



使用 **Cloud Volumes ONTAP**

Cloud Volumes ONTAP

NetApp
June 27, 2024

目录

使用 Cloud Volumes ONTAP	1
许可证管理	1
卷和 LUN 管理	14
聚合管理	40
Storage VM 管理	45
安全性和数据加密	79
系统管理	91
系统运行状况和事件	122

使用 Cloud Volumes ONTAP

许可证管理

管理基于容量的许可证

通过BlueXP数字钱包管理基于容量的许可证、确保您的NetApp帐户具有足够的容量来支持您的Cloud Volumes ONTAP 系统。

capacity-based licenses 使您能够按每 TiB 容量为 Cloud Volumes ONTAP 付费。

通过 [BlueXP数字钱包](#)、您可以从一个位置管理Cloud Volumes ONTAP 的许可证。您可以添加新许可证并更新现有许可证。

["了解有关 Cloud Volumes ONTAP 许可证的更多信息"](#)。

如何将许可证添加到BlueXP电子钱包中

从NetApp销售代表购买许可证后、NetApp将向您发送一封电子邮件、其中包含序列号和其他许可详细信息。

同时、BlueXP会自动查询NetApp的许可服务、以获取与您的NetApp 支持站点 帐户关联的许可证的详细信息。如果没有错误、BlueXP会自动将许可证添加到电子钱包中。

如果BlueXP无法添加许可证、您需要手动将其添加到电子钱包中。例如、如果Connector安装在无法访问Internet的位置、则您需要自己添加许可证。 [了解如何向您的帐户添加已购买的许可证](#)。

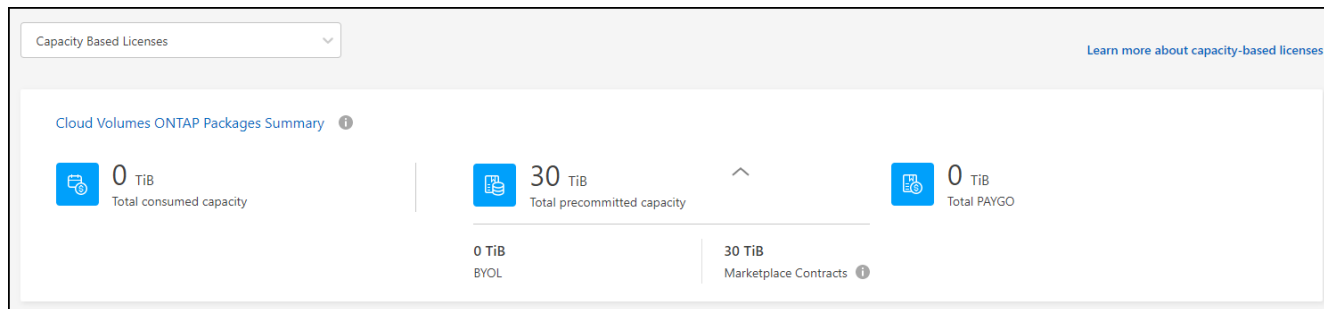
查看帐户中的已用容量

BlueXP数字钱包可显示帐户中的总已用容量以及按许可包计算的已用容量。这有助于您了解如何为您付费以及是否需要购买额外容量。

步骤

1. 从BlueXP导航菜单中、选择*[监管](#)>数字电子钱包*。
2. 在* [Cloud Volumes ONTAP 基于容量的许可证](#)*选项卡上、保持选中状态。
3. 查看软件包摘要、其中显示了已用容量、预提交的总容量和总PAYGO容量。
 - [_Total consumed capacity_](#) 是您的NetApp帐户中所有Cloud Volumes ONTAP 系统的总已配置容量。费用根据每个卷的配置大小计算、而不考虑卷中的本地、已用、已存储或有效空间。
 - [_Total precommitted capacity_](#) 是您从NetApp购买的总许可容量(BYOL或Marketplace合同)。
 - [_Total PAYGO_](#) 是使用云市场订阅的总配置容量。只有在已用容量高于许可容量或BlueXP电子钱包中没有BYOL许可证时、才会使用通过PAYGO充电。

以下是BlueXP电子钱包中的Cloud Volumes ONTAP 软件包摘要示例：



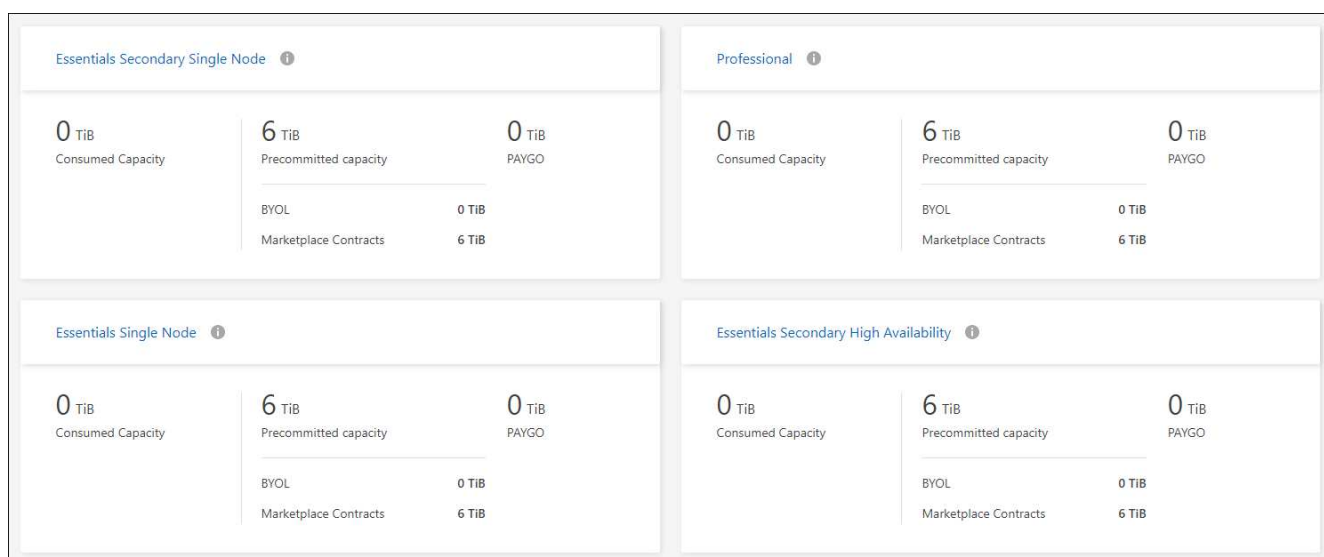
4. 在摘要下、查看每个许可包的已用容量。

- _consumed capacity_显示该软件包的卷容量。有关特定软件包的详细信息、请将鼠标悬停在工具提示上。

要更好地了解Essentials软件包显示的容量、您应熟悉充电的工作原理。"[了解Essentials软件包的收费信息](#)"。

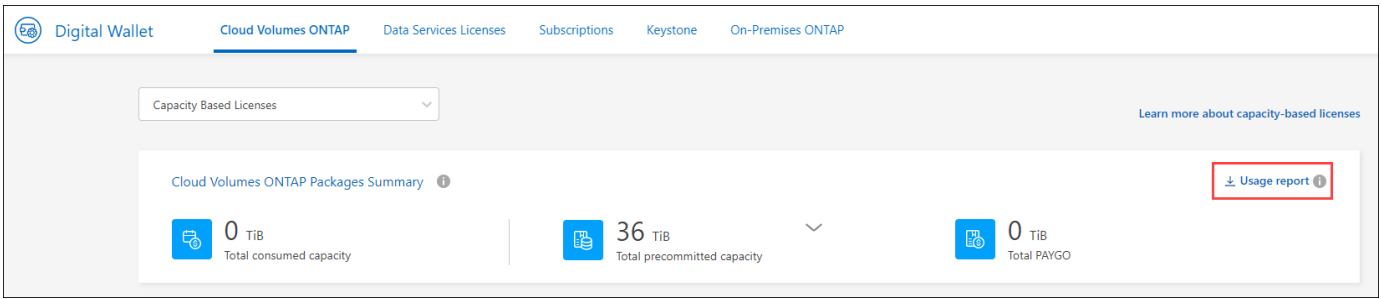
- _Precommitted Capacity_是您从NetApp购买的许可容量(BYOL或Marketplace合同)。
 - _BYOL_显示您从NetApp为此软件包类型购买的许可容量。
 - _Marketplace Contracts_显示您随此软件包类型的Marketplace合同购买的许可容量。
- _PAYGO_按许可证使用模式显示已用容量。

以下是具有多个许可包的帐户的示例：



下载使用情况报告

帐户管理员可以从BlueXP中的电子钱包下载四份使用情况报告。这些使用情况报告提供了您的订阅的容量详细信息、并告诉您Cloud Volumes ONTAP 订阅中的资源收费情况。可下载的报告可捕获某个时间点的数据、并可轻松与他人共享。



以下报告可供下载。显示的容量值以TiB为单位。

- 高级使用情况：此报告显示了数字钱包中“Cloud Volumes ONTAP 软件包摘要”卡的确切内容。其中包括以下信息：
 - 总已用容量
 - 预先提交的总容量
 - 总BYOL容量
 - Marketplace合同总容量
 - PAYGO总容量
- * Cloud Volumes ONTAP 封装使用情况*：此报告显示了电子钱包中封装卡的确切内容。其中包括除优化I/O包之外的每个软件包的以下信息：
 - 总已用容量
 - 预先提交的总容量
 - 总BYOL容量
 - Marketplace合同总容量
 - PAYGO总容量
- * Storage VM使用情况*：此报告显示如何在Cloud Volumes ONTAP 系统和Storage Virtual Machine (SVM) 之间细分已充电容量。电子钱包中的任何屏幕均不提供此信息。其中包括以下信息：
 - 工作环境ID和名称(显示为UUID)
 - 云
 - NetApp帐户ID
 - 工作环境配置
 - SVM name
 - 已配置容量
 - 已充电容量汇总
 - 商城账单条款
 - Cloud Volumes ONTAP 软件包或功能
 - 收取SaaS Marketplace订阅名称费用
 - 向SaaS Marketplace订阅ID收费
 - 工作负载类型

- 卷使用量：此报告显示如何在工作环境中按卷细分已充电容量。电子钱包中的任何屏幕均不提供此信息。其中包括以下信息：
 - 工作环境ID和名称(显示为UUID)
 - SVN名称
 - 卷 ID
 - Volume type
 - 卷配置容量



此报告不包括FlexClone卷、因为这些类型的卷不会产生费用。

步骤

1. 从BlueXP导航菜单中、选择*监管>数字电子钱包*。
2. 在*Usage* Cloud Volumes ONTAP 选项卡上，保持选中*基于容量的许可证*，然后单击*使用情况报告*。

将下载使用情况报告。

3. 打开下载的文件以访问报告。

将已购买的许可证添加到您的帐户

如果在BlueXP电子钱包中看不到已购买的许可证、则需要将这些许可证添加到BlueXP中、以便Cloud Volumes ONTAP 可以使用这些容量。

您需要的内容

- 您需要为BlueXP提供许可证或许可证文件的序列号。
- 如果要输入序列号，首先需要输入 "[将您的NetApp 支持站点 帐户添加到BlueXP](#)"。这是有权访问序列号的NetApp 支持站点帐户。

步骤

1. 从BlueXP导航菜单中、选择*监管>数字电子钱包*。
2. 在* Cloud Volumes ONTAP 基于容量的许可证*选项卡上、保持选中状态、然后单击*添加许可证*。
3. 输入基于容量的许可证的序列号或上传许可证文件。

如果您输入了序列号，则还需要选择有权访问此序列号的 NetApp 支持站点帐户。

4. 单击 * 添加许可证 * 。

更新基于容量的许可证

如果您购买了额外容量或延长了许可证期限、BlueXP会自动更新电子钱包中的许可证。您无需执行任何操作。

但是、如果您在无法访问Internet的位置部署了BlueXP、则需要在BlueXP中手动更新许可证。

您需要的内容

许可证文件（如果有 HA 对，则为 *files*）。

步骤

1. 从BlueXP导航菜单中、选择*监管>数字电子钱包*。
2. 在* Cloud Volumes ONTAP 选项卡上、单击许可证旁边的操作菜单、然后选择*更新许可证*。
3. 上传许可证文件。
4. 单击 * 上传许可证 * 。

更改充电方法

您可以更改使用基于容量的许可的Cloud Volumes ONTAP 系统的收费方法。例如、如果您使用Essentials软件包部署了Cloud Volumes ONTAP 系统、则可以在业务需求发生变化时将其更改为"Professional软件包"。

