥管理服务在 GCP 中生成和管理。

请参见 ["API 开发人员指南"](#) 有关使用 GCP 加密参数的详细信息。

此功能需要新的权限，如最新所示 ["适用于 GCP 的 Cloud Manager 策略"](#)：

- `cloudkms.cryptoKeyVersions.useToEncrypt`
- `cloudkms.cryptoKeys.get`
- `cloudkms.cryptoKeys.list`
- `cloudkms.keyRings.list`

#### 备份到 **S3** 增强功能

现在，您可以删除现有卷的备份。以前，您只能删除已删除卷的备份。

["了解有关备份到 S3 的更多信息"](#)。

## AWS 中的启动和根磁盘加密

使用 AWS 密钥管理服务（KMS）启用数据加密后，Cloud Volumes ONTAP 的启动磁盘和根磁盘也会进行加密。这包括 HA 对中调解器实例的启动磁盘。磁盘将使用您在创建工作环境时选择的 CMK 进行加密。



启动和根磁盘在 Azure 和 Google Cloud Platform 中始终加密，因为默认情况下，这些云提供商会启用加密。

### 支持 AWS 巴林地区

Cloud Manager 和 Cloud Volumes ONTAP 现在在 AWS 中东（巴林）地区受支持。

### 支持 Azure UAE 北部地区

Azure UAE 北部地区现在支持 Cloud Manager 和 Cloud Volumes ONTAP。

["查看所有受支持的区域"](#)。

## Cloud Manager 3.7.3 更新（2019 年 9 月 15 日）

现在，您可以使用 Cloud Manager 将数据从 Cloud Volumes ONTAP 备份到 Amazon S3。

### 备份到 S3

备份到 S3 是 Cloud Volumes ONTAP 的一项附加服务，可提供完全托管的备份和还原功能，以保护云数据并对其进行长期归档。备份存储在 S3 对象存储中，与用于近期恢复或克隆的卷 Snapshot 副本无关。

["了解如何开始使用"](#)。

此功能需要更新 ["Cloud Manager 策略"](#)。现在需要以下 VPC 端点权限：

```
"ec2:DescribeVpcEndpoints",  
"ec2:CreateVpcEndpoint",  
"ec2:ModifyVpcEndpoint",  
"ec2>DeleteVpcEndpoints"
```

## Cloud Manager 3.7.3（2019 年 9 月 11 日）

Cloud Manager 3.7.3 包括以下增强功能。

- [发现和适用于 AWS 的 Cloud Volumes Service](#)
- [AWS Marketplace 需要新订阅](#)
- [支持 AWS GovCloud（美国东部）](#)

### 发现和适用于 AWS 的 Cloud Volumes Service

现在，您可以通过 Cloud Manager 发现中的云卷 ["适用于 AWS 的 Cloud Volumes Service"](#) 订阅。发现后，您可以直接从 Cloud Manager 添加其他云卷。此增强功能提供了一个单一管理平台，您可以从中管理 NetApp 云存储。

["了解如何开始使用"](#)。

#### **AWS Marketplace 需要新订阅**

["AWS Marketplace 中提供了新订阅"](#)。要部署 Cloud Volumes ONTAP 9.6 PAYGO ，需要一次性订阅（30 天免费试用系统除外）。通过订阅，我们还可以为 Cloud Volumes ONTAP PAYGO 和 BYOL 提供附加功能。对于您创建的每个 Cloud Volumes ONTAP PAYGO 系统以及您启用的每个附加功能，此订阅将向您收取费用。

从 9.6 版开始，此新订阅方法将取代您先前为 Cloud Volumes ONTAP PAYGO 订阅的两个现有 AWS Marketplace 订阅。您仍需要通过订阅 ["部署 Cloud Volumes ONTAP BYOL 时的现有 AWS Marketplace 页面"](#)。

["了解有关每个 AWS Marketplace 页面的更多信息"](#)。

支持 **AWS GovCloud**（美国东部）

Cloud Manager 和 Cloud Volumes ONTAP 现在在 AWS GovCloud（美国东部）地区受支持。

#### **Cloud Volumes ONTAP 在 GCP 中全面上市（2019 年 9 月 3 日）**

现在，当您自带许可证（BYOL）时，Cloud Volumes ONTAP 在 Google 云平台（GCP）中普遍可用。此外，还提供按需购买促销。此促销活动为无限数量的系统提供免费许可证，有效期将于 2019 年 9 月底到期。

- ["了解如何开始使用 GCP"](#)
- ["查看支持的配置"](#)

#### **Cloud Manager 3.7.2（2019 年 8 月 5 日）**

- [FlexCache 许可证](#)
- [适用于 iSCSI 的 Kubernetes 存储类](#)
- [\[管理索引节点\]](#)
- [在 AWS 中为香港地区提供支持](#)
- [支持 Azure 中的澳大利亚中部地区](#)

#### **FlexCache 许可证**

现在，Cloud Manager 将为所有新的 Cloud Volumes ONTAP 系统生成 FlexCache 许可证。此许可证包含 500 GB 的使用量限制。

要生成许可证，Cloud Manager 需要访问 <https://ipa-signer.cloudmanager.netapp.com>。确保此 URL 可从防火墙访问。

#### **适用于 iSCSI 的 Kubernetes 存储类**

将 Cloud Volumes ONTAP 连接到 Kubernetes 集群时，Cloud Manager 现在还会创建两个 Kubernetes 存储类，可用于 iSCSI 永久性卷：

- \* netapp-file-san\*：用于将 iSCSI 永久性卷绑定到单节点 Cloud Volumes ONTAP 系统
- \* netapp-file-redunded-san-san：用于将 iSCSI 永久性卷绑定到 Cloud Volumes ONTAP HA 对

## 管理索引节点

Cloud Manager 现在可监控卷上的索引节点使用情况。使用 85% 的索引节点时，Cloud Manager 会增加卷的大小以增加可用索引节点的数量。卷可以包含的文件数取决于其包含的索引节点数。



只有在容量管理模式设置为自动（这是默认设置）时，Cloud Manager 才会监控索引节点使用量。

在 **AWS** 中为香港地区提供支持

Cloud Manager 和 Cloud Volumes ONTAP 现在在 AWS 的亚太地区（香港）地区受支持。

支持 **Azure** 中的澳大利亚中部地区

Cloud Manager 和 Cloud Volumes ONTAP 现在在以下 Azure 地区受支持：

- 澳大利亚中部
- 澳大利亚中部 2.

["请参见支持的区域的完整列表"](#)。

关于备份和还原的更新（**2019 年 7 月 15 日**）

从 3.7.1 版开始，Cloud Manager 不再支持下载备份并使用其还原 Cloud Manager 配置。"[您需要按照以下步骤还原 Cloud Manager](#)"。

**Cloud Manager 3.7.1**（**2019 年 7 月 1 日**）

- 此版本主要包含错误修复。
- 其中包括一项增强功能：Cloud Manager 现在可在向 NetApp 支持部门注册的每个 Cloud Volumes ONTAP 系统（新系统和现有系统）上安装 NetApp 卷加密（NVE）许可证。
  - ["将 NetApp 支持站点帐户添加到 Cloud Manager"](#)
  - ["注册按需购买的系统"](#)
  - ["设置 NetApp 卷加密"](#)



Cloud Manager 不会在位于中国地区的系统上安装 NVE 许可证。

**Cloud Manager 3.7 更新**（**2019 年 6 月 16 日**）

Cloud Volumes ONTAP 9.6 现已作为私有预览版在 AWS，Azure 和 Google 云平台中提供。要加入私有预览，请向 [ng-Cloud-Volume-ONTAP-preview@netapp.com](mailto:ng-Cloud-Volume-ONTAP-preview@netapp.com) 发送请求。

["了解 Cloud Volumes ONTAP 9.6 中的新增功能"](#)

**Cloud Manager 3.7**（**2019 年 6 月 5 日**）

- [支持即将发布的 Cloud Volumes ONTAP 9.6 版](#)
- [NetApp Cloud Central 帐户](#)

- [使用 Cloud Backup Service 进行备份和还原](#)

支持即将发布的 **Cloud Volumes ONTAP 9.6** 版

Cloud Manager 3.7 支持即将发布的 Cloud Volumes ONTAP 9.6 版。9.6 版在 Google 云平台中提供了 Cloud Volumes ONTAP 的私有预览。9.6 发布后，我们将更新发行说明。

#### NetApp Cloud Central 帐户

我们增强了您管理云资源的方式。每个 Cloud Manager 系统都将与一个 \_NetApp Cloud Central 帐户关联。该帐户支持多租户，并计划在未来用于其他 NetApp 云数据服务。

在 Cloud Manager 中，Cloud Central 帐户是 Cloud Manager 系统以及用户部署 Cloud Volumes ONTAP 的 \_workspace\_ 的容器。

["了解 Cloud Central 帐户如何支持多租户"](#)。



Cloud Manager 需要访问 { [https://cloudmanager.cloud.netapp.com\\_](https://cloudmanager.cloud.netapp.com_) } 才能连接到 Cloud Central 帐户服务。在防火墙上打开此 URL，以确保 Cloud Manager 可以联系此服务。

#### 将您的系统与 **Cloud Central** 帐户集成

升级到 Cloud Manager 3.7 后，NetApp 会选择特定的 Cloud Manager 系统与 Cloud Central 帐户集成。在此过程中，NetApp 会创建一个帐户，为每个用户分配新角色，创建工作空间并将现有工作环境放置在这些工作空间中。Cloud Volumes ONTAP 系统不会发生中断。

["如果您有任何疑问、请参阅此常见问题解答。"](#)

#### 使用 **Cloud Backup Service** 进行备份和还原

NetApp Cloud Backup Service for Cloud Volumes ONTAP 可提供完全托管的备份和还原功能，用于保护和长期归档云数据。您可以将 Cloud Backup Service 与适用于 AWS 的 Cloud Volumes ONTAP 集成。服务创建的备份存储在 AWS S3 对象存储中。

["了解有关 Cloud Backup Service 的更多信息"](#)。

要开始使用，请安装并配置备份代理，然后启动备份和还原操作。如果您需要帮助，我们建议您使用 Cloud Manager 中的聊天图标与我们联系。



不再支持此手动过程。在 3.7.3 版中，Cloud Manager 集成了备份到 S3 功能。

#### 已知问题

已知问题可确定可能妨碍您成功使用此版本产品的问题。

此版本的 Cloud Manager 中没有已知问题。

您可以在中找到 Cloud Volumes ONTAP 的已知问题 "[《Cloud Volumes ONTAP 发行说明》](#)" 和 ONTAP 软件的一般信息 "[《ONTAP 发行说明》](#)"。

## 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。

### Cloud Manager 应始终保持运行状态

Cloud Manager 是 Cloud Volumes ONTAP 运行状况和计费的关键组成部分。如果 Cloud Manager 已关闭，则在与 Cloud Manager 的通信中断 4 天以上后，Cloud Volumes ONTAP 系统将关闭。

### 不支持共享 Linux 主机

与其他应用程序共享的主机不支持 Cloud Manager。主机必须是专用主机。

### Cloud Manager 不支持 FlexGroup 卷

虽然 Cloud Volumes ONTAP 支持 FlexGroup 卷，但 Cloud Manager 不支持。如果您从 System Manager 或 CLI 创建 FlexGroup 卷，则应将 Cloud Manager 的容量管理模式设置为手动。对于 FlexGroup 卷，自动模式可能无法正常工作。

### 默认情况下，新安装的 Cloud Manager 不支持 Active Directory

从 3.4 版开始，Cloud Manager 的新安装不支持使用您组织的 Active Directory 身份验证进行用户管理。如果需要，NetApp 可以帮助您使用 Cloud Manager 设置 Active Directory。单击“云管理器”右下角的聊天图标以获得帮助。

### AWS Govcloud（美国）地区的限制

- 如果您要在 AWS 政府云（美国）地区启动 Cloud Volumes ONTAP 实例，则必须在 AWS 政府云（美国）地区部署 Cloud Manager。
- 当部署在 AWS 政府云（美国）区域时，Cloud Manager 无法在适用于 Microsoft Azure 配置的 NetApp 私有存储或适用于 SoftLayer 配置的 NetApp 私有存储中发现 ONTAP 集群。

### Cloud Manager 不设置 iSCSI 卷

使用 Storage System View 在 Cloud Manager 中创建卷时，可以选择 NFS 或 CIFS 协议。必须使用 OnCommand System Manager 为 iSCSI 创建卷。

### 存储虚拟机（SVM）限制

Cloud Volumes ONTAP 支持一个数据服务 SVM 和一个或多个用于灾难恢复的 SVM。一个提供数据的 SVM 跨整个 Cloud Volumes ONTAP 系统（HA 对或单个节点）。

Cloud Manager 不为 SVM 灾难恢复提供任何设置或业务流程支持。它也不支持在任何其他 SVM 上执行与存储相关的任务。必须使用 System Manager 或 CLI 进行 SVM 灾难恢复。

# 概念

## Cloud Manager 和 Cloud Volumes ONTAP 概述

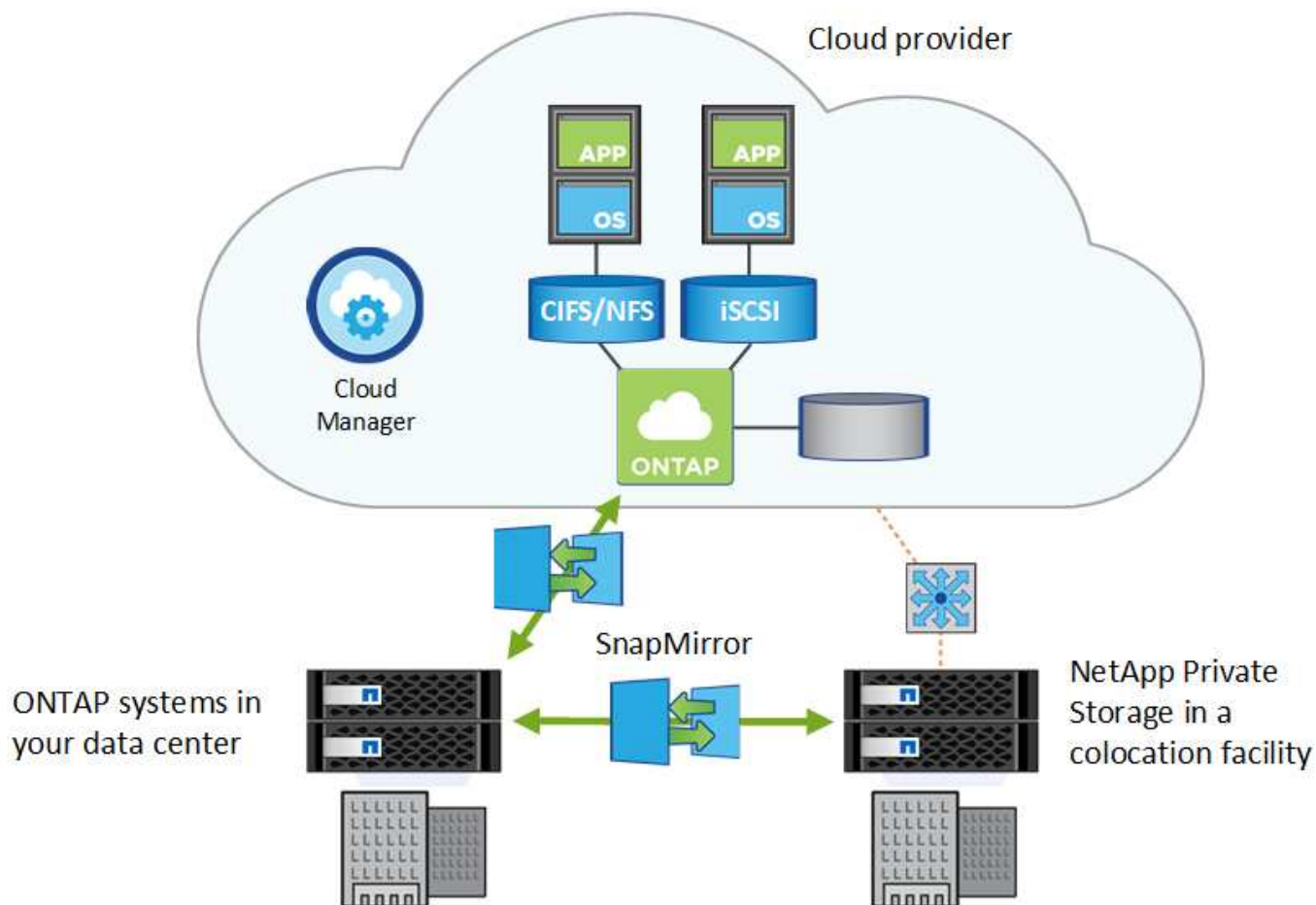
您可以通过 Cloud Manager 部署 Cloud Volumes ONTAP，为云存储提供企业级功能，并在基于 NetApp 的混合云之间轻松复制数据。

### 云管理器

构建云管理器时充分考虑了简单性。它可指导您完成 Cloud Volumes ONTAP 设置的几个步骤，通过简化存储配置和自动化容量管理简化数据管理，并支持在混合云中拖放数据复制等。

需要使用 Cloud Manager 来部署和管理 Cloud Volumes ONTAP，但它还可以发现并配置内部 ONTAP 集群的存储。这为您的云和内部存储基础架构提供了一个中央控制点。

您可以在云或网络中运行 Cloud Manager — 只需连接到要部署 Cloud Volumes ONTAP 的网络即可。下图显示了在云提供商中运行的 Cloud Manager 和 Cloud Volumes ONTAP。它还显示了跨混合云的数据复制。



["了解有关 Cloud Manager 的更多信息"](#)

### Cloud Volumes ONTAP

Cloud Volumes ONTAP 是一款纯软件存储设备、它在云中运行 ONTAP 数据管理软件。您可以将 Cloud

Volumes ONTAP 用于生产工作负载、灾难恢复、 DevOps 、文件共享和数据库管理。

Cloud Volumes ONTAP 通过以下关键功能将企业存储扩展到云：

- 存储效率利用内置的重复数据删除、数据压缩、精简配置和克隆来最大限度地降低存储成本。
- 高可用性可确保在云环境发生故障时企业级可靠性和持续运行。
- Data Replication Cloud Volumes ONTAP 利用 NetApp 行业领先的复制技术 SnapMirror 将内部数据复制到云中、以便在多个使用案例中轻松获得二级副本。
- 数据分层可按需在高性能存储池和低性能存储池之间切换，而无需使应用程序脱机。
- 应用程序一致性使用 NetApp SnapCenter 确保 NetApp Snapshot 副本的一致性。



Cloud Volumes ONTAP 中包含 ONTAP 功能的许可证。

["查看支持的 Cloud Volumes ONTAP 配置"](#)

["了解有关 Cloud Volumes ONTAP 的更多信息"](#)

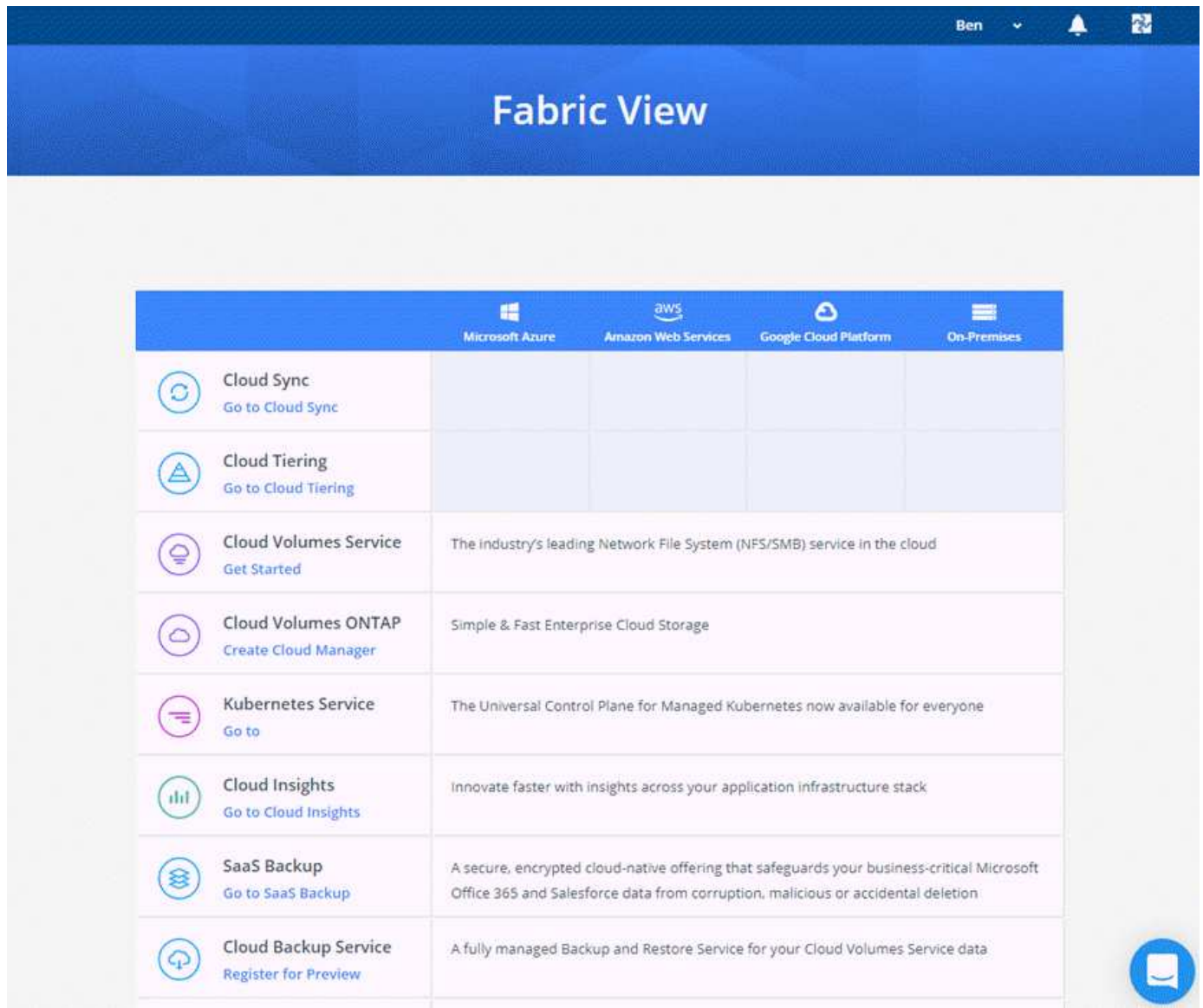
## NetApp Cloud Central

"NetApp Cloud Central" 提供一个中央位置，用于访问和管理 NetApp 云数据服务。这些服务使您能够在云中运行关键应用程序、创建自动化灾难恢复站点、备份 SaaS 数据、并在多个云中有效地迁移和控制数据。

Cloud Manager 与 NetApp Cloud Central 的集成提供了多种优势、包括简化的部署体验、查看和管理多个云管理系统的单一位置以及集中式用户身份验证。

通过集中式用户身份验证、您可以在云管理器系统之间以及云管理器与其他数据服务（如云同步）之间使用相同的凭据集。如果您忘记了密码、也可以轻松地重置密码。





## Cloud Central 帐户

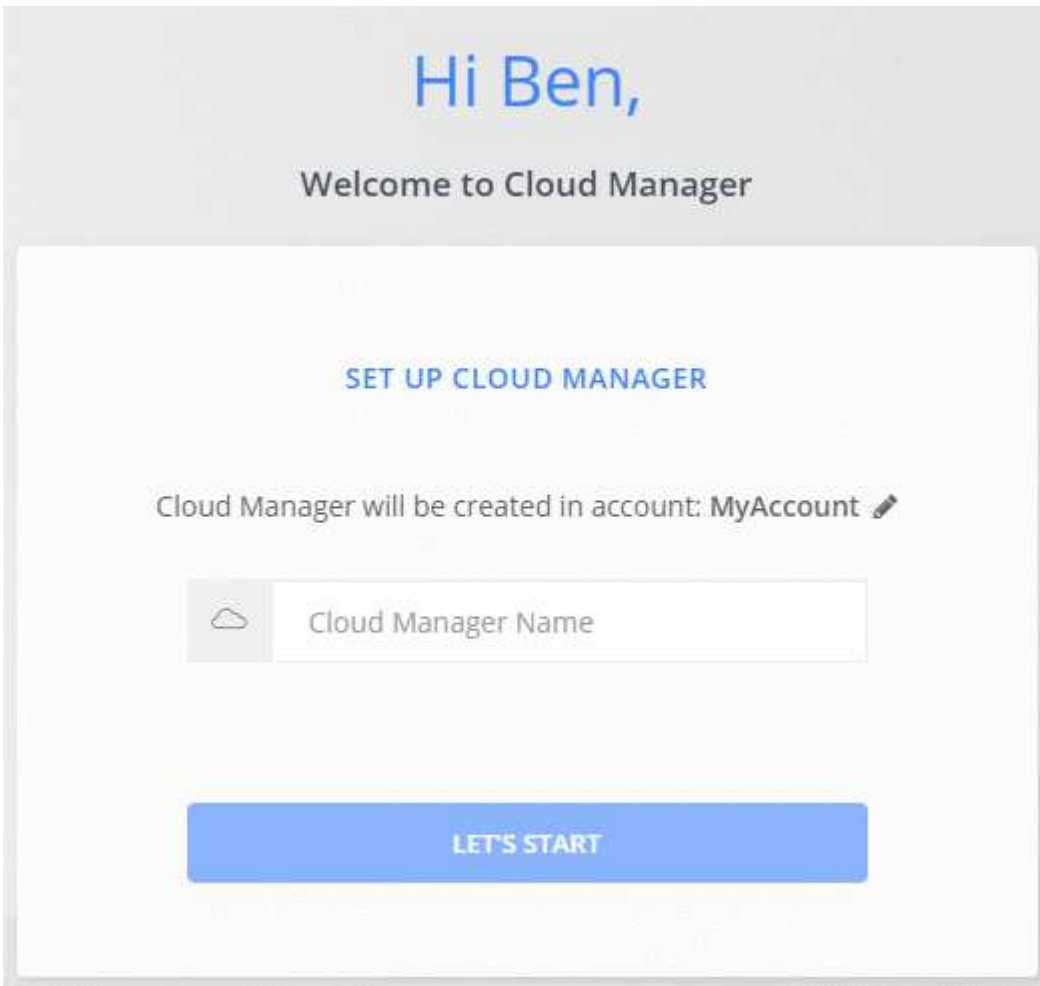
每个 Cloud Manager 系统都与一个 \_NetApp Cloud Central 帐户关联。Cloud Central 帐户可提供多租户功能，并可用于在隔离的工作空间中组织用户和资源。

Cloud Central 帐户支持多租户：

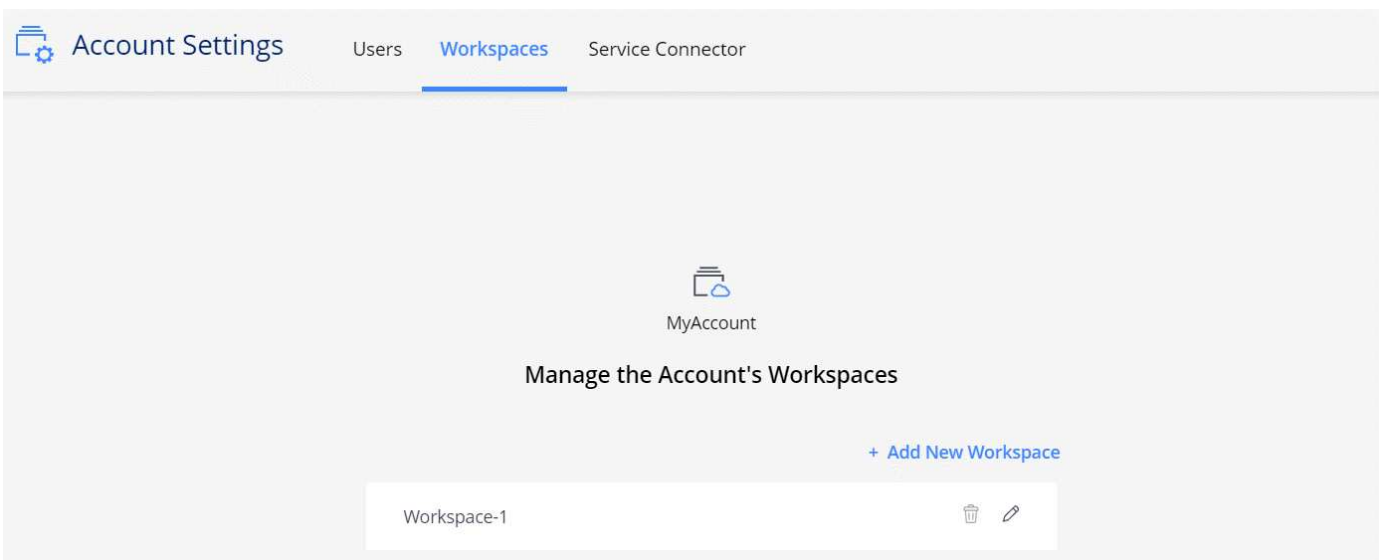
- 一个 Cloud Central 帐户可以包含多个 Cloud Manager 系统，以满足不同的业务需求。  
由于用户与 Cloud Central 帐户关联，因此无需为每个 Cloud Manager 系统配置用户。
- 在每个 Cloud Manager 系统中，多个用户可以在称为工作空间的隔离环境中部署和管理 Cloud Volumes ONTAP 系统。

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。

部署 Cloud Manager 时，您可以选择要与系统关联的 Cloud Central 帐户：



然后，帐户管理员可以通过管理用户，工作空间和服务连接器来修改此帐户的设置：



有关分步说明，请参见 "设置 Cloud Central 帐户"。



Cloud Manager 需要访问 { [https://cloudmanager.cloud.netapp.com\\_](https://cloudmanager.cloud.netapp.com_) } 才能连接到 Cloud Central 帐户服务。在防火墙上打开此 URL，以确保 Cloud Manager 可以联系此服务。

## 用户，工作空间和服务连接器

通过 Cloud Manager 中的 "Account Settings" 小工具，客户管理员可以管理 Cloud Central 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，工作空间和服务连接器。

### 用户

这些是您与 Cloud Central 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。

### 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

### 服务连接器

服务连接器是 Cloud Manager 的一部分。它可运行 Cloud Manager 软件的大部分内容（如用户界面），但它连接到的几个 Cloud Central 服务除外（*auth0* 和 Cloud Central 帐户）。服务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。

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

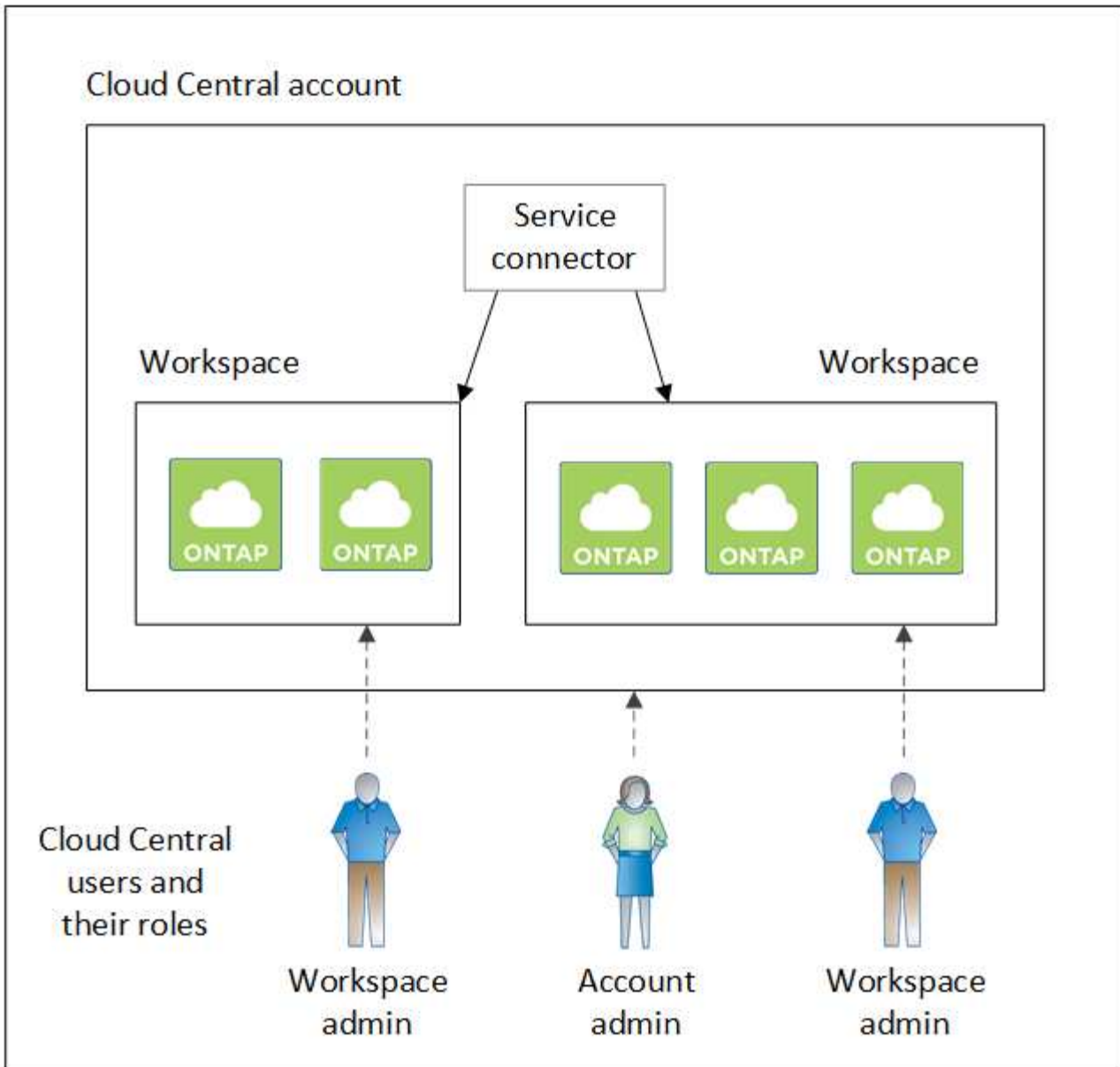
## 示例

以下示例显示了一个使用两个工作空间为 Cloud Volumes ONTAP 系统创建隔离环境的帐户。例如，一个工作空间可能用于暂存环境，而另一个工作空间则用于生产环境。



Cloud Manager 和 Cloud Volumes ONTAP 系统实际上并不驻留在 NetApp Cloud Central 帐户中——它们在云提供商中运行。这是每个组件之间关系的概念表示。

## NetApp Cloud Central

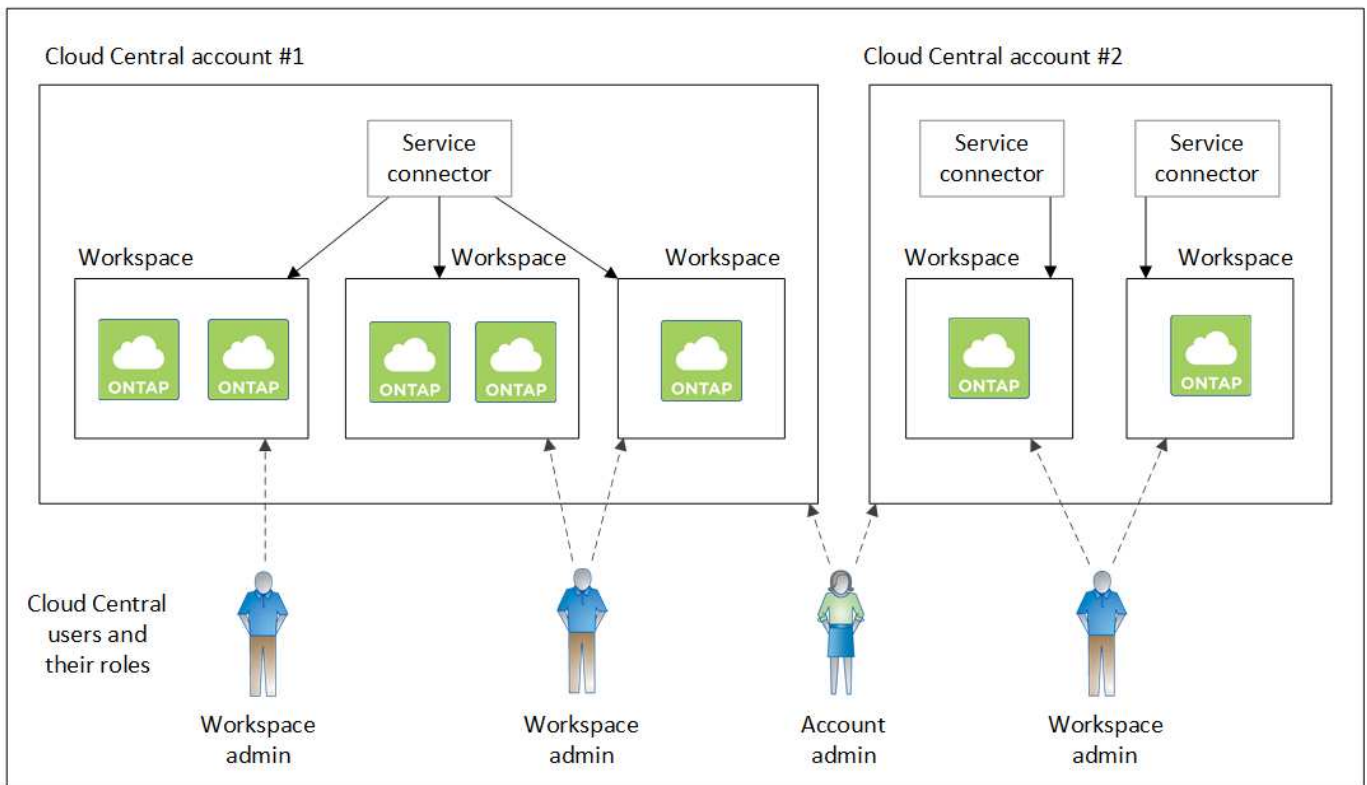


下面是另一个示例，通过使用两个单独的 Cloud Central 帐户显示了最高的多租户级别。例如，服务提供商可能会在一个 Cloud Central 帐户中使用 Cloud Manager 为其客户提供服务，而使用另一个帐户为其业务单位之一提供灾难恢复。

请注意，帐户 2 包含两个单独的服务连接器。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。



同样，Cloud Manager 和 Cloud Volumes ONTAP 系统实际上并不驻留在 NetApp Cloud Central 帐户中——它们在云提供商中运行。这是每个组件之间关系的概念表示。



## 与 Cloud Central 帐户集成的常见问题解答

升级到 Cloud Manager 3.7 后，NetApp 会选择特定的 Cloud Manager 系统与 Cloud Central 帐户集成。此常见问题解答可以回答您可能对流程提出的问题。

此过程需要多长时间？

只需几分钟。

**Cloud Manager** 是否不可用？

不可以，您仍然可以访问 Cloud Manager 系统。

**Cloud Volumes ONTAP** 如何？

Cloud Volumes ONTAP 系统不会发生中断。

在此过程中会发生什么情况？

NetApp 会在集成过程中执行以下操作：

1. 创建一个新的 Cloud Central 帐户并将其与您的 Cloud Manager 系统关联。
2. 为每个现有用户分配新角色：
  - Cloud Manager 管理员成为客户管理员
  - 租户管理员和工作环境管理员成为 Workspace 管理员

3. 创建用于替换现有租户的工作空间。
4. 将您的工作环境放置在这些工作空间中。
5. 将服务连接器与所有工作空间相关联。

我在哪里安装了 **Cloud Manager** 系统是否重要？

否无论系统位于 AWS ， Azure 还是您的内部， NetApp 都将与 Cloud Central 帐户集成。

## 云提供商帐户

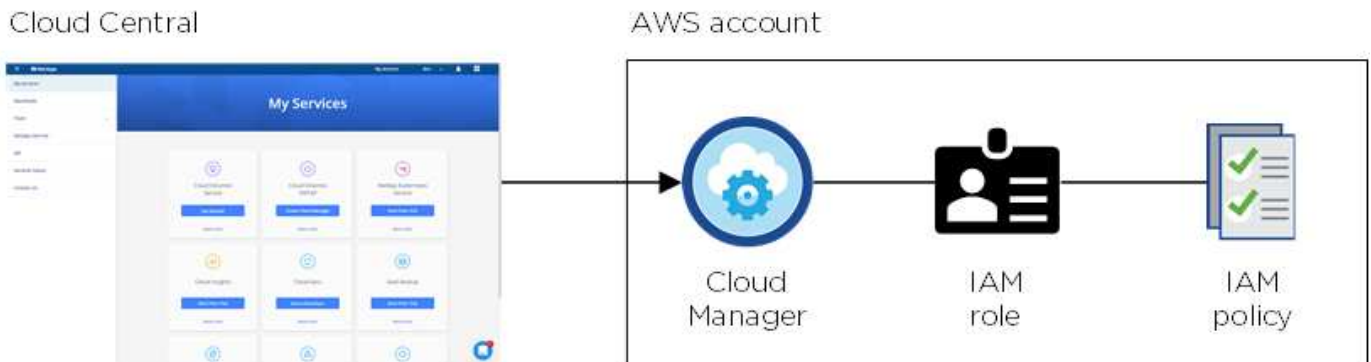
### AWS 帐户和权限

通过 Cloud Manager ，您可以选择要在其中部署 Cloud Volumes ONTAP 系统的 AWS 帐户。您可以在初始 AWS 帐户中部署所有 Cloud Volumes ONTAP 系统，也可以设置其他帐户。

#### 初始 AWS 帐户

从 NetApp Cloud Central 部署 Cloud Manager 时，您需要使用有权启动 Cloud Manager 实例的 AWS 帐户。中列出了所需的权限 ["适用于 AWS 的 NetApp Cloud Central 策略"](#)。

当 Cloud Central 在 AWS 中启动 Cloud Manager 实例时，它会为此实例创建 IAM 角色和实例配置文件。它还会附加一个策略，为 Cloud Manager 提供在该 AWS 帐户中部署和管理 Cloud Volumes ONTAP 的权限。 ["查看 Cloud Manager 如何使用权限"](#)。



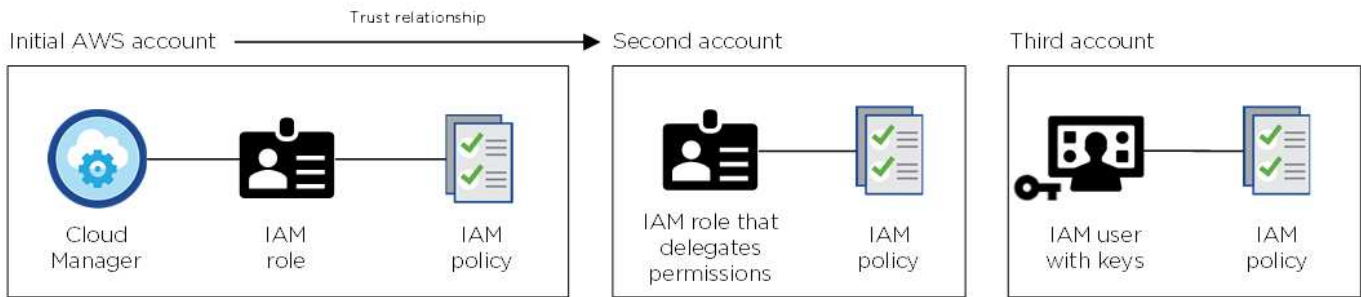
Cloud Manager 会在您创建新的工作环境时默认选择此云提供商帐户：

### Details & Credentials

This working environment will be created in Cloud Provider Account: **Instance Profile** | Account ID: XXXXXXXXXX | [Switch Account](#)

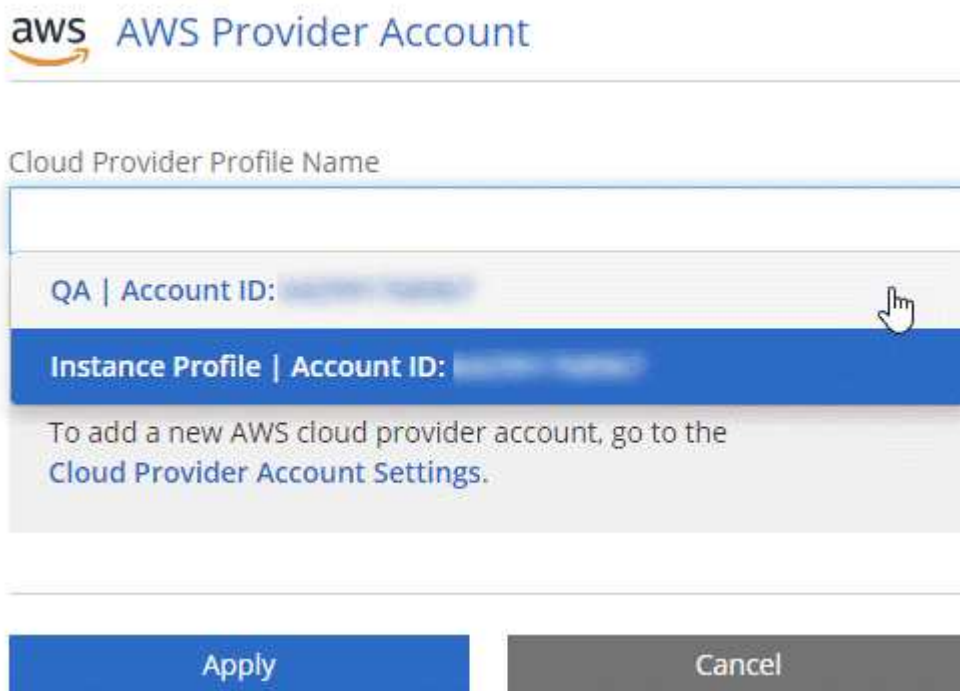
#### 其他 AWS 帐户

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 "将云提供商帐户添加到 Cloud Manager" 指定 IAM 角色的 Amazon 资源名称（ARN）或 IAM 用户的 AWS 密钥。

添加其他帐户后，您可以在创建新的工作环境时切换到该帐户：



### 市场部署和内部部署如何？

以上各节介绍了 NetApp Cloud Central 中建议的部署方法。您也可以从在 AWS 中部署 Cloud Manager "AWS Marketplace" 您可以做到 "在内部安装 Cloud Manager"。

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。

## Azure 帐户和权限

通过 Cloud Manager，您可以选择要在其中部署 Cloud Volumes ONTAP 系统的 Azure 帐户。您可以在初始 Azure 帐户中部署所有 Cloud Volumes ONTAP 系统，也可以设置其他帐户。

### 初始 Azure 帐户

从 NetApp Cloud Central 部署 Cloud Manager 时，您需要使用具有部署 Cloud Manager 虚拟机权限的 Azure 帐户。中列出了所需的权限 ["适用于 Azure 的 NetApp Cloud Central 策略"](#)。

当 Cloud Central 在 Azure 中部署 Cloud Manager 虚拟机时，它会启用 ["系统分配的受管身份"](#) 在 Cloud Manager 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 提供了在该 Azure 订阅中部署和管理 Cloud Volumes ONTAP 的权限。 ["查看 Cloud Manager 如何使用权限"](#)。



Cloud Manager 会在您创建新的工作环境时默认选择此云提供商帐户：

### Details & Credentials

This working environment will be created in Cloud Provider Account: Managed Service Identity | Azure Subscription: OCCM QA1 | [Switch Account](#)

### 初始帐户的其他 Azure 订阅

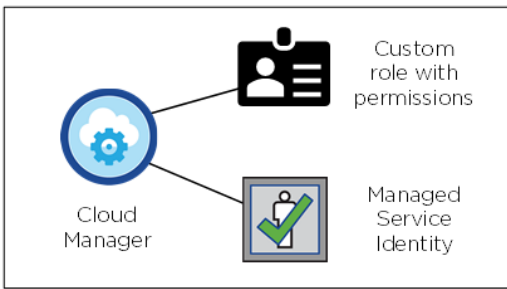
托管身份与您启动 Cloud Manager 的订阅相关联。如果要选择其他 Azure 订阅，则需要 ["将托管身份与这些订阅相关联"](#)。

### 其他 Azure 帐户

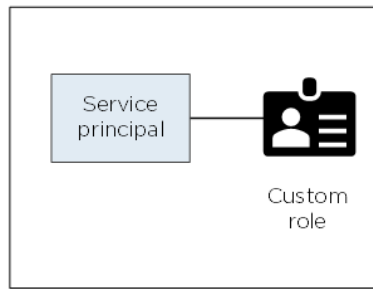
如果要在不同的 Azure 帐户中部署 Cloud Volumes ONTAP，则必须通过授予所需权限 ["在 Azure Active Directory 中创建和设置服务主体"](#) 对于每个 Azure 帐户。下图显示了另外两个帐户，每个帐户都设置有一个服务主体和一个提供权限的自定义角色：



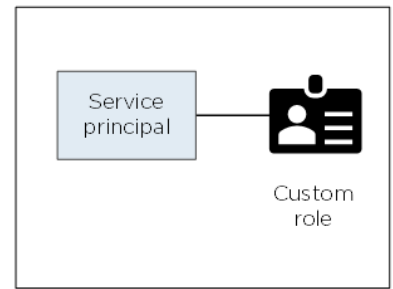
Initial Azure account



Second account



Third account



您可以这样做 "将云提供商帐户添加到 Cloud Manager" 提供有关 AD 服务主体的详细信息。

添加其他帐户后，您可以在创建新的工作环境时切换到该帐户：



## Microsoft Azure Provider Account

Cloud Provider Profile Name

Azure Keys | Application ID: [redacted] ...

Dev Keys | Application ID: [redacted] ...

**Managed Service Identity**

To add a new Azure cloud provider account, go to the [Cloud Provider Account Settings](#).

Apply

Cancel

### 市场部署和内部部署如何？

以上各节介绍了 NetApp Cloud Central 中建议的部署方法。您也可以从在 Azure 中部署 Cloud Manager "Azure Marketplace"，您可以 "在内部安装 Cloud Manager"。

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 Cloud Manager 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 Cloud Manager 系统设置托管身份，但可以像为其他帐户提供权限一样提供权限。

## Google Cloud 项目，权限和帐户

通过服务帐户，Cloud Manager 可以在与 Cloud Manager 相同的项目或不同的项目中部署和管理 Cloud Volumes ONTAP 系统。您添加到 Cloud Manager 的 Google Cloud 帐户用于启用数据分层。

### Cloud Manager 的项目和权限

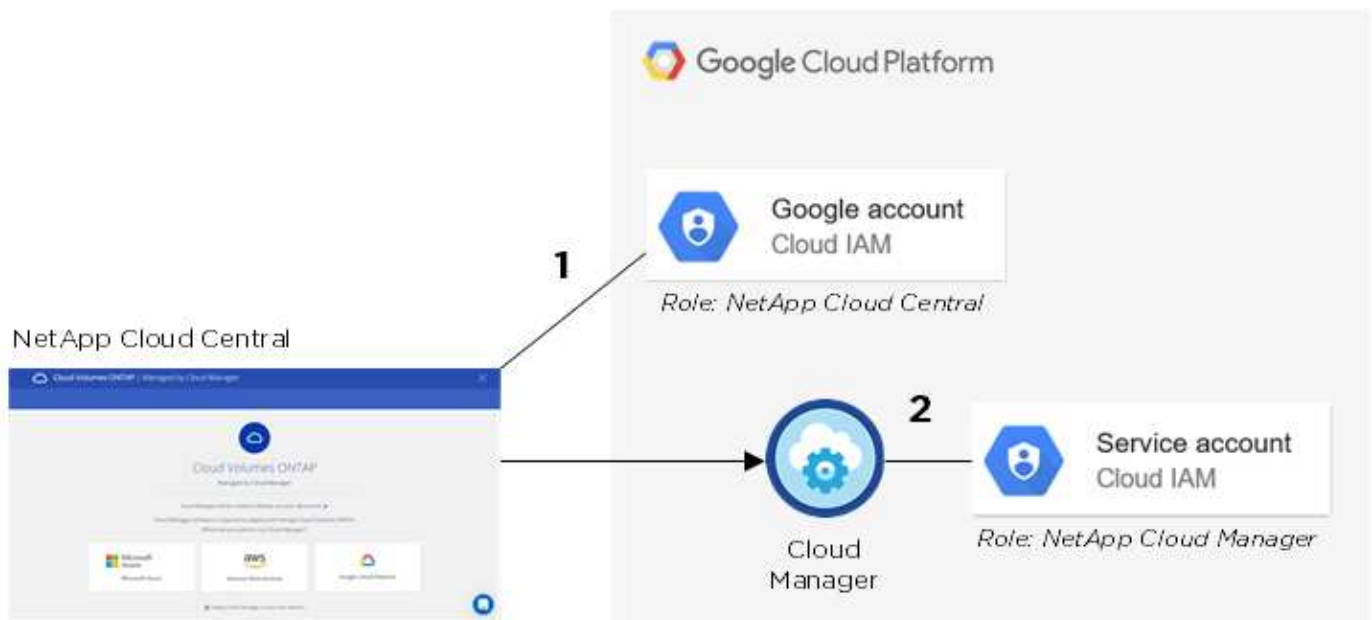
在 Google Cloud 中部署 Cloud Volumes ONTAP 之前，必须先在 Google Cloud 项目中部署 Cloud Manager。Cloud Manager 不能在您的内部环境或其他云提供商中运行。

在部署 Cloud Manager 之前，必须具有两组权限 "NetApp Cloud Central":

1. 您需要使用有权从 Cloud Central 启动 Cloud Manager VM 实例的 Google 帐户部署 Cloud Manager。
2. 部署 Cloud Manager 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 Cloud Manager 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 Cloud Manager 服务帐户和角色添加到该项目中。

- "了解如何设置 Cloud Manager 服务帐户 (请参见第 4 步)"。
- "了解如何在 GCP 中部署 Cloud Volumes ONTAP 并选择项目"。

### 数据分层的帐户

要在 Cloud Volumes ONTAP 系统上启用数据分层，需要向 Cloud Manager 添加 Google Cloud 帐户。数据分层

功能会自动将冷数据分层到低成本的对象存储，使您能够回收主存储上的空间并缩减二级存储。

添加帐户时，您需要为 Cloud Manager 提供具有存储管理员权限的服务帐户的存储访问密钥。Cloud Manager 可使用访问密钥设置和管理用于数据分层的云存储分段。

添加 Google Cloud 帐户后，您可以在创建，修改或复制单个卷时对其启用数据分层。

- "了解如何在 [Cloud Manager](#) 中设置和添加 GCP 帐户"。
- "了解如何将非活动数据分层到低成本对象存储"。

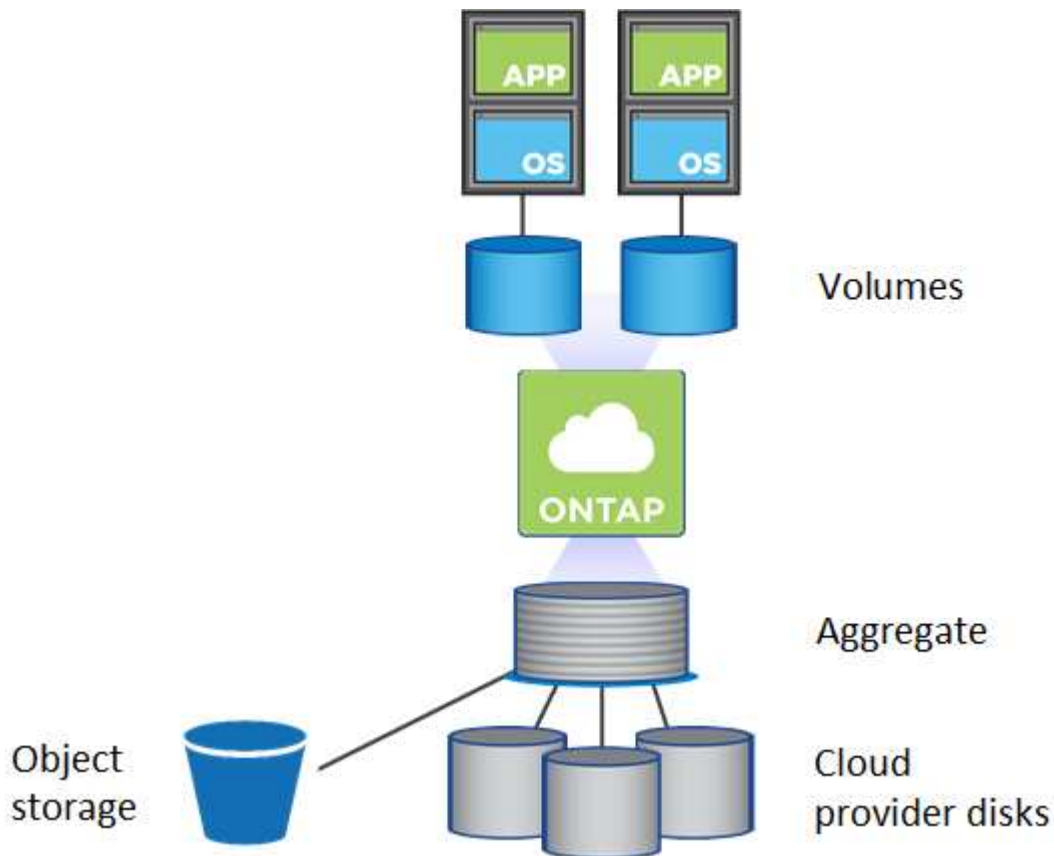
## 存储

### 磁盘和聚合

了解 Cloud Volumes ONTAP 如何使用云存储可以帮助您了解存储成本。

#### 概述

Cloud Volumes ONTAP 使用云提供商存储作为磁盘，并将其分组为一个或多个聚合。聚合可为一个或多个卷提供存储。



支持多种类型的云磁盘。您可以在创建卷时选择磁盘类型，在部署 Cloud Volumes ONTAP 时选择默认磁盘大小。



从云提供商购买的存储总量为 *raw capacity*。可用容量\_较小，因为预留给 Cloud Volumes ONTAP 使用的开销约为 12 到 14%。例如，如果 Cloud Manager 创建了一个 500 GB 聚合、则可用容量为 442.94 GB。

## AWS 存储

在 AWS 中，Cloud Volumes ONTAP 将 EBS 存储用于用户数据，并将本地 NVMe 存储用作某些 EC2 实例类型的 Flash Cache。

### EBS 存储

在 AWS 中，一个聚合最多可以包含 6 个大小相同的磁盘。最大磁盘大小为 16 TB。

底层 EBS 磁盘类型可以是通用 SSD、配置的 IOPS SSD、吞吐量优化 HDD 或冷 HDD。您可以将 EBS 磁盘与 Amazon S3 配对 "[将非活动数据分层到低成本对象存储](#)"。

在较高级别上、EBS 磁盘类型之间的区别如下所示：

- 通用 SSD\_ 磁盘可平衡各种工作负载的成本和性能。性能是根据 IOPS 来定义的。
- *provisioned IOPS SSD* 磁盘适用于需要以较高成本获得最高性能的关键应用程序。
- *Throughput Optimized HDD* 磁盘适用于经常访问的工作负载，这些工作负载需要以更低的价格实现快速一致的吞吐量。
- 冷 HDD\_ 磁盘用于备份或不常访问的数据，因为性能非常低。与吞吐量优化的 HDD 磁盘一样、性能也是根据吞吐量来定义的。



HA 配置和数据分层不支持冷 HDD 磁盘。

### 本地 NVMe 存储

某些 EC2 实例类型包括本地 NVMe 存储，Cloud Volumes ONTAP 将其用作 "[Flash Cache](#)"。

- [相关链接 \\*](#)
- ["AWS 文档：EBS 卷类型"](#)
- ["了解如何在 AWS 中为您的系统选择磁盘类型和磁盘大小"](#)
- ["查看 AWS 中 Cloud Volumes ONTAP 的存储限制"](#)
- ["查看 AWS 中支持的 Cloud Volumes ONTAP 配置"](#)

## Azure 存储

在 Azure 中，一个聚合最多可以包含 12 个大小相同的磁盘。磁盘类型和最大磁盘大小取决于您使用的是单节点系统还是 HA 对：

### 单节点系统

单节点系统可以使用三种类型的 Azure 受管磁盘：

- *\_Premium SSD 受管磁盘\_* 以较高的成本为 I/O 密集型工作负载提供高性能。
- *标准 SSD 受管磁盘\_* 可为需要低 IOPS 的工作负载提供稳定一致的性能。

- 如果您不需要高 IOPS 并希望降低成本，[\\_Standard HDD 受管磁盘\\_](#) 是一个不错的选择。

每个受管磁盘类型的最大磁盘大小为 32 TB。

您可以将受管磁盘与 Azure Blob 存储配对 ["将非活动数据分层到低成本对象存储"](#)。

## HA 对

HA 对使用高级页面 Blobs，这些页面的最大磁盘大小为 8 TB。

- 相关链接 \*
- ["Microsoft Azure 文档：Microsoft Azure 存储简介"](#)
- ["了解如何在 Azure 中为您的系统选择磁盘类型和磁盘大小"](#)
- ["查看 Azure 中 Cloud Volumes ONTAP 的存储限制"](#)

## GCP 存储

在 GCP 中，一个聚合最多可以包含 6 个大小相同的磁盘。最大磁盘大小为 16 TB。

磁盘类型可以是 *zonal SSD persistent disks\_or\_zonal standard persistent disks*。您可以将永久性磁盘与 Google 存储分段配对 ["将非活动数据分层到低成本对象存储"](#)。

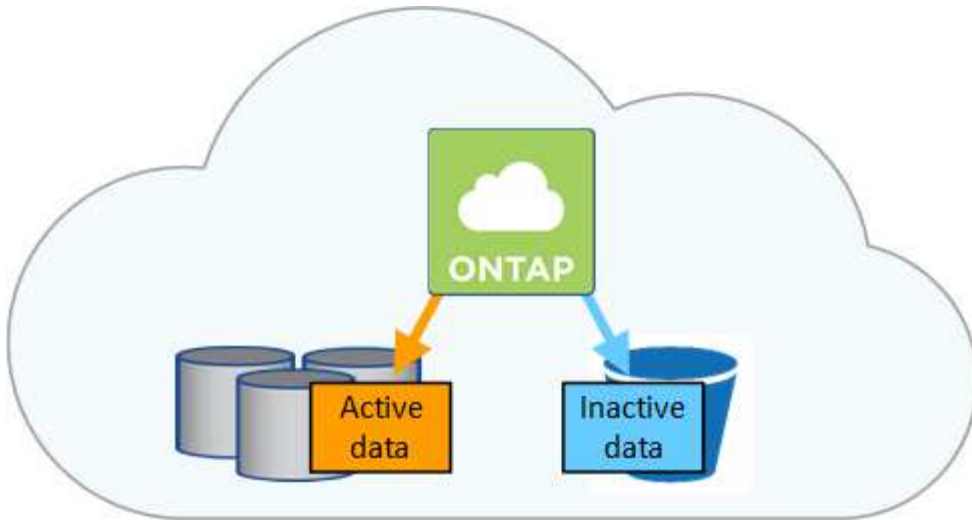
- 相关链接 \*
- ["Google Cloud Platform 文档：存储选项"](#)
- ["查看 GCP 中 Cloud Volumes ONTAP 的存储限制"](#)

## RAID 类型

每个 Cloud Volumes ONTAP 聚合的 RAID 类型为 RAID0（条带化）。不支持其他 RAID 类型。Cloud Volumes ONTAP 依靠云提供商提供磁盘可用性和持久性。

## 数据分层概述

通过将非活动数据自动分层到低成本的对象存储，降低存储成本。活动数据保留在高性能 SSD 或 HDD 中，而非活动数据则分层到低成本对象存储中。这使您可以回收主存储上的空间并缩减二级存储。



Cloud Volumes ONTAP 支持在 AWS ， Azure 和 Google 云平台中进行数据分层。数据分层由 FabricPool 技术提供支持。



您无需安装功能许可证即可启用数据分层（FabricPool）。

## AWS 中的数据分层

在 AWS 中启用数据分层时，Cloud Volumes ONTAP 会将 EBS 用作热数据的性能层，而将 AWS S3 用作非活动数据的容量层。通过更改系统的分层级别，您可以选择其他 S3 存储类。

### 性能层

性能层可以是通用 SSD 、配置的 IOPS SSD 或吞吐量优化的 HDD 。

### Capacity tier

Cloud Volumes ONTAP 系统使用 *Standard* 存储类将非活动数据分层到一个 S3 存储分段。Standard 是存储在多个可用性区域中的频繁访问数据的理想选择。



Cloud Manager 会为每个工作环境创建一个 S3 存储分段，并将其命名为 *fabric-pool-cluster unique identifier* 。不会为每个卷创建不同的 S3 存储分段。

### 分层级别

如果您不打算访问非活动数据，可以通过将系统的分层级别更改为以下级别之一来降低存储成本：*Intelligent Tierage* ， *one-Zone Inrequent Access* 或 *Standard-Intimic Access* 。更改分层级别后，如果 30 天后未访问非活动数据，则非活动数据将从标准存储类开始，并移至选定的存储类。

如果您确实访问数据，访问成本会更高，因此在更改分层级别之前，请考虑这一点。"[了解有关 Amazon S3 存储类的更多信息](#)"。

创建系统后，可以更改分层级别。有关详细信息，请参见 "[将非活动数据分层到低成本对象存储](#)"。

分层级别在系统范围内—不是每个卷。

## Azure 中的数据分层

在 Azure 中启用数据分层后，Cloud Volumes ONTAP 会将 Azure 托管磁盘用作热数据的性能层，并将 Azure

Blob 存储用作非活动数据的容量层。通过更改系统的分层级别，您可以选择其他 Azure 存储层。

### 性能层

性能层可以是 SSD 或 HDD。

### Capacity tier

Cloud Volumes ONTAP 系统会使用 Azure *hot* 存储层将非活动数据分层到一个 Blob 容器中。热层非常适合经常访问的数据。



Cloud Manager 会为每个 Cloud Volumes ONTAP 工作环境创建一个新的存储帐户，其中包含一个容器。存储帐户的名称是随机的。不会为每个卷创建不同的容器。

### 分层级别

如果您不打算访问非活动数据，可以通过将系统的分层级别更改为 Azure *cool* 存储层来降低存储成本。更改分层级别后，如果 30 天后未访问非活动数据，则非活动数据将从热存储层开始，并移至冷存储层。

如果您确实访问数据，访问成本会更高，因此在更改分层级别之前，请考虑这一点。"[详细了解 Azure Blob 存储访问层](#)"。

创建系统后，可以更改分层级别。有关详细信息，请参见 "[将非活动数据分层到低成本对象存储](#)"。

分层级别在系统范围内—不是每个卷。

## GCP 中的数据分层

在 GCP 中启用数据分层时，Cloud Volumes ONTAP 会使用永久性磁盘作为热数据的性能层，并使用 Google 云存储分段作为非活动数据的容量层。

### 性能层

性能层可以是 SSD 或 HDD（标准磁盘）。

### Capacity tier

Cloud Volumes ONTAP 系统使用 *Region* 存储类将非活动数据分层到一个 Google Cloud 存储分段。



Cloud Manager 会为每个工作环境创建一个分段，并将其命名为 *fabric-pool-cluster unique identifier*。不会为每个卷创建不同的存储分段。

### 分层级别

目前不支持其他 GCP 存储类。

### 数据分层和容量限制

如果启用数据分层，系统的容量限制将保持不变。此限制分布在性能层和容量层中。

### 卷分层策略

要启用数据分层，您必须在创建、修改或复制卷时选择卷分层策略。您可以为每个卷选择不同的策略。

某些分层策略具有相关的最小冷却周期，这将设置卷中的用户数据必须保持非活动状态的时间，以便将数据视为“冷”并移动到容量层。

通过 Cloud Manager ，您可以在创建或修改卷时从以下卷分层策略中进行选择：

### 仅快照

在聚合达到 50% 容量后、Cloud Volumes ONTAP 将不与活动文件系统关联的 Snapshot 副本的冷用户数据分层到容量层。冷却时间约为 2 天。

如果已读取、则容量层上的冷数据块会变得很热并移动到性能层。

### 自动

在聚合达到 50% 容量后、Cloud Volumes ONTAP 会将卷中的冷数据块分层到容量层。冷数据不仅包括 Snapshot 副本、还包括来自活动文件系统的冷用户数据。冷却期约为 31 天。

从 Cloud Volumes ONTAP 9.4 开始支持此策略。

如果通过随机读取进行读取、则容量层中的冷数据块会变得很热并移动到性能层。如果按顺序读取（例如与索引和防病毒扫描关联的读取）进行读取、冷数据块将保持冷态并且不会移动到性能层。

### 无

将卷的数据保留在性能层中、防止将其移动到容量层。

复制卷时，您可以选择是否将数据分层到对象存储。否则，Cloud Manager 会将 \* 备份 \* 策略应用于数据保护卷。从 Cloud Volumes ONTAP 9.6 开始，\* 所有 \* 分层策略将取代备份策略。

关闭 **Cloud Volumes ONTAP** 会影响冷却期

数据块通过散热扫描进行冷却。在此过程中，未使用的块的块温度会移动（冷却）到下一个较低的值。默认散热时间取决于卷分层策略：

- 自动：31 天
- 仅 Snapshot：2 天

要使散热扫描正常运行，必须运行 Cloud Volumes ONTAP。如果关闭 Cloud Volumes ONTAP，则散热也会停止。因此，散热时间可能会更长。

### 设置数据分层

有关说明以及支持的配置列表，请参见 ["将非活动数据分层到低成本对象存储"](#)。

## 存储管理

Cloud Manager 可简化和高级管理 Cloud Volumes ONTAP 存储。



必须直接从 Cloud Manager 创建和删除所有磁盘和聚合。不应从其他管理工具执行这些操作。这样做可能会影响系统稳定性、妨碍将来添加磁盘的能力、并可能产生冗余云提供商费用。

### 存储配置

通过为您购买磁盘和管理聚合、Cloud Manager 可以轻松地为 Cloud Volumes ONTAP 进行存储配置。您只需创建卷即可。如果需要，您可以使用高级分配选项自行配置聚合。



