系统管理
Cloud Volumes ONTAP

NetApp
February 19, 2026

This PDF was generated from https://docs.netapp.com/zh-cn/storage-management-cloud-volumes-ontap/task-updating-ontap-cloud.html on February 19, 2026. Always check docs.netapp.com for the latest.

目录

系统管理 1
升级Cloud Volumes ONTAP 1
升级概述 1
准备升级 5
升级Cloud Volumes ONTAP 7
修复使用 Google Cloud NAT 网关时下载失败的问题 10
注册Cloud Volumes ONTAP即用即付系统 11
将Cloud Volumes ONTAP基于节点的许可证转换为基于容量的许可证 13
不同超标量中的定价 14
启动和停止Cloud Volumes ONTAP系统 15
安排Cloud Volumes ONTAP自动关闭 15
停止Cloud Volumes ONTAP 17
使用 NTP 服务器同步Cloud Volumes ONTAP系统时间 18
修改系统写入速度 18
更改Cloud Volumes ONTAP集群管理员密码 19
添加、移除或删除系统 20
将现有的Cloud Volumes ONTAP系统添加到NetApp Console 20
从NetApp Console中删除Cloud Volumes ONTAP系统 21
从NetApp Console删除Cloud Volumes ONTAP系统 21
AWS 管理 22
修改 AWS 中Cloud Volumes ONTAP系统的 EC2 实例类型 22
修改多个 AWS AZ 中的Cloud Volumes ONTAP HA 对的路由表 25
Azure 管理 25
更改Cloud Volumes ONTAP的 Azure VM 类型 25
覆盖 Azure 中Cloud Volumes ONTAP HA 对的 CIFS 锁 26
为Cloud Volumes ONTAP系统使用 Azure Private Link 或服务端点 27
在 Azure 控制台中移动Cloud Volumes ONTAP的 Azure 资源组 31
在 Azure 中隔离SnapMirror流量 31
Google Cloud 管理 37
更改Cloud Volumes ONTAP的 Google Cloud 机器类型 37
将现有 Cloud Volumes ONTAP 部署转换为 Infrastructure Manager 38
使用系统管理器管理Cloud Volumes ONTAP 44
功能 44
支持的配置 44
限制 44
配置访问系统管理器的身份验证 45
开始使用系统管理器 45
有关使用系统管理器的帮助 46
从 CLI 管理Cloud Volumes ONTAP 46

系统管理

升级Cloud Volumes ONTAP

从NetApp Console升级Cloud Volumes ONTAP以获取最新的功能和增强功能。在升级软件之前，您应该准备好Cloud Volumes ONTAP系统。

升级概述

在开始Cloud Volumes ONTAP升级过程之前，您应该注意以下事项。

仅从控制台升级

您不应使用ONTAP系统管理器或ONTAP CLI 升级Cloud Volumes ONTAP ，而应仅使用控制台升级。否则可能会影响系统稳定性。

控制台提供了两种升级Cloud Volumes ONTAP 的方法：

- 通过关注系统上显示的升级通知
- 通过将升级映像放置在 HTTPS 位置，然后向控制台提供 URL

支持的升级路径

您可以升级的 Cloud Volumes ONTAP 版本取决于您当前运行的版本。下表中发行版中的每个通用版本或修补程序版本表示可用于升级的基本版本。有关可用修补程序的详细信息，请参见每个版本的 "版本化发行说明"。

支持的 **AWS** 升级路径

当前版本	可直接升级到的版本
9.17.1 P1	9.18.1
9.16.1	9.17.1 P1
9.15.1	9.16.1
9.15.0	9.15.1
9.14.1	9.15.1
	9.15.0
9.14.0	9.14.1
9.13.1	9.14.1
	9.14.0
9.13.0	9.13.1
9.12.1	9.13.1
	9.13.0
9.12.0	9.12.1

当前版本	可直接升级到的版本
9.11.1	9.12.1
	9.12.0
9.11.0	9.11.1
9.10.1	9.11.1
	9.11.0
9.10.0	9.10.1
9.9.1	9.10.1
	9.10.0
9.9.0	9.9.1
9.8	9.9.1
9.7	9.8
9.6	9.7
9.5	9.6
9.4	9.5
9.3	9.4
9.2	9.3
9.1	9.2
9.0	9.1
8.3	9.0

Azure 支持的升级路径

当前版本	可直接升级到的版本
9.17.1 P1	9.18.1
9.16.1 P3	9.17.1 P1
9.15.1 P10	9.16.1 P3
9.14.1 P13	9.15.1 P10
9.13.1 P16	9.14.1 P13
9.12.1 P18	9.13.1 P16
9.11.1 P20	9.12.1 P18

如果您在 Azure 中拥有较低版本的Cloud Volumes ONTAP ，则必须首先升级到下一个版本，然后按照支持的升级路径达到目标版本。例如，如果您有Cloud Volumes ONTAP 9.7 P7，请遵循以下升级路径：

- 9.7 P7 → 9.8 P18
- 9.8 P18 → 9.9.1 P15

- 9.9.1 P15 → 9.10.1 P12
- 9.10.1 P12 → 9.11.1 P20

支持的 **Google Cloud** 升级路径

当前版本	可直接升级到的版本
9.17.1 P1	9.18.1
9.16.1	9.17.1 P1
9.15.1	9.16.1
9.15.0	9.15.1
9.14.1	9.15.1
	9.15.0
9.14.0	9.14.1
9.13.1	9.14.1
	9.14.0
9.13.0	9.13.1
9.12.1	9.13.1
	9.13.0
9.12.0	9.12.1
9.11.1	9.12.1
	9.12.0
9.11.0	9.11.1
9.10.1	9.11.1
	9.11.0
9.10.0	9.10.1
9.9.1	9.10.1
	9.10.0
9.9.0	9.9.1
9.8	9.9.1
9.7	9.8
9.6	9.7
9.5	9.6
9.4	9.5
9.3	9.4
9.2	9.3
9.1	9.2

当前版本	可直接升级到的版本
9.0	9.1
8.3	9.0

请注意以下事项：

- Cloud Volumes ONTAP支持的升级路径与本地ONTAP集群支持的升级路径不同。
- 如果您按照系统中出现的通知进行升级，控制台将提示您升级到遵循这些支持的升级路径的版本。
- 如果通过将升级映像放置在 HTTPS 位置来进行升级，请务必遵循这些支持的升级路径。
- 在某些情况下，您可能需要升级几次才能达到目标版本。

  例如，如果您正在运行版本 9.8 并且想要升级到 9.10.1，则首先需要升级到版本 9.9.1，然后再升级到 9.10.1。

补丁版本

从 2024 年 1 月开始，仅当Cloud Volumes ONTAP的三个最新版本发布补丁时才可进行补丁升级。当 RC 或 GA 版本无法部署时，偶尔会有补丁版本可供部署。

我们使用最新的 GA 版本来确定要在控制台中显示的最新版本。例如，如果当前 GA 版本是 9.13.1，则控制台中会出现 9.11.1-9.13.1 的补丁。

对于补丁版本 9.11.1 或更低版本，您需要使用手动升级程序下载ONTAP映像。

作为补丁版本的一般规则，您可以从较低的补丁版本升级到相同或下一个Cloud Volumes ONTAP版本中的任何较高补丁版本。

以下是几个例子：

- 9.13.0 → 9.13.1 P15
- 9.12.1 → 9.13.1 P2

恢复或降级

不支持将Cloud Volumes ONTAP恢复或降级到以前的版本。

支持注册

必须在NetApp支持处注册Cloud Volumes ONTAP才能使用本页描述的任何方法升级软件。这适用于现收现付（PAYGO）和自带许可证（BYOL）。你需要"手动注册PAYGO系统"，而 BYOL 系统是默认注册的。

未注册支持的系统仍会在有新版本可用时收到控制台中出现的软件更新通知。但您需要先注册系统才能升级软件。

HA 调解器的升级

控制台还会在Cloud Volumes ONTAP升级过程中根据需要更新中介实例。

使用 **c4**、**m4** 和 **r4 EC2** 实例类型在 **AWS** 中进行升级

Cloud Volumes ONTAP不再支持 c4、m4 和 r4 EC2 实例类型。您可以使用这些实例类型将现有部署升级到Cloud Volumes ONTAP版本 9.8-9.12.1。升级之前，我们建议您更改实例类型。如果您无法更改实例类型，则需要启用增强联网升级之前。阅读以下部分以了解有关更改实例类型和启用增强联网的更多信息。

在运行 9.13.0 及更高版本的Cloud Volumes ONTAP中，您无法使用 c4、m4 和 r4 EC2 实例类型进行升级。在这种情况下，您需要减少磁盘数量，然后更改实例类型或者部署具有 c5、m5 和 r5 EC2 实例类型的新 HA 对配置并迁移数据。

更改实例类型

c4、m4 和 r4 EC2 实例类型允许每个节点拥有比 c5、m5 和 r5 EC2 实例类型更多的磁盘。如果您正在运行的 c4、m4 或 r4 EC2 实例每个节点的磁盘数低于 c5、m5 和 r5 实例每个节点的最大磁盘限额，则可以将 EC2 实例类型更改为 c5、m5 或 r5。

"检查 EC2 实例的磁盘和分层限制" "更改Cloud Volumes ONTAP的 EC2 实例类型"

如果您无法更改实例类型，请按照[启用增强联网]。

启用增强联网

要升级到Cloud Volumes ONTAP 9.8 及更高版本，您必须在运行 c4、m4 或 r4 实例类型的集群上启用_增强网络_。要启用 ENA，请参阅知识库文章"如何在 AWS Cloud Volumes ONTAP实例上启用 SR-IOV 或 ENA 等增强网络"。

准备升级

在执行升级之前，您必须验证系统已准备就绪并进行任何必要的配置更改。

- [规划停机时间]
- [验证自动交还是否仍然启用]
- 暂停SnapMirror传输
- [验证聚合是否在线]
- 验证所有 LIF 是否位于主端口

规划停机时间

升级单节点系统时，升级过程会使系统离线最多 25 分钟，在此期间 I/O 会中断。

在许多情况下，升级 HA 对不会造成中断，并且 I/O 也不会中断。在此无中断升级过程中，每个节点都会同步升级，以继续为客户端提供 I/O 服务。

面向会话的协议在升级过程中可能会对某些区域的客户端和应用程序造成不利影响。有关详细信息，请参阅 "ONTAP 文档"

验证自动交还是否仍然启用

必须在Cloud Volumes ONTAP HA 对上启用自动交还（这是默认设置）。如果不是，则操作将失败。

"ONTAP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的传输。

尽管NetApp Backup and Recovery使用SnapMirror的实现来创建备份文件（称为SnapMirror Cloud），但在系统升级时无需暂停备份。

关于此任务

以下步骤介绍了如何使用ONTAP System Manager 9.3 及更高版本。

步骤

1. 从目标系统登录到系统管理器。

   您可以通过将 Web 浏览器指向集群管理 LIF 的 IP 地址来登录系统管理器。您可以在Cloud Volumes ONTAP系统中找到 IP 地址。

   您从中访问控制台的计算机必须具有与Cloud Volumes ONTAP 的网络连接。例如，您可能需要从云提供商网络中的跳转主机登录到控制台。

2. 单击*保护>关系*。
3. 选择关系并单击*操作>静默*。

验证聚合是否在线

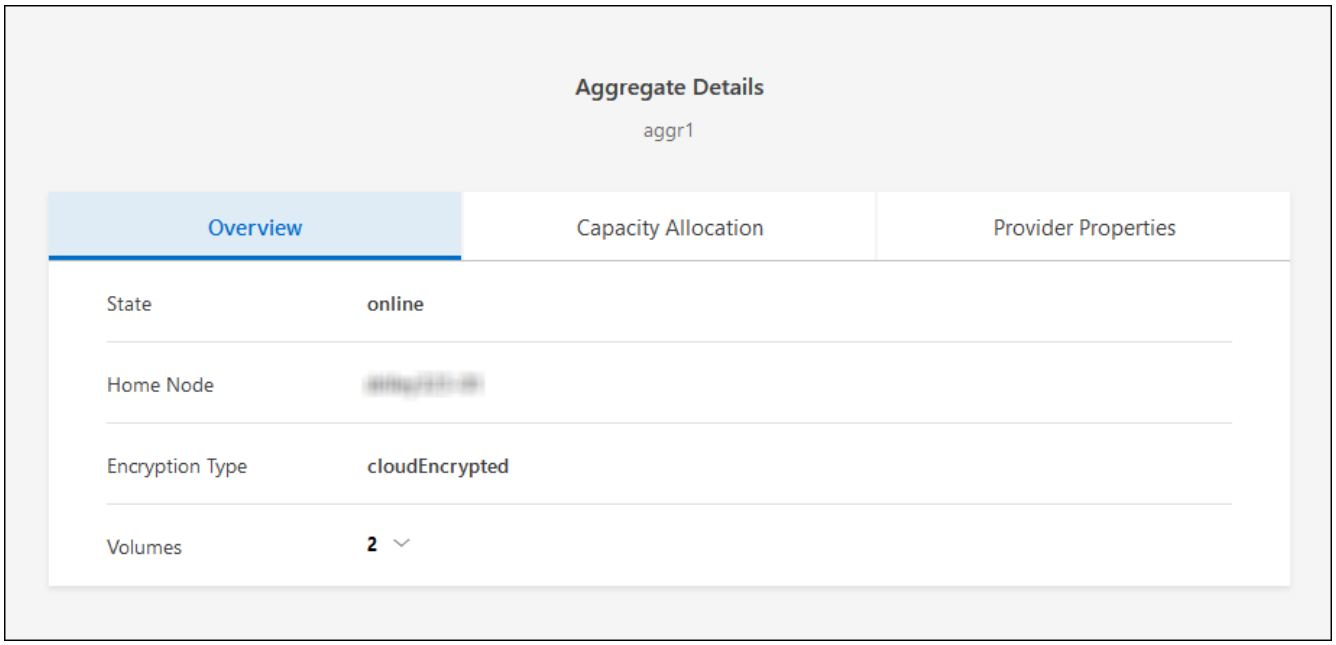
在更新软件之前， Cloud Volumes ONTAP的聚合必须处于在线状态。在大多数配置中，聚合应该处于在线状态，但如果没有，则应将其置于在线状态。

关于此任务

以下步骤介绍了如何使用ONTAP System Manager 9.3 及更高版本。

步骤

1. 在Cloud Volumes ONTAP系统上，单击 **Aggregates** 选项卡。
2. 在所需的聚合图块上，单击 ••• 图标，然后选择*查看汇总详情*。



3. 如果聚合处于脱机状态，请使用ONTAP系统管理器使聚合处于联机状态：
   a. 单击“存储”>“聚合和磁盘”>“聚合”。
   b. 选择聚合，然后单击*更多操作>状态>在线*。