限制

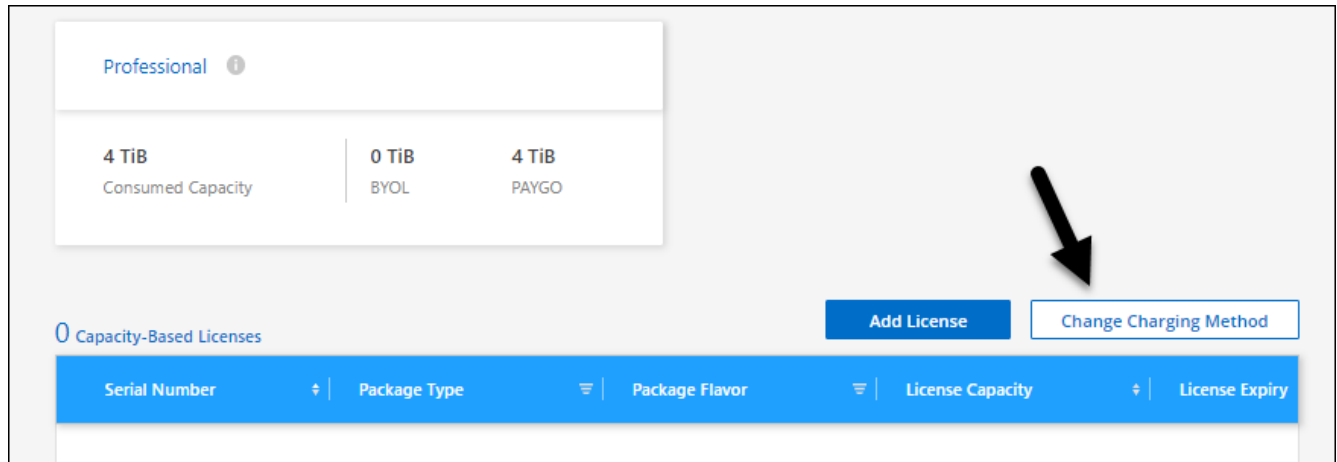
不支持更改Edge Cache许可证或从Edge Cache许可证更改。

重要注意事项

如果您在云提供商的市场上有私人优惠或合同、则更改为合同中未包含的收费方式将导致对BYOL (如果您从NetApp购买了许可证)或PAYGO进行收费。

步骤

1. 从BlueXP导航菜单中、选择*监管>数字电子钱包*。
2. 在* Cloud Volumes ONTAP 选项卡上、单击*更改充电方法*。



3. 选择一工作环境、选择新的充电方式、然后确认您已了解更改软件包类型将影响服务费用。

Change Charging Method

Select a working environment

CloudVolumesONTAP2

Current Cloud Volumes ONTAP charging method

Freemium

Select new Cloud Volumes ONTAP charging method

Essential

I understand that changing the package type will affect service charges

Change Charging Method Cancel

4. 单击*更改充电方法*。

结果

BlueXP更改了Cloud Volumes ONTAP 系统的充电方法。

您可能还会注意到、BlueXP数字钱包会刷新每种包类型的已用容量、以反映您刚刚所做的更改。

删除基于容量的许可证

如果基于容量的许可证已过期且不再使用，则可以随时将其删除。

步骤

1. 从BlueXP导航菜单中、选择*监管>数字电子钱包*。
2. 在* Cloud Volumes ONTAP 删除许可证*选项卡上、单击许可证旁边的操作菜单、然后选择*删除许可证*。
3. 单击 * 删除 * 进行确认。

管理Keystone订阅

通过启用与Cloud Volumes ONTAP 配合使用的订阅、从BlueXP数字钱包管理Keystone订阅。您还可以请求更改已提交容量，并取消订阅链接。

Keystone订阅是NetApp提供的"按需购买"存储服务。

通过_ BlueXP数字钱包_、您可以从一个位置管理Cloud Volumes ONTAP 的许可证。您可以添加新许可证并更新

现有许可证。

["了解有关 Cloud Volumes ONTAP 许可证的更多信息"](#)。

授权您的帐户

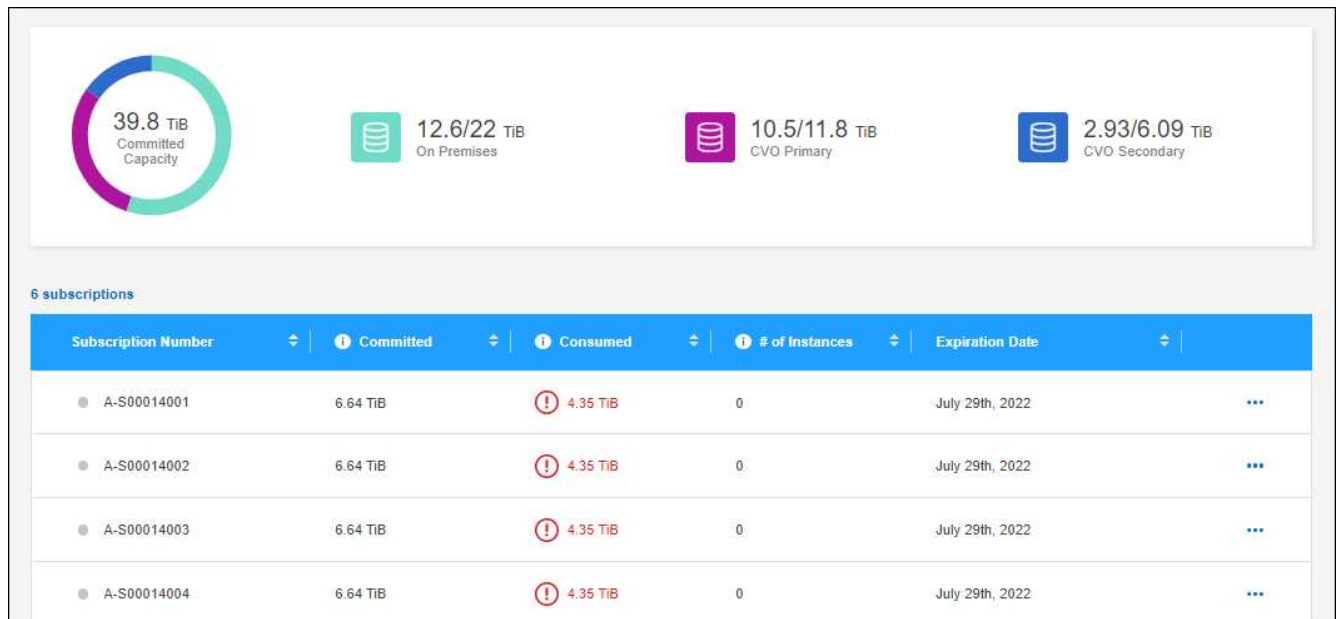
在BlueXP中使用和管理Keystone订阅之前、您需要联系NetApp、为您的BlueXP用户帐户授权Keystone订阅。

步骤

1. 从BlueXP导航菜单中、选择*监管>数字电子钱包*。
2. 选择* Keystone*。
3. 如果您看到 * 欢迎使用 NetApp Keystone * 页面，请向此页面上列出的地址发送电子邮件。

NetApp 代表将通过授权您的用户帐户访问订阅来处理您的请求。

4. 返回到* Keystone订阅*查看您的订阅。



下一步是什么？

链接要用于 Cloud Volumes ONTAP 的订阅。

链接订阅

在NetApp授权您的帐户后、您需要链接Keystone订阅、以便用于Cloud Volumes ONTAP。通过此操作，用户可以选择订阅作为新 Cloud Volumes ONTAP 系统的收费方法。

步骤

1. 从BlueXP导航菜单中、选择*监管>数字电子钱包*。
2. 选择* Keystone*。
3. 对于要链接的订阅，请单击 ... 并选择 * 链接 * 。

Subscription Number	Committed	Consumed	# of Instances	Expiration Date	
A-S00014001	6.64 TiB	4.35 TiB	0	July 29th, 2022	⋮
A-S00014002	6.64 TiB	4.35 TiB	0	July 29th, 2022	View detail and edit
A-S00014003	6.64 TiB	4.35 TiB	0	July 29th, 2022	Link

结果

现在，订阅将链接到您的BlueXP帐户、并可在创建Cloud Volumes ONTAP 工作环境时进行选择。

请求更多或更少的已提交容量

如果您需要调整订阅的已提交容量、可以直接从BlueXP界面发送请求。

步骤

1. 从BlueXP导航菜单中、选择*监管>数字电子钱包*。
2. 选择* Keystone*。
3. 对于要调整容量的订阅，请单击 ⋮ 并选择 * 查看详细信息并编辑 *。
4. 输入一个或多个订阅请求的已提交容量。

Subscription Modification for A-S00014001

Service Level	Current Committed Capacity	Current Consumed Capacity	Requested Committed Capacity
Extreme	0.977 TiB	0.293 TiB	<input type="text" value="Enter amount"/> TiB
Premium	0.977 TiB	0.488 TiB	<input type="text" value="Enter amount"/> TiB
Performance	0 TiB	0 TiB	<input type="text" value="Enter amount"/> TiB
Standard	0.732 TiB	0.439 TiB	<input type="text" value="Enter amount"/> TiB
Value	0.977 TiB	0.879 TiB	<input type="text" value="Enter amount"/> TiB
Data Tiering	0 TiB	0 TiB	<input type="text" value="Enter amount"/> TiB
CVO Primary	1.96 TiB	1.76 TiB	<input type="text" value="3"/> TiB
CVO Secondary	1.02 TiB	0.488 TiB	<input type="text" value="Enter amount"/> TiB

Additional Information

Is there anything else we should know about your request?
Please be as descriptive as possible.

Enter your notes here

5. 向下滚动，输入请求的任何其他详细信息，然后单击 * 提交 *。


结果

您的请求会在 NetApp 系统中创建一个服务单以供处理。

取消订阅链接

如果您不想再对新的Cloud Volumes ONTAP 系统使用Keystone订阅、则可以取消订阅链接。请注意，您只能取消链接未附加到现有 Cloud Volumes ONTAP 订阅的订阅。

步骤

1. 从BlueXP导航菜单中、选择*监管>数字电子钱包*。
2. 选择* Keystone*。
3. 对于要取消链接的订阅，请单击  并选择 * 取消链接 *。

结果

订阅将与您的BlueXP帐户解除链接、并且在创建Cloud Volumes ONTAP 工作环境时无法再选择此订阅。

管理基于节点的许可证

在BlueXP数字钱包中管理基于节点的许可证、以确保每个Cloud Volumes ONTAP 系统都具有具有所需容量的有效许可证。

基于节点的许可证 _ 是上一代许可模式（不适用于新客户）：

- 从 NetApp 购买的 BYOL 许可证
- 从云提供商的市场订阅每小时按需购买（PAYGO）

通过 BlueXP数字钱包、您可以从一个位置管理Cloud Volumes ONTAP 的许可证。您可以添加新许可证并更新现有许可证。

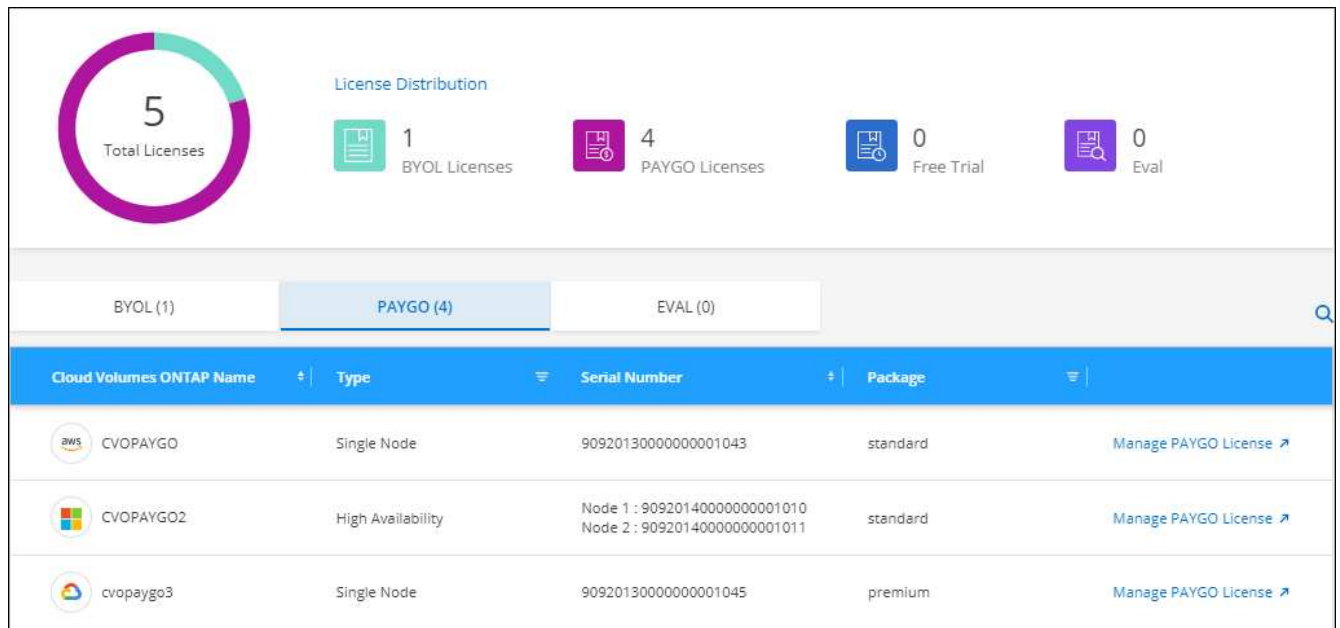
["了解有关 Cloud Volumes ONTAP 许可证的更多信息"](#)。

管理PAYGO许可证

通过BlueXP数字钱包页面、您可以查看有关每个PAYGO Cloud Volumes ONTAP 系统的详细信息、包括序列号和PAYGO许可证类型。

步骤

1. 从BlueXP导航菜单中、选择*监管>数字电子钱包*。
2. 在* Cloud Volumes ONTAP 基于节点的许可证*选项卡上、从下拉列表中选择*基于节点的许可证*。
3. 单击 * PAYGO*。
4. 在表中查看有关每个 PAYGO 许可证的详细信息。



5. 如果需要，请单击 * 管理 PAYGO 许可证 * 以更改 PAYGO 许可证或更改实例类型。

管理 BYOL 许可证

通过添加和删除系统许可证和额外容量许可证来管理直接从 NetApp 购买的许可证。

添加未分配的许可证

将基于节点的许可证添加到BlueXP数字工具包中、以便在创建新的Cloud Volumes ONTAP 系统时选择此许可证。电子钱包将这些许可证标识为_UNASSERUDE_。

步骤

1. 从BlueXP导航菜单中、选择*监管>数字电子钱包*。
2. 在* Cloud Volumes ONTAP 基于节点的许可证*选项卡上、从下拉列表中选择*基于节点的许可证*。
3. 单击 * 未分配 *。
4. 单击 * 添加未分配的许可证 *。
5. 输入许可证的序列号或上传许可证文件。

如果您还没有许可证文件，请参阅以下部分。

6. 单击 * 添加许可证 *。

结果

BlueXP将许可证添加到电子钱包中。在将许可证与新的 Cloud Volumes ONTAP 系统关联之前，此许可证将被标识为未分配。之后，许可证将移至数字钱包中的*BYOL*选项卡。