## 简化配置

聚合可为卷提供云存储。当您启动实例以及配置其他卷时、Cloud Manager 会为您创建聚合。

创建卷时、Cloud Manager 会执行以下三项操作之一：

- 它将卷放置在现有聚合上、该聚合具有足够的可用空间。
- 它通过为该聚合购买更多磁盘将卷放在现有聚合上。
- 它为新聚合购买磁盘并将卷置于该聚合上。

Cloud Manager 通过查看以下几个因素来确定放置新卷的位置：聚合的最大大小，是否已启用精简配置以及聚合的可用空间阈值。



帐户管理员可以从 \* 设置 \* 页面修改可用空间阈值。

## AWS 中聚合的磁盘大小选择

当 Cloud Manager 在 AWS 中为 Cloud Volumes ONTAP 创建新聚合时，随着系统中聚合的数量的增加，它会逐渐增加聚合中的磁盘大小。Cloud Manager 这样做是为了确保您可以在系统容量达到 AWS 允许的最大数据磁盘数之前利用系统的最大容量。

例如、Cloud Manager 可能会为 Cloud Volumes ONTAP Premium 或 BYOL 系统中的聚合选择以下磁盘大小：

聚合编号	Disk size	最大聚合容量
1.	500 MB	3 TB
4.	1 TB	6 TB
6.	2 TB	12 TB

您可以使用高级分配选项自行选择磁盘大小。

## 高级分配

您可以自己管理聚合而不是让云管理器为您管理聚合。"从 \* 高级分配 \* 页面"，您可以创建包含特定数量磁盘的新聚合，向现有聚合添加磁盘以及在特定聚合中创建卷。

## 容量管理

客户管理员可以选择 Cloud Manager 是否通知您存储容量决策，或者 Cloud Manager 是否自动管理您的容量需求。这可能有助于您了解这些模式的工作原理。

## 自动容量管理

默认情况下，容量管理模式设置为自动。在此模式下，Cloud Manager 会在需要更多容量时自动为 Cloud Volumes ONTAP 实例购买新磁盘，删除未使用的磁盘集合（聚合），根据需要在聚合之间移动卷以及尝试解除磁盘故障。

以下示例说明了此模式的工作原理：

- 如果具有 5 个或更少 EBS 磁盘的聚合达到容量阈值、则 Cloud Manager 会自动为该聚合购买新磁盘、以便

卷可以继续增长。

- 如果具有 12 个 Azure 磁盘的聚合达到容量阈值、Cloud Manager 会自动将卷从该聚合移动到具有可用容量的聚合或新聚合。

如果 Cloud Manager 为卷创建新聚合，则它会选择一个可容纳该卷大小的磁盘大小。

请注意，可用空间现在在原始聚合上可用。现有卷或新卷可以使用该空间。在此方案中，空间不能返回到 AWS 或 Azure 。

- 如果聚合包含的卷不超过 12 小时、Cloud Manager 将删除该卷。

### 通过自动容量管理来管理索引节点

Cloud Manager 可监控卷上的索引节点使用情况。使用 85% 的索引节点时，Cloud Manager 会增加卷的大小以增加可用索引节点的数量。卷可以包含的文件数取决于其包含的索引节点数。

### 手动容量管理

如果帐户管理员将容量管理模式设置为手动，则在必须做出容量决策时，Cloud Manager 会显示 Action Required 消息。自动模式中描述的相同示例适用于手动模式，但您可以接受这些操作。

## WORM 存储

您可以在 Cloud Volumes ONTAP 系统上激活一次写入、多次读取（WORM）存储、以及在指定的保留期内以未经修改的形式保留文件。WORM 存储由 SnapLock 技术在企业模式下提供支持、这意味着 WORM 文件在文件级别得到保护。

一旦将文件提交到 WORM 存储，即使保留期已过，也无法对其进行修改。防篡改时钟将确定 WORM 文件的保留期已过。

保留期结束后、您将负责删除不再需要的任何文件。

### 激活 WORM 存储

您可以在创建新的工作环境时在 Cloud Volumes ONTAP 系统上激活 WORM 存储。这包括指定激活代码和设置文件的默认保留期。您可以使用云管理器界面右下角的聊天图标获取激活代码。



您不能在单个卷上激活 WORM 存储—必须在系统级别激活 WORM 。

下图显示了如何在创建工作环境时激活 WORM 存储：

## WORM | *Preview*

You can use **write once, read many (WORM)** storage to retain critical files in unmodified form for regulatory and governance purposes and to protect from malware attacks. WORM files are protected at the file level. [Learn More](#)

Disable WORM     Activate WORM

**Notice:** If you enable WORM storage, you cannot enable data tiering to object storage.

WORM Activation Code 

Worm-1111122222aaaaa

Retention Period

15

years 

将文件提交到 **WORM**

您可以使用应用程序通过 NFS 或 CIFS 将文件提交到 WORM，或者使用 ONTAP CLI 自动将文件提交到 WORM。您还可以使用 WORM 附加文件来保留增量写入的数据，例如日志信息。

在 Cloud Volumes ONTAP 系统上激活 WORM 存储后，必须使用 ONTAP CLI 对 WORM 存储进行所有管理。有关说明，请参见 "[ONTAP 文档](#)"。



Cloud Volumes ONTAP 对 WORM 存储的支持等同于 SnapLock Enterprise 模式。

限制

- 如果直接从 AWS 或 Azure 删除或移动磁盘、则可以在卷到期日期之前删除该卷。
- 激活 WORM 存储后、无法启用到对象存储的数据分层。

## 高可用性对

### AWS 中的高可用性对

Cloud Volumes ONTAP High Availability (HA) 配置提供无中断操作和容错功能。在 AWS 中，数据会在两个节点之间同步镜像。

## 概述

在 AWS 中，Cloud Volumes ONTAP HA 配置包括以下组件：

- 两个 Cloud Volumes ONTAP 节点之间的数据同步镜像。
- 一种调解器实例，在节点之间提供通信通道以帮助存储接管和恢复过程。



调解器实例在 T2.Micro 实例上运行 Linux 操作系统，并使用一个大约为 8 GB 的 EBS 磁盘。

## 存储接管和恢复

如果某个节点出现故障、另一个节点可以为其合作伙伴提供数据以提供持续的数据服务。客户机可以从伙伴节点访问相同的数据，因为数据已同步镜像到合作伙伴。

节点重新引导后、合作伙伴必须重新同步数据才能返回存储。重新同步数据所需的时间取决于节点关闭时更改了多少数据。

## RPO 和 RTO

HA 配置可保持数据的高可用性，如下所示：

- 恢复点目标（RPO）为 0 秒。您的数据在传输过程中不会丢失数据。
- 恢复时间目标（RTO）为 60 秒。如果发生中断、数据应在 60 秒或更短的时间内可用。

## HA 部署模式

您可以通过在多个可用性区域（AZs）或在单个 AZ 中部署 HA 配置来确保数据的高可用性。您应该查看有关每个配置的更多详细信息、以选择最适合您需求的配置。

## 多个可用性区域中的 Cloud Volumes ONTAP HA

在多个可用性区域 (AZS) 中部署 HA 配置可确保在运行 Cloud Volumes ONTAP 节点的 AZ 或实例发生故障时数据的高可用性。您应该了解 NAS IP 地址如何影响数据访问和存储故障转移。

## NFS 和 CIFS 数据访问

当 HA 配置分布在多个可用性区域中时，*floating IP Addresses* 会启用 NAS 客户端访问。浮动 IP 地址必须位于该区域中所有 VPC 的 CIDR 块之外、在发生故障时可以在节点之间迁移。除非您的情况，否则 VPC 外部的客户端无法本机访问它们 "[设置 AWS 传输网关](#)"。

如果无法设置传输网关，则 VPC 外部的 NAS 客户端可以使用专用 IP 地址。但是，这些 IP 地址是静态的，无法在节点之间进行故障转移。

在跨多个可用性区域部署 HA 配置之前，应先检查浮动 IP 地址和路由表的要求。部署配置时，必须指定浮动 IP 地址。私有 IP 地址由 Cloud Manager 自动创建。

有关详细信息，请参见 "[适用于多个 AWS 中的 Cloud Volumes ONTAP HA 的 AWS 网络要求](#)"。

## iSCSI 数据访问

由于 iSCSI 不使用浮动 IP 地址，因此交叉 VPC 数据通信不是一个问题。

## 适用于 iSCSI 的存储接管和恢复

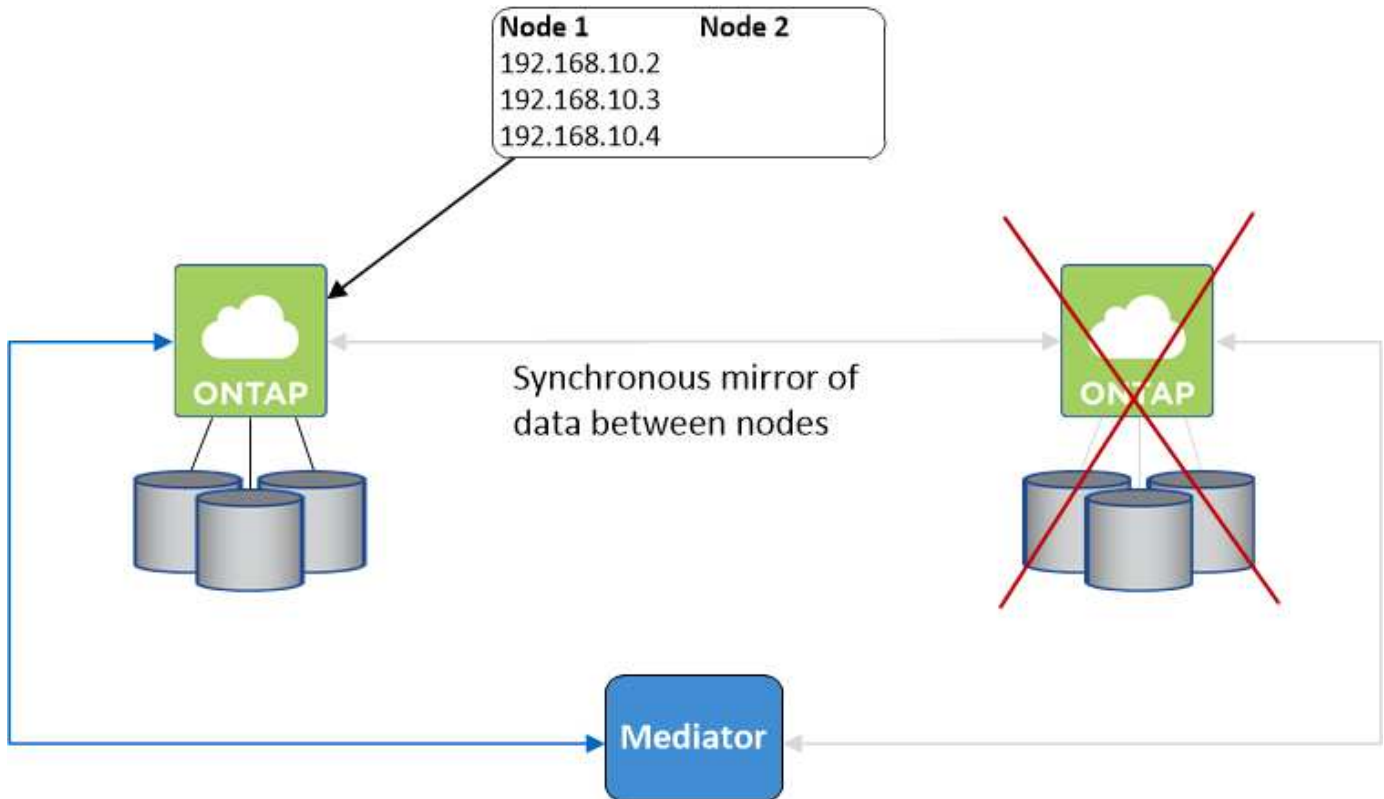
对于 iSCSI、Cloud Volumes ONTAP 使用多路径 I/O (MPIO) 和非对称逻辑单元访问 (ALUA) 来管理活动优化路径和非优化路径之间的路径故障转移。



有关哪些特定主机配置支持 ALUA 的信息，请参见 ["NetApp 互操作性表工具"](#) 以及适用于您的主机操作系统的《Host Utilities 安装和设置指南》。

## 适用于 NAS 的存储接管和恢复

在使用浮动 IP 的 NAS 配置中发生接管时，客户端用于访问数据的节点的浮动 IP 地址将移至另一节点。下图描述了使用浮动 IPS 的 NAS 配置中的存储接管。如果节点 2 出现故障、节点 2 的浮动 IP 地址将移至节点 1。



如果发生故障、用于外部 VPC 访问的 NAS 数据 IPS 将无法在节点之间迁移。如果某个节点脱机、则必须使用另一个节点上的 IP 地址将卷手动重新装入 VPC 外部的客户端。

故障节点重新联机后、使用原始 IP 地址将客户端重新装入卷。需要执行此步骤以避免在两个 HA 节点之间传输不必要的数据、这可能会对性能和稳定性造成重大影响。

通过选择卷并单击 \* 挂载命令 \*，您可以从 Cloud Manager 轻松识别正确的 IP 地址。

## 在单个可用性区域中使用 Cloud Volumes ONTAP HA

如果运行 Cloud Volumes ONTAP 节点的实例出现故障、在单可用性区域 (AZ) 中部署 HA 配置可以确保数据的高可用性。所有数据均可从 VPC 外部本地访问。



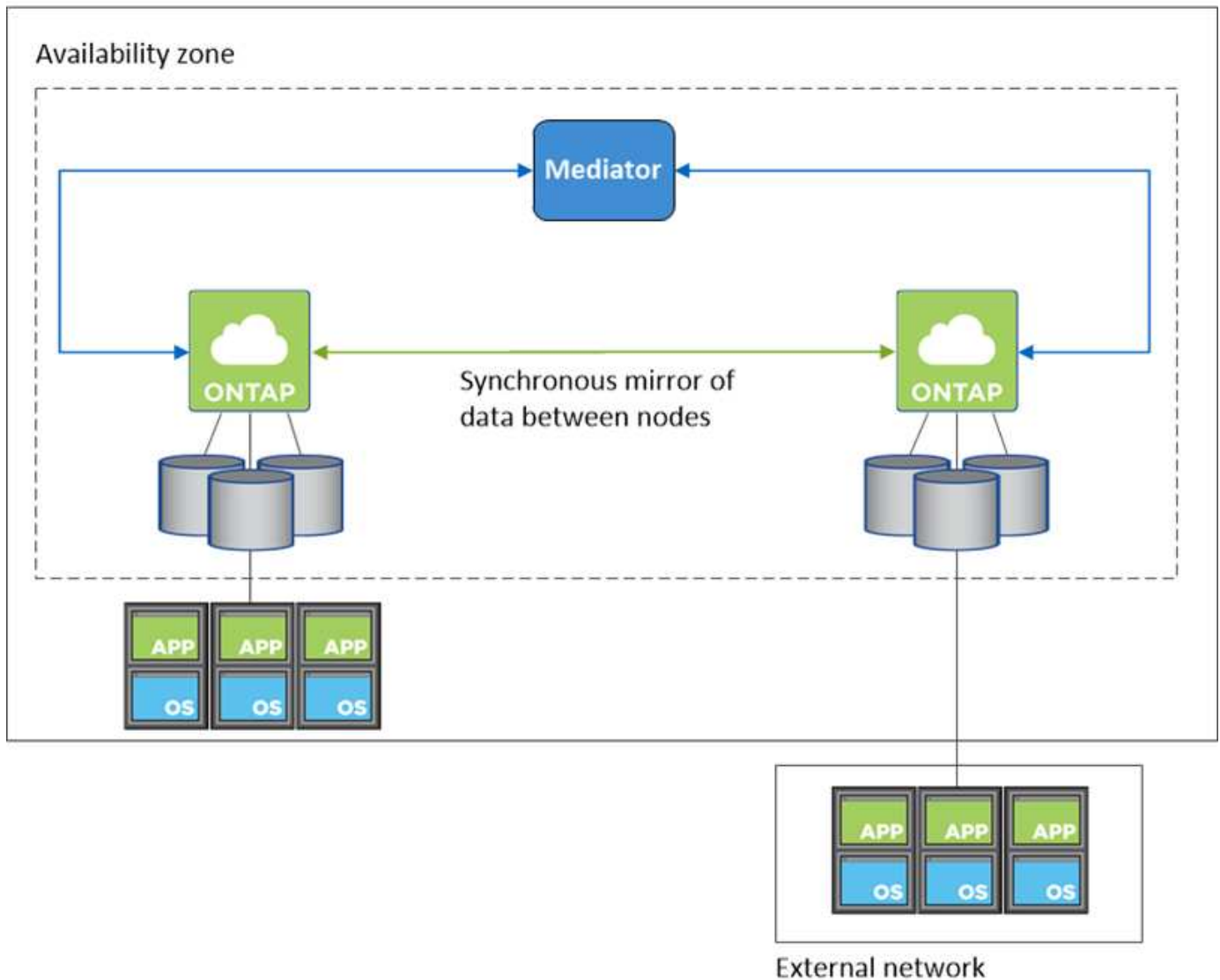
Cloud Manager 将创建 "AWS 分布放置组" 并启动该放置组中的两个 HA 节点。放置组通过将实例分散在不同的底层硬件上，降低同时发生故障的风险。此功能可从计算角度而不是从磁盘故障角度提高冗余。

### 数据访问

由于此配置位于单个 AZ 中，因此不需要浮动 IP 地址。您可以使用相同的 IP 地址从 VPC 内部和 VPC 外部进行数据访问。

下图显示了单个 AZ 中的 HA 配置。可以从 VPC 内部和 VPC 外部访问数据。

### VPC in AWS



### 存储接管和恢复

对于 iSCSI、Cloud Volumes ONTAP 使用多路径 I/O (MPIO) 和非对称逻辑单元访问 (ALUA) 来管理活动优化路径和非优化路径之间的路径故障转移。



有关哪些特定主机配置支持 ALUA 的信息，请参见 ["NetApp 互操作性表工具"](#) 以及适用于您的主机操作系统的《Host Utilities 安装和设置指南》。

对于 NAS 配置、如果发生故障、数据 IP 地址可以在 HA 节点之间迁移。这样可以确保客户端访问存储。

### 存储如何在 HA 对中工作

与 ONTAP 集群不同、Cloud Volumes ONTAP HA 对中的存储不在节点之间共享。而是在节点之间同步镜像数据，以便在发生故障时数据可用。

### 存储分配

创建新卷并需要附加磁盘时、Cloud Manager 会为两个节点分配相同数量的磁盘、创建镜像聚合、然后创建新卷。例如，如果卷需要两个磁盘、则 Cloud Manager 会为每个节点分配两个磁盘、总共四个磁盘。

### 存储配置

您可以将 HA 对用作主动 - 主动配置、两个节点都将数据提供给客户端、也可以用作主动 - 被动配置、仅当被动节点接管了主动节点的存储时才响应数据请求。



仅当在存储系统视图中使用 Cloud Manager 时，您才可以设置主动 - 主动配置。

### 对 HA 配置的性能期望值

Cloud Volumes ONTAP HA 配置可同步复制节点之间的数据、从而消耗网络带宽。因此，与单节点 Cloud Volumes ONTAP 配置相比，您可以期望以下性能：

- 对于仅从一个节点提供数据的 HA 配置、读取性能与单个节点配置的读取性能不相上下、而写入性能较低。
- 对于为来自两个节点的数据提供服务的 HA 配置、读取性能高于单节点配置的读取性能、写入性能相同或更高。

有关 Cloud Volumes ONTAP 性能的详细信息，请参见 ["性能"](#)。

### 客户端访问存储

客户端应使用卷所在节点的数据 IP 地址访问 NFS 和 CIFS 卷。如果 NAS 客户端使用伙伴节点的 IP 地址访问卷、则两个节点之间的通信量都会降低性能。

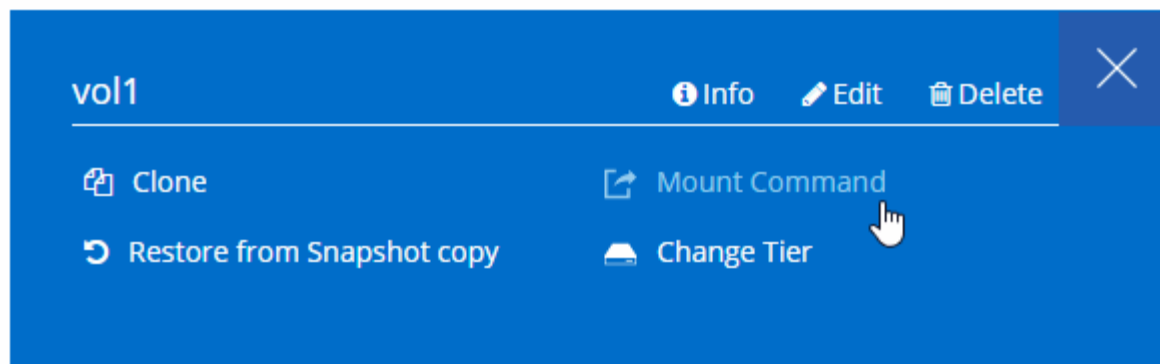


如果在 HA 对中的节点之间移动卷、则应使用其他节点的 IP 地址重新装入卷。否则，您可能会遇到性能降低的问题。如果客户机支持 NFSv4 引用或 CIFS 文件夹重定向、则可以在 Cloud Volumes ONTAP 系统上启用这些功能以避免重新装入卷。有关详细信息，请参见 ONTAP 文档。

您可以从 Cloud Manager 轻松确定正确的 IP 地址。

## Volumes

2 Volumes | 0.22 TB Allocated | < 0.01 TB Used (0 TB in S3)



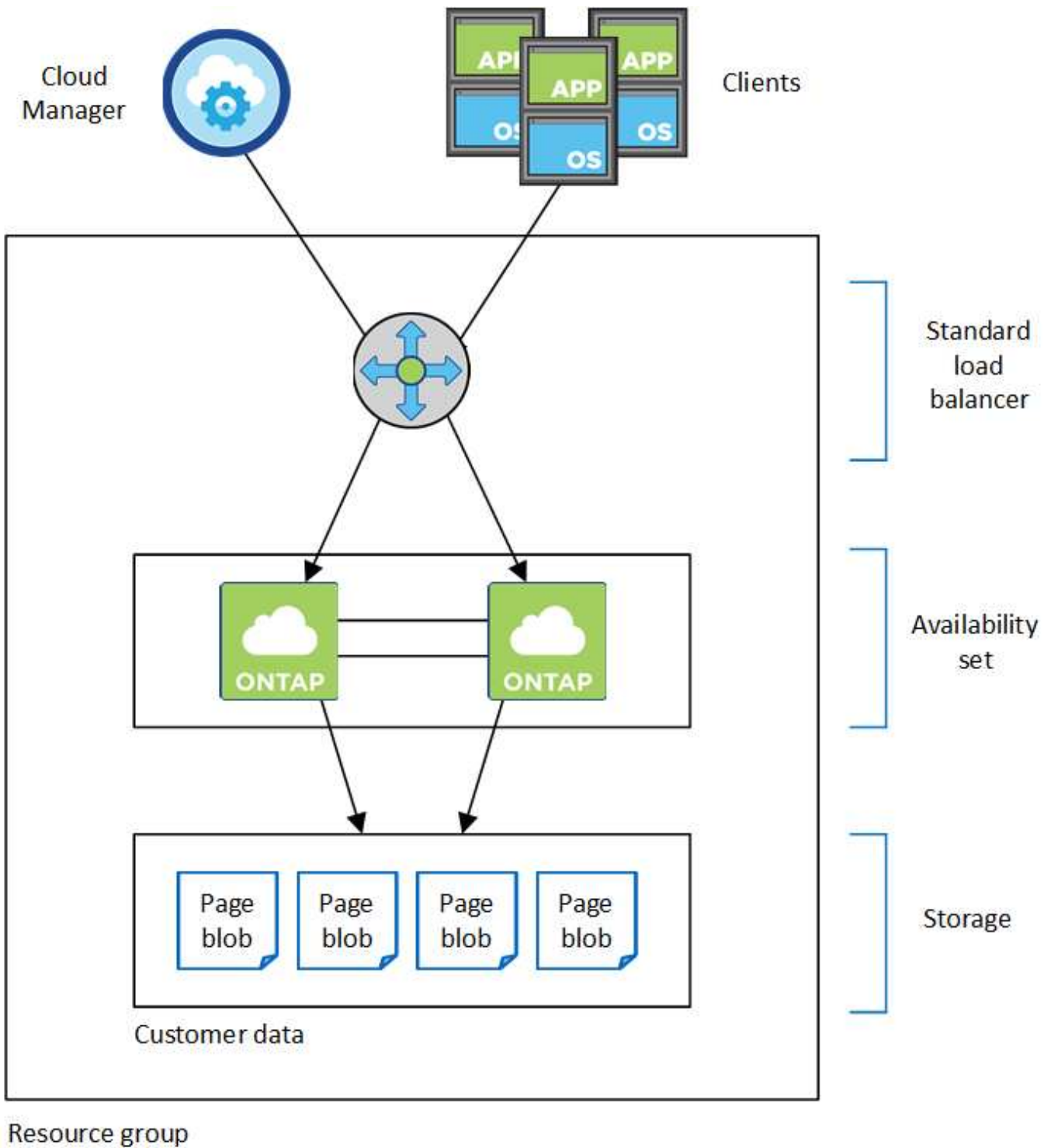
### Azure 中的高可用性对

Cloud Volumes ONTAP 高可用性（High Availability，HA）对可在云环境发生故障时提供企业级可靠性和持续运行。在 Azure 中，存储在两个节点之间共享。

#### HA 组件

Azure 中的 Cloud Volumes ONTAP HA 配置包括以下组件：





请注意以下有关 Cloud Manager 为您部署的 Azure 组件的信息：

#### Azure 标准负载均衡器

负载均衡器管理传入 Cloud Volumes ONTAP HA 对的流量。

#### 可用性集

可用性集可确保节点位于不同的故障域和更新域中。

## Disks

客户数据位于高级存储页面 Blobs 上。每个节点都可以访问另一节点的存储。启动，根和核心数据还需要额外的存储：

- 两个用于启动卷的 90 GB 高级 SSD 磁盘（每个节点一个）
- 根卷的两个 140 GB 高级存储页面 Blobs（每个节点一个）
- 两个 128 GB 标准 HDD 磁盘，用于节省核心（每个节点一个）

## 存储帐户

- 受管磁盘需要一个存储帐户。
- 高级存储页面 Blobs 需要一个或多个存储帐户，因为已达到每个存储帐户的磁盘容量限制。

["Azure 文档：存储帐户的 Azure 存储可扩展性和性能目标"](#)。

- 要将数据分层到 Azure Blob 存储，需要一个存储帐户。

## RPO 和 RTO

HA 配置可保持数据的高可用性，如下所示：

- 恢复点目标（RPO）为 0 秒。您的数据在传输过程中不会丢失数据。
- 恢复时间目标（RTO）为 60 秒。如果发生中断，数据应在 60 秒或更短的时间内可用。

## 存储接管和恢复

与物理 ONTAP 集群类似，Azure HA 对中的存储在节点之间共享。通过连接到配对节点的存储，可以使每个节点在发生 *takeover* 时访问另一个节点的存储。网络路径故障转移机制可确保客户端和主机继续与正常运行的节点进行通信。当节点恢复联机时，配对节点 *gives back storage*。

对于 NAS 配置，如果发生故障，数据 IP 地址会自动在 HA 节点之间迁移。

对于 iSCSI、Cloud Volumes ONTAP 使用多路径 I/O（MPIO）和非对称逻辑单元访问（ALUA）来管理活动优化路径和非优化路径之间的路径故障转移。



有关哪些特定主机配置支持 ALUA 的信息，请参见 ["NetApp 互操作性表工具"](#) 以及适用于您的主机操作系统的《Host Utilities 安装和设置指南》。

## 存储配置

您可以将 HA 对用作主动 - 主动配置、两个节点都将数据提供给客户端、也可以用作主动 - 被动配置、仅当被动节点接管了主动节点的存储时才响应数据请求。

## HA 限制

以下限制会影响 Azure 中的 Cloud Volumes ONTAP HA 对：

- Cloud Volumes ONTAP 标准版，高级版和 BYOL 支持 HA 对。不支持浏览。
- 不支持 NFSv4。支持 NFSv3。

- 某些地区不支持 HA 对。

"请参见支持的 [Azure 区域列表](#)"。

"了解如何在 Azure 中部署 HA 系统"。

## 评估

您可以在为软件付费之前对 Cloud Volumes ONTAP 进行评估。

可从获取单节点 Cloud Volumes ONTAP 系统 30 天免费试用版 "NetApp Cloud Central"。每小时不收取软件费用，但基础架构费用仍然适用。免费试用版在过期后会自动转换为按小时付费的订阅。

如果您需要有关概念验证的帮助，请联系 "销售团队" 或者通过提供的聊天选项联系 "NetApp Cloud Central" 以及 Cloud Manager 中的。

## 许可

每个 Cloud Volumes ONTAP BYOL 系统都必须安装一个许可证并进行有效订阅。如果未安装活动许可证，则 Cloud Volumes ONTAP 系统将在 30 天后自行关闭。Cloud Manager 通过管理您的许可证以及在许可证过期前通知您来简化流程。

### 新系统的许可证管理

创建 BYOL 系统时，Cloud Manager 会提示您输入 NetApp 支持站点帐户。Cloud Manager 使用帐户从 NetApp 下载许可证文件并将其安装在 Cloud Volumes ONTAP 系统上。

"了解如何将 NetApp 支持站点帐户添加到 Cloud Manager"。

如果云管理器无法通过安全 Internet 连接访问许可证文件，您可以自己获取该文件，然后手动将该文件上传到云管理器。有关说明，请参见 "[在 Cloud Volumes ONTAP BYOL 系统上安装许可证文件](#)"。

### 许可证到期

Cloud Manager 会在许可证到期前 30 天以及许可证到期后再次向您发出警告。下图显示了 30 天到期警告：



您可以选择工作环境来查看消息。

如果不及时续订许可证，Cloud Volumes ONTAP 系统将自行关闭。如果重新启动它，它会再次自动关闭。



Cloud Volumes ONTAP 还可以使用 EMS（事件管理系统）事件通知通过电子邮件、SNMP 陷阱主机或系统日志服务器通知您。有关说明，请参见 "[《ONTAP 9 EMS 配置快速指南》](#)"。

## 许可证续订

当您通过联系 NetApp 代表续订 BYOL 订阅时，Cloud Manager 会自动从 NetApp 获取新许可证并将其安装在 Cloud Volumes ONTAP 系统上。

如果云管理器无法通过安全 Internet 连接访问许可证文件，您可以自己获取该文件，然后手动将该文件上传到云管理器。有关说明，请参见 "[在 Cloud Volumes ONTAP BYOL 系统上安装许可证文件](#)"。

## 安全性

Cloud Volumes ONTAP 支持数据加密，并提供防病毒和勒索软件保护。

### 空闲数据加密

Cloud Volumes ONTAP 支持以下加密技术：

- NetApp 卷加密（从 Cloud Volumes ONTAP 9.5 开始）
- AWS 密钥管理服务
- Azure 存储服务加密
- Google Cloud Platform 默认加密

您可以将 NetApp 卷加密与原生 AWS，Azure 或 GCP 加密结合使用，以便在虚拟机管理程序级别对数据进行加密。

### NetApp 卷加密

NetApp 卷加密（NVE）是一种基于软件的技术，用于一次对一个卷上的空闲数据进行加密。数据，Snapshot 副本和元数据已加密。数据访问由一个唯一的 XTS-AES-256 密钥提供，每个卷一个。

Cloud Volumes ONTAP 通过外部密钥管理服务器支持 NetApp 卷加密。不支持板载密钥管理器。您可以在中找到支持的密钥管理器 "[NetApp 互操作性表工具](#)" 在 \* 密钥管理器 \* 解决方案下。

您可以使用 CLI 或 System Manager 在新卷或现有卷上启用 NetApp 卷加密。Cloud Manager 不支持 NetApp 卷加密。有关说明，请参见 "[使用 NetApp 卷加密对卷进行加密](#)"。

### AWS 密钥管理服务

在 AWS 中启动 Cloud Volumes ONTAP 系统时，您可以使用启用数据加密 "[AWS 密钥管理服务（KMS）](#)"。Cloud Manager 使用客户主密钥（CMK）请求数据密钥。



创建 Cloud Volumes ONTAP 系统后，您无法更改 AWS 数据加密方法。

如果要使用此加密选项，则必须确保正确设置 AWS KMS。有关详细信息，请参见 "[设置 AWS KMS](#)"。

## Azure 存储服务加密

"Azure 存储服务加密" 默认情况下， Azure 中的 Cloud Volumes ONTAP 数据会启用空闲数据。无需设置。



Cloud Volumes ONTAP 不支持客户管理的密钥。

## Google Cloud Platform 默认加密

"Google Cloud Platform 空闲数据加密" 默认情况下， Cloud Volumes ONTAP 处于启用状态。无需设置。

虽然 Google Cloud Storage 始终会在数据写入磁盘之前对数据进行加密，但您可以使用 Cloud Manager API 创建使用 *customer-managed encryption keys* 的 Cloud Volumes ONTAP 系统。这些密钥可通过云密钥管理服务在 GCP 中生成和管理。

请参见 "API 开发人员指南" 有关使用 GCP 加密参数的详细信息。

## ONTAP 病毒扫描

您可以在 ONTAP 系统上使用集成的防病毒功能来保护数据免受病毒或其他恶意代码的攻击。

称为 *Vscan* 的 ONTAP 病毒扫描将同类最佳的第三方防病毒软件与 ONTAP 功能相结合，让您灵活地控制扫描哪些文件以及何时扫描。

有关 Vscan 支持的供应商，软件和版本的信息，请参见 "NetApp 互操作性表"。

有关如何在 ONTAP 系统上配置和管理防病毒功能的信息，请参见 "《ONTAP 9 防病毒配置指南》"。

## 勒索软件保护

勒索软件攻击可能会耗费业务时间，资源和声誉。您可以通过 Cloud Manager 实施 NetApp 解决方案 for 勒索软件，它可以提供有效的工具来实现可见性，检测和补救。

- Cloud Manager 可识别不受 Snapshot 策略保护的卷，并允许您在这些卷上激活默认 Snapshot 策略。

Snapshot 副本为只读副本，可防止勒索软件损坏。它们还可以提供创建单个文件副本或完整灾难恢复解决方案映像的粒度。

- Cloud Manager 还支持您通过启用 ONTAP 的 FPolicy 解决方案来阻止常见的勒索软件文件扩展名。

The screenshot displays two panels from the Cloud Manager interface. The left panel, titled "1 Enable Snapshot Copy Protection", shows a progress indicator at 40% Protection and a notification that 3 volumes lack a Snapshot Policy. It includes a button to "Activate Snapshot Policy". The right panel, titled "2 Block Ransomware File Extensions", features a shield icon with an 'F' and explains that ONTAP's native FPolicy configuration monitors and blocks file operations based on file extensions. It includes a button to "Activate FPolicy" and a link to "View Denied File Names".

["了解如何实施适用于勒索软件的 NetApp 解决方案"](#)。

## 性能

您可以查看性能结果、帮助您确定哪些工作负载适合 Cloud Volumes ONTAP 。

有关适用于 AWS 的 Cloud Volumes ONTAP ，请参见 ["NetApp 技术报告 4383：使用应用程序工作负载在 Amazon Web Services 中对 Cloud Volumes ONTAP 进行性能特征描述"](#)。

有关适用于 Microsoft Azure 的 Cloud Volumes ONTAP ，请参见 ["NetApp 技术报告 4671： Azure 中的 Cloud Volumes ONTAP 的性能特征与应用程序工作负载"](#)。

# 入门

## 部署概述

开始之前，您可能希望更好地了解部署 Cloud Manager 和 Cloud Volumes ONTAP 的选项。

### 安装 Cloud Manager

部署和管理 Cloud Volumes ONTAP 需要 Cloud Manager 软件。您可以在以下任意位置部署 Cloud Manager：

- Amazon Web Services (AWS)
- Microsoft Azure
- Google 云平台

在 GCP 中部署 Cloud Volumes ONTAP 时，Cloud Manager 必须位于 Google 云平台中。

- IBM 云
- 在您自己的网络中

如何部署 Cloud Manager 取决于您选择的位置：

Cloud Manager 的位置	如何部署 Cloud Manager
AWS	<ol style="list-style-type: none"><li>1. "从 NetApp Cloud Central 部署 Cloud Manager" 建议</li><li>2. "从 AWS Marketplace 部署"</li><li>3. "在 Linux 主机上下载并安装软件"</li></ol>
AWS C2S	"从 AWS 智能社区市场部署 Cloud Manager"
Azure 通用区域	<ol style="list-style-type: none"><li>1. "从 NetApp Cloud Central 部署 Cloud Manager" 建议</li><li>2. "从 Azure Marketplace 部署"</li><li>3. "在 Linux 主机上下载并安装软件"</li></ol>
Azure 政府	"从 Azure 美国政府市场部署 Cloud Manager"
Azure 德国	"在 Linux 主机上下载并安装软件"
Google 云平台	<ol style="list-style-type: none"><li>1. "从 NetApp Cloud Central 部署 Cloud Manager" 建议</li><li>2. "在 Linux 主机上下载并安装软件"</li></ol> <p> 您无法从 GCP Marketplace 在 Google Cloud 中部署 Cloud Manager</p>
IBM 云	"在 Linux 主机上下载并安装软件"

Cloud Manager 的位置	如何部署 Cloud Manager
内部网络	<a href="#">"在 Linux 主机上下载并安装软件"</a>

## 云管理器设置

在安装 Cloud Manager 后，您可能需要执行其他设置，例如添加其他云提供商帐户，安装 HTTPS 证书等。

- ["设置 Cloud Central 帐户"](#)
- ["将 AWS 帐户添加到 Cloud Manager"](#)
- ["将 Azure 帐户添加到 Cloud Manager"](#)
- ["安装 HTTPS 证书"](#)
- ["设置 AWS KMS"](#)

## Cloud Volumes ONTAP 部署

启动并运行 Cloud Manager 后，您可以开始在云提供商中部署 Cloud Volumes ONTAP。

["AWS 入门"](#)，["Azure 入门"](#)，和 ["GCP 入门"](#) 提供有关快速启动和运行 Cloud Volumes ONTAP 的说明。有关其他帮助信息，请参阅以下内容：

- ["AWS 中的 Cloud Volumes ONTAP 9.7 支持的配置"](#)
- ["Azure 中 Cloud Volumes ONTAP 9.7 支持的配置"](#)
- ["GCP 中的 Cloud Volumes ONTAP 9.7 支持的配置"](#)
- ["规划配置"](#)
- ["在 AWS 中启动 Cloud Volumes ONTAP"](#)
- ["在 Azure 中启动 Cloud Volumes ONTAP"](#)
- ["在 GCP 中启动 Cloud Volumes ONTAP"](#)

## AWS 中的 Cloud Volumes ONTAP 入门

先设置 AWS，然后从 NetApp Cloud Central 启动 Cloud Manager 软件，开始使用 Cloud Volumes ONTAP。我们为您在 AWS 中发布的第一个 Cloud Volumes ONTAP 系统提供 30 天免费试用。



### 1 设置网络

1. 支持从目标 VPC 进行出站 Internet 访问，以便 Cloud Manager 和 Cloud Volumes ONTAP 可以与多个端点联系。

此步骤非常重要，因为 Cloud Manager 无法在没有出站 Internet 访问的情况下部署 Cloud Volumes ONTAP。如果需要限制出站连接，请参阅的端点列表 ["云管理器"](#) 和 ["Cloud Volumes ONTAP"](#)。



2. 将 VPC 端点设置为 S3 服务。

如果要将冷数据从 Cloud Volumes ONTAP 分层到低成本对象存储，则需要 VPC 端点。

## 2

提供所需的 **AWS** 权限

从 NetApp Cloud Central 部署 Cloud Manager 时，您需要使用具有部署实例权限的 AWS 帐户。

1. 转到 AWS IAM 控制台，然后通过复制和粘贴的内容来创建策略 "[适用于 AWS 的 NetApp Cloud Central 策略](#)"。
2. 将策略附加到 IAM 用户。

## 3

从 **AWS Marketplace** 创建

"[从 AWS Marketplace 订阅 Cloud Manager](#)" 确保在免费试用 Cloud Volumes ONTAP 结束后不会中断服务。对于您创建的每个 Cloud Volumes ONTAP PAYGO 系统以及您启用的每个附加功能，此订阅将向您收取费用。

如果您要通过自带许可证（BYOL）启动 Cloud Volumes ONTAP，"[然后，您需要在 AWS Marketplace 中订阅该产品](#)"。

## 4

从 **NetApp Cloud Central** 启动 **Cloud Manager**

部署和管理 Cloud Volumes ONTAP 需要 Cloud Manager 软件。从启动 Cloud Manager 实例只需几分钟 "[Cloud Central](#)"。

## 5

使用 **Cloud Manager** 启动 **Cloud Volumes ONTAP**

在 Cloud Manager 准备就绪后、只需单击“创建”、选择要启动的系统类型并完成向导中的步骤。25 分钟后、您的第一个 Cloud Volumes ONTAP 系统应该已启动并正在运行。

观看以下视频、了解这些步骤：

► [https://docs.netapp.com/zh-cn/occm37//media/video\\_getting\\_started\\_aws.mp4](https://docs.netapp.com/zh-cn/occm37//media/video_getting_started_aws.mp4) (video)

相关链接

- "[评估](#)"
- "[云管理器的网络要求](#)"
- "[AWS 中的 Cloud Volumes ONTAP 的网络要求](#)"
- "[AWS 的安全组规则](#)"
- "[将 AWS 帐户添加到 Cloud Manager](#)"
- "[Cloud Manager 如何使用 AWS 权限](#)"
- "[在 AWS 中启动 Cloud Volumes ONTAP](#)"

- ["从 AWS Marketplace 启动 Cloud Manager"](#)

## 开始在 **Azure** 中使用 **Cloud Volumes ONTAP**

首先从 Cloud Volumes ONTAP 开始，先设置 Azure ，然后从 NetApp Cloud Central 部署 Cloud Manager 软件。有关在中部署 Cloud Manager 的说明，请参见 ["Azure 美国政府区域"](#) 和中的 ["Azure 德国地区"](#)。



### 设置网络

从目标 VNet 启用出站 Internet 访问，以便 Cloud Manager 和 Cloud Volumes ONTAP 可以与多个端点联系。

此步骤非常重要，因为没有出站 Internet 访问、Cloud Manager 无法部署 Cloud Volumes ONTAP 。如果需要限制出站连接，请参阅的端点列表 ["云管理器"](#) 和 ["Cloud Volumes ONTAP"](#)。



### 提供所需的 **Azure** 权限

从 NetApp Cloud Central 部署 Cloud Manager 时，您需要使用具有部署 Cloud Manager 虚拟机权限的 Azure 帐户。

1. 下载 ["适用于 Azure 的 NetApp Cloud Central 策略"](#)。
2. 通过将 Azure 订阅 ID 添加到 "AssignableScops" 字段来修改 JSON 文件。
3. 使用 JSON 文件在 Azure 中创建名为 *Azure SetupAsService* 的自定义角色。

示例： \*AZ 角色定义 create -role-definition C : \Policy\_for\_Setup\_as\_Service\_Azure.json\*

4. 在 Azure 门户中，将自定义角色分配给将从 Cloud Central 部署 Cloud Manager 的用户。



### 从 **NetApp Cloud Central** 启动 **Cloud Manager**

部署和管理 Cloud Volumes ONTAP 需要 Cloud Manager 软件。从启动 Cloud Manager 实例只需几分钟 ["Cloud Central"](#)。



### 使用 **Cloud Manager** 启动 **Cloud Volumes ONTAP**

在 Cloud Manager 准备就绪后、只需单击“创建”、选择要部署的系统类型并完成向导中的步骤。25 分钟后、您的第一个 Cloud Volumes ONTAP 系统应该已启动并正在运行。

相关链接

- ["评估"](#)
- ["云管理器的网络要求"](#)
- ["Azure 中的 Cloud Volumes ONTAP 的网络要求"](#)

- ["Azure 的安全组规则"](#)
- ["将 Azure 帐户添加到 Cloud Manager"](#)
- ["Cloud Manager 使用 Azure 权限的功能"](#)
- ["在 Azure 中启动 Cloud Volumes ONTAP"](#)
- ["从 Azure Marketplace 启动 Cloud Manager"](#)

## 在 Google 云平台中开始使用 Cloud Volumes ONTAP

先设置 GCP ， 然后从 NetApp Cloud Central 部署 Cloud Manager 软件， 开始使用 Cloud Volumes ONTAP 。

要在 GCP 中部署 Cloud Volumes ONTAP ， 必须在 Google 云平台中安装 Cloud Manager 。



### 设置网络

支持从目标 VPC 进行出站 Internet 访问， 以便 Cloud Manager 和 Cloud Volumes ONTAP 可以与多个端点联系。

此步骤非常重要， 因为 Cloud Manager 无法在没有出站 Internet 访问的情况下部署 Cloud Volumes ONTAP 。 如果需要限制出站连接， 请参阅的端点列表 ["云管理器"](#) 和 ["Cloud Volumes ONTAP"](#)。



### Set up GCP permissions and projects

确保已设置两组权限：

1. 确保从 NetApp Cloud Central 部署 Cloud Manager 的 GCP 用户在中具有权限 ["GCP 的 Cloud Central 策略"](#)。

["您可以使用 YAML 文件创建自定义角色"](#) 然后将其附加到用户。 您需要使用 gcloud 命令行创建角色。

2. 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。

您将在第 6 步中将此服务帐户与 Cloud Manager VM 关联。

- ["在 GCP 中创建角色"](#) 其中包括定义的权限 ["适用于 GCP 的 Cloud Manager 策略"](#)。 同样， 您需要使用 gcloud 命令行。

此 YAML 文件中包含的权限与步骤 2a 中的权限不同。

- ["创建 GCP 服务帐户并应用刚刚创建的自定义角色"](#)。
- 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。

### 3

#### 设置用于数据分层的 GCP

要将冷数据从 Cloud Volumes ONTAP 9.7 分层到低成本对象存储（Google 云存储分段），必须满足两项要求：

1. "创建服务帐户" 具有预定义的存储管理员角色和作为用户的 Cloud Manager 服务帐户。

稍后在创建 Cloud Volumes ONTAP 工作环境时，您需要选择此服务帐户。此服务帐户与您在第 2 步中创建的服务帐户不同。

2. "为专用 Google 访问配置 Cloud Volumes ONTAP 子网"。

如果要在 Cloud Volumes ONTAP 9.6 中使用数据分层，"然后，按照以下步骤进行操作"。

### 4

#### 启用 Google Cloud API

"在项目中启用以下 Google Cloud API"。部署 Cloud Manager 和 Cloud Volumes ONTAP 需要使用这些 API。

- Cloud Deployment Manager V2 API
- Cloud Resource Manager API
- 计算引擎 API
- Stackdriver 日志记录 API

### 5

#### 从 GCP Marketplace 订阅

"从 GCP Marketplace 订阅 Cloud Volumes ONTAP" 确保在免费试用结束后不会中断服务。对于您创建的每个 Cloud Volumes ONTAP PAYGO 系统，此订阅将向您收取费用。

### 6

#### 从 NetApp Cloud Central 启动 Cloud Manager

部署和管理 Cloud Volumes ONTAP 需要 Cloud Manager 软件。在 GCP 中启动 Cloud Manager 实例只需几分钟 "Cloud Central"。

选择 GCP 作为云提供商时，Google 会提示您登录到您的帐户并授予权限。单击 "允许" 可授予对部署 Cloud Manager 所需计算 API 的访问权限。

### 7

#### 使用 Cloud Manager 启动 Cloud Volumes ONTAP

在 Cloud Manager 准备就绪后、只需单击“创建”、选择要部署的系统类型并完成向导中的步骤。25 分钟后、您的第一个 Cloud Volumes ONTAP 系统应该已启动并正在运行。

相关链接

- "评估"

- "云管理器的网络要求"
- "GCP 中的 Cloud Volumes ONTAP 的网络要求"
- "GCP 的防火墙规则"
- "Cloud Manager 如何使用 GCP 权限"
- "在 GCP 中启动 Cloud Volumes ONTAP"
- "在 Linux 主机上下载并安装 Cloud Manager 软件"

## 设置 Cloud Manager

在 **Cloud Central** 帐户中设置工作空间和用户

每个 Cloud Manager 系统都与一个 \_NetApp Cloud Central 帐户关联。设置与 Cloud Manager 系统关联的 Cloud Central 帐户，以使用户可以访问 Cloud Manager 并在工作空间中部署 Cloud Volumes ONTAP 系统。只需添加一个用户或添加多个用户和工作空间即可。

此帐户在 Cloud Central 中维护，因此您所做的任何更改均可供其他 Cloud Manager 系统和其他 NetApp 云数据服务使用。"详细了解 Cloud Central 帐户的工作原理"。

正在添加工作空间

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，并将不同的用户与这些工作空间关联起来。

步骤

1. 单击 \* 帐户设置 \*。



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

完成后

现在，您可以将用户和服务连接器与工作空间相关联。

添加用户

将 Cloud Central 用户与 Cloud Central 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](#)" 并创建帐户。
2. 在 Cloud Manager 中，单击 \* 帐户设置 \*。
3. 在用户选项卡中，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。
5. 如果选择了 Workspace Admin，请选择一个或多个要与该用户关联的工作空间。

**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

6. 单击 \* 关联用户 \*。

## 结果

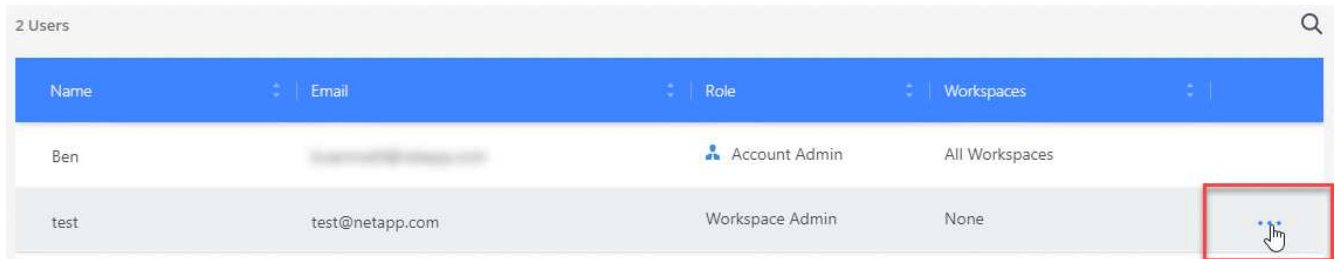
用户应从 NetApp Cloud Central 收到一封标题为 " 客户关联 " 的电子邮件。此电子邮件包含访问 Cloud Manager 所需的信息。

## 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. 单击 \* 帐户设置 \*。
2. 单击与用户对应的行中的操作菜单。



Name	Email	Role	Workspaces
Ben	[REDACTED]	Account Admin	All Workspaces
test	test@netapp.com	Workspace Admin	None

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 \*。

### 结果

现在，只要服务连接器也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。

## 将服务连接器与工作空间相关联

服务连接器是 Cloud Manager 系统的一部分。它可以在云提供商中部署的虚拟机实例上运行，也可以在您配置的内部主机上运行。您需要将此服务连接器与工作空间相关联，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，则不需要将服务连接器与工作空间相关联。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，工作空间和服务连接器"](#)。

### 步骤

1. 单击 \* 帐户设置 \*。
2. 单击 \* 服务连接器 \*。
3. 单击要关联的服务连接器的 \* 管理工作空间 \*。
4. 选择一个或多个工作空间，然后单击 \* 应用 \*。

### 结果

现在，只要用户同时与工作空间关联，Workspace 管理员就可以访问关联的工作空间。

## 设置 **AWS** 帐户并将其添加到 **Cloud Manager**

如果要在不同的 AWS 帐户中部署 Cloud Volumes ONTAP，则需要提供所需权限并将详细信息添加到 Cloud Manager。如何提供权限取决于您是要为 Cloud Manager 提供 AWS

密钥还是要为受信任帐户中某个角色提供 ARN 。



从 Cloud Central 部署 Cloud Manager 时，Cloud Manager 会自动添加部署 Cloud Manager 的 AWS 帐户。如果您在现有系统上手动安装 Cloud Manager 软件，则不会添加初始帐户。["了解 AWS 帐户和权限"](#)。

- 选项 \*
- [通过提供 AWS 密钥授予权限](#)
- [在其他帐户中使用 IAM 角色来授予权限](#)

### 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. 从下载 Cloud Manager IAM 策略 "[Cloud Manager 策略页面](#)"。
2. 从 IAM 控制台，通过从 Cloud Manager IAM 策略复制和粘贴文本来创建您自己的策略。

["AWS 文档：创建 IAM 策略"](#)

3. 将策略附加到 IAM 角色或 IAM 用户。
  - ["AWS 文档：创建 IAM 角色"](#)
  - ["AWS 文档：添加和删除 IAM 策略"](#)

#### 结果

现在，此帐户具有所需权限。 [现在，您可以将其添加到 Cloud Manager 中。](#)

### 在其他帐户中使用 **IAM** 角色来授予权限

您可以使用 IAM 角色在部署 Cloud Manager 实例的源 AWS 帐户与其他 AWS 帐户之间建立信任关系。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，然后选择 \* 其他 AWS 帐户 \* 来创建 IAM 角色。

请务必执行以下操作：

- 输入 Cloud Manager 实例所在帐户的 ID 。
- 附加 Cloud Manager IAM 策略，该策略可从获得 "[Cloud Manager 策略页面](#)"。



## Create role



### Select type of trusted entity

Four options for trusted entity type are shown in a row:

- AWS service**: EC2, Lambda and others.
- Another AWS account**: Belonging to you or 3rd party. This option is selected and highlighted with a blue border.
- Web identity**: Cognito or any OpenID provider.
- SAML 2.0 federation**: Your corporate directory.

Allows entities in other accounts to perform actions in this account. [Learn more](#)

### Specify accounts that can use this role

Account ID\*

- Options**
- Require external ID (Best practice when a third party will assume this role)
  - Require MFA

2. 转到 Cloud Manager 实例所在的源帐户，然后选择附加到该实例的 IAM 角色。

- 单击 \* 信任关系 > 编辑信任关系 \*。
- 添加 "STS : AssumeRole" 操作以及您在目标帐户中创建的角色 ARN。
  - 示例 \*

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "sts:AssumeRole",
    "Resource": "arn:aws:iam::ACCOUNT-B-ID:role/ACCOUNT-B-ROLENAME"
  }
}
```

### 结果

现在，此帐户具有所需权限。 [现在，您可以将其添加到 Cloud Manager 中。](#)

### 将 AWS 帐户添加到 Cloud Manager

在为 AWS 帐户提供所需权限后，您可以将此帐户添加到 Cloud Manager 中。这样，您就可以在该帐户中启动 Cloud Volumes ONTAP 系统。

### 步骤

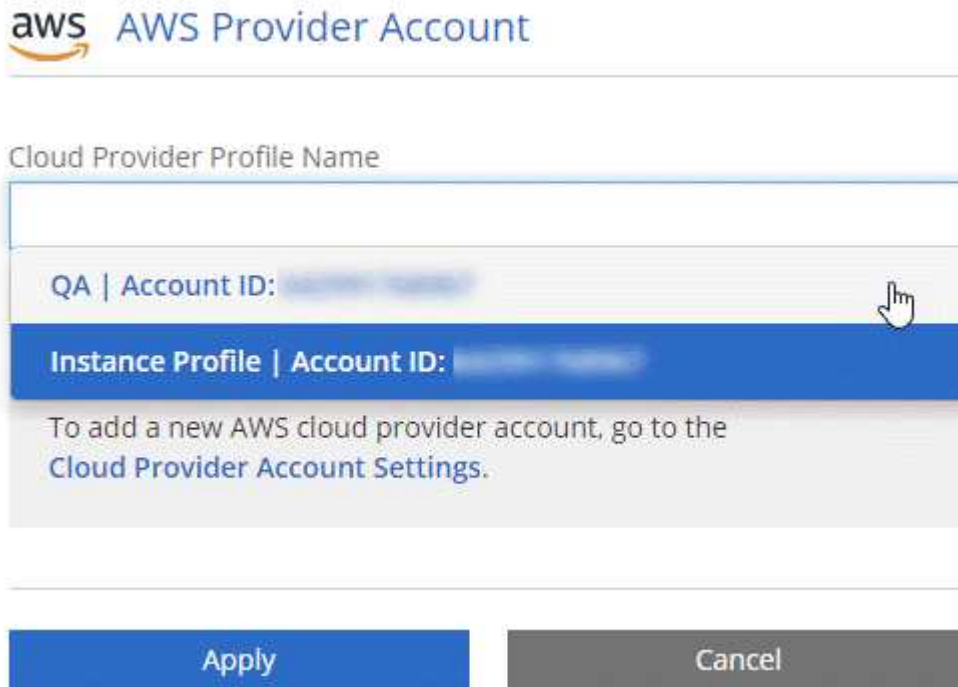
- 在 Cloud Manager 控制台的右上角，单击设置图标，然后选择 \* 云提供商和支持帐户 \*。



2. 单击 \* 添加新帐户 \* 并选择 \* AWS \* 。
3. 选择是要提供 AWS 密钥还是要提供可信 IAM 角色的 ARN 。
4. 确认已满足策略要求，然后单击 \* 创建帐户 \* 。

结果

现在，在创建新的工作环境时，您可以从 " 详细信息和凭据 " 页面切换到其他帐户：



## 设置 Azure 帐户并将其添加到 Cloud Manager

如果要在不同的 Azure 帐户中部署 Cloud Volumes ONTAP ，则需要为这些帐户提供所需的权限，然后将有关这些帐户的详细信息添加到 Cloud Manager 。



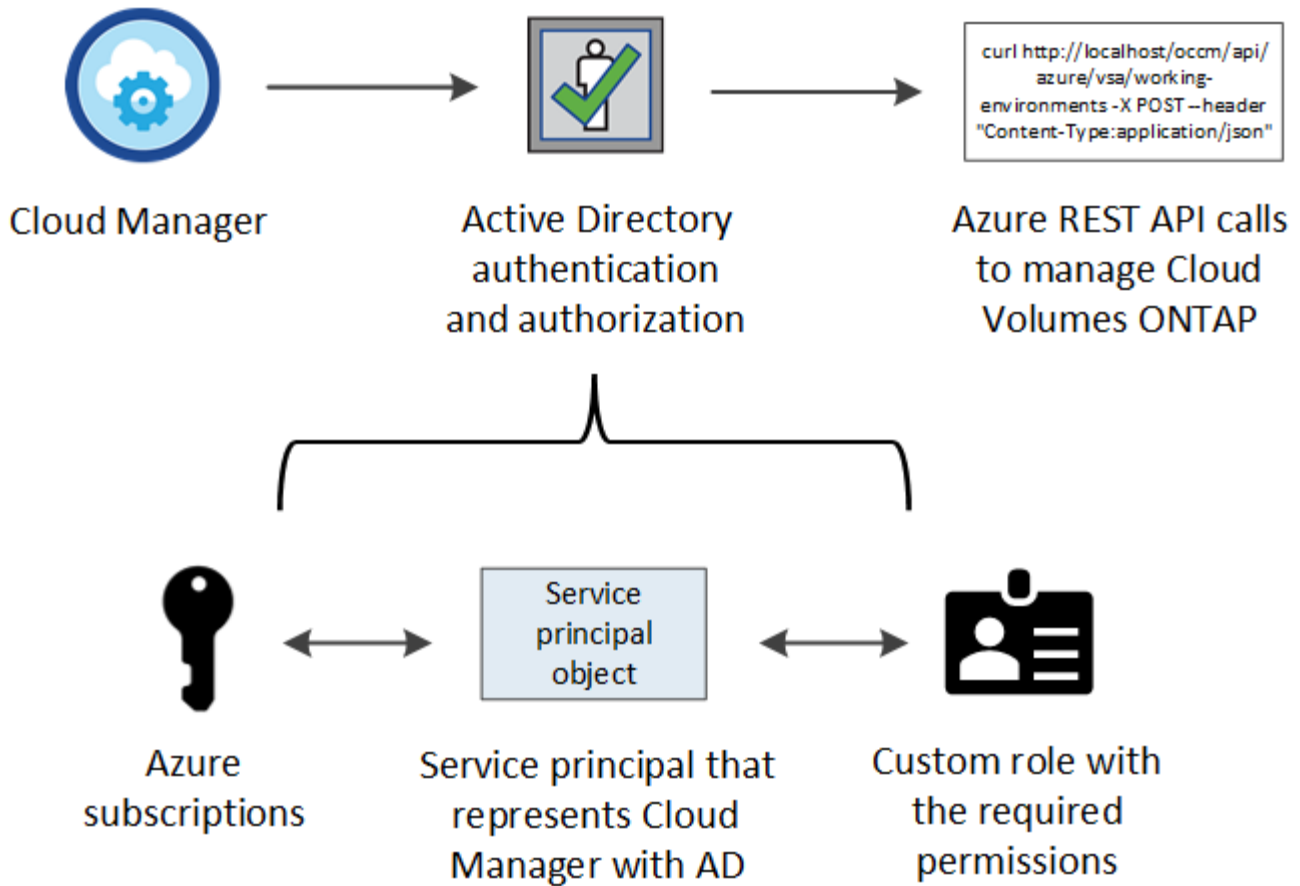
从 Cloud Central 部署 Cloud Manager 时，Cloud Manager 会自动添加部署 Cloud Manager 的 Azure 帐户。如果您在现有系统上手动安装 Cloud Manager 软件，则不会添加初始帐户。 ["了解 Azure 帐户和权限"](#)。

### 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。

### 关于此任务

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

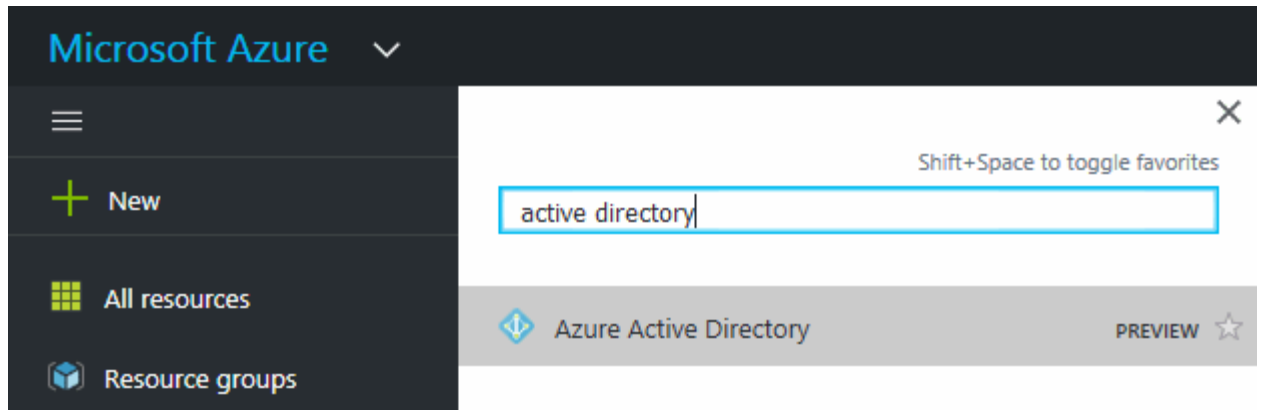
创建一个 Azure Active Directory（AD）应用程序和服务主体，Cloud Manager 可使用该应用程序和服务主体进行基于角色的访问控制。

## 开始之前

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\*：选择 \* 网络 \*，然后输入任何 URL，例如 https://url
5. 单击 \* 注册 \*。

## 结果

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. 下载 "[Cloud Manager Azure 策略](#)"。
  - 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。

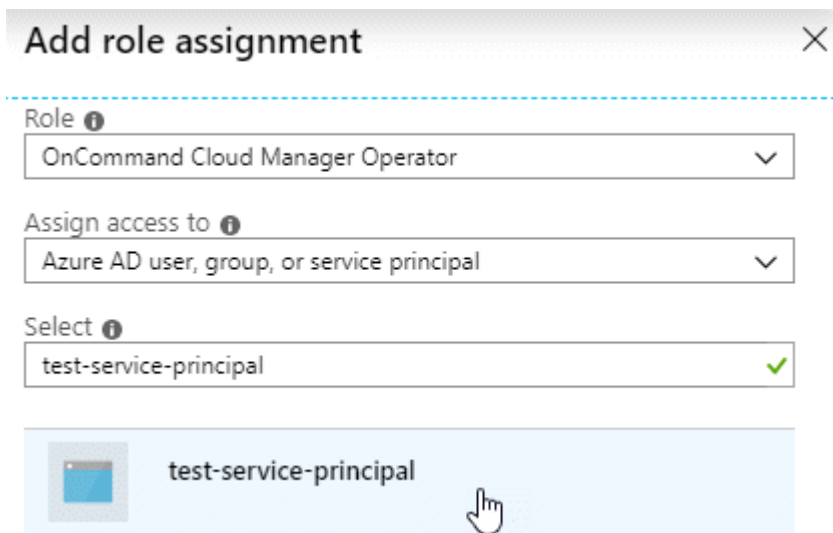
以下示例说明了如何使用 Azure CLI 2.0 创建自定义角色：

- AZ 角色定义 create -role-definition C : \Policy\_for\_cloud Manager\_Azure\_3.7.4.json\*

现在，您应具有一个名为 \_Cloud OnCommand 管理器操作员\_ 的自定义角色。

## 2. 将应用程序分配给角色：

- 从 Azure 门户中，打开 \* 订阅 \* 服务。
- 选择订阅。
- 单击 \* 访问控制 (IAM) > 添加 > 添加角色分配 \*。
- 选择 \* OnCommand 云管理器操作员 \* 角色。
- 保持选择 \* Azure AD 用户，组或服务主体 \*。
- 搜索应用程序的名称（滚动无法在列表中找到）。



- 选择应用程序并单击 \* 保存 \*。

Cloud Manager 的服务主体现在具有该订阅所需的 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


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

<b>Microsoft Graph</b> 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](#)

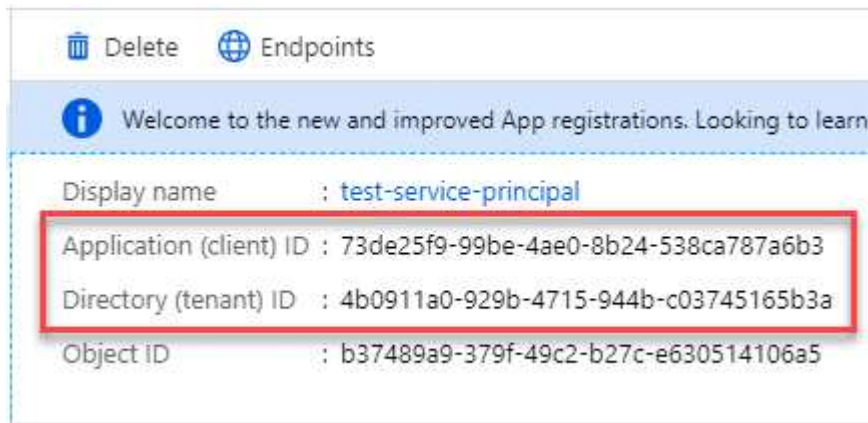
PERMISSION	ADMIN CONSENT REQUIRED
<input checked="" type="checkbox"/> <b>user_impersonation</b> Access Azure Service Management as organization users (preview) 	-

### 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。



将帐户添加到 Cloud Manager 时，Cloud Manager 会将客户端密钥称为应用程序密钥。

### 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	Copy to clipboard
test secret	8/16/2020	*sZ1jSe2By:D*-ZR0v4NLfdAcY7:+0vA	

### 结果

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 Azure 帐户添加到 Cloud Manager

在为 Azure 帐户提供所需权限后，您可以将此帐户添加到 Cloud Manager 中。这样，您就可以在该帐户中启动 Cloud Volumes ONTAP 系统。

### 步骤

1. 在 Cloud Manager 控制台的右上角，单击设置图标，然后选择 \* 云提供商和支持帐户 \* 。



2. 单击 \* 添加新帐户 \* 并选择 \* Microsoft Azure\* 。
3. 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 ID：请参见 [获取应用程序 ID 和目录 ID](#)。
  - 租户 ID（或目录 ID）：请参见 [获取应用程序 ID 和目录 ID](#)。
  - 应用程序密钥（客户端密钥）：请参见 [\[创建客户端密钥\]](#)。
4. 确认已满足策略要求，然后单击 \* 创建帐户 \* 。

### 结果

现在，在创建新的工作环境时，您可以从 " 详细信息和凭据 " 页面切换到其他帐户：





## Cloud Provider Profile Name

Azure Keys | Application ID: [redacted] ...

Dev Keys | Application ID: [redacted] ...

**Managed Service Identity**

To add a new Azure cloud provider account, go to the [Cloud Provider Account Settings](#).

Apply

Cancel

## 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 帐户和订阅。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。

## 关于此任务

托管身份为 "初始 Azure 帐户" 从 NetApp Cloud Central 部署 Cloud Manager 时。部署云管理器后、Cloud Central 创建了 OnCommand Cloud Manager 操作员角色并将其分配给云管理器虚拟机。

## 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 系统的订阅。
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 \* OnCommand 云管理器操作员 \* 角色。



OnCommand 云管理器操作员是中提供的默认名称 "Cloud Manager 策略"。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。
- 选择创建云管理器虚拟机的订阅。

- 选择 Cloud Manager 虚拟机。
- 单击 \* 保存 \*。

4. 对其他订阅重复这些步骤。

## 结果

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。

Microsoft Azure Provider Account

Cloud Provider Profile Name

Managed Service Identity

Azure Subscription

OCCM Dev

OCCM QA1 (Default)

To add a new Azure cloud provider account, go to the [Cloud Provider Account Settings](#).

Apply Cancel

## 设置 GCP 帐户并将其添加到 Cloud Manager

如果要启用 ... "数据分层" 在 Cloud Volumes ONTAP 系统上，您需要为具有存储管理员权限的服务帐户为 Cloud Manager 提供存储访问密钥。Cloud Manager 可使用访问密钥设置和管理用于数据分层的云存储分段。

为 **Google Cloud Storage** 设置服务帐户和访问密钥

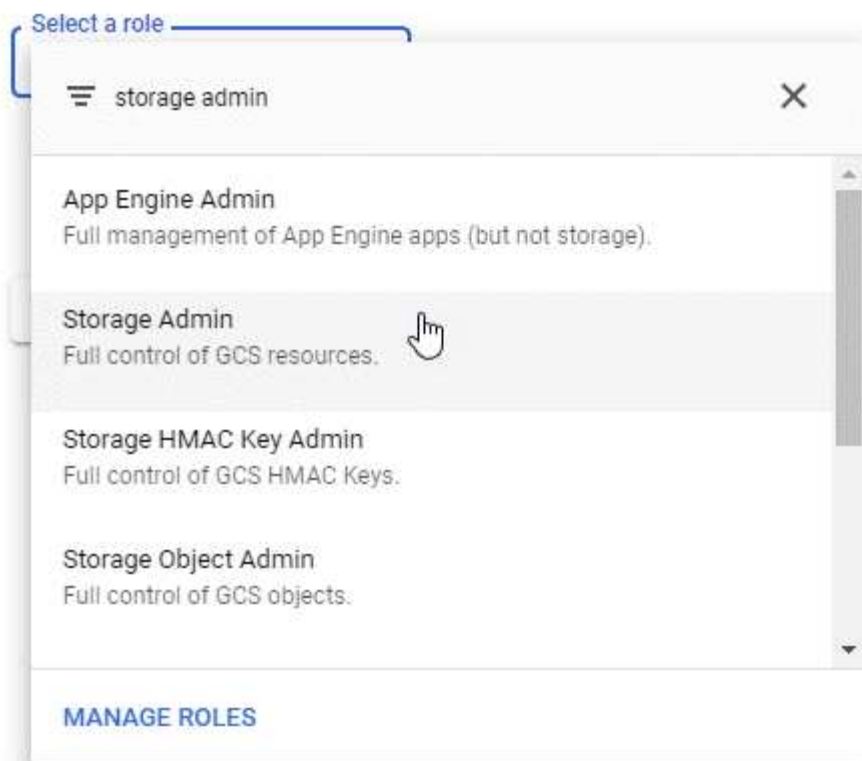
通过服务帐户，Cloud Manager 可以对用于数据分层的云存储分段进行身份验证和访问。需要提供密钥，以便 Google Cloud Storage 知道谁在发出请求。

## 步骤

1. 打开 GCP IAM 控制台和 "创建具有存储管理员角色的服务帐户"。

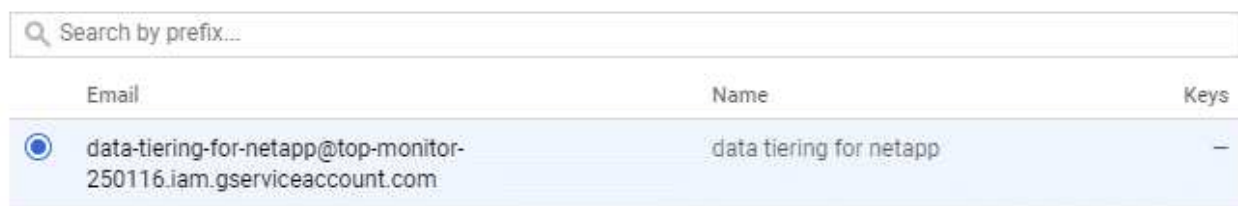
## Service account permissions (optional)

Grant this service account access to My Project 99247 so that it has permission to complete specific actions on the resources in your project. [Learn more](#)



2. 转至 "GCP 存储设置"。
3. 如果出现提示，请选择一个项目。
4. 单击 \* 互操作性 \* 选项卡。
5. 如果尚未启用互操作性访问，请单击 \* 启用互操作性访问 \*。
6. 在 \* 服务帐户的访问密钥 \* 下，单击 \* 为服务帐户创建密钥 \*。
7. 选择您在步骤 1 中创建的服务帐户。

## Select a service account



[CANCEL](#) [CREATE KEY](#) | [CREATE NEW ACCOUNT](#)

8. 单击 \* 创建密钥 \*。
9. 复制访问密钥和密钥。

在添加用于数据分层的 GCP 帐户时，您需要在 Cloud Manager 中输入此信息。

## 将 GCP 帐户添加到 Cloud Manager

现在，您已有服务帐户的访问密钥，您可以将其添加到 Cloud Manager 中。

### 步骤

1. 在 Cloud Manager 控制台的右上角，单击设置图标，然后选择 \* 云提供商和支持帐户 \*。



2. 单击 \* 添加新帐户 \* 并选择 \* GCP \*。
3. 输入服务帐户的访问密钥和密钥。

Cloud Manager 可通过这些密钥设置用于数据分层的云存储分段。

4. 确认已满足策略要求，然后单击 \* 创建帐户 \*。

### 下一步是什么？

现在，您可以在创建，修改或复制单个卷时对其启用数据分层。有关详细信息，请参见 ["将非活动数据分层到低成本对象存储"](#)。

但是，在执行此操作之前，请确保 Cloud Volumes ONTAP 所在的子网已配置为专用 Google 访问。有关说明，请参见 ["Google Cloud 文档：配置私有 Google Access"](#)。

## 将 NetApp 支持站点帐户添加到 Cloud Manager

要部署 BYOL 系统，需要将 NetApp 支持站点帐户添加到 Cloud Manager。此外，还需要注册按需购买系统并升级 ONTAP 软件。

观看以下视频，了解如何将 NetApp 支持站点帐户添加到 Cloud Manager。或向下滚动以阅读步骤。

<https://img.youtube.com/vi/V2fLTyztqYQ/maxresdefault.jpg>

### 步骤

1. 如果您还没有 NetApp 支持站点帐户，["注册一个"](#)。
2. 在 Cloud Manager 控制台的右上角，单击设置图标，然后选择 \* 云提供商和支持帐户 \*。



3. 单击 \* 添加新帐户 \* 并选择 \* NetApp 支持站点 \*。
4. 指定帐户的名称，然后输入用户名和密码。
  - 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 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。
5. 单击 \* 创建帐户。 \*

下一步是什么？

现在，用户可以在创建新 Cloud Volumes ONTAP 系统和注册现有系统时选择帐户。

- ["在 AWS 中启动 Cloud Volumes ONTAP"](#)
- ["在 Azure 中启动 Cloud Volumes ONTAP"](#)
- ["注册按需购买的系统"](#)
- ["了解 Cloud Manager 如何管理许可证文件"](#)

## 安装用于安全访问的 HTTPS 证书

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。

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	<ol style="list-style-type: none"> <li>a. 输入 Cloud Manager 主机的主机名或 DNS（其公用名），然后单击 * 生成 CSR*。</li> </ol> <p>Cloud Manager 将显示证书签名请求。</p> <ol style="list-style-type: none"> <li>b. 使用 CSR 向 CA 提交 SSL 证书请求。</li> </ol> <p>证书必须使用 Privacy Enhanced Mail（PEM）Base - 64 编码的 X.509 格式。</p> <ol style="list-style-type: none"> <li>c. 复制签名证书的内容，将其粘贴到证书字段中，然后单击 * 安装 *。</li> </ol>

选项	Description
安装您自己的 CA 签名证书	<p>a. 选择 * 安装 CA 签名证书 * 。</p> <p>b. 加载证书文件和私钥，然后单击 * 安装 * 。</p> <p>证书必须使用 Privacy Enhanced Mail （ PEM ） Base - 64 编码的 X.509 格式。</p>

## 结果

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：

### Cloud Manager HTTPS certificate

Expiration:

⚠ Oct 27, 2016 05:13:28 am

Issuer:

CN=localhost, O=NetApp, OU=Tel-Aviv,  
EMAILADDRESS=admin@example.com

Subject:

EMAILADDRESS=admin@example.com ,  
OU=Tel-Aviv, O=NetApp, CN=localhost

 [View Certificate](#)

 [Renew HTTPS Certificate](#)

## 设置 AWS KMS

如果要在 Cloud Volumes ONTAP 中使用 Amazon 加密，则需要设置 AWS 密钥管理服务（KMS）。

### 步骤

1. 确保存在有效的客户主密钥（CMK）。

CMK 可以是 AWS 管理的 CMK 或客户管理的 CMK。它可以与 Cloud Manager 和 Cloud Volumes ONTAP 位于同一个 AWS 帐户中，也可以位于不同的 AWS 帐户中。

["AWS 文档：客户主密钥（CMK）"](#)

2. 通过添加 IAM 角色来修改每个 CMK 的密钥策略，该角色以 `key user_` 的身份为 Cloud Manager 提供权限。

将 IAM 角色添加为密钥用户可为 Cloud Manager 提供在 Cloud Volumes ONTAP 中使用 CMK 的权限。

["AWS 文档：编辑密钥"](#)

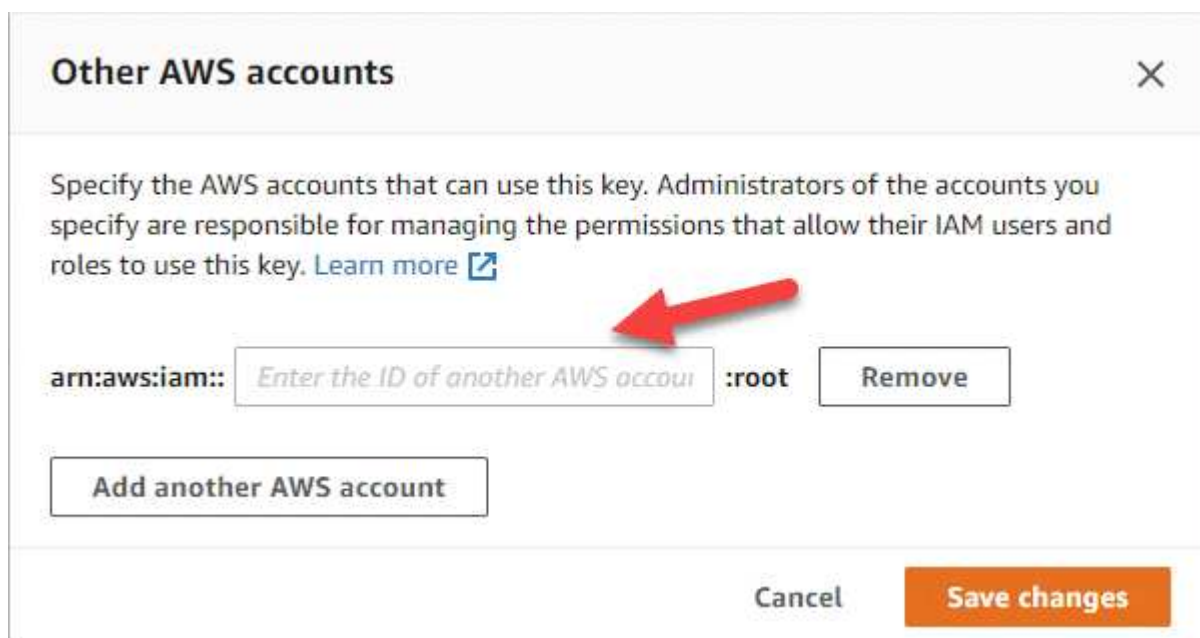
3. 如果 CMK 位于其他 AWS 帐户中，请完成以下步骤：

- a. 从 CMK 所在的帐户转到 KMS 控制台。
- b. 选择密钥。
- c. 在 \* 常规配置 \* 窗格中，复制密钥的 ARN 。

创建 Cloud Volumes ONTAP 系统时，您需要为 Cloud Manager 提供 ARN 。

- d. 在 \* 其他 AWS 帐户 \* 窗格中，添加为 Cloud Manager 提供权限的 AWS 帐户。

在大多数情况下，这是 Cloud Manager 所在的帐户。如果 Cloud Manager 未安装在 AWS 中，则您会为其提供 Cloud Manager 的 AWS 访问密钥。



- e. 现在，切换到为 Cloud Manager 提供权限的 AWS 帐户，然后打开 IAM 控制台。
- f. 创建一个包含以下权限的 IAM 策略。
- g. 将策略附加到为 Cloud Manager 提供权限的 IAM 角色或 IAM 用户。

以下策略提供了 Cloud Manager 从外部 AWS 帐户使用 CMK 所需的权限。请务必在 " 资源 " 部分中修改区域和帐户 ID 。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowUseOfTheKey",
      "Effect": "Allow",
      "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
      ],
      "Resource": [
        "arn:aws:kms:us-east-
1:externalaccountid:key/externalkeyid"
      ]
    },
    {
      "Sid": "AllowAttachmentOfPersistentResources",
      "Effect": "Allow",
      "Action": [
        "kms:CreateGrant",
        "kms:ListGrants",
        "kms:RevokeGrant"
      ],
      "Resource": [
        "arn:aws:kms:us-east-
1:externalaccountid:key/externalaccountid"
      ],
      "Condition": {
        "Bool": {
          "kms:GrantIsForAWSResource": true
        }
      }
    }
  ]
}