验证所有 **LIF** 是否位于主端口

升级之前，所有 LIF 必须位于主端口上。请参阅ONTAP文档"验证所有 LIF 是否位于主端口"。

如果出现升级失败错误，请查阅知识库 (KB) 文章"Cloud Volumes ONTAP升级失败"。

升级Cloud Volumes ONTAP

当有新版本可供升级时，控制台会通知您。您可以从此通知开始升级过程。有关更多信息，请参阅[从控制台通知升级] 。

执行软件升级的另一种方法是使用外部 URL 上的图像。如果控制台无法访问 S3 存储桶来升级软件或者您获得了补丁，则此选项很有用。有关更多信息，请参阅通过 URL 上的可用图像进行升级 。

从控制台通知升级

当有新版本的Cloud Volumes ONTAP Cloud Volumes ONTAP工作环境中显示通知：

您必须拥有NetApp支持站点帐户，然后才能通过通知升级Cloud Volumes ONTAP 。

您可以从此通知开始升级过程，该通知通过从 S3 存储桶获取软件映像、安装映像，然后重新启动系统来自动执行该过程。

开始之前

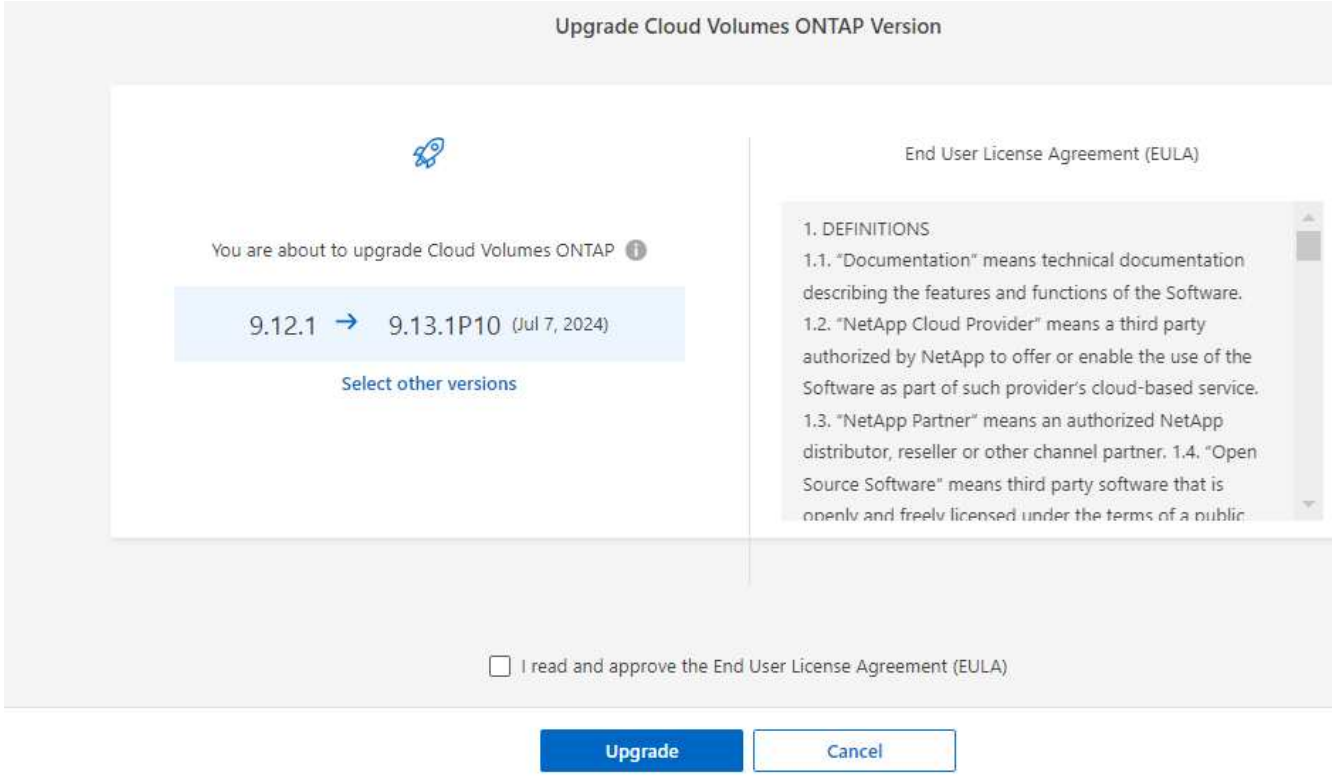
Cloud Volumes ONTAP系统上不得进行卷或聚合创建等操作。

步骤

1. 从左侧导航菜单中，选择“存储”>“管理”。
2. 选择一个Cloud Volumes ONTAP系统。

   如果有新版本可用，概览选项卡中会出现通知：

3. 如果要升级已安装的Cloud Volumes ONTAP版本，请单击“立即升级！”默认情况下，您会看到最新的、兼容的升级版本。

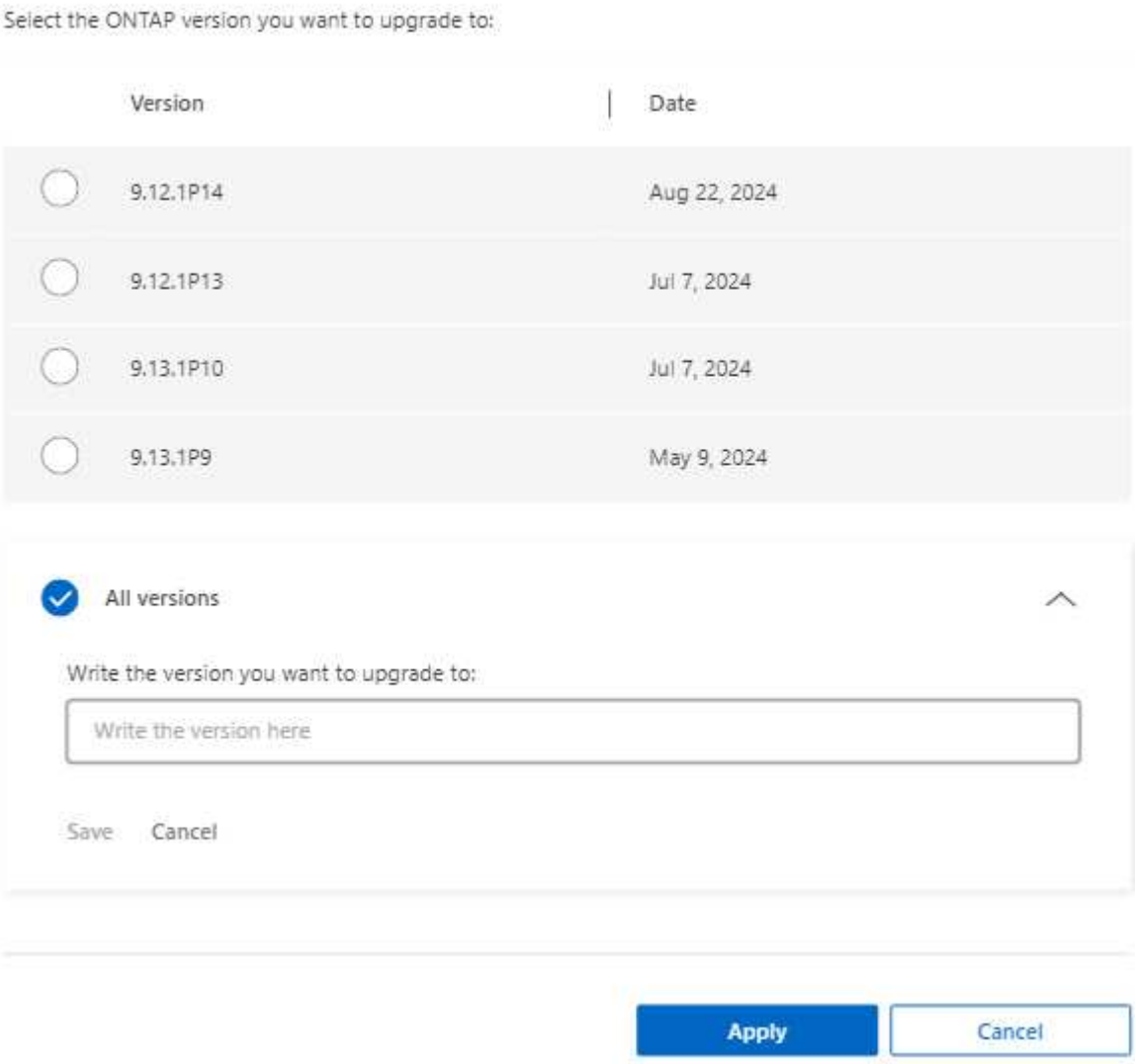


   如果要升级到其他版本，请单击“选择其他版本”。您会看到列出的最新Cloud Volumes ONTAP版本，这些版本也与您系统上安装的版本兼容。例如，您的系统上安装的版本是9.12.1P3，并且有以下兼容版本可用：

   - 9.12.1P4 至 9.12.1P14
   - 9.13.1 和 9.13.1P1 您会看到 9.13.1P1 是升级的默认版本，而 9.12.1P13、9.13.1P14、9.13.1 和 9.13.1P1 是其他可用版本。

4. 或者，您可以单击“所有版本”来输入要升级到的另一个版本（例如，已安装版本的下一个补丁）。有关当前Cloud Volumes ONTAP版本的兼容升级路径，请参阅"支持的升级路径"。

5. 单击“保存”，然后单击“应用”



。

6. 在升级Cloud Volumes ONTAP页面中，阅读 EULA，然后选择 我已阅读并同意 **EULA**。
7. 选择*升级*。
8. 要查看进度，请在Cloud Volumes ONTAP系统上选择 **Audit**。

结果

控制台开始软件升级。软件更新完成后，您可以在系统上执行操作。

完成后

如果您暂停了SnapMirror传输，请使用系统管理器恢复传输。

通过 **URL** 上的可用图像进行升级

您可以将Cloud Volumes ONTAP软件映像放在控制台代理或 HTTP 服务器上，然后从控制台启动软件升级。如果控制台无法访问 S3 存储桶来升级软件，您可以使用此选项。

开始之前

- Cloud Volumes ONTAP系统上不得进行卷或聚合创建等操作。

- 如果您使用 HTTPS 托管ONTAP映像，则升级可能会由于缺少证书而导致的 SSL 身份验证问题而失败。解决方法是生成并安装 CA 签名的证书，用于ONTAP和控制台之间的身份验证。

  转至NetApp知识库查看分步说明：

  "NetApp KB：如何将控制台配置为 HTTPS 服务器来托管升级映像"

步骤

1. 可选：设置可以托管Cloud Volumes ONTAP软件映像的 HTTP 服务器。

   如果您有与虚拟网络的 VPN 连接，则可以将Cloud Volumes ONTAP软件映像放置在您自己网络中的 HTTP 服务器上。否则，您必须将文件放在云中的 HTTP 服务器上。

2. 如果您对Cloud Volumes ONTAP使用自己的安全组，请确保出站规则允许 HTTP 连接，以便Cloud Volumes ONTAP可以访问软件映像。

   预定义的Cloud Volumes ONTAP安全组默认允许出站 HTTP 连接。

3. 从以下位置获取软件映像 "NetApp支持站点"。
4. 将软件映像复制到控制台代理或将提供该文件的 HTTP 服务器上的目录中。

   有两条路径可用。正确的路径取决于您的控制台代理版本。

   - `/opt/application/netapp/cloudmanager/docker_occm/data/ontap/images/`
   - `/opt/application/netapp/cloudmanager/ontap/images/`
5. 在系统上，单击 ••• 图标，然后单击*更新Cloud Volumes ONTAP*。
6. 在更新Cloud Volumes ONTAP版本页面上，输入 URL，然后单击 更改图像。

   如果您将软件映像复制到上面显示的路径中的控制台代理，则需要输入以下 URL：

   http://<Console_agent_private-IP-address>/ontap/images/<图像文件名>

   在 URL 中，**image-file-name** 必须遵循“cot.image.9.13.1P2.tgz”格式。

7. 单击“继续”进行确认。

结果

控制台开始软件更新。软件更新完成后，您就可以在系统上执行操作。

完成后

如果您暂停了SnapMirror传输，请使用系统管理器恢复传输。

修复使用 **Google Cloud NAT** 网关时下载失败的问题

控制台代理会自动下载Cloud Volumes ONTAP 的软件更新。如果您的配置使用 Google Cloud NAT 网关，则下载可能会失败。您可以通过限制软件映像划分的部分数来解决此问题。您必须使用 API 来完成此步骤。

步骤

1. 向 `/occm/`config 提交 PUT 请求，并将以下 JSON 作为正文：

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

maxDownloadSessions 的值可以是 1 或任何大于 1 的整数。如果值为1，则下载的图像不会被分割。

请注意，32 是一个示例值。您应该使用的值取决于您的 NAT 配置和您可以同时拥有的会话数。

"了解有关 /occm/config API 调用的更多信息" 。

注册Cloud Volumes ONTAP即用即付系统

Cloud Volumes ONTAP即用即付 (PAYGO) 系统包含NetApp的支持，但您必须首先通过向NetApp注册系统来激活支持。

需要向NetApp注册 PAYGO 系统才能使用任何方法升级ONTAP软件"本页描述"。

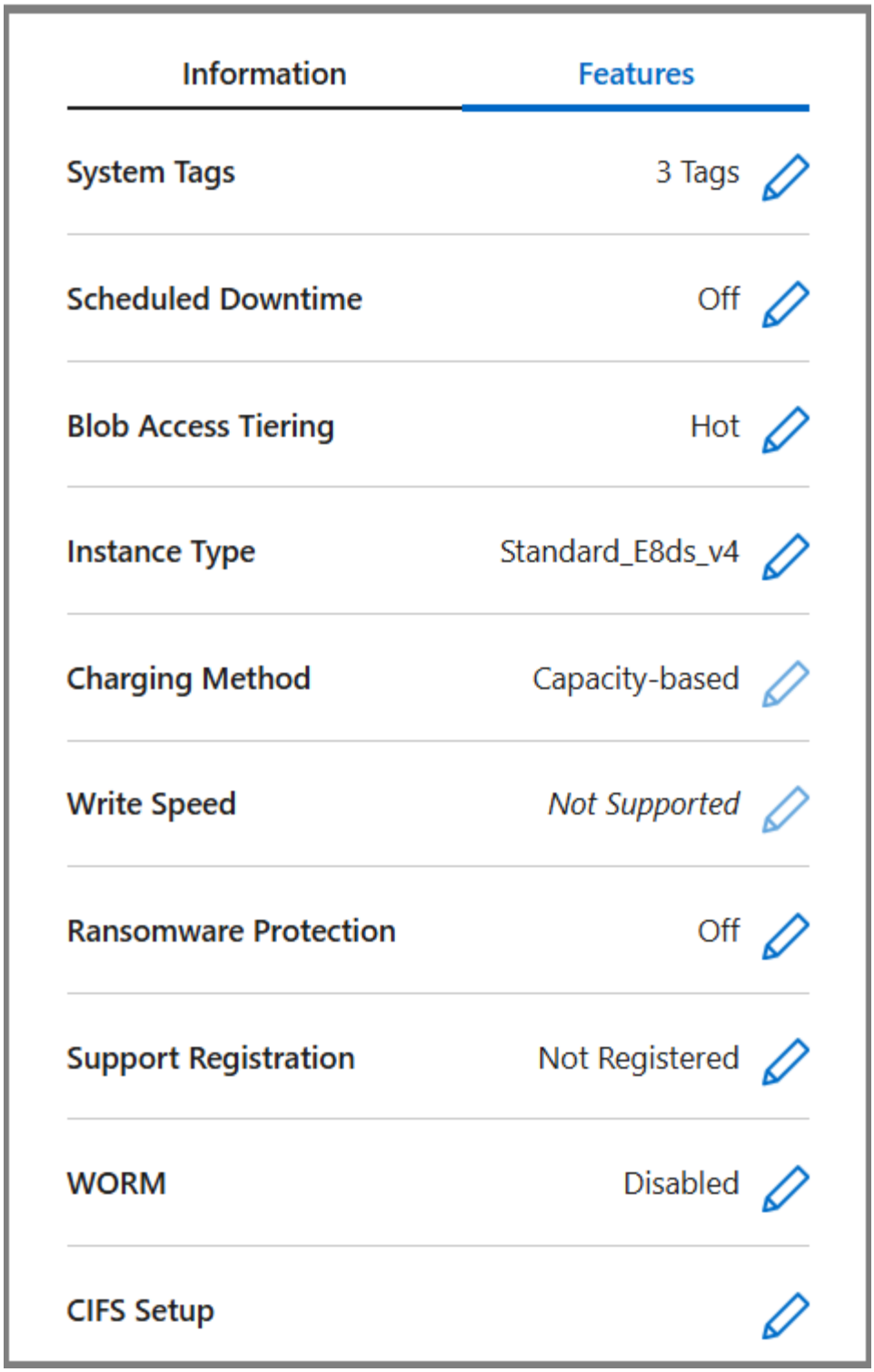
未注册支持的系统仍会在有新版本可用时收到NetApp Console中显示的软件更新通知。但您需要先注册系统才能升级软件。