Exchange 未分配的基于节点的许可证

如果您尚未使用Cloud Volumes ONTAP 的基于节点的未分配许可证、则可以通过将其转换为BlueXP备份和恢复许可证、BlueXP分类许可证或BlueXP分层许可证来交换此许可证。

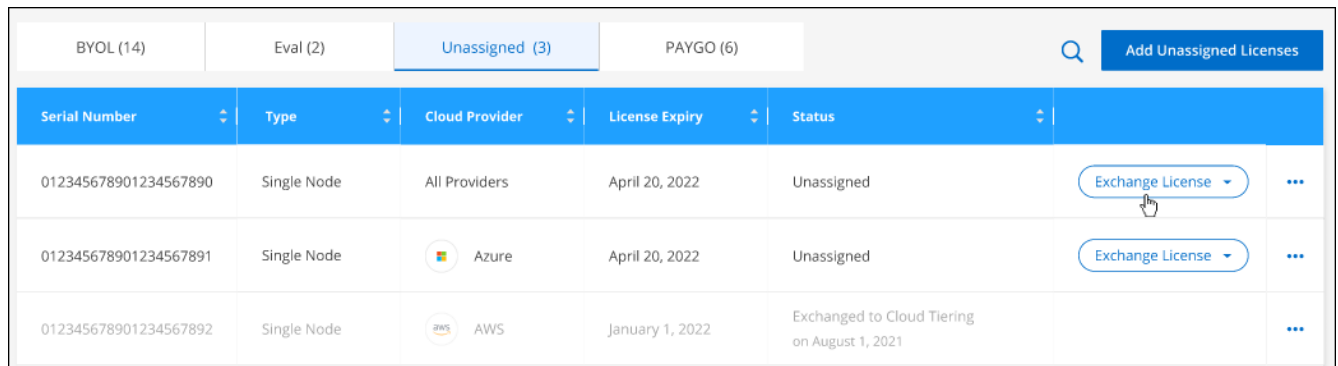
交换许可证将撤消 Cloud Volumes ONTAP 许可证并为此服务创建一个等价于美元的许可证：

- Cloud Volumes ONTAP HA 对的许可转换为 51 TiB 数据服务许可证
- Cloud Volumes ONTAP 单个节点的许可将转换为 32 TiB 数据服务许可证

转换后的许可证与 Cloud Volumes ONTAP 许可证具有相同的到期日期。

步骤

1. 从BlueXP导航菜单中、选择*监管>数字电子钱包*。
2. 在* Cloud Volumes ONTAP 基于节点的许可证*选项卡上、从下拉列表中选择*基于节点的许可证*。
3. 单击 * 未分配 *。
4. 单击 * Exchange 许可证 *。



Serial Number	Type	Cloud Provider	License Expiry	Status	
012345678901234567890	Single Node	All Providers	April 20, 2022	Unassigned	Exchange License
012345678901234567891	Single Node	Azure	April 20, 2022	Unassigned	Exchange License
012345678901234567892	Single Node	AWS	January 1, 2022	Exchanged to Cloud Tiering on August 1, 2021	

5. 选择要与之交换许可证的服务。
6. 如果出现提示，请为此 HA 对选择一个额外的许可证。
7. 阅读法律同意书，然后单击 * 同意 *。

结果

BlueXP会将未分配的许可证转换为您选择的服务。您可以在 * 数据服务许可证 * 选项卡中查看新许可证。

获取系统许可证文件

在大多数情况下、BlueXP可以使用您的NetApp 支持站点 帐户自动获取您的许可证文件。但是，如果无法上传，则需要手动上传许可证文件。如果您没有许可证文件，可以从 netapp.com 获取该文件。

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 *

License Generator

The following fields are pre-populated based on the NetApp SSO login provided.
To download the corresponding NetApp license file, re-enter your SSO password along with the correct Product Line and Product Serial number.

First Name

Last Name

Company

Email Address

Username

Product Line*

ONTAP Select - Standard
 ONTAP Select - Premium
 ONTAP Select - Premium XL
 Cloud Volumes ONTAP for AWS (single node)
 Cloud Volumes ONTAP for AWS (HA)
 Cloud Volumes ONTAP for GCP (single node or HA)
 Cloud Volumes ONTAP for Microsoft Azure (single node)
 Cloud Volumes ONTAP for Microsoft Azure (HA)
 Service Level Manager - SLO Advanced
 StorageGRID Webscale
 StorageGRID WhiteBox
 SnapCenter Standard (capacity-based)

Not only is protecting your data required by law, it's also the right thing to do. [Learn more](#)

I have read NetApp's new **Global Data Privacy Policy** and agree that NetApp may use my personal data.

3. 选择是通过电子邮件还是直接下载接收 serialnumber.nif JSON 文件。

更新系统许可证

在联系NetApp代表续订BYOL订阅时、BlueXP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BlueXP无法通过安全Internet连接访问此许可证文件、您可以自行获取此文件、然后手动将此文件上传到BlueXP。

步骤

1. 从BlueXP导航菜单中、选择*监管>数字电子钱包*。
2. 在* Cloud Volumes ONTAP 基于节点的许可证*选项卡上、从下拉列表中选择*基于节点的许可证*。
3. 在 * BYOL* 选项卡中, 展开 Cloud Volumes ONTAP 系统的详细信息。
4. 单击系统许可证旁边的操作菜单, 然后选择 * 更新许可证 *。
5. 上传许可证文件 (如果有 HA 对, 则上传文件)。
6. 单击 * 更新许可证 *。

结果

BlueXP会更新Cloud Volumes ONTAP 系统上的许可证。

管理额外容量许可证

您可以为 Cloud Volumes ONTAP BYOL 系统购买额外容量许可证, 以分配比 BYOL 系统许可证提供的 368 TiB

以上的容量。例如，您可以额外购买一个许可证容量，以便为 Cloud Volumes ONTAP 分配高达 736 TiB 的容量。或者，您也可以购买三个额外容量许可证，以获得高达 1.4 PiB 的容量。

您可以为单节点系统或 HA 对购买的许可证数量不受限制。

添加容量许可证

通过BlueXP右下角的聊天图标联系我们、购买额外容量许可证。购买许可证后，您可以将其应用于 Cloud Volumes ONTAP 系统。

步骤

1. 从BlueXP导航菜单中、选择*监管>数字电子钱包*。
2. 在* Cloud Volumes ONTAP 基于节点的许可证*选项卡上、从下拉列表中选择*基于节点的许可证*。
3. 在 * BYOL* 选项卡中，展开 Cloud Volumes ONTAP 系统的详细信息。
4. 单击 * 添加容量许可证 *。
5. 输入序列号或上传许可证文件（如果有 HA 对，则为文件）。
6. 单击 * 添加容量许可证 *。

更新容量许可证

如果您延长了额外容量许可证的期限、则需要在BlueXP中更新此许可证。

步骤

1. 从BlueXP导航菜单中、选择*监管>数字电子钱包*。
2. 在* Cloud Volumes ONTAP 基于节点的许可证*选项卡上、从下拉列表中选择*基于节点的许可证*。
3. 在 * BYOL* 选项卡中，展开 Cloud Volumes ONTAP 系统的详细信息。
4. 单击容量许可证旁边的操作菜单，然后选择 * 更新许可证 *。
5. 上传许可证文件（如果有 HA 对，则上传文件）。
6. 单击 * 更新许可证 *。

删除容量许可证

如果额外容量许可证已过期且不再使用，则可以随时将其删除。

步骤

1. 从BlueXP导航菜单中、选择*监管>数字电子钱包*。
2. 在* Cloud Volumes ONTAP 基于节点的许可证*选项卡上、从下拉列表中选择*基于节点的许可证*。
3. 在 * BYOL* 选项卡中，展开 Cloud Volumes ONTAP 系统的详细信息。
4. 单击容量许可证旁边的操作菜单，然后选择 * 删除许可证 *。
5. 单击 * 删除 *。

将评估版许可证转换为 **BYOL**

评估许可证有效期为 30 天。您可以在评估版许可证之上应用新的 BYOL 许可证，以便进行原位升级。

将评估版许可证转换为BYOL后、BlueXP将重新启动Cloud Volumes ONTAP 系统。

- 对于单节点系统，重新启动会在重新启动过程中导致 I/O 中断。
- 对于 HA 对，重新启动将启动接管和交还，以继续为客户端提供 I/O 。

步骤

1. 从BlueXP导航菜单中、选择*监管>数字电子钱包*。
2. 在* Cloud Volumes ONTAP 基于节点的许可证*选项卡上、从下拉列表中选择*基于节点的许可证*。
3. 单击 * 评估 * 。
4. 在表中，单击 Cloud Volumes ONTAP 系统的 * 转换为 BYOL 许可证 * 。
5. 输入序列号或上传许可证文件。
6. 单击 * 转换许可证 * 。

结果

BlueXP将启动转换过程。在此过程中， Cloud Volumes ONTAP 会自动重新启动。备份时，许可信息将反映新许可证。

PAYGO和BYOL之间的更改

不支持将系统从PAYGO单节点许可转换为BYOL单节点许可(反之亦然)。如果要在按需购买订阅和BYOL订阅之间切换、则需要部署新系统并将现有系统中的数据复制到新系统。

步骤

1. 创建新的 Cloud Volumes ONTAP 工作环境。
2. 在系统之间为需要复制的每个卷设置一次性数据复制。

["了解如何在系统之间复制数据"](#)

3. 通过删除原始工作环境来终止不再需要的 Cloud Volumes ONTAP 系统。

["了解如何删除Cloud Volumes ONTAP 工作环境"](#)。

卷和 LUN 管理

创建 FlexVol 卷

如果在启动初始Cloud Volumes ONTAP 系统后需要更多存储、则可以从BlueXP为NFS、CIFS或iSCSI创建新的FlexVol 卷。

BlueXP提供了多种创建新卷的方法：

- 指定新卷的详细信息、并让BlueXP为您处理底层数据聚合。 [了解更多信息。](#)
- 在您选择的数据聚合上创建卷。 [了解更多信息。](#)
- 使用模板创建卷，以根据特定应用程序（例如数据库或流式服务）的工作负载要求优化卷。 [了解更多信息。](#)

- 在 HA 配置中的第二个节点上创建卷。 [了解更多信息](#)。

开始之前

有关卷配置的一些注意事项：

- 创建iSCSI卷时、BlueXP会自动为您创建LUN。我们通过为每个卷仅创建一个 LUN 来简化此过程，因此无需进行管理。创建卷后， ["使用 IQN 从主机连接到 LUN"](#)。
- 您可以从 System Manager 或 CLI 创建其他 LUN 。
- 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"](#)。
- 如果您的Cloud Volumes ONTAP 配置支持Amazon EBS弹性卷功能、则可能需要 ["详细了解创建卷时会发生什么情况"](#)。

创建卷

创建卷的最常见方法是指定所需的卷类型、然后由BlueXP为您处理磁盘分配。但是，您也可以选择要在其中创建卷的特定聚合。

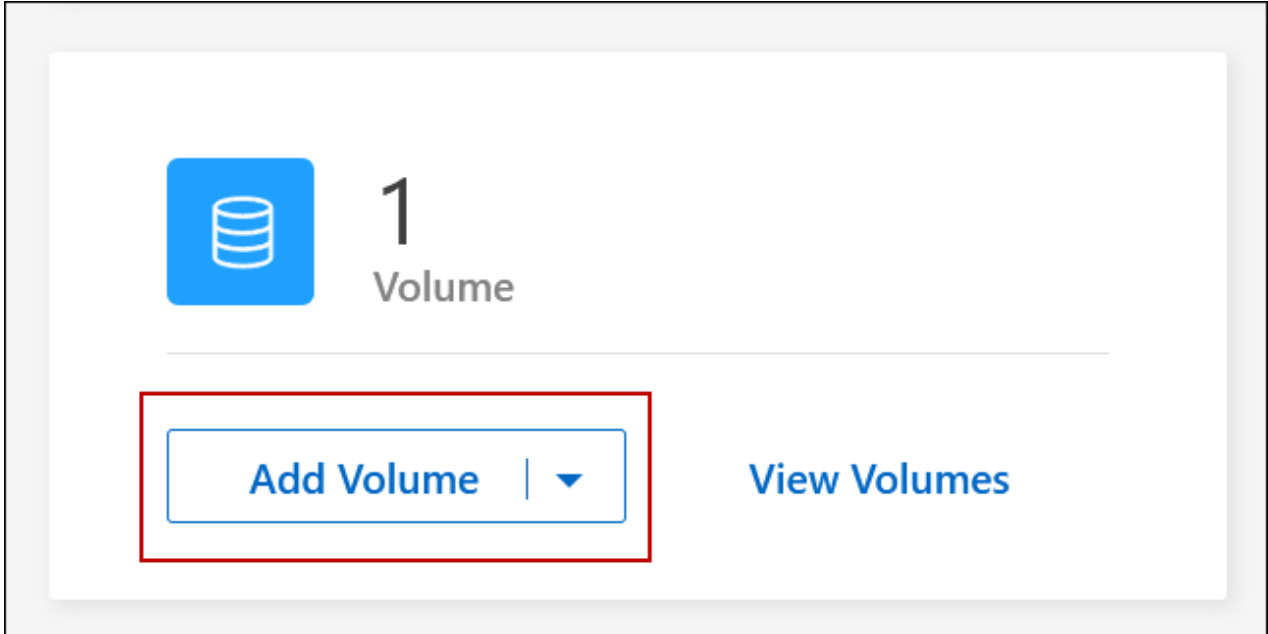
步骤

1. 从左侧导航菜单中、选择*存储>画布*。
2. 在 "画布 " 页面上，双击要配置 FlexVol 卷的 Cloud Volumes ONTAP 系统的名称。
3. 通过让BlueXP为您处理磁盘分配来创建新卷、或者为此卷选择特定聚合。