```

+  
 有关此过程的其他详细信息，请参见 ["AWS 文档：允许外部 AWS 帐户访问 CMK"](#)。



# 网络要求

## 云管理器的网络要求

设置您的网络，以便 Cloud Manager 可以在 AWS，Microsoft Azure 或 Google 云平台中部署 Cloud Volumes ONTAP 系统。最重要的步骤是确保对各种端点的出站 Internet 访问。



如果您的网络使用代理服务器与 Internet 进行所有通信、则在安装过程中，Cloud Manager 会提示您指定代理。也可以从 "设置" 页指定代理服务器。请参见 ["配置 Cloud Manager 以使用代理服务器"](#)。

### 连接到目标网络

Cloud Manager 需要与要部署 Cloud Volumes ONTAP 的 VPC 和 VN 集建立网络连接。

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

### 出站 Internet 访问

Cloud Manager 需要通过出站 Internet 访问来部署和管理 Cloud Volumes ONTAP。从 Web 浏览器访问 Cloud Manager 时以及在 Linux 主机上运行 Cloud Manager 安装程序时，也需要进行出站 Internet 访问。

以下各节将标识特定的端点。

#### 用于在 AWS 中管理 Cloud Volumes ONTAP 的端点

在 AWS 中部署和管理 Cloud Volumes ONTAP 时、Cloud Manager 需要通过出站 Internet 访问与以下端点联系：

端点	目的
AWS 服务 (AmazonAWS.com)： <ul style="list-style-type: none"><li>云形成</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> 确切的端点取决于您部署 Cloud Volumes ONTAP 的区域。"有关详细信息，请参阅 <a href="#">AWS 文档</a> 。"	支持 Cloud Manager 在 AWS 中部署和管理 Cloud Volumes ONTAP。
<a href="https://api.services.cloud.netapp.com:443">https://api.services.cloud.netapp.com:443</a>	对 NetApp Cloud Central 的 API 请求。
<a href="https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com">https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com</a>	提供对软件映像、清单和模板的访问。

端点	目的
<a href="https://cognito-idp.us-east-1.amazonaws.com">https://cognito-idp.us-east-1.amazonaws.com</a> <a href="https://cognito-identity.us-east-1.amazonaws.com">https://cognito-identity.us-east-1.amazonaws.com</a>	支持 Cloud Manager 访问和下载清单、模板和 Cloud Volumes ONTAP 升级映像。
<a href="https://kinesis.us-east-1.amazonaws.com">https://kinesis.us-east-1.amazonaws.com</a>	使 NetApp 能够从审计记录流化数据。
<a href="https://cloudmanager.cloud.netapp.com">https://cloudmanager.cloud.netapp.com</a>	与 Cloud Manager 服务进行通信，其中包括 Cloud Central 帐户。
<a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a>	与 NetApp Cloud Central 进行通信以实现集中式用户身份验证。
<a href="https://w86yt021u5.execute-api.us-east-1.amazonaws.com/production/whitelist">https://w86yt021u5.execute-api.us-east-1.amazonaws.com/production/whitelist</a>	用于将您的 AWS 帐户 ID 添加到备份到 S3 的允许用户列表中。
<a href="https://support.netapp.com/aods/asupmessage">https://support.netapp.com/aods/asupmessage</a> <a href="https://support.netapp.com/asupprod/post/1.0/postAsup">https://support.netapp.com/asupprod/post/1.0/postAsup</a>	与 NetApp AutoSupport 通信。
<a href="https://support.netapp.com/svgw">https://support.netapp.com/svgw</a> <a href="https://support.netapp.com/servicegw/">https://support.netapp.com/servicegw/</a> 授权	与 NetApp 沟通以获得系统许可和支持注册。
<a href="https://ipa-signer.cloudmanager.netapp.com">https://ipa-signer.cloudmanager.netapp.com</a>	允许 Cloud Manager 生成许可证（例如，适用于 Cloud Volumes ONTAP 的 FlexCache 许可证）
<a href="https://packages.cloud.google.com/yum">https://packages.cloud.google.com/yum</a> <a href="https://github.com/NetApp/trident/releases/download/">https://github.com/NetApp/trident/releases/download/</a>	要将 Cloud Volumes ONTAP 系统连接到 Kubernetes 集群，需要此许可证。这些端点支持安装 NetApp Trident。
各种第三方位置，例如： <ul style="list-style-type: none"> <li>• <a href="https://repo1.maven.org/maven2">https://repo1.maven.org/maven2</a></li> <li>• <a href="https://oss.sonatype.org/content/repository">https://oss.sonatype.org/content/repository</a></li> <li>• <a href="https://repo.typesafe.org">https://repo.typesafe.org</a></li> </ul> <p>第三方位置可能会发生变化。</p>	在升级过程中、Cloud Manager 会下载最新的软件包以满足第三方依赖性。

用于在 Azure 中管理 Cloud Volumes ONTAP 的端点

在 Microsoft Azure 中部署和管理 Cloud Volumes ONTAP 时，Cloud Manager 需要通过出站 Internet 访问与以下端点联系：

端点	目的
<a href="https://management.azure.com">https://management.azure.com</a> <a href="https://login.microsoftonline.com">https://login.microsoftonline.com</a>	支持 Cloud Manager 在大多数 Azure 区域部署和管理 Cloud Volumes ONTAP。
<a href="https://management.microsoftazure.de">https://management.microsoftazure.de</a> <a href="https://login.microsoftonline.de">https://login.microsoftonline.de</a>	支持 Cloud Manager 在 Azure Germany 地区部署和管理 Cloud Volumes ONTAP。
<a href="https://management.usgovcloudapi.net">https://management.usgovcloudapi.net</a> <a href="https://login.microsoftonline.com">https://login.microsoftonline.com</a>	支持 Cloud Manager 在 Azure US Gov 区域部署和管理 Cloud Volumes ONTAP。
<a href="https://api.services.cloud.netapp.com:443">https://api.services.cloud.netapp.com:443</a>	对 NetApp Cloud Central 的 API 请求。

端点	目的
<a href="https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com">https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com</a>	提供对软件映像、清单和模板的访问。
<a href="https://cognito-idp.us-east-1.amazonaws.com">https://cognito-idp.us-east-1.amazonaws.com</a> <a href="https://cognito-identity.us-east-1.amazonaws.com">https://cognito-identity.us-east-1.amazonaws.com</a> <a href="https://sts.amazonaws.com">https://sts.amazonaws.com</a>	支持 Cloud Manager 访问和下载清单、模板和 Cloud Volumes ONTAP 升级映像。
<a href="https://kinesis.us-east-1.amazonaws.com">https://kinesis.us-east-1.amazonaws.com</a>	使 NetApp 能够从审计记录流化数据。
<a href="https://cloudmanager.cloud.netapp.com">https://cloudmanager.cloud.netapp.com</a>	与 Cloud Manager 服务进行通信，其中包括 Cloud Central 帐户。
<a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a>	与 NetApp Cloud Central 进行通信以实现集中式用户身份验证。
<a href="https://mysupport.netapp.com">https://mysupport.netapp.com</a>	与 NetApp AutoSupport 通信。
<a href="https://support.netapp.com/svgw">https://support.netapp.com/svgw</a> <a href="https://support.netapp.com/servicegw/">https://support.netapp.com/servicegw/</a> 授权	与 NetApp 沟通以获得系统许可和支持注册。
<a href="https://ipa-signer.cloudmanager.netapp.com">https://ipa-signer.cloudmanager.netapp.com</a>	允许 Cloud Manager 生成许可证（例如，适用于 Cloud Volumes ONTAP 的 FlexCache 许可证）
<a href="https://packages.cloud.google.com/yum">https://packages.cloud.google.com/yum</a> <a href="https://github.com/NetApp/trident/releases/download/">https://github.com/NetApp/trident/releases/download/</a>	要将 Cloud Volumes ONTAP 系统连接到 Kubernetes 集群，需要此许可证。这些端点支持安装 NetApp Trident。
各种第三方位置，例如： <ul style="list-style-type: none"> <li>• <a href="https://repo1.maven.org/maven2">https://repo1.maven.org/maven2</a></li> <li>• <a href="https://oss.sonatype.org/content/repository">https://oss.sonatype.org/content/repository</a></li> <li>• <a href="https://repo.typesafe.org">https://repo.typesafe.org</a></li> </ul> <p>第三方位置可能会发生变化。</p>	在升级过程中、Cloud Manager 会下载最新的软件包以满足第三方依赖性。

用于在 GCP 中管理 Cloud Volumes ONTAP 的端点

在 GCP 中部署和管理 Cloud Volumes ONTAP 时、Cloud Manager 需要通过出站 Internet 访问与以下端点联系：

端点	目的
<a href="https://www.googleapis.com">https://www.googleapis.com</a>	使 Cloud Manager 能够联系 Google API 以在 GCP 中部署和管理 Cloud Volumes ONTAP。
<a href="https://api.services.cloud.netapp.com:443">https://api.services.cloud.netapp.com:443</a>	对 NetApp Cloud Central 的 API 请求。
<a href="https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com">https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com</a>	提供对软件映像、清单和模板的访问。
<a href="https://cognito-idp.us-east-1.amazonaws.com">https://cognito-idp.us-east-1.amazonaws.com</a> <a href="https://cognito-identity.us-east-1.amazonaws.com">https://cognito-identity.us-east-1.amazonaws.com</a> <a href="https://sts.amazonaws.com">https://sts.amazonaws.com</a>	支持 Cloud Manager 访问和下载清单、模板和 Cloud Volumes ONTAP 升级映像。

端点	目的
<a href="https://kinesis.us-east-1.amazonaws.com">https://kinesis.us-east-1.amazonaws.com</a>	使 NetApp 能够从审计记录流化数据。
<a href="https://cloudmanager.cloud.netapp.com">https://cloudmanager.cloud.netapp.com</a>	与 Cloud Manager 服务进行通信，其中包括 Cloud Central 帐户。
<a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a>	与 NetApp Cloud Central 进行通信以实现集中式用户身份验证。
<a href="https://mysupport.netapp.com">https://mysupport.netapp.com</a>	与 NetApp AutoSupport 通信。
<a href="https://support.netapp.com/svgw">https://support.netapp.com/svgw</a> <a href="https://support.netapp.com/servicegw/">https://support.netapp.com/servicegw/</a> 授权	与 NetApp 沟通以获得系统许可和支持注册。
<a href="https://ipa-signer.cloudmanager.netapp.com">https://ipa-signer.cloudmanager.netapp.com</a>	允许 Cloud Manager 生成许可证（例如，适用于 Cloud Volumes ONTAP 的 FlexCache 许可证）
<a href="https://packages.cloud.google.com/yum">https://packages.cloud.google.com/yum</a> <a href="https://github.com/NetApp/trident/releases/download/">https://github.com/NetApp/trident/releases/download/</a>	要将 Cloud Volumes ONTAP 系统连接到 Kubernetes 集群，需要此许可证。这些端点支持安装 NetApp Trident。
<p>各种第三方位置，例如：</p> <ul style="list-style-type: none"> <li>• <a href="https://repo1.maven.org/maven2">https://repo1.maven.org/maven2</a></li> <li>• <a href="https://oss.sonatype.org/content/repository">https://oss.sonatype.org/content/repository</a></li> <li>• <a href="https://repo.typesafe.org">https://repo.typesafe.org</a></li> </ul> <p>第三方位置可能会发生变化。</p>	在升级过程中、Cloud Manager 会下载最新的软件包以满足第三方依赖性。

从 **Web** 浏览器访问的端点

用户必须从 Web 浏览器访问 Cloud Manager。运行 Web 浏览器的计算机必须连接到以下端点：

端点	目的
云管理器主机	<p>要加载 Cloud Manager 控制台，必须从 Web 浏览器输入主机的 IP 地址。</p> <p>根据您与云提供商的连接，您可以使用分配给主机的专用 IP 或公有 IP：</p> <ul style="list-style-type: none"> <li>• 如果您对虚拟网络具有 VPN 和直接连接访问权限，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>在任何情况下，您都应确保安全组规则仅允许从授权的 IP 或子网进行访问，从而确保网络访问的安全。</p>
<a href="https://auth0.com">https://auth0.com</a> <a href="https://cdn.auth0.com">https://cdn.auth0.com</a> <a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.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。

用于在 Linux 主机上安装 Cloud Manager 的端点

在安装过程中，Cloud Manager 安装程序必须访问以下 URL：

- <http://dev.mysql.com/get/mysql-community-release-el7-5.noarch.rpm>
- <https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm>
- <https://s3.amazonaws.com/aws-cli/awscsi-bundle.zip>

端口和安全组

- 如果您是从 Cloud Central 或 Marketplace 映像部署 Cloud Manager，请参阅以下内容：
  - ["AWS 中云管理器的安全组规则"](#)
  - ["Azure 中云管理器的安全组规则"](#)
  - ["GCP 中 Cloud Manager 的防火墙规则"](#)
- 如果您在现有 Linux 主机上安装 Cloud Manager，请参见 ["云管理器主机要求"](#)。

## AWS 中的 Cloud Volumes ONTAP 的网络要求

设置 AWS 网络，以便 Cloud Volumes ONTAP 系统可以正常运行。

适用于 Cloud Volumes ONTAP 的一般 AWS 网络要求

以下要求必须在 AWS 中满足。

### Cloud Volumes ONTAP 节点的出站 Internet 访问

Cloud Volumes ONTAP 节点需要出站 Internet 访问才能向 NetApp AutoSupport 发送消息、NetApp AutoSupport 主动监控存储的运行状况。

路由和防火墙策略必须允许 AWS HTTP/HTTPS 流量传输到以下端点，以便 Cloud Volumes ONTAP 可以发送 AutoSupport 消息：

- <https://support.netapp.com/aods/asupmessage>
- <https://support.netapp.com/asupprod/post/1.0/postAsup>

如果您有 NAT 实例，则必须定义允许 HTTPS 流量从私有子网传输到 Internet 的入站安全组规则。

### HA 调解器的出站 Internet 访问

HA 调解器实例必须具有与 AWS EC2 服务的出站连接，以便能够帮助进行存储故障转移。要提供连接，可以添加公共 IP 地址、指定代理服务器或使用手动选项。

手动选项可以是 NAT 网关或从目标子网到 AWS EC2 服务的接口 VPC 端点。有关 VPC 端点的详细信息，请参见 ["AWS 文档：接口 VPC 端点（AWS PrivateLink）"](#)。

### IP 地址数

Cloud Manager 会将以下数量的 IP 地址分配给 AWS 中的 Cloud Volumes ONTAP：

- 单个节点：6 个 IP 地址

- 单个 AZs 中的 HA 对： 15 个地址
- 多个 AZs 中的 HA 对： 15 或 16 个 IP 地址

请注意， Cloud Manager 会在单节点系统上创建 SVM 管理 LIF ， 但不会在单个 AZ 中的 HA 对上创建。您可以选择是否在多个 AZs 中的 HA 对上创建 SVM 管理 LIF 。



LIF 是与物理端口关联的 IP 地址。 SnapCenter 等管理工具需要 SVM 管理 LIF 。

## 安全组

您不需要创建安全组， 因为 Cloud Manager 可以为您提供这些功能。 如果您需要使用自己的， 请参见 ["安全组规则"](#)。

## 从 Cloud Volumes ONTAP 连接到 AWS S3 以进行数据分层

如果要将 EBS 用作性能层、 将 AWS S3 用作容量层、 则必须确保 Cloud Volumes ONTAP 与 S3 建立连接。 提供该连接的最佳方法是创建到 S3 服务的 VPC 端点。 有关说明， 请参见 ["AWS 文档： 创建网关端点"](#)。

创建 VPC 端点时， 请确保选择与 Cloud Volumes ONTAP 实例对应的区域、 VPC 和路由表。 您还必须修改安全组才能添加出站 HTTPS 规则、 该规则允许通信到 S3 端点。 否则， Cloud Volumes ONTAP 无法连接到 S3 服务。

如果遇到任何问题， 请参见 ["AWS 支持知识中心： 为什么我无法使用网关 VPC 端点连接到 S3 存储分段？"](#)

## 连接到其他网络中的 ONTAP 系统

要在 AWS 中的 Cloud Volumes ONTAP 系统和其他网络中的 ONTAP 系统之间复制数据、 您必须在 AWS VPC 和其他网络之间建立 VPN 连接—例如 Azure VNet 或您的公司网络。 有关说明， 请参见 ["AWS 文档： 设置 AWS VPN 连接"](#)。

## 用于 CIFS 的 DNS 和 Active Directory

如果要配置 CIFS 存储、 必须在 AWS 中设置 DNS 和 Active Directory 或将内部设置扩展到 AWS 。

DNS 服务器必须为 Active Directory 环境提供名称解析服务。 您可以将 DHCP 选项集配置为使用默认的 EC2 DNS 服务器、 该服务器不能是 Active Directory 环境使用的 DNS 服务器。

有关说明， 请参见 ["AWS 文档： AWS 云上的 Active Directory 域服务： 快速入门参考部署"](#)。

## 适用于多个 AWS 中的 Cloud Volumes ONTAP HA 的 AWS 网络要求

其他 AWS 网络要求适用于使用多可用性区域（ Azs ） 的 Cloud Volumes ONTAP HA 配置。 您应该在启动 HA 对之前查看这些要求、 因为您必须在 Cloud Manager 中输入网络详细信息。

要了解 HA 对的工作原理， 请参见 ["高可用性对"](#)。

## 可用性区域

此 HA 部署模型使用多个 AUS 来确保数据的高可用性。 您应该为每个 Cloud Volumes ONTAP 实例和调解器实例使用专用的 AZ ， 该实例在 HA 对之间提供通信通道。

## 用于 NAS 数据和集群 /SVM 管理的浮动 IP 地址

多个 AZs 中的 HA 配置使用浮动 IP 地址， 如果发生故障， 这些地址会在节点之间迁移。 除非您自己， 否则它们不能从 VPC 外部本机访问 ["设置 AWS 传输网关"](#)。

一个浮动 IP 地址用于集群管理、一个用于节点 1 上的 NFS/CIFS 数据、一个用于节点 2 上的 NFS/CIFS 数据。SVM 管理的第四个浮动 IP 地址是可选的。



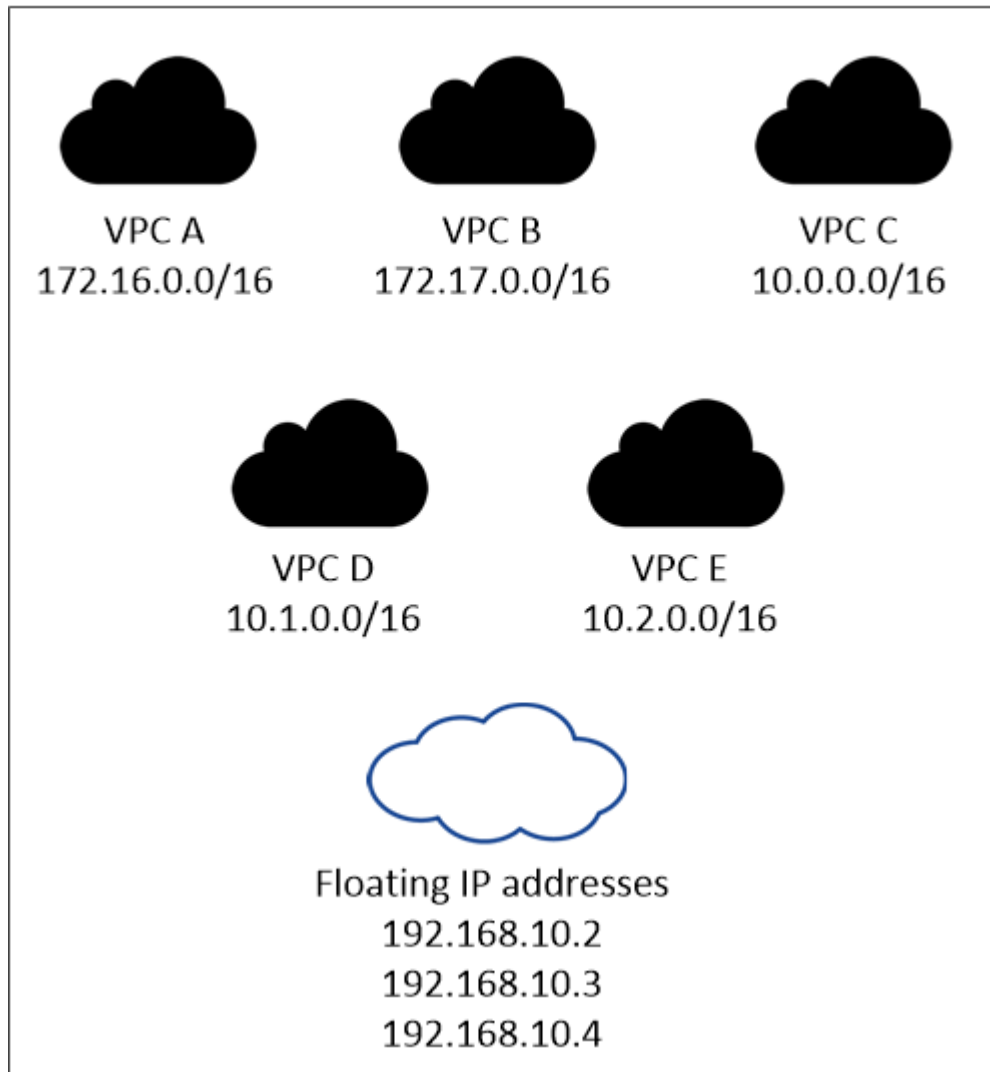
如果将 SnapDrive for Windows 或 SnapCenter 与 HA 对结合使用，则 SVM 管理 LIF 需要浮动 IP 地址。如果在部署系统时未指定 IP 地址，则可以稍后创建 LIF。有关详细信息，请参见["设置 Cloud Volumes ONTAP"](#)。

创建 Cloud Volumes ONTAP HA 工作环境时，您需要在 Cloud Manager 中输入浮动 IP 地址。在启动系统时，Cloud Manager 会将 IP 地址分配给 HA 对。

对于部署 HA 配置的 AWS 区域中的所有 vPC，浮动 IP 地址必须不在 CIDR 块的范围内。将浮动 IP 地址视为您所在地区 VPC 之外的逻辑子网。

以下示例显示了 AWS 区域中浮动 IP 地址与 VPC 之间的关系。虽然浮动 IP 地址不在所有 VPC 的 CIDR 块之外，但它们可以通过路由表路由到子网。

### AWS region



Cloud Manager 可自动创建用于 iSCSI 访问和从 VPC 外部的客户端进行 NAS 访问的静态 IP 地址。您无需满足这些类型的 IP 地址的任何要求。

传输网关，用于从 **VPC** 外部启用浮动 IP 访问

"设置 [AWS 传输网关](#)" 允许从 HA 对所在的 VPC 外部访问 HA 对的浮动 IP 地址。

## 路由表

在 Cloud Manager 中指定浮动 IP 地址后，您需要选择应包含浮动 IP 地址路由的路由表。这将启用客户端对 HA 对的访问。

如果 VPC 中的子网只有一个路由表（主路由表），则 Cloud Manager 会自动将浮动 IP 地址添加到该路由表中。如果您有多个路由表，则在启动 HA 对时选择正确的路由表非常重要。否则，某些客户端可能无法访问 Cloud Volumes ONTAP。

例如，您可能有两个子网与不同的路由表相关联。如果选择路由表 A，而不选择路由表 B，则与路由表 A 关联的子网中的客户端可以访问 HA 对，但与路由表 B 关联的子网中的客户端无法访问。

有关路由表的详细信息，请参见 "[AWS 文档：路由表](#)"。

## 与 **NetApp** 管理工具的连接

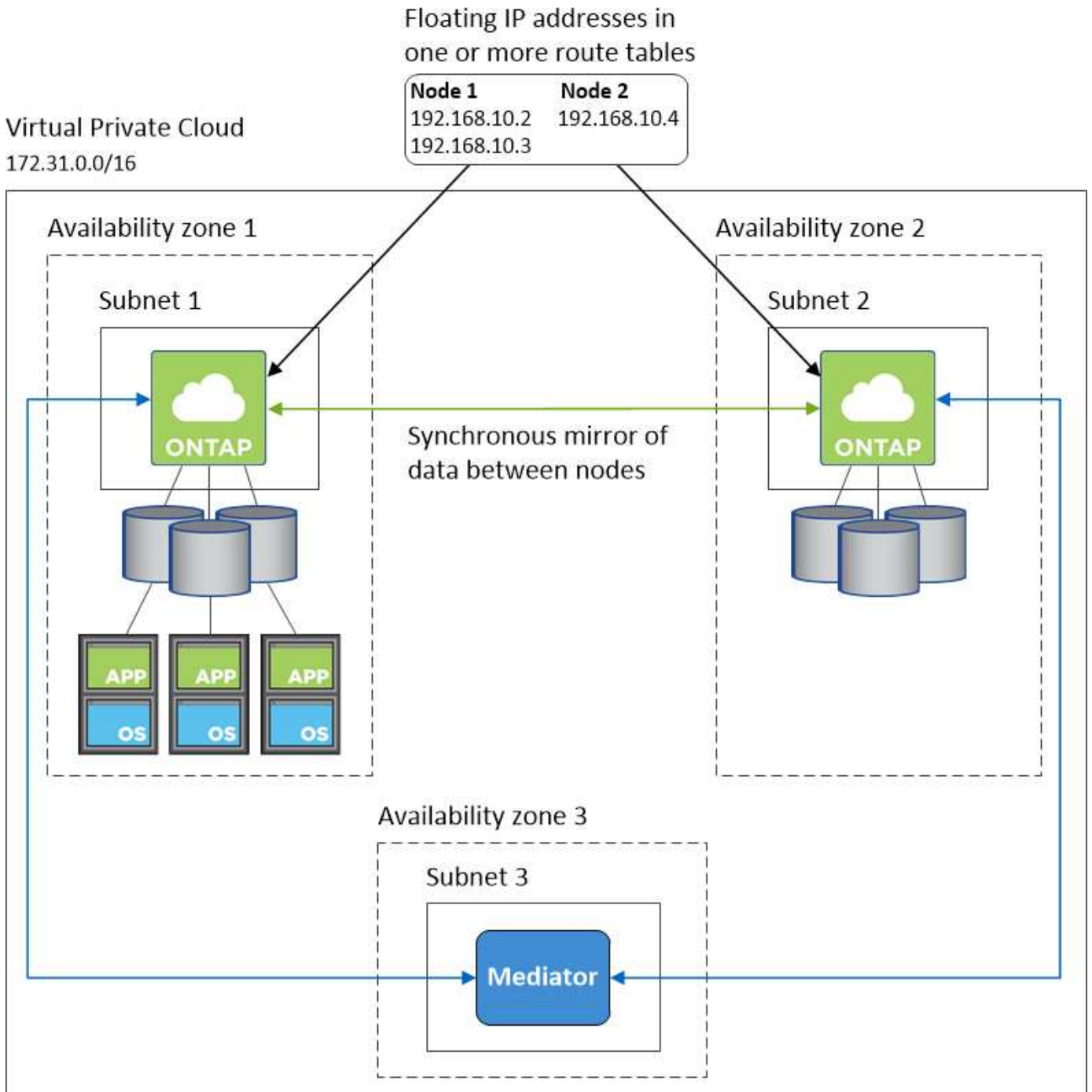
要对多个 AZs 中的 HA 配置使用 NetApp 管理工具，您可以选择两种连接方式：

1. 在其他 VPC 和中部署 NetApp 管理工具 "[设置 AWS 传输网关](#)"。通过网关，可以从 VPC 外部访问集群管理接口的浮动 IP 地址。
2. 在与 NAS 客户端具有类似路由配置的另一 VPC 中部署 NetApp 管理工具。

## 配置示例

下图显示了作为主动 - 被动配置运行的 AWS 中的最佳 HA 配置：





### VPC 配置示例

为了更好地了解如何在 AWS 中部署 Cloud Manager 和 Cloud Volumes ONTAP、您应该查看最常见的 VPC 配置。

- 具有公共和私有子网以及 NAT 设备的 VPC
- 一台带有专用子网和 VPN 连接的 VPC 到您的网络

#### 具有公共和私有子网以及 NAT 设备的 VPC

此 VPC 配置包括公共和私有子网、将 VPC 连接到 Internet 的 Internet 网关、以及公共子网中启用来自私有子网的出站 Internet 流量的 NAT 网关或 NAT 实例。在此配置中、您可以在公共子网或私有子网中运行 Cloud

Manager、但建议使用公共子网，因为它允许从 VPC 外部的进行访问。然后，您可以在私有子网中启动 Cloud Volumes ONTAP 实例。

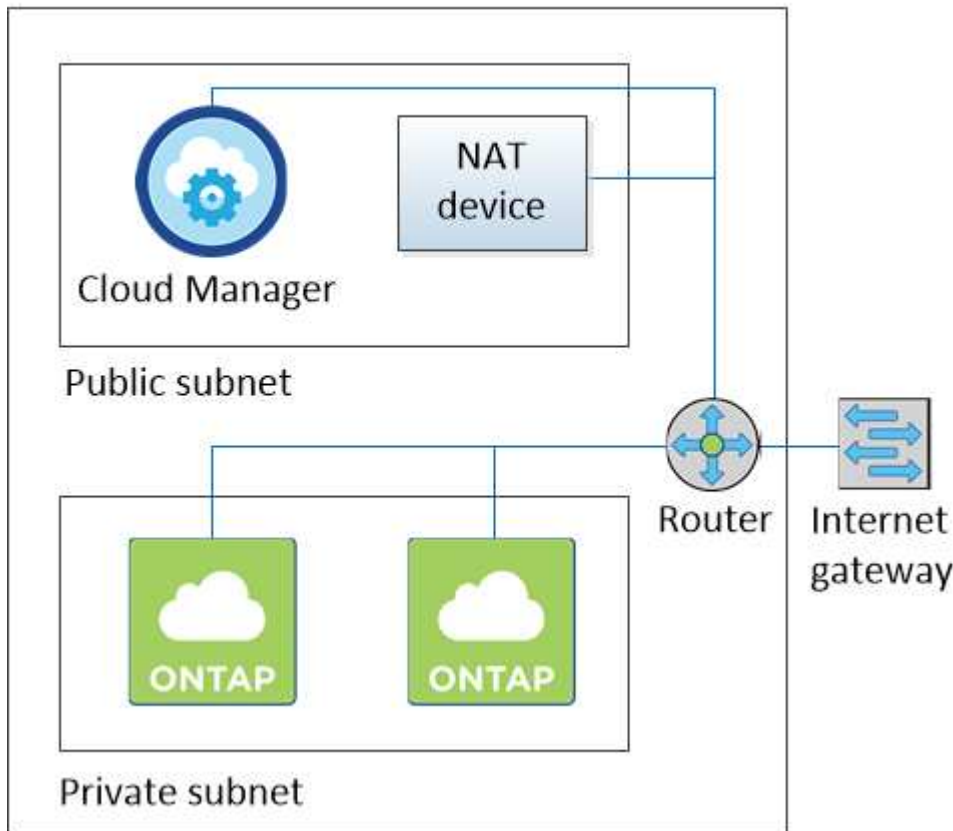


您可以使用 HTTP 代理来提供 Internet 连接，而不是 NAT 设备。

有关此场景的更多详细信息，请参见 ["AWS 文档：场景 2：采用公有和专用子网（NAT）的 VPC"](#)。

下图显示了在公共子网中运行的云管理器以及在私有子网中运行的单节点系统：

## Virtual Private Cloud



一台带有专用子网和 VPN 连接的 VPC 到您的网络

此 VPC 配置是一种混合云配置，其中 Cloud Volumes ONTAP 将成为私有环境的扩展。此配置包括私有子网和虚拟专用网关、该网关与您的网络建立 VPN 连接。通过 VPN 隧道进行路由允许 EC2 实例通过网络和防火墙访问 Internet。您可以在私有子网或数据中心运行 Cloud Manager。然后，您将在私有子网中启动 Cloud Volumes ONTAP。



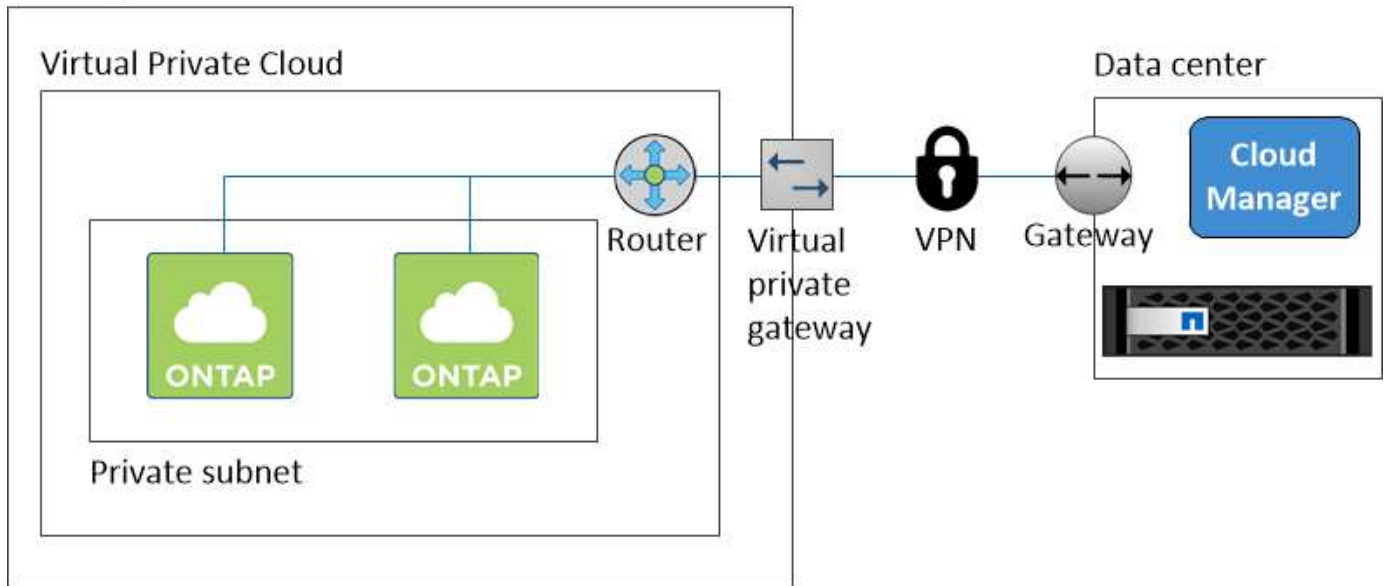
您也可以使用此配置中的代理服务器来允许 Internet 访问。代理服务器可以位于数据中心或 AWS 中。

如果要在数据中心的 FAS 系统和 AWS 中的 Cloud Volumes ONTAP 系统之间复制数据，则应使用 VPN 连接以确保链接的安全。

有关此场景的更多详细信息，请参见 ["AWS 文档：场景 4：仅使用专用子网的 VPC 和 AWS 托管 VPN 访问"](#)。

下图显示了在数据中心的云管理器以及在私有子网中运行的单节点系统：

## AWS region



## 为多个 AZs 中的 HA 对设置 AWS 传输网关

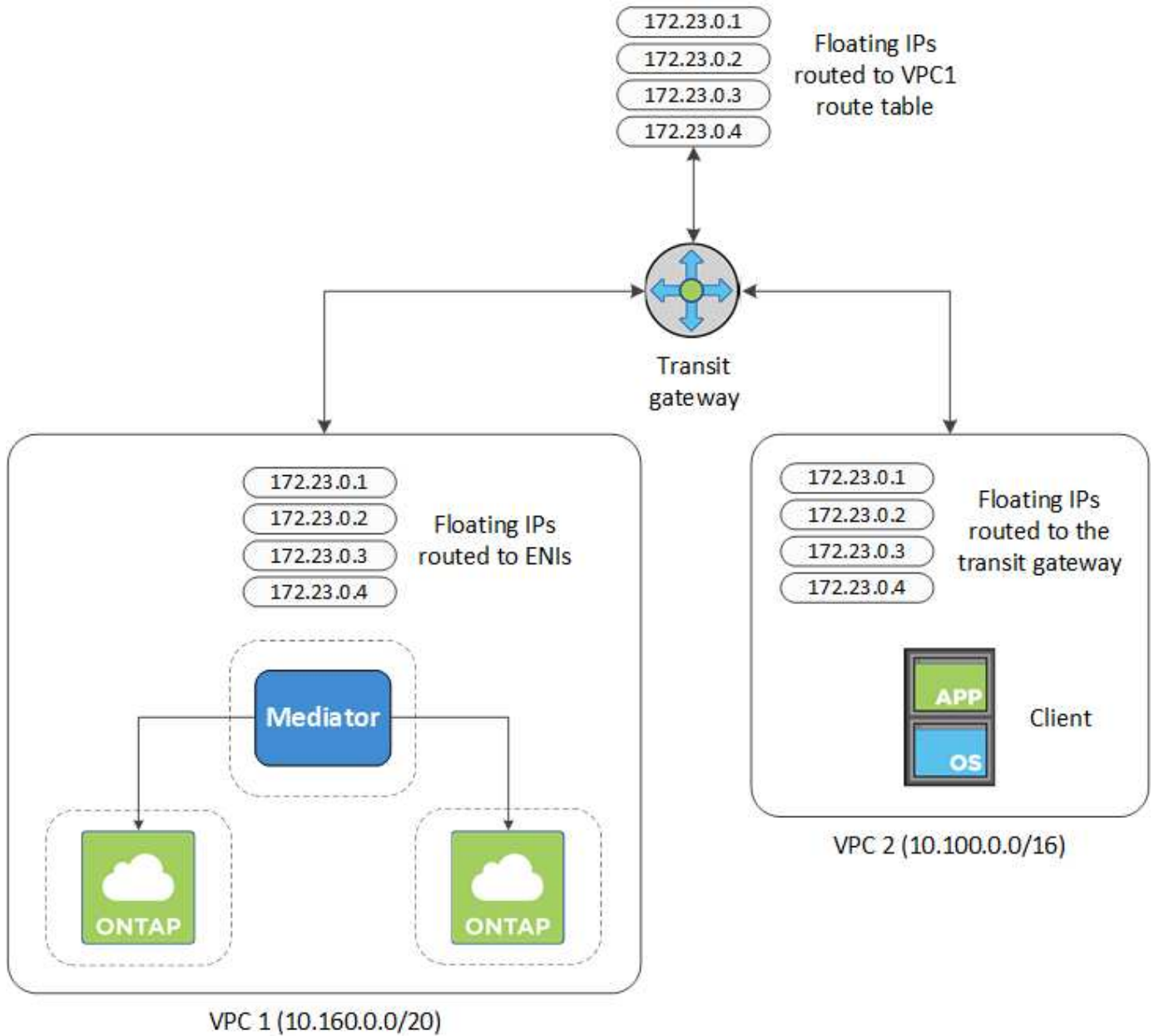
设置 AWS 传输网关，以便能够从 HA 对所在的 VPC 外部访问 HA 对的浮动 IP 地址。

如果 Cloud Volumes ONTAP HA 配置分布在多个 AWS 可用性区域中，则从 VPC 内部访问 NAS 数据需要浮动 IP 地址。这些浮动 IP 地址可以在发生故障时在节点之间迁移，但无法从 VPC 外部本机访问。独立的专用 IP 地址可从 VPC 外部提供数据访问，但不提供自动故障转移。

集群管理接口和可选 SVM 管理 LIF 也需要浮动 IP 地址。

如果您设置了 AWS 传输网关，则可以从 HA 对所在的 VPC 外部访问浮动 IP 地址。这意味着 VPC 外部的 NAS 客户端和 NetApp 管理工具可以访问浮动 IP。

以下示例显示了通过传输网关连接的两个 vPC。一个 HA 系统驻留在一个 VPC 中，而一个客户端驻留在另一个 VPC 中。然后，您可以使用浮动 IP 地址在客户端上挂载 NAS 卷。



以下步骤说明了如何设置类似的配置。

#### 步骤

1. "创建传输网关并将 vPC 连接到该网关"。
2. 通过指定 HA 对的浮动 IP 地址，在传输网关的路由表中创建路由。

您可以在 Cloud Manager 的 "工作环境信息" 页面上找到浮动 IP 地址。以下是一个示例：

## NFS & CIFS access from within the VPC using Floating IP

### Auto failover

Cluster Management : 172.23.0.1

Data (nfs,cifs) : Node 1: 172.23.0.2 | Node 2: 172.23.0.3

### Access

SVM Management : 172.23.0.4

下图示例显示了传输网关的路由表。它包括到 Cloud Volumes ONTAP 所使用的两个 vPC 的 CIDR 块和四个浮动 IP 地址的路由。

Transit Gateway Route Table: tgw-rtb-0ea8ee291c7aeddd3

Details Associations Propagations **Routes** Tags

The table below will return a maximum of 1000 routes. Narrow the filter or use export routes to view more routes.

Create route Replace route Delete route

Filter by attributes or search by keyword

<input type="checkbox"/>	CIDR	Attachment	Resource type	Route type	Route state
<input type="checkbox"/>	10.100.0.0/16	tgw-attach-05e77bd34e2ff91f8   vpc-0b2bc30e0dc8e0db1	VPC2	propagated	active
<input type="checkbox"/>	10.160.0.0/20	tgw-attach-00eba3eac3250d7db   vpc-673ae603	VPC1	propagated	active
<input type="checkbox"/>	172.23.0.1/32	tgw-attach-00eba3eac3250d7db   vpc-673ae603	VPC	static	active
<input type="checkbox"/>	172.23.0.2/32	tgw-attach-00eba3eac3250d7db   vpc-673ae603	Floating IP	static	active
<input type="checkbox"/>	172.23.0.3/32	tgw-attach-00eba3eac3250d7db   vpc-673ae603	Floating IP	static	active
<input type="checkbox"/>	172.23.0.4/32	tgw-attach-00eba3eac3250d7db   vpc-673ae603	Floating IP	static	active

**Floating IP Addresses**

3. 修改需要访问浮动 IP 地址的 vPC 的路由表。

- 向浮动 IP 地址添加路由条目。
- 向 HA 对所在 VPC 的 CIDR 块添加路由条目。

下图示例显示了 VPC 2 的路由表，其中包括指向 VPC 1 的路由和浮动 IP 地址。

Route Table: rtb-0569a1bd740ed033f

Summary Routes Subnet Associations Route Propagation Tags

Edit routes

View All routes

Destination	Target	Status	Propagated
10.100.0.0/16	local	active	No
0.0.0.0/0	igw-07250bd01781e67df	active	No
10.160.0.0/20	tgw-015b7c249661ac279	active	No
172.23.0.1/32	tgw-015b7c249661ac279	active	No
172.23.0.2/32	tgw-015b7c249661ac279	active	No
172.23.0.3/32	tgw-015b7c249661ac279	active	No
172.23.0.4/32	tgw-015b7c249661ac279	active	No

VPC1  
Floating IP Addresses

4. 通过向需要访问浮动 IP 地址的 VPC 添加路由来修改 HA 对的 VPC 的路由表。

此步骤非常重要，因为它会完成 VPC 之间的路由。

下图示例显示了 VPC 1 的路由表。它包括一条指向浮动 IP 地址和客户端所在 VPC 2 的路由。Cloud Manager 在部署 HA 对时会自动将浮动 IP 添加到路由表中。

Summary Routes Subnet Associations Route Propagation Tags

Edit routes

View All routes

Destination	Target	Status
10.160.0.0/20	local	active
pl-68a54001 (com.amazonaws.us-west-2.s3, 54.231.160.0/19, 52.218.128.0/17, 52.92.32.0/22)	vpce-cb51a0a2	active
0.0.0.0/0	igw-b2182cd7	active
10.60.29.0/25	pcx-589c3331	active
10.100.0.0/16	tgw-015b7c249661ac279	active
10.129.0.0/20	pcx-f7e1396	active
172.23.0.1/32	eni-0854d4715559c3cdb	active
172.23.0.2/32	eni-0854d4715559c3cdb	active
172.23.0.3/32	eni-0f76681216c3108ed	active
172.23.0.4/32	eni-0854d4715559c3cdb	active

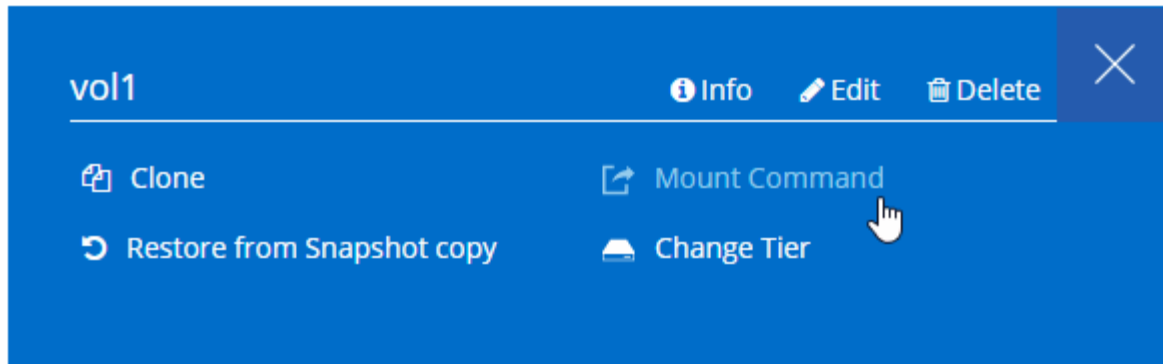
VPC2  
Floating IP Addresses

5. 使用浮动 IP 地址将卷挂载到客户端。

通过选择卷并单击 \* 挂载命令 \*，您可以在 Cloud Manager 中找到正确的 IP 地址。

# Volumes

2 Volumes | 0.22 TB Allocated | < 0.01 TB Used (0 TB in S3)



- 相关链接 \*
- "AWS 中的高可用性对"
- "AWS 中的 Cloud Volumes ONTAP 的网络要求"

## Azure 中的 Cloud Volumes ONTAP 的网络要求

设置 Azure 网络，以便 Cloud Volumes ONTAP 系统可以正常运行。

### Cloud Volumes ONTAP 的出站 Internet 访问

Cloud Volumes ONTAP 要求出站 Internet 访问向 NetApp AutoSupport 发送消息、NetApp AutoSupport 主动监控存储的运行状况。

路由和防火墙策略必须允许通过 HTTP/HTTPS 流量访问以下端点，以便 Cloud Volumes ONTAP 可以发送 AutoSupport 消息：

- <https://support.netapp.com/aods/asupmessage>
- <https://support.netapp.com/asupprod/post/1.0/postAsup>

### 安全组

您不需要创建安全组，因为 Cloud Manager 可以为您提供这些功能。如果您需要使用自己的，请参见 "安全组规则"。

### IP 地址数

Cloud Manager 会将以下数量的 IP 地址分配给 Azure 中的 Cloud Volumes ONTAP：

- 单个节点：5 个 IP 地址
- HA 对：16 个 IP 地址

请注意，Cloud Manager 会在 HA 对上创建 SVM 管理 LIF，但不会在 Azure 中的单节点系统上创建。



LIF 是与物理端口关联的 IP 地址。SnapCenter 等管理工具需要 SVM 管理 LIF。

## 从 Cloud Volumes ONTAP 连接到 Azure Blob 存储以进行数据分层

如果要将冷数据分层到 Azure Blob 存储，只要 Cloud Manager 具有所需权限，您就无需在性能层和容量层之间设置连接。如果 Cloud Manager 策略具有以下权限，则 Cloud Manager 将为您启用 vNet 服务端点：

```
"Microsoft.Network/virtualNetworks/subnets/write",  
"Microsoft.Network/routeTables/join/action"
```

这些权限包含在最新版本中 ["Cloud Manager 策略"](#)。

有关设置数据分层的详细信息，请参见 ["将冷数据分层到低成本对象存储"](#)。

## 连接到其他网络中的 ONTAP 系统

要在 Azure 和 ONTAP 系统中的 Cloud Volumes ONTAP 系统之间复制数据，您必须在 Azure VNet 和其他网络之间建立 VPN 连接—例如 AWS VPC 或您的公司网络。

有关说明，请参见 ["Microsoft Azure 文档：在 Azure 门户中创建站点到站点连接"](#)。

## GCP 中的 Cloud Volumes ONTAP 的网络要求

设置您的 Google 云平台网络，以便 Cloud Volumes ONTAP 系统可以正常运行。

### 共享 VPC

Cloud Manager 和 Cloud Volumes ONTAP 在 Google 云平台共享 VPC 中受支持。

通过共享 VPC，您可以跨多个项目配置和集中管理虚拟网络。您可以在 *host project* 中设置共享 VPC 网络，并在 *service project* 中部署 Cloud Manager 和 Cloud Volumes ONTAP 虚拟机实例。["Google Cloud 文档：共享 VPC 概述"](#)。

唯一要求是为共享 VPC 主机项目中的 Cloud Manager 服务帐户提供以下权限：

```
compute.s防火墙。 * compute.networks.* compute.subnetworks.*
```

Cloud Manager 需要这些权限才能查询主机项目中的防火墙，VPC 和子网。

### Cloud Volumes ONTAP 的出站 Internet 访问

Cloud Volumes ONTAP 要求出站 Internet 访问向 NetApp AutoSupport 发送消息、NetApp AutoSupport 主动监控存储的运行状况。

路由和防火墙策略必须允许通过 HTTP/HTTPS 流量访问以下端点，以便 Cloud Volumes ONTAP 可以发送 AutoSupport 消息：

- <https://support.netapp.com/aods/asupmessage>
- <https://support.netapp.com/asupprod/post/1.0/postAsup>

### IP 地址数

Cloud Manager 会在 GCP 中为 Cloud Volumes ONTAP 分配 5 个 IP 地址。

请注意，Cloud Manager 不会在 GCP 中为 Cloud Volumes ONTAP 创建 SVM 管理 LIF。





LIF 是与物理端口关联的 IP 地址。SnapCenter 等管理工具需要 SVM 管理 LIF。

## 防火墙规则

您无需创建防火墙规则，因为 Cloud Manager 可以为您创建。如果您需要使用自己的，请参见 ["GCP 防火墙规则"](#)。

## 从 **Cloud Volumes ONTAP** 连接到 **Google** 云存储以进行数据分层

如果要将冷数据分层到 Google 云存储分段，则必须为 Cloud Volumes ONTAP 所在的子网配置私有 Google 访问。有关说明，请参见 ["Google Cloud 文档：配置私有 Google Access"](#)。

有关在 Cloud Manager 中设置数据分层所需的其他步骤，请参见 ["将冷数据分层到低成本对象存储"](#)。

## 连接到其他网络中的 **ONTAP** 系统

要在 GCP 中的 Cloud Volumes ONTAP 系统与其他网络中的 ONTAP 系统之间复制数据，您必须在 VPC 与其他网络（例如公司网络）之间建立 VPN 连接。

有关说明，请参见 ["Google Cloud 文档：Cloud VPN 概述"](#)。

# 其他部署选项

## 云管理器主机要求

如果您在自己的主机上安装了 Cloud Manager，则必须验证对配置的支持、包括操作系统要求、端口要求等。



您可以在 GCP 中自己的主机上安装 Cloud Manager，但不能在内部网络中安装 Cloud Manager。要在 GCP 中部署 Cloud Volumes ONTAP，必须在 GCP 中安装 Cloud Manager。

## 需要一个专用主机

与其他应用程序共享的主机不支持 Cloud Manager。主机必须是专用主机。

## 支持的 **AWS EC2** 实例类型

- T2.medium
- T3.medium（建议）
- m4.large
- m5.xlarge
- m5.2xlarge
- m5.4xlarge
- m5.8xlarge

## 支持的 **Azure VM** 大小

A2，D2 v2 或 D2 v3（取决于可用性）

## 支持的 **GCP** 计算机类型

一种计算机类型，至少具有 2 个 vCPU 和 4 GB 内存。

## 支持的操作系统

- CentOS 7.2
- CentOS 7.3.
- CentOS 7.4.
- CentOS 7.5
- Red Hat Enterprise Linux 7.2
- Red Hat Enterprise Linux 7.3
- Red Hat Enterprise Linux 7.4
- Red Hat Enterprise Linux 7.5

Red Hat Enterprise Linux 系统必须在 Red Hat 订购管理中注册。如果未注册、系统将无法在安装 Cloud Manager 期间访问存储库以更新所需的第三方软件。

这些操作系统的英语版本支持 Cloud Manager 。

## 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 ? "]

## CPU

具有两个内核的 2.27 GHz 或更高性能

## RAM

4 GB

## 可用磁盘空间

50 GB

## 出站 Internet 访问

安装 Cloud Manager 和使用 Cloud Manager 部署 Cloud Volumes ONTAP 时需要进行出站 Internet 访问。有关端点列表，请参见 "[云管理器的网络要求](#)"。

## 端口

以下端口必须可用：

- 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

如果其他服务正在使用这些端口、则安装 Cloud Manager 失败。



端口 3306 可能存在冲突。如果 MySQL 的另一个实例在主机上运行，则默认情况下使用端口 3306。您必须更改现有 MySQL 实例使用的端口。

您可以在安装 Cloud Manager 时更改默认 HTTP 和 HTTPS 端口。您无法更改 MySQL 数据库的默认端口。如果更改了 HTTP 和 HTTPS 端口、则必须确保用户可以从远程主机访问 Cloud Manager Web 控制台：

- 修改安全组以允许通过端口进行入站连接。
- 在输入 Cloud Manager Web 控制台的 URL 时指定端口。

## 在现有 Linux 主机上安装 Cloud Manager

最常见的 Cloud Manager 部署方式是从 Cloud Central 或云提供商的市场。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 Cloud Manager 软件。



您可以在 GCP 中自己的主机上安装 Cloud Manager，但不能在内部网络中安装 Cloud Manager。要在 GCP 中部署 Cloud Volumes ONTAP，必须在 GCP 中安装 Cloud Manager。

### 开始之前

- Red Hat Enterprise Linux 系统必须在 Red Hat 订购管理中注册。如果未注册、系统将无法在安装 Cloud Manager 期间访问存储库以更新所需的第三方软件。
- 在安装过程中，Cloud Manager 安装程序会访问多个 URL。您必须确保允许这些端点进行出站 Internet 访问。请参见 ["云管理器的网络要求"](#)。

### 关于此任务

- 安装 Cloud Manager 不需要 root 权限。
- Cloud Manager 将安装 AWS 命令行工具（AWSCLI）以启用 NetApp 支持的恢复过程。

如果您收到安装 AWSCLI 失败的消息，则可以安全地忽略该消息。如果没有这些工具、Cloud Manager 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，Cloud Manager 将自动更新自身。

### 步骤

1. 查看网络要求：
  - ["云管理器的网络要求"](#)
  - ["AWS 中的 Cloud Volumes ONTAP 的网络要求"](#)
  - ["Azure 中的 Cloud Volumes ONTAP 的网络要求"](#)
  - ["GCP 中的 Cloud Volumes ONTAP 的网络要求"](#)
2. 请查看 ["云管理器主机要求"](#)。
3. 从下载软件 ["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"](#)。

4. 分配执行脚本的权限。

- 示例 \*

```
chmod +x OnCommandCloudManager-V3.7.0.sh
. 运行安装脚本:
```

```
./OnCommandCloudManager-V3.7.0.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 Cloud Manager 主机位于代理服务器之后，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。

5. 除非指定了 *silent* 参数，否则请键入 \*。Y\* 继续执行脚本，然后在出现提示时输入 HTTP 和 HTTPS 端口。

如果更改了 HTTP 和 HTTPS 端口、则必须确保用户可以从远程主机访问 Cloud Manager Web 控制台：

- 修改安全组以允许通过端口进行入站连接。
- 在输入 Cloud Manager Web 控制台的 URL 时指定端口。

现在已安装 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。

6. 打开 Web 浏览器并输入以下 URL：

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

*ipaddress* 可以是 localhost，专用 IP 地址或公有 IP 地址，具体取决于 Cloud Manager 主机的配置。例如，如果云管理器位于公共云中而没有公共 IP 地址，则必须从连接到云管理器主机的主机中输入私有 IP 地址。

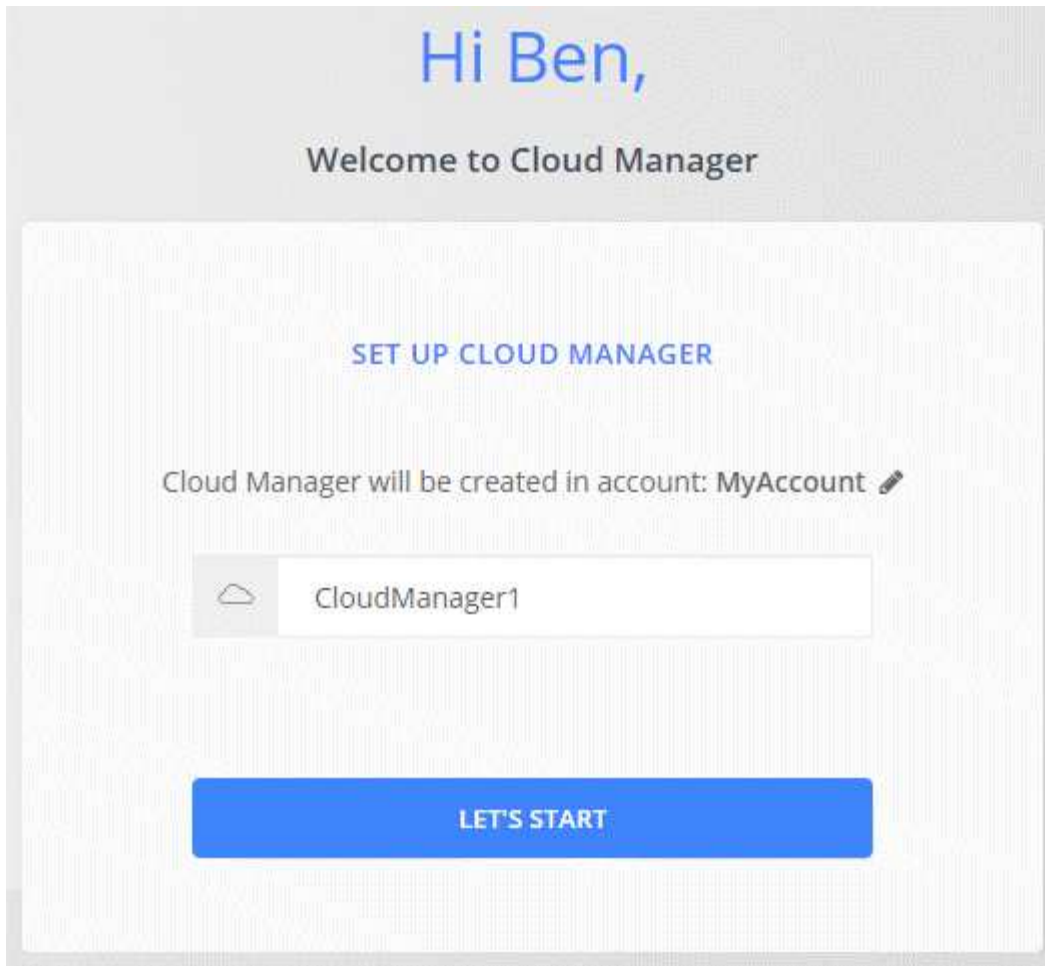
如果更改了默认 HTTP（80）或 HTTPS（443）端口，则需要 *port*。例如，如果 HTTPS 端口更改为 8443，则应输入 