步骤

1. 如果您尚未将NetApp支持站点帐户添加到控制台，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“系统”页面上，双击要注册的系统的名称。
3. 在“概述”选项卡上，单击“功能”面板，然后单击“支持注册”旁边的铅笔图标。



4. 选择NetApp支持站点帐户并单击“注册”。

结果

该系统已在NetApp注册。

将Cloud Volumes ONTAP基于节点的许可证转换为基于容量的许可证

在基于节点的许可证的可用性终止 (EOA) 之后，您应该使用NetApp Console中的许可证转换工具过渡到基于容量的许可证。

对于年度或长期承诺， NetApp建议您在 EOA 日期（2024 年 11 月 11 日）或许可证到期日之前联系您的NetApp代表，以确保过渡的先决条件到位。如果您没有Cloud Volumes ONTAP节点的长期合同，并且根据按需付费 (PAYGO) 订阅运行您的系统，那么在 2024 年 12 月 31 日支持终止 (EOS) 之前规划您的转换非常重要。在这两种情况下，您都应确保您的系统满足要求，然后再使用NetApp Console中的许可证转换工具实现无缝过渡。

有关 EOA 和 EOS 的信息，请参阅"基于节点的许可证的可用性终止"。

关于此任务

- 当您使用许可证转换工具时，从基于节点到基于容量的许可模型的转换是在现场在线进行的，从而无需进行任何数据迁移或配置额外的云资源。
- 它是一种无中断操作，不会发生服务中断或应用程序停机。
- Cloud Volumes ONTAP系统中的帐户和应用程序数据保持不变。
- 转换后，底层云资源不受影响。
- 许可证转换工具支持所有部署类型，例如单节点、单可用区 (AZ) 中的高可用性 (HA)、多 AZ 中的 HA、自带许可证 (BYOL) 和 PAYGO。
- 该工具支持所有基于节点的许可证作为源，以及所有基于容量的许可证作为目标。例如，如果您拥有基于节点的 PAYGO 标准许可证，则可以将其转换为通过市场购买的任何基于容量的许可证。NetApp已限制 BYOL 许可证的购买、延期和续订。有关更多信息，请参阅 "Cloud Volumes ONTAP的 BYOL 许可可用性受限" 。
- 所有云提供商、AWS、Azure 和 Google Cloud 都支持转换。
- 转换后，基于节点的许可证的序列号将被基于容量的格式取代。这是转换的一部分，并反映在您的NetApp支持站点 (NSS) 帐户中。
- 当您过渡到基于容量的模型时，您的数据将继续保留在与基于节点的许可相同的位置。这种方法保证了数据放置不会中断，并在整个过渡过程中坚持数据主权原则。

开始之前

- 您应该拥有一个具有客户访问权限或管理员访问权限的 NSS 帐户。
- 您的 NSS 帐户应使用您用于访问控制台的用户凭据进行注册。
- Cloud Volumes ONTAP系统应链接到具有客户访问权限或管理员访问权限的 NSS 帐户。
- 您应该拥有有效的基于容量的许可证，可以是 BYOL 许可证或市场订阅。
- 您的帐户中应该有基于容量的许可证。此许可证可以是市场订阅，也可以是控制台中 **Licenses and subscriptions** 下提供的 BYOL/私人优惠包。
- 在选择目的地套餐之前，请了解以下标准：
  - 如果账户具有基于容量的 BYOL 许可证，则所选目标包应与账户的 BYOL 基于容量的许可证保持一致：
    - 什么时候 `Professional`被选为目标包，该帐户应具有带有专业包的 BYOL 许可证：
    - 什么时候 `Essentials`被选为目标包，该帐户应具有 Essentials 包的 BYOL 许可证。

- 如果目标包与帐户的 BYOL 许可证可用性不一致，则意味着基于容量的许可证可能不包含所选包。在这种情况下，我们将通过您的市场订阅向您收费。
- 如果没有基于容量的 BYOL 许可证而只有市场订阅，则应确保所选包包含在基于容量的市场订阅中。
- 如果您现有的基于容量的许可证中没有足够的容量，并且您有市场订阅来对额外的容量使用收费，那么您将通过市场订阅为额外的容量付费。
- 如果您现有的基于容量的许可证中没有足够的容量，并且您没有市场订阅来收取额外容量使用的费用，则无法进行转换。您应该添加市场订阅来收取额外容量或将可用容量扩展到当前许可证。
- 如果目标包与帐户的 BYOL 许可证可用性不一致，并且您现有的基于容量的许可证中没有足够的容量，那么您将通过市场订阅付费。

如果任何一项要求未得到满足，则许可证转换不会发生。在特定情况下，许可证可能会转换，但不能使用。单击信息图标来识别问题并采取纠正措施。

步骤

1. 在“系统”页面上，双击要修改许可证类型的系统的名称。
2. 在“概述”选项卡上，单击“功能”面板。
3. 检查*充电方式*旁边的铅笔图标。如果您的系统的充电方式是 `Node Based`，可以将其转换为按容量充电。

如果您的Cloud Volumes ONTAP系统已按容量收费，或者任何要求未满足，则该图标将被禁用。

4. 在*将基于节点的许可证转换为基于容量的许可证*屏幕上，验证系统名称和源许可证详细信息。
5. 选择转换现有许可证的目标包：
   - 必需品。默认值为 `Essentials`。
   - 专业的
6. 如果您拥有 BYOL 许可证，则可以在转换完成后选中复选框以从控制台中删除基于节点的许可证。如果转换仍在进行中，选中此复选框将不会从控制台中删除许可证。此选项不适用于市场订阅。
7. 选中复选框以确认您了解更改的含义，然后单击“继续”。

完成后

查看新的许可证序列号并在控制台的*Licenses and subscriptions*菜单中验证更改。

不同超标量中的定价

有关定价的详细信息，请访问 "NetApp Console网站"。

有关特定超标量中的私人优惠的信息，请写信至：

- AWS - awspo@netapp.com
- Azure - azurepo@netapp.com
- Google Cloud - gcppo@netapp.com

启动和停止Cloud Volumes ONTAP系统

您可以从NetApp Console停止和启动Cloud Volumes ONTAP来管理您的云计算成本。

安排Cloud Volumes ONTAP自动关闭

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。您无需手动执行此操作，而是可以将控制台配置为在特定时间自动关闭然后重新启动系统。