只有在您很好地了解 Cloud Volumes ONTAP 系统上的数据聚合时，才建议选择特定聚合。

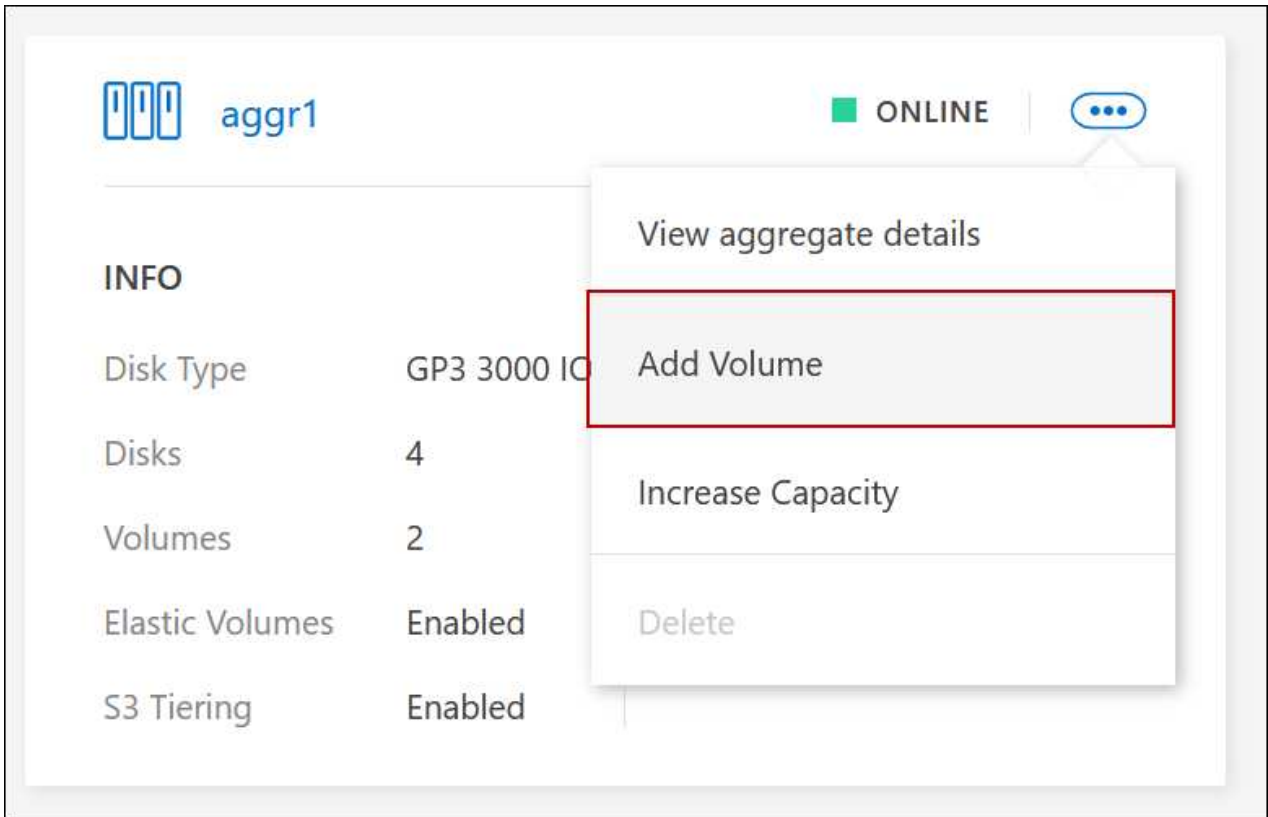
任何聚合

在概述选项卡上、导航到卷磁贴、然后单击*添加卷*。



特定聚合

在聚合选项卡上、导航到所需的聚合图块。单击菜单图标、然后单击*添加卷*。



4. 按照向导中的步骤创建卷。

a. 卷、详细信息、保护和标记：输入有关卷的基本详细信息并选择Snapshot策略。

此页面上的某些字段不言自明。以下列表介绍了可能需要指导的字段：

字段	Description
卷名称	可以为新卷输入的可标识名称。
卷大小	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。
Tags	添加到卷的标记将与关联 "应用程序模板服务" 可帮助您组织和简化资源管理。
Storage VM (SVM)	Storage VM 是在 ONTAP 中运行的虚拟机，可为客户端提供存储和数据服务。您可能会将其视为 SVM 或 SVM。默认情况下，Cloud Volumes ONTAP 配置有一个 Storage VM，但某些配置支持额外的 Storage VM。您可以为新卷指定 Storage VM。
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。

- b. * 协议 *：选择卷的协议（NFS，CIFS 或 iSCSI），然后提供所需信息。

如果您选择CIFS并且服务器未设置、则在单击*下一步*后、BlueXP将提示您设置CIFS连接。

["了解支持的客户端协议和版本"](#)。

以下各节介绍了可能需要指导的字段。这些说明按协议进行组织。

NFS

访问控制

选择一个自定义导出策略以使此卷可供客户端使用。

导出策略

定义子网中可访问卷的客户端。默认情况下、BlueXP输入一个值、用于访问子网中的所有实例。

CIFS

权限和用户 / 组

用于控制用户和组（也称为访问控制列表或 ACL）对 SMB 共享的访问级别。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、则必须使用域 \ 用户名格式包括用户的域。

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）。

如果要配置 Google Managed Active Directory，则默认情况下可以使用 169.254.169.254 IP 地址访问 AD。

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 AWS 托管 Microsoft AD 配置为 Cloud Volumes ONTAP 的 AD 服务器，请在此字段中输入 * OU=Computers，OU=corp*。
- 要将 Azure AD 域服务配置为 Cloud Volumes ONTAP 的 AD 服务器，请在此字段中输入 * OU=AADDC Computers * 或 * OU=AADDC Users*。
"[Azure 文档：在 Azure AD 域服务托管域中创建组织单位（OU）](#)"
- 要将 Google Managed Microsoft AD 配置为 Cloud Volumes ONTAP 的 AD 服务器，请在此字段中输入 * OU=Computers，OU=Cloud*。
"[Google Cloud 文档：Google Managed Microsoft AD 中的组织单位](#)"

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 ["BlueXP自动化文档"](#) 了解详细信息。

请注意，只有在创建 CIFS 服务器时才能配置 NTP 服务器。在创建 CIFS 服务器后，它不可配置。

iSCSI

LUN

iSCSI 存储目标称为 LUN（逻辑单元），并作为标准块设备提供给主机。创建 iSCSI 卷时，BlueXP 会自动为您创建 LUN。我们通过为每个卷仅创建一个 LUN 来简化此过程，因此无需进行管理。创建卷后，["使用 IQN 从主机连接到 LUN"](#)。

启动程序组

启动程序组（igroup）指定哪些主机可以访问存储系统上的指定 LUN

主机启动程序（IQN）

iSCSI 目标通过标准以太网网络适配器（NIC），带软件启动程序的 TCP 卸载引擎（TOE）卡，融合网络适配器（CNA）或专用主机总线适配器（HBA）连接到网络，并通过 iSCSI 限定名称（IQN）进行标识。

a. * 磁盘类型 *：根据性能需求和成本要求为卷选择底层磁盘类型。

- ["在 AWS 中估算系统规模"](#)
- ["在 Azure 中估算系统规模"](#)
- ["在 Google Cloud 中调整系统规模"](#)

5. * 使用情况配置文件和分层策略 *：选择是在卷上启用还是禁用存储效率功能，然后选择 ["卷分层策略"](#)。

ONTAP 包含多种存储效率功能、可以减少您所需的存储总量。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。

6. * 审阅 *：查看有关卷的详细信息，然后单击 * 添加 *。

结果

BlueXP 会在 Cloud Volumes ONTAP 系统上创建卷。

使用模板创建卷

如果您的组织已创建 Cloud Volumes ONTAP 卷模板，以便您可以部署针对特定应用程序的工作负载要求进行优

化的卷，请按照本节中的步骤进行操作。

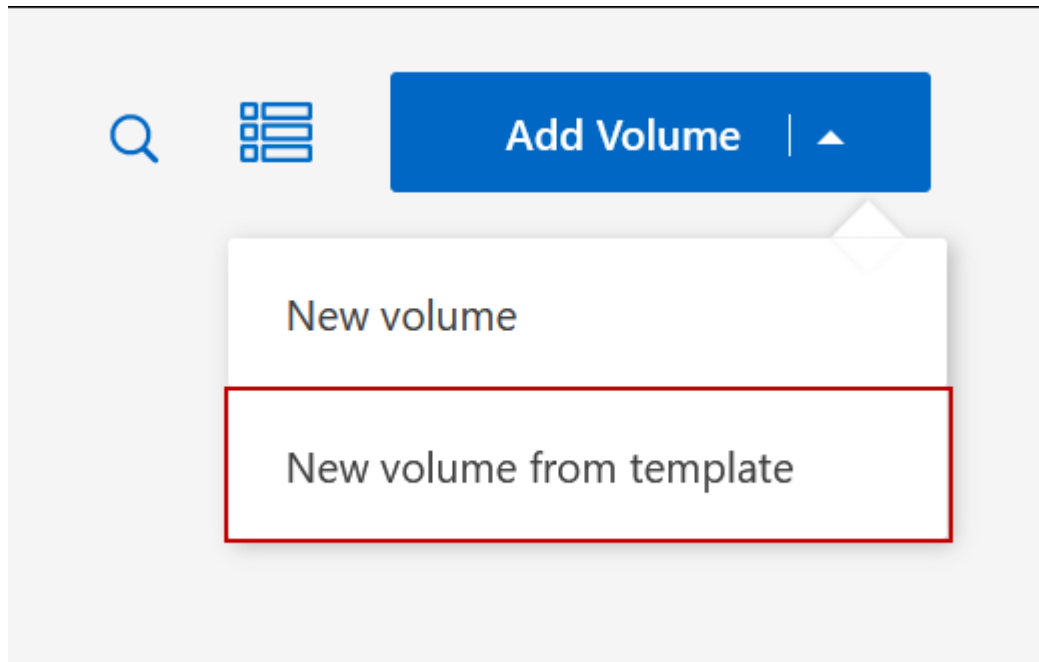
此模板应使您的工作更轻松，因为模板中已定义某些卷参数，例如磁盘类型，大小，协议，快照策略，云提供程序，等等。如果已预定义某个参数，则只需跳到下一个 volume 参数即可。