```
<a href="https://<em>ipaddress</em>:8443" class="bare">https://<em>ipaddress</em>:8443</a>
```

7. 请在 NetApp Cloud Central 上注册或登录。
8. 登录后，设置 Cloud Manager：
  - a. 指定要与此 Cloud Manager 系统关联的 Cloud Central 帐户。

"了解 Cloud Central 帐户"。

- b. 输入系统名称。



完成后

设置权限，以便 Cloud Manager 可以在您的云提供商中部署 Cloud Volumes ONTAP：

- 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"。
- GCP：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。
  - a. "在 GCP 中创建角色" 其中包括中定义的权限 "适用于 GCP 的 Cloud Manager 策略"。
  - b. "创建 GCP 服务帐户并应用刚刚创建的自定义角色"。
  - c. "将此服务帐户与 Cloud Manager VM 关联"。
  - d. 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。

## 从 AWS Marketplace 启动 Cloud Manager

最好使用在 AWS 中启动 Cloud Manager "NetApp Cloud Central"，但如果需要，您可以从 AWS Marketplace 启动它。



如果您从 AWS Marketplace 启动 Cloud Manager、Cloud Manager 仍与 NetApp Cloud Central 集成。"了解有关集成的更多信息"。

## 关于此任务

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 \* 操作无法执行此操作。

## 步骤

- 为 EC2 实例创建 IAM 策略和角色：
  - 从以下位置下载 Cloud Manager IAM 策略：  
["NetApp Cloud Manager：AWS，Azure 和 GCP 策略"](#)
  - 从 IAM 控制台，通过从 Cloud Manager IAM 策略复制和粘贴文本来创建您自己的策略。
  - 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。
- "从 AWS Marketplace 订阅" 确保在免费试用 Cloud Volumes ONTAP 结束后不会中断服务。对于您创建的每个 Cloud Volumes ONTAP 9.6 及更高版本的 PAYGO 系统以及您启用的每个附加功能，此订阅将向您收取费用。
- 现在转到 ["AWS Marketplace 上的 Cloud Manager 页面"](#) 从 AMI 部署 Cloud Manager。
- 在 Marketplace 页面上，单击 \* 继续订阅 \*，然后单击 \* 继续配置 \*。
- 更改任何默认选项，然后单击 \* 继续启动 \*。
- 在 \* 选择操作 \* 下，选择 \* 通过 EC2 启动 \*，然后单击 \* 启动 \*。
- 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.medium）。  
["查看支持的实例类型列表"](#)。
  - \* 配置实例 \*：选择 VPC 和子网，您在第 1 步中创建的 IAM 角色以及其他符合您要求的配置选项。

Number of instances	<input type="text" value="1"/>	<a href="#">Launch into Auto Scaling Group</a>
Purchasing option	<input type="checkbox"/> Request Spot instances	
Network	<input type="text" value="vpc-a76d91c2   VPC4QA (default)"/>	<a href="#">Create new VPC</a>
Subnet	<input type="text" value="subnet-05525c38   QASubnet4   us-east-1e"/> 251 IP Addresses available	<a href="#">Create new subnet</a>
Auto-assign Public IP	<input type="text" value="Enable"/>	
Placement group	<input type="checkbox"/> Add instance to placement group	
Capacity Reservation	<input type="text" value="Open"/>	<a href="#">Create new Capacity Reservation</a>
IAM role	<input type="text" value="Cloud_Manager"/>	<a href="#">Create new IAM role</a>

- \* 添加存储 \* : 保留默认存储选项。
- \* 添加标记 \* : 根据需要进行实例的标记。
- \* 配置安全组 \* : 指定 Cloud Manager 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。云管理器实例和软件应在大约五分钟内运行。

8. 从连接到云管理器虚拟机的主机上打开 Web 浏览器, 然后输入以下 URL :

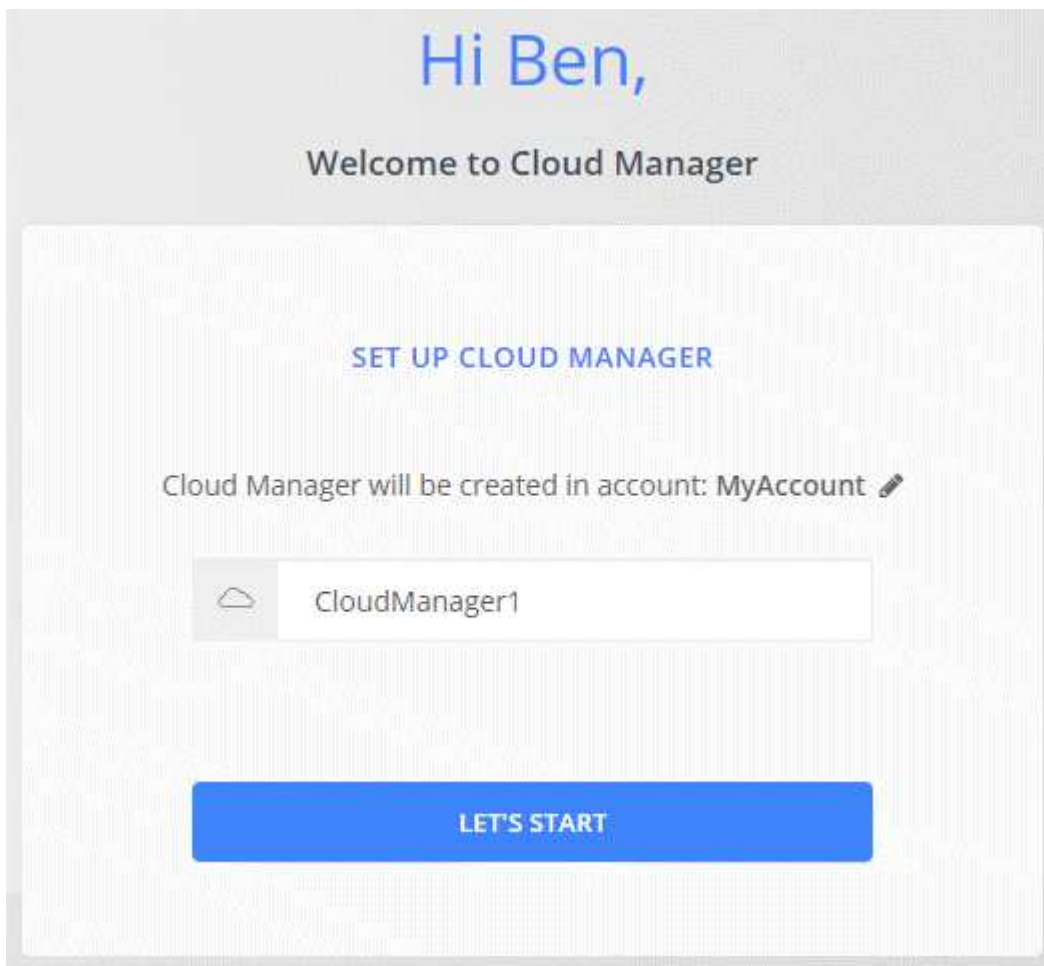
`<a href="http://<em>ipaddress</em>:80" class="bare">http://<em>ipaddress</em>:80</a>`

9. 登录后, 设置 Cloud Manager :

a. 指定要与此 Cloud Manager 系统关联的 Cloud Central 帐户。

"了解 Cloud Central 帐户"。

b. 输入系统名称。



结果

现在已安装并设置了 Cloud Manager 。

## 从 Azure Marketplace 部署 Cloud Manager

最好使用在 Azure 中部署 Cloud Manager "NetApp Cloud Central"，但如果需要，您可以从 Azure Marketplace 进行部署。

有关在中部署 Cloud Manager 的说明，请参见 "Azure 美国政府区域" 和中的 "Azure 德国地区"。



如果您从 Azure Marketplace 部署 Cloud Manager、Cloud Manager 仍与 NetApp Cloud Central 集成。"了解有关集成的更多信息"。

### 在 Azure 中部署 Cloud Manager

您需要安装和设置 Cloud Manager、以便使用它在 Azure 中启动 Cloud Volumes ONTAP。

#### 步骤

1. "转至 [Azure Marketplace 页面的 Cloud Manager](#)。"
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。
- 选择一个建议的虚拟机大小：A2，D2 v2 或 D2 v3（取决于可用性）。
- 对于网络安全组，Cloud Manager 要求使用 SSH，HTTP 和 HTTPS 进行进站连接。

"详细了解 [Cloud Manager 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 Cloud Manager 启用。

此设置非常重要，因为托管身份允许 Cloud Manager 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。虚拟机和云管理器软件应在大约五分钟内运行。

5. 从连接到云管理器虚拟机的主机上打开 Web 浏览器，然后输入以下 URL：

`<a href="http://<em>ipaddress</em>:80" class="bare">http://<em>ipaddress</em>:80</a>`

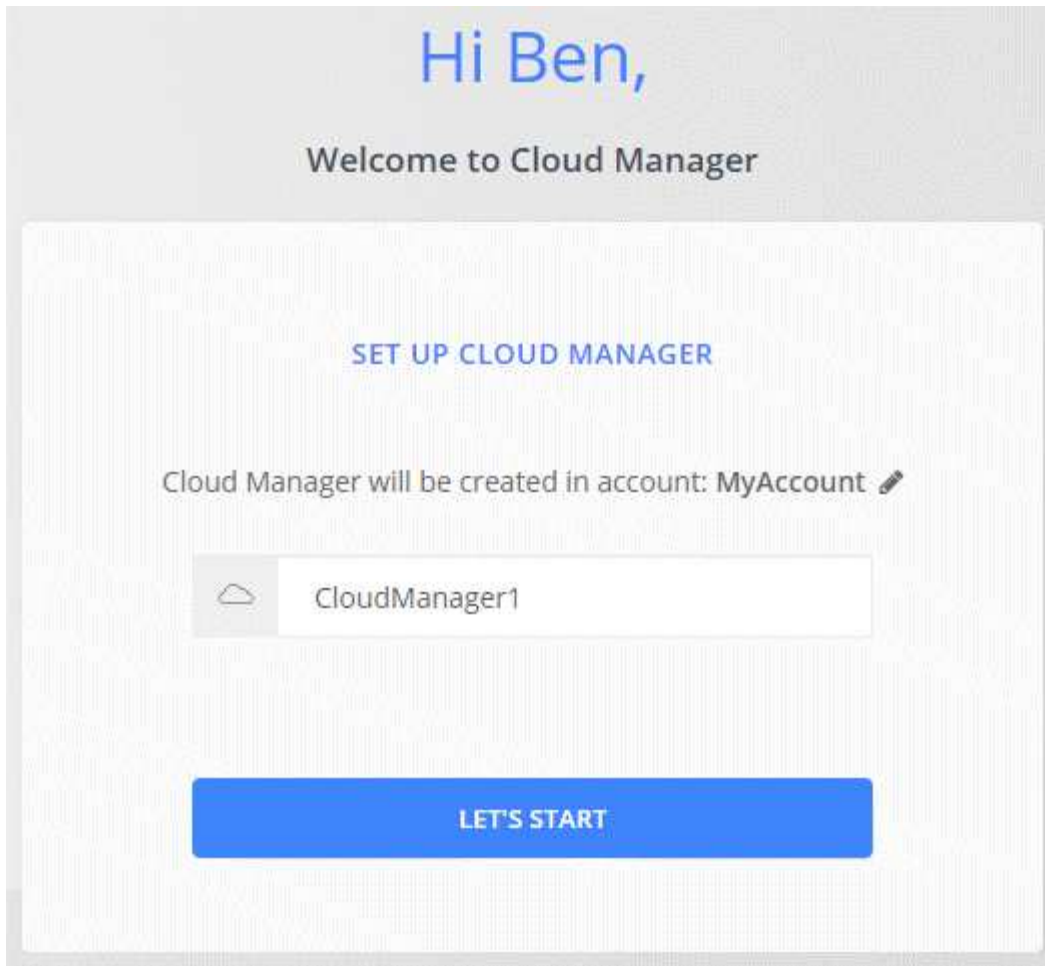
6. 登录后，设置 Cloud Manager：

- a. 指定要与此 Cloud Manager 系统关联的 Cloud Central 帐户。

"了解 [Cloud Central 帐户](#)"。

- b. 输入系统名称。





## 结果

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

## 向 Cloud Manager 授予 Azure 权限

在 Azure 中部署 Cloud Manager 时，您应已启用 ["系统分配的受管身份"](#)。现在，您必须通过创建自定义角色、然后为一个或多个订阅将角色分配给 Cloud Manager 虚拟机来授予所需的 Azure 权限。

## 步骤

1. 使用云管理器策略创建自定义角色：
  - a. 下载 ["Cloud Manager Azure 策略"](#)。
  - 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-C25 FBzzzzz"、  
"/subscriptions/54b91999 - b3e6-4599 - 908e-416e0zzzzz"、 "/subscription/398e471c - 3b4ae-  
7b5bzzz"
```

c. 使用 JSON 文件在 Azure 中创建自定义角色。

以下示例说明了如何使用 Azure CLI 2.0 创建自定义角色：

- AZ 角色定义 create -role-definition C : \Policy\_for\_cloud Manager\_Azure\_3.7.4.json\*

现在，您应该拥有一个名为 OnCommand Cloud Manager Operator 的自定义角色、您可以将其分配给 Cloud Manager 虚拟机。

2. 为一个或多个订阅的 Cloud Manager 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) \*。

c. 单击 \* 添加 \* > \* 添加角色分配 \*，然后添加权限：

- 选择 \* OnCommand 云管理器操作员 \* 角色。



OnCommand 云管理器操作员是中提供的默认名称 "[Cloud Manager 策略](#)"。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。
- 选择创建云管理器虚拟机的订阅。
- 选择 Cloud Manager 虚拟机。
- 单击 \* 保存 \*。

d. 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。

结果

Cloud Manager 现在拥有在 Azure 中部署和管理 Cloud Volumes ONTAP 所需的权限。

## 在美国 Azure 政府区域部署 Cloud Manager

要在美国政府区域启动和运行 Cloud Manager，请首先从 Azure 政府市场部署 Cloud Manager。然后，提供 Cloud Manager 部署和管理 Cloud Volumes ONTAP 系统所需的权限。

有关受支持的 Azure 美国政府区域的列表，请参见 "[Cloud Volumes 全球地区](#)"。

### 从 Azure 美国政府市场部署 Cloud Manager

Cloud Manager 可作为映像 [在 Azure 美国政府市场中提供](#)。

步骤

1. 确保您的订阅已启用 Azure 政府市场：

a. 以企业管理员身份登录到门户。

b. 导航到 \* 管理 \*。

c. 在 \* 注册详细信息 \* 下，单击 \* Azure Marketplace \* 旁边的铅笔图标。

d. 选择 \* 已启用 \*。

e. 单击 \* 保存 \*。

["Microsoft Azure 文档： Azure 政府市场"](#)

2. 在 Azure 美国政府门户中搜索 OnCommand 云管理器。

3. 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。
- 您应选择一个建议的虚拟机大小： A2， D2 v2 或 D2 v3（取决于可用性）。
- 对于网络安全组，最好选择 \* 高级 \*。
  - 高级 \* 选项将创建一个新的安全组，其中包含 Cloud Manager 所需的入站规则。如果选择基本，请参见 ["安全组规则"](#) 所需规则的列表。

4. 在摘要页面上，查看所做的选择，然后单击 \* 创建 \* 以开始部署。

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

5. 从连接到云管理器虚拟机的主机上打开 Web 浏览器，然后输入以下 URL：

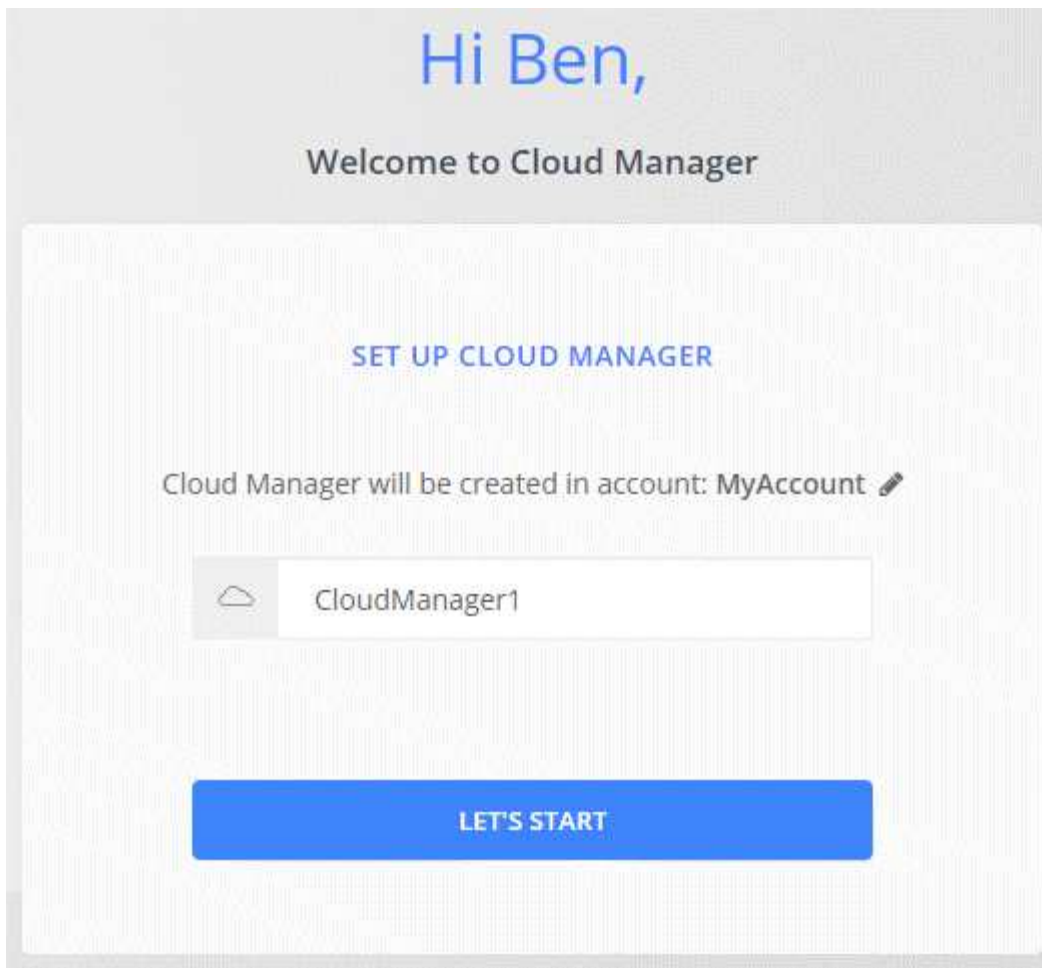
`<a href="http://<em>ipaddress</em>:80" class="bare">http://<em>ipaddress</em>:80</a>`

6. 登录后，设置 Cloud Manager：

a. 指定要与此 Cloud Manager 系统关联的 Cloud Central 帐户。

["了解 Cloud Central 帐户"](#)。

b. 输入系统名称。



## 结果

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

## 使用托管身份向 **Cloud Manager** 授予 **Azure** 权限

提供权限的最简单方法是启用 ["托管身份"](#) 在 Cloud Manager 虚拟机上，然后为虚拟机分配所需权限。如果首选，另一种方法是 ["使用服务主体授予 Azure 权限"](#)。

## 步骤

1. 在 Cloud Manager 虚拟机上启用托管身份：
  - a. 导航到 Cloud Manager 虚拟机并选择 \* 身份 \*。
  - b. 在 \* 系统已分配 \* 下，单击 \* 打开 \*，然后单击 \* 保存 \*。
2. 使用云管理器策略创建自定义角色：
  - a. 下载 ["Cloud Manager Azure 策略"](#)。
  - 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 \*

"AssignablesCaps" : ["/subscriptions/d333af45-0d07-4154 - 943D-C25 FBzzzzz"、  
"/subscriptions/54b91999 - b3e6-4599 - 908e-416e0zzzzz"、 "/subscription/398e471c - 3b4ae-  
7b5bzzz"

- c. 使用 JSON 文件在 Azure 中创建自定义角色。

以下示例说明了如何使用 Azure CLI 2.0 创建自定义角色：

- AZ 角色定义 create -role-definition C : \Policy\_for\_cloud Manager\_Azure\_3.7.4.json\*

现在，您应该拥有一个名为 OnCommand Cloud Manager Operator 的自定义角色、您可以将其分配给 Cloud Manager 虚拟机。

3. 为一个或多个订阅的 Cloud Manager 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 ) \*。
- c. 单击 \* 添加 \*，单击 \* 添加角色分配 \*，然后添加权限：
  - 选择 \* OnCommand 云管理器操作员 \* 角色。



OnCommand 云管理器操作员是中提供的默认名称 "[Cloud Manager 策略](#)"。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。
  - 选择创建云管理器虚拟机的订阅。
  - 键入虚拟机的名称，然后将其选中。
  - 单击 \* 保存 \*。
- d. 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。

## 结果

Cloud Manager 现在拥有在 Azure 中部署和管理 Cloud Volumes ONTAP 所需的权限。

## 在德国 Azure 地区安装 Cloud Manager

Azure Marketplace 在德国 Azure 地区不可用，因此您必须从 NetApp 支持站点下载 Cloud Manager 安装程序并将其安装在该地区的现有 Linux 主机上。

## 步骤

1. "[查看 Azure 的网络要求](#)。"
2. "[查看云管理器主机要求](#)。"
3. "[下载并安装 Cloud Manager](#)。"
4. "[使用服务主体向 Cloud Manager 授予 Azure 权限](#)"。

## 完成后

Cloud Manager 现在可以像任何其他地区一样在 Azure Germany 地区部署 Cloud Volumes ONTAP。但是，您可能需要先执行其他设置。

## 保持 **Cloud Manager** 正常运行

Cloud Manager 应始终保持运行状态。

Cloud Manager 是 Cloud Volumes ONTAP 运行状况和计费的关键组成部分。如果 Cloud Manager 已关闭，则在与 Cloud Manager 的通信中断 4 天以上后，Cloud Volumes ONTAP 系统将关闭。

# 部署 Cloud Volumes ONTAP

## 在创建 Cloud Volumes ONTAP 系统之前

在使用 Cloud Manager 创建和管理 Cloud Volumes ONTAP 系统之前、您的云管理器管理员应已准备好网络并安装和设置了 Cloud Manager 。

在开始部署 Cloud Volumes ONTAP 之前应存在以下条件：

- 已满足 Cloud Manager 和 Cloud Volumes ONTAP 的网络连接要求。
- Cloud Manager 有权在您选择的云提供商中执行操作。
- 对于 AWS ， 您已订阅相应的 AWS Marketplace 页面：
  - 如果要部署 PAYGO 系统或启用附加功能："[Cloud Manager（适用于 Cloud Volumes ONTAP）页面](#)"。
  - 如果要部署 BYOL 系统："[AWS Marketplace 中的单个节点或 HA 页面](#)"。
- 已安装云管理器。

### 相关链接

- "[AWS 入门](#)"
- "[Azure 入门](#)"
- "[GCP 入门](#)"
- "[设置云管理器](#)"

## 登录到 Cloud Manager

您可以从任何连接到云管理器系统的 Web 浏览器登录到云管理器。您应使用登录 "[NetApp Cloud Central](#)" 用户帐户

### 步骤

1. 打开 Web 浏览器并登录到 "[NetApp Cloud Central](#)"。

此步骤应自动将您定向到 Fabric 视图。如果没有，请单击 \* Fabric View\* 。

2. 选择要访问的 Cloud Manager 系统。

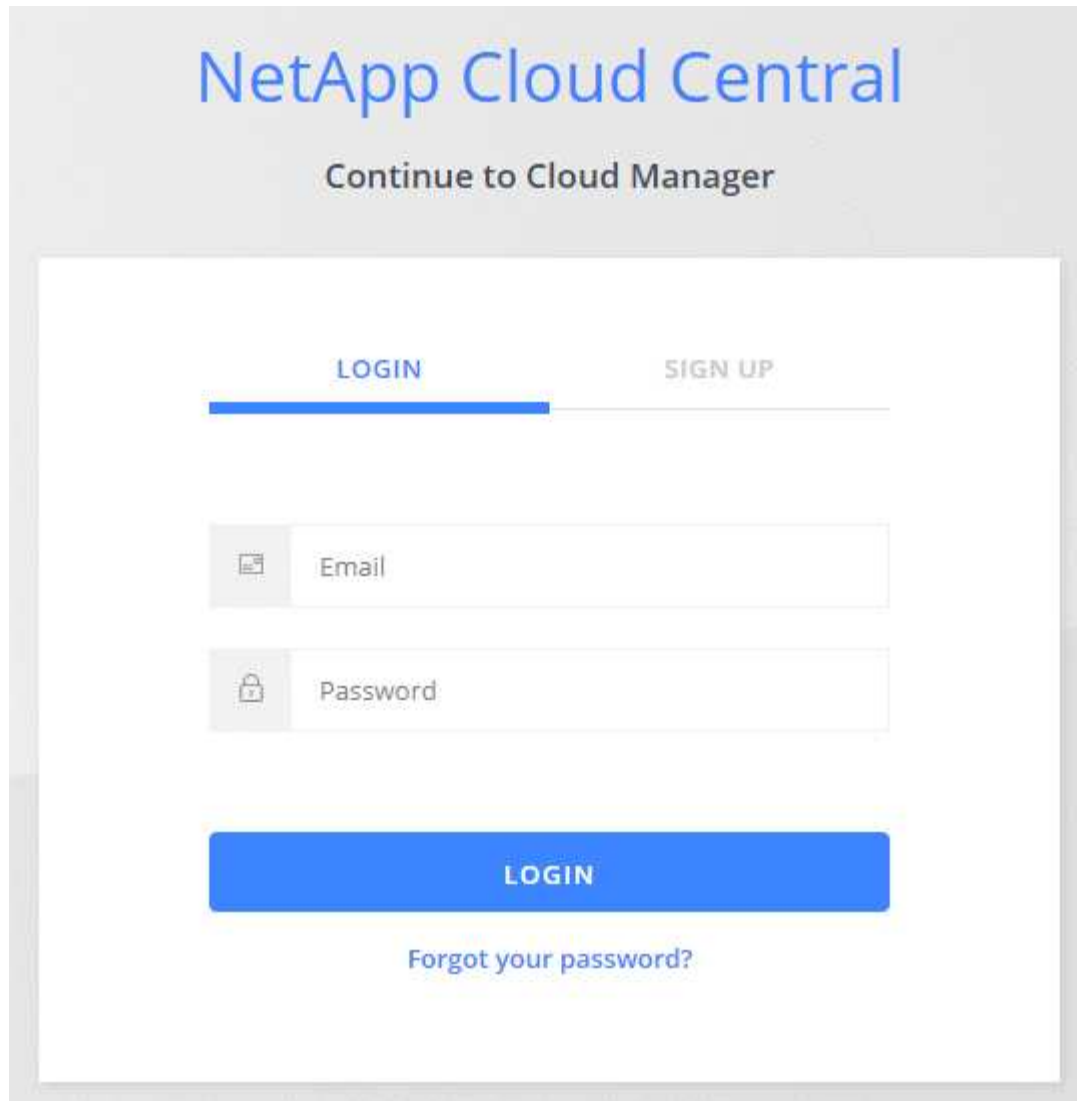


如果您未看到列出任何系统，请确保帐户管理员已将您添加到与 Cloud Manager 系统关联的 Cloud Central 帐户。

3. 使用您的 NetApp Cloud Central 凭据登录到 Cloud Manager 。

# NetApp Cloud Central

Continue to Cloud Manager

The image shows the NetApp Cloud Central login interface. At the top, the title "NetApp Cloud Central" is displayed in blue. Below it, the text "Continue to Cloud Manager" is centered. The main content area is a white box with a light gray border. At the top of this box, there are two tabs: "LOGIN" (which is selected and highlighted with a blue underline) and "SIGN UP". Below the tabs are two input fields: "Email" with an envelope icon and "Password" with a lock icon. A large blue "LOGIN" button is positioned below the input fields. At the bottom of the form, there is a link that says "Forgot your password?".

## 规划 Cloud Volumes ONTAP 配置

部署 Cloud Volumes ONTAP 时、您可以选择符合工作负载要求的预配置系统、也可以创建自己的配置。如果您选择自己的配置、则应了解可用的选项。

### 选择许可证类型

Cloud Volumes ONTAP 有两种定价选项：按需购买和自带许可证（BYOL）。对于按需购买、可从三种许可证中进行选择：Explore、Standard 或 Premium。每个许可证提供不同的容量和计算选项。

- ["AWS 中的 Cloud Volumes ONTAP 9.7 支持的配置"](#)
- ["Azure 中 Cloud Volumes ONTAP 9.7 支持的配置"](#)
- ["GCP 中的 Cloud Volumes ONTAP 9.7 支持的配置"](#)

### 了解存储限制

Cloud Volumes ONTAP 系统的原始容量限制与许可证相关。附加限制会影响聚合和卷的大小。在规划配置时，



您应该了解这些限制。

- ["AWS 中 Cloud Volumes ONTAP 9.7 的存储限制"](#)
- ["Azure 中 Cloud Volumes ONTAP 9.7 的存储限制"](#)
- ["GCP 中 Cloud Volumes ONTAP 9.7 的存储限制"](#)

## 选择写入速度

利用 Cloud Manager，您可以为单节点 Cloud Volumes ONTAP 系统选择写入速度设置。在选择写入速度之前、您应该了解正常和高设置之间的差异、以及使用高速写入速度时的风险和和建议。

正常写入速度和高速写入速度之间的差异

选择正常写入速度后、数据将直接写入磁盘、从而减少发生计划外系统中断时数据丢失的可能性。

如果选择高速写入速度、则在将数据写入磁盘之前将数据缓冲在内存中、从而提供更快的写入性能。由于这种缓存，如果发生计划外系统中断，则可能会导致数据丢失。

在发生计划外系统中断时可能丢失的数据量是最后两个一致性点的范围。一致性点是将缓冲数据写入磁盘的操作。写入日志已满或 10 秒后（以先到者为准）会出现一致性点。但是，AWS EBS 卷性能可能会影响一致性点处理时间。

何时使用高速写入

如果您的工作负载需要快速写入性能、并且您可以在发生计划外系统中断时承受数据丢失的风险、则可以选择高速写入速度。

使用高速写入时的建议

如果启用高速写入速度、则应确保应用程序层的写保护。

## 选择卷使用情况配置文件

ONTAP 包含多种存储效率功能、可以减少您所需的存储总量。在 Cloud Manager 中创建卷时，您可以选择启用这些功能的配置文件或禁用这些功能的配置文件。您应该了解有关这些功能的更多信息、以帮助确定要使用的配置文件。

NetApp 存储效率功能具有以下优势：

精简配置

为主机或用户提供的逻辑存储比实际在物理存储池中提供的存储多。在写入数据时，存储空间将动态分配给每个卷而不是预先分配存储空间。

重复数据删除

通过定位相同的数据块并将其替换为单个共享块的引用来提高效率。此技术通过消除驻留在同一卷中的冗余数据块来降低存储容量需求。

压缩

通过在主存储、二级存储和归档存储上的卷中压缩数据来减少存储数据所需的物理容量。

## AWS 规划

通过调整系统规模并查看需要输入的网络信息，规划 Cloud Volumes ONTAP 在 AWS 中的部署。

- [在 AWS 中估算系统规模](#)
- [AWS 网络信息工作表](#)

### 在 AWS 中估算系统规模

对 Cloud Volumes ONTAP 系统进行规模估算有助于满足性能和容量要求。在选择实例类型，磁盘类型和磁盘大小时，应注意以下要点：

#### Instance type

- 将工作负载要求与每个 EC2 实例类型的最大吞吐量和 IOPS 相匹配。
- 如果多个用户同时向系统写入数据，请选择一种具有足够 CPU 来管理请求的实例类型。
- 如果您的应用程序大部分是读取的，请选择具有足够 RAM 的系统。
  - ["AWS 文档： Amazon EC2 实例类型"](#)
  - ["AWS 文档： Amazon EBS 优化实例"](#)

#### EBS 磁盘类型

通用 SSD 是 Cloud Volumes ONTAP 最常见的磁盘类型。要查看 EBS 磁盘的使用情形，请参见 ["AWS 文档： EBS 卷类型"](#)。

#### EBS 磁盘大小

启动 Cloud Volumes ONTAP 系统时，您需要选择初始磁盘大小。之后，您可以 ["让 Cloud Manager 为您管理系统的容量"](#)，但如果需要 ["自行构建聚合"](#)，请注意以下事项：

- 聚合中的所有磁盘大小必须相同。
- EBS 磁盘的性能取决于磁盘大小。该大小决定了 SSD 磁盘的基准 IOPS 和最大突发持续时间以及 HDD 磁盘的基准和突发吞吐量。
- 最后，您应选择磁盘大小，以获得所需的 `_stimed_perform` 性能。
- 即使您选择了更大的磁盘（例如六个 4 TB 磁盘）、但由于 EC2 实例可以达到其带宽限制，因此您可能无法获得全部 IOPS。

有关 EBS 磁盘性能的详细信息，请参见 ["AWS 文档： EBS 卷类型"](#)。

有关在 AWS 中调整 Cloud Volumes ONTAP 系统规模的更多详细信息，请观看以下视频：

 | <https://img.youtube.com/vi/GELcXmOuYPw/maxresdefault.jpg>

#### AWS 网络信息工作表

在 AWS 中启动 Cloud Volumes ONTAP 时，需要指定有关 VPC 网络的详细信息。您可以使用工作表从管理员收集信息。

## Cloud Volumes ONTAP 的网络信息

AWS 信息	您的价值
Region	
VPC	
Subnet	
安全组（如果使用您自己的）	

## 多个 AWS 中 HA 对的网络信息

AWS 信息	您的价值
Region	
VPC	
安全组（如果使用您自己的）	
节点 1 可用性区域	
节点 1 子网	
节点 2 可用性区域	
节点 2 子网	
调解器可用性区域	
调解器子网	
调解器的密钥对	
用于集群管理端口的浮动 IP 地址	
节点 1 上数据的浮动 IP 地址	
节点 2 上数据的浮动 IP 地址	
浮动 IP 地址的路由表	

## Azure 规划

通过调整系统规模并查看需要输入的网络信息，规划 Cloud Volumes ONTAP 在 Azure 中的部署。

- [在 Azure 中估算系统规模](#)
- [Azure 网络信息工作表](#)

### 在 Azure 中估算系统规模

对 Cloud Volumes ONTAP 系统进行规模估算有助于满足性能和容量要求。在选择虚拟机类型，磁盘类型和磁盘大小时，您应注意几个要点：

#### 虚拟机类型

在中查看支持的虚拟机类型 " [《 Cloud Volumes ONTAP 发行说明》](#) " 然后查看有关每个受支持 VM 类型的详

细信息。请注意，每种 VM 类型都支持特定数量的数据磁盘。

- ["Azure 文档：通用虚拟机大小"](#)
- ["Azure 文档：内存优化的虚拟机大小"](#)

### Azure 磁盘类型

当您为 Cloud Volumes ONTAP 创建卷时、需要选择 Cloud Volumes ONTAP 用作磁盘的底层云存储。

HA 系统使用高级页面 Blobs 。同时，单节点系统可以使用两种类型的 Azure 受管磁盘：

- [\\_Premium SSD 受管磁盘\\_](#) 以较高的成本为 I/O 密集型工作负载提供高性能。
- [标准 SSD 受管磁盘\\_](#) 可为需要低 IOPS 的工作负载提供稳定一致的性能。
- 如果您不需要高 IOPS 并希望降低成本，[\\_Standard HDD 受管磁盘\\_](#) 是一个不错的选择。

有关这些磁盘的使用情形的其他详细信息，请参见 ["Microsoft Azure 文档： Microsoft Azure 存储简介"](#)。

### Azure 磁盘大小

启动 Cloud Volumes ONTAP 实例时，必须为聚合选择默认磁盘大小。Cloud Manager 将此磁盘大小用于初始聚合以及在您使用简单配置选项时创建的任何其他聚合。您可以创建使用与默认大小不同的磁盘大小的聚合 ["使用高级分配选项"](#)。



聚合中的所有磁盘大小必须相同。

选择磁盘大小时，应考虑多个因素。磁盘大小会影响您为存储支付的费用、可以在聚合中创建的卷大小、可用于 Cloud Volumes ONTAP 的总容量以及存储性能。

Azure 高级存储的性能取决于磁盘大小。更大的磁盘可提供更高的 IOPS 和吞吐量。例如，选择 1 TB 磁盘可以提供比 500 GB 磁盘更好的性能、而且成本更高。

标准存储的磁盘大小之间没有性能差异。应根据需要的容量选择磁盘大小。

有关按磁盘大小显示的 IOPS 和吞吐量，请参见 Azure：

- ["Microsoft Azure：受管磁盘定价"](#)
- ["Microsoft Azure：页面 Blob 定价"](#)

### Azure 网络信息工作表

在 Azure 中部署 Cloud Volumes ONTAP 时，需要指定有关虚拟网络的详细信息。您可以使用工作表从管理员收集信息。

Azure 信息	您的价值
Region	
虚拟网络（VNet）	
Subnet	

Azure 信息	您的价值
网络安全组（如果使用您自己的组）	

## GCP 规划

通过调整系统规模并查看需要输入的网络信息，规划 Cloud Volumes ONTAP 在 Google 云平台中的部署。

- [在 GCP 中估算系统规模](#)
- [GCP 网络信息工作表](#)

### 在 GCP 中估算系统规模

对 Cloud Volumes ONTAP 系统进行规模估算有助于满足性能和容量要求。在选择计算机类型，磁盘类型和磁盘大小时，您应注意几个要点：

#### 计算机类型

在中查看支持的计算机类型 "[《Cloud Volumes ONTAP 发行说明》](#)" 然后查看 Google 提供的有关每个受支持计算机类型的详细信息。将工作负载要求与此计算机类型的 vCPU 和内存数量相匹配。请注意，每个 CPU 核心都会提高网络连接性能。

有关更多详细信息，请参见以下内容：

- "[Google Cloud 文档：N1 标准计算机类型](#)"
- "[Google Cloud 文档：性能](#)"

### GCP 磁盘类型

在为 Cloud Volumes ONTAP 创建卷时，您需要选择 Cloud Volumes ONTAP 用于磁盘的底层云存储。磁盘类型可以是 *zonal SSD persistent disks\_or\_zonal standard persistent disks*。

SSD 持久磁盘最适合需要高随机 IOPS 速率的工作负载，而标准持久磁盘经济实惠，可处理顺序读 / 写操作。有关详细信息，请参见 "[Google Cloud 文档：区域持久性磁盘（标准和 SSD）](#)"。

### GCP 磁盘大小

部署 Cloud Volumes ONTAP 系统时，您需要选择初始磁盘大小。之后，您可以让 Cloud Manager 为您管理系统的容量，但如果您要自行构建聚合，请注意以下事项：

- 聚合中的所有磁盘大小必须相同。
- 确定所需空间，同时考虑性能。
- 永久性磁盘的性能会随磁盘大小和系统可用的 vCPU 数量自动扩展。

有关更多详细信息，请参见以下内容：

- "[Google Cloud 文档：区域持久性磁盘（标准和 SSD）](#)"
- "[Google Cloud 文档：优化持久磁盘和本地 SSD 性能](#)"

## GCP 网络信息工作表

在 GCP 中部署 Cloud Volumes ONTAP 时，需要指定有关虚拟网络的详细信息。您可以使用工作表从管理员收集信息。

GCP 信息	您的价值
Region	
分区	
VPC 网络	
Subnet	
防火墙策略（如果使用自己的策略）	

## 正在查找 Cloud Manager 系统 ID

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

### 步骤

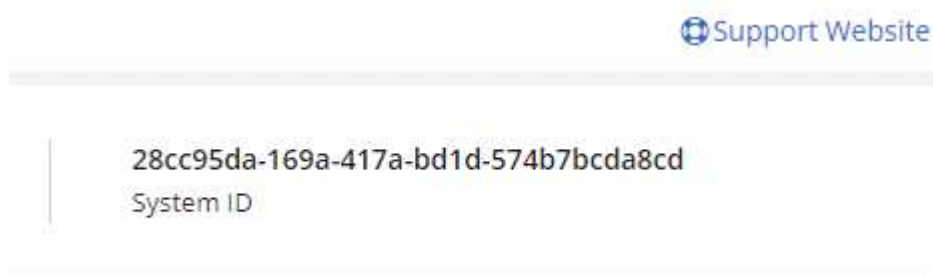
1. 在 Cloud Manager 控制台右上角，单击设置图标。



2. 单击 \* 支持信息板 \*。

您的系统 ID 显示在右上角。

- 示例 \*



## 在 Cloud Volumes ONTAP 上启用 Flash Cache

AWS 和 Azure 中的某些 Cloud Volumes ONTAP 配置包括本地 NVMe 存储，Cloud Volumes ONTAP 使用这些存储作为 *Flash Cache* 来提高性能。

## 什么是Flash Cache?

Flash Cache 通过实时智能缓存最近读取的用户数据和 NetApp 元数据来加快数据访问速度。它适用于随机读取密集型工作负载，包括数据库，电子邮件和文件服务。

### 限制

- 必须在所有卷上禁用数据压缩，才能利用 Flash Cache 性能改进功能。
- Cloud Volumes ONTAP 不支持在重新启动后重新恢复缓存。

## 在 AWS 中的 Cloud Volumes ONTAP 上启用 Flash Cache

Cloud Volumes ONTAP 高级版和 AWS 中的 BYOL 支持 Flash Cache 。

### 步骤

1. 使用新的或现有的 Cloud Volumes ONTAP 高级版或 BYOL 系统选择以下 EC2 实例类型之一：
  - c5d.4xlarge
  - c5d.9x 大型
  - r5d.2xlarge
2. 在所有卷上禁用数据压缩，以利用 Flash Cache 性能改进。

在使用 Cloud Manager 创建卷时选择 "无存储效率"，或者先创建卷，然后再创建卷 "[使用命令行界面禁用数据压缩](#)"。

## 在 Azure 中的 Cloud Volumes ONTAP 上启用 Flash Cache

单节点系统上的 Cloud Volumes ONTAP BYOL 支持 Flash Cache 。

### 步骤

1. 在 Azure 中选择具有单节点 Cloud Volumes ONTAP BYOL 系统的 Standard\_L8s\_v2 VM 类型。
2. 在所有卷上禁用数据压缩，以利用 Flash Cache 性能改进。

在使用 Cloud Manager 创建卷时选择 "无存储效率"，或者先创建卷，然后再创建卷 "[使用命令行界面禁用数据压缩](#)"。

## 在 AWS 中启动 Cloud Volumes ONTAP

您可以在单系统配置中或在 AWS 中作为 HA 对启动 Cloud Volumes ONTAP 。

### 从 AWS Marketplace 订阅

从 AWS Marketplace 订阅即可按需购买 Cloud Volumes ONTAP，也可以部署 Cloud Volumes ONTAP BYOL。

## 订阅 PAYGO

"从 AWS Marketplace 订阅" 确保在免费试用 Cloud Volumes ONTAP 结束后不会中断服务。对于您创建的每个 Cloud Volumes ONTAP 9.6 及更高版本的 PAYGO 系统以及您启用的每个附加功能，此订阅将向您收取费用。

以下视频显示了订阅过程：


► [https://docs.netapp.com/zh-cn/occm37//media/video\\_subscribing\\_aws.mp4](https://docs.netapp.com/zh-cn/occm37//media/video_subscribing_aws.mp4) (video)



如果多个 IAM 用户在同一个 AWS 帐户中工作，则每个用户都需要订阅。在第一个用户订阅后，AWS 会向后续用户显示他们已订阅，如下图所示。虽然已为 AWS 帐户订阅，但每个 IAM 用户都需要将自己与订阅关联起来。如果您看到以下消息，请单击 \* 单击此处 \* 链接以转到 Cloud Central 并完成此过程。

### Cloud Manager (for Cloud Volumes ONTAP)

You are currently subscribed to this product and will be charged for your accumulated usage at the end of your next billing cycle, based on the costs listed in Pricing information on the right.

**Having issues signing up for your product?**  
If you were unable to complete the set-up process for this software, please [click here](#) to be taken to the product's registration area.

[Subscribe](#)

You are already subscribed to this product

#### Pricing Details

Software Fees

## 订阅 BYOL

如果您要通过自带许可证（BYOL）启动 Cloud Volumes ONTAP，"然后，您需要在 AWS Marketplace 中订阅该产品"。

"了解有关每个 AWS Marketplace 页面的更多信息"。

## 在 AWS 中启动单个 Cloud Volumes ONTAP 系统

如果要在 AWS 中启动 Cloud Volumes ONTAP、则需要在 Cloud Manager 中创建新的工作环境。

### 开始之前

- 您应该已准备好选择配置并从管理员处获取 AWS 网络信息。有关详细信息，请参见 "[规划 Cloud Volumes ONTAP 配置](#)"。
- 如果要启动 BYOL 系统，必须具有 20 位序列号（许可证密钥）。
- 如果要使用 CIFS、必须设置 DNS 和 Active Directory。有关详细信息，请参见 "[AWS 中的 Cloud Volumes ONTAP 的网络要求](#)"。

### 关于此任务

在创建工作环境之后、Cloud Manager 会立即在指定的 VPC 中启动测试实例以验证连接性。如果成功、Cloud Manager 会立即终止实例、然后开始部署 Cloud Volumes ONTAP 系统。如果 Cloud Manager 无法验证连接性、则无法创建工作环境。该测试实例可以是 t2.nano（对于默认 vPC 占用）或 m3.medium（对于专用 vPC 占用）。

### 步骤



1. 在工作环境页面上，单击 \* 创建 Cloud Volumes ONTAP \* 并按照提示进行操作。
2. \* 定义您的工作环境 \*：选择 \* Amazon Web Services\* 和 \* Cloud Volumes ONTAP \*。
3. \* 详细信息和凭据 \*：可选择更改 AWS 帐户和 Marketplace 订阅，输入工作环境名称，根据需要添加标记，然后输入密码。

本页中的某些字段是不言自明的。下表介绍了可能需要指导的字段：

字段	Description
Account	如果您选择其他帐户，则可以选择此帐户 <a href="#">"向 Cloud Manager 添加了其他 AWS 帐户"</a> 。
市场订阅	如果要更改要从中收取费用的 AWS 帐户，请选择其他订阅。要添加新订阅，" <a href="#">转到 AWS Marketplace 中的产品</a> "。
工作环境名称	Cloud Manager 使用工作环境名称来命名 Cloud Volumes ONTAP 系统和 Amazon EC2 实例。如果您选择了预定义安全组的前缀，则它还会使用该名称作为前缀。
添加标记	AWS 标记是 AWS 资源的元数据。Cloud Manager 将这些标记添加到 Cloud Volumes ONTAP 实例以及与该实例关联的每个 AWS 资源。在创建工作环境时，最多可以从用户界面添加四个标签，然后可以在创建工作环境后添加更多标签。请注意，在创建工作环境时，API 不会将您限制为四个标记。有关标记的信息，请参见 <a href="#">"AWS 文档：标记 Amazon EC2 资源"</a> 。
凭据	这些是 Cloud Volumes ONTAP 集群管理员帐户的凭据。您可以使用这些凭据通过 OnCommand System Manager 或其 CLI 连接到 Cloud Volumes ONTAP。

4. \* 服务 \*：保持服务处于启用状态或禁用不想在此 Cloud Volumes ONTAP 系统中使用的单个服务。
  - ["了解有关备份到 S3 的更多信息"](#)。
  - ["了解有关云合规性的更多信息"](#)。
5. \* 位置和连接 \*：输入您在 AWS 工作表中记录的网络信息。

下图显示了已填写的页面：

Location

AWS Region

US West | Oregon

VPC

vpc-3a01e05f - 172.31.0.0/16

Subnet

172.31.5.0/24 (OCCM subnet)

Connectivity

Security Group

Generated security group  Use existing security group

SSH Authentication Method

Password  Key Pair

6. \* 数据加密 \*：不选择数据加密或 AWS 管理的加密。

对于 AWS 管理的加密，您可以从您的帐户或其他 AWS 帐户中选择其他客户主密钥（CMK）。



创建 Cloud Volumes ONTAP 系统后，您无法更改 AWS 数据加密方法。

["了解如何为 Cloud Volumes ONTAP 设置 AWS KMS"](#)。

["了解有关支持的加密技术的更多信息"](#)。

7. \* 许可证和支持站点帐户 \*：指定是要使用按需购买还是 BYOL，然后指定 NetApp 支持站点帐户。

要了解许可证的工作原理，请参见 ["许可"](#)。

对于按需购买，NetApp 支持站点帐户是可选的，但对于 BYOL 系统则是必需的。 ["了解如何添加 NetApp 支持站点帐户"](#)。

8. \* 预配置软件包 \*：选择一个软件包以快速启动 Cloud Volumes ONTAP，或者单击 \* 创建自己的配置 \*。

如果选择其中一个包、则只需指定卷、然后检查并批准配置。

9. \* IAM 角色 \*：您应保留默认选项，让 Cloud Manager 为您创建角色。

如果您希望使用自己的策略，则必须满足 ["Cloud Volumes ONTAP 节点的策略要求"](#)。

10. \* 许可 \*：根据需要更改 Cloud Volumes ONTAP 版本，选择许可证，实例类型和实例租户。

如果启动实例后需要更改、则可以稍后修改许可证或实例类型。



如果选定版本有较新的候选版本、一般可用性或修补程序版本可用、则在创建工作环境时，Cloud Manager 会将系统更新为该版本。例如，如果您选择 Cloud Volumes ONTAP 9.4 RC1 和 9.4 GA 可用，则会发生此更新。此更新不会从一个版本更新到另一个版本，例如从 9.3 到 9.4。

11. \* 底层存储资源 \*：选择初始聚合的设置：磁盘类型，每个磁盘的大小以及是否应启用 S3 分层。

磁盘类型用于初始卷。您可以为后续卷选择不同的磁盘类型。

磁盘大小适用于初始聚合中的所有磁盘以及使用 Simple Provisioning（简单配置）选项时 Cloud Manager 创建的任何其他聚合。您可以使用高级分配选项创建使用不同磁盘大小的聚合。

有关选择磁盘类型和大小的帮助，请参见 ["在 AWS 中估算系统规模"](#)。

12. \* 写入速度和 WORM\*：选择 \* 正常 \* 或 \* 高 \* 写入速度，并根据需要激活一次写入，多次读取（WORM）存储。

["了解有关写入速度的更多信息"](#)。

["了解有关 WORM 存储的更多信息"](#)。

13. \* 创建卷 \*：输入新卷的详细信息或单击 \* 跳过 \*。

如果要为 iSCSI 创建卷，则可以跳过此步骤。Cloud Manager 仅为 NFS 和 CIFS 设置卷。

本页中的某些字段是不言自明的。下表介绍了可能需要指导的字段：

字段	Description
Size	您可以输入的最大大小在很大程度上取决于您是否启用精简配置、这样您就可以创建一个大于当前可用物理存储的卷。
访问控制（仅适用于 NFS）	导出策略定义子网中可以访问卷的客户端。默认情况下，Cloud Manager 会输入一个值、用于访问子网中的所有实例。
权限和用户 / 组（仅限 CIFS）	这些字段使您能够控制用户和组对共享的访问级别（也称为访问控制列表或 ACL）。您可以指定本地或域 Windows 用户或组、UNIX 用户或组。如果指定域 Windows 用户名，则必须使用 domain\username 格式包含用户的域。
快照策略	Snapshot 副本策略指定自动创建的 NetApp Snapshot 副本的频率和数量。NetApp Snapshot 副本是一个时间点文件系统映像、对性能没有影响、并且只需要极少的存储。您可以选择默认策略或无。您可以为瞬态数据选择无：例如，Microsoft SQL Server 的 tempdb。

下图显示了已填写 CIFS 协议的卷页面：

### Details & Protection

Volume Name:  Size (GB):

Snapshot Policy:

Default Policy

### Protocol

NFS Protocol  CIFS Protocol

Share name:  Permissions:

Users / Groups:

Valid users and groups separated by a semicolon

14. \* CIFS 设置 \*：如果选择 CIFS 协议，请设置 CIFS 服务器。

字段	Description
DNS 主 IP 地址和次 IP 地址	为 CIFS 服务器提供名称解析的 DNS 服务器的 IP 地址。列出的 DNS 服务器必须包含为 CIFS 服务器将加入的域定位 Active Directory LDAP 服务器和域控制器所需的服务位置记录（服务位置记录）。
要加入的 Active Directory 域	您希望 CIFS 服务器加入的 Active Directory（AD）域的 FQDN。
授权加入域的凭据	具有足够权限将计算机添加到 AD 域中指定组织单位 (OU) 的 Windows 帐户的名称和密码。
CIFS server NetBIOS name	在 AD 域中唯一的 CIFS 服务器名称。
组织单位	AD 域中要与 CIFS 服务器关联的组织单元。默认值为 cn = computers。如果将 AWS 托管 Microsoft AD 配置为 Cloud Volumes ONTAP 的 AD 服务器，则应在此字段中输入 * OU=Computers，OU=corp*。
DNS 域	Cloud Volumes ONTAP Storage Virtual Machine（SVM）的 DNS 域。在大多数情况下，域与 AD 域相同。

字段	Description
NTP 服务器	选择 * 使用 Active Directory 域 * 以使用 Active Directory DNS 配置 NTP 服务器。如果需要使用其他地址配置 NTP 服务器，则应使用 API。请参见 " <a href="#">Cloud Manager API 开发人员指南</a> " 了解详细信息。

15. \* 使用情况配置文件，磁盘类型和分层策略 \*：选择是否要启用存储效率功能，并根据需要编辑 S3 分层策略。

有关详细信息，请参见 "[了解卷使用情况配置文件](#)" 和 "[数据分层概述](#)"。

16. \* 审核并批准 \*：审核并确认您的选择。
- 查看有关配置的详细信息。
  - 单击 \* 更多信息 \* 可查看有关 Cloud Manager 将购买的支持和 AWS 资源的详细信息。
  - 选中 \* 我了解 ... \* 复选框。
  - 单击 \* 执行 \*。

## 结果

Cloud Manager 将启动 Cloud Volumes ONTAP 实例。您可以跟踪时间链中的进度。

如果在启动 Cloud Volumes ONTAP 实例时遇到任何问题，请查看故障消息。您还可以选择工作环境并单击重新创建环境。

要获得更多帮助，请转至 "[NetApp Cloud Volumes ONTAP 支持](#)"。

## 完成后

- 如果配置了 CIFS 共享、请授予用户或组对文件和文件夹的权限、并验证这些用户是否可以访问该共享并创建文件。
- 如果要对卷应用配额、请使用 System Manager 或 CLI。

配额允许您限制或跟踪用户、组或 qtree 使用的磁盘空间和文件数量。

## 在 AWS 中启动 Cloud Volumes ONTAP HA 对

如果要在 AWS 中启动 Cloud Volumes ONTAP HA 对、则需要在 Cloud Manager 中创建 HA 工作环境。

### 开始之前

- 您应该已准备好选择配置并从管理员处获取 AWS 网络信息。有关详细信息，请参见 "[规划 Cloud Volumes ONTAP 配置](#)"。
- 如果您购买了 BYOL 许可证，则每个节点必须具有一个 20 位序列号（许可证密钥）。
- 如果要使用 CIFS、必须设置 DNS 和 Active Directory。有关详细信息，请参见 "[AWS 中的 Cloud Volumes ONTAP 的网络要求](#)"。

### 关于此任务

在创建工作环境之后、Cloud Manager 会立即在指定的 VPC 中启动测试实例以验证连接性。如果成功、Cloud Manager 会立即终止实例、然后开始部署 Cloud Volumes ONTAP 系统。如果 Cloud Manager 无法验证连接性、则无法创建工作环境。该测试实例可以是 t2.nano（对于默认 vPC 占用）或 m3.medium（对于专用 vPC

占用)。

#### 步骤

1. 在工作环境页面上，单击 \* 创建 Cloud Volumes ONTAP \* 并按照提示进行操作。
2. \* 定义您的工作环境 \*：选择 \* Amazon Web Services\* 和 \* Cloud Volumes ONTAP HA\*。
3. \* 详细信息和凭据 \*：可选择更改 AWS 帐户和 Marketplace 订阅，输入工作环境名称，根据需要添加标记，然后输入密码。

本页中的某些字段是不言自明的。下表介绍了可能需要指导的字段：

字段	Description
Account	如果您选择其他帐户，则可以选择此帐户 <a href="#">"向 Cloud Manager 添加了其他 AWS 帐户"</a> 。
市场订阅	如果要更改要从中收取费用的 AWS 帐户，请选择其他订阅。要添加新订阅，" <a href="#">转到 AWS Marketplace 中的产品</a> "。
工作环境名称	Cloud Manager 使用工作环境名称来命名 Cloud Volumes ONTAP 系统和 Amazon EC2 实例。如果您选择了预定义安全组的前缀，则它还会使用该名称作为前缀。
添加标记	AWS 标记是 AWS 资源的元数据。Cloud Manager 将这些标记添加到 Cloud Volumes ONTAP 实例以及与该实例关联的每个 AWS 资源。在创建工作环境时，最多可以从用户界面添加四个标签，然后可以在创建工作环境后添加更多标签。请注意，在创建工作环境时，API 不会将您限制为四个标记。有关标记的信息，请参见 <a href="#">"AWS 文档：标记 Amazon EC2 资源"</a> 。
凭据	这些是 Cloud Volumes ONTAP 集群管理员帐户的凭据。您可以使用这些凭据通过 OnCommand System Manager 或其 CLI 连接到 Cloud Volumes ONTAP。

4. \* 服务 \*：保持服务处于启用状态或禁用不想在此 Cloud Volumes ONTAP 系统中使用的单个服务。
  - ["了解有关备份到 S3 的更多信息"](#)。
  - ["了解有关云合规性的更多信息"](#)。
5. \* 高可用性部署模式 \*：选择一个高可用性配置。

有关部署模式的概述，请参见 ["适用于 AWS 的 Cloud Volumes ONTAP HA"](#)。

6. \* 地区和 VPC\*：输入您在 AWS 工作表中记录的网络信息。

下图显示了为多 AZ 配置填写的页面：

<b>AWS Region</b> US West   Oregon	<b>VPC</b> vpc-3a01e05f   172.31.0.0/16	<b>Security group</b> Use a generated security group
---------------------------------------	--------------------------------------------	---------------------------------------------------------

---

<b>Node 1:</b> Availability Zone us-west-2a Subnet 172.31.16.0/20	<b>Node 2:</b> Availability Zone us-west-2b Subnet 172.31.32.0/20	<b>Mediator:</b> Availability Zone us-west-2c Subnet 172.31.0.0/20 Key Pair newKey
-------------------------------------------------------------------------------	-------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------

7. \* 连接和 SSH 身份验证 \*：选择 HA 对和调解器的连接方法。

8. \* 浮动 IP\*：如果选择多个 AZs，请指定浮动 IP 地址。

该区域中所有 VPC 的 IP 地址必须位于 CIDR 块之外。有关其他详细信息，请参见 ["适用于多个 AWS 中的 Cloud Volumes ONTAP HA 的 AWS 网络要求"](#)。

9. \* 路由表 \*：如果选择多个 AZs，请选择应包含指向浮动 IP 地址的路由的路由表。

如果有多个路由表、则选择正确的路由表非常重要。否则，某些客户端可能无法访问 Cloud Volumes ONTAP HA 对。有关路由表的详细信息，请参见 ["AWS 文档：路由表"](#)。

10. \* 数据加密 \*：不选择数据加密或 AWS 管理的加密。

对于 AWS 管理的加密，您可以从您的帐户或其他 AWS 帐户中选择其他客户主密钥（CMK）。



创建 Cloud Volumes ONTAP 系统后，您无法更改 AWS 数据加密方法。

["了解如何为 Cloud Volumes ONTAP 设置 AWS KMS"](#)。

["了解有关支持的加密技术的更多信息"](#)。

11. \* 许可证和支持站点帐户 \*：指定是要使用按需购买还是 BYOL，然后指定 NetApp 支持站点帐户。

要了解许可证的工作原理，请参见 ["许可"](#)。

对于按需购买，NetApp 支持站点帐户是可选的，但对于 BYOL 系统则是必需的。 ["了解如何添加 NetApp 支持站点帐户"](#)。

12. \* 预配置软件包 \*：选择一个软件包以快速启动 Cloud Volumes ONTAP 系统，或者单击 \* 创建自己的配置 \*。

如果选择其中一个包、则只需指定卷、然后检查并批准配置。

13. \* IAM 角色 \*：您应保留默认选项，让 Cloud Manager 为您创建角色。

如果您希望使用自己的策略，则必须满足 ["Cloud Volumes ONTAP 节点和 HA 调解器的策略要求"](#)。

14. \* 许可 \*：根据需要更改 Cloud Volumes ONTAP 版本，选择许可证，实例类型和实例租户。

如果在启动实例后需要更改、您可以稍后修改许可证或实例类型。



如果选定版本有较新的候选版本、一般可用性或修补程序版本可用、则在创建工作环境时，Cloud Manager 会将系统更新为该版本。例如，如果您选择 Cloud Volumes ONTAP 9.4 RC1 和 9.4 GA 可用，则会发生此更新。此更新不会从一个版本更新到另一个版本，例如从 9.3 到 9.4。

15. \* 底层存储资源 \*：选择初始聚合的设置：磁盘类型，每个磁盘的大小以及是否应启用 S3 分层。

磁盘类型用于初始卷。您可以为后续卷选择不同的磁盘类型。

磁盘大小适用于初始聚合中的所有磁盘以及使用 Simple Provisioning（简单配置）选项时 Cloud Manager 创建的任何其他聚合。您可以使用高级分配选项创建使用不同磁盘大小的聚合。

有关选择磁盘类型和大小的帮助，请参见 ["在 AWS 中估算系统规模"](#)。

16. \* WORM\*：根据需要激活一次写入，多次读取（WORM）存储。

["了解有关 WORM 存储的更多信息。"](#)

17. \* 创建卷 \*：输入新卷的详细信息或单击 \* 跳过 \*。

如果要为 iSCSI 创建卷，则可以跳过此步骤。Cloud Manager 仅为 NFS 和 CIFS 设置卷。

本页中的某些字段是不言自明的。下表介绍了可能需要指导的字段：

字段	Description
Size	您可以输入的最大大小在很大程度上取决于您是否启用精简配置、这样您就可以创建一个大于当前可用物理存储的卷。
访问控制（仅适用于 NFS）	导出策略定义子网中可以访问卷的客户端。默认情况下，Cloud Manager 会输入一个值、用于访问子网中的所有实例。
权限和用户 / 组（仅限 CIFS）	这些字段使您能够控制用户和组对共享的访问级别（也称为访问控制列表或 ACL）。您可以指定本地或域 Windows 用户或组、UNIX 用户或组。如果指定域 Windows 用户名，则必须使用 domain\username 格式包含用户的域。
快照策略	Snapshot 副本策略指定自动创建的 NetApp Snapshot 副本的频率和数量。NetApp Snapshot 副本是一个时间点文件系统映像、对性能没有影响、并且只需要极少的存储。您可以选择默认策略或无。您可以为瞬态数据选择无：例如，Microsoft SQL Server 的 tempdb。

下图显示了已填写 CIFS 协议的卷页面：

## Details & Protection

Volume Name:  Size (GB):

Snapshot Policy:

Default Policy

## Protocol

NFS Protocol  CIFS Protocol

Share name:  Permissions:

Users / Groups:

Valid users and groups separated by a semicolon

18. \* CIFS 设置 \* : 如果选择 CIFS 协议, 请设置 CIFS 服务器。

字段	Description
DNS 主 IP 地址和次 IP 地址	为 CIFS 服务器提供名称解析的 DNS 服务器的 IP 地址。列出的 DNS 服务器必须包含为 CIFS 服务器将加入的域定位 Active Directory LDAP 服务器和域控制器所需的服务位置记录 (服务位置记录)。
要加入的 Active Directory 域	您希望 CIFS 服务器加入的 Active Directory (AD) 域的 FQDN。
授权加入域的凭据	具有足够权限将计算机添加到 AD 域中指定组织单位 (OU) 的 Windows 帐户的名称和密码。
CIFS server NetBIOS name	在 AD 域中唯一的 CIFS 服务器名称。
组织单位	AD 域中要与 CIFS 服务器关联的组织单元。默认值为 cn = computers。如果将 AWS 托管 Microsoft AD 配置为 Cloud Volumes ONTAP 的 AD 服务器, 则应在此字段中输入 * OU=Computers, OU=corp*。
DNS 域	Cloud Volumes ONTAP Storage Virtual Machine (SVM) 的 DNS 域。在大多数情况下, 域与 AD 域相同。
NTP 服务器	选择 * 使用 Active Directory 域 * 以使用 Active Directory DNS 配置 NTP 服务器。如果需要使用其他地址配置 NTP 服务器, 则应使用 API。请参见 " <a href="#">Cloud Manager API 开发人员指南</a> " 了解详细信息。

19. \* 使用情况配置文件, 磁盘类型和分层策略 \* : 选择是否要启用存储效率功能, 并根据需要编辑 S3 分层策略。

有关详细信息, 请参见 "[了解卷使用情况配置文件](#)" 和 "[数据分层概述](#)"。

20. \* 审核并批准 \* : 审核并确认您的选择。

- 查看有关配置的详细信息。
- 单击 \* 更多信息 \* 可查看有关 Cloud Manager 将购买的支持和 AWS 资源的详细信息。
- 选中 \* 我了解 ... \* 复选框。
- 单击 \* 执行 \*。

结果



Cloud Manager 将启动 Cloud Volumes ONTAP HA 对。您可以跟踪时间链中的进度。

如果在启动 HA 对时遇到任何问题、请查看故障消息。您还可以选择工作环境并单击重新创建环境。

要获得更多帮助，请转至 "[NetApp Cloud Volumes ONTAP 支持](#)"。

完成后

- 如果配置了 CIFS 共享、请授予用户或组对文件和文件夹的权限、并验证这些用户是否可以访问该共享并创建文件。
- 如果要对卷应用配额、请使用 System Manager 或 CLI 。

配额允许您限制或跟踪用户、组或 qtree 使用的磁盘空间和文件数量。

## 在 Azure 中启动 Cloud Volumes ONTAP

您可以通过在 Cloud Manager 中创建 Cloud Volumes ONTAP 工作环境在 Azure 中启动单节点系统或 HA 对。

开始之前

- 确保您的 Azure 帐户具有所需权限，尤其是在您从先前版本升级并首次部署 HA 系统时。

最新权限位于中 "[适用于 Azure 的 NetApp Cloud Central 策略](#)"。

- 您应已选择配置并从管理员处获取 Azure 网络信息。有关详细信息，请参见 "[规划 Cloud Volumes ONTAP 配置](#)"。
- 要部署 BYOL 系统，您需要每个节点的 20 位序列号（许可证密钥）。

关于此任务

当 Cloud Manager 在 Azure 中创建 Cloud Volumes ONTAP 系统时，它会创建多个 Azure 对象，例如资源组，网络接口和存储帐户。您可以在向导结束时查看资源摘要。

步骤

1. 在工作环境页面上，单击 \* 创建 Cloud Volumes ONTAP \* 并按照提示进行操作。
2. \* 定义工作环境 \*：选择 \* Microsoft Azure\*，然后选择一个节点或 HA 对。
3. \* 详细信息和凭据 \*：可选择更改 Azure 帐户或订阅，指定集群名称和资源组名称，根据需要添加标记，然后指定凭据。

下表介绍了可能需要指导的字段：

字段	Description
交换机帐户	如果需要，您可以选择其他帐户或订阅 " <a href="#">设置它们并将其添加到 Cloud Manager 中</a> "。
工作环境名称	Cloud Manager 使用工作环境名称来命名 Cloud Volumes ONTAP 系统和 Azure 虚拟机。如果您选择了预定义安全组的前缀，则它还会使用该名称作为前缀。
资源组名称	如果取消选中 * 使用默认值 *，则可以输入新资源组的名称。如果要使用现有资源组，则必须使用 API。