关于此任务

- 当您计划自动关闭Cloud Volumes ONTAP系统时，如果正在进行活动数据传输，控制台会推迟关闭。

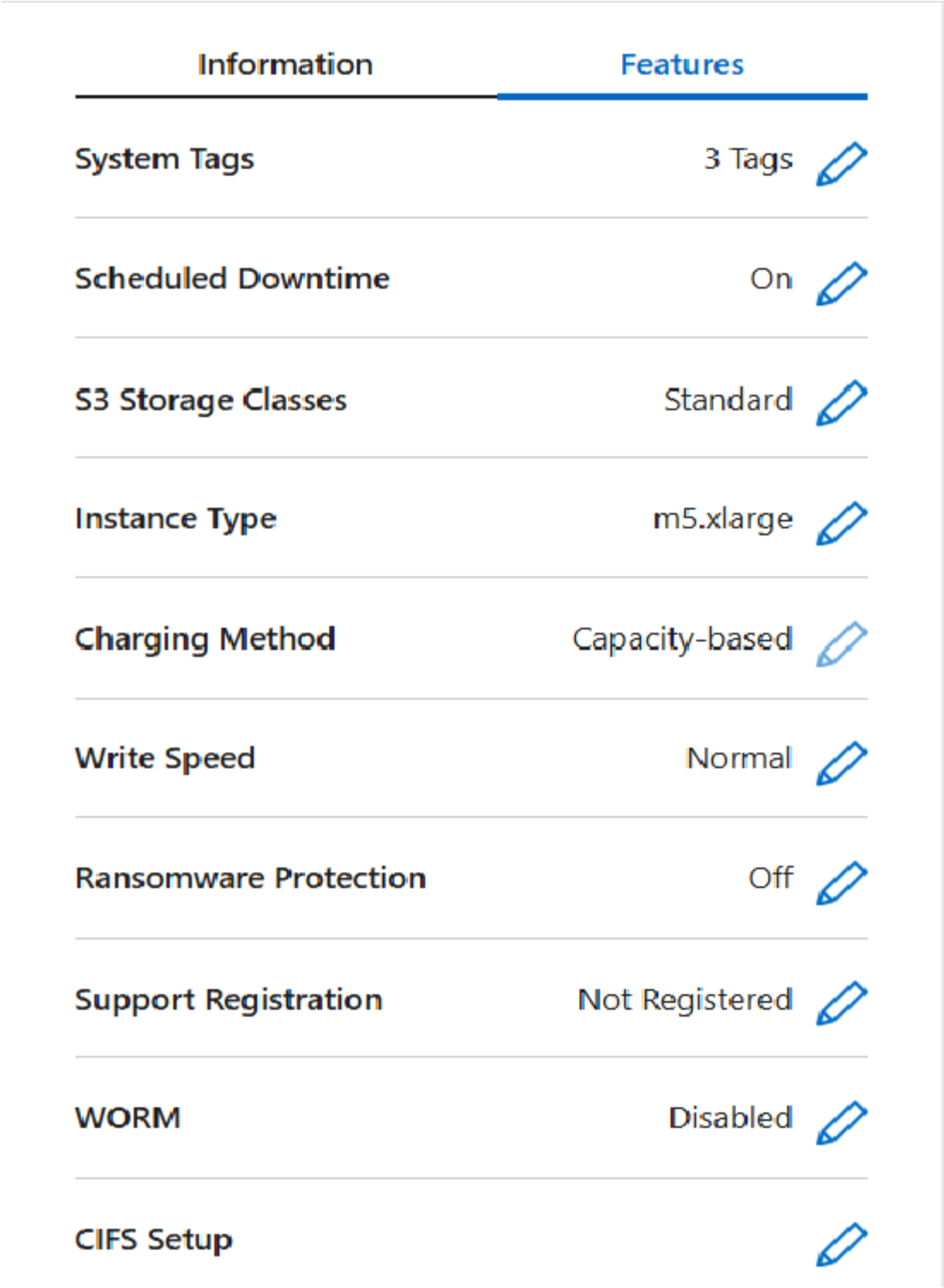
  传输完成后，系统将关闭。

- 此任务计划自动关闭 HA 对中的两个节点。
- 通过计划关闭来关闭Cloud Volumes ONTAP时，不会创建启动磁盘和根磁盘的快照。

  如下一节所述，只有在执行手动关机时才会自动创建快照。

步骤

1. 在*系统*页面上，双击Cloud Volumes ONTAP系统。
2. 在“概览”选项卡上，单击“功能”面板，然后单击“计划停机时间”旁边的铅笔图标。



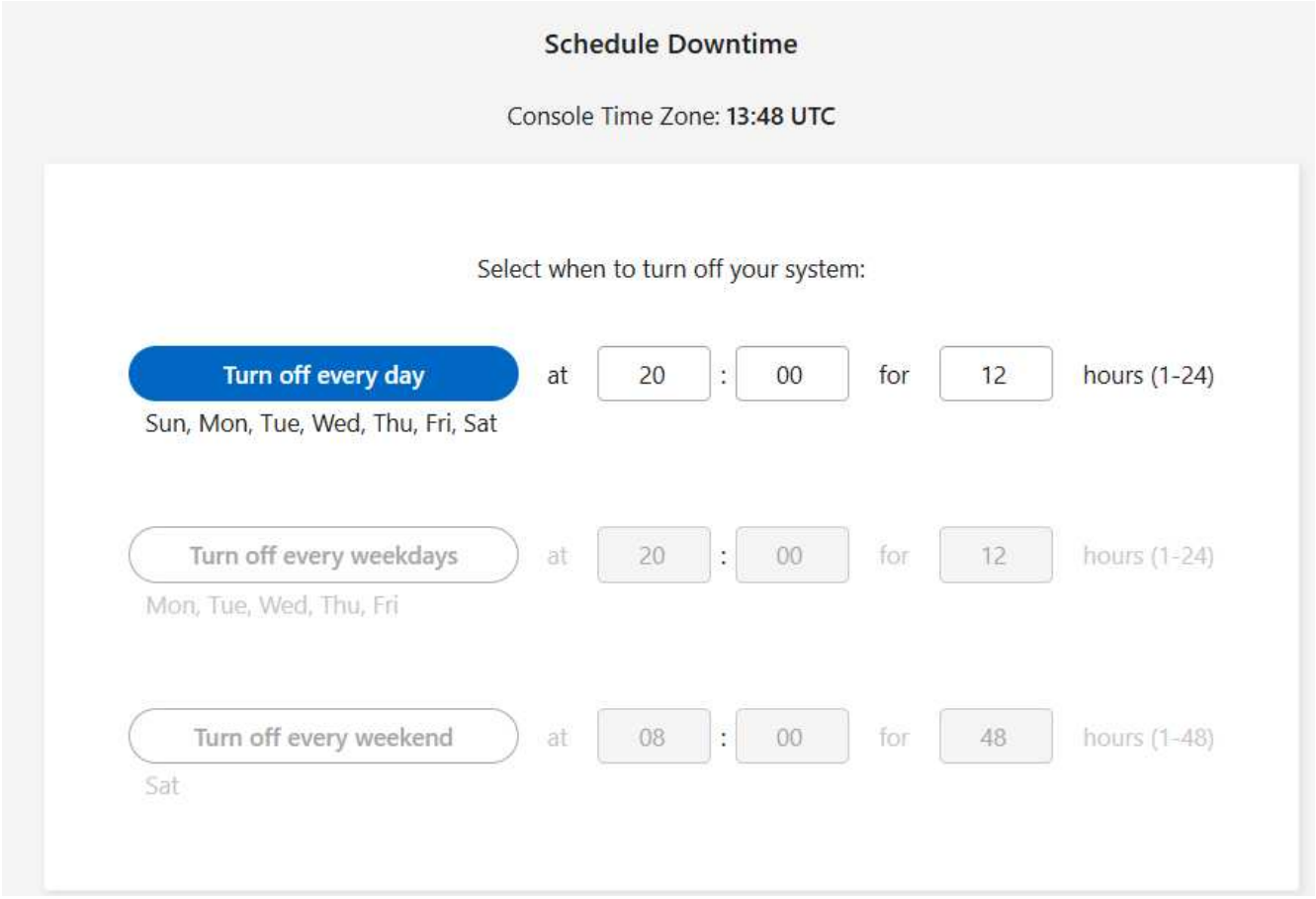
3. 指定关机计划：

   a. 选择是否每天、每个工作日、每个周末或三个选项的任意组合关闭系统。

   b. 指定您想要关闭系统的时间以及关闭系统的时间长度。

      例子

      下图显示了一个时间表，指示控制台每周六晚上 20:00（晚上 8:00）关闭系统 12 小时。控制台每周一凌晨 12:00 重启系统



4. 单击“保存”。

结果

时间表已保存。功能面板下相应的计划停机时间行项目显示“开启”。

停止Cloud Volumes ONTAP

停止Cloud Volumes ONTAP可节省计算成本并创建根磁盘和启动磁盘的快照，这有助于排除故障。

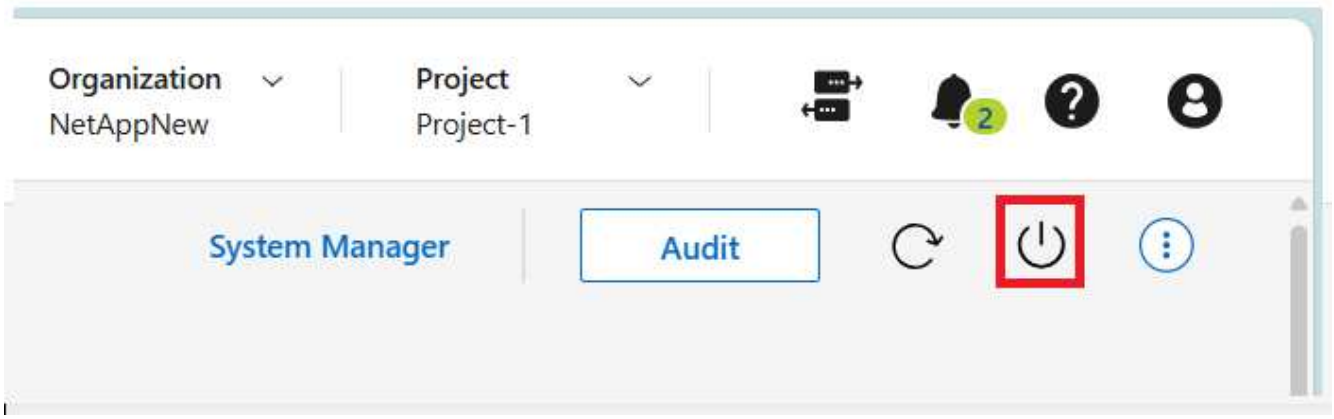
为了降低成本，控制台会定期删除根和启动磁盘的旧快照。根磁盘和启动磁盘仅保留最近的两个快照。

关于此任务

当您停止 HA 对时，控制台将关闭两个节点。

步骤

1. 在系统中，单击“关闭”图标。



2. 保持创建快照的选项处于启用状态，因为快照可以启用系统恢复。
3. 单击“关闭”。

   停止系统可能需要几分钟的时间。您可以稍后从*系统*页面重新启动系统。

   重启时会自动创建快照。

使用 NTP 服务器同步Cloud Volumes ONTAP系统时间

为确保准确的时间同步，您必须为Cloud Volumes ONTAP系统设置网络时间协议 (NTP) 服务器。请确保在所有云提供商上为Cloud Volumes ONTAP系统配置 NTP 服务器，以保持网络内时间同步的一致性。

如果您不配置 NTP 服务器，可能会遇到服务中断和时间同步不准确的情况。

您可以使用以下命令指定 NTP 服务器：

- "NetApp ConsoleAPI"。
- ONTAP CLI 命令 "创建集群时间服务 NTP 服务器"。

相关链接

- 知识库（KB）文章： "CVO集群如何使用NTP？ "
- "准备使用 API"
- "Cloud Volumes ONTAP工作流程"
- "获取所需的标识符"
- "使用NetApp Console的 REST API"

修改系统写入速度

您可以在NetApp Console中为Cloud Volumes ONTAP选择正常或高写入速度。默认写入速度正常。如果您的工作负载需要快速写入性能，您可以更改为高写入速度。

所有类型的单节点系统和一些 HA 对配置均支持高写入速度。在 "Cloud Volumes ONTAP发行说明"中查看支持的配置

在更改写入速度之前，您应该"了解正常设置和高设置之间的差异"。

关于此任务

- 确保卷或聚合创建等操作尚未进行。
- 请注意，此更改将重新启动Cloud Volumes ONTAP系统。这是一个破坏性的过程，需要整个系统停机。

步骤

1. 在*系统*页面上，双击您配置写入速度的系统的名称。
2. 在“概述”选项卡上，单击“功能”面板，然后单击“写入速度”旁边的铅笔图标。
3. 选择*正常*或*高*。

   如果您选择“高”，那么您需要阅读“我明白……”声明并通过勾选方框进行确认。

   从 9.13.0 版本开始，Google Cloud 中的Cloud Volumes ONTAP HA 对支持 高 写入速度选项。

4. 单击“保存”，查看确认消息，然后单击“批准”。

更改Cloud Volumes ONTAP集群管理员密码

Cloud Volumes ONTAP包含一个集群管理员帐户。如果需要，您可以从NetApp Console更改此帐户的密码。

您不应通过ONTAP系统管理器或ONTAP CLI 更改管理员帐户的密码。密码不会反映在控制台中。因此，控制台无法正确监控实例。

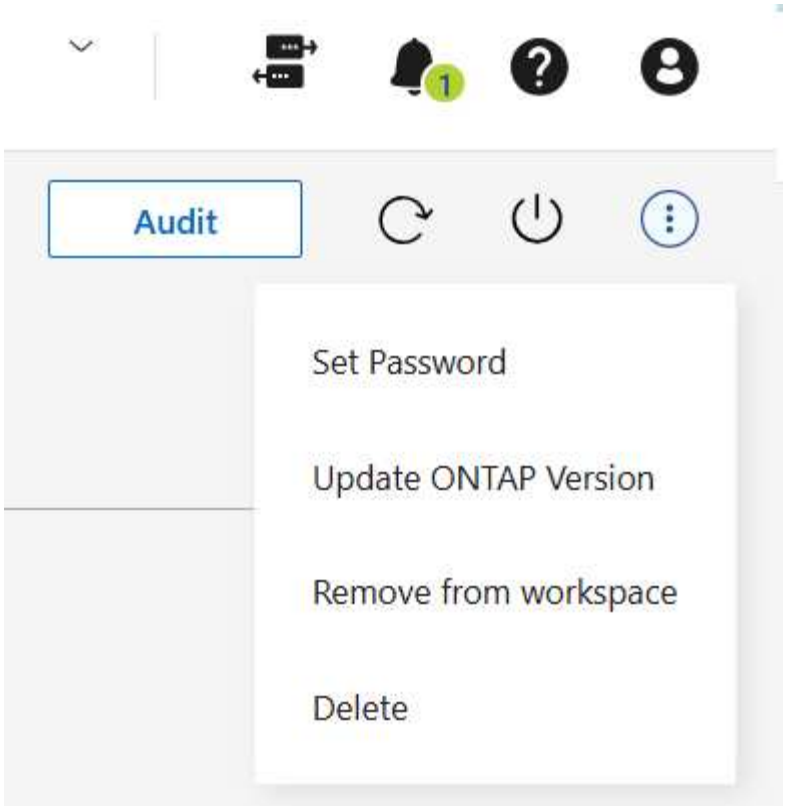
关于此任务

密码必须遵守一些规则。新密码：

- 不应包含该词 `admin`
- 长度必须介于 8 到 50 个字符之间
- 必须至少包含一个英文字母和一个数字
- 不应包含以下特殊字符： `/ ( ) { } [ ] # : % " ? \`

步骤

1. 在*系统*页面上，双击Cloud Volumes ONTAP系统的名称。
2. 在控制台的右上角，单击 ••• 图标，然后选择*设置密码*。



添加、移除或删除系统

将现有的Cloud Volumes ONTAP系统添加到NetApp Console

您可以发现现有的 Cloud Volumes ONTAP 系统并将其添加到 NetApp Console 进行集中管理。当您使用帐户载入系统时，系统将使用该帐户进行注册。在具有多个帐户或组织的环境中，您只能发现和管理使用您的 Console 登录帐户注册的系统。

使用系统注册时，请确保所有操作都在最初启用系统的相同组织和帐户中执行。例如，当迁移停留在同一组织内时，您可以将 Cloud Volumes ONTAP 系统移动到新的 Console 代理。

您无法发现、查看或管理在其他帐户或组织中注册的系统。

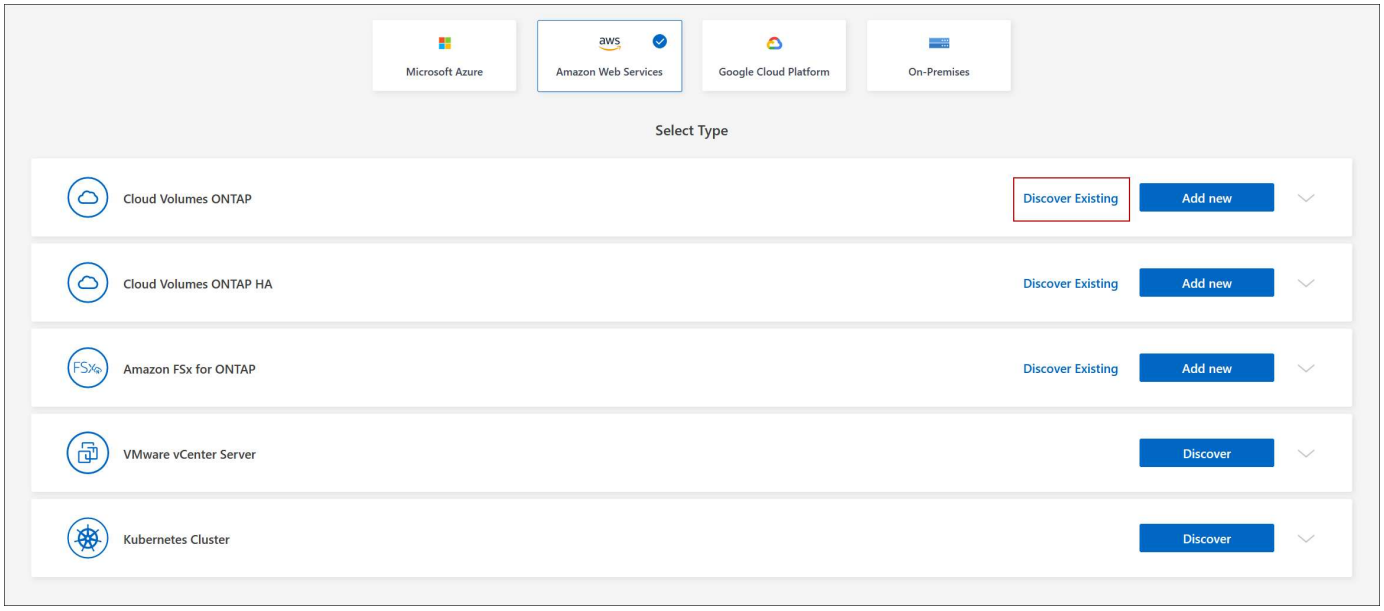
开始之前

您必须知道Cloud Volumes ONTAP管理员用户帐户的密码。

步骤

1. 从左侧导航菜单中，选择“存储”>“管理”。
2. 在*系统*页面上，单击*添加系统*。
3. 选择系统所在的云提供商。
4. 选择要添加的Cloud Volumes ONTAP系统的类型。
5. 单击链接即可发现现有系统。

+



1. 在“区域”页面上，选择一个区域。您可以看到在所选区域中运行的系统。

   Cloud Volumes ONTAP系统在此页面中以实例形式表示。从列表中，您可以仅选择使用当前帐户注册的那些实例。

2. 在“凭据”页面上，输入Cloud Volumes ONTAP管理员用户的密码，然后选择“**Go**”。

结果

控制台将Cloud Volumes ONTAP系统添加到 系统 页面。

从NetApp Console中删除Cloud Volumes ONTAP系统

您可以删除Cloud Volumes ONTAP系统以将其移动到另一个系统或解决发现问题。

关于此任务

删除Cloud Volumes ONTAP系统会将其从NetApp Console中删除。它不会删除Cloud Volumes ONTAP系统。如果需要，您可以稍后重新发现该系统。

步骤

1. 在*系统*页面上，双击要删除的系统。
2. 在控制台的右上角，单击 ••• 图标，然后选择*从工作区中删除*。
3. 在*从工作区中删除*窗口中，单击*删除*。

结果

控制台删除系统。用户可以随时从*系统*页面重新发现已删除的系统。

从NetApp Console删除Cloud Volumes ONTAP系统

您应该始终从NetApp Console中删除Cloud Volumes ONTAP系统，而不是从云提供商的应用程序中删除。例如，如果您终止了云提供商许可的Cloud Volumes ONTAP实例，则您不

能将该许可证密钥用于另一个实例。您必须从控制台中删除Cloud Volumes ONTAP系统才能释放许可证。

当您删除系统时，控制台会终止Cloud Volumes ONTAP实例并删除磁盘和快照。

> 删除系统时，不会删除其他资源，例如NetApp Backup and Recovery管理的备份以及NetApp Data Classification的实例。您需要手动删除它们。如果您不这样做，那么您将继续为这些资源支付费用。