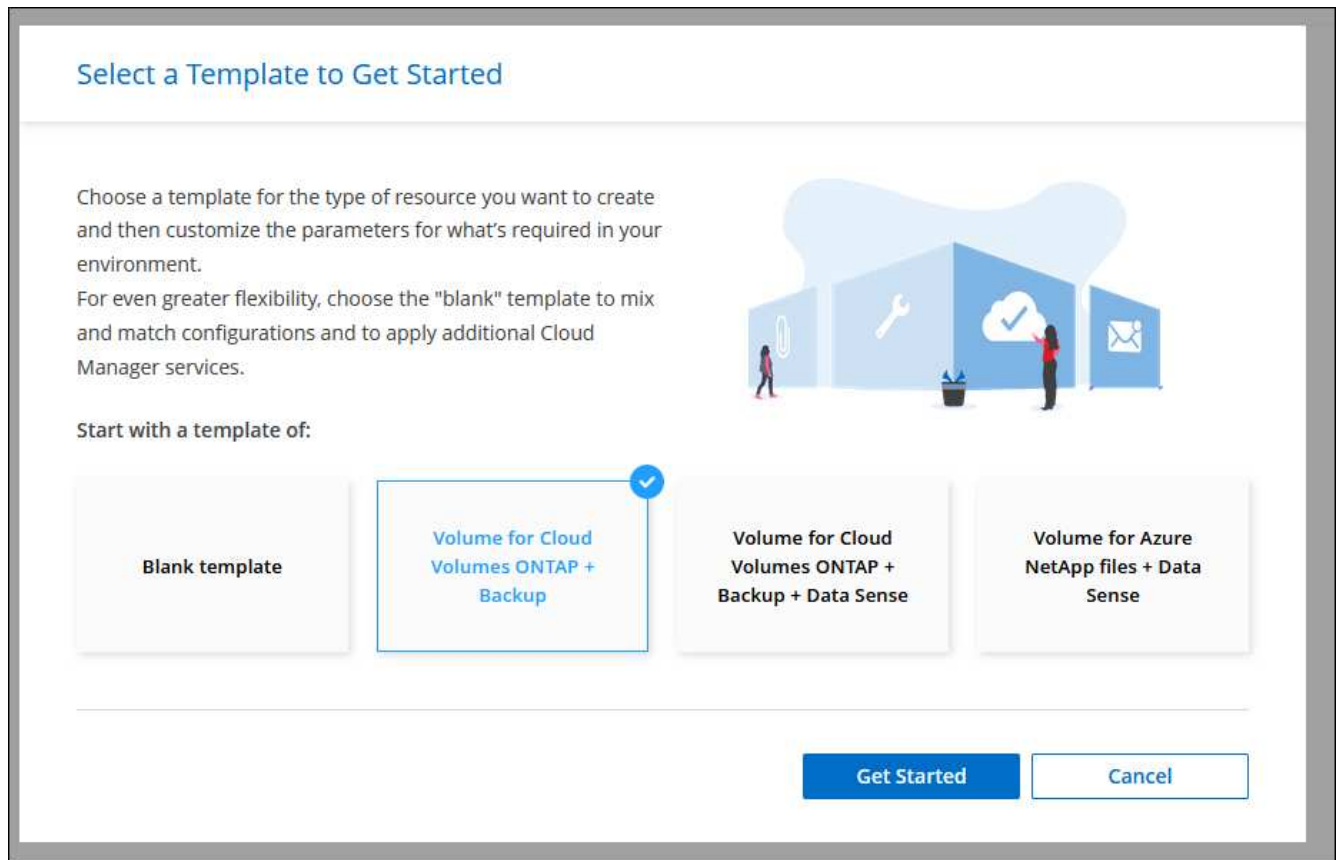
使用模板时，您只能创建 NFS 或 CIFS 卷。

步骤

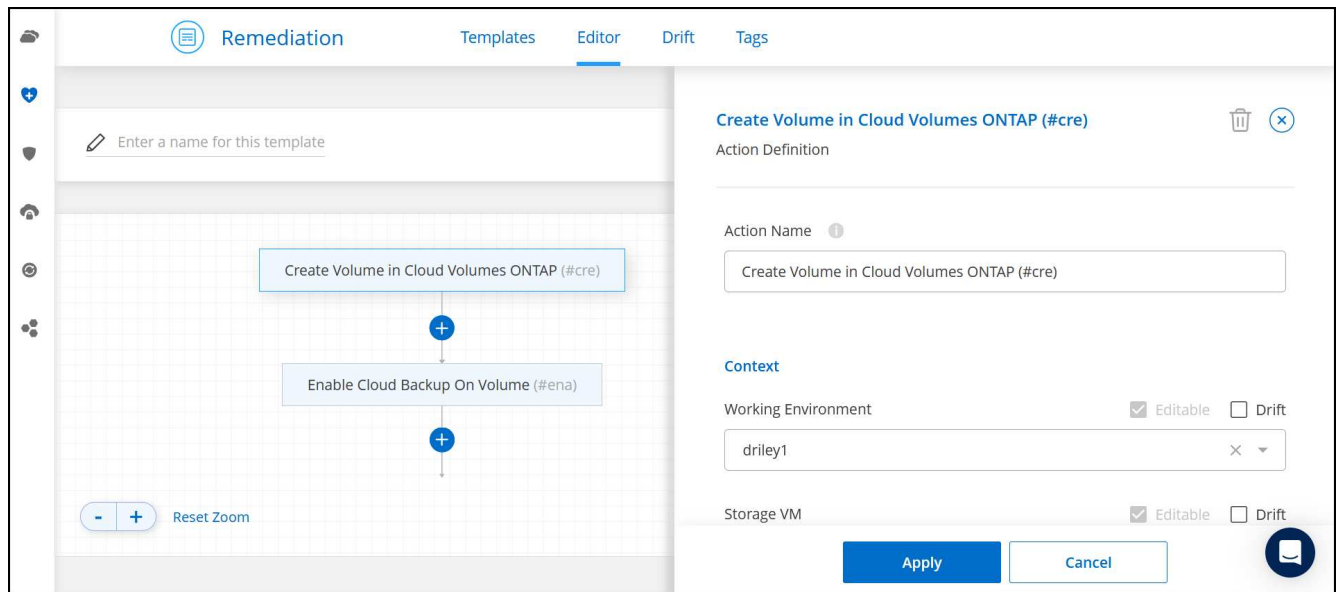
1. 从左侧导航菜单中、选择*存储>画布*。
2. 在 "画布 " 页面上，单击要配置卷的 Cloud Volumes ONTAP 系统的名称。
3. 导航到卷选项卡、然后单击*添加卷*>*从模板新建卷*。



4. 在 *Select Template* 页面中，选择要用于创建卷的模板，然后单击 * 下一步 * 。

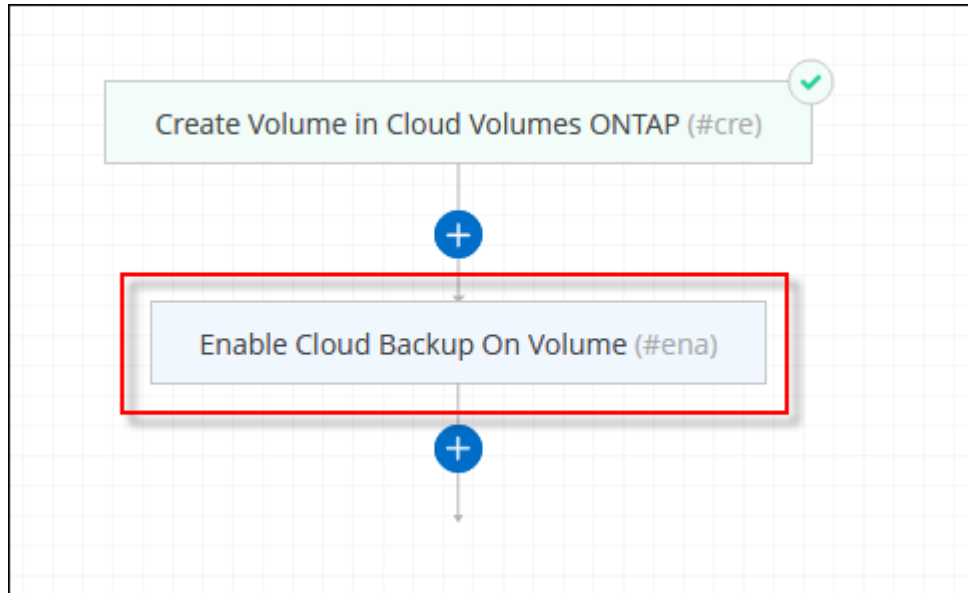


此时将显示 _Editor_ 页面。



5. 在 _Action_ 面板上方、输入模板的名称。
6. 在 _context_ 下、工作环境将填入您启动的工作环境的名称。选择要创建卷的* Storage VM*。
7. 为模板中未硬编码的所有参数添加值。请参见 [创建卷](#) 有关完成Cloud Volumes ONTAP 卷部署所需的所有参数的详细信息。
8. 单击*应用*将配置的参数保存到选定操作。
9. 如果没有需要定义的其他操作(例如，配置BlueXP备份和恢复)，请单击*保存模板*。

如果还有其他操作，请单击左窗格中的操作以显示需要完成的参数。



例如、如果"启用卷上的云备份"操作要求您选择备份策略、您现在可以执行此操作。

10. 完成模板操作的配置后、单击*保存模板*。

结果

Cloud Volumes ONTAP 会配置卷并显示一个页面，以便您可以查看进度。

Actions status	
Create Volume in Cloud Volumes ONTAP	Success
Enable Cloud Backup	Pending

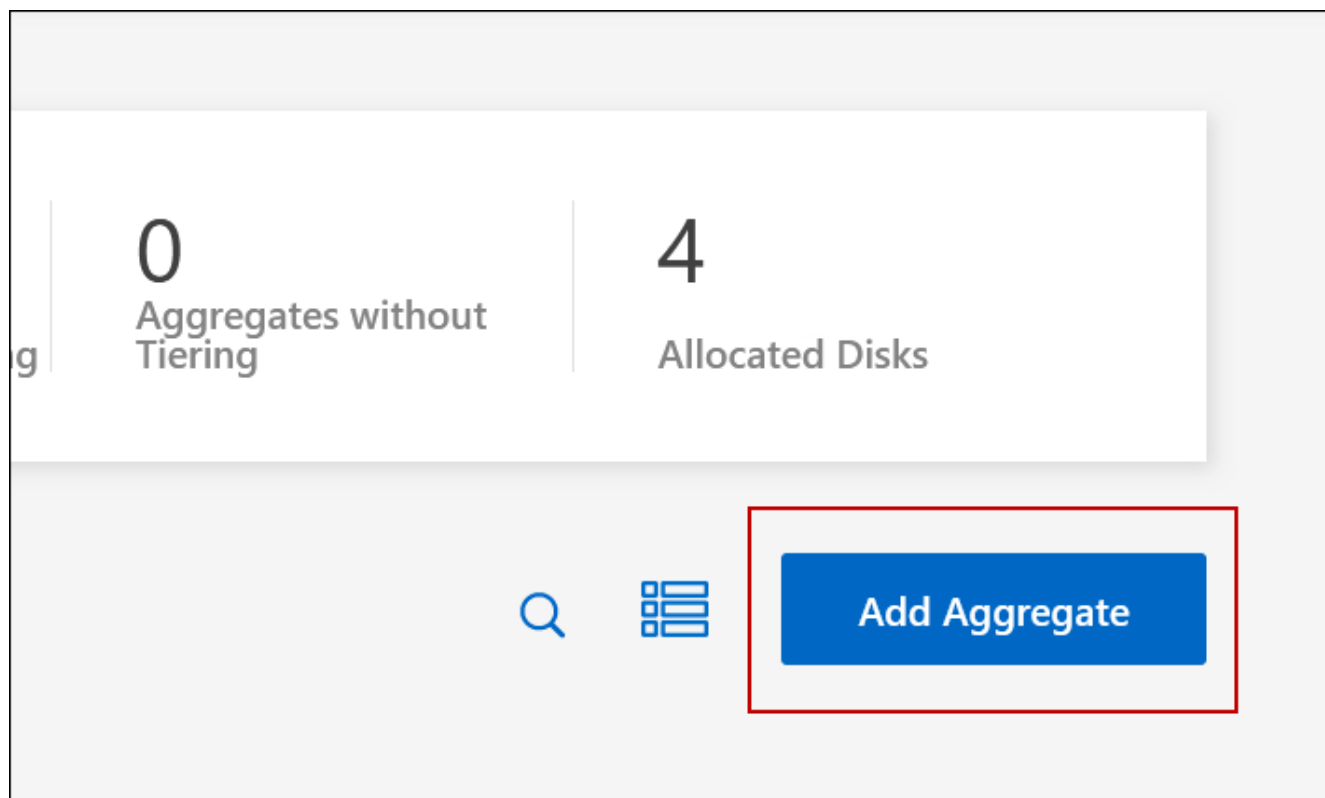
此外、如果在模板中实施了任何二级操作、例如在卷上启用BlueXP备份和恢复、则也会执行该操作。

在 **HA** 配置中的第二个节点上创建卷

默认情况下、BlueXP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. 从左侧导航菜单中、选择*存储>画布*。
2. 在 "画布" 页面上，双击要管理聚合的 Cloud Volumes ONTAP 工作环境的名称。
3. 在聚合选项卡上、单击*添加聚合*。
4. 在_Add aggregate_屏幕中、创建聚合。



5. 对于主节点，请在 HA 对中选择第二个节点。
6. 在BlueXP创建聚合后、选择该聚合、然后单击*创建卷*。
7. 输入新卷的详细信息，然后单击 * 创建 *。

结果

BlueXP会在HA对中的第二个节点上创建卷。



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。

创建卷后

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。

管理现有卷

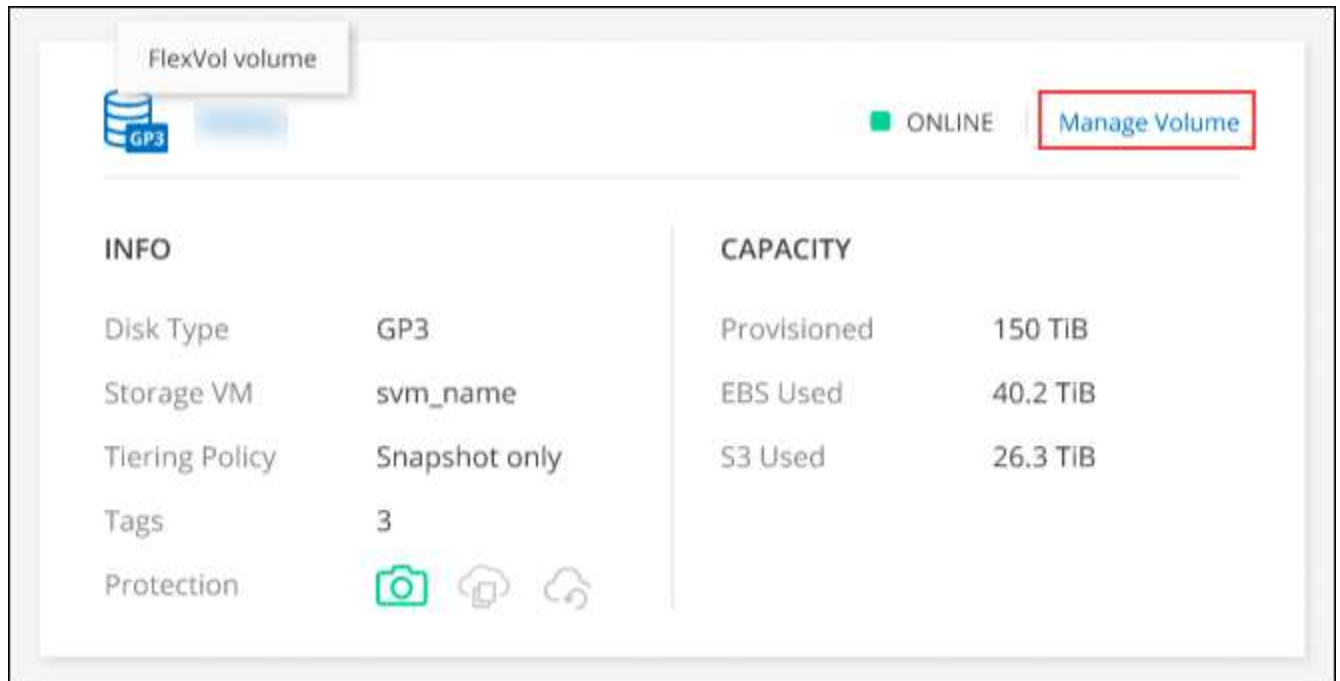
通过BlueXP、您可以管理卷和CIFS服务器。它还会提示您移动卷以避免容量问题。

管理卷

您可以在存储需求发生变化时管理卷。您可以查看、编辑、克隆、恢复和删除卷。

步骤


1. 从左侧导航菜单中、选择*存储>画布*。
2. 在 "画布" 页面上，双击要管理卷的 Cloud Volumes ONTAP 工作环境。
3. 在工作环境中、单击*卷*选项卡。



4. 在卷选项卡上、导航到所需的卷标题、然后单击*管理卷*以访问管理卷右侧面板。

任务	Action
查看有关卷的信息	在管理卷面板的卷操作下、单击*查看卷详细信息*。
获取 NFS 挂载命令	a. 在管理卷面板的卷操作下、单击*挂载命令*。 b. 单击 * 复制 *。