字段	Description
Tags	标记是 Azure 资源的元数据。Cloud Manager 将这些标记添加到 Cloud Volumes ONTAP 系统以及与系统关联的每个 Azure 资源。在创建工作环境时，最多可以从用户界面添加四个标签，然后可以在创建工作环境后添加更多标签。请注意，在创建工作环境时，API 不会将您限制为四个标记。有关标记的信息，请参见 <a href="#">"Microsoft Azure 文档：使用标记组织 Azure 资源"</a> 。
凭据	这些是 Cloud Volumes ONTAP 集群管理员帐户的凭据。您可以使用这些凭据通过 OnCommand System Manager 或其 CLI 连接到 Cloud Volumes ONTAP 。

4. \* 服务 \*：如果您不想在此 Cloud Volumes ONTAP 系统中使用云合规性，请保持启用或禁用它。

["了解有关云合规性的更多信息"](#)。

5. \* 位置和连接 \*：选择一个位置和安全组，然后选中此复选框以确认 Cloud Manager 与目标位置之间的网络连接。

6. \* 许可证和支持站点帐户 \*：指定是要使用按需购买还是 BYOL，然后指定 NetApp 支持站点帐户。

要了解许可证的工作原理，请参见 ["许可"](#)。

对于按需购买，NetApp 支持站点帐户是可选的，但对于 BYOL 系统则是必需的。["了解如何添加 NetApp 支持站点帐户"](#)。

7. \* 预配置的软件包 \*：查找其中一个软件包以快速部署 Cloud Volumes ONTAP 系统，或者单击 \* 创建自己的配置 \*。

如果选择其中一个包、则只需指定卷、然后检查并批准配置。

8. \* 许可 \*：根据需要更改 Cloud Volumes ONTAP 版本，选择许可证并选择虚拟机类型。

如果在启动系统后需要更改、您可以稍后修改许可证或虚拟机类型。



如果选定版本有较新的候选版本、一般可用性或修补程序版本可用、则在创建工作环境时，Cloud Manager 会将系统更新为该版本。例如，如果您选择 Cloud Volumes ONTAP 9.5 RC1 和 9.5 GA 可用，则会发生此更新。更新不会从一个版本更新到另一个版本，例如从 9.4 到 9.5。

9. \* 订阅 Azure Marketplace \*：如果 Cloud Manager 无法启用 Cloud Volumes ONTAP 的编程部署，请按照以下步骤操作。

10. \* 底层存储资源 \*：选择初始聚合的设置：磁盘类型，每个磁盘的大小以及是否应启用到 Blob 存储的数据分层。

磁盘类型用于初始卷。您可以为后续卷选择不同的磁盘类型。

磁盘大小适用于初始聚合中的所有磁盘以及使用 Simple Provisioning（简单配置）选项时 Cloud Manager 创建的任何其他聚合。您可以使用高级分配选项创建使用不同磁盘大小的聚合。

有关选择磁盘类型和大小的帮助，请参见 ["在 Azure 中估算系统规模"](#)。

11. \* 写入速度和 WORM\*：选择 \* 正常 \* 或 \* 高 \* 写入速度，并根据需要激活一次写入，多次读取（WORM）存储。



仅单节点系统支持选择写入速度。

"了解有关写入速度的更多信息。"

"了解有关 WORM 存储的更多信息。"

12. \* 创建卷 \* : 输入新卷的详细信息或单击 \* 跳过 \* 。

如果要使用 iSCSI ， 则应跳过此步骤。使用 Cloud Manager ， 您可以仅为 NFS 和 CIFS 创建卷。

本页中的某些字段是不言自明的。下表介绍了可能需要指导的字段：

字段	Description
Size	您可以输入的最大大小在很大程度上取决于您是否启用精简配置、这样您就可以创建一个大于当前可用物理存储的卷。
访问控制（仅适用于 NFS）	导出策略定义子网中可以访问卷的客户端。默认情况下， Cloud Manager 会输入一个值、用于访问子网中的所有实例。
权限和用户 / 组（仅限 CIFS）	这些字段使您能够控制用户和组对共享的访问级别（也称为访问控制列表或 ACL）。您可以指定本地或域 Windows 用户或组、UNIX 用户或组。如果指定域 Windows 用户名，则必须使用 domain\username 格式包含用户的域。
快照策略	Snapshot 副本策略指定自动创建的 NetApp Snapshot 副本的频率和数量。NetApp Snapshot 副本是一个时间点文件系统映像、对性能没有影响、并且只需要极少的存储。您可以选择默认策略或无。您可以为瞬态数据选择无：例如， Microsoft SQL Server 的 tempdb。

下图显示了已填写 CIFS 协议的卷页面：

### Details & Protection

Volume Name:  Size (GB):

Snapshot Policy:

Default Policy

### Protocol

NFS Protocol  CIFS Protocol

Share name:  Permissions:

Users / Groups:

Valid users and groups separated by a semicolon

13. \* CIFS 设置 \* : 如果选择 CIFS 协议，请设置 CIFS 服务器。

字段	Description
DNS 主 IP 地址和次 IP 地址	为 CIFS 服务器提供名称解析的 DNS 服务器的 IP 地址。列出的 DNS 服务器必须包含为 CIFS 服务器将加入的域定位 Active Directory LDAP 服务器和域控制器所需的服务位置记录（服务位置记录）。

字段	Description
要加入的 Active Directory 域	您希望 CIFS 服务器加入的 Active Directory (AD) 域的 FQDN。
授权加入域的凭据	具有足够权限将计算机添加到 AD 域中指定组织单位 (OU) 的 Windows 帐户的名称和密码。
CIFS server NetBIOS name	在 AD 域中唯一的 CIFS 服务器名称。
组织单位	AD 域中要与 CIFS 服务器关联的组织单元。默认值为 cn = computers。要将 Azure AD 域服务配置为 Cloud Volumes ONTAP 的 AD 服务器, 应在此字段中输入 * OU=ADDC Computers * 或 * OU=ADDC Users*。 。 <a href="https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou">https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou</a> ["Azure 文档: 在 Azure AD 域服务托管域中创建组织单位 (OU)"]
DNS 域	Cloud Volumes ONTAP Storage Virtual Machine (SVM) 的 DNS 域。在大多数情况下, 域与 AD 域相同。
NTP 服务器	选择 * 使用 Active Directory 域 * 以使用 Active Directory DNS 配置 NTP 服务器。如果需要使用其他地址配置 NTP 服务器, 则应使用 API。请参见 " <a href="#">Cloud Manager API 开发人员指南</a> " 了解详细信息。

14. \* 使用情况配置文件, 磁盘类型和分层策略 \* : 选择是否要启用存储效率功能, 并根据需要更改分层策略。

有关详细信息, 请参见 "[了解卷使用情况配置文件](#)" 和 "[数据分层概述](#)"。

15. \* 审核并批准 \* : 审核并确认您的选择。

- a. 查看有关配置的详细信息。
- b. 单击 \* 更多信息 \* 以查看有关支持和 Cloud Manager 将购买的 Azure 资源的详细信息。
- c. 选中 \* 我了解 ... \* 复选框。
- d. 单击 \* 执行 \* 。

## 结果

Cloud Manager 部署了 Cloud Volumes ONTAP 系统。您可以跟踪时间链中的进度。

如果您在部署 Cloud Volumes ONTAP 系统时遇到任何问题、请查看故障消息。您也可以选择工作环境并单击 \* 重新创建环境 \* 。

要获得更多帮助, 请转至 "[NetApp Cloud Volumes ONTAP 支持](#)"。

## 完成后

- 如果配置了 CIFS 共享、请授予用户或组对文件和文件夹的权限、并验证这些用户是否可以访问该共享并创建文件。
- 如果要对卷应用配额、请使用 System Manager 或 CLI 。

配额允许您限制或跟踪用户、组或 qtree 使用的磁盘空间和文件数量。

# 在 GCP 中启动 Cloud Volumes ONTAP

您可以通过创建工作环境在 GCP 中启动单节点 Cloud Volumes ONTAP 系统。

开始之前

- 您应已选择配置并从管理员处获取 GCP 网络信息。有关详细信息，请参见 ["规划 Cloud Volumes ONTAP 配置"](#)。
- 要部署 BYOL 系统，您需要每个节点的 20 位序列号（许可证密钥）。

步骤


1. **【订阅】** 在 "工作环境" 页面上，单击 \* 创建 Cloud Volumes ONTAP \* 并按照提示进行操作。
2. \* 定义您的工作环境 \*：单击 \* 继续 \*。
3. \* 订阅 Cloud Volumes ONTAP \*：如果出现提示，请在 GCP 市场中订阅 Cloud Volumes ONTAP。

以下视频显示了订阅过程：

► [https://docs.netapp.com/zh-cn/occm37//media/video\\_subscribing\\_gcp.mp4](https://docs.netapp.com/zh-cn/occm37//media/video_subscribing_gcp.mp4) (video)

4. \* 详细信息和凭据 \*：选择项目，指定集群名称，可选择添加标签，然后指定凭据。

下表介绍了可能需要指导的字段：

字段	Description
Google Cloud Project	<p>选择要 Cloud Volumes ONTAP 驻留的项目。默认项目是 Cloud Manager 所在的项目。</p> <p>如果您在下拉列表中未看到任何其他项目，则表示您尚未将 Cloud Manager 服务帐户与其他项目关联。转到 Google Cloud 控制台，打开 IAM 服务，然后选择项目。将具有 Cloud Manager 角色的服务帐户添加到该项目中。您需要对每个项目重复此步骤。</p> <p> 这是您为 Cloud Manager 设置的服务帐户，"<a href="#">如本页的步骤 4b 中所述</a>"。</p>
工作环境名称	Cloud Manager 使用工作环境名称来命名 Cloud Volumes ONTAP 系统和 GCP VM 实例。如果您选择了预定义安全组的前缀，则它还会使用该名称作为前缀。
添加标签	标签是 GCP 资源的元数据。Cloud Manager 会将标签添加到与该系统关联的 Cloud Volumes ONTAP 系统和 GCP 资源中。在创建工作环境时，您最多可以从用户界面添加四个标签，然后可以在创建后添加更多标签。请注意，在创建工作环境时，API 不会将您限制为四个标签。有关标签的信息，请参见 <a href="#">"Google Cloud 文档：标记资源"</a> 。
凭据	这些是 Cloud Volumes ONTAP 集群管理员帐户的凭据。您可以使用这些凭据通过 System Manager 或其命令行界面连接到 Cloud Volumes ONTAP。

5. \* 位置和连接 \*：选择一个位置，选择防火墙策略，然后选中复选框以确认与 Google Cloud 存储的网络连接以进行数据分层。

如果要将冷数据分层到 Google 云存储分段，则必须为 Cloud Volumes ONTAP 所在的子网配置私有 Google 访问。有关说明，请参见 ["Google Cloud 文档：配置私有 Google Access"](#)。

6. \* 许可证和支持站点帐户 \*：指定是要使用按需购买还是 BYOL，然后指定 NetApp 支持站点帐户。

要了解许可证的工作原理，请参见 ["许可"](#)。

对于按需购买，NetApp 支持站点帐户是可选的，但对于 BYOL 系统则是必需的。 ["了解如何添加 NetApp 支持站点帐户"](#)。

7. \* 预配置软件包 \*：选择一个软件包以快速部署 Cloud Volumes ONTAP 系统，或者单击 \* 创建自己的配置 \*。

如果选择其中一个包、则只需指定卷、然后检查并批准配置。

8. \* 许可 \*：根据需要更改 Cloud Volumes ONTAP 版本，选择许可证并选择虚拟机类型。

如果在启动系统后需要更改、您可以稍后修改许可证或虚拟机类型。



如果选定版本有较新的候选版本、一般可用性或修补程序版本可用、则在创建工作环境时，Cloud Manager 会将系统更新为该版本。例如，如果您选择 Cloud Volumes ONTAP 9.5 RC1 和 9.5 GA 可用，则会发生此更新。更新不会从一个版本更新到另一个版本，例如从 9.4 到 9.5。

9. \* 底层存储资源 \*：选择初始聚合的设置：磁盘类型，每个磁盘的大小以及是否应启用数据分层。

磁盘类型用于初始卷。您可以为后续卷选择不同的磁盘类型。

磁盘大小适用于初始聚合中的所有磁盘以及使用 Simple Provisioning（简单配置）选项时 Cloud Manager 创建的任何其他聚合。您可以使用高级分配选项创建使用不同磁盘大小的聚合。

有关选择磁盘类型和大小的帮助，请参见 ["在 GCP 中估算系统规模"](#)。

10. \* 写入速度和 WORM\*：选择 \* 正常 \* 或 \* 高 \* 写入速度，并根据需要激活一次写入，多次读取（WORM）存储。

["了解有关写入速度的更多信息。"](#)

["了解有关 WORM 存储的更多信息。"](#)

11. \* 创建卷 \*：输入新卷的详细信息或单击 \* 跳过 \*。

如果要使用 iSCSI，则应跳过此步骤。使用 Cloud Manager，您可以仅为 NFS 和 CIFS 创建卷。

本页中的某些字段是不言自明的。下表介绍了可能需要指导的字段：

字段	Description
Size	您可以输入的最大大小在很大程度上取决于您是否启用精简配置、这样您就可以创建一个大于当前可用物理存储的卷。
访问控制（仅适用于 NFS）	导出策略定义子网中可以访问卷的客户端。默认情况下，Cloud Manager 会输入一个值、用于访问子网中的所有实例。

字段	Description
权限和用户 / 组（仅限 CIFS）	这些字段使您能够控制用户和组对共享的访问级别（也称为访问控制列表或 ACL）。您可以指定本地或域 Windows 用户或组、UNIX 用户或组。如果指定域 Windows 用户名，则必须使用 domain\username 格式包含用户的域。
快照策略	Snapshot 副本策略指定自动创建的 NetApp Snapshot 副本的频率和数量。NetApp Snapshot 副本是一个时间点文件系统映像、对性能没有影响、并且只需要极少的存储。您可以选择默认策略或无。您可以为瞬态数据选择无：例如，Microsoft SQL Server 的 tempdb。

下图显示了已填写 CIFS 协议的卷页面：

### Details & Protection

Volume Name:  Size (GB):

Snapshot Policy:

Default Policy

### Protocol

NFS Protocol  CIFS Protocol

Share name:  Permissions:

Users / Groups:

Valid users and groups separated by a semicolon

12. \* CIFS 设置 \*：如果选择 CIFS 协议，请设置 CIFS 服务器。

字段	Description
DNS 主 IP 地址和次 IP 地址	为 CIFS 服务器提供名称解析的 DNS 服务器的 IP 地址。列出的 DNS 服务器必须包含为 CIFS 服务器将加入的域定位 Active Directory LDAP 服务器和域控制器所需的服务位置记录（服务位置记录）。
要加入的 Active Directory 域	您希望 CIFS 服务器加入的 Active Directory（AD）域的 FQDN。
授权加入域的凭据	具有足够权限将计算机添加到 AD 域中指定组织单位 (OU) 的 Windows 帐户的名称和密码。
CIFS server NetBIOS name	在 AD 域中唯一的 CIFS 服务器名称。
组织单位	AD 域中要与 CIFS 服务器关联的组织单元。默认值为 cn = computers。
DNS 域	Cloud Volumes ONTAP Storage Virtual Machine（SVM）的 DNS 域。在大多数情况下，域与 AD 域相同。
NTP 服务器	选择 * 使用 Active Directory 域 * 以使用 Active Directory DNS 配置 NTP 服务器。如果需要其他地址配置 NTP 服务器，则应使用 API。请参见 <a href="#">"Cloud Manager API 开发人员指南"</a> 了解详细信息。

13. \* 使用情况配置文件，磁盘类型和分层策略 \*：选择是否要启用存储效率功能，并根据需要更改分层策略。

有关详细信息，请参见 ["了解卷使用情况配置文件"](#) 和 ["数据分层概述"](#)。

14. \* 用于数据分层的 Google Cloud Platform 帐户 \*：通过为 Google Cloud Platform 帐户提供可互操作的存储访问密钥来设置数据分层。单击 \* 跳过 \* 以禁用数据分层。

Cloud Manager 可通过这些密钥设置用于数据分层的云存储分段。有关详细信息，请参见 ["设置 GCP 帐户并将其添加到 Cloud Manager"](#)。

15. \* 审核并批准 \*：审核并确认您的选择。
  - a. 查看有关配置的详细信息。
  - b. 单击 \* 更多信息 \* 可查看有关 Cloud Manager 将购买的支持和 GCP 资源的详细信息。
  - c. 选中 \* 我了解 ... \* 复选框。
  - d. 单击 \* 执行 \*。

## 结果

Cloud Manager 部署了 Cloud Volumes ONTAP 系统。您可以跟踪时间链中的进度。

如果您在部署 Cloud Volumes ONTAP 系统时遇到任何问题、请查看故障消息。您也可以选择工作环境并单击 \* 重新创建环境 \*。

要获得更多帮助，请转至 ["NetApp Cloud Volumes ONTAP 支持"](#)。

## 完成后

- 如果配置了 CIFS 共享、请授予用户或组对文件和文件夹的权限、并验证这些用户是否可以访问该共享并创建文件。
- 如果要对卷应用配额、请使用 System Manager 或 CLI。

配额允许您限制或跟踪用户、组或 qtree 使用的磁盘空间和文件数量。

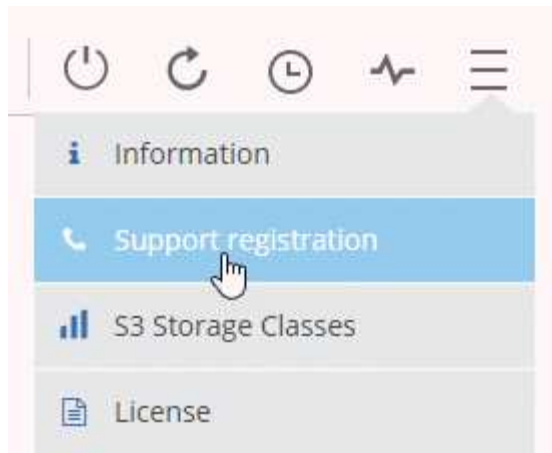
## 注册按需购买的系统

Cloud Volumes ONTAP Explore，标准版和高级版系统均提供 NetApp 支持，但您必须先向 NetApp 注册这些系统，以激活支持。

## 步骤

1. 如果您尚未将 NetApp 支持站点帐户添加到 Cloud Manager，请转到 \* 帐户设置 \* 并立即添加。  
["了解如何添加 NetApp 支持站点帐户"](#)。
2. 在 "工作环境" 页上，双击要注册的系统的名称。
3. 单击菜单图标，然后单击 \* 支持注册 \*：





4. 选择一个 NetApp 支持站点帐户，然后单击 \* 注册 \*。

结果

Cloud Manager 将系统注册到 NetApp。

## 设置 Cloud Volumes ONTAP

部署 Cloud Volumes ONTAP 后、您可以通过使用 NTP 同步系统时间以及从系统管理器或 CLI 执行几项可选任务来对其进行设置。

任务	Description															
使用 NTP 同步系统时间	<p>指定 NTP 服务器可同步网络中各个系统之间的时间，这有助于防止因时间差异而出现问题。</p> <p>在设置 CIFS 服务器时，使用 Cloud Manager API 或从用户界面指定 NTP 服务器。</p> <ul style="list-style-type: none"> <li>• <a href="#">"修改 CIFS 服务器"</a></li> <li>• <a href="#">"Cloud Manager API 开发人员指南"</a></li> </ul> <p>例如，下面是 AWS 中单节点系统的 API：</p> <div style="border: 1px solid #ccc; padding: 10px; background-color: #f0f8e8;"> <p><b>POST</b> /vsa/working-environments/{workingEnvironmentId}/ntp</p> <p><b>Setup NTP server.</b> Operation may only be performed on working environments whose status is: ON, DEGRADED.</p> <p><b>Parameters</b></p> <table border="1"> <thead> <tr> <th>Parameter</th> <th>Value</th> <th>Description</th> <th>Parameter Type</th> <th>Data Type</th> </tr> </thead> <tbody> <tr> <td>workingEnvironmentId</td> <td><input type="text"/></td> <td>Public Id of working environment</td> <td>path</td> <td>string</td> </tr> <tr> <td>body</td> <td>(required) <input type="text"/></td> <td><b>NTP Configuration request</b></td> <td>body</td> <td>Model   Model Schema <b>NTPConfigurationRequest</b> {   ntpServer (string): NTPS server }</td> </tr> </tbody> </table> <p>Parameter content type: <span>application/json</span></p> <p><a href="#">Try it out!</a></p> </div>	Parameter	Value	Description	Parameter Type	Data Type	workingEnvironmentId	<input type="text"/>	Public Id of working environment	path	string	body	(required) <input type="text"/>	<b>NTP Configuration request</b>	body	Model   Model Schema <b>NTPConfigurationRequest</b> { ntpServer (string): NTPS server }
Parameter	Value	Description	Parameter Type	Data Type												
workingEnvironmentId	<input type="text"/>	Public Id of working environment	path	string												
body	(required) <input type="text"/>	<b>NTP Configuration request</b>	body	Model   Model Schema <b>NTPConfigurationRequest</b> { ntpServer (string): NTPS server }												

任务	Description
可选：配置 AutoSupport	AutoSupport 会主动监控系统的运行状况，并在默认情况下自动将消息发送给 NetApp 技术支持。如果帐户管理员在启动实例之前向 Cloud Manager 添加了代理服务器，则 Cloud Volumes ONTAP 会配置为使用该代理服务器处理 AutoSupport 消息。您应该测试 AutoSupport 以确保它可以发送消息。有关说明，请参见 System Manager 帮助或 " <a href="#">《 ONTAP 9 系统管理参考》</a> "。
可选：配置 EMS	事件管理系统 (EMS) 收集并显示有关在 Cloud Volumes ONTAP 系统上发生的事件的信息。要接收事件通知、您可以为特定事件严重性设置事件目标（电子邮件地址、SNMP 陷阱主机或系统日志服务器）和事件路由。您可以使用 CLI 配置 EMS。有关说明，请参见 " <a href="#">《 ONTAP 9 EMS 配置快速指南》</a> "。
可选：为多个 AWS 可用性区域中的 HA 系统创建 SVM 管理网络接口（LIF）	<p>如果要将 SnapCenter 或 SnapDrive for Windows 与 HA 对一起使用、则需要存储虚拟机（SVM）管理网络接口（LIF）。在多个 AWS 可用性区域之间使用 HA 对时，SVM 管理 LIF 必须使用 <i>float</i> IP 地址。</p> <p>启动 HA 对时，Cloud Manager 会提示您指定浮动 IP 地址。如果未指定 IP 地址、则可以通过 System Manager 或 CLI 自行创建 SVM 管理 LIF。以下示例说明了如何从 CLI 创建 LIF：</p> <pre data-bbox="548 821 1487 1077">network interface create -vserver svm_cloud -lif svm_mgmt -role data -data-protocol none -home-node cloud-01 -home-port e0a -address 10.0.2.126 -netmask 255.255.255.0 -status-admin up -firewall -policy mgmt</pre>
可选：更改配置文件的备份位置	Cloud Volumes ONTAP 会自动创建配置备份文件、其中包含有关其正常运行所需的可配置选项的信息。默认情况下，Cloud Volumes ONTAP 会每 8 小时将文件备份到 Cloud Manager 主机。如果要将备份发送到备用位置、可以将位置更改为数据中心或 AWS 中的 FTP 或 HTTP 服务器。例如，您可能已经拥有 FAS 存储系统的备份位置。您可以使用 CLI 更改备份位置。请参见 " <a href="#">《 ONTAP 9 系统管理参考》</a> "。

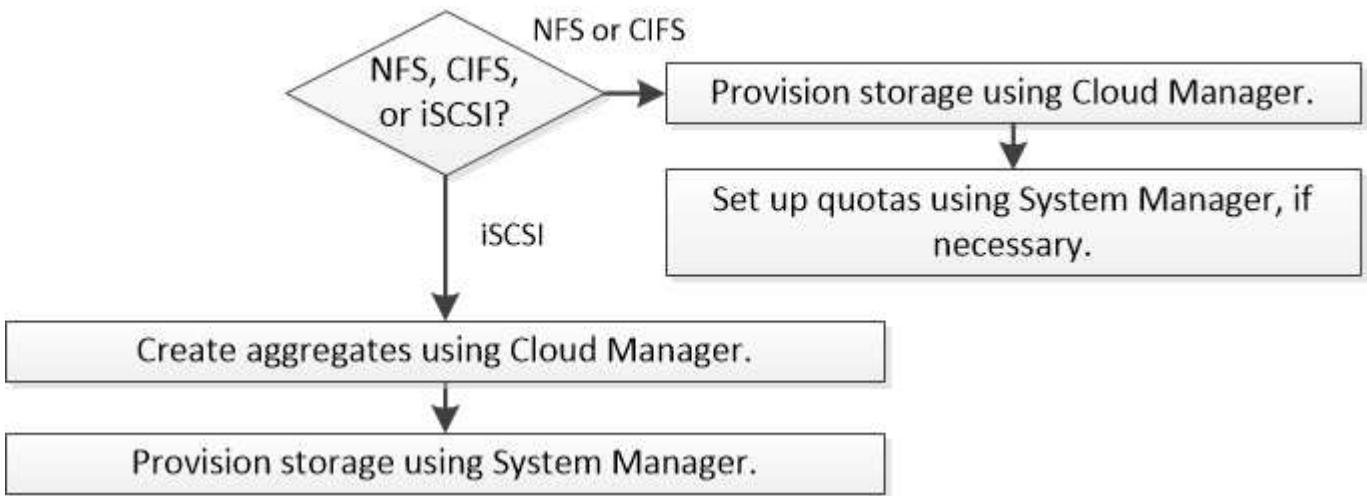
# 配置存储

## 配置存储

通过管理卷和聚合，您可以从 Cloud Manager 为您的 Cloud Volumes ONTAP 系统配置其他 NFS 和 CIFS 存储。如果需要创建 iSCSI 存储、则应从 System Manager 执行此操作。



必须直接从 Cloud Manager 创建和删除所有磁盘和聚合。不应从其他管理工具执行这些操作。这样做可能会影响系统稳定性、妨碍将来添加磁盘的能力、并可能产生冗余云提供商费用。



## 创建 FlexVol 卷

如果在启动 Cloud Volumes ONTAP 系统后需要更多存储，则可以从 Cloud Manager 为 NFS 或 CIFS 创建新的 FlexVol 卷。

开始之前

如果要在 AWS 中使用 CIFS、则必须设置 DNS 和 Active Directory。有关详细信息，请参见 "[Cloud Volumes ONTAP for AWS 的网络要求](#)"。

步骤

1. 在工作环境页面上，双击要配置 FlexVol 卷的 Cloud Volumes ONTAP 系统的名称。
2. 在任何聚合或特定聚合上创建新卷：

Action	步骤
创建新卷并让云管理器选择包含的聚合	单击 * 添加新卷 *。
在特定聚合上创建新卷	a. 单击菜单图标，然后单击 * 高级 > 高级分配 *。 b. 单击聚合的菜单。 c. 单击 * 创建卷 *。

3. 输入新卷的详细信息，然后单击 \* 继续 \*。

本页中的某些字段是不言自明的。下表介绍了可能需要指导的字段：

字段	Description
Size	您可以输入的最大大小在很大程度上取决于您是否启用精简配置、这样您就可以创建一个大于当前可用物理存储的卷。
访问控制（仅适用于 NFS）	导出策略定义子网中可以访问卷的客户端。默认情况下，Cloud Manager 会输入一个值、用于访问子网中的所有实例。
权限和用户 / 组（仅限 CIFS）	这些字段使您能够控制用户和组对共享的访问级别（也称为访问控制列表或 ACL）。您可以指定本地或域 Windows 用户或组、UNIX 用户或组。如果指定域 Windows 用户名，则必须使用 domain\username 格式包含用户的域。
快照策略	Snapshot 副本策略指定自动创建的 NetApp Snapshot 副本的频率和数量。NetApp Snapshot 副本是一个时间点文件系统映像、对性能没有影响、并且只需要极少的存储。您可以选择默认策略或无。您可以为瞬态数据选择无：例如，Microsoft SQL Server 的 tempdb。

4. 如果您选择了 CIFS 协议并且 CIFS 服务器尚未设置，请在创建 CIFS 服务器对话框中指定该服务器的详细信息，然后单击 \* 保存并继续 \*：

字段	Description
DNS 主 IP 地址和次 IP 地址	为 CIFS 服务器提供名称解析的 DNS 服务器的 IP 地址。列出的 DNS 服务器必须包含为 CIFS 服务器将加入的域定位 Active Directory LDAP 服务器和域控制器所需的服务位置记录（服务位置记录）。
要加入的 Active Directory 域	您希望 CIFS 服务器加入的 Active Directory（AD）域的 FQDN。
授权加入域的凭据	具有足够权限将计算机添加到 AD 域中指定组织单位 (OU) 的 Windows 帐户的名称和密码。
CIFS server NetBIOS name	在 AD 域中唯一的 CIFS 服务器名称。
组织单位	AD 域中要与 CIFS 服务器关联的组织单元。默认值为 cn = computers。 <ul style="list-style-type: none"> <li>要将 AWS 托管 Microsoft AD 配置为 Cloud Volumes ONTAP 的 AD 服务器，您应在此字段中输入 * OU=Computers，OU=corp*。</li> <li>要将 Azure AD 域服务配置为 Cloud Volumes ONTAP 的 AD 服务器，应在此字段中输入 * OU=ADDC Computers * 或 * OU=ADDC Users*。https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou["Azure 文档：在 Azure AD 域服务托管域中创建组织单位（OU）"]</li> </ul>
DNS 域	Cloud Volumes ONTAP Storage Virtual Machine（SVM）的 DNS 域。在大多数情况下，域与 AD 域相同。
NTP 服务器	选择 * 使用 Active Directory 域 * 以使用 Active Directory DNS 配置 NTP 服务器。如果需要其他地址配置 NTP 服务器，则应使用 API。请参见 "Cloud Manager API 开发人员指南" 了解详细信息。

5. 在使用情况配置文件，磁盘类型和分层策略页面上，选择是否要启用存储效率功能，选择磁盘类型，并根据

需要编辑分层策略。

有关帮助信息，请参阅以下内容：

- ["了解卷使用情况配置文件"](#)
- ["在 AWS 中估算系统规模"](#)
- ["在 Azure 中估算系统规模"](#)
- ["数据分层概述"](#)

6. 单击 \* 执行 \*。

结果

Cloud Volumes ONTAP 配置卷。

完成后

如果配置了 CIFS 共享、请授予用户或组对文件和文件夹的权限、并验证这些用户是否可以访问该共享并创建文件。

如果要对卷应用配额、则必须使用系统管理器或 CLI。配额允许您限制或跟踪用户、组或 qtree 使用的磁盘空间和文件数量。

## 在 HA 配置中的第二个节点上创建 FlexVol 卷

默认情况下，Cloud Manager 会在 HA 配置中的第一个节点上创建卷。如果需要双活动配置（两个节点都将数据提供给客户端）、则必须在第二个节点上创建聚合和卷。

步骤

1. 在“工作环境”页面上，双击要管理聚合的 Cloud Volumes ONTAP 工作环境的名称。
2. 单击菜单图标，然后单击 \* 高级 > 高级分配 \*。
3. 单击 \* 添加聚合 \*，然后创建聚合。
4. 对于主节点，请在 HA 对中选择第二个节点。
5. Cloud Manager 创建聚合后，选择该聚合，然后单击 \* 创建卷 \*。
6. 输入新卷的详细信息，然后单击 \* 创建 \*。

完成后

如果需要，您可以在此聚合上创建其他卷。



对于部署在多个 AWS 可用性区域中的 HA 对，您必须使用卷所在节点的浮动 IP 地址将卷挂载到客户端。

## 创建聚合

您可以自己创建聚合或让 Cloud Manager 在创建卷时为您执行此操作。自行创建聚合的优势在于，您可以选择底层磁盘大小，从而根据需要的容量或性能对聚合进行大小调整。

步骤

1. 在“工作环境”页面上，双击要管理聚合的 Cloud Volumes ONTAP 实例的名称。
2. 单击菜单图标，然后单击 \* 高级 > 高级分配 \*。
3. 单击 \* 添加聚合 \*，然后指定聚合的详细信息。

有关磁盘类型和磁盘大小的帮助，请参见 ["规划配置"](#)。

4. 单击 \* 执行 \*，然后单击 \* 批准和购买 \*。

## 配置 iSCSI LUN

如果要创建 iSCSI LUN，则需要从 System Manager 创建。

开始之前

- 必须在要连接到 LUN 的主机上安装和设置主机实用程序。
- 必须已从主机记录 iSCSI 启动程序名称。为 LUN 创建 igroup 时需要提供此名称。
- 在 System Manager 中创建卷之前，必须确保具有具有足够空间的聚合。您需要在 Cloud Manager 中创建聚合。有关详细信息，请参见 ["创建聚合"](#)。

关于此任务

这些步骤介绍了如何将 System Manager 用于版本 9.3 和更高版本。

步骤

1. ["登录到系统管理器。"](#)
2. 单击 \* 存储 > LUN\*。
3. 单击 \* 创建 \*，然后按照提示创建 LUN。
4. 从主机连接到 LUN。

有关说明，请参见 ["Host Utilities 文档"](#) 适用于您的操作系统。

## 使用 FlexCache 卷加速数据访问

FlexCache 卷是一种存储卷，用于缓存原始（或源）卷中的 NFS 读取数据。后续读取缓存的数据会加快对该数据的访问速度。

您可以使用 FlexCache 卷加快数据访问速度，或者从访问量较多的卷卸载流量。FlexCache 卷有助于提高性能，尤其是在客户端需要重复访问相同数据时，因为可以直接提供数据，而无需访问原始卷。FlexCache 卷非常适合读取密集型系统工作负载。

Cloud Manager 目前不提供 FlexCache 卷的管理，但您可以使用 ONTAP 命令行界面或 ONTAP 系统管理器创建和管理 FlexCache 卷：

- ["《FlexCache 卷加快数据访问高级指南》"](#)
- ["在 System Manager 中创建 FlexCache 卷"](#)

从 3.7.2 版开始，Cloud Manager 将为所有新的 Cloud Volumes ONTAP 系统生成 FlexCache 许可证。此许可证包含 500 GB 的使用量限制。



要生成许可证，Cloud Manager 需要访问 <https://ipa-signer.cloudmanager.netapp.com>。确保此 URL 可从防火墙访问。



## 将非活动数据分层到低成本对象存储

您可以通过将热数据的 SSD 或 HDD 性能层与非活动数据的对象存储容量层相结合来降低存储成本。有关简要概述，请参见 ["数据分层概述"](#)。

要设置数据分层、您只需执行以下操作：



选择支持的配置

支持大多数配置。如果您的 Cloud Volumes ONTAP 标准版，高级版或 BYOL 系统运行的是最新版本，则最好继续操作。 ["了解更多信息。"](#)



确保 **Cloud Volumes ONTAP** 与对象存储之间的连接

- 对于 AWS ， S3 需要一个 VPC 端点。 [了解更多信息。](#)
- 对于 Azure ， 只要 Cloud Manager 具有所需权限， 您就无需执行任何操作。 [了解更多信息。](#)
- 对于 GCP ， 您需要向 Cloud Manager 添加一个 GCP 帐户并为 Private Google Access 配置子网。 [了解更多信息。](#)

### 3

创建，修改或复制卷时，请选择分层策略

在创建，修改或复制卷时，Cloud Manager 会提示您选择分层策略。

- "对读写卷上的数据进行分层"
- "分层数据保护卷上的数据"



数据分层不需要什么？

- 您无需安装功能许可证即可启用数据分层。
- 您无需创建容量层（S3 存储分段，Azure Blob 容器或 GCP 存储分段）。云管理器可以为您提供这种功能。

## 支持数据分层的配置

您可以在使用特定配置和功能时启用数据分层：

- Cloud Volumes ONTAP 标准版，高级版和 BYOL 支持数据分层，从以下版本开始：
  - AWS 中的 9.2 版
  - 采用单节点系统的 Azure 中的 9.4 版
  - 使用 HA 对的 Azure 中的 9.6 版
  - GCP 中的 9.6 版



采用 DS3\_v2 虚拟机类型的 Azure 不支持数据分层。

- 在 AWS 中，性能层可以是通用 SSD、配置的 IOPS SSD 或吞吐量优化 HDD。
- 在 Azure 中，性能层可以是高级 SSD 受管磁盘，标准 SSD 受管磁盘或标准 HDD 受管磁盘。
- 在 GCP 中，性能层可以是 SSD 或 HDD（标准磁盘）。
- 加密技术支持数据分层。
- 必须在卷上启用精简配置。

## 将冷数据分层到 AWS S3 的要求

确保 Cloud Volumes ONTAP 已连接到 S3。提供该连接的最佳方法是创建到 S3 服务的 VPC 端点。有关说明，请参见 ["AWS 文档：创建网关端点"](#)。

创建 VPC 端点时，请确保选择与 Cloud Volumes ONTAP 实例对应的区域、VPC 和路由表。您还必须修改安全组才能添加出站 HTTPS 规则、该规则允许通信到 S3 端点。否则，Cloud Volumes ONTAP 无法连接到 S3 服务。

如果遇到任何问题，请参见 ["AWS 支持知识中心：为什么我无法使用网关 VPC 端点连接到 S3 存储分段？"](#)。



## 将冷数据分层到 Azure Blob 存储的要求

只要 Cloud Manager 具有所需权限，您就无需在性能层和容量层之间设置连接。如果 Cloud Manager 策略具有以下权限，则 Cloud Manager 将为您启用 vNet 服务端点：

```
"Microsoft.Network/virtualNetworks/subnets/write",  
"Microsoft.Network/routeTables/join/action",
```

权限包含在最新版本中 ["Cloud Manager 策略"](#)。

## 将冷数据分层到 Google Cloud 存储分段的要求

- 您需要通过输入服务帐户的存储访问密钥将 Google Cloud Platform 帐户添加到 Cloud Manager。Cloud Manager 可通过这些密钥设置用于数据分层的云存储分段。有关说明，请参见 ["设置 GCP 帐户并将其添加到 Cloud Manager"](#)。
- 必须为 Cloud Volumes ONTAP 所在的子网配置专用 Google 访问。有关说明，请参见 ["Google Cloud 文档：配置私有 Google Access"](#)。

## 对读写卷中的数据进行分层

Cloud Volumes ONTAP 可以将读写卷上的非活动数据分层到经济高效的对象存储中，从而腾出性能层来存储热数据。

### 步骤

1. 在工作环境中、创建新卷或更改现有卷的层：

任务	Action
创建新卷	单击 * 添加新卷 *。
修改现有卷	选择卷并单击 * 更改磁盘类型和分层策略 *。

2. 选择仅快照策略或自动策略。

有关这些策略的问题描述，请参见 ["数据分层概述"](#)。

- 示例 \*



## Tiering data to object storage

### Volume Tiering Policy

- Auto** - Tiers cold Snapshot copies and cold user data from the active file system to object storage.
- Snapshot Only** - Tiers cold Snapshot copies to object storage
- None** - Data tiering is disabled.

如果启用数据分层的聚合尚未存在，则 Cloud Manager 会为该卷创建一个新聚合。



如果您希望自己创建聚合、则可以在创建聚合时对聚合启用数据分层。

## 对数据保护卷中的数据进行分层

Cloud Volumes ONTAP 可以将数据从数据保护卷分层到容量层。如果激活目标卷、则数据将在读取时逐渐移动到性能层。

### 步骤

1. 在 "工作环境" 页上、选择包含源卷的工作环境、然后将其拖到要将卷复制到的工作环境中。
2. 按照提示操作、直至到达分层页面并启用到对象存储的数据分层。

◦ 示例 \*



### S3 Tiering

What are storage tiers?

- Enabled**
- Disabled**

**Note:** If you enable S3 tiering, thin provisioning must be enabled on volumes created in this aggregate.

有关复制数据的帮助，请参见 ["将数据复制到云中或从云中复制数据"](#)。

## 在 AWS 或 Azure 中更改分层级别

启用数据分层后，Cloud Volumes ONTAP 会将非活动数据分层到 AWS 中的 S3 *Standard* 存储类或 Azure 中的 *hot* 存储层。部署 Cloud Volumes ONTAP 后，您可以通过更改 30 天内未访问的非活动数据的分层级别来降低存储成本。如果您确实访问了数据、访问成本会更高、因此在更改分层级别之前必须考虑到这一点。



您不能更改 GCP 中的分层级别，因为此时仅支持 `_Region_storage` 类。

关于此任务

分层级别为 System Wide - 恢复不是每个卷。

在 AWS 中，您可以更改分层级别，以便非活动数据在 30 天后移至以下存储类之一：

- 智能分层
- 标准—不经常访问
- 一个 ZONE 不常访问

在 Azure 中，您可以更改分层级别，以便非活动数据在 30 天后移至 *cool* 存储层。

有关分层级别工作原理的详细信息，请参见 "数据分层概述"。

步骤

1. 在工作环境中，单击菜单图标，然后单击 \* S3 存储类 \* 或 \* Blob 存储分层 \*。
2. 选择分层级别，然后单击 \* 保存 \*。

## 使用 ONTAP 作为 Kubernetes 的永久性存储

Cloud Manager 可以自动部署 "NetApp Trident" 在 Kubernetes 集群上，以便可以使用 ONTAP 作为容器的永久性存储。这适用于 Cloud Volumes ONTAP 和内部 ONTAP 集群。

在完成这些步骤之前，您需要 "创建 Cloud Volumes ONTAP 系统" 或 "发现内部 ONTAP 集群" 通过 Cloud Manager。

如果您使用部署 Kubernetes 集群 "NetApp Kubernetes Service"，Cloud Manager 可以通过您的 NetApp Cloud Central 帐户自动发现集群。如果是这种情况，请跳过前两个步骤，从第 3 步开始。

### 1

#### 验证网络连接

1. Cloud Manager 和 Kubernetes 集群之间以及从 Kubernetes 集群到 ONTAP 系统之间必须具有网络连接。
2. 安装 Trident 时，Cloud Manager 需要出站 Internet 连接才能访问以下端点：

<https://packages.cloud.google.com/yum> <https://github.com/NetApp/trident/releases/download/>

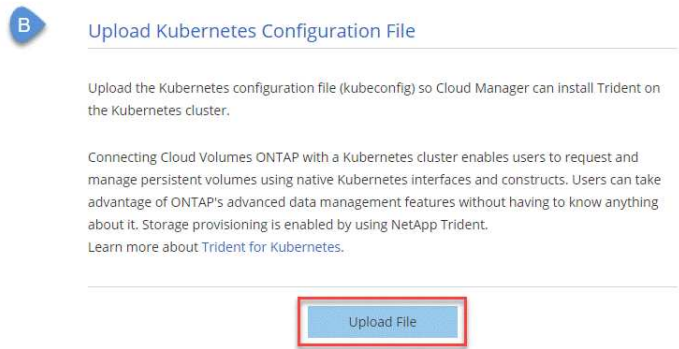
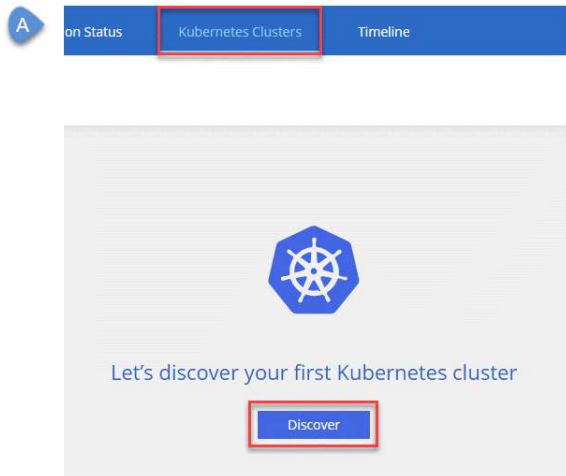
当您在工作环境连接到 Kubernetes 集群时，Cloud Manager 会在该集群上安装 Trident。

### 2

#### 将 Kubernetes 配置文件上传到 Cloud Manager

对于每个 Kubernetes 集群，帐户管理员需要上传一个 YAML 格式的配置文件（`kubeconfig`）。上传文件后，Cloud Manager 会验证与集群的连接，并保存 `kubeconfig` 文件的加密副本。

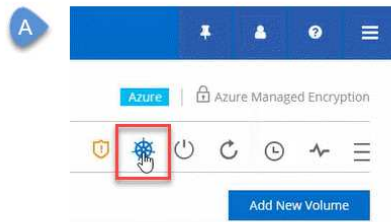
单击 \* Kubernetes Clusters > Discover > Upload File\*，然后选择 `kubeconfig` 文件。



### 3 将您的工作环境连接到 Kubernetes 集群

在工作环境中，单击 Kubernetes 图标并按照提示进行操作。您可以将不同的集群连接到不同的 ONTAP 系统，将多个集群连接到同一个 ONTAP 系统。

您可以选择将 NetApp 存储类设置为 Kubernetes 集群的默认存储类。默认情况下，当用户创建永久性卷时，Kubernetes 集群可以使用已连接的 ONTAP 系统作为后端存储。



### 4 开始配置永久性卷

使用原生 Kubernetes 接口和构造请求和管理永久性卷。Cloud Manager 会创建四个 Kubernetes 存储类，您可以在配置永久性卷时使用这些存储类：

- \* NetApp 文件 \*：用于将永久性卷绑定到单节点 ONTAP 系统
- \* netapp-file-san\*：用于将 iSCSI 永久性卷绑定到单节点 ONTAP 系统
- \* netapp-file-redundred\*：用于将永久性卷绑定到 ONTAP HA 对
- \* netapp-file-redundred-san-san：用于将 iSCSI 永久性卷绑定到 ONTAP HA 对

Cloud Manager 会将 Trident 配置为默认使用以下配置选项：

- 精简卷
- 默认 Snapshot 策略
- 可访问的 Snapshot 目录

["了解有关使用适用于 Kubernetes 的 Trident 配置第一个卷的更多信息"](#)

## 什么是 trident 卷？

Cloud Manager 会在连接到 Kubernetes 集群的第一个 ONTAP 系统上创建一个卷。卷的名称将附加 "\_trident 或 trident 。" ONTAP 使用此卷连接到 Kubernetes 集群。您不应删除这些卷。

## 断开或删除 Kubernetes 集群时会发生什么情况？

使用 Cloud Manager ，您可以断开各个 ONTAP 系统与 Kubernetes 集群的连接。断开系统连接后，不能再将该 ONTAP 系统用作容器的永久性存储。不会删除现有永久性卷。

从 Kubernetes 集群断开所有系统的连接后，您还可以从 Cloud Manager 中删除整个 Kubernetes 配置。删除集群时，Cloud Manager 不会卸载 Trident ，也不会删除任何永久性卷。

这两种操作都只能通过 API 来执行。我们计划在未来版本中将这些操作添加到界面中。["单击此处了解有关 API 的详细信息"](#)。

## 使用 NetApp 卷加密对卷进行加密

NetApp 卷加密（NVE）是一种基于软件的技术，用于一次对一个卷上的空闲数据进行加密。数据，Snapshot 副本和元数据已加密。数据访问由一个唯一的 XTS-AES-256 密钥提供，每个卷一个。

关于此任务

- 从 Cloud Manager 3.7.1 开始，向 NetApp 支持部门注册的每个 Cloud Volumes ONTAP 系统都会自动安装 NetApp 卷加密许可证。
  - ["将 NetApp 支持站点帐户添加到 Cloud Manager"](#)
  - ["注册按需购买的系统"](#)



Cloud Manager 不会在位于中国地区的系统上安装 NVE 许可证。

- 目前，Cloud Volumes ONTAP 通过外部密钥管理服务器支持 NetApp 卷加密。不支持板载密钥管理器。
- 您需要从 ONTAP 命令行界面设置 NetApp 卷加密。

然后，您可以使用命令行界面或 System Manager 对特定卷启用加密。Cloud Manager 不支持从其用户界面及其 API 进行 NetApp 卷加密。

["了解有关支持的加密技术的更多信息"](#)。

## 步骤

1. 查看中支持的密钥管理器列表 "[NetApp 互操作性表工具](#)"。



搜索 \* 密钥管理器 \* 解决方案。

2. "[连接到 Cloud Volumes ONTAP 命令行界面](#)"。
3. 安装 SSL 证书并连接到外部密钥管理服务器。

["ONTAP 9 NetApp 加密高级指南：配置外部密钥管理"](#)

4. 使用命令行界面或 System Manager 创建新的加密卷或转换现有的未加密卷。

- 命令行界面

- 对于新卷，请使用带有 `-encrypt` 参数的 `* volume cre*` 命令。

["ONTAP 9 NetApp 加密高级指南：在新卷上启用加密"](#)

- 对于现有卷，请使用 `* volume encryption conversion start*` 命令。

["ONTAP 9 NetApp 加密高级指南：使用 volume encryption conversion start 命令在现有卷上启用加密"](#)

- System Manager

- 对于新卷，请单击 \* 存储 > 卷 > 创建 > 创建 FlexVol \*，然后选择 \* 已加密 \*。

["使用 System Manager 进行 ONTAP 9 集群管理：创建 FlexVol 卷"](#)

- 对于现有卷，请选择卷，单击 \* 编辑 \*，然后选择 \* 加密 \*。

["使用 System Manager 进行 ONTAP 9 集群管理：编辑卷属性"](#)

## 管理现有存储

利用 Cloud Manager，您可以管理卷、聚合和 CIFS 服务器。它还会提示您移动卷以避免容量问题。

### 管理现有卷


您可以根据存储需求的变化管理现有卷。您可以查看、编辑、克隆、恢复和删除卷。

#### 步骤

1. 在“工作环境”页面上，双击要管理卷的 Cloud Volumes ONTAP 工作环境。
2. 管理卷：

任务	Action
查看有关卷的信息	选择一个卷，然后单击 * 信息 *。

任务	Action
编辑卷（仅限读写卷）	<p>a. 选择一个卷，然后单击 * 编辑 *。</p> <p>b. 修改卷的 Snapshot 策略， NFS 访问控制列表或共享权限，然后单击 * 更新 *。</p> <p> 如果需要自定义 Snapshot 策略，可以使用 System Manager 创建这些策略。</p>
克隆卷	<p>a. 选择一个卷，然后单击 * 克隆 *。</p> <p>b. 根据需要修改克隆名称，然后单击 * 克隆 *。</p> <p>此过程将创建 FlexClone 卷。FlexClone 卷是一个可写的时间点副本、节省空间、因为它对元数据使用少量空间、然后仅在更改或添加数据时占用额外空间。</p> <p>要了解有关 FlexClone 卷的详细信息，请参见 "《<a href="#">ONTAP 9 逻辑存储管理指南</a>》"。</p>
将数据从 Snapshot 副本恢复到新卷	<p>a. 选择一个卷，然后单击 * 从 Snapshot 副本还原 *。</p> <p>b. 选择 Snapshot 副本，输入新卷的名称，然后单击 * 还原 *。</p>
按需创建 Snapshot 副本	<p>a. 选择一个卷，然后单击 * 创建 Snapshot 副本 *。</p> <p>b. 根据需要更改名称，然后单击 * 创建 *。</p>
获取 NFS 挂载命令	<p>a. 选择一个卷，然后单击 * 挂载命令 *。</p> <p>b. 单击 * 复制 *。</p>
更改底层磁盘类型	<p>a. 选择一个卷，然后单击 * 更改磁盘类型和分层策略 *。</p> <p>b. 选择磁盘类型，然后单击 * 更改 *。</p> <p> Cloud Manager 会将卷移动到使用选定磁盘类型的现有聚合中、或者为卷创建新聚合。</p>
更改分层策略	<p>a. 选择一个卷，然后单击 * 更改磁盘类型和分层策略 *。</p> <p>b. 单击 * 编辑策略 *。</p> <p>c. 选择其他策略，然后单击 * 更改 *。</p> <p> Cloud Manager 会将卷移动到使用选定磁盘类型并进行分层的现有聚合中、或者为卷创建一个新聚合。</p>

任务	Action
为卷启用或禁用与 S3 的同步	选择一个卷，然后单击 * 同步到 S3* 或 * 删除同步关系 *。   必须先启用 Sync to S3 功能，然后才能使用这些选项。有关说明，请参见 <a href="#">"将数据同步到 AWS S3"</a>
删除卷	a. 选择一个卷，然后单击 * 删除 *。 b. 再次单击 * 删除 * 进行确认。

## 管理现有聚合

您可以通过添加磁盘，查看聚合相关信息以及删除聚合来自行管理聚合。

开始之前


如果要删除聚合、必须先删除聚合中的卷。

关于此任务

如果聚合空间不足，则可以使用 OnCommand System Manager 将卷移动到另一个聚合。

步骤

1. 在“工作环境”页面上，双击要管理聚合的 Cloud Volumes ONTAP 工作环境。
2. 单击菜单图标，然后单击 \* 高级 > 高级分配 \*。
3. 管理聚合：

任务	Action
查看有关聚合的信息	选择一个聚合并单击 * 信息 *。
在特定聚合上创建卷	选择一个聚合并单击 * 创建卷 *。
将磁盘添加到聚合	a. 选择一个聚合，然后单击 * 添加 AWS 磁盘 * 或 * 添加 Azure 磁盘 *。 b. 选择要添加的磁盘数，然后单击 * 添加 *。   聚合中的所有磁盘大小必须相同。
删除聚合	a. 选择不包含任何卷的聚合，然后单击 * 删除 *。 b. 再次单击 * 删除 * 进行确认。

## 修改 CIFS 服务器

如果您更改了 DNS 服务器或 Active Directory 域、则需要 Cloud Volumes ONTAP 中修改 CIFS 服务器、以便它可以继续为客户端提供存储。



## 步骤

1. 在工作环境中，单击菜单图标，然后单击 \* 高级 > CIFS 设置 \*。
2. 指定 CIFS 服务器的设置：

任务	Action
DNS 主 IP 地址和次 IP 地址	为 CIFS 服务器提供名称解析的 DNS 服务器的 IP 地址。列出的 DNS 服务器必须包含为 CIFS 服务器将加入的域定位 Active Directory LDAP 服务器和域控制器所需的服务位置记录（服务位置记录）。
要加入的 Active Directory 域	您希望 CIFS 服务器加入的 Active Directory（AD）域的 FQDN。
授权加入域的凭据	具有足够权限将计算机添加到 AD 域中指定组织单位 (OU) 的 Windows 帐户的名称和密码。
CIFS server NetBIOS name	在 AD 域中唯一的 CIFS 服务器名称。
组织单位	AD 域中要与 CIFS 服务器关联的组织单元。默认值为 cn = computers。如果将 AWS 托管 Microsoft AD 配置为 Cloud Volumes ONTAP 的 AD 服务器，则应在此字段中输入 * OU=Computers，OU=corp*。
DNS 域	Cloud Volumes ONTAP Storage Virtual Machine（SVM）的 DNS 域。在大多数情况下，域与 AD 域相同。
NTP 服务器	选择 * 使用 Active Directory 域 * 以使用 Active Directory DNS 配置 NTP 服务器。如果需要其他地址配置 NTP 服务器，则应使用 API。请参见 <a href="#">"Cloud Manager API 开发人员指南"</a> 了解详细信息。

3. 单击 \* 保存 \*。

## 结果

Cloud Volumes ONTAP 会根据更改更新 CIFS 服务器。

## 移动卷以避免容量问题

云管理器可能会显示一条需要执行的操作消息、指出需要移动卷以避免容量问题、但无法提供解决问题的建议。如果发生这种情况，您需要确定如何更正问题、然后移动一个或多个卷。

## 步骤

1. [确定如何解决此问题。](#)
2. 根据您的分析、移动卷以避免容量问题：
  - [将卷移动到另一个系统。](#)
  - [将卷移动到同一系统上的另一个聚合。](#)

## 确定如何解决容量问题

如果云管理器无法提供移动卷以避免容量问题的建议、则必须确定需要移动的卷以及是否应将它们移动到同一系统上的另一个聚合或另一个系统上。

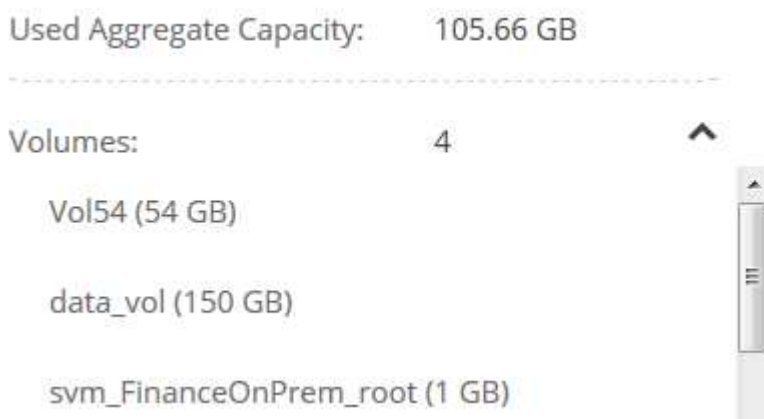
## 步骤

1. 查看“Action Required”（需要操作）消息中的高级信息以确定已达到其容量限制的聚合。

例如，高级信息应显示类似于以下内容的内容：聚合 aggr1 已达到其容量限制。

2. 确定要从聚合中移出的一个或多个卷：

- a. 在工作环境中，单击菜单图标，然后单击 \* 高级 > 高级分配 \*。
- b. 选择聚合，然后单击 \* 信息 \*。
- c. 展开卷列表。



- d. 检查每个卷的大小并选择一个或多个卷以从聚合中移出。

您应该选择足够大的卷来释放聚合中的空间、以便将来避免出现额外的容量问题。

3. 如果系统未达到磁盘限制、则应将卷移动到同一系统上的现有聚合或新聚合。

有关详细信息，请参见 ["将卷移动到另一个聚合以避免容量问题"](#)。

4. 如果系统已达到磁盘限制，请执行以下任一操作：

- a. 删除所有未使用的卷。
- b. 重新排列卷以释放聚合上的空间。

有关详细信息，请参见 ["将卷移动到另一个聚合以避免容量问题"](#)。

- c. 将两个或多个卷移动到另一个具有空间的系统。

有关详细信息，请参见 ["将卷移动到另一个系统以避免容量问题"](#)。

### 将卷移动到另一个系统以避免容量问题

您可以将一个或多个卷移动到另一个 Cloud Volumes ONTAP 系统以避免容量问题。如果系统达到其磁盘限制，则可能需要执行此操作。

#### 关于此任务

您可以按照此任务中的步骤更正以下需要执行的操作消息：

Moving a volume is necessary to avoid capacity issues; however, Cloud Manager cannot perform this action for you because the system has reached the disk limit.

.步骤

- . 确定具有可用容量的 Cloud Volumes ONTAP 系统或部署新系统。
- . 将源工作环境拖放到目标工作环境中以执行卷的一次性数据复制。

+

有关详细信息，请参见 ["在系统之间复制数据"](#)。

1. 转到复制状态页，然后中断 SnapMirror 关系、将复制的卷从数据保护卷转换为读 / 写卷。

有关详细信息，请参见 ["管理数据复制计划和关系"](#)。

2. 配置卷以进行数据访问。

有关为数据访问配置目标卷的信息，请参见 ["《ONTAP 9 卷灾难恢复快速指南》"](#)。

3. 删除原始卷。

有关详细信息，请参见 ["管理现有卷"](#)。

将卷移动到另一个聚合以避免容量问题

您可以将一个或多个卷移动到另一个聚合中以避免容量问题。

关于此任务

您可以按照此任务中的步骤更正以下需要执行的操作消息：

Moving two or more volumes is necessary to avoid capacity issues; however, Cloud Manager cannot perform this action for you.

.步骤

- . 验证现有聚合是否具有需要移动的卷的可用容量：

+

.. 在工作环境中，单击菜单图标，然后单击 \* 高级 > 高级分配 \*。

.. 选择每个聚合，单击 \* 信息 \*，然后查看可用容量（聚合容量减去已用聚合容量）。

+

## aggr1

Aggregate Capacity: 442.94 GB

---

Used Aggregate Capacity: 105.66 GB

---

1. 如果需要，请将磁盘添加到现有聚合：
  - a. 选择聚合，然后单击 \* 添加磁盘 \*。
  - b. 选择要添加的磁盘数，然后单击 \* 添加 \*。
2. 如果没有聚合可用容量，请创建新聚合。

有关详细信息，请参见 ["创建聚合"](#)。
3. 使用 System Manager 或 CLI 将卷移动到聚合。
4. 在大多数情况下，您可以使用 System Manager 移动卷。

有关说明，请参见 "《[ONTAP 9 卷移动快速指南](#)》"。

# 复制和保护数据

## 发现和管理 ONTAP 集群

Cloud Manager 可以在内部环境、NetApp 私有存储配置和 IBM Cloud 中发现 ONTAP 集群。通过发现这些集群，您可以直接从 Cloud Manager 轻松地在混合云环境中复制数据。

### 发现 ONTAP 集群

通过在 Cloud Manager 中发现 ONTAP 集群，您可以在混合云中配置存储和复制数据。

#### 开始之前

要将集群添加到云管理器中，您必须具有管理员用户帐户的集群管理 IP 地址和密码。

Cloud Manager 使用 HTTPS 发现 ONTAP 集群。如果使用自定义防火墙策略，则它们必须满足以下要求：

- Cloud Manager 主机必须允许通过端口 443 进行出站 HTTPS 访问。

如果 Cloud Manager 位于 AWS 中，则预定义安全组允许所有出站通信。

- ONTAP 集群必须允许通过端口 443 进行入站 HTTPS 访问。






默认的“管理”防火墙策略允许从所有 IP 地址进行入站 HTTPS 访问。如果修改了此默认策略、或者创建了自己的防火墙策略，则必须将 HTTPS 协议与该策略关联并启用从云管理器主机进行访问。

#### 步骤

1. 在工作环境页面上，单击 \* 发现 \* 并选择 \* ONTAP Cluster\* 。
2. 在 \* ONTAP 集群详细信息 \* 页面上，输入集群管理 IP 地址，管理员用户帐户的密码以及集群的位置。

#### ONTAP Cluster Details

Provide a few details about your ONTAP cluster so Cloud Manager can discover it.