当控制台在您的云提供商中部署Cloud Volumes ONTAP时，它会对实例启用终止保护。此选项有助于防止意外终止。

步骤

1. 如果您在系统上启用了备份和恢复功能，请确定是否仍然需要备份的数据，然后…… "如有必要，删除备份"。

   备份和恢复在设计上独立于Cloud Volumes ONTAP 。当您删除Cloud Volumes ONTAP系统时，备份和恢复不会自动删除备份，并且 UI 中当前不支持在系统被删除后删除备份。

2. 如果您在此系统上启用了数据分类，并且没有其他系统使用此服务，那么您需要删除该服务的实例。

   "了解有关数据分类实例的更多信息" 。

3. 删除Cloud Volumes ONTAP系统。
   a. 在“系统”页面上，双击要删除的Cloud Volumes ONTAP系统的名称。
   b. 在控制台的右上角，单击 ••• 图标，然后选择*删除*。
   c. 输入要删除的系统的名称，然后单击“删除”。删除系统最多可能需要五分钟。

> 仅对于Cloud Volumes ONTAP Professional 许可证，备份和恢复是免费的。此免费福利不适用于已删除的环境。如果Cloud Volumes ONTAP环境的备份副本保留在备份和恢复实例中，则您将需要为备份副本付费，直到它们被删除为止。

AWS 管理

修改 AWS 中Cloud Volumes ONTAP系统的 EC2 实例类型

在 AWS 中启动Cloud Volumes ONTAP时，您可以从多个实例或类型中进行选择。如果您确定实例类型太小或太大，无法满足您的需求，您可以随时更改实例类型。

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）。如果不是，则操作将失败。

  "ONTAP 9 文档：用于配置自动交还的命令"

- 更改实例类型可能会影响 AWS 服务费用。
- 该操作重新启动Cloud Volumes ONTAP。

对于单节点系统，I/O 被中断。

对于 HA 对来说，这种变化是无中断的。 HA 对继续提供数据。

NetApp Console通过启动接管并等待返回来一次更改一个节点。 NetApp 的质量保证团队在此过程中对文件的写入和读取进行了测试，并且没有发现客户端的任何问题。随着连接的变化，在 I/O 级别观察到一些重试，但应用层克服了 NFS/CIFS 连接的重新连接。

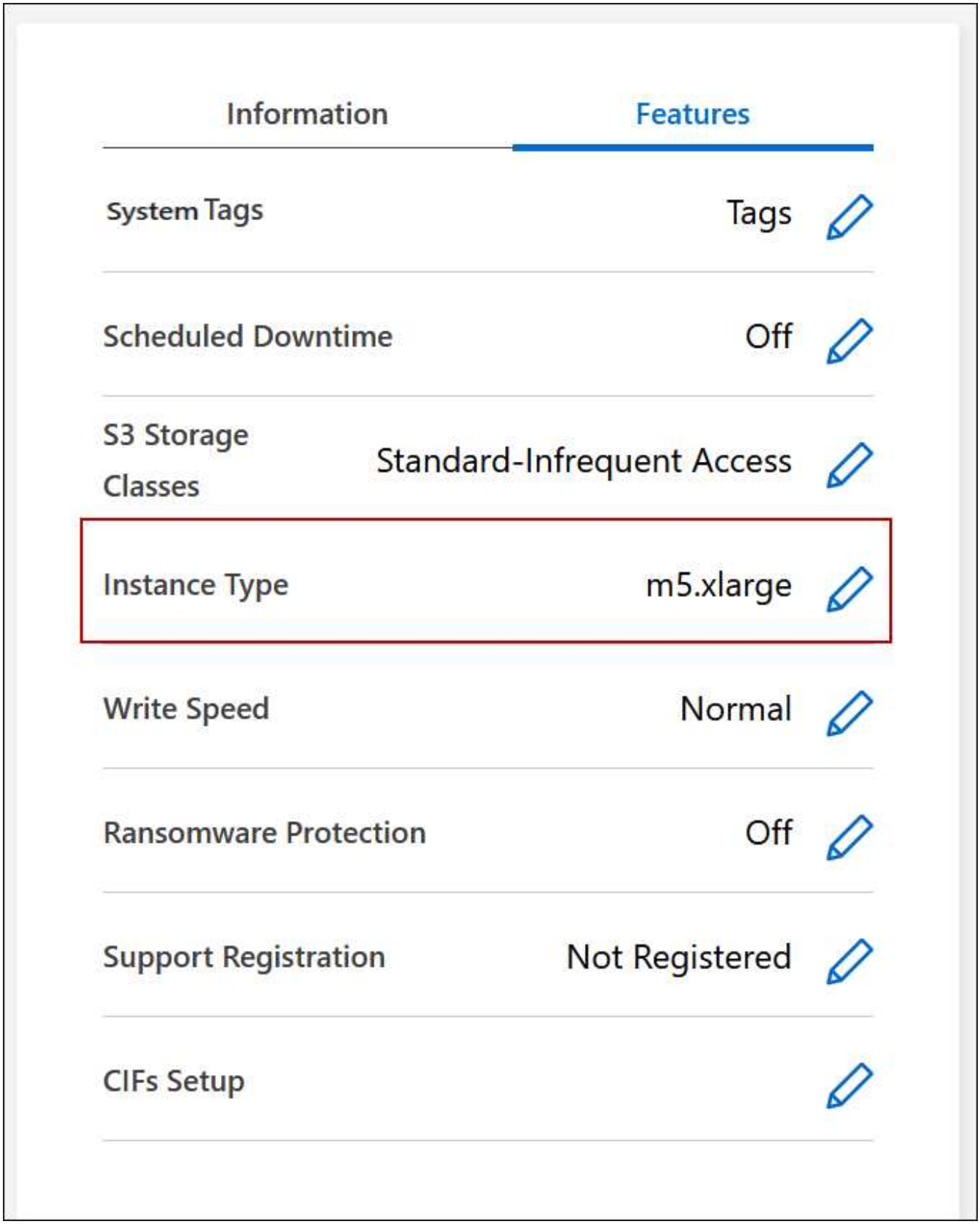
参考

有关 AWS 支持的实例类型列表，请参阅"支持的 EC2 实例"。

如果您无法将实例类型从 c4、m4 或 r4 实例更改为其他类型，请参阅知识库文章"将 AWS Xen CVO 实例转换为 Nitro (KVM)"。

步骤

1. 在*系统*页面上，选择系统。
2. 在概览选项卡上，单击功能面板，然后单击*实例类型*旁边的铅笔图标。



如果您使用的是基于节点的即用即付 (PAYGO) 许可证，则可以通过单击“许可证类型”旁边的铅笔图标来选择不同的许可证和实例类型。

3. 选择一个实例类型，选中复选框以确认您了解更改的含义，然后单击*更改*。

结果

Cloud Volumes ONTAP使用新配置重新启动。

修改多个 **AWS AZ** 中的**Cloud Volumes ONTAP HA** 对的路由表

您可以修改 AWS 路由表，其中包含部署在多个 AWS 可用区 (AZ) 中的 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，您可以这样做。

步骤

1. 在*系统*页面上，选择系统。
2. 在概览选项卡上，单击功能面板，然后单击*路由表*旁边的铅笔图标。
3. 修改所选路由表列表，然后单击“保存”。

结果

NetApp Console发送 AWS 请求来修改路由表。

Azure 管理

更改**Cloud Volumes ONTAP**的 **Azure VM** 类型

在 Microsoft Azure 中启动Cloud Volumes ONTAP时，您可以从多种 VM 类型中进行选择。如果您确定虚拟机类型太小或太大，无法满足您的需求，您可以随时更改虚拟机类型。

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）。如果不是，则操作将失败。

  "ONTAP 9 文档：用于配置自动交还的命令"

- 更改 VM 类型可能会影响 Microsoft Azure 服务费用。
- 该操作重新启动Cloud Volumes ONTAP。

  对于单节点系统，I/O 被中断。

  对于 HA 对来说，这种变化是无中断的。 HA 对继续提供数据。

NetApp Console通过启动接管并等待返回来一次更改一个节点。 NetApp 的质量保证团队在此过程中对文件的写入和读取进行了测试，并且没有发现客户端的任何问题。随着连接的变化，在 I/O 级别观察到一些重试，但应用层克服了 NFS/CIFS 连接的重新连接。

步骤

1. 在*系统*页面上，选择系统。
2. 在“概述”选项卡上，单击“功能”面板，然后单击“**VM** 类型”旁边的铅笔图标。

   如果您使用的是基于节点的即用即付 (PAYGO) 许可证，则可以通过单击“许可证类型”旁边的铅笔图标来选择不同的许可证和 VM 类型。

3. 选择一种 VM 类型，选中复选框以确认您了解更改的含义，然后单击“更改”。

结果

Cloud Volumes ONTAP使用新配置重新启动。

覆盖 Azure 中Cloud Volumes ONTAP HA 对的 CIFS 锁

组织或帐户管理员可以在NetApp Console中启用一项设置，以防止在 Azure 维护事件期间出现Cloud Volumes ONTAP存储交还问题。启用此设置后， Cloud Volumes ONTAP将否决 CIFS 锁定并重置活动的 CIFS 会话。

关于此任务

Microsoft Azure 会安排其虚拟机的定期维护事件。当Cloud Volumes ONTAP HA 对上发生维护事件时，HA 对会启动存储接管。如果在此维护事件期间有活动的 CIFS 会话，则 CIFS 文件上的锁定可能会阻止存储恢复。

如果启用此设置， Cloud Volumes ONTAP将否决锁定并重置活动的 CIFS 会话。因此，HA 对可以在这些维护事件期间完成存储交还。

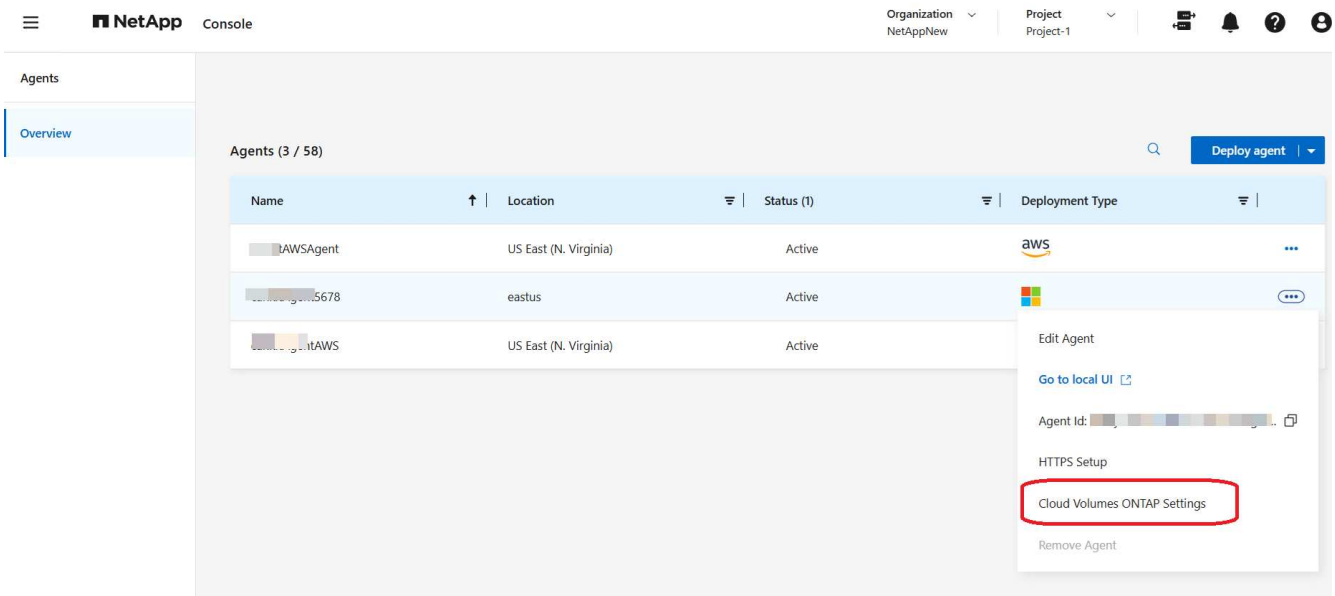
此过程可能会对 CIFS 客户端造成破坏。 CIFS 客户端未提交的数据可能会丢失。

开始之前

您需要先创建控制台代理，然后才能更改控制台设置。 "了解详情" 。

步骤

1. 从左侧导航窗格转到*管理>代理*。
2. 点击 ••• 管理Cloud Volumes ONTAP系统的控制台代理的图标。
3. 选择* Cloud Volumes ONTAP设置*。



4. 在“Azure”下，单击“Azure HA 系统的 Azure CIFS 锁”。
5. 单击复选框以启用该功能，然后单击“保存”。

为Cloud Volumes ONTAP系统使用 Azure Private Link 或服务端点

Cloud Volumes ONTAP使用 Azure Private Link 连接到其关联的存储帐户。如果需要，您可以禁用 Azure Private Links 并改用服务端点。

概述

默认情况下， NetApp Console启用 Azure Private Link 来建立Cloud Volumes ONTAP与其关联存储帐户之间的连接。 Azure 专用链接可保护 Azure 中端点之间的连接并提供性能优势。

如果需要，您可以将Cloud Volumes ONTAP配置为使用服务端点而不是 Azure Private Link。

无论采用哪种配置，控制台始终限制Cloud Volumes ONTAP和存储帐户之间的连接的网络访问。网络访问仅限于部署Cloud Volumes ONTAP 的VNet 和部署控制台代理的 VNet。

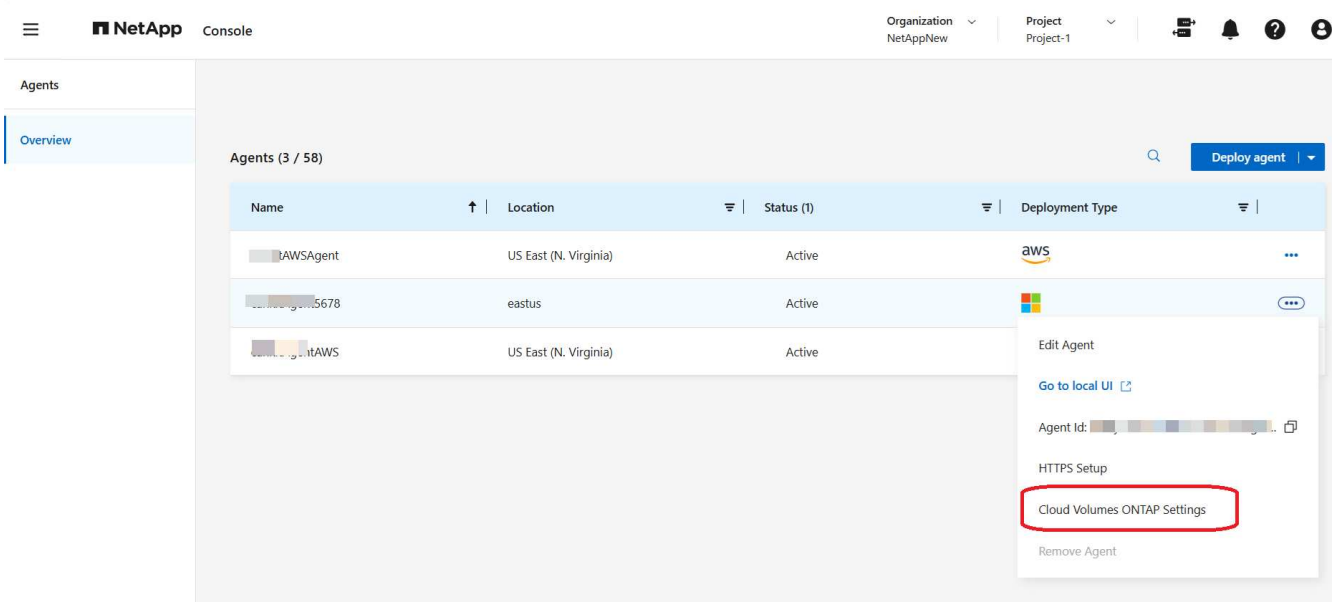
禁用 **Azure Private Links** 并改用服务终结点

如果您的业务需要，您可以在控制台中更改设置，以便将Cloud Volumes ONTAP配置为使用服务端点而不是 Azure Private Link。更改此设置适用于您创建的新Cloud Volumes ONTAP系统。服务端点仅支持"Azure 区域对"控制台代理和Cloud Volumes ONTAP VNet 之间。