任务	Action
克隆卷	<p>a. 在管理卷面板的卷操作下、单击*克隆卷*。</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 "《ONTAP 9 逻辑存储管理指南》"。</p>
编辑卷标记(仅限读写卷)	<p>a. 在管理卷面板的卷操作下、单击*编辑卷标记*以修改分配给选定卷的卷标记。</p> <p>b. 在提供的字段下输入卷标记密钥和值。</p> <p>c. 要包括其他标记、请单击*添加新标记*。</p> <p>d. 单击 * 保存 *。</p>
编辑卷 (仅限读写卷)	<p>a. 在管理卷面板的卷操作下、单击*编辑卷设置*</p> <p>b. 修改卷的Snapshot策略、NFS协议版本、NFS访问控制列表(导出策略)或共享权限、然后单击*应用*。</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p> 如果需要自定义 Snapshot 策略，可以使用 System Manager 创建这些策略。</p> </div>
删除卷	<p>a. 在管理卷面板的卷操作下、单击*删除卷*。</p> <p>b. 在删除卷窗口下、输入要删除的卷的名称。</p> <p>c. 再次单击 * 删除 * 进行确认。</p>
按需创建 Snapshot 副本	<p>a. 在管理卷面板的保护操作下、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>
将数据从 Snapshot 副本恢复到新卷	<p>a. 在管理卷面板的保护操作下、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>
更改底层磁盘类型	<p>a. 在管理卷面板的高级操作下、单击*更改磁盘类型*。</p> <p>b. 选择磁盘类型，然后单击 * 更改 *。</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p> BlueXP会将卷移动到使用选定磁盘类型的现有聚合、或者为卷创建新聚合。</p> </div>

任务	Action
更改分层策略	<p>a. 在管理卷面板的高级操作下、单击*更改分层策略*。</p> <p>b. 选择其他策略，然后单击 * 更改 * 。</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  BlueXP会将卷移动到使用选定磁盘类型进行分层的现有聚合、或者为卷创建新聚合。 </div>
删除卷	<p>a. 选择一个卷，然后单击 * 删除 * 。</p> <p>b. 在对话框中键入卷的名称。</p> <p>c. 再次单击 * 删除 * 进行确认。</p>

调整卷大小

默认情况下，卷在空间不足时会自动增长到最大大小。默认值为 1,000，这意味着卷可以增长到其大小的 11 倍。此值可在 Connector 的设置中进行配置。

如果需要调整卷大小，可以通过执行此操作 "[ONTAP 系统管理器](#)"。调整卷大小时，请务必考虑系统的容量限制。转至 "[《 Cloud Volumes ONTAP 发行说明》](#)" 有关详细信息：

修改 CIFS 服务器

如果您更改了 DNS 服务器或 Active Directory 域、则需要在 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. 从工作环境的概述选项卡中、单击右侧面板下的功能选项卡。
2. 在CIFS设置字段下、单击*铅笔图标*以显示CIFS设置窗口。
3. 指定 CIFS 服务器的设置：

任务	Action
选择Storage VM (SVM)	选择Cloud Volume ONTAP Storage Virtual Machine (SVM)可显示其已配置的CIFS信息。
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。

任务	Action
DNS 主 IP 地址和次 IP 地址	<p>为 CIFS 服务器提供名称解析的 DNS 服务器的 IP 地址。</p> <p>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）。</p> <p>ifdef: : gcp[]</p> <p>如果要配置 Google Managed Active Directory，则默认情况下可以使用 169.254.169.254 IP 地址访问 AD。</p> <p>字节名称: : : gcp[]</p>
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。
CIFS server NetBIOS name	在 AD 域中唯一的 CIFS 服务器名称。
组织单位	<p>AD 域中要与 CIFS 服务器关联的组织单元。默认值为 cn = computers。</p> <ul style="list-style-type: none"> • 要将 AWS 托管 Microsoft AD 配置为 Cloud Volumes ONTAP 的 AD 服务器，请在此字段中输入 * OU=Computers，OU=corp*。 • 要将 Azure AD 域服务配置为 Cloud Volumes ONTAP 的 AD 服务器，请在此字段中输入 * OU=AADDC Computers * 或 * OU=AADDC Users*。 "Azure 文档：在 Azure AD 域服务托管域中创建组织单位（OU）" • 要将 Google Managed Microsoft AD 配置为 Cloud Volumes ONTAP 的 AD 服务器，请在此字段中输入 * OU=Computers，OU=Cloud*。 "Google Cloud 文档：Google Managed Microsoft AD 中的组织单位"

4. 单击*设置*。

结果

Cloud Volumes ONTAP 会根据更改更新 CIFS 服务器。

移动卷

移动卷以提高容量利用率，提高性能并满足服务级别协议的要求。

您可以在 System Manager 中移动卷，方法是选择卷和目标聚合，启动卷移动操作，并可选择监控卷移动作业。使用 System Manager 时，卷移动操作会自动完成。

步骤

1. 使用 System Manager 或 CLI 将卷移动到聚合。

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》"。

当BlueXP显示Action Required消息时移动卷

BlueXP可能会显示一条"需要操作"消息、指出移动卷对于避免容量问题是必要的、但您需要自行更正问题描述。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。



当聚合已达到90%的已用容量时、BlueXP会显示这些"需要执行操作"消息。如果启用了数据分层，则在聚合已达到 80% 已用容量时会显示消息。默认情况下，为数据分层预留 10% 的可用空间。"详细了解数据分层的可用空间比率"。

步骤

1. [\[确定如何更正容量问题\]](#)。
2. 根据您的分析、移动卷以避免容量问题：
 - [\[将卷移动到另一个系统以避免容量问题\]](#)。
 - [\[将卷移动到另一个聚合以避免容量问题\]](#)。

确定如何更正容量问题

如果BlueXP无法提供移动卷以避免容量问题的建议、您必须确定需要移动的卷、以及是否应将其移动到同一系统上的另一个聚合或另一个系统。

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信息：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*聚合选项卡*。
 - b. 导航到所需的聚合图块、然后单击*。(椭圆图标)>查看聚合详细信息*。
 - c. 在聚合详细信息屏幕的概述选项卡下、查看每个卷的大小、然后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。

Aggregate Details	
aggr1	
Overview	Capacity Allocation
State	online
Home Node	shiloh01
Encryption Type	cloudEncrypted
Volumes	2 ^
	www_shiloh01_vvol1 (1 GiB)
	DATA01 (500 GiB)

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 [将卷移动到另一个聚合以避免容量问题](#)。

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：

要避免容量问题、必须移动卷；但是、BlueXP无法为您执行此操作、因为系统已达到磁盘限制。

步骤

1. 确定具有可用容量的 Cloud Volumes ONTAP 系统或部署新系统。

2. 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"](#)。

3. 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"](#)。

4. 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》"](#)。

5. 删除原始卷。

有关详细信息，请参见 ["管理卷"](#)。

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

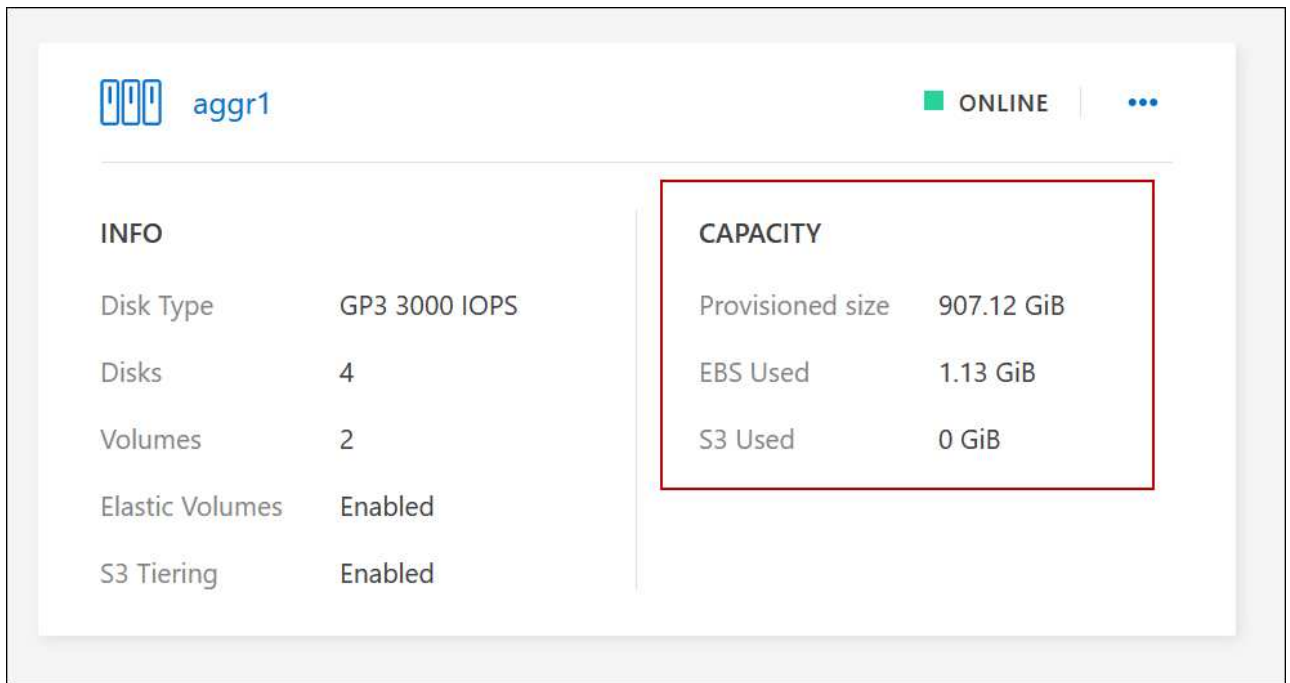
您可以按照此任务中的步骤更正以下需要执行的操作消息：

要避免容量问题、必须移动两个或更多卷；但是、BlueXP无法为您执行此操作。

步骤

1. 验证现有聚合是否具有需要移动的卷的可用容量：

- a. 在工作环境中、单击*聚合选项卡*。
- b. 导航到所需的聚合图块、然后单击*。(椭圆图标)>查看聚合详细信息*。
- c. 在聚合区块下、查看可用容量(已配置大小减去已用聚合容量)。



2. 如果需要，请将磁盘添加到现有聚合：
 - a. 选择聚合、然后单击*。(椭圆图标)>添加磁盘*。
 - b. 选择要添加的磁盘数，然后单击 * 添加 *。
3. 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"](#)。
4. 使用 System Manager 或 CLI 将卷移动到聚合。
5. 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](#)》"。

卷移动速度可能较慢的原因

如果 Cloud Volumes ONTAP 满足以下任一条件，则移动卷所需时间可能会比预期长：

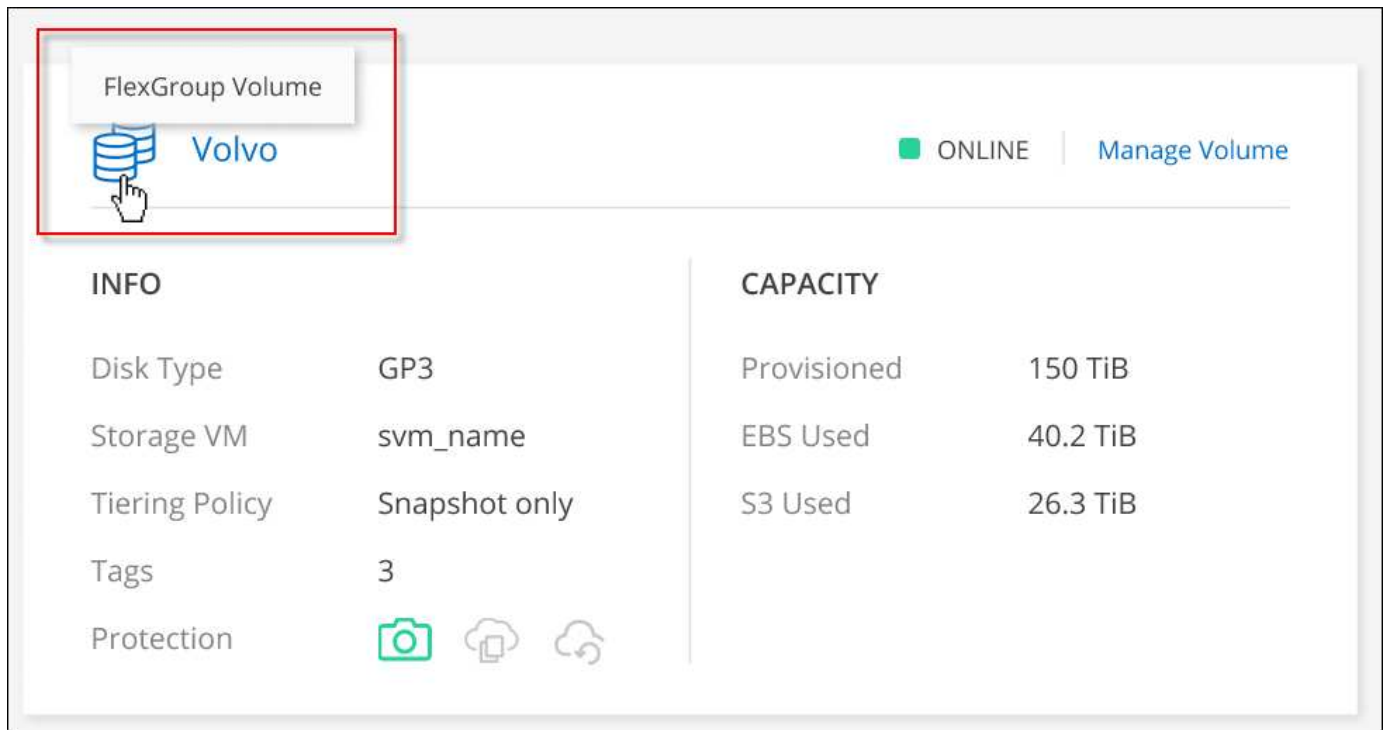
- 此卷为克隆卷。
- 卷是克隆的父卷。
- 源聚合或目标聚合具有一个吞吐量优化型 HDD（st1）磁盘。
- 其中一个聚合对对象使用的命名方案较旧。两个聚合必须使用相同的名称格式。

如果在 9.4 版或更早版本中的聚合上启用了数据分层，则会使用较早的命名方案。

- 源聚合和目标聚合上的加密设置不匹配，或者正在重新设置密钥。
- 在卷移动时指定了 `-tiering-policy` 选项以更改分层策略。
- 在卷移动时指定了 `-generate-destination-key` 选项。