Cluster Details	Cluster Location
<p>Cluster management IP address</p> <input type="text" value="170.10.15.32"/>	 On Premises
<p>User name</p> <input type="text" value="admin"/>	 IBM Cloud
<p>Password</p> <input type="password" value="*****"/>	 Microsoft Azure
	 Amazon Web Services
	 Google Cloud

3. 在详细信息页面上，输入工作环境的名称和问题描述，然后单击 \* 执行 \* 。

#### 结果

Cloud Manager 可发现集群。您现在可以创建卷、将数据复制到集群或从集群复制数据、并启动 OnCommand System Manager 来执行高级任务。

## 在 ONTAP 集群上配置卷

利用 Cloud Manager，您可以在 ONTAP 集群上配置 NFS 和 CIFS 卷。

开始之前

必须在集群上设置 NFS 或 CIFS。您可以使用 System Manager 或 CLI 设置 NFS 和 CIFS。

关于此任务

您可以在现有聚合上创建卷。无法从 Cloud Manager 创建新聚合。

步骤

1. 在“工作环境”页面上，双击要在其上配置卷的 ONTAP 集群的名称。
2. 单击 \* 添加新卷 \*。
3. 在创建新卷页面上，输入卷的详细信息，然后单击 \* 创建 \*。

本页中的某些字段是不言自明的。下表介绍了可能需要指导的字段：

字段	Description
Size	您可以输入的最大大小在很大程度上取决于您是否启用精简配置、这样您就可以创建一个大于当前可用物理存储的卷。
访问控制（仅适用于 NFS）	导出策略定义子网中可以访问卷的客户端。默认情况下，Cloud Manager 会输入一个值、用于访问子网中的所有实例。
权限和用户 / 组（仅限 CIFS）	这些字段使您能够控制用户和组对共享的访问级别（也称为访问控制列表或 ACL）。您可以指定本地或域 Windows 用户或组、UNIX 用户或组。如果指定域 Windows 用户名，则必须使用 domain\username 格式包含用户的域。
使用情况配置文件	使用情况配置文件定义了为卷启用的 NetApp 存储效率功能。
快照策略	Snapshot 副本策略指定自动创建的 NetApp Snapshot 副本的频率和数量。NetApp Snapshot 副本是一个时间点文件系统映像、对性能没有影响、并且只需要极少的存储。您可以选择默认策略或无。您可以为瞬态数据选择无：例如，Microsoft SQL Server 的 tempdb。

## 在系统之间复制数据

您可以在工作环境之间复制数据、方法是选择一次性数据复制以进行数据传输、或者选择灾难恢复或长期保留的重复计划。例如，您可以设置从内部 ONTAP 系统到 Cloud Volumes ONTAP 的数据复制，以便进行灾难恢复。

使用 SnapMirror 和 SnapVault 技术、Cloud Manager 可以简化不同系统上卷之间的数据复制。您只需标识源卷和目标卷、然后选择复制策略和计划即可。Cloud Manager 购买所需的磁盘、配置关系、应用复制策略、然后启动卷之间的基准传输。



基线传输包括源数据的完整副本。后续传输包含源数据的差异副本。

## 数据复制要求

在复制数据之前、您应该确认是否满足了 Cloud Volumes ONTAP 系统和 ONTAP 集群的特定要求。

### 版本要求

在复制数据之前，您应该验证源卷和目标卷是否运行兼容的 ONTAP 版本。有关详细信息，请参见 ["数据保护高级指南"](#)。

### 特定于 **Cloud Volumes ONTAP** 的要求

- 实例的安全组必须包含所需的入站和出站规则：具体来说，是 ICMP 以及端口 10000，11104 和 11105 的规则。

这些规则包括在预定义的安全组中。

- 要在不同子网的两个 Cloud Volumes ONTAP 系统之间复制数据、必须将子网路由在一起（这是默认设置）。
- 要在 AWS 中的 Cloud Volumes ONTAP 系统和 Azure 中的系统之间复制数据，您必须在 AWS VPC 和 Azure VNet 之间建立 VPN 连接。

### 特定于 **ONTAP** 集群的要求

- 必须安装活动 SnapMirror 许可证。
- 如果集群位于您的内部，则您应该从公司网络连接到 AWS 或 Azure（通常是 VPN 连接）。
- ONTAP 集群必须满足其他子网、端口、防火墙和集群要求。

有关详细信息，请参见适用于您的 ONTAP 版本的集群和 SVM 对等快速指南。

## 在系统之间设置数据复制

您可以在 Cloud Volumes ONTAP 系统和 ONTAP 集群之间复制数据、方法是选择一次性数据复制、该复制可以帮助您将数据移入或移出云、或定期计划、这有助于灾难恢复或长期保留。

### 关于此任务

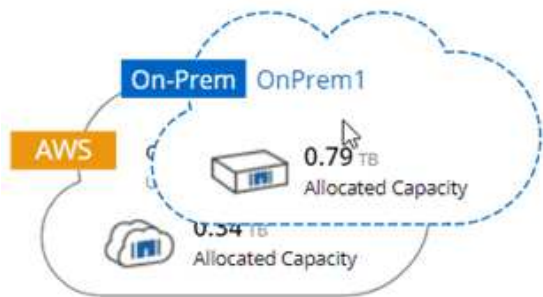
Cloud Manager 支持简单、扇出和级联数据保护配置：

- 在简单的配置中、从卷 A 复制到卷 B
- 在扇出配置中、从卷 A 复制到多个目标。
- 在级联配置中、从卷 A 复制到卷 B、从卷 B 复制到卷 C

通过在系统之间设置多个数据复制、您可以在 Cloud Manager 中配置扇出和级联配置。例如，将卷从系统 A 复制到系统 B、然后将同一卷从系统 B 复制到系统 C

### 步骤

1. 在 "工作环境" 页上、选择包含源卷的工作环境、然后将其拖到要将卷复制到的工作环境中：



2. 如果出现源和目标对等设置页，请为集群对等关系选择所有集群间 LIF 。

应配置集群间网络，使集群对等方具有 成对的全网状连接，这意味着集群对等关系中的每个集群对都在其所有集群间 LIF 之间建立连接。

如果具有多个 LIF 的 ONTAP 集群是源或目标，则会显示这些页面。

3. 在 "源卷选择" 页面上，选择要复制的卷。

4. 在目标卷名称和分层页面上，指定目标卷名称，选择底层磁盘类型，更改任何高级选项，然后单击 \* 继续 \* 。

如果目标是 ONTAP 集群、则还必须指定目标 SVM 和聚合。

5. 在 "最大传输速率" 页面上，指定数据传输的最大速率（以兆字节 / 秒为单位）。

6. 在复制策略页面上，选择一个默认策略或单击 \* 其他策略 \*，然后选择一个高级策略。

有关帮助，请参见 ["选择复制策略"](#)。

如果选择自定义备份（SnapVault）策略、与策略关联的标签必须与源卷上 Snapshot 副本的标签匹配。有关详细信息，请参见 ["备份策略的工作原理"](#)。

7. 在 "计划" 页面上，选择一次性副本或重复计划。

有多个默认计划可用。如果您需要其他计划，则必须使用 System Manager 在 `_destination_cluster` 上创建一个新计划。

8. 在 Review 页面上，查看您选择的内容，然后单击 \* 执行 \* 。

## 结果

Cloud Manager 将启动数据复制过程。您可以在 "复制状态" 页面中查看有关复制的详细信息。

## 管理数据复制计划和关系

在两个系统之间设置数据复制后、您可以从 Cloud Manager 管理数据复制计划和关系。

## 步骤

1. 在工作环境页面上，查看工作空间中所有工作环境或特定工作环境的复制状态：



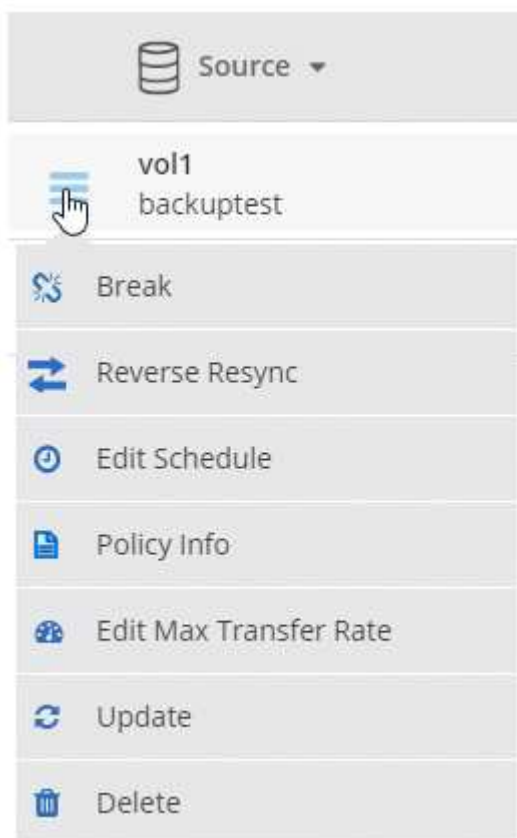
选项	Action
工作空间中的所有工作环境	在 Cloud Manager 顶部，单击 * 复制状态 *。
特定的工作环境	打开工作环境，然后单击 * 复制 *。

2. 检查数据复制关系的状态以验证它们是否正常。



如果关系的状态为空闲且镜像状态未初始化，则必须初始化目标系统的关系，以便根据定义的计划进行数据复制。您可以使用系统管理器或命令行界面（CLI）初始化关系。当目标系统发生故障后又重新联机时，可能会显示这些状态。

3. 选择源卷旁边的菜单图标，然后选择一个可用操作。



下表介绍了可用的操作：

Action	Description
中断	断开源卷和目标卷之间的关系、并激活目标卷以进行数据访问。当源卷由于数据损坏、意外删除或脱机状态等事件而无法提供数据时，通常会使用此选项。有关为数据访问配置目标卷和重新激活源卷的信息、请参见《ONTAP 9 卷灾难恢复快速指南》。

Action	Description
重新同步	<p>重新建立卷之间断开的关系并根据定义的计划恢复数据复制。</p> <p> 重新同步卷时、目标卷上的内容将被源卷上的内容覆盖。</p> <p>要执行反向重新同步，以便将数据从目标卷重新同步到源卷，请参见 "<a href="#">《ONTAP 9 卷灾难恢复快速指南》</a>"。</p>
反向重新同步	<p>反转源卷和目标卷的角色。原始源卷中的内容将被目标卷的内容覆盖。当您要重新激活脱机的源卷时，这非常有用。在上次数据复制和源卷禁用之间写入到原始源卷的任何数据都不会保留。</p>
编辑计划	<p>允许您为数据复制选择不同的计划。</p>
策略信息	<p>显示分配给数据复制关系的保护策略。</p>
编辑最大传输速率	<p>允许您编辑数据传输的最大速率（以千字节 / 秒为单位）。</p>
更新	<p>启动增量传输以更新目标卷。</p>
删除	<p>删除源卷和目标卷之间的数据保护关系，这意味着数据复制不再发生在卷之间。此操作不会激活目标卷以进行数据访问。如果系统之间没有其他数据保护关系，此操作还会删除集群对等关系和存储虚拟机（SVM）对等关系。</p>

## 结果

选择操作后、Cloud Manager 将更新关系或计划。

## 选择复制策略

在 Cloud Manager 中设置数据复制时，您可能需要有关选择复制策略的帮助。复制策略定义存储系统如何将数据从源卷复制到目标卷。

### 复制策略的作用

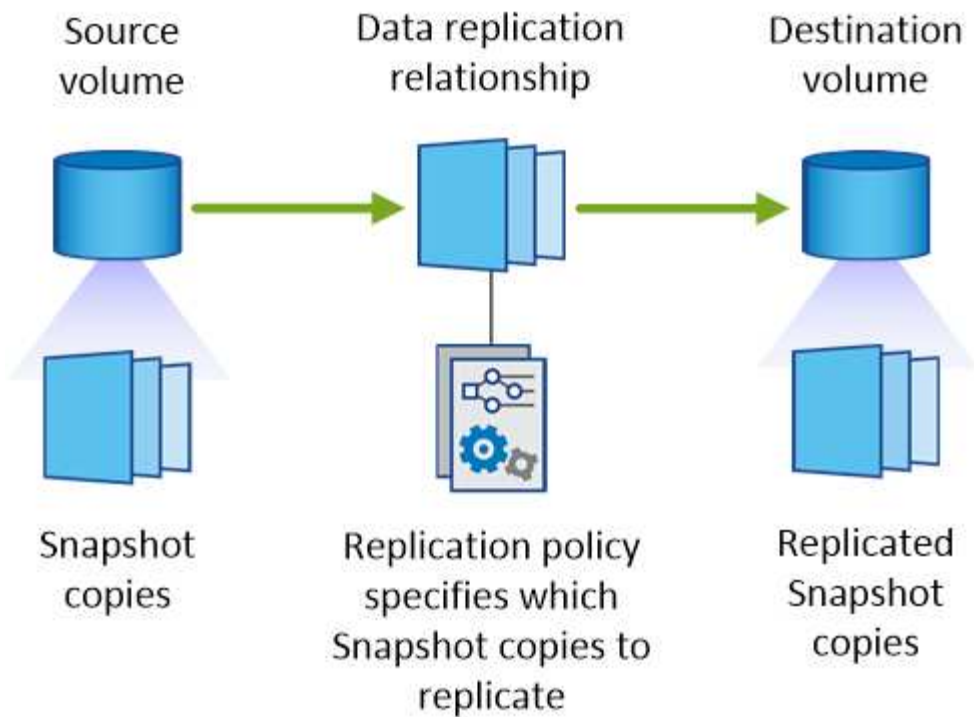
ONTAP 操作系统会自动创建称为 Snapshot 副本的备份。Snapshot 副本是卷的只读映像、可在某个时间点捕获文件系统的状态。

在系统之间复制数据时、您会将 Snapshot 副本从源卷复制到目标卷。复制策略指定要从源卷复制到目标卷的快照副本。



复制策略也称为 *protection* 策略，因为它们由 SnapMirror 和 SnapVault 技术提供支持，这些技术可提供灾难恢复保护以及磁盘到磁盘备份和恢复。

下图显示了 Snapshot 副本和复制策略之间的关系：



## 复制策略的类型

复制策略有三种类型：

- *Mirror* 策略会将新创建的 Snapshot 副本复制到目标卷。

您可以使用这些 Snapshot 副本保护源卷、为灾难恢复或一次性数据复制做好准备。您可以随时激活目标卷以进行数据访问。

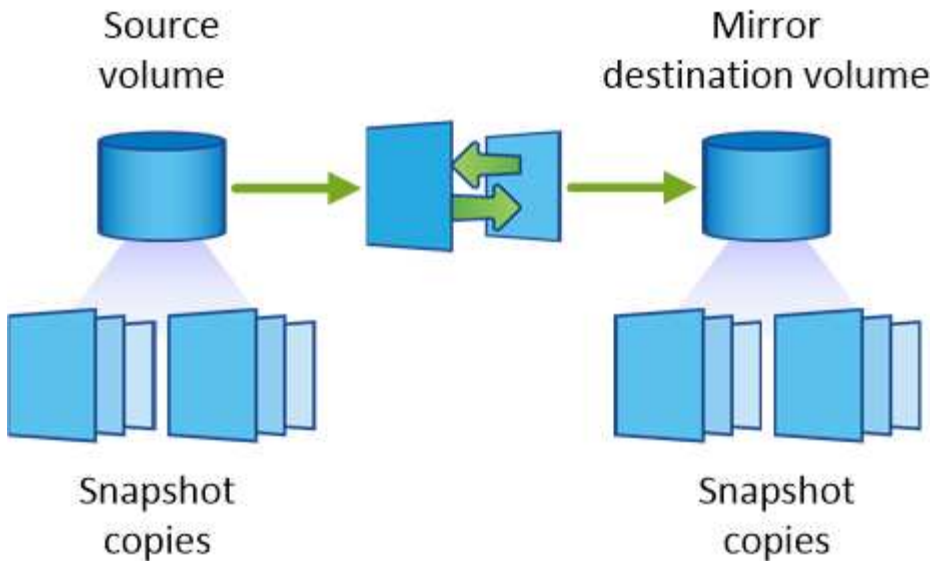
- *Backup* 策略会将特定 Snapshot 副本复制到目标卷，并且这些副本的保留时间通常比源卷上的保留时间长。

您可以在数据损坏或丢失时从这些 Snapshot 副本中恢复数据、并保留这些数据以符合标准和其他与管理相关的目的。

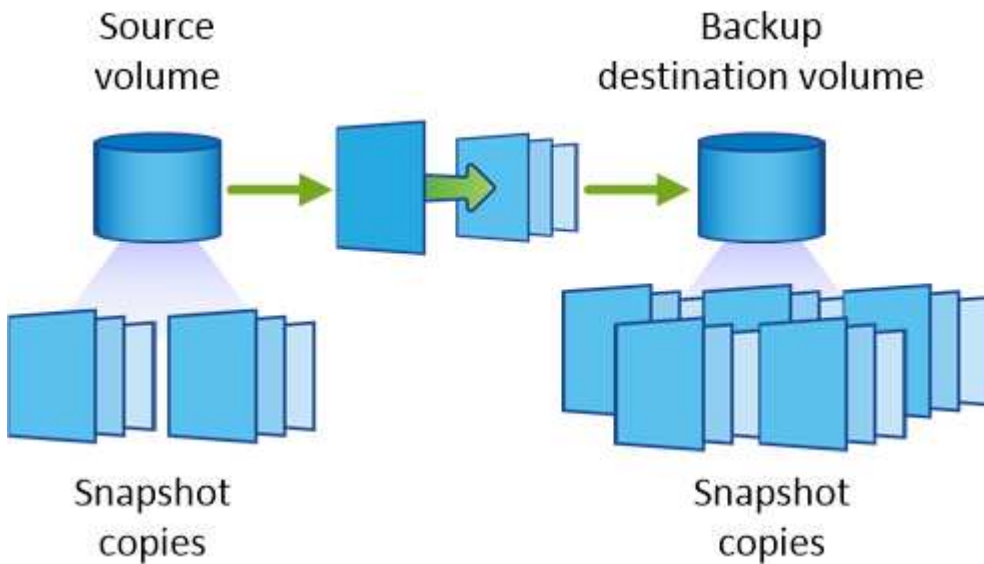
- *Mirror and Backup* 策略可提供灾难恢复和长期保留。

每个系统都包括一个默认镜像和备份策略、它可以在许多情况下正常工作。如果您发现需要自定义策略、则可以使用 System Manager 创建自己的策略。

以下映像显示镜像策略和备份策略之间的区别。镜像策略镜像源卷上可用的 Snapshot 副本。



备份策略通常保留 Snapshot 副本的时间比保留在源卷上的时间长：



### 备份策略的工作原理

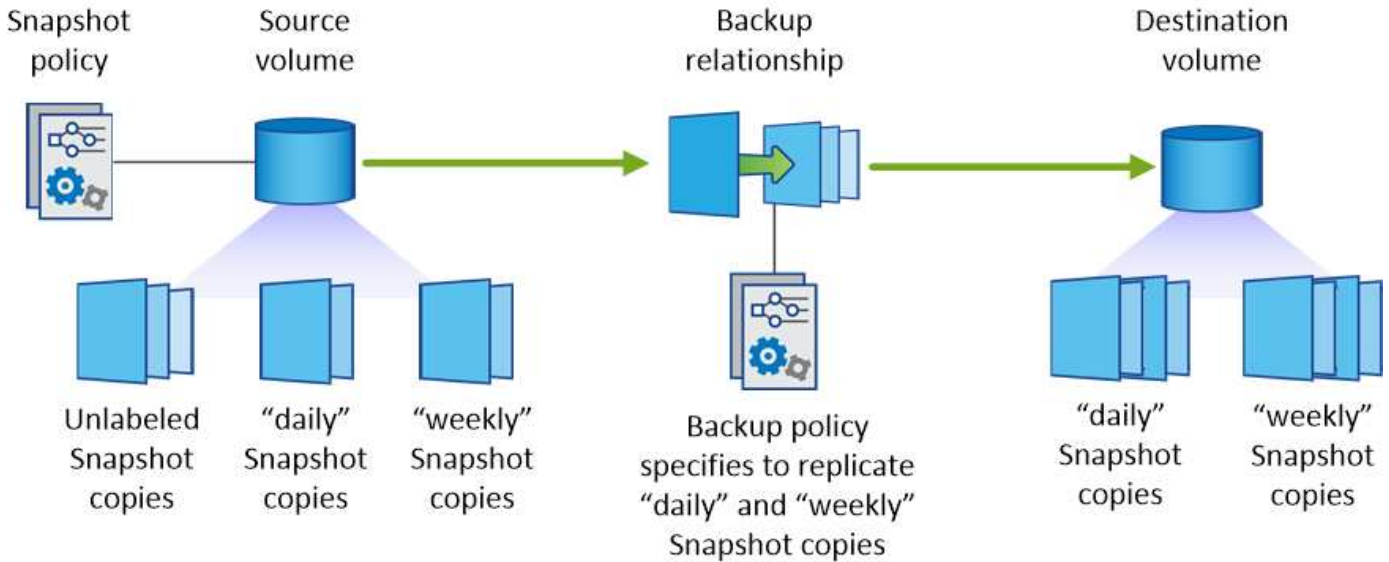
与镜像策略不同、备份（SnapVault）策略将特定的 Snapshot 副本复制到目标卷。如果要使用自己的策略而不是默认策略、了解备份策略的工作原理非常重要。

#### 了解 Snapshot 副本标签与备份策略之间的关系

Snapshot 策略定义系统如何创建卷的 Snapshot 副本。该策略指定创建 Snapshot 副本的时间、要保留的副本数量以及如何对其进行标记。例如，系统可能每天在上午 12 点 10 分创建一个 Snapshot 副本、保留最近的两个副本并将其标记为“每日”。

备份策略包括指定要复制到目标卷的标有 Snapshot 副本以及要保留的副本数量的规则。备份策略中定义的标签必须与快照策略中定义的一个或多个标签匹配。否则，系统将无法复制任何 Snapshot 副本。

例如，包含标签“daily”和“weekly”的备份策略会导致复制仅包含这些标签的 Snapshot 副本。不会复制其他 Snapshot 副本，如下图所示：



#### 默认策略和自定义策略

默认 Snapshot 策略会创建每小时、每天和每周 Snapshot 副本、保留六个小时、每天两个和每周两个 Snapshot 副本。

您可以轻松地将默认备份策略与默认快照策略一起使用。默认备份策略复制每日和每周 Snapshot 副本、保留每天七个 Snapshot 副本和每周 52 个 Snapshot 副本。

如果创建自定义策略，则这些策略定义的标签必须匹配。您可以使用 System Manager 创建自定义策略。

## 将数据备份到 Amazon S3

备份到 S3 是 Cloud Volumes ONTAP 的一项附加功能，可提供完全托管的备份和还原功能，以保护云数据并对其进行长期归档。备份存储在 S3 对象存储中，与用于近期恢复或克隆的卷 Snapshot 副本无关。

启用备份到 S3 后，此服务将对数据执行完整备份。所有附加备份均为增量备份，这意味着仅备份更改的块和新块。

"有关定价详细信息，请访问 [NetApp Cloud Central](#)"。

请注意，您必须使用 Cloud Manager 执行所有备份和还原操作。直接从 ONTAP 或 Amazon S3 执行的任何操作都会导致配置不受支持。

### 快速入门

按照以下步骤快速入门，或者向下滚动到其余部分以了解完整详细信息。



验证是否支持您的配置

验证以下内容：

- Cloud Volumes ONTAP 9.4 或更高版本正在受支持的 AWS 区域中运行： N.弗吉尼亚州，俄勒冈州，爱尔兰，法兰克福或悉尼
- 您已订阅新的 "Cloud Manager Marketplace 产品"
- 对于 Cloud Volumes ONTAP 安全组上的出站流量， TCP 端口 5010 处于打开状态（默认情况下处于打开状态）
- 对于 Cloud Manager 安全组上的出站流量， TCP 端口 8088 处于打开状态（默认情况下处于打开状态）
- 可从 Cloud Manager 访问以下端点：

<https://w86yt021u5.execute-api.us-east-1.amazonaws.com/production/whitelist>

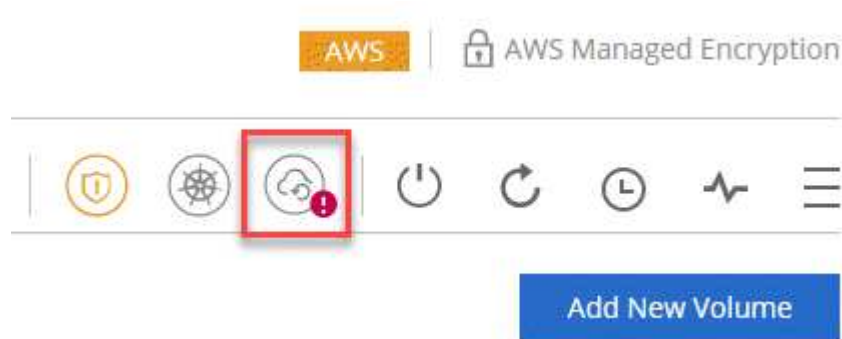
- Cloud Manager 可以在 VPC 中最多分配两个接口 VPC 端点（每个 VPC 的 AWS 限制为 20）
- Cloud Manager 有权使用最新列出的 VPC 端点权限 "Cloud Manager 策略"：

```
"ec2:DescribeVpcEndpoints",
"ec2:CreateVpcEndpoint",
"ec2:ModifyVpcEndpoint",
"ec2>DeleteVpcEndpoints"
```

2

在新系统或现有系统上启用备份到云

- 新系统：在工作环境向导中，默认情况下会启用备份到 S3 功能。请务必保持此选项处于启用状态。
- 现有系统：打开工作环境，单击备份设置图标并启用备份。



3

If needed, modify the backup policy

默认策略每天备份卷，并为每个卷保留 30 个备份副本。如果需要，您可以更改要保留的备份副本数。

## Backup to S3

**Backup Working Environment**  Automatically back up all volumes

---

**Policy - Retention & Schedule**

Backup every:  Number of backups to retain:

## 4

根据需要还原数据

在 Cloud Manager 顶部，单击 \* 备份和还原 \*，选择一个卷，选择一个备份，然后将数据从备份还原到新卷。

vol1

Select the backup you want to restore

Aug 21, 2019 05:01:34 PM UTC



## 要求

开始将卷备份到 S3 之前，请阅读以下要求，以确保您的配置受支持。

### 支持的 **ONTAP** 版本

Cloud Volume ONTAP 9.4 及更高版本支持备份到 S3。

### 支持的 **AWS** 区域

在以下 AWS 地区，Cloud Volumes ONTAP 支持备份到 S3：

- 美国东部（N.维吉尼亚）
- US West（俄勒冈州）
- 欧盟（爱尔兰）
- 欧盟（法兰克福）
- 亚太地区（悉尼）

## 需要 AWS 权限

为 Cloud Manager 提供权限的 IAM 角色必须包括以下内容：

```
"ec2:DescribeVpcEndpoints",  
"ec2:CreateVpcEndpoint",  
"ec2:ModifyVpcEndpoint",  
"ec2>DeleteVpcEndpoints"
```

## AWS 订阅要求

从 3.7.3 版开始，AWS Marketplace 中提供了一个新的 Cloud Manager 订阅。此订阅可用于部署 Cloud Volumes ONTAP 9.6 及更高版本的 PAYGO 系统以及备份到 S3 功能。您需要 ["订阅此新的 Cloud Manager 订阅"](#) 在启用备份到 S3 之前。备份到 S3 功能的计费通过此订阅完成。

## 端口要求

- TCP 端口 5010 必须处于打开状态，才能传输从 Cloud Volumes ONTAP 到备份服务的出站流量。
- 对于 Cloud Manager 安全组上的出站流量，必须打开 TCP 端口 8088。

如果使用预定义的安全组，则这些端口已打开。但是，如果您使用自己的端口，则需要打开这些端口。

## 出站 Internet 访问

确保可从 Cloud Manager 访问以下端点：<https://w86yt021u5.execute-api.us-east-1.amazonaws.com/production/whitelist>

Cloud Manager 会联系此端点，将您的 AWS 帐户 ID 添加到备份到 S3 的允许用户列表中。

## 接口 VPC 端点

启用备份到 S3 功能后，Cloud Manager 会在运行 Cloud Volumes ONTAP 的 VPC 中创建接口 VPC 端点。此 *backup endpoint* 连接到运行备份到 S3 的 NetApp VPC。如果还原卷，Cloud Manager 会创建一个额外的接口 VPC 端点，即 *restore endpoint*。

VPC 中的任何其他 Cloud Volumes ONTAP 系统都使用这两个 VPC 端点。

["接口 VPC 端点的默认限制为每个 VPC 20 个"](#)。在启用此功能之前，请确保您的 VPC 未达到此限制。

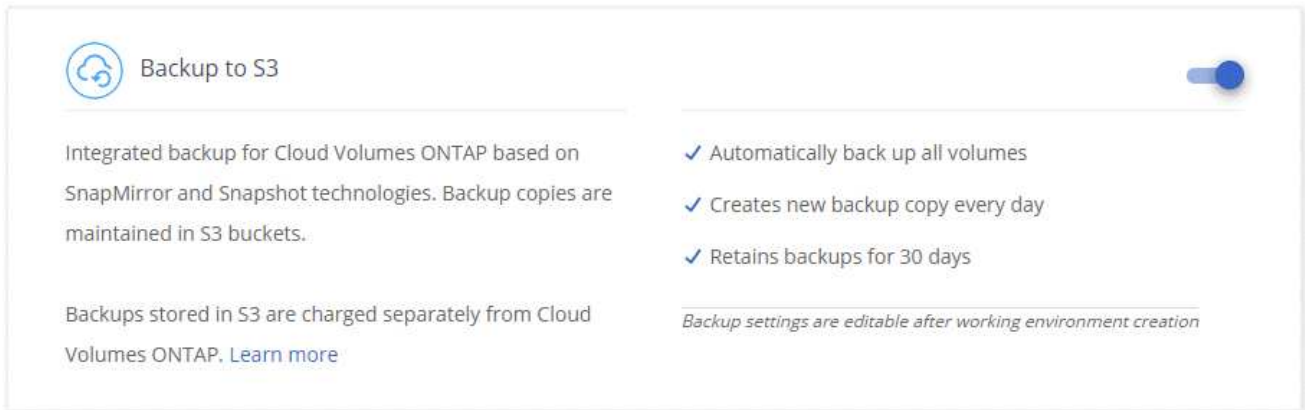
## 在新系统上启用 S3 备份

默认情况下，"备份到 S3" 功能在工作环境向导中处于启用状态。请务必保持此选项处于启用状态。

### 步骤

1. 单击 \* 创建 Cloud Volumes ONTAP \*。
2. 选择 Amazon Web Services 作为云提供商，然后选择单个节点或 HA 系统。
3. 填写详细信息和凭据页面。
4. 在备份到 S3 页面上，保持此功能处于启用状态，然后单击 \* 继续 \*。





5. 完成向导中的页面以部署系统。

#### 结果

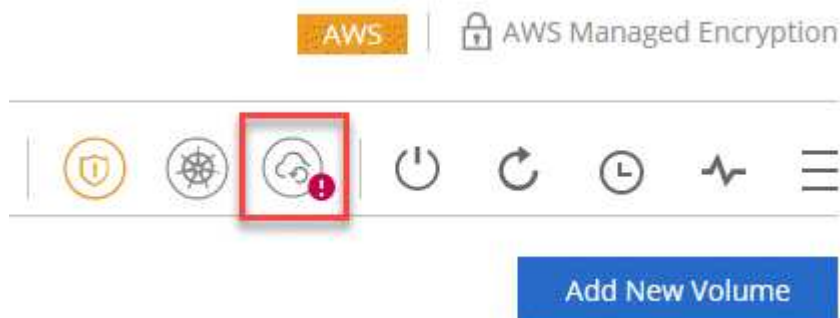
系统上已启用备份到 S3 功能，每天备份卷并保留 30 个备份副本。 [了解如何修改备份保留](#)。

### 在现有系统上启用 S3 备份

您可以在现有 Cloud Volumes ONTAP 系统上启用到 S3 的备份，前提是您运行的配置受支持。有关详细信息，请参见 [\[要求\]](#)。

#### 步骤

1. 打开工作环境。
2. 单击备份设置图标。



3. 选择 \* 自动备份所有卷 \*。
4. 选择您的备份保留，然后单击 \* 保存 \*。

## Backup to S3

**Backup Working Environment**  Automatically back up all volumes

---

**Policy - Retention & Schedule**

Backup every:  Number of backups to retain:

### 结果

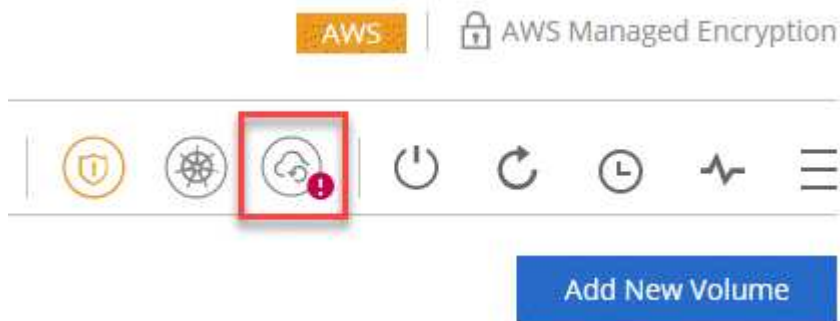
备份到 S3 功能将开始对每个卷进行初始备份。

### 更改备份保留

默认策略每天备份卷，并为每个卷保留 30 个备份副本。您可以更改要保留的备份副本数。

### 步骤

1. 打开工作环境。
2. 单击备份设置图标。



3. 更改备份保留，然后单击 \* 保存 \* 。

## Backup to S3

**Backup Working Environment**  Automatically back up all volumes

---

**Policy - Retention & Schedule**

Backup every:  Number of backups to retain:

## 还原卷

从备份还原数据时，Cloud Manager 会将完整卷还原到 *new* 卷。您可以将数据还原到同一工作环境或其他工作环境。

### 步骤

1. 在 Cloud Manager 顶部，单击 \* 备份和还原 \*。
2. 选择要还原的卷。

Working Environment	Source Volume	Last Backup	Policy	Retention	Relationship Status	
BackupandRestore (On)	vol1 (Available)	Aug 21, 2019 05:01:34 PM U...	Daily	30	Active (idle)	<a href="#">View Backup List</a>

3. 找到要从中还原的备份，然后单击还原图标。

vol1

Select the backup you want to restore

Aug 21, 2019 05:01:34 PM UTC



4. 选择要将卷还原到的工作环境。
5. 输入卷的名称。
6. 单击 \* 还原 \*。

< vol1



### Restore Backup to a new volume

Aug 21, 2019 05:01:34 PM UTC

Select Working Environment

BackupandRestore

Volume Name

vol1\_restore

#### Volume Info

Volume Size: 100 GB

Snapshot Policy: Default

NFS Protocol: Custom export policy, 172.31.0.0/16

Storage Efficiency: ON

Disk Type: GP2

Tiering: auto

Restore

Cancel

## 删除备份

所有备份都会保留在 S3 中，直到您从 Cloud Manager 中删除为止。删除卷或删除 Cloud Volumes ONTAP 系统时，不会删除备份。

### 步骤

1. 在 Cloud Manager 顶部，单击 \* 备份和还原 \*。
2. 选择一个卷。
3. 找到要删除的备份，然后单击删除图标。

vol1

Select the backup you want to restore



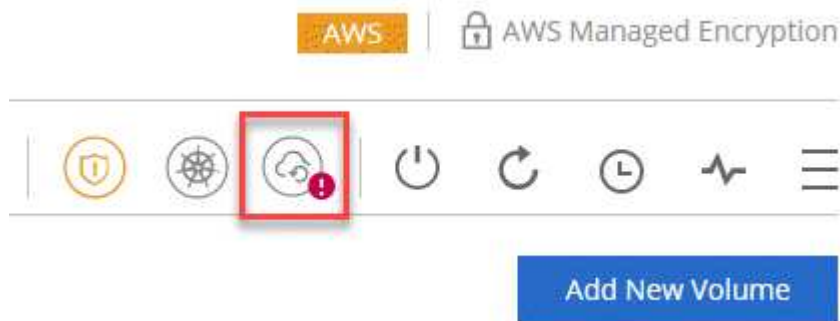
4. 确认要删除备份。

## 禁用 S3 备份

禁用 S3 备份会禁用系统上每个卷的备份。不会删除任何现有备份。

步骤

1. 打开工作环境。
2. 单击备份设置图标。



3. 禁用 \* 自动备份所有卷 \* ，然后单击 \* 保存 \* 。

## 备份到 S3 的工作原理

以下各节提供了有关备份到 S3 功能的详细信息。

### 备份所在位置

备份副本存储在 NetApp 拥有的 S3 存储分段中，该分段与 Cloud Volumes ONTAP 系统所在的区域相同。

### 备份是增量备份

对数据进行初始完整备份后，所有其他备份都是增量备份，这意味着只会备份更改的块和新块。

### 备份在午夜进行

每天的备份在每天午夜后开始。此时，您无法计划在用户指定的时间执行备份操作。

## 备份副本与您的 **Cloud Central** 帐户关联

备份副本与关联 "[Cloud Central 帐户](#)" Cloud Manager 所在位置。

如果您在同一 Cloud Central 帐户中有多个 Cloud Manager 系统，则每个 Cloud Manager 系统将显示相同的备份列表。其中包括与其他 Cloud Manager 系统中的 Cloud Volumes ONTAP 实例关联的备份。

## 备份策略在系统范围内执行

要保留的备份数是在系统级别定义的。您不能为系统上的每个卷设置不同的策略。

## 安全性

使用 AES-256 位空闲加密和正在传输的 TLS 1.2 HTTPS 连接保护备份数据。

数据通过安全的 Direct Connect 链路传输到服务，并通过 AES 256 位加密在空闲时提供保护。然后，加密数据将使用 HTTPS TLS 1.2 连接写入云。数据也只能通过安全的 VPC 端点连接传输到 Amazon S3，因此不会通过 Internet 发送任何流量。

除了服务拥有的整体加密密钥之外，还会为每个用户分配一个租户密钥。这一要求类似于需要一对密钥才能在银行内为客户提供安全保护。所有密钥作为云凭据，均由服务安全存储，并且仅限负责维护服务的特定 NetApp 人员使用。

## 限制

- 如果您使用以下任一实例类型，则 Cloud Volumes ONTAP 系统最多可以将 20 个卷备份到 S3：
  - m4.xlarge
  - m5.xlarge
  - r4.xlarge
  - R5.xlarge
- 您在 Cloud Manager 外部创建的卷不会自动备份到 S3。

例如，如果您使用 ONTAP 命令行界面，ONTAP API 或 System Manager 创建卷，则不会自动备份该卷。

如果要备份这些卷，则需要禁用备份到 S3，然后重新启用它。

- 从备份还原数据时，Cloud Manager 会将完整卷还原到 *new* 卷。此新卷不会自动备份到 S3。

如果要备份通过还原操作创建的卷，则需要禁用备份到 S3，然后重新启用它。

- 您可以备份大小不超过 50 TB 的卷。
- 备份到 S3 最多可以为一个卷保留 245 个备份。
- 启用备份到 S3 后，Cloud Volumes ONTAP 系统不支持 WORM 存储。

## 正在将数据同步到 **Amazon S3**

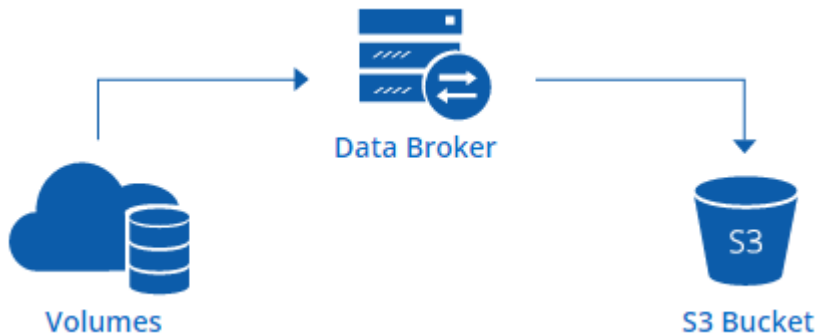
您可以通过将工作环境与集成来将 ONTAP 卷中的数据同步到 Amazon S3 存储分段 "[NetApp Cloud Sync](#)"。然后，您可以将同步数据用作二级副本或使用 AWS 服务（如

EMR 和 RedShift ) 进行数据处理。

## 同步到 S3 功能的工作原理

您可以随时将工作环境与云同步服务集成。在集成工作环境时、Cloud Sync Service 会将选定卷中的数据同步到单个 S3 存储区。该集成可与 Cloud Volumes ONTAP 工作环境以及内部或部分 NetApp 私有存储 ( NPS ) 配置的 ONTAP 集群配合使用。

要同步数据、服务将在 VPC 中启动数据代理实例。Cloud Sync 在每个工作环境中使用一个数据代理将卷中的数据同步到 S3 数据桶。初始同步后、服务每天在午夜对任何更改的数据进行一次同步。



如果要执行高级云同步操作、请直接转至 Cloud Sync 服务。您可以在其中执行操作，例如从 S3 同步到 NFS 服务器、为卷选择不同的 S3 存储区以及修改计划。

### 14 天免费试用

如果您是新的 Cloud Sync 用户、则前 14 天免费。免费试用结束后，您必须按小时费率或通过购买许可证为每个 \_sync 关系支付费用。您与 S3 存储池同步的每个卷都被视为同步关系。您可以在许可证设置页面中直接从 Cloud Sync 设置这两个付款选项。

### 如何获得帮助

使用以下选项可获得与 Cloud Manager Sync to S3 功能相关的任何支持或通常的 Cloud Sync 功能：

- 一般产品反馈： [ng-CloudSync-contact@netapp.com](mailto:ng-CloudSync-contact@netapp.com)
- 技术支持选项：
  - NetApp Cloud Sync 社区
  - 产品内聊天 ( Cloud Manager 右下角)

## 将工作环境与云同步服务集成

如果要直接从 Cloud Manager 将卷同步到 Amazon S3 ，则必须将工作环境与 Cloud Sync 服务集成。

□ | [https://img.youtube.com/vi/3hOtLs70\\_xE/maxresdefault.jpg](https://img.youtube.com/vi/3hOtLs70_xE/maxresdefault.jpg)

### 步骤

1. 打开一个工作环境，然后单击 \* 同步到 S3\* 。

2. 单击 \* 同步 \* ，然后按照提示将数据同步到 S3 。



您无法将数据保护卷同步到 S3 。卷必须可写。

## 管理卷同步关系

将工作环境与 Cloud Sync 服务集成后、您可以同步其他卷、停止同步卷并删除与 Cloud Sync 的集成。

### 步骤

1. 在“工作环境”页面上，双击要管理同步关系的工作环境。
2. 如果要为卷启用或禁用与 S3 的同步，请选择此卷，然后单击 \* 同步到 S3\* 或 \* 删除同步关系 \* 。
3. 如果要删除工作环境中的所有同步关系，请单击 \* 同步到 S3\* 选项卡，然后单击 \* 删除同步 \* 。

此操作不会从 S3 存储区中删除已同步的数据。如果数据代理未在任何其他同步关系中使用，则 Cloud Sync 服务将删除数据代理。



# 深入了解数据隐私

## 了解云合规性

云合规性是一项适用于 AWS 和 Azure 中 Cloud Volumes ONTAP 的数据隐私和合规服务。借助人工智能（AI）驱动的技术，云合规性可帮助企业了解数据环境并识别 Cloud Volumes ONTAP 系统中的敏感数据。

Cloud Compliance 目前作为受控可用性版本提供。

["了解 Cloud Compliance 的用例"](#)。

## 功能

Cloud Compliance 提供了多种工具，可帮助您完成合规工作。您可以使用 Cloud Compliance：

- 识别个人身份信息（PII）
- 根据 GDPR，CCPA，PCI 和 HIPAA 隐私法规的要求确定广泛的敏感信息
- 响应数据主体访问请求（DSAR）

## 成本

云合规性是 NetApp 为 Cloud Volumes ONTAP 提供的一项附加服务，无需额外付费。激活云合规性需要部署云实例，您的云提供商将向您收取此实例的费用。数据传入或传出不收费，因为数据不会在网络外部流动。

## Cloud Compliance 的工作原理

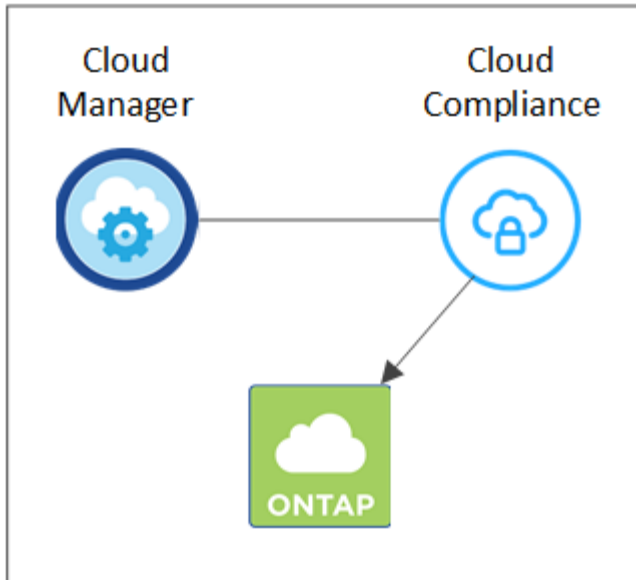
概括地说，云合规性的工作原理如下：

1. 您可以在一个或多个 Cloud Volumes ONTAP 系统上启用云合规性。
2. Cloud Compliance 使用 AI 学习流程扫描数据。
3. 在 Cloud Manager 中，单击 \* 合规性 \*，然后使用提供的信息板和报告工具帮助您实现合规性。

## Cloud Compliance 实例

在一个或多个 Cloud Volumes ONTAP 系统上启用云合规性后，Cloud Manager 会在请求中的第一个 Cloud Volumes ONTAP 系统所在的同一 VPC 或 vNet 中部署一个云合规实例。

## VPC or VNet



有关此实例，请注意以下事项：

- 在 Azure 中，Cloud Compliance 在具有 512 GB 磁盘的 Standard\_d16s\_v3 VM 上运行。
- 在 AWS 中，Cloud Compliance 在具有 500 GB IO1 磁盘的 m5.4xlarge 实例上运行。  
在 m5.4xlarge 不可用的区域中，Cloud Compliance 会在 m4.4xlarge 实例上运行。
- 此实例名为 *CloudCompliance*，并与生成的哈希（UUID）串联在一起。例如：*CloudCompliance" — 16bb6564-38AD-4080-9a92 — 36f5fd2f71c7*
- 每个 Cloud Manager 系统仅部署一个 Cloud Compliance 实例。
- Cloud Compliance 软件的升级是自动化的—您无需担心。



此实例应始终保持运行状态，因为云合规性会持续扫描 Cloud Volumes ONTAP 系统上的数据。

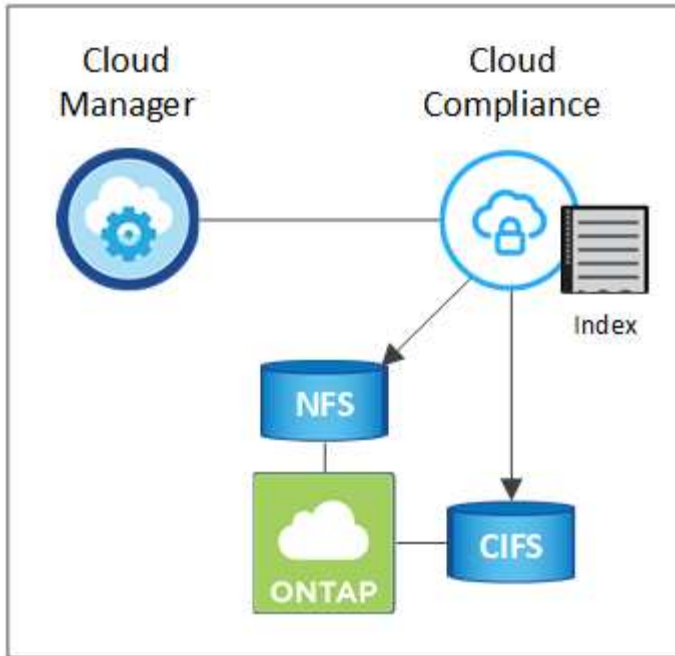
## 扫描的工作原理

启用 Cloud Compliance 后，它会立即开始扫描您的数据以识别个人和敏感数据。

Cloud Compliance 通过挂载 NFS 和 CIFS 卷与任何其他客户端一样连接到 Cloud Volumes ONTAP。NFS 卷会自动以只读方式访问，而您需要提供 Active Directory 凭据来扫描 CIFS 卷。

Cloud Compliance 会扫描每个卷上的非结构化数据以查找一系列个人信息。它会映射您的组织数据，对每个文件进行分类，并标识和提取数据中的实体和预定义模式。扫描的结果是个人信息，敏感个人信息和数据类别的索引。

## VPC or VNet



在初始扫描之后，Cloud Compliance 会持续扫描每个卷以检测增量更改（因此，保持实例运行非常重要）。

您可以在工作环境级别打开和关闭扫描，但不能在卷级别打开和关闭扫描。 ["了解如何操作"](#)。

## Cloud Compliance 索引的信息

Cloud Compliance 收集非结构化数据（文件）并为其编制索引和分配类别。Cloud Compliance 索引的数据包括以下内容：

### 标准元数据

Cloud Compliance 收集有关文件的标准元数据：文件类型，大小，创建和修改日期等。

### 个人数据

个人身份信息，例如电子邮件地址，标识号或信用卡号。 ["了解有关个人数据的更多信息"](#)。

### 敏感的个人数据

GDPR 和其他隐私法规定的特殊类型的敏感信息，例如健康数据，种族或政治观点。 ["了解有关敏感个人数据的更多信息"](#)。

### 类别

Cloud Compliance 会获取所扫描的数据并将其划分为不同类型的类别。类别是基于 AI 对每个文件的内容和元数据的分析而得出的主题。 ["了解有关类别的更多信息"](#)。

### 名称实体识别

Cloud Compliance 使用 AI 从文档中提取自然人的姓名。 ["了解如何响应数据主体访问请求"](#)。

## 网络概述

Cloud Manager 会使用专用 IP 地址和安全组部署 Cloud Compliance 实例，以便从 Cloud Manager 启用入站

HTTP 连接。通过此连接，您可以从 Cloud Manager 界面访问 Cloud Compliance 信息板。

出站规则完全开放。此实例通过 Cloud Manager 的代理连接到 Cloud Volumes ONTAP 系统和 Internet。要升级 Cloud Compliance 软件并发送使用情况指标，需要访问 Internet。

如果您有严格的网络连接要求，"[了解 Cloud Compliance 所联系的端点](#)"。



索引数据永远不会离开 Cloud Compliance 实例—数据不会在虚拟网络外部中继，也不会发送到 Cloud Manager。

## 用户访问合规性信息

Cloud Manager 管理员可以查看所有工作环境的合规性信息。

Workspace 管理员只能查看其有权访问的系统的合规性信息。如果 Workspace 管理员无法访问 Cloud Manager 中的工作环境，则在合规性选项卡中看不到该工作环境的任何合规性信息。

"[了解有关 Cloud Manager 角色的更多信息](#)"。

# Cloud Volumes ONTAP 云合规性入门

完成几个步骤，开始在 AWS 或 Azure 中使用适用于 Cloud Volumes ONTAP 的云合规性。

## 快速入门

按照以下步骤快速入门，或者向下滚动到其余部分以了解完整详细信息。



### Verify that your configuration can meet the requirements

- 确保 Cloud Compliance 实例可以访问出站 Internet。

Cloud Manager 将实例部署在与请求中的第一个 Cloud Volumes ONTAP 系统相同的 VPC 或 vNet 中。

- 确保用户可以从直接连接到 AWS 或 Azure 的主机访问 Cloud Manager 界面，也可以从与 Cloud Compliance 实例位于同一网络中的主机（此实例将具有专用 IP 地址）访问 Cloud Manager 界面。
- 确保您可以使 Cloud Compliance 实例保持运行。



### Enable Cloud Compliance on Cloud Volumes ONTAP

- 新工作环境：在创建工作环境时，请确保始终启用 Cloud Compliance（默认情况下处于启用状态）。
- 现有工作环境：单击 \* 合规性 \*，也可以编辑工作环境列表，然后单击 \* 显示合规性信息板 \*。



### 确保能够访问卷

现在已启用 Cloud Compliance ，请确保它可以访问卷。

- 云合规性实例需要与每个 Cloud Volumes ONTAP 子网建立网络连接。
- Cloud Volumes ONTAP 的安全组必须允许来自云合规性实例的入站连接。
- NFS 卷导出策略必须允许从 Cloud Compliance 实例进行访问。
- Cloud Compliance 需要 Active Directory 凭据才能扫描 CIFS 卷。

单击 \* 合规性 \* > \* CIFS 扫描状态 \* > \* 编辑 CIFS 凭据 \* 并提供凭据。凭据可以是只读的，但提供管理员凭据可确保 Cloud Compliance 可以读取需要提升权限的数据。



#### Ensure connectivity between Cloud Manager and Cloud Compliance

- Cloud Manager 的安全组必须允许通过端口 80 与 Cloud Compliance 实例之间的入站和出站流量。
- 如果您的 AWS 网络不使用 NAT 或代理访问 Internet ，则 Cloud Manager 的安全组必须允许通过 TCP 端口 3128 从 Cloud Compliance 实例传输入站流量。

### 查看前提条件

在启用 Cloud Compliance 之前，请查看以下前提条件以确保您的配置受支持。启用 Cloud Compliance 后，您需要确保组件之间的连接。下面将介绍这些内容。

#### 启用出站 Internet 访问

云合规性要求出站 Internet 访问。如果您的虚拟网络使用代理服务器访问 Internet ，请确保 Cloud Compliance 实例可以通过出站 Internet 访问与以下端点联系：

端点	目的
<a href="https://cloudmanager.cloud.netapp.com">https://cloudmanager.cloud.netapp.com</a>	与 Cloud Manager 服务进行通信，其中包括 Cloud Central 帐户。
<a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a>	与 NetApp Cloud Central 进行通信以实现集中式用户身份验证。
<a href="https://cloud-compliance-support-netapp.s3.us-west-1.amazonaws.com">https://cloud-compliance-support-netapp.s3.us-west-1.amazonaws.com</a> <a href="https://hub.docker.com">https://hub.docker.com</a>	提供对软件映像、清单和模板的访问。
<a href="https://kinesis.us-east-1.amazonaws.com">https://kinesis.us-east-1.amazonaws.com</a>	使 NetApp 能够从审计记录流化数据。
<a href="https://cognito-idp.us-east-1.amazonaws.com">https://cognito-idp.us-east-1.amazonaws.com</a> <a href="https://cognito-identity.us-east-1.amazonaws.com">https://cognito-identity.us-east-1.amazonaws.com</a>	支持 Cloud Compliance 访问和下载清单和模板，以及发送日志和指标。

#### 验证 Web 浏览器与 Cloud Compliance 的连接

Cloud Compliance 实例使用专用 IP 地址来确保索引数据无法通过 Internet 访问。因此，用于访问 Cloud Manager 的 Web 浏览器必须连接到该专用 IP 地址。此连接可以来自与 AWS 或 Azure 的直接连接（例如 VPN ），也可以来自与 Cloud Compliance 实例位于同一网络中的主机。



如果您要从公有 IP 地址访问 Cloud Manager，则您的 Web 浏览器可能未在网络中的主机上运行。

## 保持云合规性正常运行

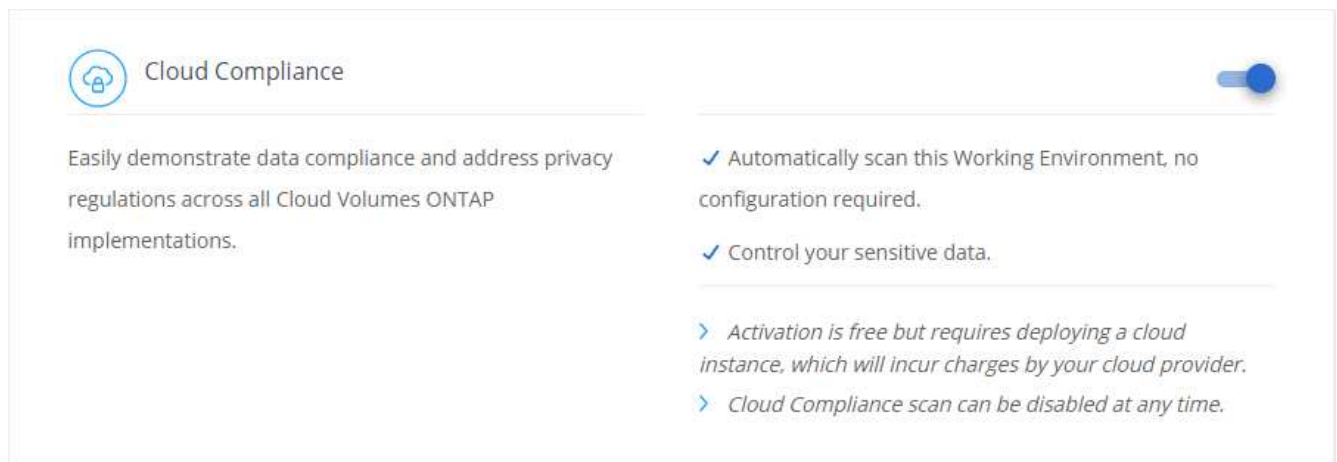
云合规性实例需要保持运行状态，才能持续扫描数据。

## 在新的工作环境中实现云合规性

默认情况下，工作环境向导会启用 Cloud Compliance。请务必保持此选项处于启用状态。

### 步骤

1. 单击 \* 创建 Cloud Volumes ONTAP \*。
2. 选择 Amazon Web Services 或 Microsoft Azure 作为云提供商，然后选择单个节点或 HA 系统。
3. 填写详细信息和凭据页面。
4. 在服务页面上，保持 Cloud Compliance 处于启用状态，然后单击 \* 继续 \*。



5. 完成向导中的页面以部署系统。

有关帮助，请参见 ["在 AWS 中启动 Cloud Volumes ONTAP"](#) 和 ["在 Azure 中启动 Cloud Volumes ONTAP"](#)。

### 结果

已在 Cloud Volumes ONTAP 系统上启用云合规性。如果这是您首次启用 Cloud Compliance，Cloud Manager 会在您的云提供商中部署 Cloud Compliance 实例。一旦实例可用，它就会在将数据写入您创建的每个卷时开始扫描数据。

## 在现有工作环境中实现云合规性

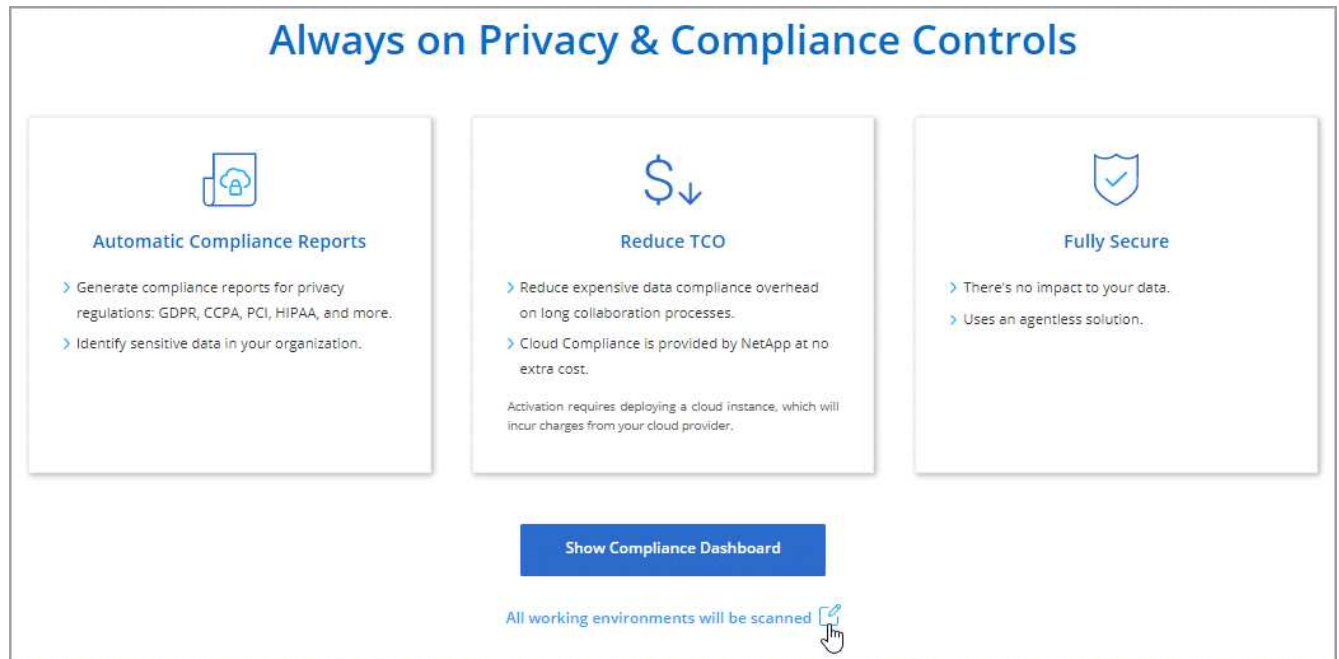
从 Cloud Manager 的 \* 合规性 \* 选项卡在现有 Cloud Volumes ONTAP 系统上启用云合规性。

另一个选项是，通过分别选择每个工作环境，从 \* 工作环境 \* 选项卡中启用 Cloud Compliance。除非您只有一个系统，否则完成此操作需要较长时间。

### 适用于多个工作环境的步骤

1. 在 Cloud Manager 顶部，单击 \* 合规性 \*。
2. 如果要在特定工作环境中启用 Cloud Compliance，请单击编辑图标。

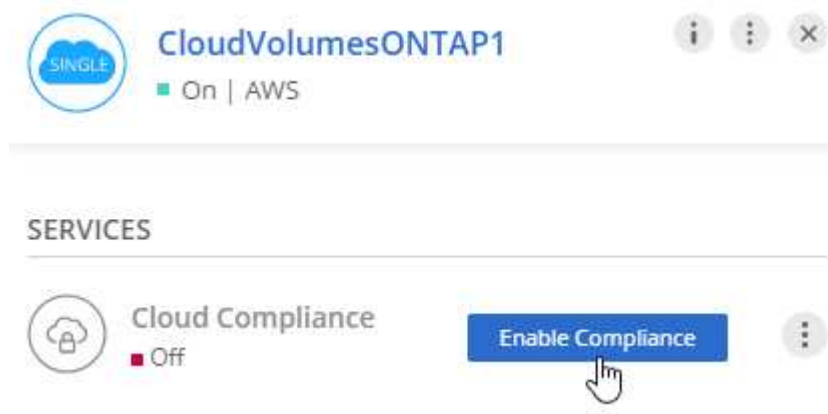
否则，Cloud Manager 将设置为在您有权访问的所有工作环境中启用 Cloud Compliance。



3. 单击 \* 显示合规性信息板 \*。

适用于单个工作环境的步骤

1. 在 Cloud Manager 顶部，单击 \* 工作环境 \*。
2. 选择工作环境。
3. 在右侧窗格中，单击 \* 启用合规性 \*。



结果

如果这是您首次启用 Cloud Compliance，Cloud Manager 会在您的云提供商中部署 Cloud Compliance 实例。

Cloud Compliance 开始扫描每个工作环境中的数据。一旦 Cloud Compliance 完成初始扫描，合规性信息板中就会显示数据。所需时间取决于数据量—可能需要几分钟或几小时。

## 验证 Cloud Compliance 是否有权访问卷

通过检查网络，安全组和导出策略，确保云合规性可以访问 Cloud Volumes ONTAP 上的卷。您需要为 Cloud Compliance 提供 CIFS 凭据，以便它可以访问 CIFS 卷。

### 步骤

1. 确保云合规性实例与每个 Cloud Volumes ONTAP 子网之间存在网络连接。

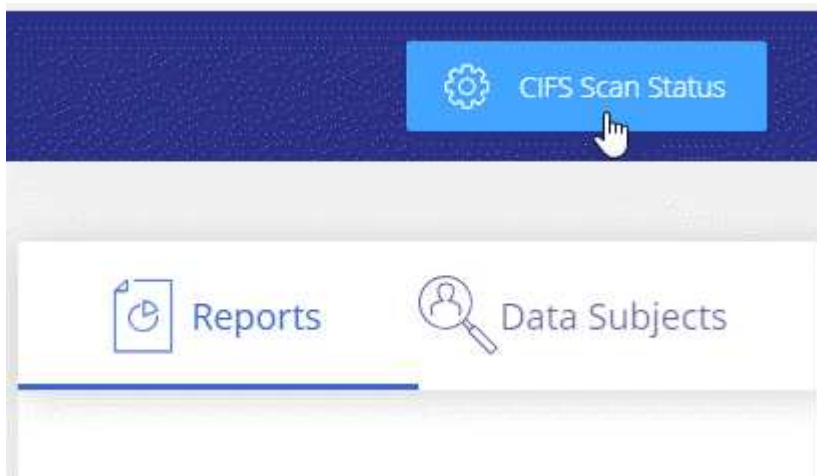
Cloud Manager 将云合规性实例部署在与请求中的第一个 Cloud Volumes ONTAP 系统相同的 VPC 或 vNet 中。因此，如果某些 Cloud Volumes ONTAP 系统位于不同的子网或虚拟网络中，则此步骤非常重要。

2. 确保 Cloud Volumes ONTAP 的安全组允许来自云合规性实例的入站流量。

您可以从 Cloud Compliance 实例的 IP 地址打开流量安全组，也可以从虚拟网络内部打开所有流量的安全组。

3. 确保 NFS 卷导出策略包含 Cloud Compliance 实例的 IP 地址，以便它可以访问每个卷上的数据。
4. 如果您使用 CIFS，请为 Cloud Compliance 提供 Active Directory 凭据，以便它可以扫描 CIFS 卷。

- a. 在 Cloud Manager 顶部，单击 \* 合规性 \*。
- b. 在右上角，单击 \* CIFS 扫描状态 \*。



- c. 对于每个 Cloud Volumes ONTAP 系统，单击 \* 编辑 CIFS 凭据 \*，然后输入 Cloud Compliance 访问系统上的 CIFS 卷所需的用户名和密码。

凭据可以是只读的，但提供管理员凭据可确保 Cloud Compliance 可以读取任何需要提升权限的数据。这些凭据存储在 Cloud Compliance 实例上。

输入凭据后，您应看到一条消息，指出所有 CIFS 卷均已成功通过身份验证。





## 验证 Cloud Manager 是否可以访问 Cloud Compliance

确保 Cloud Manager 与 Cloud Compliance 之间的连接，以便您可以查看 Cloud Compliance 发现的合规性洞察。

### 步骤

1. 请确保 Cloud Manager 的安全组允许通过端口 80 传入和传出云合规性实例的流量。

通过此连接，您可以在合规性选项卡中查看信息。

2. 如果 AWS 网络不使用 NAT 或代理访问 Internet，请修改 Cloud Manager 的安全组，以允许通过 TCP 端口 3128 从 Cloud Compliance 实例传输入站流量。

这是必需的，因为 Cloud Compliance 实例使用 Cloud Manager 作为代理访问 Internet。



默认情况下，此端口在所有新的 Cloud Manager 实例上处于打开状态，从 3.1.5 版开始。它不会在该版本之前创建的 Cloud Manager 实例上打开。

## 获得私有数据的可见性和控制权

通过查看有关组织中个人数据和敏感个人数据的详细信息来控制您的私有数据。您还可以查看数据中的 Cloud Compliance 类别和文件类型来获得可见性。

### 个人数据

Cloud Compliance 会自动识别数据中的特定字词，字符串和模式（Reex）。例如，个人身份信息（"Personal Identification"，Pi2），信用卡号，社会保险号，银行帐号等。 [请参见完整列表](#)。

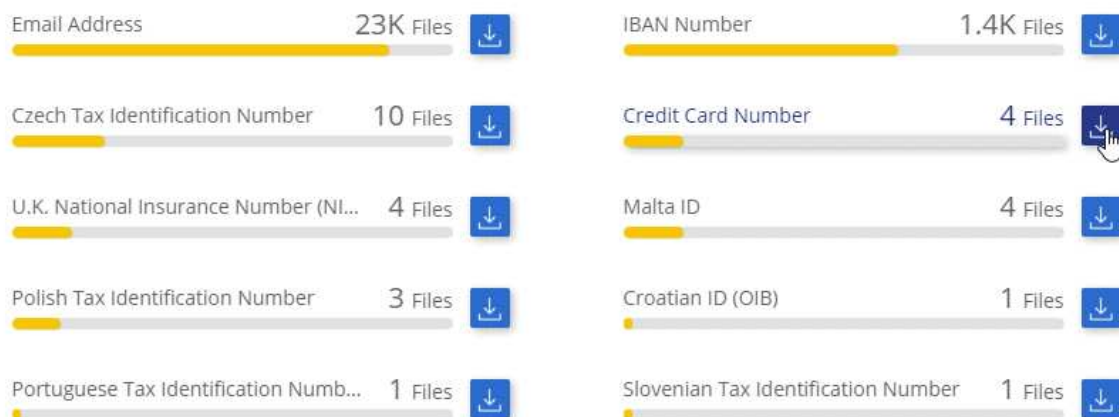
对于某些类型的个人数据，Cloud Compliance 会使用 *proximity validation* 来验证其结果。通过查找与所发现的个人数据相邻的一个或多个预定义关键字来进行验证。例如，Cloud Compliance 会标识一个美国如果在 SSN 旁边看到一个接近词，则将社会安全号（SSN）作为 SSN，例如 `_SSN` 或 `_社交 安全_`。 [以下列表](#) 显示 Cloud Compliance 何时使用接近验证。

### 查看包含个人数据的文件

#### 步骤

1. 在 Cloud Manager 顶部，单击 \* 合规性 \*。
2. 直接从主屏幕下载前 2 种文件类型之一的详细信息，或者单击 \* 查看全部 \*，然后下载找到的任何个人数据类型的列表。

## 12 Types | 23K Files



### 个人数据的类型

文件中的个人数据可以是常规个人数据或国家标识符。第三列确定 Cloud Compliance 是否使用 [接近验证](#) 以验证其对标识符的发现。

Type	标识符	是否进行接近验证?
常规	电子邮件地址	否
	信用卡号	否
	IBAN 编号 (国际银行帐号)	否
	IP 地址	是的。

Type	标识符	是否进行接近验证?
国家标识符	比利时 ID ( Numero National )	是的。
	Bulgarian" ID ( 统一民号 )	是的。
	塞浦路斯税务识别号 ( TIC )	是的。
	丹麦税务识别号 ( CPR )	是的。
	爱沙尼亚语 ID ( Isikukood )	是的。
	芬兰语 ID ( henkilötunnus )	是的。
	法国税务识别号 ( SPI )	是的。
	德国税务识别号 ( Steuerliche Identifikationsnummer )	是的。
	匈牙利税务识别号 ( Adóazonosító jel )	是的。
	爱尔兰 ID ( PPs )	是的。
	以色列 ID	是的。
	意大利语 ID ( Codice Fiscale )	是的。
	Latvian Tax Identification" 编号	是的。
	Lithuanian ID ( Asmens kodas )	是的。
	卢森堡 ID	是的。
	马耳他 ID	是的。
	荷兰 ID ( BSN )	是的。
	波兰税务标识号	是的。
	葡萄牙税务识别号 ( NIF )	是的。
	罗马尼亚税务标识号	是的。
	斯洛伐克税务标识号	是的。
	斯洛文尼亚税务识别号	是的。
	南非 ID	是的。
	西班牙语税务标识号	是的。
	瑞典税务标识号	是的。
	英国国家保险号 ( Nino )	是的。
美国社会保险号 ( SSN )	是的。	

## 敏感的个人数据

Cloud Compliance 会根据隐私法规的定义自动识别特殊类型的敏感个人信息，例如 "《一般数据保护条例》第 9 条和第 10 条"。例如，有关个人健康，种族或性取向的信息。 [请参见完整列表。](#)

Cloud Compliance 使用人工智能 ( AI ) ，自然语言处理 ( NLP ) ，机器学习 ( ML ) 和认知计算 ( CC ) 来了解其扫描内容的含义，以便提取实体并对其进行相应的分类。

例如，一个敏感的 GDPR 数据类别是种族起源。由于其 NLP 功能，Cloud Compliance 可以区分 "George is Convency"（表示《一般数据保护条例》第 9 条中指定的敏感数据）与 "George is eating Mexican f尽" 这两种句子之间的区别。



扫描敏感个人数据时，仅支持英语。稍后将添加对更多语言的支持。

查看包含敏感个人数据的文件

步骤

1. 在 Cloud Manager 顶部，单击 \* 合规性 \*。
2. 直接从主屏幕下载前 2 种文件类型之一的详细信息，或者单击 \* 查看全部 \*，然后下载找到的任何敏感个人数据类型的列表。

### Sensitive Personal Files

6 Types | 26K Files



### 敏感个人数据的类型

Cloud Compliance 可在文件中找到的敏感个人数据包括：

#### 《刑事诉讼参考》

有关自然人的犯罪和犯罪的数据。

#### 《种族参考》

与自然人的种族或种族有关的数据。

#### 运行状况参考

有关自然人健康的数据。

#### 《理念参考》

与自然人的理念相关的数据。

#### 《宗教信仰参考》

有关自然人的宗教信仰的数据。

#### 性寿命或方向参考

有关自然人的性生活或性取向的数据。

## 类别

Cloud Compliance 会获取所扫描的数据并将其划分为不同类型的类别。类别是基于 AI 对每个文件的内容和元数据的分析而得出的主题。 [查看类别列表](#)。

类别可以通过向您显示所拥有的信息类型来帮助您了解数据的变化。例如，恢复或员工合同等类别可以包含敏感数据。下载 CSV 报告时，您可能会发现员工合同存储在不安全的位置。然后，您可以更正此问题描述。



类别仅支持英语。稍后将添加对更多语言的支持。

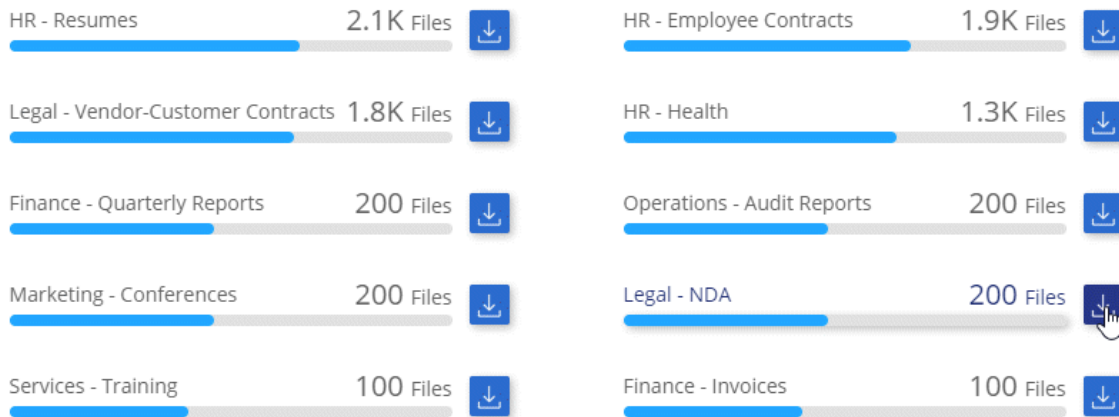
### 按类别查看文件

#### 步骤

1. 在 Cloud Manager 顶部，单击 \* 合规性 \*。
2. 直接从主屏幕下载前 4 种文件类型之一的详细信息，或者单击 \* 全部查看 \*，然后下载任意类别的列表。

#### Categories

27 Categories | 127.3K Files



### 类别类型

Cloud Compliance 会按如下方式对您的数据进行分类：

#### 财务

- 资产负债表
- 采购订单
- 发票
- 季度报告

#### 人力资源

- 后台检查
- 薪酬计划

- 员工合同
- 员工审核
- 运行状况
- 恢复

#### 法律

- NDA
- 供应商 - 客户合同

#### 营销

- 营销活动
- 会议

#### 操作

- 审核报告

#### 销售

- 销售订单

#### 服务

- RFI
- RFP
- 培训

#### 支持

- 投诉和服务单

#### 其他

- 归档文件
- 音频
- CAD 文件
- 代码
- 可执行文件
- 映像

## 文件类型

Cloud Compliance 会获取所扫描的数据，并按文件类型对其进行细分。Cloud Compliance 可以显示扫描中发现的所有文件类型。

查看文件类型有助于控制敏感数据，因为您可能会发现某些文件类型存储不正确。例如，您可能存储的 CAD 文件包含有关您的组织的非常敏感的信息。如果这些文件不安全，您可以通过限制权限或将文件移动到其他位置来控制敏感数据。

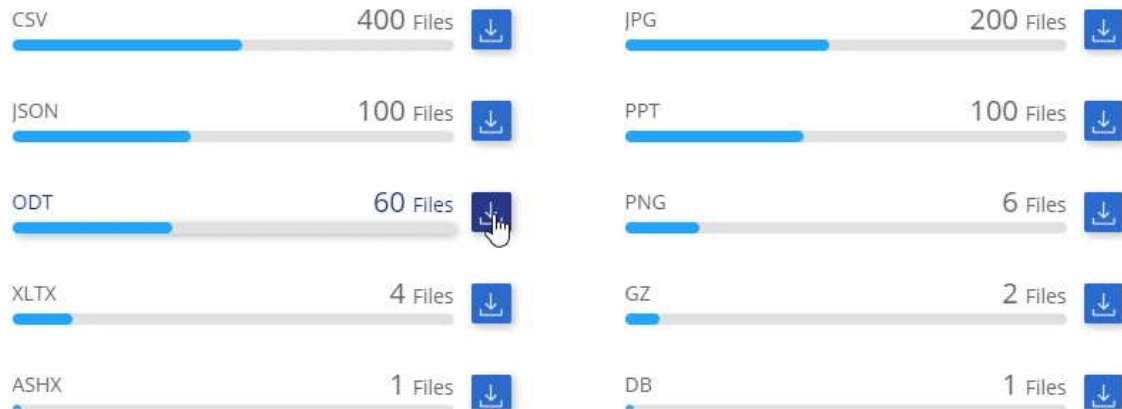
## 查看文件类型

### 步骤

1. 在 Cloud Manager 顶部，单击 \* 合规性 \*。
2. 直接从主屏幕下载前 4 种文件类型之一的详细信息，或者单击 \* 查看全部 \*，然后下载任意文件类型的列表。