控制台代理应部署在与其管理的Cloud Volumes ONTAP系统相同的 Azure 区域中，或者部署在 "Azure 区域对"适用于Cloud Volumes ONTAP系统。

步骤

1. 从左侧导航窗格转到*管理>代理*。
2. 点击 ••• 管理Cloud Volumes ONTAP系统的控制台代理的图标。
3. 选择* Cloud Volumes ONTAP设置*。



4. 在“**Azure**”下，单击“使用 **Azure** 专用链接”。
5. 取消选择* Cloud Volumes ONTAP和存储帐户之间的专用链接连接*。
6. 单击“保存”。

完成后

如果您禁用了 Azure Private Links 并且控制台代理使用代理服务器，则必须启用直接 API 流量。

"了解如何在控制台代理上启用直接 API 流量"

使用 **Azure Private Links**

在大多数情况下，您无需执行任何操作即可设置与Cloud Volumes ONTAP 的Azure Private 链接。控制台为您管理 Azure 专用链接。但是如果您使用现有的 Azure 私有 DNS 区域，则需要编辑配置文件。

自定义 **DNS** 的要求

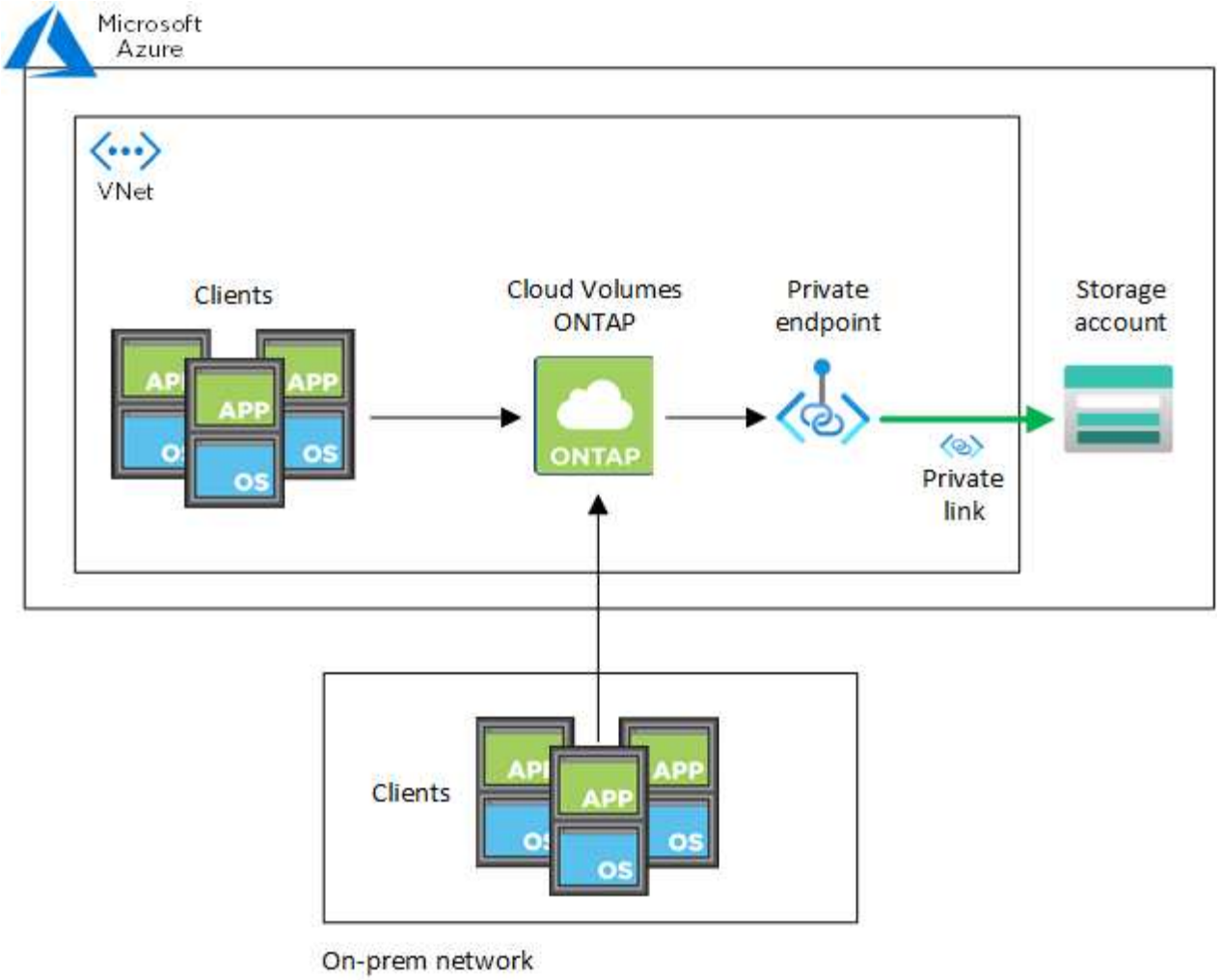
或者，如果您使用自定义 DNS，则需要从自定义 DNS 服务器创建到 Azure 私有 DNS 区域的条件转发器。要了解更多信息，请参阅"Azure 关于使用 DNS 转发器的文档"。

专用链接连接的工作原理

当控制台在 Azure 中部署Cloud Volumes ONTAP时，它会在资源组中创建一个私有端点。私有端点与Cloud Volumes ONTAP 的存储帐户相关联。因此，对Cloud Volumes ONTAP存储的访问需要通过 Microsoft 主干网络。

当客户端与Cloud Volumes ONTAP位于同一 VNet 内、位于对等 VNet 内或位于本地网络中时，客户端访问将通过专用链接进行。

以下示例展示了客户端如何通过专用链接从同一 VNet 内部以及从具有专用 VPN 或 ExpressRoute 连接的本地网络进行访问。



如果控制台代理和Cloud Volumes ONTAP系统部署在不同的 VNet 中，则必须在部署控制台代理的 VNet 和部署Cloud Volumes ONTAP系统的 VNet 之间设置 VNet 对等连接。

提供有关 **Azure** 专用 **DNS** 的详细信息

如果你使用 "Azure 专用 DNS"，那么就需要在每个Console代理上修改一个配置文件。否则，控制台无法设置Cloud Volumes ONTAP与其关联存储帐户之间的 Azure Private Link 连接。

请注意，DNS 名称必须符合 Azure DNS 命名要求 "如 Azure 文档所示"。

步骤

1. 通过 SSH 连接到控制台代理主机并登录。
2. 导航至 `/opt/application/netapp/cloudmanager/docker_occm/data`目录。
3. 编辑 `app.conf`通过添加 `user-private-dns-zone-settings`具有以下关键字-值对的参数：

```
"user-private-dns-zone-settings" : {
   "resource-group" : "<resource group name of the DNS zone>",
   "subscription" : "<subscription ID>",
   "use-existing" : true,
   "create-private-dns-zone-link" : true
}
```

这 `subscription`仅当私有 DNS 区域与控制台代理的订阅不同时才需要关键字。

4. 保存文件并注销控制台代理。

   不需要重新启动。

启用故障回滚

如果控制台无法在特定操作中创建 Azure 专用链接，它将在没有 Azure 专用链接连接的情况下完成该操作。创建新系统（单个节点或 HA 对）时，或者在 HA 对上执行以下操作时，可能会发生这种情况：创建新聚合、向现有聚合添加磁盘或在超过 32 TiB 时创建新的存储帐户。

如果控制台无法创建 Azure 专用链接，您可以通过启用回滚来更改此默认行为。这有助于确保您完全遵守公司的安全规定。

如果启用回滚，控制台将停止该操作并回滚作为该操作的一部分创建的所有资源。

您可以通过 API 或更新 app.conf 文件来启用回滚。

通过 **API** 启用回滚

步骤

1. 使用 `PUT /occm/config`具有以下请求主体的 API 调用：

```
{ "rollbackOnAzurePrivateLinkFailure": true }
```

通过更新 **app.conf** 启用回滚

步骤

1. 通过 SSH 连接到控制台代理的主机并登录。
2. 导航到以下目录：/opt/application/netapp/cloudmanager/docker_occm/data
3. 编辑 app.conf，添加以下参数和值：

```
 "rollback-on-private-link-failure": true
```

. 保存文件并注销控制台代理。

不需要重新启动。

在 **Azure** 控制台中移动**Cloud Volumes ONTAP**的 **Azure** 资源组

Cloud Volumes ONTAP支持 Azure 资源组移动，但工作流程仅在 Azure 控制台中进行。

您可以将Cloud Volumes ONTAP系统从同一 Azure 订阅内的一个资源组移动到 Azure 中的另一个资源组。不支持在不同的 Azure 订阅之间移动资源组。

步骤

1. 删除Cloud Volumes ONTAP系统。请参阅"删除Cloud Volumes ONTAP系统" 。
2. 在 Azure 控制台中执行资源组移动。

   要完成移动，请参阅"Microsoft Azure 文档中的“将资源移动到新的资源组或订阅”"。

3. 在*系统*页面上，发现系统。
4. 在系统信息中查找新的资源组。

结果

系统及其资源（虚拟机、磁盘、存储帐户、网络接口、快照）位于新的资源组中。

在 **Azure** 中隔离**SnapMirror**流量

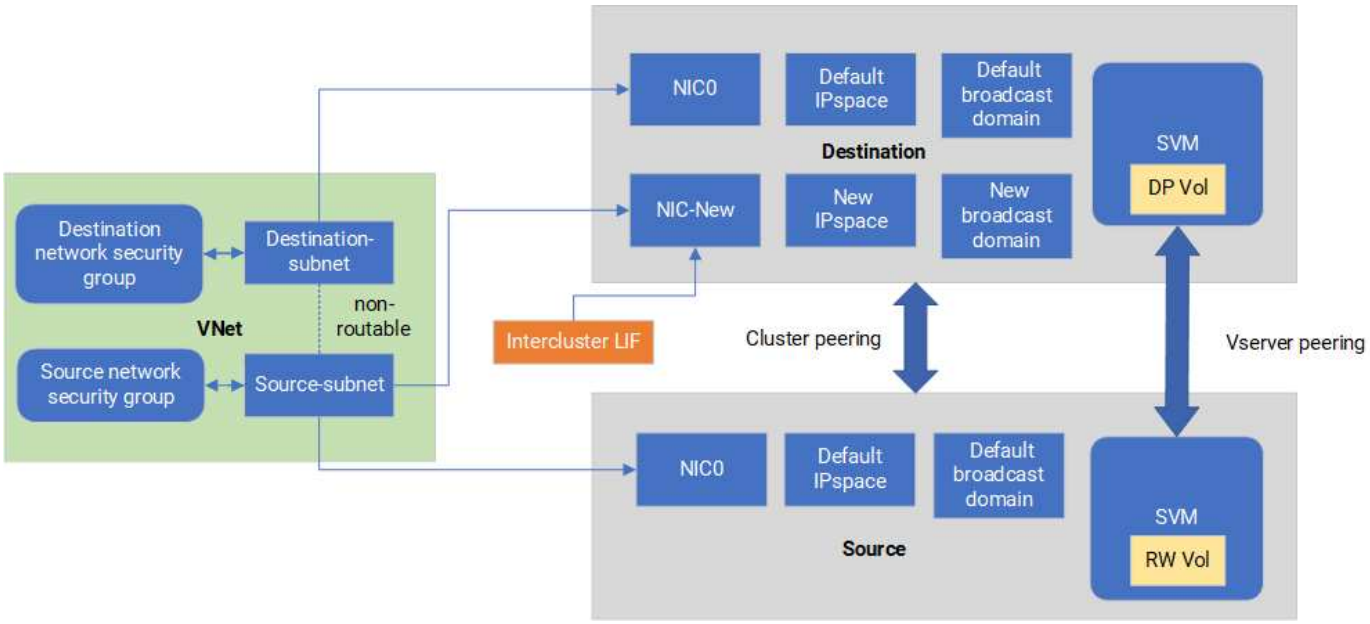
使用 Azure 中的Cloud Volumes ONTAP ，您可以将SnapMirror复制流量与数据和管理流量分离。为了将SnapMirror复制流量与数据流量隔离，您需要添加一个新的网络接口卡 (NIC)、一个相关的集群间 LIF 和一个不可路由的子网。

关于 **Azure** 中的**SnapMirror**流量隔离

默认情况下， NetApp Console会在同一子网上配置Cloud Volumes ONTAP部署中的所有 NIC 和 LIF。在这样的配置中， SnapMirror复制流量和数据和管理流量使用相同的子网。隔离SnapMirror流量利用了无法路由到用于数据和管理流量的现有子网的额外子网。

图 **1**

下图显示了在单节点部署中使用附加 NIC、关联的集群间 LIF 和不可路由子网对SnapMirror复制流量进行隔离。HA 对部署略有不同。



开始之前

回顾以下注意事项：

- 您只能向Cloud Volumes ONTAP单节点或 HA 对部署（VM 实例）添加单个 NIC 以实现SnapMirror流量隔离。
- 要添加新的 NIC，您部署的 VM 实例类型必须具有未使用的 NIC。
- 源集群和目标集群应该可以访问同一个虚拟网络 (VNet)。目标集群是 Azure 中的Cloud Volumes ONTAP系统。源集群可以是 Azure 中的Cloud Volumes ONTAP系统或ONTAP系统。

步骤 **1**：创建额外的 **NIC** 并连接到目标 **VM**

本节提供有关如何创建附加 NIC 并将其附加到目标 VM 的说明。目标 VM 是 Azure 中Cloud Volumes ONTAP中的单节点或 HA 对系统，您要在其中设置额外的 NIC。