查看FlexGroup 卷

您可以直接通过BlueXP中的卷选项卡查看通过命令行界面或System Manager创建的FlexGroup 卷。与为FlexVol 卷提供的信息相同、BlueXP通过专用的卷图块提供有关已创建的跳蚤组卷的详细信息。在卷磁贴下、您可以通过图标的悬停文本来标识每个FlexGroup 卷组。此外、您还可以通过卷模式列在卷列表视图下标识FlexGroup 卷并对其进行排序。



目前、您只能在BlueXP下查看现有FlexGroup 卷。在BlueXP中创建FlexGroup 卷的功能不可用、但计划在未来版本中使用。

将非活动数据分层到低成本对象存储

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，您可以降低 Cloud Volumes ONTAP 的存储成本。数据分层由 FabricPool 技术提供支持。有关简要概述，请参见 ["数据分层概述"](#)。

要设置数据分层，您需要执行以下操作：

1

选择支持的配置

支持大多数配置。如果您的 Cloud Volumes ONTAP 系统运行的是最新版本，则最好继续操作。 ["了解更多信息"](#)。

2

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BlueXP具有所需权限、您就无需执行任何操作。 [了解更多信息](#)。。

- 对于Google Cloud、您需要为专用Google Access配置子网并设置服务帐户。 [了解更多信息。](#)

3

确保已启用分层的聚合

必须在聚合上启用数据分层，才能在卷上启用数据分层。您应了解新卷和现有卷的要求。 [了解更多信息。](#)

4

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、BlueXP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。
- 您无需为容量层创建对象存储。BlueXP可以为您提供这种服务。
- 您无需在系统级别启用数据分层。



在创建系统时、BlueXP会为冷数据创建一个对象存储、[只要没有连接或权限问题](#)。之后，您只需在卷上启用数据分层（在某些情况下，[在聚合上](#)）。

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。

AWS支持

- 从Cloud Volumes ONTAP 9.2开始、AWS支持数据分层。
- 性能层可以是通用 SSD（GP3 或 GP2）或配置的 IOPS SSD（IO1）。



使用吞吐量优化型 HDD（st1）时，不建议将数据分层到对象存储。

支持 Azure

- Azure支持数据分层、如下所示：
 - 使用单节点系统时为9.4版
 - 使用HA对的9.6版
- 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。

支持Google Cloud

- 从Cloud Volumes ONTAP 9.6开始、Google Cloud支持数据分层。
- 性能层可以是 SSD 永久性磁盘，平衡永久性磁盘或标准永久性磁盘。

功能互操作性

- 加密技术支持数据分层。
- 必须在卷上启用精简配置。

要求

根据您的云提供商，必须设置某些连接和权限，以便 Cloud Volumes ONTAP 可以将冷数据分层到对象存储。

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BlueXP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Connector的自定义角色具有以下权限、则BlueXP将为您启用vNet服务端点：

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

默认情况下、权限包括在自定义角色中。 ["查看Connector的Azure权限"](#)

将冷数据分层到 **Google Cloud** 存储分段的要求

- 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"](#)。
- 服务帐户必须附加到Cloud Volumes ONTAP。

["了解如何设置此服务帐户"](#)。

创建Cloud Volumes ONTAP 工作环境时、系统会提示您选择此服务帐户。

如果您在部署期间未选择服务帐户、则需要关闭Cloud Volumes ONTAP、转到Google云控制台、然后将服务帐户附加到Cloud Volumes ONTAP 实例。然后、您可以按照下一节所述启用数据分层。

- 要使用客户管理的加密密钥对存储分段进行加密，请启用 Google Cloud 存储分段以使用此密钥。

["了解如何在 Cloud Volumes ONTAP 中使用客户管理的加密密钥"](#)。

在实施要求后启用数据分层

只要不存在连接或权限问题、BlueXP就会在创建系统时为冷数据创建一个对象存储。如果在创建系统之前未实施上述要求、则需要通过API或System Manager手动启用分层、从而创建对象存储。



未来的Cloud Volumes ONTAP版本将提供通过BlueXP用户界面启用层的功能。

确保在聚合上启用分层

必须在聚合上启用数据分层，才能在卷上启用数据分层。您应了解新卷和现有卷的要求。

• * 新卷 *

如果要在新卷上启用数据分层，则无需担心在聚合上启用数据分层。BlueXP会在已启用分层的现有聚合上创建卷、或者如果尚未存在已启用数据分层的聚合、则它会为卷创建一个新聚合。

• * 现有卷 *

如果要在现有卷上启用数据分层，则需要确保在底层聚合上启用数据分层。如果现有聚合未启用数据分层，则需要使用 System Manager 将现有聚合附加到对象存储。

确认是否已在聚合上启用分层的步骤

1. 在BlueXP中打开工作环境。
2. 单击聚合选项卡。
3. 导航到所需的区块、并验证是否已在聚合上启用或禁用分层。

The screenshot shows the configuration for an aggregation named 'aggr1'. The status is 'ONLINE'. The configuration is divided into two columns: 'INFO' and 'CAPACITY'.

INFO		CAPACITY	
Disk Type	GP3 3000 IOPS	Provisioned size	907.12 GiB
Disks	4	EBS Used	1.13 GiB
Volumes	2	S3 Used	0 GiB
Elastic Volumes	Enabled		
S3 Tiering	Enabled		

在聚合上启用分层的步骤

1. 在 System Manager 中，单击 * 存储 > 层 *。

2. 单击聚合的操作菜单并选择 * 附加云层 *。
3. 选择要附加的云层，然后单击 * 保存 *。

下一步是什么？

现在，您可以在新卷和现有卷上启用数据分层，如下一节所述。

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

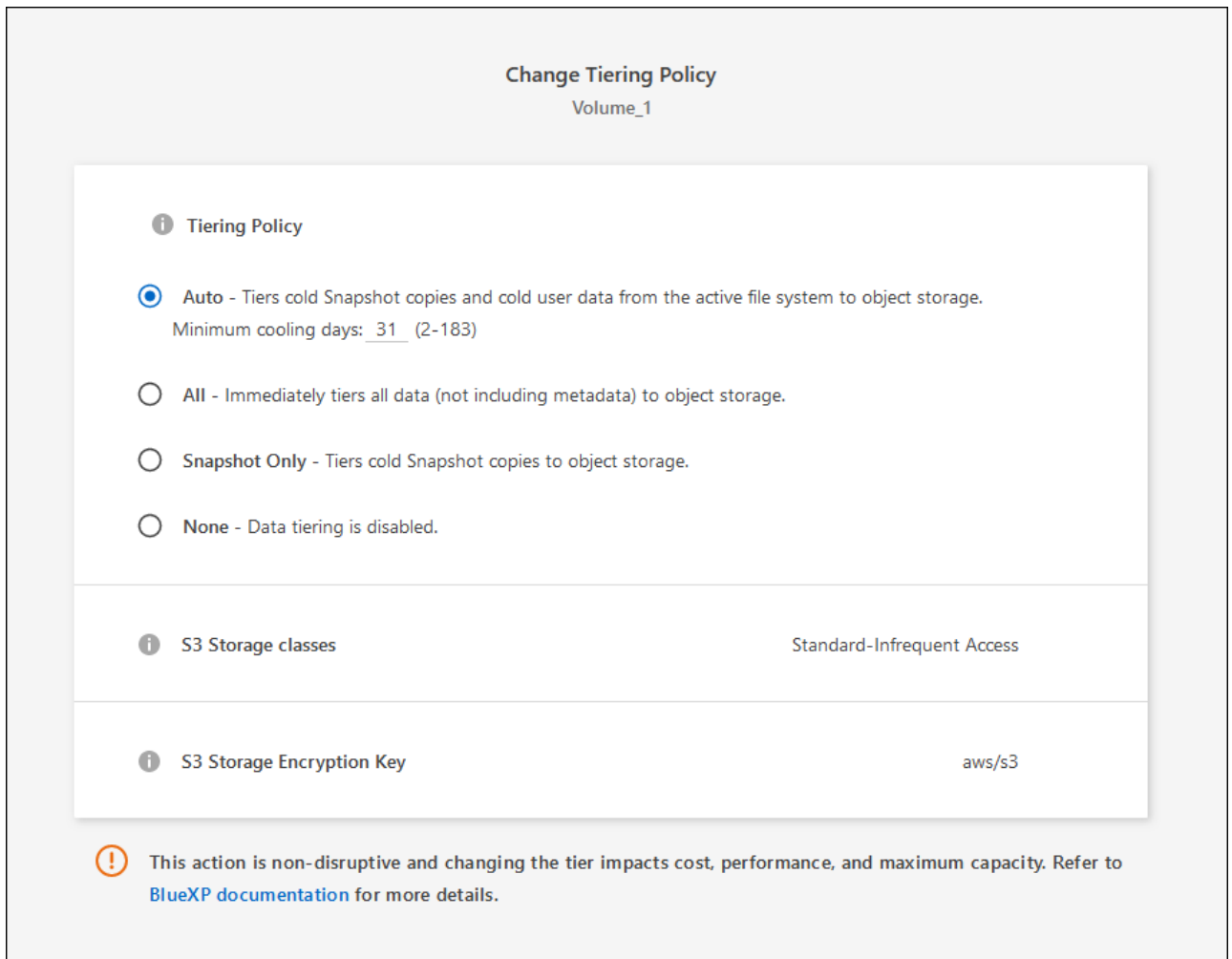
1. 在工作环境下的卷选项卡中、创建新卷或更改现有卷的层：

任务	Action
创建新卷	单击 * 添加新卷 *。
修改现有卷	选择所需的卷磁贴、单击*管理卷*以访问管理卷右侧面板、然后单击右侧面板下的*高级操作*和*更改分层策略*。

2. 选择分层策略。

有关这些策略的问题描述，请参见 ["数据分层概述"](#)。

- 示例 *



如果启用了数据分层的聚合尚不存在、则BlueXP将为卷创建一个新聚合。

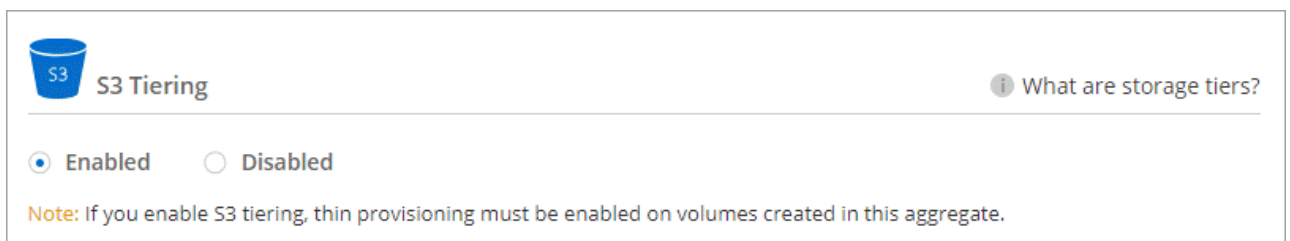
对数据保护卷中的数据进行分层

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. 从左侧导航菜单中、选择*存储>画布*。
2. 在 "画布" 页面上，选择包含源卷的工作环境，然后将其拖动到要将该卷复制到的工作环境。
3. 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 *



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"](#)。

更改分层数据的存储类

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存储类来降低存储成本。如果您确实访问数据，访问成本会更高，因此在更改存储类之前，必须考虑到这一点。

分层数据的存储类在系统范围内—不是每个卷的 it。

有关支持的存储类的信息，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 * 存储类 * 或 * Blob 存储分层 *。
2. 选择一个存储类，然后单击 * 保存 *。

更改数据分层的可用空间比率

数据分层的可用空间比率用于定义将数据分层到对象存储时，Cloud Volumes ONTAP SSD/HDD 上需要多少可用空间。默认设置为 10% 的可用空间，但您可以根据需要调整此设置。

例如，您可以选择小于 10% 的可用空间，以确保您正在利用所购买的容量。然后、当需要额外容量时、BlueXP 可以为您购买额外的磁盘(直到达到聚合的磁盘限制为止)。

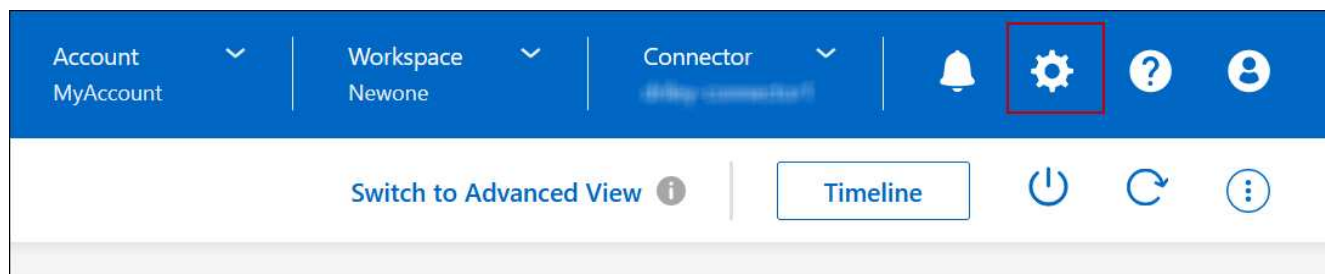


如果空间不足，则 Cloud Volumes ONTAP 无法移动数据，并且可能会出现性能下降。任何更改都应谨慎进行。如果您不确定，请联系 NetApp 支持部门以获得指导。

此比率对于灾难恢复场景非常重要，因为从对象存储读取数据时，Cloud Volumes ONTAP 会将数据移至 SSD/HDD 以提高性能。如果空间不足，则 Cloud Volumes ONTAP 无法移动数据。在更改比率时，请考虑这一点，以便满足您的业务需求。

步骤

1. 在 BlueXP 控制台的右上角、单击 * 设置 * 图标、然后选择 * 连接器设置 *。



2. 在 * 容量 * 下，单击 * 聚合容量阈值 - 数据分层的可用空间比率 *。
3. 根据需要更改可用空间比率，然后单击 * 保存 *。

更改自动分层策略的冷却期

如果您使用 `_auto_tiering` 策略在 Cloud Volumes ONTAP 卷上启用了数据分层，则可以根据业务需求调整默认冷却期。仅使用 API 和 CLI 支持此操作。