### File Types

19 File Types | 127.3K Files



## 发现的信息准确性

NetApp 无法保证 Cloud Compliance 所识别的个人数据和敏感个人数据的 100% 准确性。您应始终通过查看数据来验证此信息。

根据我们的测试，下表显示了 Cloud Compliance 发现的信息的准确性。我们将其细分为 *precision* 和 *recall*：

### 精确度

正确识别 Cloud Compliance 的可能性。例如，个人数据的精确率为 90% 意味着，在被确定包含个人信息的 10 个文件中，有 9 个文件实际上包含个人信息。每 10 个文件中就有 1 个是误报文件。

### 重新调用

云合规性找到所需内容的可能性。例如，个人数据的重新调用率为 70%，这意味着 Cloud Compliance 可以识别贵组织中实际包含个人信息的 10 个文件中的 7 个文件。Cloud Compliance 会丢失 30% 的数据，并且不会显示在信息板中。

Cloud Compliance 采用受控可用性版本，我们会不断提高结果的准确性。这些改进功能将在未来的 Cloud Compliance 版本中自动提供。

Type	精确度	重新调用
个人数据—常规	90% 到 95%	60%-80%
个人数据—国家 / 地区标识符	30% 到 60%	40%-60%

Type	精确度	重新调用
敏感的个人数据	80%-95%	20%-30%
类别	90% 到 97%	60%-80%

## 每个文件列表报告中包含的内容（CSV 文件）

通过信息板，您可以下载包含已标识文件详细信息的数据列表（CSV 格式）。如果结果超过 10,000 个，则列表中仅显示排名前 10,000 位的结果（稍后将添加对更多结果的支持）。

每个文件列表包含以下信息：

- 文件名
- 位置类型
- 位置
- 文件路径
- 文件类型
- 类别
- 个人信息
- 敏感的个人数据
- 删除检测日期

删除检测日期用于标识文件被删除或移动的日期。这样，您就可以确定何时移动了敏感文件。已删除的文件不属于信息板中显示的文件编号。这些文件仅显示在 CSV 报告中。

## 查看隐私风险评估报告

根据 GDPR 和 CCPA 等隐私法规的要求，隐私风险评估报告概述了贵组织的隐私风险状态。



NetApp 无法保证 Cloud Compliance 所识别的个人数据和敏感个人数据的 100% 准确性。您应始终通过查看数据来验证此信息。

此报告包含以下信息：

### 合规状态

严重性得分（有关详细信息，请参见下文）以及数据分布，无论数据是非敏感数据，个人数据还是敏感数据。

### 评估概述

所发现的个人数据类型以及数据类别的细分。

### 此评估中的数据主题

按地点列出的发现了国家标识符的人数。

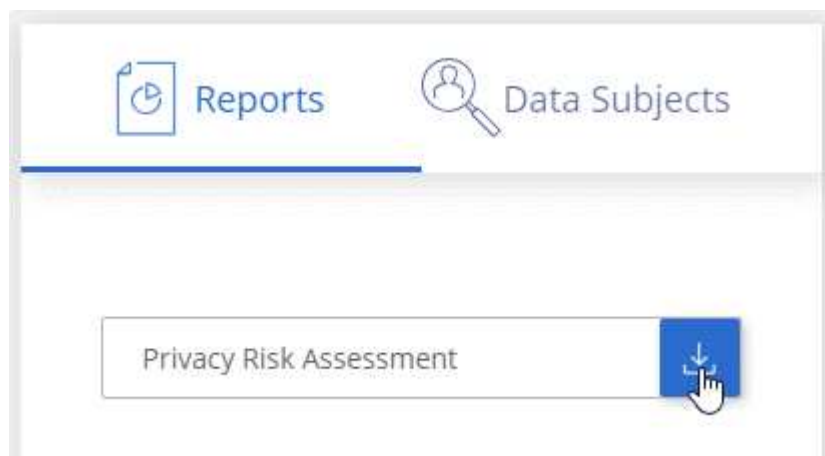


## 生成隐私风险评估报告

转到合规性选项卡以生成报告。

### 步骤

1. 在 Cloud Manager 顶部，单击 \* 合规性 \*。
2. 在 \* 报告 \* 下，单击 \* 隐私风险评估 \* 旁边的下载图标。



### 结果

Cloud Compliance 会生成 PDF 报告，您可以根据需要查看该报告并将其发送给其他组。

## 严重性得分

Cloud Compliance 会根据以下三个变量计算隐私风险评估报告的严重性得分：

- 个人数据在所有数据中所占的百分比。
- 敏感个人数据在所有数据中所占的百分比。
- 包含数据主体的文件百分比，由国家 ID，社会保障号和税务 ID 号等国家标识符确定。

用于确定得分的逻辑如下：

严重性得分	逻辑
0	所有这三个变量都恰好为 0%
1.	其中一个变量大于 0%
2.	其中一个变量大于 3%
3.	其中两个变量大于 3%
4.	其中三个变量大于 3%
5.	其中一个变量大于 6%
6.	其中两个变量大于 6%
7.	其中三个变量大于 6%

严重性得分	逻辑
8.	其中一个变量大于 15%
9	其中两个变量大于 15%
10	其中三个变量大于 15%

## 响应数据主体访问请求

通过搜索主题的全名或已知标识符（例如电子邮件地址）并下载报告来响应数据主体访问请求（Data Subject Access Request，DAR）。本报告旨在帮助贵组织满足 GDPR 或类似数据隐私法律的要求。



NetApp 无法保证 Cloud Compliance 所识别的个人数据和敏感个人数据的 100% 准确性。您应始终通过查看数据来验证此信息。

### 什么是数据主体访问请求？

欧洲 GDPR 等隐私法规授予数据主体（如客户或员工）访问其个人数据的权利。当数据主体请求此信息时，此信息称为 DSAar（数据主体访问请求）。组织必须“无不当延迟”地对这些请求做出响应，并且最迟在收到请求后一个月内做出响应。

### 云合规性如何帮助您应对 DAR？

执行数据主题搜索时，Cloud Compliance 会查找包含此人的名称或标识符的所有文件。Cloud Compliance 会检查最新的预索引数据中的名称或标识符。它不会启动新扫描。

搜索完成后，您可以下载文件列表或数据主体访问请求报告。该报告汇总了数据中的洞察信息，并将其纳入法律条款中，您可以将其发回给相关人员。

### 搜索数据主题并下载报告

搜索数据主体的全名或已知标识符，然后下载文件列表报告或 DSAL 报告。您可以搜索依据“[任何个人信息类型](#)”。

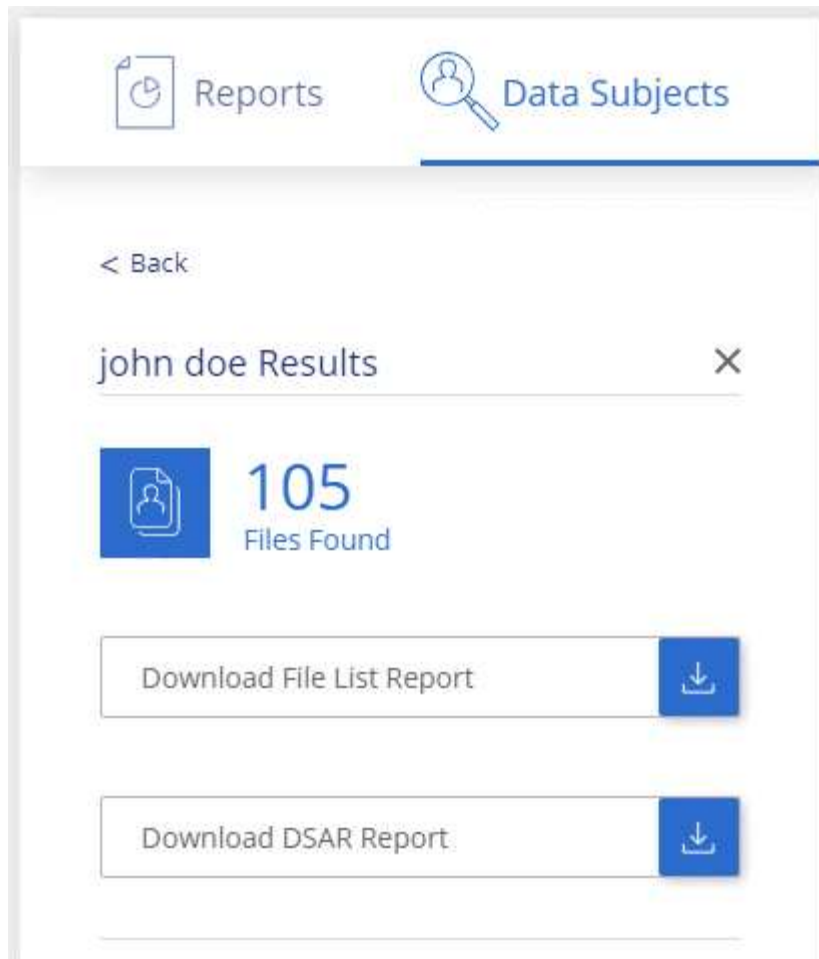


搜索数据主题的名称时，仅支持英语。稍后将添加对更多语言的支持。

#### 步骤

1. 在 Cloud Manager 顶部，单击 \* 合规性 \*。
2. 单击 \* 数据主题 \*。
3. 搜索数据主体的全名或已知标识符。

以下示例显示了对名称 *john doe* 的搜索：



#### 4. 选择一个可用选项：

- \* 下载文件列表报告 \*：包含数据主题相关信息的文件列表。



如果结果超过 10,000 个，则报告中仅显示排名前 10,000 位的结果（稍后将添加对更多结果的支持）。

- \* 下载 DSAI 报告 \*：对访问请求的正式响应，您可以将此响应发送给数据主体。此报告包含根据 Cloud Compliance 在数据主题上找到的数据自动生成的信息，该信息可用作模板。您应填写此表单并在内部进行审核，然后再将其发送给数据主体。

## 禁用 Cloud Compliance

如果需要，您可以阻止 Cloud Compliance 扫描一个或多个工作环境。如果您不再希望对 Cloud Volumes ONTAP 系统使用云合规，也可以删除云合规实例。

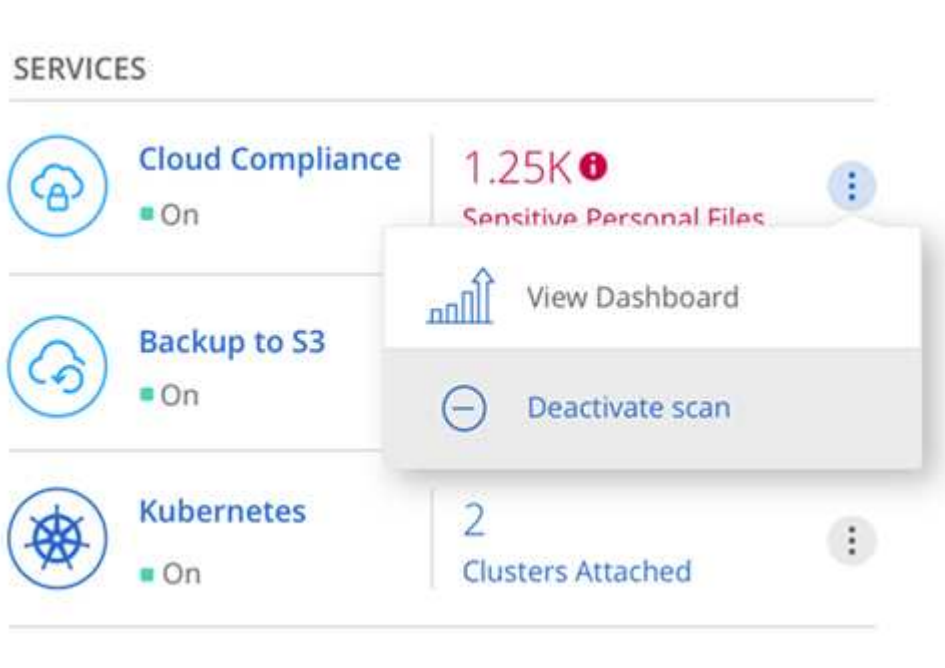
### 为工作环境停用合规性扫描

停用扫描后，Cloud Compliance 将不再扫描系统上的数据，并从 Cloud Compliance 实例中删除索引的合规性洞察（不会删除工作环境本身的数据）。

#### 步骤

1. 在 Cloud Manager 顶部，单击 \* 工作环境 \*。

2. 选择工作环境。
3. 在右侧面板中，单击 Cloud Compliance 服务的操作图标，然后选择 \* 停用扫描 \*。



## 正在删除 Cloud Compliance 实例

如果您不再希望将云合规性与 Cloud Volumes ONTAP 结合使用，则可以删除云合规性实例。删除此实例还会删除索引数据所在的关联磁盘。

### 步骤

1. 转到云提供商的控制台并删除 Cloud Compliance 实例。

此实例名为 *CloudCompliance*，并与生成的哈希（UUID）串联在一起。例如：*CloudCompliance" — 16bb6564-38AD-4080-9a92 — 36f5fd2f71c7*

## 有关云合规性的常见问题解答

如果您只是在寻找一个问题的快速答案，此常见问题解答将会有所帮助。

### 什么是云合规性？

Cloud Compliance 是一款全新的 NetApp 云产品。借助人工智能（AI）驱动的技术，云合规性可帮助企业了解数据环境，并识别 AWS 或 Azure 中托管的 Cloud Volumes ONTAP 系统中的敏感数据。

云合规性提供了预定义参数（例如敏感信息类型和类别），用于满足有关数据隐私和敏感度的新数据合规性法规，例如 GDPR，CCPA 等。

### 为什么要使用 Cloud Compliance？

云合规性可以为您提供数据，帮助您：

- 遵守数据合规性和隐私法规。
- 遵守数据保留策略。
- 根据 GDPR ， CCPA 和其他数据隐私法规的要求，轻松找到并报告特定数据以响应数据主题。

## Cloud Compliance 的常见用例有哪些？

- 识别个人信息（PII）。
- 根据 GDPR 和 CCPA 隐私法规的要求确定广泛的敏感信息。
- 遵守新的和即将出台的数据隐私法规。

["了解有关 Cloud Compliance 用例的更多信息"](#)。

## 可以使用 Cloud Compliance 扫描哪些类型的数据？

Cloud Compliance 支持通过 NFS 和 CIFS 协议扫描非结构化数据。目前，云合规性会扫描由 Cloud Volumes ONTAP 管理的数据。

["了解扫描的工作原理"](#)。

## 支持哪些云提供商？

Cloud Compliance 作为 Cloud Manager 的一部分运行，目前支持 AWS 和 Azure 。这样，您的组织就可以在不同的云提供商之间实现统一的隐私可见性。不久将增加对 Google Cloud Platform （GCP）的支持。

## 如何访问 Cloud Compliance ？

Cloud Compliance 通过 Cloud Manager 进行操作和管理。您可以从 Cloud Manager 中的 \* 合规性 \* 选项卡访问云合规性功能。

## 云合规性的工作原理是什么？

云合规部除了部署 Cloud Manager 系统和 Cloud Volumes ONTAP 实例之外，还部署了另一层人工智能。然后，它会扫描 Cloud Volumes ONTAP 上的数据，并为找到的数据洞察力编制索引。

["详细了解 Cloud Compliance 的工作原理"](#)。

## 云合规性的成本是多少？

云合规性作为 Cloud Volumes ONTAP 的一部分提供，不需要任何额外成本。将来，自定义功能可能需要额外成本。



Cloud Compliance 要求在云提供商中部署一个实例，您的云提供商将为此实例付费。

## Cloud Compliance 扫描我的数据的频率如何？

数据经常更改，因此 Cloud Compliance 会持续扫描您的数据，而不会影响您的数据。虽然数据的初始扫描可能需要较长时间，但后续扫描只会扫描增量更改，从而缩短系统扫描时间。

["了解扫描的工作原理"](#)。

## Cloud Compliance 是否提供报告？

是的。Cloud Compliance 提供的信息可能与您组织中的其他利益相关方相关，因此我们可以帮助您生成报告以分享这些见解。

以下报告可用于 Cloud Compliance：

### 隐私风险评估报告

根据您的数据提供隐私洞察力并获得隐私风险得分。 ["了解更多信息。"](#)

### 数据主体访问请求报告

用于提取包含数据主体的特定名称或个人标识符相关信息的所有文件的报告。 ["了解更多信息。"](#)

### 报告特定信息类型

我们提供的报告包含有关包含个人数据和敏感个人数据的已识别文件的详细信息。您还可以查看按类别和文件类型细分的文件。 ["了解更多信息。"](#)

## 要实现云合规性，需要哪种类型的实例或虚拟机？

- 在 Azure 中，Cloud Compliance 在具有 512 GB 磁盘的 Standard\_d16s\_v3 VM 上运行。
- 在 AWS 中，Cloud Compliance 在具有 500 GB IO1 磁盘的 m5.4xlarge 实例上运行。

在 m5.4xlarge 不可用的区域中，Cloud Compliance 会在 m4.4xlarge 实例上运行。

["详细了解 Cloud Compliance 的工作原理"](#)。

## 扫描性能是否有所不同？

扫描性能可能因网络带宽和云环境中的平均文件大小而异。

## 如何启用云合规性？

您可以在创建新的工作环境时启用 Cloud Compliance。您可以从 \* 合规性 \* 选项卡（仅限首次激活时）或通过选择特定的工作环境在现有工作环境中启用它。

["了解如何开始使用"](#)。



激活 Cloud Compliance 会立即执行初始扫描。之后不久将显示合规性结果。

## 如何禁用 Cloud Compliance？

选择单个工作环境后，您可以从 " 工作环境 " 页面禁用 Cloud Compliance。

["了解更多信息。"](#)



要完全删除 Cloud Compliance 实例，您可以从云提供商的门户手动删除 Cloud Compliance 实例。

## 如果在 **Cloud Volumes ONTAP** 上启用了数据分层，会发生什么情况？

您可能希望在 Cloud Volumes ONTAP 系统上启用云合规性，以便将冷数据分层到对象存储。如果启用了数据分层，则 Cloud Compliance 会扫描所有数据—磁盘上的数据以及分层到对象存储的冷数据。

合规性扫描不会加热冷数据，它会保持冷数据并分层到对象存储。

## 是否可以使用云合规性扫描内部 **ONTAP** 存储？

否Cloud Compliance 目前作为 Cloud Manager 的一部分提供，并支持 Cloud Volumes ONTAP。我们计划通过 Cloud Volumes Service 和 Azure NetApp Files 等其他云产品支持云合规性。

## **Cloud Compliance** 是否可以向我的组织发送通知？

不可以，但您可以下载状态报告，这些报告可以在组织内部共享。

## 我是否可以根据组织的需求自定义服务？

Cloud Compliance 提供对数据的即装即用洞察力。您可以根据组织的需求提取和利用这些洞察信息。

## 我是否可以将云合规性信息限制为特定用户？

是的，Cloud Compliance 与 Cloud Manager 完全集成。Cloud Manager 用户只能根据其工作空间权限查看其有资格查看的工作环境的信息。

["了解更多信息。"](#)

# 管理 Cloud Volumes ONTAP

## 连接到 Cloud Volumes ONTAP

如果您需要对 Cloud Volumes ONTAP 执行高级管理、则可以使用 OnCommand System Manager 或命令行界面执行此操作。

### 正在连接到 OnCommand System Manager

您可能需要从 OnCommand System Manager 执行一些 Cloud Volumes ONTAP 任务、这是一个基于浏览器的管理工具、运行在 Cloud Volumes ONTAP 系统上。例如，如果要创建 LUN，则需要使用 System Manager。

开始之前

要访问 Cloud Manager 的计算机必须与 Cloud Volumes ONTAP 建立网络连接。例如，您可能需要从 AWS 或 Azure 中的跳转主机登录到 Cloud Manager。



在多个 AWS 可用性区域中部署时、Cloud Volumes ONTAP HA 配置将浮动 IP 地址用于集群管理界面、这意味着外部路由不可用。您必须从属于同一路由域的主机进行连接。

步骤

1. 在“工作环境”页面中，双击要使用 System Manager 管理的 Cloud Volumes ONTAP 系统。
2. 单击菜单图标，然后单击 \* 高级 > 系统管理器 \*。
3. 单击 \* 启动 \*。

System Manager 将在新的浏览器选项卡中加载。

4. 在登录屏幕的 "User Name" 字段中输入 \* 管理 \*，输入创建工作环境时指定的密码，然后单击 \* 登录 \*。

结果

系统管理器控制台即会加载。您现在可以使用它来管理 Cloud Volumes ONTAP。

### 连接到 Cloud Volumes ONTAP CLI

Cloud Volumes ONTAP CLI 使您可以执行所有管理命令、并且是执行高级任务或使用 CLI 更舒适的理想选择。您可以使用 Secure Shell (SSH) 连接到 CLI。

开始之前

使用 SSH 连接到 Cloud Volumes ONTAP 的主机必须与 Cloud Volumes ONTAP 建立网络连接。例如，您可能需要从 AWS 或 Azure 中的跳转主机使用 SSH。



当部署在多个 Azs 中时、Cloud Volumes ONTAP HA 配置将浮动 IP 地址用于集群管理界面、这意味着外部路由不可用。您必须从属于同一路由域的主机进行连接。

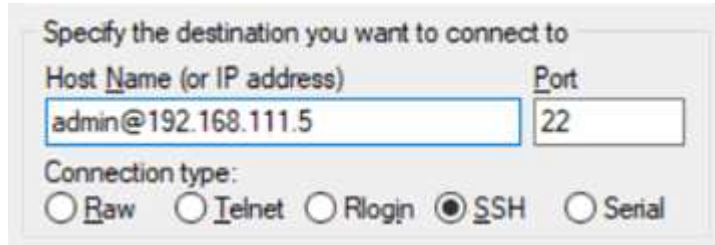
步骤

1. 在 Cloud Manager 中，确定集群管理界面的 IP 地址：
  - a. 在“工作环境”页面上，选择 Cloud Volumes ONTAP 系统。



- b. 复制右窗格中显示的集群管理 IP 地址。
2. 使用 SSH 使用管理员帐户连接到集群管理接口 IP 地址。
    - 示例 \*

下图显示了使用 PuTTY 的示例：



3. 在登录提示符处，输入管理员帐户的密码。
  - 示例 \*

```
Password: *****  
COT2::>
```

## 更新 Cloud Volumes ONTAP 软件

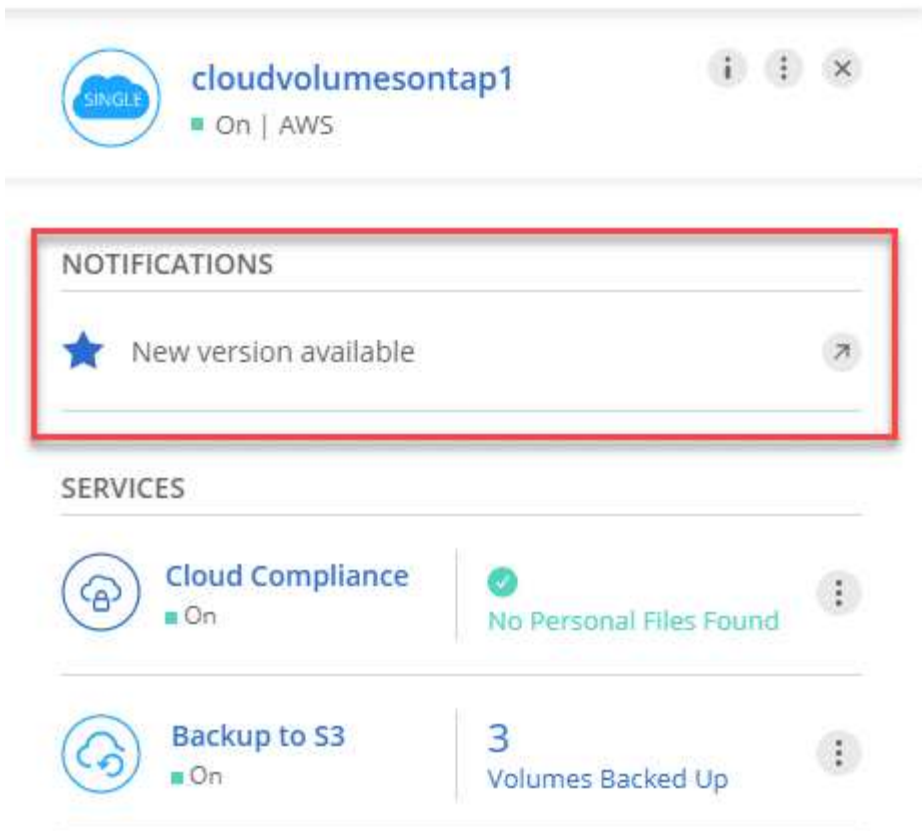
Cloud Manager 包括多个选项、您可以使用这些选项升级到当前的 Cloud Volumes ONTAP 版本或将 Cloud Volumes ONTAP 降级到早期版本。您应该在升级或降级软件之前准备 Cloud Volumes ONTAP 系统。

### 软件更新必须由 **Cloud Manager** 完成

Cloud Volumes ONTAP 升级必须从 Cloud Manager 完成。您不应使用 System Manager 或命令行界面升级 Cloud Volumes ONTAP 。这样做可能会影响系统稳定性。

### 更新 **Cloud Volumes ONTAP** 的方法

当推出新版本的 Cloud Volumes ONTAP 时，Cloud Manager 会在 Cloud Volumes ONTAP 工作环境中显示通知：



您可以从此通知开始升级过程、通过从 S3 存储区获取软件映像、安装映像、然后重新启动系统来自动执行该过程。有关详细信息，请参见 [从 Cloud Manager 升级 Cloud Volumes ONTAP 通知](#)。



对于 AWS 中的 HA 系统，Cloud Manager 可能会在升级过程中升级 HA 调解器。

### 软件更新的高级选项

Cloud Manager 还提供以下高级选项来更新 Cloud Volumes ONTAP 软件：

- 使用外部 URL 上的图像进行软件更新

如果 Cloud Manager 无法访问 S3 Bucket 来升级软件、是否提供了修补程序、或者您希望将软件降级为特定版本、则此选项非常有用。

有关详细信息，请参见 [使用 HTTP 或 FTP 服务器升级或降级 Cloud Volumes ONTAP](#)。

- 使用系统上的备用映像进行软件更新

您可以使用此选项通过将备用软件映像设置为默认映像来降级到以前的版本。此选项不适用于 HA 对。

有关详细信息，请参见 [使用本地映像降级 Cloud Volumes ONTAP](#)。

## 准备更新 Cloud Volumes ONTAP 软件

在执行升级或降级之前，您必须验证系统是否已准备就绪并进行必要的配置更改。

- [\[规划停机时间\]](#)
- [\[查看版本要求\]](#)
- [\[验证是否仍启用自动交还\]](#)
- [暂停 SnapMirror 传输](#)
- [\[验证聚合是否联机\]](#)

### 规划停机时间

升级单节点系统时，升级过程会使系统脱机长达 25 分钟，在此期间 I/O 会中断。

升级 HA 对无中断，I/O 不会中断。在此无中断升级过程中，每个节点会同时进行升级，以继续为客户端提供 I/O。

### 查看版本要求

您可以升级或降级到的 ONTAP 版本因系统上当前运行的 ONTAP 版本而异。

要了解版本要求，请参见 ["ONTAP 9 文档：集群更新要求"](#)。

### 验证是否仍启用自动交还

必须在 Cloud Volumes ONTAP HA 对上启用自动交还（这是默认设置）。否则，操作将失败。

["ONTAP 9 文档：用于配置自动交还的命令"](#)

### 暂停 SnapMirror 传输

如果 Cloud Volumes ONTAP 系统具有活动的 SnapMirror 关系、最好在更新 Cloud Volumes ONTAP 软件之前暂停传输。暂停传输可防止 SnapMirror 故障。您必须暂停从目标系统进行的传输。

### 关于此任务

这些步骤介绍了如何将 System Manager 用于版本 9.3 和更高版本。

### 步骤

1. ["登录到系统管理器。"](#) 从目标系统。
2. 单击 \* 保护 > 关系 \*。
3. 选择关系，然后单击 \* 操作 > 暂停 \*。

### 验证聚合是否联机

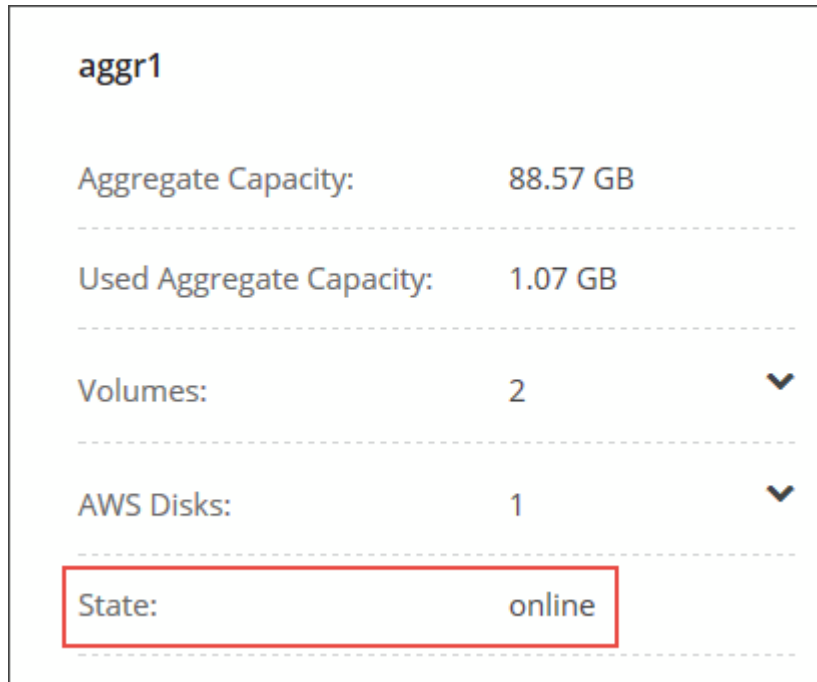
在更新软件之前，Cloud Volumes ONTAP 的聚合必须处于联机状态。聚合在大多数配置中都应该联机、但如果不联机、则应将其联机。

### 关于此任务

这些步骤介绍了如何将 System Manager 用于版本 9.3 和更高版本。

#### 步骤

1. 在工作环境中，单击菜单图标，然后单击 \* 高级 > 高级分配 \*。
2. 选择一个聚合，单击 \* 信息 \*，然后验证此状态是否为联机。



<b>aggr1</b>		
Aggregate Capacity:	88.57 GB	
-----		
Used Aggregate Capacity:	1.07 GB	
-----		
Volumes:	2	▼
-----		
AWS Disks:	1	▼
-----		
State:	online	

3. 如果聚合处于脱机状态，请使用 System Manager 使聚合联机：
  - a. ["登录到系统管理器。"](#)
  - b. 单击 \* 存储 > 聚合和磁盘 > 聚合 \*。
  - c. 选择聚合，然后单击 \* 更多操作 > 状态 > 联机 \*。

## 从 Cloud Manager 升级 Cloud Volumes ONTAP 通知

Cloud Manager 会在新版本的 Cloud Volumes ONTAP 可用时向您发出通知。单击通知以启动升级过程。

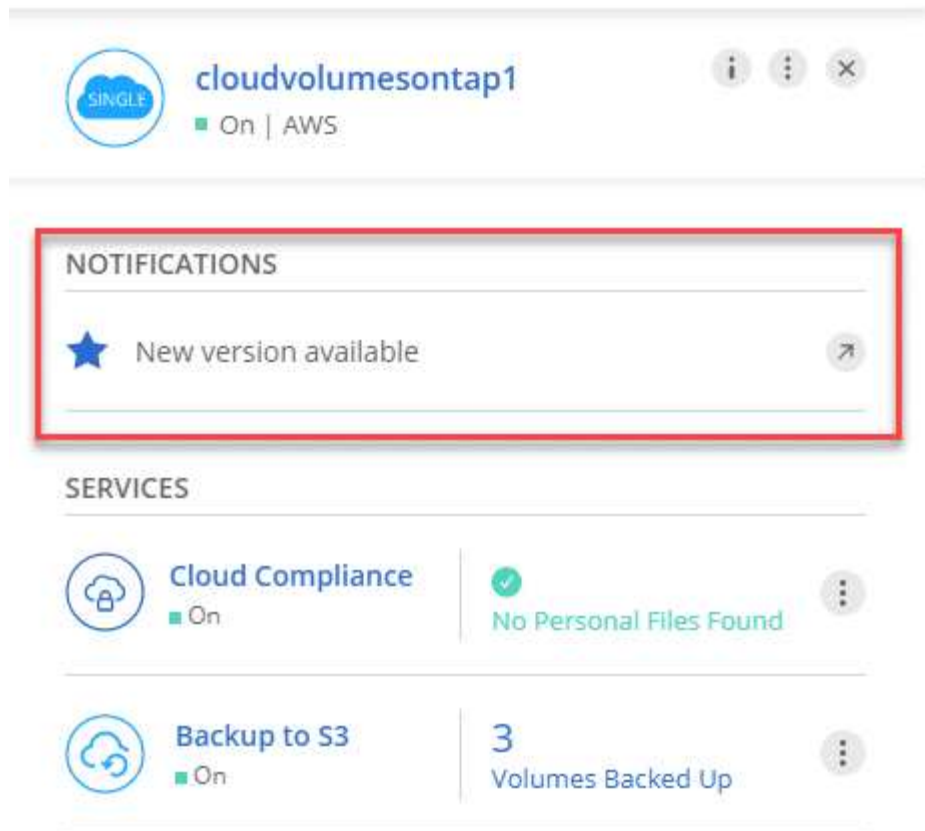
#### 开始之前

对于 Cloud Volumes ONTAP 系统，不能在执行云管理器操作（如卷或聚合创建）。

#### 步骤

1. 单击 \* 工作环境 \*。
2. 选择工作环境。

如果有新版本可用，则右窗格中将显示通知：



3. 如果有新版本，请单击 \* 升级 \*。
4. 在发行信息页面中，单击链接以阅读指定版本的发行说明，然后选中 \* 我已阅读 ... \* 复选框。
5. 在最终用户许可协议（EULA）页面中，阅读 EULA，然后选择 \* 我阅读并批准 EULA \*。
6. 在 Review and Approve 页面中，阅读重要说明，选择 \* 我了解 ... \*，然后单击 \* 执行 \*。

#### 结果

Cloud Manager 将启动软件升级。软件更新完成后，您可以在工作环境中执行操作。

#### 完成后

如果暂停了 SnapMirror 传输、请使用 System Manager 恢复传输。

## 使用 HTTP 或 FTP 服务器升级或降级 Cloud Volumes ONTAP

您可以将 Cloud Volumes ONTAP 软件映像放置在 HTTP 或 FTP 服务器上、然后从 Cloud Manager 启动软件更新。如果云管理器无法访问 S3 存储区以升级软件或要降级软件，则可以使用此选项。

#### 步骤

1. 设置可托管 Cloud Volumes ONTAP 软件映像的 HTTP 服务器或 FTP 服务器。
2. 如果您已通过 VPN 连接到虚拟网络，则可以将 Cloud Volumes ONTAP 软件映像放置在您自己网络中的 HTTP 服务器或 FTP 服务器上。否则，您必须将文件放置在云中的 HTTP 服务器或 FTP 服务器上。

3. 如果对 Cloud Volumes ONTAP 使用您自己的安全组、请确保出站规则允许 HTTP 或 FTP 连接、以便 Cloud Volumes ONTAP 可以访问软件映像。



默认情况下，预定义的 Cloud Volumes ONTAP 安全组允许出站 HTTP 和 FTP 连接。

4. 从获取软件映像 "[NetApp 支持站点](#)".
5. 将软件映像复制到 HTTP 或 FTP 服务器上的目录中、该文件将从该目录中提供服务。
6. 在 Cloud Manager 的工作环境中，单击菜单图标，然后单击 \* 高级 > 更新 Cloud Volumes ONTAP \*。
7. 在更新软件页面上，选择 \* 选择可从 URL\* 获得的映像，输入 URL ，然后单击 \* 更改映像 \*。
8. 单击 \* 继续 \* 进行确认。

#### 结果

Cloud Manager 将启动软件更新。软件更新完成后，您可以在工作环境中执行操作。

#### 完成后

如果暂停了 SnapMirror 传输、请使用 System Manager 恢复传输。

## 使用本地映像降级 Cloud Volumes ONTAP

将 Cloud Volumes ONTAP 过渡到同一版本系列中的早期版本（例如 9.5 至 9.4 ）称为降级。您可以在降级新集群或测试集群时降级而不需要帮助，但是如果降级生产集群，则应联系技术支持。

每个 Cloud Volumes ONTAP 系统都可以包含两个软件映像：当前运行的映像和可引导的备用映像。云管理器可以将备用映像更改为默认映像。如果当前映像出现问题，您可以使用此选项降级到以前版本的 Cloud Volumes ONTAP 。

#### 关于此任务

此降级过程仅适用于单个 Cloud Volumes ONTAP 系统。不适用于 HA 对。

#### 步骤

1. 在工作环境中，单击菜单图标，然后单击 \* 高级 > 更新 Cloud Volumes ONTAP \*。
2. 在更新软件页面上，选择备用映像，然后单击 \* 更改映像 \*。
3. 单击 \* 继续 \* 进行确认。

#### 结果

Cloud Manager 将启动软件更新。软件更新完成后，您可以在工作环境中执行操作。

#### 完成后

如果暂停了 SnapMirror 传输、请使用 System Manager 恢复传输。

## 修改 Cloud Volumes ONTAP 系统

您可能需要在存储需求发生变化时更改 Cloud Volumes ONTAP 实例的配置。例如，您可以在“按需购买、渐进扩展”配置之间进行更改、更改实例或 VM 类型以及移至备用订阅。

## 在 Cloud Volumes ONTAP BYOL 系统上安装许可证文件

如果 Cloud Manager 无法从 NetApp 获取 BYOL 许可证文件、您可以自己获取该文件、然后手动将该文件上载到 Cloud Manager、以便它可以在 Cloud Volumes ONTAP 系统上安装许可证。

### 步骤

1. 转至 "[NetApp 许可证文件生成器](#)" 并使用您的 NetApp 支持站点凭据登录。
2. 输入密码，选择您的产品，输入序列号，确认您已阅读并接受隐私策略，然后单击 \* 提交 \*。

◦ 示例 \*

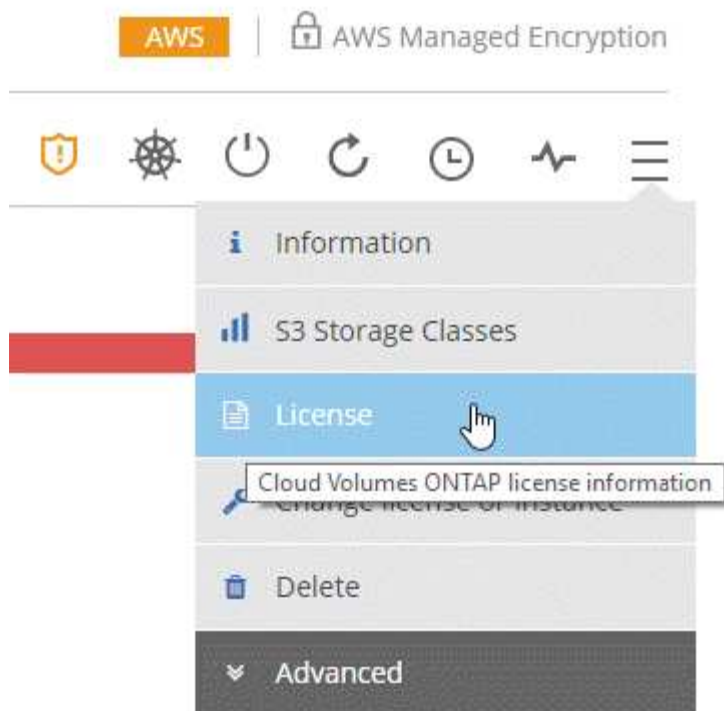
Password*	<input type="password" value="●●●●●●●●"/>
Product Line*	<input type="text" value="NetApp ONTAP Cloud BYOL for AWS"/>
Product Serial #*	<input type="text" value="90120130000000000555"/>

Not only is protecting your data required by law, but your privacy is also very important to us. Please read and agree to the NetApp [Data Privacy Policy](#) before you continue. For information related to NetApp's privacy policy please click here [Privacy Policy](#) or contact [privacy@netapp.com](mailto:privacy@netapp.com).

I have read NetApp's new [Global Data Privacy Policy](#) and understand how NetApp and its selected partners may use my personal data.

Submit

3. 选择是通过电子邮件还是直接下载接收 serialnumber.nlf JSON 文件。
4. 在 Cloud Manager 中，打开 Cloud Volumes ONTAP BYOL 工作环境。
5. 单击菜单图标，然后单击 \* 许可证 \*。



6. 单击 \* 上传许可证文件 \*。
7. 单击 \* 上传 \*，然后选择文件。

#### 结果

Cloud Manager 会在 Cloud Volumes ONTAP 系统上安装新的许可证文件。

## 更改 Cloud Volumes ONTAP 的实例或计算机类型

在 AWS，Azure 或 GCP 中启动 Cloud Volumes ONTAP 时，您可以从多种实例或计算机类型中进行选择。如果您确定实例或计算机类型的大小不足或过大，则可以随时更改此实例或计算机类型。

#### 关于此任务

- 必须在 Cloud Volumes ONTAP HA 对上启用自动交还（这是默认设置）。否则，操作将失败。

["ONTAP 9 文档：用于配置自动交还的命令"](#)

- 该操作将重新启动 Cloud Volumes ONTAP。

对于单节点系统，I/O 中断。

对于 HA 对、更改不会中断。HA 对继续为数据提供服务。

- 更改实例或计算机类型会影响云提供商的服务费用。

#### 步骤

1. 在工作环境中，单击菜单图标，然后单击 \* 更改 AWS 的许可证或实例 \*，\* 更改 Azure 的许可证或 VM\* 或 \* 更改 GCP 的许可证或计算机 \*。
2. 如果您使用的是按需付费配置、则可以选择其他许可证。



3. 选择一个实例或计算机类型，选中此复选框以确认您了解更改的含义，然后单击 \* 确定 \*。

## 结果

Cloud Volumes ONTAP 会使用新配置重新启动。

## 在按需购买配置之间进行更改

启动按需购买的 Cloud Volumes ONTAP 系统后、您可以随时通过修改许可证在 Explore、Standard 和 Premium 配置之间进行更改。更改许可证会增加或减少原始容量限制，并允许您从不同的 AWS 实例类型或 Azure 虚拟机类型中进行选择。



在 GCP 中，每个按需购买配置都有一种计算机类型。您不能在不同的计算机类型之间进行选择。

## 关于此任务

请注意以下有关在“按需购买、渐进扩展”许可证之间进行更改的信息：

- 该操作将重新启动 Cloud Volumes ONTAP。
  - 对于单节点系统，I/O 中断。
  - 对于 HA 对、更改不会中断。HA 对继续为数据提供服务。
- 更改实例或计算机类型会影响云提供商的服务费用。

## 步骤

1. 在工作环境中，单击菜单图标，然后单击 \* 更改 AWS 的许可证或实例 \*，\* 更改 Azure 的许可证或 VM\* 或 \* 更改 GCP 的许可证或计算机 \*。
2. 选择许可证类型和实例类型或计算机类型，选中此复选框以确认您了解更改的含义，然后单击 \* 确定 \*。

## 结果

Cloud Volumes ONTAP 将使用新许可证，实例类型或计算机类型或这两者重新启动。

## 迁移到备用 Cloud Volumes ONTAP 配置

如果要在按需付费订阅和 BYOL 订阅之间或在单个 Cloud Volumes ONTAP 系统和 HA 对之间移动、则可以部署新系统、然后将数据从现有系统复制到新系统。

## 步骤

1. 创建新的 Cloud Volumes ONTAP 工作环境。
  - ["在 AWS 中启动 Cloud Volumes ONTAP"](#)
  - ["在 Azure 中启动 Cloud Volumes ONTAP"](#)
  - ["在 GCP 中启动 Cloud Volumes ONTAP"](#)
2. "设置一次性数据复制" 必须复制的每个卷的系统之间。
3. 终止不再需要的 Cloud Volumes ONTAP 系统 ["删除原始工作环境"](#)。

## 更改 AWS Marketplace 订阅

如果要更改要从中收取费用的 AWS 帐户，请更改 Cloud Volumes ONTAP 系统的 AWS Marketplace 订阅。

### 步骤

1. 如果您尚未添加新订阅，请从添加新订阅 ["AWS Marketplace 中的 Cloud Manager 产品"](#)。
2. 在 Cloud Manager 的工作环境中，单击菜单图标，然后单击 \* 市场订阅 \*。
3. 从下拉列表中选择一个订阅。
4. 单击 \* 保存 \*。

## 将写入速度更改为正常或较高

Cloud Volumes ONTAP 的默认写入速度为正常。如果工作负载需要快速写入性能，则可以更改为高写入速度。在更改写入速度之前，您应先执行此操作 ["了解正常设置与高设置之间的区别"](#)。

### 关于此任务

- 确保卷或聚合创建等操作未在进行中。
- 请注意，此更改将重新启动 Cloud Volumes ONTAP。

对于单节点系统，I/O 中断。

对于 HA 对、更改不会中断。HA 对继续为数据提供服务。

### 步骤

1. 在工作环境中，单击菜单图标，然后单击 \* 高级 > 写入速度 \*。
2. 选择 \* 正常 \* 或 \* 高 \*。

如果您选择 "高"，则需要阅读 "我了解 ..." 陈述并通过选中此复选框进行确认。

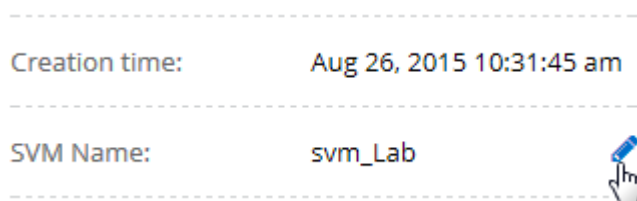
3. 单击 \* 保存 \*，查看确认消息，然后单击 \* 继续 \*。

## 修改存储虚拟机名称

Cloud Manager 会自动命名 Cloud Volumes ONTAP 的存储虚拟机（SVM）。如果您有严格的命名标准，则可以修改 SVM 的名称。例如，您可能希望它与您为 ONTAP 集群命名 SVM 的方式匹配。

### 步骤

1. 在工作环境中，单击菜单图标，然后单击 \* 信息 \*。
2. 单击 SVM 名称右侧的编辑图标。



3. 在修改 SVM 名称对话框中，修改 SVM 名称，然后单击 \* 保存 \*。

## 更改 Cloud Volumes ONTAP 的密码

Cloud Volumes ONTAP 包括集群管理员帐户。如果需要，您可以从 Cloud Manager 更改此帐户的密码。



不应通过 System Manager 或 CLI 更改管理员帐户的密码。该密码不会反映在 Cloud Manager 中。因此，Cloud Manager 无法正确监控实例。

### 步骤

1. 在工作环境中，单击菜单图标，然后单击 \* 高级 > 设置密码 \*。
2. 输入新密码两次，然后单击 \* 保存 \*。

新密码必须不同于您使用的最后六个密码之一。

## 更改 c4.4xLarge 和 c4.8xLarge 实例的网络 MTU

默认情况下，当您在 AWS 中选择 c4.4xLarge 实例或 c4.8xLarge 实例时，Cloud Volumes ONTAP 配置为使用 9000 MTU（也称为巨型帧）。如果网络配置更适合，则可以将网络 MTU 更改为 1,500 字节。

### 关于此任务

网络最大传输单元（MTU）为 9000 字节可为特定配置提供最高的网络吞吐量。

如果同一 VPC 中的客户端与 Cloud Volumes ONTAP 系统通信、并且其中一些或全部客户端也支持 9000 MTU、则最好选择 9000 MTU。如果流量离开 VPC、则可能会出现数据包碎片，从而降低性能。

如果 VPC 以外的客户端或系统与 Cloud Volumes ONTAP 系统进行通信，则网络 MTU 为 1,500 字节是理想的选择。

### 步骤

1. 在工作环境中，单击菜单图标，然后单击 \* 高级 > 网络利用率 \*。
2. 选择 \* 标准 \* 或 \* 巨型帧 \*。
3. 单击 \* 更改 \*。

## 更改多个 AWS AZs 中与 HA 对关联的路由表

您可以修改 AWS 路由表，其中包含指向 HA 对的浮动 IP 地址的路由。如果新的 NFS 或 CIFS 客户端需要访问 AWS 中的 HA 对，则可以执行此操作。

### 步骤

1. 在工作环境中，单击菜单图标，然后单击 \* 信息 \*。
2. 单击 \* 路由表 \*。
3. 修改选定路由表的列表，然后单击 \* 保存 \*。

### 结果

Cloud Manager 发送 AWS 请求以修改路由表。

# 管理 Cloud Volumes ONTAP 的状态

您可以从 Cloud Manager 停止并启动 Cloud Volumes ONTAP 来管理您的云计算成本。

## 计划自动关闭 Cloud Volumes ONTAP

您可能希望在特定时间间隔内关闭 Cloud Volumes ONTAP 以降低计算成本。您可以将 Cloud Manager 配置为在特定时间自动关闭然后重新启动系统，而不是手动执行此操作。

关于此任务

计划自动关闭 Cloud Volumes ONTAP 系统时，如果正在进行活动数据传输，则 Cloud Manager 会推迟关闭。传输完成后，Cloud Manager 将关闭系统。

此任务会安排 HA 对中两个节点的自动关闭。

步骤

1. 在工作环境中，单击时钟图标：



2. 指定关机计划：

- a. 选择是每天、每工作日、每周末还是三个选项的任意组合来关闭系统。
- b. 指定关闭系统的时间以及关闭系统的时间。

▪ 示例 \*

下图显示了指示 Cloud Manager 每星期六 12:00 A.M. 关闭系统的计划48 小时。Cloud Manager 每周一上午 12:00 重新启动系统

<input type="checkbox"/>	<b>Turn off every weekday</b> Mon, Tue, Wed, Thu, Fri	turn off at	08 : 00	PM	for	12	Hours (1-24)
<input checked="" type="checkbox"/>	<b>Turn off every weekend</b> Sat	turn off at	12 : 00	AM	for	48	Hours (1-48)

3. 单击 \* 保存 \*。

结果

云管理器可保存计划。时钟图标将发生变化以指示已设置计划：



## 停止 Cloud Volumes ONTAP

停止 Cloud Volumes ONTAP 可以节省计算成本并创建根磁盘和引导磁盘的快照，这有助于排除故障。

关于此任务

当您停止 HA 对时、Cloud Manager 会关闭两个节点。

步骤

1. 在工作环境中，单击 \* 关闭 \* 图标。



2. 启用创建快照的选项、因为快照可以启用系统恢复。
3. 单击 \* 关闭 \*。

可能需要几分钟才能停止系统。您可以在以后从 " 工作环境 " 页重新启动系统。

## 监控 AWS 资源成本

您可以通过 Cloud Manager 查看与在 AWS 中运行 Cloud Volumes ONTAP 相关的资源成本。您还可以了解使用 NetApp 功能可以降低存储成本节省了多少资金。

关于此任务

Cloud Manager 会在您刷新页面时更新成本。有关最终成本详细信息，请参阅 AWS 。

步骤

1. 验证 Cloud Manager 是否可以从 AWS 获取成本信息：
  - a. 确保为 Cloud Manager 提供权限的 IAM 策略包括以下操作：

```
"ce:GetReservationUtilization",  
"ce:GetDimensionValues",  
"ce:GetCostAndUsage",  
"ce:GetTags"
```

这些操作包含在最新的中 ["Cloud Manager 策略"](#)。从 NetApp Cloud Central 部署的新系统会自动包含这些权限。

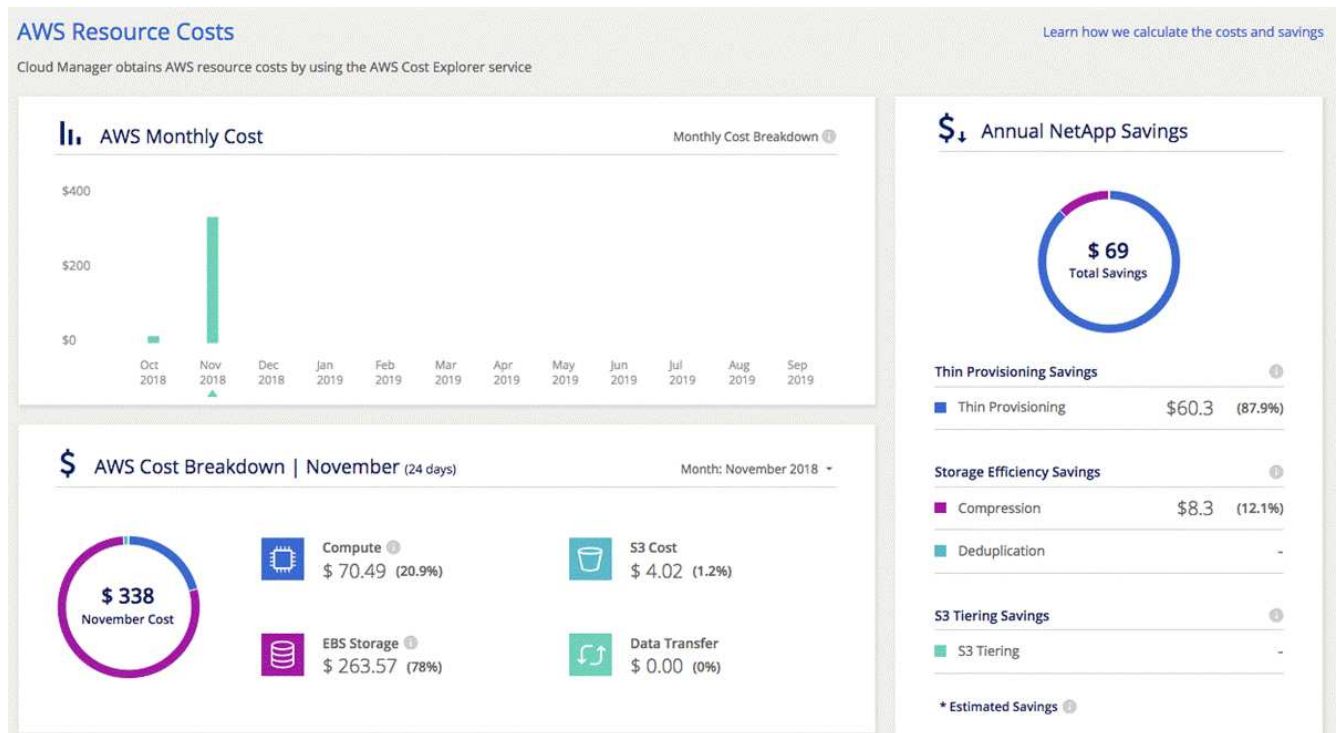
- b. ["激活 \\* 工作环境 Id\\* 标记"](#)。

为了跟踪 AWS 成本，Cloud Manager 会为 Cloud Volumes ONTAP 实例分配成本分配标记。创建首个工作环境后，激活 \* 工作环境 Id\* 标记。用户定义的标记不会显示在 AWS 计费报告中，除非您在计费和成本管理控制台中激活它们。

2. 在工作环境页面上，选择一个 Cloud Volumes ONTAP 工作环境，然后单击 \* 成本 \*。

如果您在卷上启用了 NetApp 的成本节省功能，则成本页面将显示当前月份和前几个月的成本，并显示 NetApp 每年节省的成本。

下图显示了成本页面示例：



## 提高防范勒索软件的能力

勒索软件攻击可能会耗费业务时间，资源和声誉。您可以通过 Cloud Manager 实施 NetApp 解决方案 for 勒索软件，它可以提供有效的工具来实现可见性，检测和补救。

步骤

1. 在工作环境中，单击 \* 勒索软件 \* 图标。



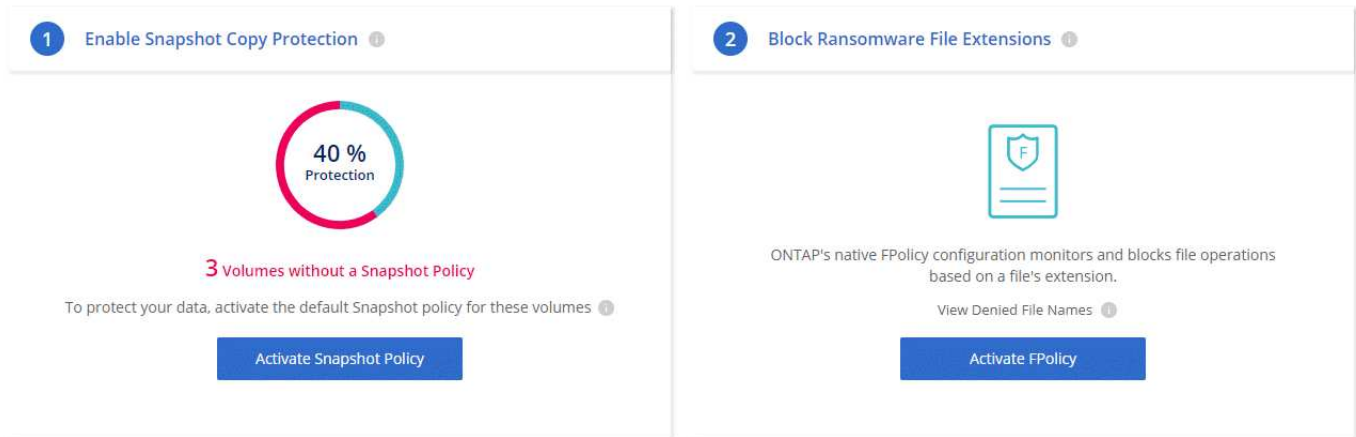
2. 实施 NetApp 解决方案 for 勒索软件：

- a. 如果卷未启用 Snapshot 策略，请单击 \* 激活 Snapshot 策略 \*。

NetApp Snapshot 技术可为勒索软件补救提供业内最佳的解决方案。成功恢复的关键在于从未受感染的备份中还原。Snapshot 副本为只读副本，可防止勒索软件损坏。它们还可以提供创建单个文件副本或完整灾难恢复解决方案映像的粒度。

- b. 单击 \* 激活 FPolicy\* 以启用 ONTAP 的 FPolicy 解决方案，它可以根据文件扩展名阻止文件操作。

此预防性解决方案可通过阻止常见的勒索软件文件类型来增强抵御勒索软件攻击的能力。



## 将现有 Cloud Volumes ONTAP 系统添加到 Cloud Manager

您可以发现现有的 Cloud Volumes ONTAP 系统并将其添加到 Cloud Manager 中。如果您部署了新的 Cloud Manager 系统，则可以执行此操作。

开始之前

您必须知道 Cloud Volumes ONTAP 管理员用户帐户的密码。

步骤

1. 在工作环境页面上，单击 \* 发现 \* 并选择 \* Cloud Volumes ONTAP \*。
2. 选择系统所在的云提供商。
3. 在区域页面上、选择实例运行所在的区域、然后选择实例。
4. 在凭据页面上，输入 Cloud Volumes ONTAP 管理员用户的密码，然后单击 \* 执行 \*。

结果

Cloud Manager 会将 Cloud Volumes ONTAP 实例添加到工作空间。

## 删除 Cloud Volumes ONTAP 工作环境

最好从 Cloud Manager 中删除 Cloud Volumes ONTAP 系统，而不是从云提供商的控制台删除。例如，如果您从 AWS 终止已获得许可的 Cloud Volumes ONTAP 实例，则不能将此许可证密钥用于其他实例。您必须从 Cloud Manager 中删除工作环境才能发布许可证。

## 关于此任务

删除工作环境时、Cloud Manager 会终止实例、删除磁盘和快照。



Cloud Volumes ONTAP 实例启用了终止保护、有助于防止 AWS 意外终止。但是，如果确实要从 AWS 终止 Cloud Volumes ONTAP 实例，则必须转到 AWS CloudFormation 控制台并删除该实例的堆栈。堆栈名称是工作环境的名称。

## 步骤

1. 在工作环境中，单击菜单图标，然后单击 \* 删除 \*。
2. 键入工作环境的名称，然后单击 \* 删除 \*。

删除工作环境最多可能需要 5 分钟。



# 管理 Cloud Manager

## 更新 Cloud Manager

您可以将 Cloud Manager 更新为最新版本或使用 NetApp 人员与您共享的补丁程序。

### 启用自动更新

Cloud Manager 可以在新版本可用时自动更新自身。这样可以确保您运行的是最新版本。

关于此任务

如果没有运行任何操作，则 Cloud Manager 会在午夜 12 点自动更新。

步骤

1. 在 Cloud Manager 控制台的右上角，单击设置图标，然后选择 \* Cloud Manager 设置 \*。
2. 选中自动 Cloud Manager 更新下的复选框，然后单击 \* 保存 \*。

### 将 Cloud Manager 更新为最新版本

您应该启用对 Cloud Manager 的自动更新，但您始终可以直接从 Web 控制台执行手动更新。Cloud Manager 从 AWS 中 NetApp 拥有的 S3 存储区获取软件更新。

开始之前

您应已查看 ["此版本中的新增功能"](#) 确定新要求和支持变更。

关于此任务

软件更新需要几分钟时间。在更新期间，Cloud Manager 不可用。

步骤

1. 通过查看控制台的右下角来检查是否有新版本可用：



2. 如果有新版本，请单击 \* 时间线 \* 以确定是否正在执行任何任务。

如果正在执行任何任务，请等待任务完成后再继续执行下一步。

3. 在控制台的右下角，单击 \* 新版本可用 \*。
4. 在 Cloud Manager 软件更新页面上，单击所需版本旁边的 \* 更新 \*。
5. 完成确认对话框，然后单击 \* 确定 \*：

结果

Cloud Manager 将启动更新过程。您可以在几分钟后登录控制台。

## 使用修补程序更新 Cloud Manager

如果 NetApp 与您共享修补程序、您可以直接从 Cloud Manager Web 控制台使用提供的修补程序更新 Cloud Manager。

关于此任务

修补程序更新通常需要几分钟时间。在更新期间，Cloud Manager 不可用。

步骤

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



2. 单击链接以使用提供的修补程序更新 Cloud Manager。

If NetApp shared a patch with you, click [here](#) to update Cloud Manager with the supplied patch.