步骤

1. 在ONTAP CLI 中，停止节点。

```
dest::> halt -node <dest_node-vm>
```

2. 在 Azure 门户中，检查 VM（节点）状态是否已停止。

```
az vm get-instance-view --resource-group <dest-rg> --name <dest-vm>
--query instanceView.statuses[1].displayStatus
```

3. 使用 Azure Cloud Shell 中的 Bash 环境停止节点。
   a. 停止节点。

```
az vm stop --resource-group <dest_node-rg> --name <dest_node-vm>
```

b. 解除分配节点。

```
az vm deallocate --resource-group <dest_node-rg> --name <dest_node-vm>
```

4. 配置网络安全组规则，使两个子网（源集群子网和目标集群子网）互不可达。
   a. 在目标虚拟机上创建新的 NIC。
   b. 查找源集群子网的子网 ID。

```
az network vnet subnet show -g <src_vnet-rg> -n <src_subnet> --vnet-name <vnet> --query id
```

   c. 使用源集群子网的子网 ID 在目标虚拟机上创建新的 NIC。在这里输入新 NIC 的名称。

```
az network nic create -g <dest_node-rg> -n <dest_node-vm-nic-new> --subnet <id_from_prev_command> --accelerated-networking true
```

   d. 保存私有IP地址。此 IP 地址 <new_added_nic_primary_addr> 用于在广播域，新 NIC 的集群间 LIF。
5. 将新的 NIC 附加到 VM。

```
az vm nic add -g <dest_node-rg> --vm-name <dest_node-vm> --nics <dest_node-vm-nic-new>
```

6. 启动虚拟机（节点）。

```
az vm start --resource-group <dest_node-rg>  --name <dest_node-vm>
```

7. 在 Azure 门户中，转到 网络 并确认新的 NIC（例如 nic-new）存在并且加速网络已启用。

```
az network nic list --resource-group azure-59806175-60147103-azure-rg --query "[].{NIC: name, VM: virtualMachine.id}"
```

对于 HA 对部署，请对合作伙伴节点重复这些步骤。

步骤 **2**：为新 **NIC** 创建新的 **IP** 空间、广播域和集群间 **LIF**

集群间 LIF 的单独 IP 空间为集群间复制的网络功能提供了逻辑分离。

使用ONTAP CLI 执行以下步骤。

步骤

1. 创建新的 IP 空间（new_ipspace）。

```
dest::> network ipspace create -ipspace <new_ipspace>
```

2. 在新的 IP 空间（new_ipspace）上创建一个广播域并添加 nic-new 端口。

```
dest::> network port show
```

3. 对于单节点系统，新添加的端口为 *e0b*。对于具有托管磁盘的 HA 对部署，新添加的端口为 *e0d*。对于具有页面 blob 的 HA 对部署，新添加的端口为 *e0e*。使用节点名称而不是 VM 名称。通过运行 `node show`查找节点名称。

```
dest::> broadcast-domain create -broadcast-domain <new_bd> -mtu 1500
-ipspace <new_ipspace> -ports <dest_node-cot-vm:e0b>
```

4. 在新的广播域 (new_bd) 和新的 NIC (nic-new) 上创建集群间 LIF。

```
dest::> net int create -vserver <new_ipspace> -lif <new_dest_node-ic-
lif> -service-policy default-intercluster -address
<new_added_nic_primary_addr> -home-port <e0b> -home-node <node> -netmask
<new_netmask_ip> -broadcast-domain <new_bd>
```

5. 验证新的集群间 LIF 的创建。

```
dest::> net int show
```

对于 HA 对部署，请对合作伙伴节点重复这些步骤。

步骤 **3**：验证源系统和目标系统之间的集群对等连接

本节提供有关如何验证源系统和目标系统之间的对等关系的说明。

使用ONTAP CLI 执行以下步骤。

步骤

1. 验证目标集群的集群间 LIF 是否可以对源集群的集群间 LIF 执行 ping 操作。由于目标集群执行此命令，因

此目标 IP 地址是源上的集群间 LIF IP 地址。

```
dest::> ping -lif <new_dest_node-ic-lif> -vserver <new_ipspace>
-destination <10.161.189.6>
```

2. 验证源集群的集群间 LIF 是否可以 ping 通目标集群的集群间 LIF。目标是在目标上创建的新 NIC 的 IP 地址。

```
src::> ping -lif <src_node-ic-lif> -vserver <src_svm> -destination
<10.161.189.18>
```

对于 HA 对部署，请对合作伙伴节点重复这些步骤。

步骤 **4**：在源系统和目标系统之间创建 **SVM** 对等连接

本节提供有关如何在源系统和目标系统之间创建 SVM 对等的说明。

使用ONTAP CLI 执行以下步骤。

步骤

1. 使用源集群间 LIF IP 地址作为目标在目标上创建集群对等 `-peer-addrs`。对于 HA 对，列出两个节点的源集群间 LIF IP 地址作为 `-peer-addrs`。

```
dest::> cluster peer create -peer-addrs <10.161.189.6> -ipspace
<new_ipspace>
```

2. 输入并确认密码。
3. 使用目标集群 LIF IP 地址作为源集群的 IP 地址，在源上创建集群对等连接 `peer-addrs`。对于 HA 对，列出两个节点的目标集群间 LIF IP 地址作为 `-peer-addrs`。

```
src::> cluster peer create -peer-addrs <10.161.189.18>
```

4. 输入并确认密码。
5. 检查集群是否对等。

```
src::> cluster peer show
```

成功的对等连接在可用性字段中显示 可用。

6. 在目标上创建 SVM 对等连接。源 SVM 和目标 SVM 都应该是数据 SVM。

```
dest::> vserver peer create -vserver <dest_svm> -peer-vserver <src_svm>
-peer-cluster <src_cluster> -applications snapmirror``
```

7. 接受 SVM 对等连接。

```
src::> vserver peer accept -vserver <src_svm> -peer-vserver <dest_svm>
```

8. 检查 SVM 是否已对等。

```
dest::> vserver peer show
```

同行国家显示*peered* 和对等应用程序显示*snapmirror*.

步骤 **5**：在源系统和目标系统之间创建**SnapMirror**复制关系

本节提供有关如何在源系统和目标系统之间创建SnapMirror复制关系的说明。

要移动现有的SnapMirror复制关系，必须先中断现有的SnapMirror复制关系，然后再创建新的SnapMirror复制关系。

使用ONTAP CLI 执行以下步骤。

步骤

1. 在目标 SVM 上创建数据保护卷。

```
dest::> vol create -volume <new_dest_vol> -vserver <dest_svm> -type DP
-size <10GB> -aggregate <aggr1>
```

2. 在目标上创建SnapMirror复制关系，其中包括复制的SnapMirror策略和计划。

```
dest::> snapmirror create -source-path src_svm:src_vol  -destination
-path  dest_svm:new_dest_vol -vserver dest_svm -policy
MirrorAllSnapshots -schedule 5min
```

3. 在目标上初始化SnapMirror复制关系。

```
dest::> snapmirror initialize -destination-path  <dest_svm:new_dest_vol>
```

4. 在ONTAP CLI 中，通过运行以下命令验证SnapMirror关系状态：

```
dest::> snapmirror show
```

关系状态是 `Snapmirrored`关系的健康是 `true`。

5. 可选：在ONTAP CLI 中，运行以下命令查看SnapMirror关系的操作历史记录。

```
dest::> snapmirror show-history
```

或者，您可以挂载源卷和目标卷，将文件写入源卷，并验证卷是否复制到目标卷。

Google Cloud 管理

更改Cloud Volumes ONTAP的 Google Cloud 机器类型

在 Google Cloud 中启动Cloud Volumes ONTAP时，您可以从多种机器类型中进行选择。如果您确定实例或机器类型太小或太大，无法满足您的需求，您可以随时更改实例或机器类型。

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）。如果不是，则操作将失败。

  "ONTAP 9 文档：用于配置自动交还的命令"

- 更改机器类型可能会影响 Google Cloud 服务费用。
- 该操作重新启动Cloud Volumes ONTAP。

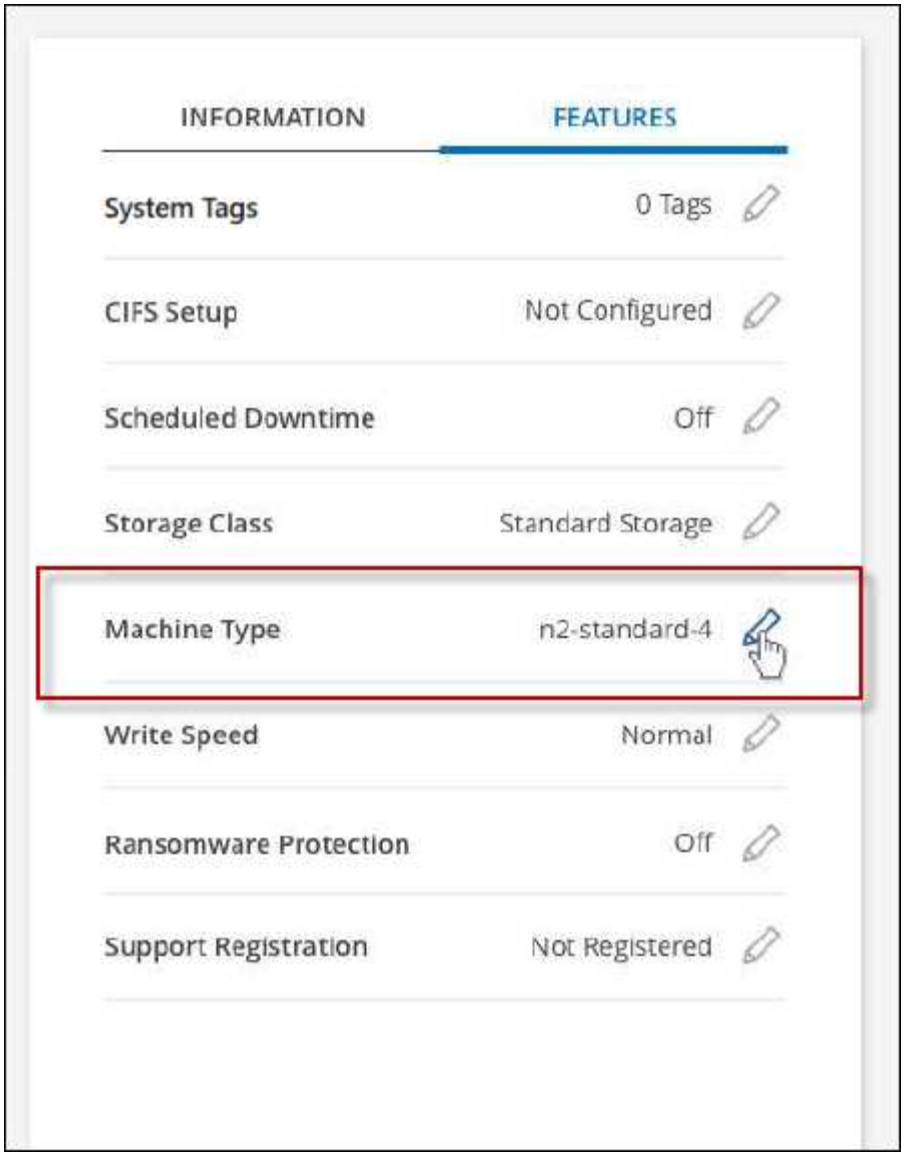
  对于单节点系统，I/O 被中断。

  对于 HA 对来说，这种变化是无中断的。 HA 对继续提供数据。

NetApp Console通过启动接管并等待返回来一次更改一个节点。 NetApp 的质量保证团队在此过程中对文件的写入和读取进行了测试，并且没有发现客户端的任何问题。随着连接的变化，在 I/O 级别观察到一些重试，但应用层克服了 NFS/CIFS 连接的重新连接。

步骤

1. 在*系统*页面上，选择系统。
2. 在概览选项卡上，单击功能面板，然后单击*机器类型*旁边的铅笔图标。



如果您使用的是基于节点的即用即付 (PAYGO) 许可证，则可以通过单击“许可证类型”旁边的铅笔图标来选择不同的许可证和机器类型。

1. 选择一种机器类型，选中复选框以确认您了解更改的含义，然后单击*更改*。

结果

Cloud Volumes ONTAP使用新配置重新启动。

将现有 **Cloud Volumes ONTAP** 部署转换为 **Infrastructure Manager**

从 2026 年 1 月 12 日起，Google Cloud 中的新 Cloud Volumes ONTAP 部署可以使用 Google Cloud Infrastructure Manager。Google 即将弃用 Google Cloud Deployment Manager，转而使用 Infrastructure Manager。因此，您需要手动运行过渡工具，将现有 Cloud Volumes ONTAP 部署从 Deployment Manager 转换为 Infrastructure Manager。这是一个一次性流程，之后您的系统将自动开始使用 Infrastructure Manager。

关于此任务

转换工具在 "NetApp 支持站点" 中可用，并创建以下工件：

- Terraform 工件，保存在 `conversion_output/deployment_name`中。
- 转化摘要，保存在 `conversion_output/batch_summary_<deployment_name>_<timestamp>.json`。
- 调试日志，保存在 `<gcp project number>-<region>-blueprint-config/<cvo name>` 目录中。您需要这些日志来进行故障排除。 `<gcp project number>-<region>-blueprint-config` 存储桶存储 Terraform 日志。

> 使用 Infrastructure Manager 的 Cloud Volumes ONTAP 系统将数据和记录存储在 Google Cloud Storage 存储桶中。您可能需要为这些存储桶支付额外费用，但不要编辑或删除存储桶或其内容：
>
> - `gs://netapp-cvo-infrastructure-manager-<project id>/dm-to-im-convert`: 用于存储 Cloud Volumes ONTAP Terraform 文件
> - `<gcp project number>-<region>-blueprint-config`: 用于存储 Google Cloud Terraform 工件

开始之前

- 确保您的 Cloud Volumes ONTAP 系统为 9.16.1 或更高版本。
- 请确保未从 Google Cloud Console 手动编辑任何 Cloud Volumes ONTAP 资源或其属性。
- 请确保已启用 Google Cloud API。请参阅 "启用 Google Cloud API"。请确保与其他 API 一起启用 Google Cloud Quotas API。
- 验证 NetApp Console 代理的服务帐户是否具有所需的所有权限。请参阅 "控制台代理的 Google Cloud 权限"。
- 转换工具使用以下域。在网络中的端口 443 上启用它们：

域	端口	协议	方向	目的
cloudresourcemanager.googleapis.com	443	TCP	EGRESS	项目验证
deploymentmanager.googleapis.com	443	TCP	EGRESS	部署发现
config.googleapis.com	443	TCP	EGRESS	基础架构管理器 API
storage.googleapis.com	443	TCP	EGRESS	GCS 存储桶操作
iam.googleapis.com	443	TCP	EGRESS	服务帐户验证
compute.googleapis.com	443	TCP	EGRESS	Google Cloud 和 Terraform Import 和 Plan 使用的计算 API 调用
openidconnect.googleapis.com	443	TCP	EGRESS	身份验证

域	端口	协议	方向	目的
oauth2.googleapis.com	443	TCP	EGRESS	OAuth2 令牌交换
registry.terraform.io	443	TCP	EGRESS	Terraform 提供程序注册表
releases.hashicorp.com	443	TCP	EGRESS	Terraform 二进制文件下载
apt.releases.hashicorp.com	443	TCP	EGRESS	HashiCorp APT 存储库
us-central1-docker.pkg.dev	443	TCP	EGRESS	GCP Artifact Registry
metadata.google.internal	80	HTTP	内部	VM 元数据和身份验证令牌

步骤

按照下面的步骤从部署管理器过渡到基础架构管理器，并为现有的 Cloud Volumes ONTAP 部署运行工具。

1. 创建角色并将其附加到服务帐户：
    a. 创建具有以下权限的 YAML 文件：

```
title: NetApp Dm TO IM Convert Solution
description: Permissions for the service account associated with the
VM where the tool will run.
stage: GA
includedPermissions:
- compute.addresses.get
- compute.disks.get
- compute.forwardingRules.get
- compute.healthChecks.get
- compute.instanceGroups.get
- compute.instances.get
- compute.regionBackendServices.get
- config.deployments.create
- config.deployments.get
- config.deployments.getLock
- config.deployments.lock
- config.deployments.unlock
- config.deployments.update
- config.deployments.delete
- config.deployments.updateState
- config.operations.get
- deploymentmanager.deployments.get
- deploymentmanager.deployments.list
- deploymentmanager.manifests.get
- iam.serviceAccounts.get
- storage.buckets.create
- storage.objects.create
- storage.objects.delete
- storage.objects.get
- storage.objects.list
```

b. 使用 YAML 文件中定义的权限在 Google Cloud 中创建自定义角色。
`gcloud iam roles create dmtoim_convert_tool_role --project=PROJECT_ID \
--file=YAML_FILE_PATH`有关详细信息，请参阅 "创建和管理自定义角色"。

c. 将自定义角色附加到将用于创建 VM 的服务帐户。

d. 将 `roles/iam.serviceAccountUser`角色添加到此服务帐户。请参阅 "服务账户概述"。

2. 使用以下配置创建虚拟机。在此虚拟机上运行工具。

- 机器类型：Google Compute Engine 机器类型 e2-medium
- 操作系统：Ubuntu 25.10 AMD64 Minimal（镜像：ubuntu-minimal-2510-amd64）
- 网络：允许 HTTP 和 HTTPS 的防火墙
- 磁盘大小：20GB
- 安全：服务帐户：您创建的服务帐户

- 安全性：访问范围 - 为每个 API 设置访问权限：
  - 云平台：已启用
  - Compute Engine：只读
  - 存储：只读（默认）
  - Google Cloud Logging（以前称为 Stackdriver Logging）API：仅写入（默认）
  - Stackdriver Monitoring（现已成为 Google Cloud Operations 的一部分）API：仅写入（默认）
  - 服务管理：只读（默认）
  - 服务控制：已启用（默认）
  - Google Cloud Trace（以前称为 Stackdriver Trace）：仅写入（默认）

3. 使用 SSH 连接到新创建的虚拟机： `gcloud compute ssh dmtoim-convert-executor-vm --zone <region where VM is deployed>`
4. 使用您的 NSS 凭据从 "NetApp 支持站点"下载转换工具： `wget <download link from NetApp Support site>`
5. 提取下载的 TAR 文件： `tar -xvf <downloaded file name>`
6. 下载并安装以下必备软件包：
   - Docker：28.2.2 build 28.2.2-0ubuntu1 或更高版本
   - Terraform：1.14.1 或更高版本
   - Python：3.13.7、python3-pip、python3 venv

   ```
   sudo apt-get update
   sudo apt-get install python3-pip python3-venv -y
   wget -O - https://apt.releases.hashicorp.com/gpg | sudo gpg --dearmor
   -o /usr/share/keyrings/hashicorp-archive-keyring.gpg
   echo "deb [arch=$(dpkg --print-architecture) signed-
   by=/usr/share/keyrings/hashicorp-archive-keyring.gpg]
   https://apt.releases.hashicorp.com noble main" | sudo tee
   /etc/apt/sources.list.d/hashicorp.list
   sudo apt update && sudo apt install terraform
   sudo apt-get install -y docker.io
   sudo systemctl start docker
   ```

   Google Cloud CLI `gcloud` 已预安装在虚拟机上。

7. 将当前用户添加到 Docker 组中，以便该工具可以在没有 `sudo`权限的情况下使用 Docker。

   ```
   sudo usermod -aG docker $USER
   newgrp docker
   ```

8. 安装转换工具：

```
cd <folder where you extracted the tool>
 ./install.sh
```

这将在隔离环境中安装工具， `dmconvert-venv`，并验证是否已安装所有必需的软件包。

9. 输入安装工具的环境： `source dmconvert-venv/bin/activate`
10. 以 `non-sudo` 用户身份运行转换工具。请确保使用与 Console 代理的服务帐户相同的服务帐户，并且服务帐户具有所有 "Google Cloud Infrastructure Manager 的必要权限"。

```
dmconvert \
--project-id=<the Google Cloud project ID for the Cloud Volumes ONTAP
deployment> \
--cvo-name=<Cloud Volumes ONTAP system name> \
--service-account=<the service account attached to the Console agent>
```

完成后

该工具显示所有 Cloud Volumes ONTAP 系统和 SVM 详细信息的列表。当它完成运行时，您可以看到所有已转换系统的状态。每个转换后的系统都以 *<converted system name-imdeploy>* 格式显示在 Google Console 的 Infrastructure Manager 下，表明 Console 现在使用 Infrastructure Manager API 来管理该 Cloud Volumes ONTAP 系统。

转换后，请勿在 Google Cloud Console 中删除 Deployment Manager 的部署对象。此部署对象包含 Infrastructure Manager 用于管理 Cloud Volumes ONTAP 系统的元数据。

如果需要回滚转换，则必须使用相同的 VM。如果已转换所有系统，并且不需要回滚到 Deployment Manager，则可以删除 VM。

回滚转换

如果不想继续转换，可以按照以下步骤回滚到 Deployment Manager：

步骤

1. 在同一个 为运行工具而创建的虚拟机 上，运行此命令：

```
dmconvert \
--project-id=<the Google Cloud project ID for the Cloud Volumes ONTAP
deployment> \
--cvo-name=<Cloud Volumes ONTAP system name> \
--service-account=<the service account attached to the Console agent> \
--rollback
```

2. 等待回滚完成。

相关链接

- "NetApp Console Agent 4.2.0 发行说明"
- "Google Cloud Infrastructure Manager 所需的权限"

使用系统管理器管理Cloud Volumes ONTAP

Cloud Volumes ONTAP中的高级存储管理功能可通过ONTAP系统管理器 (ONTAP System Manager) 使用，它是ONTAP系统提供的管理界面。您可以直接从NetApp Console访问系统管理器。

功能

您可以使用控制台中的ONTAP系统管理器执行各种存储管理功能。以下列表包含其中一些功能，但并不详尽：

- 高级存储管理：管理一致性组、共享、qtree、配额和存储虚拟机。
- 成交量变动： "将卷移动到不同的聚合。"
- 网络管理：管理 IP 空间、网络接口、端口集和以太网端口。
- 管理FlexGroup卷：您只能通过系统管理器创建和管理FlexGroup卷。BlueXP控制台不支持FlexGroup卷创建。
- 事件和作业：查看事件日志、系统警报、作业和审计日志。
- 高级数据保护：保护存储虚拟机、LUN 和一致性组。
- 主机管理：设置 SAN 启动器组和 NFS 客户端。
- ONTAP S3 对象存储管理：Cloud Volumes ONTAP 中的 ONTAP S3 存储管理功能仅在 System Manager 中可用，在 Console 中不可用。

支持的配置

- 标准云区域中的Cloud Volumes ONTAP 9.10.0 及更高版本可通过ONTAP System Manager 进行高级存储管理。
- GovCloud 区域或没有出站互联网访问的区域不支持系统管理器集成。

限制

Cloud Volumes ONTAP不支持系统管理器界面中显示的一些功能：

- NetApp Cloud Tiering： Cloud Volumes ONTAP不支持 Cloud Tiering。创建卷时，您应该直接从标准视图设置数据分层到对象存储。
- 层级：系统管理器不支持聚合管理（包括本地层级和云层级）。您必须直接从标准视图管理聚合。
- 固件升级： Cloud Volumes ONTAP不支持从系统管理器的 集群 **>** 设置 页面进行自动固件更新。
- 基于角色的访问控制：系统管理器不支持基于角色的访问控制。
- SMB 持续可用性 (CA)： Cloud Volumes ONTAP不支持 "持续可用的 SMB 共享"实现无中断运行。

配置访问系统管理器的身份验证

作为管理员，您可以为从控制台访问ONTAP系统管理器的用户激活身份验证。您可以根据ONTAP用户角色确定正确的访问权限级别，并根据需要启用或禁用身份验证。如果启用身份验证，则用户每次从控制台访问系统管理器或重新加载页面时都需要输入其ONTAP用户凭据，因为控制台不会在内部存储凭据。如果您禁用身份验证，用户可以使用管理员凭据访问系统管理器。

此设置适用于您组织或帐户中的ONTAP用户的每个控制台代理，无论Cloud Volumes ONTAP系统如何。

所需权限

您需要分配组织或帐户管理员权限才能修改Cloud Volumes ONTAP用户身份验证的控制台代理设置。

步骤

1. 从左侧导航窗格转到*管理>代理*。
2. 点击 ••• 所需控制台代理的图标并选择*编辑控制台代理*。
3. 在*强制用户凭据*下，选中*启用/禁用*复选框。默认情况下，身份验证是禁用的。

   如果将此值设置为*启用*，身份验证将被重置，并且您必须修改任何现有工作流程以适应此更改。

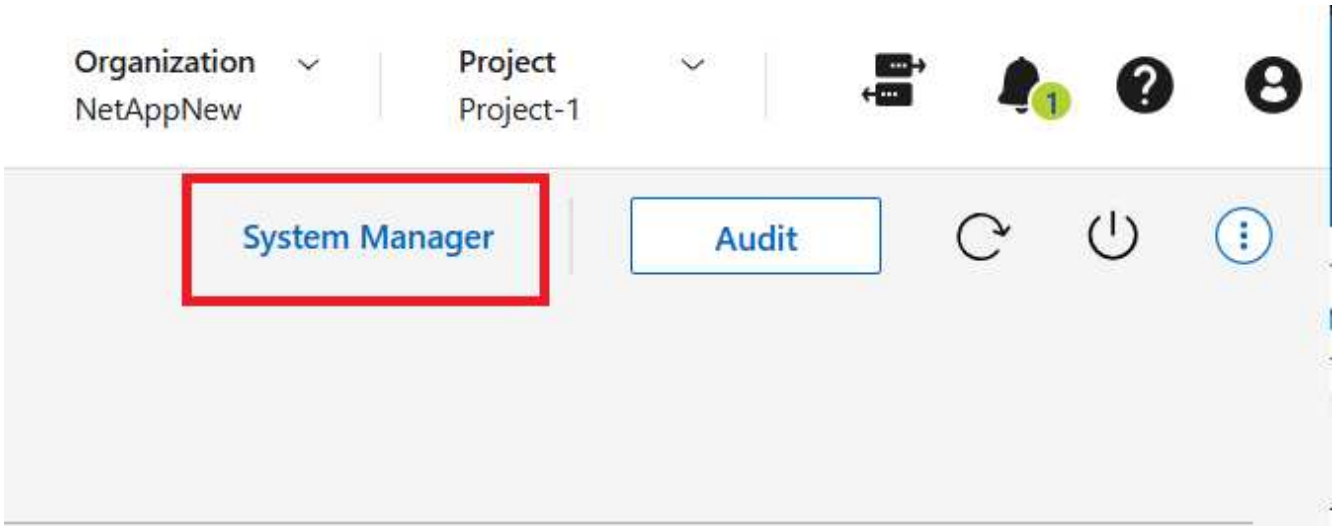
4. 单击“保存”。

开始使用系统管理器

您可以从Cloud Volumes ONTAP系统访问ONTAP System Manager。

步骤

1. 从左侧导航菜单中，选择“存储”>“管理”。
2. 在*系统*页面上，双击所需的Cloud Volumes ONTAP系统。
3. 单击“系统管理器”。



4. 如果出现提示，请输入您的ONTAP用户凭据并单击 登录。
5. 如果出现确认消息，请仔细阅读并单击“关闭”。

使用系统管理器来管理您的Cloud Volumes ONTAP系统。您可以单击“返回”返回控制台。

有关使用系统管理器的帮助

如果您需要有关使用 System Manager 和Cloud Volumes ONTAP 的帮助，您可以参考 "ONTAP 文档"以获得分步说明。以下是一些可能有帮助的ONTAP文档链接：

- "ONTAP角色、应用程序和身份验证"
- "使用 System Manager 访问集群" 。
- "卷和 LUN 管理"
- "网管"
- "数据保护"
- "创建持续可用的 SMB 共享"

从 CLI 管理Cloud Volumes ONTAP

Cloud Volumes ONTAP CLI 使您能够运行所有管理命令，对于高级任务或您更喜欢使用 CLI 来说，它是一个不错的选择。您可以使用安全外壳 (SSH) 连接到 CLI。

开始之前

使用 SSH 连接到Cloud Volumes ONTAP 的主机必须具有与Cloud Volumes ONTAP 的网络连接。例如，您可能需要从云提供商网络中的跳转主机进行 SSH。

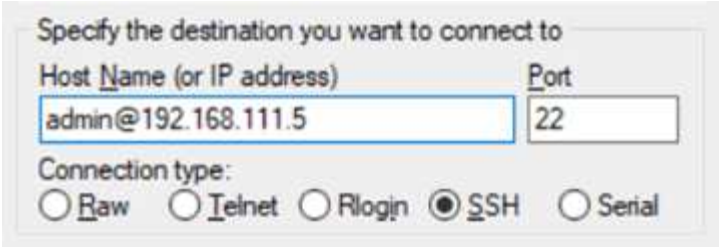
> 当部署在多个 AZ 中时， Cloud Volumes ONTAP HA 配置使用浮动 IP 地址作为集群管理接口，这意味着外部路由不可用。您必须从属于同一路由域的主机进行连接。

步骤

1. 在NetApp Console中，确定集群管理接口的 IP 地址：
   a. 从左侧导航菜单中，选择“存储”>“管理”。
   b. 在*系统*页面上，选择Cloud Volumes ONTAP系统。
   c. 复制右侧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。

   例子

   下图显示了使用 PuTTY 的示例：



3. 在登录提示符下，输入管理员帐户的密码。

   例子

```
Password: ********
COT2::>
```

版权信息

版权所有 © 2026 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，本文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。