3. 完成确认对话框，然后单击 \* 确定 \*：
4. 选择提供的修补程序。

结果

Cloud Manager 将应用此修补程序。您可以在几分钟后登录控制台。

## 在 Cloud Central 帐户中管理工作空间和用户

"[执行初始设置后](#)"，您可能需要稍后管理用户，工作空间和服务连接器。

"[详细了解 Cloud Central 帐户的工作原理](#)"。

### 添加用户

将 Cloud Central 用户与 Cloud Central 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](#)" 并创建帐户。
2. 在 Cloud Manager 中，单击 \* 帐户设置 \*。
3. 在用户选项卡中，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。

5. 如果选择了 Workspace Admin ， 请选择一个或多个要与该用户关联的工作空间。

**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

6. 单击 \* 关联用户 \* 。

#### 结果

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。

#### 结果

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。

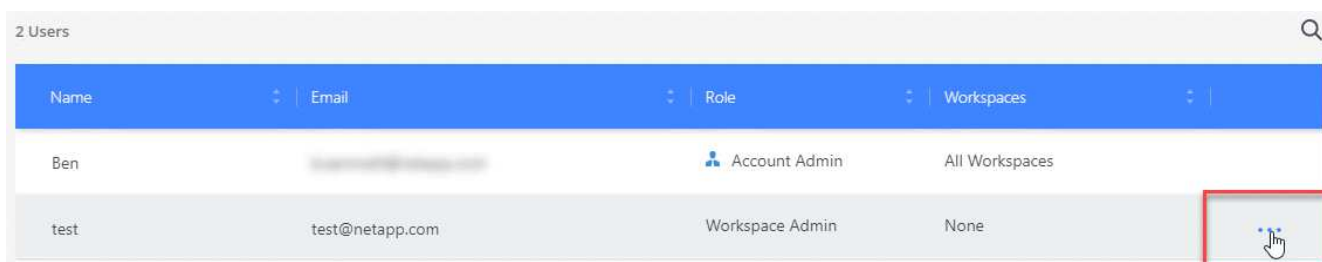
## 删除用户

解除用户关联后，用户将无法再访问 Cloud Central 帐户中的资源。

#### 步骤

1. 单击 \* 帐户设置 \* 。

2. 单击与用户对应的行中的操作菜单。



Name	Email	Role	Workspaces
Ben		Account Admin	All Workspaces
test	test@netapp.com	Workspace Admin	None

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

## 结果

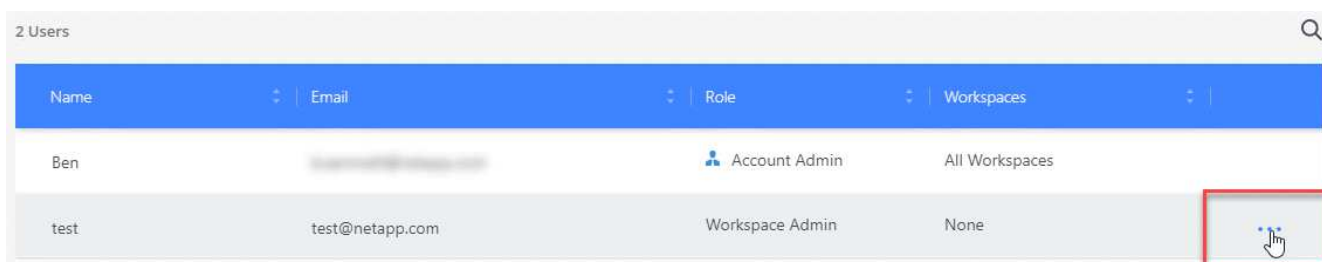
用户无法再访问此 Cloud Central 帐户中的资源。

## 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. 单击 \* 帐户设置 \* 。
2. 单击与用户对应的行中的操作菜单。



Name	Email	Role	Workspaces
Ben		Account Admin	All Workspaces
test	test@netapp.com	Workspace Admin	None

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 \* 。

## 结果

现在，只要服务连接器也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。

## 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. 单击 \* 帐户设置 \* 。
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Service Connector的工作空间

您需要将服务连接器与工作空间关联，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，则不需要将服务连接器与工作空间相关联。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，工作空间和服务连接器"](#)。

### 步骤

1. 单击 \* 帐户设置 \*。
2. 单击 \* 服务连接器 \*。
3. 单击要关联的服务连接器的 \* 管理工作空间 \*。
4. 选择要与服务连接器关联的工作空间，然后单击 \* 应用 \*。

## 删除 Cloud Volumes ONTAP 工作环境

帐户管理员可以删除 Cloud Volumes ONTAP 工作环境以将其移至其他系统或对发现问题进行故障排除。

### 关于此任务

删除 Cloud Volumes ONTAP 工作环境会将其从 Cloud Manager 中删除。它不会删除 Cloud Volumes ONTAP 系统。您可以在以后重新发现工作环境。

通过从云管理器中删除工作环境，您可以执行以下操作：

- 在另一个工作空间中重新发现它
- 从另一个 Cloud Manager 系统重新发现它
- 如果在初始查找期间遇到问题，请重新发现该问题

### 步骤

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



2. 在工具页面中，单击 \* 启动 \*。
3. 选择要删除的 Cloud Volumes ONTAP 工作环境。
4. 在 Review and Approve 页面上，单击 \* 执行 \*。

## 结果

Cloud Manager 可消除工作环境。用户可以随时从 " 工作环境 " 页重新发现此工作环境。

## 配置 Cloud Manager 以使用代理服务器

首次部署 Cloud Manager 时，如果系统无法访问 Internet、则会提示您输入代理服务器。您也可以通过 Cloud Manager 的设置手动输入和修改代理。

### 关于此任务

如果您的公司策略要求您使用代理服务器进行与 Internet 的所有 HTTP 通信、则必须配置 Cloud Manager 以使用该代理服务器。代理服务器可以位于云中或网络中。

当您将 Cloud Manager 配置为使用代理服务器时、Cloud Manager、Cloud Volumes ONTAP 和 HA 调解器都使用代理服务器。

### 步骤

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



2. 在 HTTP 代理下，使用语法输入服务器 `<a href="http://<em>address:port</em>" class="bare">http://<em>address:port</em></a>` 下，如果服务器需要基本身份验证，请指定用户名和密码，然后单击 \* 保存 \*。



Cloud Manager 不支持包含 @ 字符的密码。

## 结果

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。

## 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 \* 续订 HTTPS 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。

## 结果

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

# 正在还原 Cloud Manager

您的 "NetApp Cloud Central 帐户" 让您可以轻松还原 Cloud Manager 配置。此帐户是在 Cloud Central 中运行的一项服务，因此您与此帐户关联的用户，工作空间和服务连接器始终可以访问。即使您的 Cloud Manager 系统被意外删除也是如此。



从 3.7.1 版开始，Cloud Manager 不再支持下载备份并使用其还原配置。您需要按照以下步骤还原 Cloud Manager。

## 步骤

1. 在现有 Cloud Central 帐户中部署新的 Cloud Manager 系统。

### "部署选项"

2. 将您的云提供商帐户和 NetApp 支持站点帐户添加到 Cloud Manager 中。

此步骤将准备好 Cloud Manager，以便您可以在云提供商中创建其他 Cloud Volumes ONTAP 系统。

如果您使用 AWS 密钥部署要在此新的 Cloud Manager 系统上发现的现有 Cloud Volumes ONTAP 系统，请务必完成此步骤。Cloud Manager 需要 AWS 密钥才能正确发现和管理 Cloud Volumes ONTAP。

- "将 AWS 帐户添加到 Cloud Manager"
- "将 Azure 帐户添加到 Cloud Manager"
- "将 NetApp 支持站点帐户添加到 Cloud Manager"

3. 重新发现您的工作环境：Cloud Volumes ONTAP 系统，内部集群和适用于云的 NetApp 私有存储配置。

- "将现有 Cloud Volumes ONTAP 系统添加到 Cloud Manager"
- "发现 ONTAP 集群"

## 结果

现在，Cloud Manager 配置将随您的帐户，设置和工作环境一起还原。

# 卸载 Cloud Manager

Cloud Manager 包含一个卸载脚本、您可以使用该脚本卸载软件以排除问题或从主机中永久删除软件。

## 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。

# 为文件服务配置卷

## 管理 Azure NetApp Files 的卷

查看并创建 NFS 卷 ["Azure NetApp Files"](#) 直接从 Cloud Manager 访问。

### 设置配置

您的配置需要满足一些要求，然后才能从 Cloud Manager 管理 Azure NetApp Files 的卷。

1. 必须在 Azure 门户中完成以下操作来设置 Azure NetApp Files :

- ["注册 Azure NetApp Files"](#)
- ["创建 NetApp 帐户"](#)
- ["设置容量池"](#)
- ["将子网委派给 Azure NetApp Files"](#)

2. Cloud Manager 必须按如下方式设置:

- Cloud Manager 必须在设置了 Azure NetApp Files 的帐户中的 Azure 中运行。
- Cloud Manager 虚拟机必须通过接收权限 ["托管身份"](#)。

如果您从 Cloud Central 部署了 Cloud Manager ， 则一切准备就绪。Cloud Central 会自动在 Cloud Manager 虚拟机上启用系统分配的托管身份。

如果您从 Azure Marketplace 部署了 Cloud Manager ， 则应遵循此操作 ["启用托管身份的说明"](#)。

- 分配给 Cloud Manager 虚拟机的 Azure 角色必须包含最新列出的权限 ["适用于 Azure 的 Cloud Manager 策略"](#):

```
"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"
```

设置配置后， Cloud Manager 会自动在 " 工作环境 " 页面上显示 Azure NetApp Files :





## 正在创建卷

您可以使用 Cloud Manager 为 Azure NetApp Files 创建 NFSv3 卷。

### 步骤

1. 打开工作环境。
2. 单击 \* 添加新卷 \*。
3. 在 \* 帐户信息 \* 页面中输入有关卷的基本详细信息：
  - a. 选择 Azure 订阅和 Azure NetApp Files 帐户。
  - b. 输入卷的名称。
  - c. 选择一个容量池并指定一个配额，即分配给卷的逻辑存储容量。

### Account Information

Azure Subscription	Volume Name	
<input type="text" value="OCCM QA1"/>	<input type="text" value="vol10"/>	
Azure NetApp Files Account	Capacity pool	Quota (GiB) ⓘ
<input type="text" value="vadimAnf"/>	<input type="text" value="test2 (5.0 TiB)"/>	<input type="text" value="200"/>

4. 填写 \* 位置和导出策略 \* 页面：
  - a. 选择一个 vNet 和子网。
  - b. 配置导出策略以控制对卷的访问。

### Location & Export Policy

Location	Export Policy
Vnet	Allowed Clients ⓘ
<input type="text" value="TomerANFrg-vnet"/>	<input type="text" value="172.70.2.0/32"/>
Subnet	
<input type="text" value="default   172.20.1.0/28"/>	

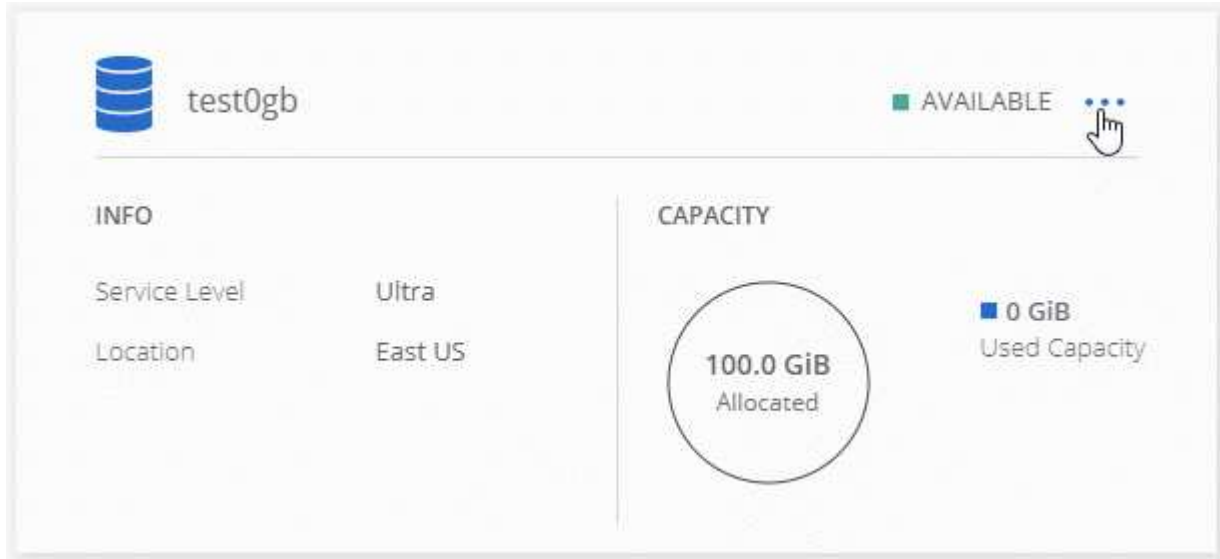
5. 单击 \* 执行 \*。

## 获取卷的挂载路径

复制卷的挂载路径，以便将卷挂载到 Linux 计算机。

### 步骤

1. 打开工作环境。
2. 将鼠标悬停在卷上，然后单击菜单。



3. 单击 \* 挂载命令 \*。



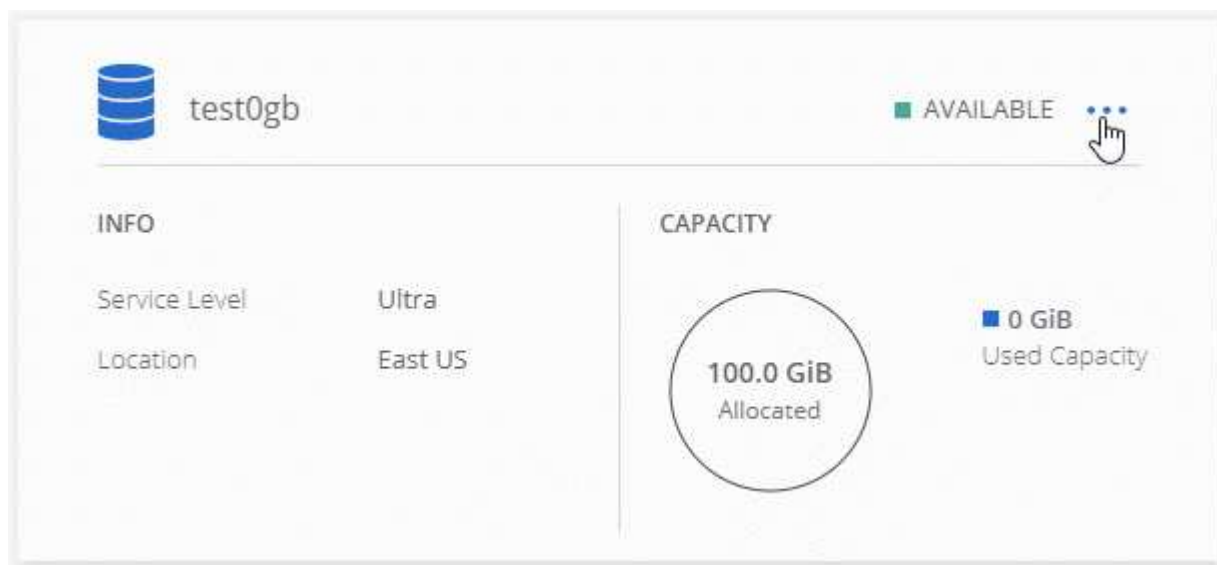
4. 复制挂载路径并使用复制的文本将卷挂载到 Linux 计算机。

## 删除卷

删除不再需要的卷。

### 步骤

1. 打开工作环境。
2. 将鼠标悬停在卷上，然后单击菜单。



3. 单击 \* 删除 \*。
4. 确认要删除此卷。

## 获取帮助

有关一般服务问题，请使用 Cloud Manager 聊天工具。

对于与 Azure NetApp Files 相关的技术支持问题，请使用 Azure 门户将支持请求记录到 Microsoft。选择关联的 Azure NetApp Files 订阅，然后在 \* 存储 \* 下选择 \* Microsoft \* 服务名称。\* 提供创建支持请求所需的其余信息。

Cloud Manager 在 \* 支持信息板 \* 菜单选项下提供本地 AutoSupport 下载。此 7z 文件包含一个 Azure 调试文件，用于显示与 Azure NetApp Files 帐户的入站和出站通信。

## 限制

- Cloud Manager 不支持 SMB 卷。
- Cloud Manager 不支持您管理容量池或卷快照。
- 您可以创建具有初始大小和单个导出策略的卷。必须从 Azure 门户中的 Azure NetApp Files 界面编辑卷。
- Cloud Manager 不支持与 Azure NetApp Files 之间的数据复制。

## 相关链接

- ["NetApp 云中心： Azure NetApp Files"](#)
- ["Azure NetApp Files 文档"](#)

# 管理适用于 AWS 的 Cloud Volumes Service

您可以通过 Cloud Manager 发现中的 NFS 云卷 "适用于 AWS 的 Cloud Volumes Service" 订阅。发现后，您可以直接从 Cloud Manager 添加其他 NFS 云卷。



Cloud Manager 不支持使用 Cloud Volumes Service for AWS 的 SMB 或双协议卷。

## 开始之前

- 通过 Cloud Manager ，可以发现 *existent* Cloud Volumes Service for AWS 订阅。请参见 "《[NetApp Cloud Volumes Service for AWS 帐户设置指南](#)》" 如果您尚未设置订阅。

您必须先对每个区域执行此设置过程，并从 Cloud Volumes Service 配置第一个卷，然后才能在 Cloud Manager 中发现该区域。

- 您需要获取 Cloud Volumes API 密钥和机密密钥，才能将其提供给 Cloud Manager 。 "有关说明，请参见 [Cloud Volumes Service for AWS 文档](#)"。

## 发现 Cloud Volumes Service for AWS 订阅

要开始使用，您需要发现 AWS 区域中的云卷。您可以稍后发现其他区域。

### 步骤

1. 在工作环境页面上，单击 \* 发现 \* 。
2. 选择 \* 适用于 AWS\* 的 Cloud Volumes Service 。

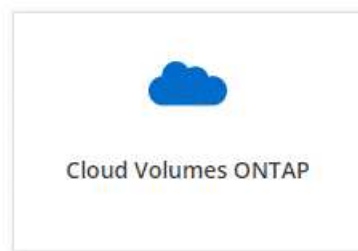
### Discover

Select the storage that you'd like to discover: an ONTAP cluster, an existing Cloud Volumes ONTAP system, or the cloud volumes in your Cloud Volumes Service for AWS subscription.



ONTAP Cluster

[Learn More](#)



Cloud Volumes ONTAP

[Learn More](#)



Cloud Volumes Service  
for AWS

[Learn More](#)

3. 提供有关 Cloud Volumes Service 订阅的信息：
  - a. 选择云卷所在的 AWS 区域。
  - b. 输入 Cloud Volumes API 密钥和机密密钥。 "有关说明，请参见 [Cloud Volumes Service for AWS 文档](#)"。
  - c. 单击 \* 执行 \* 。

## Cloud Volumes Service Details

Provide a few details about your Cloud Volumes Service subscription so Cloud Manager can discover your cloud volumes.

### Location

AWS Region

US West | Oregon

### Credentials

Cloud Volumes Service API Key

.....

Cloud Volumes Service Secret Key

.....

### 结果

Cloud Manager 现在应在 "工作环境" 页面上显示您的 Cloud Volumes Service for AWS 配置。



### 发现其他区域

如果您在其他区域有云卷，则需要发现每个区域。

### 步骤

1. 在 "工作环境" 页面上，选择工作环境（但不要双击打开它）。
2. 在右侧窗格中，单击 \* 发现其他区域的 Cloud Volumes Service \*。

## Cloud Volumes Service for AWS

1.85 TiB  
Allocated Capacity


15.05 GiB  
Used Capacity

1  
Regions

15  
Volumes



 Add New Volume

 Discover Cloud Volumes Service in another region

View Volumes

3. 提供有关 Cloud Volumes Service 订阅的信息：

- a. 选择云卷所在的 AWS 区域。
- b. 输入 Cloud Volumes API 密钥和机密密钥。"有关说明，请参见 [Cloud Volumes Service for AWS 文档](#)"。
- c. 单击 \* 执行 \*。

结果

Cloud Manager 可发现有关选定区域中的云卷的信息。

### 创建云卷

您可以使用 Cloud Manager 创建 NFSv3 云卷。您只能创建具有初始大小和单个导出策略的云卷。必须从 Cloud Volume Service 用户界面编辑卷。

1. 打开工作环境。
2. 单击 \* 添加新卷 \*。
3. 输入有关卷的详细信息：
  - a. 输入卷的名称。
  - b. 指定一个介于 100 GiB 到 90,000 GiB 范围内的大小（相当于 88 TiB）。



Cloud Manager 以 GiB 显示卷，而 Cloud Volumes Service 以 GB 显示卷。

- c. 指定服务级别：标准，高级或极速。  
["详细了解这些服务级别"](#)。
- d. 选择一个区域。您可以在 Cloud Manager 发现的区域中创建卷。
- e. 通过指定 IP 地址或无类别域间路由（CIDR）来限制客户端访问。

#### Details

Volume Name

Size (GiB)

Service Level

AWS Region

#### Export Policy

Allowed Clients

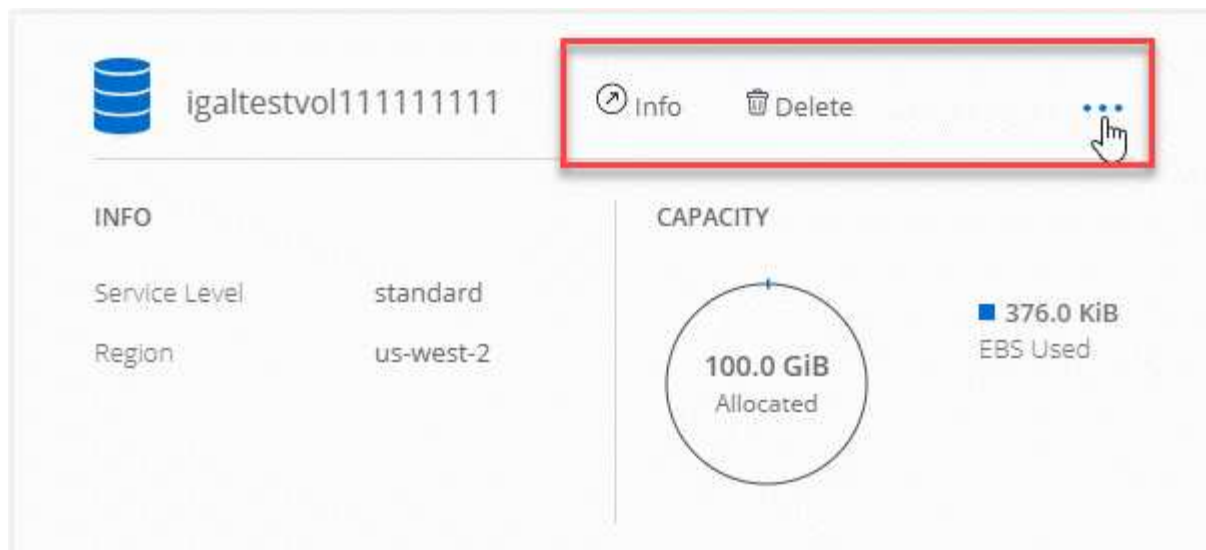
4. 单击 \* 执行 \*。

## 正在删除云卷

删除不再需要的云卷。

### 步骤

1. 打开工作环境。
2. 将鼠标悬停在卷上，然后单击菜单。单击 \* 删除 \*。



3. 确认要删除此卷。

## 获取帮助

有关一般服务问题，请使用 Cloud Manager 聊天工具。

对于与云卷相关的技术支持问题，请使用 Cloud Volumes Service 用户界面的 "支持" 选项卡中的 20 位 "930" 序列号。打开 Web 服务单或致电支持部门时，请使用此支持 ID。请务必从 Cloud Volumes Service 用户界面激活 Cloud Volumes Service 序列号以获得支持。"[此处将介绍这些步骤](#)"。

## 限制

- Cloud Manager 不支持 SMB 或双协议卷。
- 您只能创建具有初始大小和单个导出策略的云卷。必须从 Cloud Volume Service 用户界面编辑卷。
- Cloud Manager 不支持与 Cloud Volumes Service for AWS 订阅之间的数据复制。
- 不支持从 Cloud Manager 中删除 Cloud Volumes Service for AWS 订阅。从 Cloud Manager 发现某个区域不收取任何费用。

## 相关链接

- "[NetApp Cloud Central：适用于 AWS 的 Cloud Volumes Service](#)"
- "[NetApp Cloud Volumes Service for AWS 文档](#)"



# API 和自动化

## 基础架构即代码自动化示例

使用此页面上的资源获取有关将 Cloud Manager 和 Cloud Volumes ONTAP 与集成的帮助["基础架构即代码"](#)。

DevOps 团队可以使用各种工具自动设置新环境，从而将基础架构视为代码。Ansible 和 Terraform 这两种工具。我们开发了 Ansible 和 Terraform 示例，开发运营团队可以使用 Cloud Manager 来自动执行 Cloud Volumes ONTAP 并将其与基础架构即代码集成。

["查看自动化示例"](#)。

例如，您可以使用示例 Ansible 攻略手册来部署 Cloud Manager 和 Cloud Volumes ONTAP ，创建聚合并创建卷。修改环境的示例或根据示例创建新的攻略手册。

- [相关链接 \\*](#)
- ["NetApp 云博客：将 Cloud Manager REST API 与联合访问结合使用"](#)
- ["NetApp 云博客：采用 Cloud Volumes ONTAP 和 REST 的云自动化"](#)
- ["NetApp 云博客：自动化数据克隆，用于软件应用程序的基于云的测试"](#)
- ["NetApp 博客：《借助 Ansible + NetApp 加速基础架构即代码（ Infrastructure as Code ， IAC ）》"](#)
- ["NetApp thePub ：配置管理和放大；借助 Ansible 实现自动化"](#)
- ["NetApp thePub ：适用于 Ansible ONTAP 的角色"](#)

# 参考

## 常见问题：将 **Cloud Manager** 与 **NetApp Cloud Central** 集成

从 Cloud Manager 3.4 或更早版本升级时，如果尚未集成特定的 Cloud Manager 系统，NetApp 将选择这些系统与 NetApp Cloud Central 集成。此常见问题解答可以回答您可能对流程提出的问题。

### 什么是 **NetApp Cloud Central** ？

NetApp Cloud Central 为访问和管理 NetApp 云数据服务提供了一个集中位置。这些服务使您能够在云中运行关键应用程序、创建自动化灾难恢复站点、备份 SaaS 数据、并在多个云中有效地迁移和控制数据。

### 为什么 **NetApp** 将我的云管理器系统与云中心集成？

Cloud Manager 与 NetApp Cloud Central 的集成提供了多种优势、包括简化的部署体验、查看和管理多个云管理系统的单一位置以及集中式用户身份验证。

### 集成过程中会发生什么情况？

NetApp 会将您的 Cloud Manager 系统中的所有本地用户帐户迁移到 Cloud Central 中提供的集中式用户身份验证。

### 集中式用户身份验证如何工作？

通过集中式用户身份验证、您可以在云管理器系统之间以及云管理器与其他数据服务（如云同步）之间使用相同的凭据集。如果您忘记了密码、也可以轻松地重置密码。

### 我是否需要注册一个 **Cloud Central** 用户帐户？

当我们将您的云管理器系统与 Cloud Central 集成时、NetApp 将为您创建一个云中心用户帐户。您只需重置密码即可完成注册过程。

### 如果我已经拥有云中心用户帐户、该怎么办？

如果用于登录到 Cloud Manager 的电子邮件地址与 Cloud Central 用户帐户的电子邮件地址匹配，则您可以登录到您的 Cloud Manager 系统。

### 如果我的 **Cloud Manager** 系统具有多个用户帐户、该怎么办？

NetApp 将所有本地用户帐户迁移到 Cloud Central 用户帐户。每个用户都需要重置其密码。

### 如果我的用户帐户在多个云管理器系统中使用相同的电子邮件地址会怎样？

您只需重置一次密码、然后就可以使用同一个 Cloud Central 用户帐户登录到每个 Cloud Manager 系统。

如果我的本地用户帐户使用无效的电子邮件地址会怎样？

重置密码需要有效的电子邮件地址。通过 Cloud Manager 界面右下角的聊天图标与我们联系。

如果我有适用于云管理器 **API** 的自动化脚本怎么办？

所有 API 都向后兼容。如果您在重置密码时更改了密码，则需要更新使用密码的脚本。

如果我的云管理器系统使用 **LDAP**、该怎么办？

如果您的系统使用 LDAP、NetApp 将无法自动将系统与 Cloud Central 集成。您需要手动执行以下步骤：

1. 从部署新的 Cloud Manager 系统 "[NetApp Cloud Central](#)"。
2. "[使用新系统设置 LDAP](#)。"
3. "[发现现有 Cloud Volumes ONTAP 系统](#)" 从新的 Cloud Manager 系统。
4. 删除旧的云管理器系统。

我在哪里安装了 **Cloud Manager** 系统是否重要？

否无论系统驻留在何处、是在 AWS、Azure 中、还是在您的办公场所中、NetApp 都将与 Cloud Central 集成。



唯一的例外是 AWS 商业云服务环境。

## AWS 的安全组规则

Cloud Manager 创建了包含 Cloud Manager 和 Cloud Volumes ONTAP 成功运行所需的入站和出站规则的 AWS 安全组。您可能希望参考这些端口进行测试或使用自己的安全组。

### 云管理器规则

Cloud Manager 的安全组需要入站和出站规则。

#### 云管理器的入站规则

预定义安全组中入站规则的源代码为 0.0.0.0/0。

协议	Port	目的
SSH	22.	提供对云管理器主机的 SSH 访问
HTTP	80	提供从客户端 Web 浏览器到 Cloud Manager Web 控制台的 HTTP 访问以及从 Cloud Compliance 建立的连接
HTTPS	443.	提供从客户端 Web 浏览器到云管理器 Web 控制台的 HTTPS 访问
TCP	3128	如果您的 AWS 网络不使用 NAT 或代理，则可为 Cloud Compliance 实例提供 Internet 访问

## 云管理器的出站规则

为 Cloud Manager 预定义的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

为 Cloud Manager 预定义的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

如果您需要严格的出站流量规则、则可以使用以下信息仅打开 Cloud Manager 出站通信所需的端口。



源 IP 地址是 Cloud Manager 主机。

服务	协议	Port	目标	目的
Active Directory	TCP	88	Active Directory 目录林	Kerberos V 身份验证
	TCP	139.	Active Directory 目录林	NetBIOS 服务会话
	TCP	389.	Active Directory 目录林	LDAP
	TCP	445	Active Directory 目录林	Microsoft SMB/CIFS over TCP (通过 TCP) 和 NetBIOS 成帧
	TCP	464.	Active Directory 目录林	Kerberos V 更改和设置密码 (set_change)
	TCP	749	Active Directory 目录林	Active Directory Kerberos V 更改和设置密码 (RPCSEC_GSS)
	UDP	137.	Active Directory 目录林	NetBIOS 名称服务
	UDP	138.	Active Directory 目录林	NetBIOS 数据报服务
	UDP	464.	Active Directory 目录林	Kerberos 密钥管理

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、并将 AutoSupport 消息发送到 NetApp
API 调用	TCP	3000	ONTAP 集群管理 LIF	API 调用 ONTAP
	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
云合规性	HTTP	80	Cloud Compliance 实例	适用于 Cloud Volumes ONTAP 的云合规性

## Cloud Volumes ONTAP 的规则

Cloud Volumes ONTAP 的安全组需要入站和出站规则。

### Cloud Volumes ONTAP 的入站规则

预定义安全组中入站规则的源代码为 0.0.0.0/0。

协议	Port	目的
所有 ICMP	全部	Ping 实例
HTTP	80	使用集群管理 LIF 的 IP 地址对系统管理器 Web 控制台进行 HTTP 访问
HTTPS	443.	使用集群管理 LIF 的 IP 地址对 System Manager Web 控制台进行 HTTPS 访问
SSH	22.	SSH 访问集群管理 LIF 或节点管理 LIF 的 IP 地址
TCP	111.	远程过程调用 NFS
TCP	139.	用于 CIFS 的 NetBIOS 服务会话
TCP	161-162.	简单网络管理协议
TCP	445	Microsoft SMB/CIFS over TCP (通过 TCP) 和 NetBIOS 成帧
TCP	635	NFS 挂载
TCP	749	Kerberos
TCP	2049.	NFS 服务器守护进程
TCP	3260	通过 iSCSI 数据 LIF 进行 iSCSI 访问
TCP	4045	NFS 锁定守护进程
TCP	4046	NFS 的网络状态监视器
TCP	10000	使用 NDMP 备份

协议	Port	目的
TCP	11104.	管理 SnapMirror 的集群间通信会话
TCP	11105.	使用集群间 LIF 进行 SnapMirror 数据传输
UDP	111.	远程过程调用 NFS
UDP	161-162.	简单网络管理协议
UDP	635	NFS 挂载
UDP	2049.	NFS 服务器守护进程
UDP	4045	NFS 锁定守护进程
UDP	4046	NFS 的网络状态监视器
UDP	4049.	NFS Rquotad 协议

### Cloud Volumes ONTAP 的出站规则

为 Cloud Volumes ONTAP 预定义的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

为 Cloud Volumes ONTAP 预定义的安全组包括以下出站规则。

协议	Port	目的
所有 ICMP	全部	所有出站流量
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

如果您需要严格的出站流量规则、则可以使用以下信息仅打开 Cloud Volumes ONTAP 出站通信所需的端口。



源是 Cloud Volumes ONTAP 系统上的接口（IP 地址）。

服务	协议	Port	源	目标	目的	
Active Directory	TCP	88	节点管理 LIF	Active Directory 目录林	Kerberos V 身份验证	
	UDP	137.	节点管理 LIF	Active Directory 目录林	NetBIOS 名称服务	
	UDP	138.	节点管理 LIF	Active Directory 目录林	NetBIOS 数据报服务	
	TCP	139.	节点管理 LIF	Active Directory 目录林	NetBIOS 服务会话	
	TCP	389.	节点管理 LIF	Active Directory 目录林	LDAP	
	TCP	445	节点管理 LIF	Active Directory 目录林	Microsoft SMB/CIFS over TCP (通过 TCP) 和 NetBIOS 成帧	
	TCP	464.	节点管理 LIF	Active Directory 目录林	Kerberos V 更改和设置密码 (set_change)	
	UDP	464.	节点管理 LIF	Active Directory 目录林	Kerberos 密钥管理	
	TCP	749	节点管理 LIF	Active Directory 目录林	Kerberos V 更改和设置密码 (RPCSEC_GSS)	
	TCP	88	数据 LIF (NFS、CIFS)	Active Directory 目录林	Kerberos V 身份验证	
	UDP	137.	数据 LIF (NFS、CIFS)	Active Directory 目录林	NetBIOS 名称服务	
	UDP	138.	数据 LIF (NFS、CIFS)	Active Directory 目录林	NetBIOS 数据报服务	
	TCP	139.	数据 LIF (NFS、CIFS)	Active Directory 目录林	NetBIOS 服务会话	
	TCP	389.	数据 LIF (NFS、CIFS)	Active Directory 目录林	LDAP	
	TCP	445	数据 LIF (NFS、CIFS)	Active Directory 目录林	Microsoft SMB/CIFS over TCP (通过 TCP) 和 NetBIOS 成帧	
	TCP	464.	数据 LIF (NFS、CIFS)	Active Directory 目录林	Kerberos V 更改和设置密码 (set_change)	
	UDP	464.	数据 LIF (NFS、CIFS)	Active Directory 目录林	Kerberos 密钥管理	
	TCP	749	数据 LIF (NFS、CIFS)	Active Directory 目录林	Kerberos V 更改和设置密码 (RPCSEC_GSS)	
	备份到 S3	TCP	5010	集群间 LIF	备份端点或还原端点	备份到 S3 功能的备份和还原操作

服务	协议	Port	源	目标	目的
集群	所有流量	所有流量	一个节点上的所有 LIF	其它节点上的所有 LIF	集群间通信（仅限 Cloud Volumes ONTAP HA）
	TCP	3000	节点管理 LIF	HA 调解器	ZAPI 调用（仅适用于 Cloud Volumes ONTAP HA）
	ICMP	1.	节点管理 LIF	HA 调解器	保持活动状态（仅限 Cloud Volumes ONTAP HA）
DHCP	UDP	68	节点管理 LIF	DHCP	首次设置 DHCP 客户端
DHCP	UDP	67	节点管理 LIF	DHCP	DHCP 服务器
DNS	UDP	53.	节点管理 LIF 和数据 LIF（NFS、CIFS）	DNS	DNS
NDMP	TCP	18600 – 18699	节点管理 LIF	目标服务器	NDMP 副本
SMTP	TCP	25.	节点管理 LIF	邮件服务器	SMTP 警报、可用于 AutoSupport
SNMP	TCP	161.	节点管理 LIF	监控服务器	通过 SNMP 陷阱进行监控
	UDP	161.	节点管理 LIF	监控服务器	通过 SNMP 陷阱进行监控
	TCP	162.	节点管理 LIF	监控服务器	通过 SNMP 陷阱进行监控
	UDP	162.	节点管理 LIF	监控服务器	通过 SNMP 陷阱进行监控
SnapMirror	TCP	11104.	集群间 LIF	ONTAP 集群间 LIF	管理 SnapMirror 的集群间通信会话
	TCP	11105.	集群间 LIF	ONTAP 集群间 LIF	SnapMirror 数据传输
系统日志	UDP	514.	节点管理 LIF	系统日志服务器	系统日志转发消息

## HA 调解器外部安全组的规则

Cloud Volumes ONTAP HA 调解器的预定义外部安全组包括以下入站和出站规则。

### 入站规则

入站规则的源代码为 0.0.0.0/0。

协议	Port	目的
SSH	22.	SSH 与 HA 调解器的连接
TCP	3000	通过云管理器进行 REST 风格的 API 访问

### 出站规则

HA 调解器的预定义安全组将打开所有出站通信。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

HA 调解器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

如果需要严格的出站通信规则、可以使用以下信息仅打开 HA 调解器出站通信所需的端口。

协议	Port	目标	目的
HTTP	80	Cloud Manager IP 地址	下载调解器升级
HTTPS	443.	AWS API 服务	帮助进行存储故障转移
UDP	53.	AWS API 服务	帮助进行存储故障转移



您可以创建从目标子网到 AWS EC2 服务的接口 VPC 端点，而不是打开端口 443 和 53。

## HA 调解器内部安全组的规则

为 Cloud Volumes ONTAP HA 调解器预定义的内部安全组包括以下规则。Cloud Manager 始终会创建此安全组。您没有使用自己的选项。

### 入站规则

预定义的安全组包括以下入站规则。

协议	Port	目的
所有流量	全部	HA 调解器和 HA 节点之间的通信

### 出站规则

预定义的安全组包括以下出站规则。

协议	Port	目的
所有流量	全部	HA 调解器和 HA 节点之间的通信

## Azure 的安全组规则

Cloud Manager 创建了 Azure 安全组、其中包括 Cloud Manager 和 Cloud Volumes ONTAP 成功运行所需的入站和出站规则。您可能希望参考这些端口进行测试或使用自己的安全组。

## 云管理器规则

Cloud Manager 的安全组需要入站和出站规则。

### 云管理器的入站规则

预定义安全组中入站规则的源代码为 0.0.0.0/0。

Port	协议	目的
22.	SSH	提供对云管理器主机的 SSH 访问
80	HTTP	提供从客户端 Web 浏览器到云管理器 Web 控制台的 HTTP 访问
443.	HTTPS	提供从客户端 Web 浏览器到云管理器 Web 控制台的 HTTPS 访问

### 云管理器的出站规则

为 Cloud Manager 预定义的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

为 Cloud Manager 预定义的安全组包括以下出站规则。

Port	协议	目的
全部	所有 TCP	所有出站流量
全部	所有 UDP	所有出站流量

#### 高级出站规则

如果您需要严格的出站流量规则、则可以使用以下信息仅打开 Cloud Manager 出站通信所需的端口。



源 IP 地址是 Cloud Manager 主机。

服务	Port	协议	目标	目的
Active Directory	88	TCP	Active Directory 目录林	Kerberos V 身份验证
	139.	TCP	Active Directory 目录林	NetBIOS 服务会话
	389.	TCP	Active Directory 目录林	LDAP
	445	TCP	Active Directory 目录林	Microsoft SMB/CIFS over TCP (通过 TCP) 和 NetBIOS 成帧
	464.	TCP	Active Directory 目录林	Kerberos V 更改和设置密码 (set_change)
	749	TCP	Active Directory 目录林	Active Directory Kerberos V 更改和设置密码 (RPCSEC_GSS)
	137.	UDP	Active Directory 目录林	NetBIOS 名称服务
	138.	UDP	Active Directory 目录林	NetBIOS 数据报服务
	464.	UDP	Active Directory 目录林	Kerberos 密钥管理
API 调用和 AutoSupport	443.	HTTPS	出站 Internet 和 ONTAP 集群管理 LIF	API 调用 AWS 和 ONTAP、并将 AutoSupport 消息发送到 NetApp
API 调用	3000	TCP	ONTAP 集群管理 LIF	API 调用 ONTAP
DNS	53.	UDP	DNS	用于云管理器进行 DNS 解析

## Cloud Volumes ONTAP 的规则

Cloud Volumes ONTAP 的安全组需要入站和出站规则。

### 单节点系统的入站规则

除非问题描述注意到它会阻止特定入站流量，否则以下规则允许流量。

优先级和名称	端口和协议	源和目标	Description
1000 个 inbound_ssh	22 TCP	任意到任意	SSH 访问集群管理 LIF 或节点管理 LIF 的 IP 地址

优先级和名称	端口和协议	源和目标	Description
1001 inbound_http	80/TCP	任意到任意	使用集群管理 LIF 的 IP 地址对系统管理器 Web 控制台进行 HTTP 访问
1002 inbound_111_tcp	111 TCP	任意到任意	远程过程调用 NFS
1003 入站_111_UDP	111 UDP	任意到任意	远程过程调用 NFS
1004 inbound_139	139 TCP	任意到任意	用于 CIFS 的 NetBIOS 服务会话
1005 inbound_161-162_TCP	161-162 TCP	任意到任意	简单网络管理协议
1006 inbound_161-162_UDP	161-162 UDP	任意到任意	简单网络管理协议
1007 inbound_443	443/TCP	任意到任意	使用集群管理 LIF 的 IP 地址对 System Manager Web 控制台进行 HTTPS 访问
1008 inbound_445	445 TCP	任意到任意	Microsoft SMB/CIFS over TCP (通过 TCP) 和 NetBIOS 成帧
1009 inbound_635_tcp	635 TCP	任意到任意	NFS 挂载
1010 inbound_635_udp	635 UDP	任意到任意	NFS 挂载
1011 inbound_749	749 TCP	任意到任意	Kerberos
1012 inbound_2049_tcp	2049 TCP	任意到任意	NFS 服务器守护进程
1013 inbound_2049_udp	2049 UDP	任意到任意	NFS 服务器守护进程
1014 inbound_3260	3260 TCP	任意到任意	通过 iSCSI 数据 LIF 进行 iSCSI 访问
1015 Inbound_4045-4046_tcp	4045-4046 TCP	任意到任意	NFS 锁定守护进程和网络状态监控器
1016 inbound_4045-4046_udp	4045-4046 UDP	任意到任意	NFS 锁定守护进程和网络状态监控器
1017 inbound_10000	10000 TCP	任意到任意	使用 NDMP 备份
1018 inbound_11104-11105	11104-11105 TCP	任意到任意	SnapMirror 数据传输
3000 个 inbound_deny_all_tcp	任何端口 TCP	任意到任意	阻止所有其他 TCP 入站流量
3001 inbound_deny_all_udp	任何端口 UDP	任意到任意	阻止所有其他 UDP 入站流量
65000 个 AllowVnetInBound	任何端口任何协议	VirtualNetwork 到 VirtualNetwork	vNet 中的入站流量
65001 AllowAzureLoad BalancerInBound	任何端口任何协议	AzureLoadBalancer 到任何	来自 Azure 标准负载均衡器的数据流量

优先级和名称	端口和协议	源和目标	Description
65500 DenyAllInBound	任何端口任何协议	任意到任意	阻止所有其他入站流量

## HA 系统的入站规则

除非问题描述注意到它会阻止特定入站流量，否则以下规则允许流量。



与单节点系统相比，HA 系统的入站规则更少，因为入站数据流量通过 Azure 标准负载均衡器。因此，来自负载均衡器的流量应处于打开状态，如 "AllowAzureLoadBalancerInBound" 规则中所示。

优先级和名称	端口和协议	源和目标	Description
100 inbound_443	443 任何协议	任意到任意	使用集群管理 LIF 的 IP 地址对 System Manager Web 控制台进行 HTTPS 访问
101 inbound_111_tcp	111 任何协议	任意到任意	远程过程调用 NFS
102 inbound_2049_tcp	2049 任何协议	任意到任意	NFS 服务器守护进程
111 inbound_ssh	22 任何协议	任意到任意	SSH 访问集群管理 LIF 或节点管理 LIF 的 IP 地址
121 inbound_53	53 任何协议	任意到任意	DNS 和 CIFS
65000 个 AllowVnetInBound	任何端口任何协议	VirtualNetwork 到 VirtualNetwork	vNet 中的入站流量
65001 AllowAzureLoad BalancerInBound	任何端口任何协议	AzureLoadBalancer 到任何	来自 Azure 标准负载均衡器的数据流量
65500 DenyAllInBound	任何端口任何协议	任意到任意	阻止所有其他入站流量

## Cloud Volumes ONTAP 的出站规则

为 Cloud Volumes ONTAP 预定义的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

为 Cloud Volumes ONTAP 预定义的安全组包括以下出站规则。

Port	协议	目的
全部	所有 TCP	所有出站流量
全部	所有 UDP	所有出站流量

### 高级出站规则

如果您需要严格的出站流量规则、则可以使用以下信息仅打开 Cloud Volumes ONTAP 出站通信所需的端口。



源是 Cloud Volumes ONTAP 系统上的接口（IP 地址）。

服务	Port	协议	源	目标	目的	
Active Directory	88	TCP	节点管理 LIF	Active Directory 目录林	Kerberos V 身份验证	
	137.	UDP	节点管理 LIF	Active Directory 目录林	NetBIOS 名称服务	
	138.	UDP	节点管理 LIF	Active Directory 目录林	NetBIOS 数据报服务	
	139.	TCP	节点管理 LIF	Active Directory 目录林	NetBIOS 服务会话	
	389.	TCP	节点管理 LIF	Active Directory 目录林	LDAP	
	445	TCP	节点管理 LIF	Active Directory 目录林	Microsoft SMB/CIFS over TCP（通过 TCP）和 NetBIOS 成帧	
	464.	TCP	节点管理 LIF	Active Directory 目录林	Kerberos V 更改和设置密码（set_change）	
	464.	UDP	节点管理 LIF	Active Directory 目录林	Kerberos 密钥管理	
	749	TCP	节点管理 LIF	Active Directory 目录林	Kerberos V 更改和设置密码（RPCSEC_GSS）	
	88	TCP	数据 LIF（NFS、CIFS）	Active Directory 目录林	Kerberos V 身份验证	
	137.	UDP	数据 LIF（NFS、CIFS）	Active Directory 目录林	NetBIOS 名称服务	
	138.	UDP	数据 LIF（NFS、CIFS）	Active Directory 目录林	NetBIOS 数据报服务	
	139.	TCP	数据 LIF（NFS、CIFS）	Active Directory 目录林	NetBIOS 服务会话	
	389.	TCP	数据 LIF（NFS、CIFS）	Active Directory 目录林	LDAP	
	445	TCP	数据 LIF（NFS、CIFS）	Active Directory 目录林	Microsoft SMB/CIFS over TCP（通过 TCP）和 NetBIOS 成帧	
	464.	TCP	数据 LIF（NFS、CIFS）	Active Directory 目录林	Kerberos V 更改和设置密码（set_change）	
	464.	UDP	数据 LIF（NFS、CIFS）	Active Directory 目录林	Kerberos 密钥管理	
	749	TCP	数据 LIF（NFS、CIFS）	Active Directory 目录林	Kerberos V 更改和设置密码（RPCSEC_GSS）	
	DHCP	68	UDP	节点管理 LIF	DHCP	首次设置 DHCP 客户端
	DHCP	67	UDP	节点管理 LIF	DHCP	DHCP 服务器

服务	Port	协议	源	目标	目的
DNS	53.	UDP	节点管理 LIF 和数据 LIF ( NFS 、 CIFS )	DNS	DNS
NDMP	18600 – 18699	TCP	节点管理 LIF	目标服务器	NDMP 副本
SMTP	25.	TCP	节点管理 LIF	邮件服务器	SMTP 警报、可用于 AutoSupport
SNMP	161.	TCP	节点管理 LIF	监控服务器	通过 SNMP 陷阱进行监控
	161.	UDP	节点管理 LIF	监控服务器	通过 SNMP 陷阱进行监控
	162.	TCP	节点管理 LIF	监控服务器	通过 SNMP 陷阱进行监控
	162.	UDP	节点管理 LIF	监控服务器	通过 SNMP 陷阱进行监控
SnapMirror	11104.	TCP	集群间 LIF	ONTAP 集群间 LIF	管理 SnapMirror 的集群间通信会话
	11105.	TCP	集群间 LIF	ONTAP 集群间 LIF	SnapMirror 数据传输
系统日志	514.	UDP	节点管理 LIF	系统日志服务器	系统日志转发消息

## GCP 的防火墙规则

Cloud Manager 可创建包含 Cloud Manager 和 Cloud Volumes ONTAP 成功运行所需的入站和出站规则的 GCP 防火墙规则。您可能希望参考这些端口进行测试或使用自己的安全组。

### 云管理器规则

Cloud Manager 的防火墙规则需要入站和出站规则。

#### 云管理器的入站规则

预定义的防火墙规则中的入站规则源为 0.0.0.0/0 。

协议	Port	目的
SSH	22.	提供对云管理器主机的 SSH 访问
HTTP	80	提供从客户端 Web 浏览器到云管理器 Web 控制台的 HTTP 访问
HTTPS	443.	提供从客户端 Web 浏览器到云管理器 Web 控制台的 HTTPS 访问

#### 云管理器的出站规则

为 Cloud Manager 预定义的防火墙规则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

Cloud Manager 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

如果您需要严格的出站流量规则、则可以使用以下信息仅打开 Cloud Manager 出站通信所需的端口。



源 IP 地址是 Cloud Manager 主机。

服务	协议	Port	目标	目的
Active Directory	TCP	88	Active Directory 目录林	Kerberos V 身份验证
	TCP	139.	Active Directory 目录林	NetBIOS 服务会话
	TCP	389.	Active Directory 目录林	LDAP
	TCP	445	Active Directory 目录林	Microsoft SMB/CIFS over TCP (通过 TCP) 和 NetBIOS 成帧
	TCP	464.	Active Directory 目录林	Kerberos V 更改和设置密码 (set_change)
	TCP	749	Active Directory 目录林	Active Directory Kerberos V 更改和设置密码 (RPCSEC_GSS)
	UDP	137.	Active Directory 目录林	NetBIOS 名称服务
	UDP	138.	Active Directory 目录林	NetBIOS 数据报服务
	UDP	464.	Active Directory 目录林	Kerberos 密钥管理
API 调用和 AutoSupport	HTTPS	443.	出站 Internet 和 ONTAP 集群管理 LIF	API 调用 GCP 和 ONTAP、并将 AutoSupport 消息发送到 NetApp
API 调用	TCP	3000	ONTAP 集群管理 LIF	API 调用 ONTAP
DNS	UDP	53.	DNS	用于云管理器进行 DNS 解析



## Cloud Volumes ONTAP 的规则

Cloud Volumes ONTAP 的安全组需要入站和出站规则。

### Cloud Volumes ONTAP 的入站规则

预定义安全组中入站规则的源代码为 0.0.0.0/0 。

协议	Port	目的
所有 ICMP	全部	Ping 实例
HTTP	80	使用集群管理 LIF 的 IP 地址对系统管理器 Web 控制台进行 HTTP 访问
HTTPS	443.	使用集群管理 LIF 的 IP 地址对 System Manager Web 控制台进行 HTTPS 访问
SSH	22.	SSH 访问集群管理 LIF 或节点管理 LIF 的 IP 地址
TCP	111.	远程过程调用 NFS
TCP	139.	用于 CIFS 的 NetBIOS 服务会话
TCP	161-162.	简单网络管理协议
TCP	445	Microsoft SMB/CIFS over TCP (通过 TCP ) 和 NetBIOS 成帧
TCP	635	NFS 挂载
TCP	749	Kerberos
TCP	2049.	NFS 服务器守护进程
TCP	3260	通过 iSCSI 数据 LIF 进行 iSCSI 访问
TCP	4045	NFS 锁定守护进程
TCP	4046	NFS 的网络状态监视器
TCP	10000	使用 NDMP 备份
TCP	11104.	管理 SnapMirror 的集群间通信会话
TCP	11105.	使用集群间 LIF 进行 SnapMirror 数据传输
UDP	111.	远程过程调用 NFS
UDP	161-162.	简单网络管理协议
UDP	635	NFS 挂载
UDP	2049.	NFS 服务器守护进程
UDP	4045	NFS 锁定守护进程
UDP	4046	NFS 的网络状态监视器
UDP	4049.	NFS Rquotad 协议

### Cloud Volumes ONTAP 的出站规则

为 Cloud Volumes ONTAP 预定义的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

为 Cloud Volumes ONTAP 预定义的安全组包括以下出站规则。

协议	Port	目的
所有 ICMP	全部	所有出站流量
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

如果您需要严格的出站流量规则、则可以使用以下信息仅打开 Cloud Volumes ONTAP 出站通信所需的端口。



源是 Cloud Volumes ONTAP 系统上的接口（IP 地址）。

服务	协议	Port	源	目标	目的
Active Directory	TCP	88	节点管理 LIF	Active Directory 目录林	Kerberos V 身份验证
	UDP	137.	节点管理 LIF	Active Directory 目录林	NetBIOS 名称服务
	UDP	138.	节点管理 LIF	Active Directory 目录林	NetBIOS 数据报服务
	TCP	139.	节点管理 LIF	Active Directory 目录林	NetBIOS 服务会话
	TCP	389.	节点管理 LIF	Active Directory 目录林	LDAP
	TCP	445	节点管理 LIF	Active Directory 目录林	Microsoft SMB/CIFS over TCP (通过 TCP) 和 NetBIOS 成帧
	TCP	464.	节点管理 LIF	Active Directory 目录林	Kerberos V 更改和设置密码 (set_change)
	UDP	464.	节点管理 LIF	Active Directory 目录林	Kerberos 密钥管理
	TCP	749	节点管理 LIF	Active Directory 目录林	Kerberos V 更改和设置密码 (RPCSEC_GSS)
	TCP	88	数据 LIF (NFS、CIFS)	Active Directory 目录林	Kerberos V 身份验证
	UDP	137.	数据 LIF (NFS、CIFS)	Active Directory 目录林	NetBIOS 名称服务
	UDP	138.	数据 LIF (NFS、CIFS)	Active Directory 目录林	NetBIOS 数据报服务
	TCP	139.	数据 LIF (NFS、CIFS)	Active Directory 目录林	NetBIOS 服务会话
	TCP	389.	数据 LIF (NFS、CIFS)	Active Directory 目录林	LDAP
	TCP	445	数据 LIF (NFS、CIFS)	Active Directory 目录林	Microsoft SMB/CIFS over TCP (通过 TCP) 和 NetBIOS 成帧
	TCP	464.	数据 LIF (NFS、CIFS)	Active Directory 目录林	Kerberos V 更改和设置密码 (set_change)
	UDP	464.	数据 LIF (NFS、CIFS)	Active Directory 目录林	Kerberos 密钥管理
	TCP	749	数据 LIF (NFS、CIFS)	Active Directory 目录林	Kerberos V 更改和设置密码 (RPCSEC_GSS)

服务	协议	Port	源	目标	目的
集群	所有流量	所有流量	一个节点上的所有 LIF	其它节点上的所有 LIF	集群间通信（仅限 Cloud Volumes ONTAP HA）
	TCP	3000	节点管理 LIF	HA 调解器	ZAPI 调用（仅适用于 Cloud Volumes ONTAP HA）
	ICMP	1.	节点管理 LIF	HA 调解器	保持活动状态（仅限 Cloud Volumes ONTAP HA）
DHCP	UDP	68	节点管理 LIF	DHCP	首次设置 DHCP 客户端
DHCP	UDP	67	节点管理 LIF	DHCP	DHCP 服务器
DNS	UDP	53.	节点管理 LIF 和数据 LIF（NFS、CIFS）	DNS	DNS
NDMP	TCP	18600 – 18699	节点管理 LIF	目标服务器	NDMP 副本
SMTP	TCP	25.	节点管理 LIF	邮件服务器	SMTP 警报、可用于 AutoSupport
SNMP	TCP	161.	节点管理 LIF	监控服务器	通过 SNMP 陷阱进行监控
	UDP	161.	节点管理 LIF	监控服务器	通过 SNMP 陷阱进行监控
	TCP	162.	节点管理 LIF	监控服务器	通过 SNMP 陷阱进行监控
	UDP	162.	节点管理 LIF	监控服务器	通过 SNMP 陷阱进行监控
SnapMirror	TCP	11104.	集群间 LIF	ONTAP 集群间 LIF	管理 SnapMirror 的集群间通信会话
	TCP	11105.	集群间 LIF	ONTAP 集群间 LIF	SnapMirror 数据传输
系统日志	UDP	514.	节点管理 LIF	系统日志服务器	系统日志转发消息

## 适用于 Cloud Manager 和 Cloud Volumes ONTAP 的 AWS Marketplace 页面

AWS Marketplace for Cloud Manager 和 Cloud Volumes ONTAP 提供了多种产品。如果您不确定需要使用哪个页面，请阅读下面的内容，我们将根据您的目标引导您转到正确的页面。

在所有情况下，请记住，您不能从 AWS Marketplace 在 AWS 中启动 Cloud Volumes ONTAP。您需要直接从 Cloud Manager 启动它。

目标	要使用的 <b>AWS Marketplace</b> 页面	更多信息
为 9.6 及更高版本启用 Cloud Volumes ONTAP PAYGO 部署	" <a href="#">Cloud Manager（适用于 Cloud Volumes ONTAP）</a> "	通过此 AWS Marketplace 页面，可以为 Cloud Volumes ONTAP 9.6 及更高版本的 PAYGO 版本收费。它还支持为 Cloud Volumes ONTAP 附加功能收费。此页面不允许您在 AWS 中启动 Cloud Manager。此操作应通过完成 " <a href="#">NetApp Cloud Central</a> " 或使用此表第 4 行列出的 AMI。
为 Cloud Volumes ONTAP 启用附加功能（PAYGO 或 BYOL）		
使用我从 NetApp 购买的许可证（BYOL）部署 Cloud Volumes ONTAP	<ul style="list-style-type: none"> <li>• "<a href="#">适用于 AWS 的 Cloud Volumes ONTAP（BYOL）</a>"</li> <li>• "<a href="#">适用于 AWS 的 Cloud Volumes ONTAP —高可用性（BYOL）</a>"</li> </ul>	通过这些 AWS Marketplace 页面，您可以订阅单节点或 HA 版本的 Cloud Volumes ONTAP BYOL。
使用 AMI 从 AWS Marketplace 部署 Cloud Manager	" <a href="#">NetApp Cloud Manager（适用于 NetApp Cloud Volumes ONTAP）</a> "	我们建议您从中启动 AWS 中的 Cloud Manager " <a href="#">NetApp Cloud Central</a> "，但您可以根据需要从此 AWS Marketplace 页面启动它。
启用 Cloud Volumes ONTAP PAYGO（9.5 或更早版本）的部署	<ul style="list-style-type: none"> <li>• "<a href="#">适用于 AWS 的 Cloud Volumes ONTAP</a>"</li> <li>• "<a href="#">适用于 AWS 的 Cloud Volumes ONTAP —高可用性</a>"</li> </ul>	您可以通过这些 AWS Marketplace 页面订阅 Cloud Volumes ONTAP PAYGO 9.5 及更早版本的单节点或 HA 版本。从 9.6 版开始，您需要通过此表第 1 行列出的 AWS Marketplace 页面为 PAYGO 部署订阅。

## Cloud Manager 如何使用云提供商权限

Cloud Manager 需要在云提供商中执行操作的权限。中包括这些权限 "[NetApp 提供的策略](#)"。您可能希望了解 Cloud Manager 使用这些权限执行的操作。

### Cloud Manager 如何使用 AWS 权限

Cloud Manager 使用 AWS 帐户对几个 AWS 服务进行 API 调用、包括 EC2、S3、Cloudformation、IAM、Security Token Service（安全令牌服务，STS）和密钥管理服务（KMS）。

操作	目的
"EC2：StartInstances"，"EC2：StopInstances"，"EC2：DescribeInstances"，"EC2：DescribeInstanceStatus"，"EC2：RunInstances"，"EC2：终端实例"，"EC2：ModifyInstanceAttribute"，	启动 Cloud Volumes ONTAP 实例并停止、启动和监控实例。
"EC2：描述实例属性"、	验证是否已为支持的实例类型启用增强网络。
"EC2：描述图"、"EC2：描述图"、	启动 Cloud Volumes ONTAP HA 配置。

操作	目的
"EC2：创建标记"、	标记 Cloud Manager 使用 "Workingviron" 和 "Workingvironmid" 标记创建的每个资源。Cloud Manager 使用这些标签进行维护和成本分配。
"EC2：CreateVolume"，"EC2：Describe Volumes"，"EC2：ModifyVolumeAttribute"，"EC2：AttachVolume"，"EC2：DeleteVolume"，"EC2：详细卷"，	管理 Cloud Volumes ONTAP 用作后端存储的 EBS 卷。
"EC2：CreateSecurityGroup"，"EC2：DeleteSecurityGroup"，"EC2：Describe SecurityGroups"，"EC2：RevokeSecurityGroupEated"，"EC2：AuthorizeSecurityGroupEated"，"EC2：AuthorizeSecurityGroupIn防护"，"EC2：RevokeSecurityGroupIn防护"，	为 Cloud Volumes ONTAP 创建预定义的安全组。
"EC2：CreateNetworkInterface"，"EC2：Describe NetworkInterfaces"，"EC2：DeleteNetworkInterface"，"EC2：ModifyNetworkInterfaceAttribute"，	在目标子网中为 Cloud Volumes ONTAP 创建和管理网络接口。
"EC2：描述性子网"、"EC2：描述性 VPCS"、	获取目标子网和安全组的列表、在为 Cloud Volumes ONTAP 创建新的工作环境时需要这些子网和安全组。
"EC2：说明"、	确定启动 Cloud Volumes ONTAP 实例时的 DNS 服务器和默认域名。
"EC2：CreateSnapshot"、"EC2：DeleteSnapshot"、"EC2：描述性快照"、	在初始设置期间和停止 Cloud Volumes ONTAP 实例时拍摄 EBS 卷的快照。
"EC2：GetConsoleOutput"、	捕获附加到 AutoSupport 消息的 Cloud Volumes ONTAP 控制台。
"EC2：描述性密钥对"、	在启动实例时获取可用密钥对的列表。
"EC2：描述性"、	获得可用 AWS 区域的列表。
"EC2：删除标记"、"EC2：描述标记"、	管理与 Cloud Volumes ONTAP 实例关联的资源标签。
"CloudFormation：CreateStack"，"CloudFormation：DeleteStack"，"CloudFormation：Describe Stacks"，"CloudFormation：Describe StackEvents"，"CloudFormation：ValidateTemplate"，	启动 Cloud Volumes ONTAP 实例。
"IAM：PassRole"，"iam：CreateRole"，"iam：DeleteRole"，"iam：PutRolePolicy"，"iam：CreateInstanceProfile"，"IAM：DeleteRolePolicy"，"iam：AddRoleToInstanceProfile"，"iam：RemoveRoleFromInstanceProfile"，"iam：DeleteInstanceProfile"，	启动 Cloud Volumes ONTAP HA 配置。
"IAM：ListInstanceProfiles"，"STS：DecodeAuthorizationMessage"，"EC2：AssociateIamInstanceProfile"，"EC2：Describe IamInstanceProfileAssociations"，"EC2：DisassociateIamInstanceProfile"，	管理 Cloud Volumes ONTAP 实例的实例配置文件。

操作	目的
"S3 : GetBucketTagging" , "S3 : GetBucketLocation" , "S3 : ListAllMyBuckets" , "S3 : ListBucket"	获取有关 AWS S3 存储槽的信息、以便 Cloud Manager 可以与 NetApp Data Fabric Cloud Sync 服务集成。
"S3 : CreateBucket" , "S3 : DeleteBucket" , "S3 : GetLifecycleConfiguration" , "S3 : PutLifecycleConfiguration" , "S3 : PutBucketTagging" , "S3 : ListBucketVersions" ,	管理 Cloud Volumes ONTAP 系统将其用作容量层的 S3 存储区。
"KMS: List*" 、 "KMS: 描述 *"	从 AWS 密钥管理服务获取有关密钥的信息。
"CE : GetReservationUtilization" , "ce : GetDimensionValues" , "ce : GetCostAndUsage" , "ce : GetTags "	获取有关 Cloud Volumes ONTAP 的 AWS 成本数据。
"EC2 : CreatePlacementGroup" , "EC2 : DeletePlacementGroup"	在单个 AWS 可用性区域中部署 HA 配置时， Cloud Manager 会启动 AWS 分布式放置组中的两个 HA 节点和调解器。

## Cloud Manager 使用 Azure 权限的功能

Cloud Manager Azure 策略包括 Cloud Manager 在 Azure 中部署和管理 Cloud Volumes ONTAP 所需的权限。

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/storageAccouns/Read" , "microsoft.Storage/storageAccounts" , "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 。

操作	目的
"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。
"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/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。

## Cloud Manager 如何使用 GCP 权限

适用于 GCP 的 Cloud Manager 策略包括 Cloud Manager 部署和管理 Cloud Volumes ONTAP 所需的权限。

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。

操作	目的
— compute.instances.setMachineType	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。
- deploymentmanager.compositeTypes.get - deploymentmanager.compositeTypes.list - deploymentmanager.deployments.create - deploymentmanager.deployments.delete - deploymentmanager.deployments.get - deploymentmanager.deployments.list - deploymentmanager.manifes.get - deploymentmanager.manifes.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.logEnrees.list — logging.privateLogEnrees.list	获取堆栈日志驱动器。
— resourcemanager.projects.get	以支持多个项目。
— storage.桶 .create — storage.buckets.delete — storage.桶 .get — storage.桶 .list	创建和管理用于数据分层的 Google Cloud Storage 存储分段。
— cloudkms.cryptoKeyVersions.useToEncrypt — cloudkms.encryptoKeys.get — cloudkms.encryptoKeys.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。

## 默认配置

有关默认情况下如何配置 Cloud Manager 和 Cloud Volumes ONTAP 的详细信息可以帮助您管理系统。

## Linux 上的 Cloud Manager 的默认配置

如果您需要排除 Cloud Manager 或 Linux 主机故障、可能有助于了解如何配置 Cloud Manager 。

- 如果您从 NetApp Cloud Central （或直接从云提供商的市场）部署 Cloud Manager ， 请注意以下事项：
  - 在 AWS 中、 EC2 Linux 实例的用户名为 EC2-user 。
  - Cloud Manager 映像的操作系统为 Red Hat Enterprise Linux 7.4 （ HVM ） 。

操作系统不包含 GUI 。您必须使用终端访问系统。

- Cloud Manager 安装文件夹位于以下位置：

```
/opt/application/netapp/cloudmanager
```

- 日志文件包含在以下文件夹中：

```
/opt/application/netapp/cloudmanager/log
```

- 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。

- 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
  - Java
  - Kubectl
  - MySQL
  - Tridentctl
  - wget

## Cloud Volumes ONTAP 的默认配置

了解默认情况下如何配置 Cloud Volumes ONTAP 可以帮助您设置和管理系统、尤其是在您熟悉 ONTAP 的情况下、因为 Cloud Volumes ONTAP 的默认设置不同于 ONTAP 。

- Cloud Volumes ONTAP 在 AWS ， Azure 和 GCP 中作为单节点系统提供，在 AWS 和 Azure 中作为 HA 对提供。
- 在部署 Cloud Volumes ONTAP 时、 Cloud Manager 会创建一个数据服务 SVM 。不支持使用多个提供数据的 SVM 。
- Cloud Manager 会自动在 Cloud Volumes ONTAP 上安装以下 ONTAP 功能许可证：
  - CIFS
  - FlexCache
  - FlexClone

- iSCSI
- NetApp 卷加密（仅适用于 BYOL 或已注册的 PAYGO 系统）
- NFS
- SnapMirror
- SnapRestore
- SnapVault
- 默认情况下会创建多个网络接口：
  - 集群管理 LIF
  - 集群间 LIF
  - Azure 中 HA 系统上的 SVM 管理 LIF ， AWS 中的单节点系统以及多个 AWS 可用性区域中的 HA 系统上的可选 SVM 管理 LIF
  - 节点管理 LIF
  - iSCSI 数据 LIF
  - CIFS 和 NFS 数据 LIF



由于 EC2 要求，默认情况下，对于 Cloud Volumes ONTAP 禁用 LIF 故障转移。将 LIF 迁移到另一个端口会中断实例上 IP 地址和网络接口之间的外部映射、从而使 LIF 无法访问。

- Cloud Volumes ONTAP 使用 HTTPS 将配置备份发送到 Cloud Manager 。

登录到 Cloud Manager 后，可以从访问备份 <https://ipaddress/occm/offboxconfig/>

- 与其他管理工具（例如 System Manager 或 CLI）不同、Cloud Manager 设置了几个卷属性。

下表列出了 Cloud Manager 设置的与默认设置不同的卷属性：

属性	由 <b>Cloud Manager</b> 设置的价值
自动调整模式	增长
最大自动大小	1,000 %  <div style="display: flex; align-items: center;">            帐户管理员可以从 " 设置 " 页面修改此值。         </div>
安全风格	适用于 CIFS 卷的 NTFS UNIX （用于 NFS 卷）
空间保证风格	无
UNIX 权限（仅限 NFS）	777.

有关这些属性的信息，请参见 *volume crese* 手册页。

## 适用于 **Cloud Volumes ONTAP** 的引导和根数据

除了用户数据存储之外，Cloud Manager 还在每个 Cloud Volumes ONTAP 系统上购买用于引导和根数据的云存储。

### **AWS**

- 两个通用 SSD 磁盘：
  - 一个 140 GB 的根数据磁盘（每个节点一个）
  - 9.6 及更高版本：一个 86 GB 的启动数据磁盘（每个节点一个）
  - 9.5 及更早版本：一个 45 GB 磁盘，用于存储启动数据（每个节点一个）
- 每个引导磁盘和根磁盘一个 EBS 快照
- 对于 HA 对，为调解器实例配置一个 EBS 卷，大约为 8 GB

### **Azure**（单节点）

- 两个高级 SSD 磁盘：
  - 一个 90 GB 磁盘，用于存储启动数据
  - 一个 140 GB 的根数据磁盘
- 每个引导磁盘和根磁盘一个 Azure 快照

### **Azure**（HA 对）

- 两个用于启动卷的 90 GB 高级 SSD 磁盘（每个节点一个）
- 根卷的两个 140 GB 高级存储页面 Blobs（每个节点一个）
- 两个 128 GB 标准 HDD 磁盘，用于节省核心（每个节点一个）
- 每个引导磁盘和根磁盘一个 Azure 快照

### **GCP**

- 一个 10 GB 标准永久性磁盘，用于存储启动数据
- 一个 64 GB 标准永久性磁盘，用于存储根数据
- 一个用于 NVRAM 的 500 GB 标准永久性磁盘
- 一个 216 GB 标准永久性磁盘，用于节省核心
- 启动磁盘和根磁盘各一个 GCP 快照

### 磁盘驻留的位置

Cloud Manager 将存储布局如下：

- 启动数据驻留在与实例或虚拟机连接的磁盘上。

此磁盘包含引导映像、但不能用于 Cloud Volumes ONTAP。

- 包含系统配置和日志的根数据驻留在 aggr0 中。
- 存储虚拟机（SVM）根卷驻留在 aggr1 中。
- 数据卷也驻留在 aggr1 中。

## 加密

启动和根磁盘在 Azure 和 Google Cloud Platform 中始终加密，因为默认情况下，这些云提供商会启用加密。

如果您在 AWS 中使用密钥管理服务（KMS）启用数据加密，则 Cloud Volumes ONTAP 的启动磁盘和根磁盘也会进行加密。这包括 HA 对中调解器实例的启动磁盘。磁盘将使用您在创建工作环境时选择的 CMK 进行加密。

## 角色

"帐户管理员"和"工作空间管理员"角色为用户提供特定权限。

任务	帐户管理员	工作空间管理员
管理工作环境	是的。	是，适用于关联的工作空间
查看数据复制状态	是的。	是，适用于关联的工作空间
查看时间表	是的。	是，适用于关联的工作空间
删除工作环境	是的。	否
将 Kubernetes 集群连接到 Cloud Volumes ONTAP	是的。	否
接收 Cloud Volumes ONTAP 报告	是的。	否
管理 Cloud Central 帐户	是的。	否
管理云提供商帐户	是的。	否
修改 Cloud Manager 设置	是的。	否
查看和管理支持仪表板	是的。	否
从 Cloud Manager 中删除工作环境	是的。	否
更新 Cloud Manager	是的。	否
安装 HTTPS 证书	是的。	否
设置 Active Directory	是的。	否

## 相关链接

- ["在 Cloud Central 帐户中设置工作空间和用户"](#)
- ["在 Cloud Central 帐户中管理工作空间和用户"](#)

## 从何处获取帮助和查找更多信息

您可以通过各种资源（包括视频、论坛和支持）获得有关 Cloud Manager 和 Cloud

## Volumes ONTAP 的帮助和详细信息。

- ["适用于 Cloud Manager 和 Cloud Volumes ONTAP 的视频"](#)

观看视频，了解如何部署和管理 Cloud Volumes ONTAP 以及如何在混合云中复制数据。

- ["云管理器策略"](#)

下载包含 Cloud Manager 在云提供商中执行操作所需权限的 JSON 文件。

- ["Cloud Manager API 开发人员指南"](#)

阅读 API 概述、如何使用这些 API 的示例以及 API 参考。

- Cloud Volumes ONTAP 培训

- ["Cloud Volumes ONTAP 基础知识"](#)
- ["适用于 Azure 的 Cloud Volumes ONTAP 部署和管理"](#)
- ["适用于 AWS 的 Cloud Volumes ONTAP 部署和管理"](#)

- 技术报告

- ["NetApp 技术报告 4383：使用应用程序工作负载在 Amazon Web Services 中对 Cloud Volumes ONTAP 进行性能特征描述"](#)
- ["NetApp 技术报告 4671：Azure 中的 Cloud Volumes ONTAP 的性能特征与应用程序工作负载"](#)

- SVM 灾难恢复

SVM 灾难恢复是将 SVM 数据和配置从源 SVM 异步镜像到目标 SVM 的过程。如果源 SVM 不再可用，您可以快速激活目标 SVM 以进行数据访问。

- ["Cloud Volumes ONTAP 9 SVM 灾难恢复准备快速指南"](#)

介绍如何快速配置目标 SVM 以准备灾难恢复。

- ["Cloud Volumes ONTAP 9 SVM 灾难恢复快速指南"](#)

介绍如何在发生灾难后快速激活目标 SVM、然后重新激活源 SVM。

- ["《FlexCache 卷加快数据访问高级指南》"](#)

介绍如何在与原始卷相同的集群或不同的集群中创建和管理 FlexCache 卷以加快数据速度 access.es 如何在发生灾难后快速激活目标 SVM，然后重新激活源 SVM。

- ["安全建议"](#)

确定包括 ONTAP 在内的 NetApp 产品的已知漏洞（CVE）。请注意，您可以按照 ONTAP 文档修复 Cloud Volumes ONTAP 的安全漏洞。

- ["ONTAP 9 文档中心"](#)

访问 ONTAP 的产品文档、它可以帮助您使用 Cloud Volumes ONTAP。

- ["NetApp Cloud Volumes ONTAP 支持"](#)

访问支持资源以获得有关 Cloud Volumes ONTAP 的帮助和故障排除问题。

- ["NetApp 社区：云数据服务"](#)

与同行联系、提出问题、交换意见、查找资源并共享最佳实践。

- ["NetApp Cloud Central"](#)

查找有关适用于云的其他 NetApp 产品和解决方案的信息。

- ["NetApp 产品文档"](#)

在 NetApp 产品文档中搜索说明、资源和答案。



# 早期版本的 **Cloud Manager** 文档

如果您没有运行最新版本，则可以获得以前版本的 Cloud Manager 的文档。

["Cloud Manager 3.6"](#)

# 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。

- ["Cloud Manager 3.7.4 注意事项"](#)
- ["Cloud Manager 3.7.1 注意事项"](#)
- ["有关 Cloud Manager 3.7 的注意事项"](#)
- ["Cloud Backup Service 注意事项"](#)

## 版权信息

版权所有 © 2024 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

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

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

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

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

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

## 商标信息

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