冷却期是指卷中的用户数据在被视为 " 冷 " 并移至对象存储之前必须保持非活动状态的天数。

自动分层策略的默认冷却期为 31 天。您可以按如下所示更改冷却期：

- 9.8 或更高版本：2 天到 183 天
- 9.7 或更早版本：2 天到 63 天

步骤

1. 创建卷或修改现有卷时，请在 API 请求中使用 *minimumCoolingDays* 参数。

将 LUN 连接到主机

创建 iSCSI 卷时、BlueXP 会自动为您创建 LUN。我们通过为每个卷仅创建一个 LUN 来简化此过程，因此无需进行管理。创建卷后，请使用 IQN 从主机连接到 LUN。

请注意以下事项：

- BlueXP 的自动容量管理不适用于 LUN。当 BlueXP 创建 LUN 时、它会禁用自动增长功能。
- 您可以从 System Manager 或 CLI 创建其他 LUN。

步骤

1. 从左侧导航菜单中、选择*存储>画布*。
2. 在 " 画布 " 页面上，双击要管理卷的 Cloud Volumes ONTAP 工作环境。
3. 在工作环境中、单击*卷*选项卡。
4. 在卷选项卡上、导航到所需的卷标题、然后单击*管理卷*以访问管理卷右侧面板。
5. 单击*目标IQN*。
6. 单击 * 复制 * 以复制 IQN 名称。
7. 设置从主机到 LUN 的 iSCSI 连接。
 - ["适用于 Red Hat Enterprise Linux 的 ONTAP 9 iSCSI 快速配置：启动与目标的 iSCSI 会话"](#)
 - ["适用于 Windows 的 ONTAP 9 iSCSI 快速配置：启动与目标的 iSCSI 会话"](#)
 - ["ONTAP SAN 主机配置"](#)

利用 FlexCache 卷加快数据访问速度

FlexCache 卷是一种存储卷、用于缓存来自初始(或源)卷的 SMB 和 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。

BlueXP 可通过管理 FlexCache 卷 ["BlueXP 卷缓存"](#) 服务

您还可以使用 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"

BlueXP为所有新的Cloud Volumes ONTAP系统生成FlexCache许可证。此许可证包含 500 GiB 的使用量限制。



聚合管理

创建聚合

您可以自行创建聚合、也可以让BlueXP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。



必须直接从BlueXP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。

步骤

1. 从左侧导航菜单中、选择*存储>画布*。
2. 在 "画布" 页面上，双击要管理聚合的 Cloud Volumes ONTAP 实例的名称。
3. 在聚合选项卡上、单击*添加聚合*、然后指定聚合的详细信息。

AWS

- 如果系统提示您选择磁盘类型和磁盘大小、请参见 ["在AWS中规划Cloud Volumes ONTAP 配置"](#)。
- 如果系统提示您输入聚合的容量大小、则您要在支持Amazon EBS弹性卷功能的配置上创建聚合。以下屏幕截图显示了一个由GP3磁盘组成的新聚合示例。

1 Disk Type 2 Aggregate details 3 Tiering Data 4 Review

Select Disk Type

Disk Type

GP3 - General Purpose SSD Dynamic Performance

General Purpose SSD (gp3) Disk Properties

Description: General purpose SSD volume that balances price and performance (performance level is independent of storage capacity)

IOPS Value Throughput MB/s

12000 250

["了解有关支持弹性卷的更多信息"](#)。

Azure 酒店

有关磁盘类型和磁盘大小的帮助、请参见 ["在Azure中规划Cloud Volumes ONTAP 配置"](#)。

Google Cloud

有关磁盘类型和磁盘大小的帮助、请参见 ["在Google Cloud中规划Cloud Volumes ONTAP 配置"](#)。

4. 单击 * 执行 * ，然后单击 * 批准和购买 * 。

管理聚合

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。



必须直接从BlueXP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。

开始之前

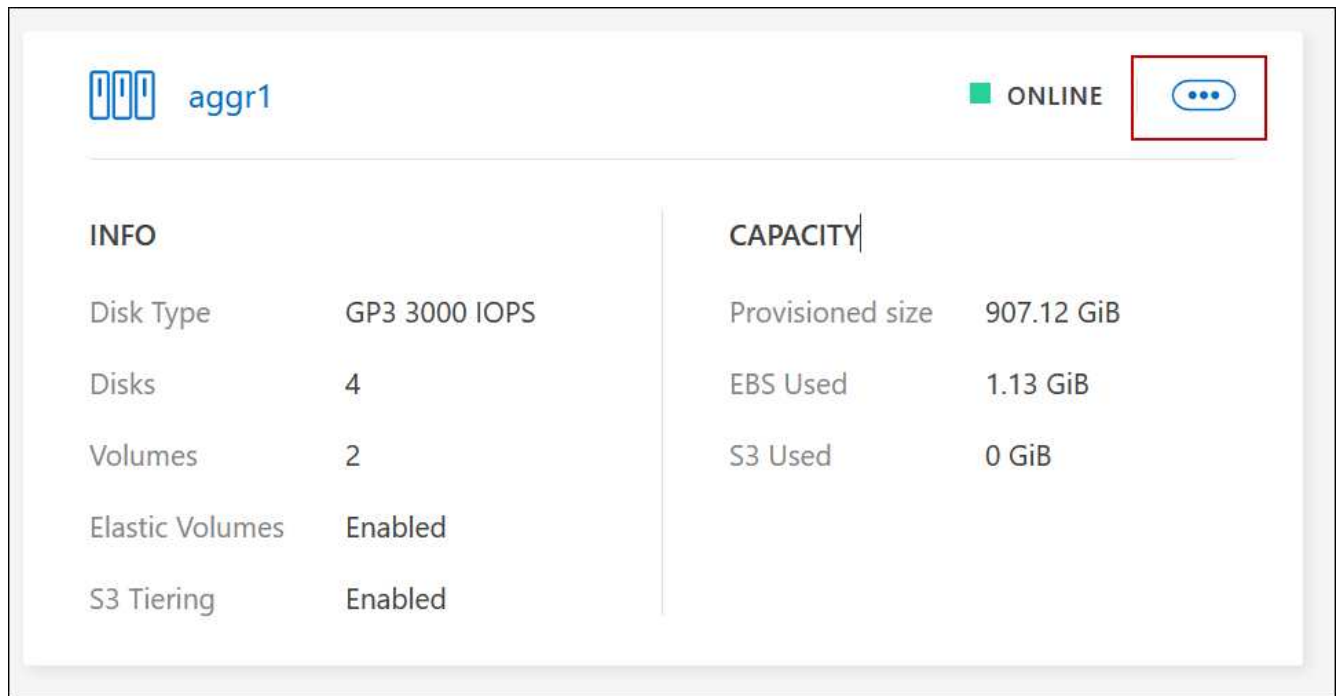
如果要删除聚合、必须先删除聚合中的卷。

关于此任务

如果某个聚合空间即将用尽，您可以使用 System Manager 将卷移动到另一个聚合。

步骤

1. 从左侧导航菜单中、选择*存储>画布*。
2. 在 "画布" 页面上，双击要管理聚合的 Cloud Volumes ONTAP 工作环境。
3. 在工作环境中、单击*聚合*选项卡。
4. 在聚合选项卡上、导航到所需标题、然后单击*。(椭圆图标)*。



5. 管理聚合：

任务	Action
查看有关聚合的信息	在...下 (椭圆图标)菜单中、单击*查看聚合详细信息*。
在特定聚合上创建卷	在...下 (椭圆图标)菜单中、单击*添加卷*。

任务	Action
将磁盘添加到聚合	<p>a. 在...下 (椭圆图标)菜单中、单击*添加磁盘*。</p> <p>b. 选择要添加的磁盘数，然后单击 * 添加 * 。</p> <p> 聚合中的所有磁盘大小必须相同。</p>
增加支持Amazon EBS弹性卷的聚合的容量	<p>a. 在...下 (椭圆图标)菜单中、单击*增加容量*。</p> <p>b. 输入要添加的额外容量、然后单击*增加*。</p> <p>请注意、您必须将聚合的容量至少增加256 GiB或聚合大小的10%。</p> <p>例如、如果您使用的是1.77 TiB聚合、则10%为181 GiB。该值低于256 GiB、因此聚合的大小必须增加到最小256 GiB。</p>
删除聚合	<p>a. 选择不包含任何卷的聚合图块单击*。(椭圆图标)>删除*。</p> <p>b. 再次单击 * 删除 * 进行确认。</p>

管理Connector上的容量设置

每个连接器都有设置、用于确定其如何管理Cloud Volumes ONTAP 的聚合容量。

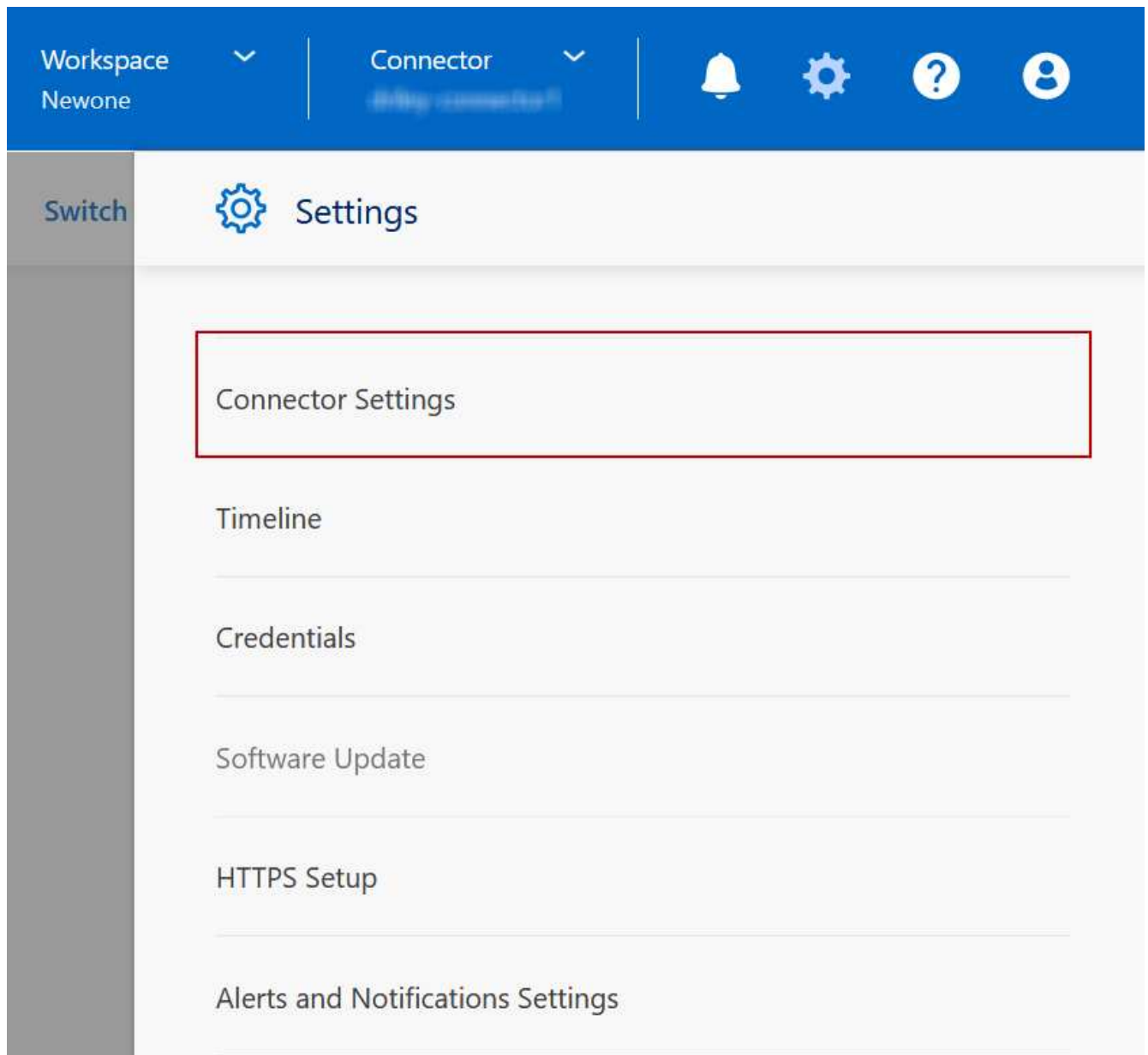
这些设置会影响由连接器管理的所有Cloud Volumes ONTAP 系统。如果您有另一个连接器、则可以对其进行不同的配置。

所需权限

要修改Connector设置、需要帐户管理员权限。

步骤

1. 在BlueXP控制台的右上角、单击设置图标、然后选择*连接器设置*。



2. 在*容量*下、修改以下任何设置：

容量管理模式

选择BlueXP是否通知您存储容量决策、或者BlueXP是否自动管理您的容量需求。

["了解容量管理模式的工作原理"](#)。

聚合容量阈值—可用空间比率

当聚合上的可用空间比率降至指定阈值以下时触发通知。

可用空间比率的计算方法如下：

$(\text{聚合容量} - \text{聚合上的总已用容量}) / \text{聚合容量}$

聚合容量阈值—数据分层的可用空间比率

定义将数据分层到容量层(对象存储)时、性能层(磁盘)需要多少可用空间。

此比率对于灾难恢复情形非常重要。从容量层读取数据时、Cloud Volumes ONTAP 会将数据移至性能层以提高性能。如果空间不足，则 Cloud Volumes ONTAP 无法移动数据。

3. 单击 * 保存 *。

Storage VM 管理

在BlueXP中管理Storage VM

Storage VM 是在 ONTAP 中运行的虚拟机，可为客户端提供存储和数据服务。您可能会将其识别为 *svm* 或 *vserver*。默认情况下，Cloud Volumes ONTAP 配置有一个 Storage VM，但某些配置支持额外的 Storage VM。

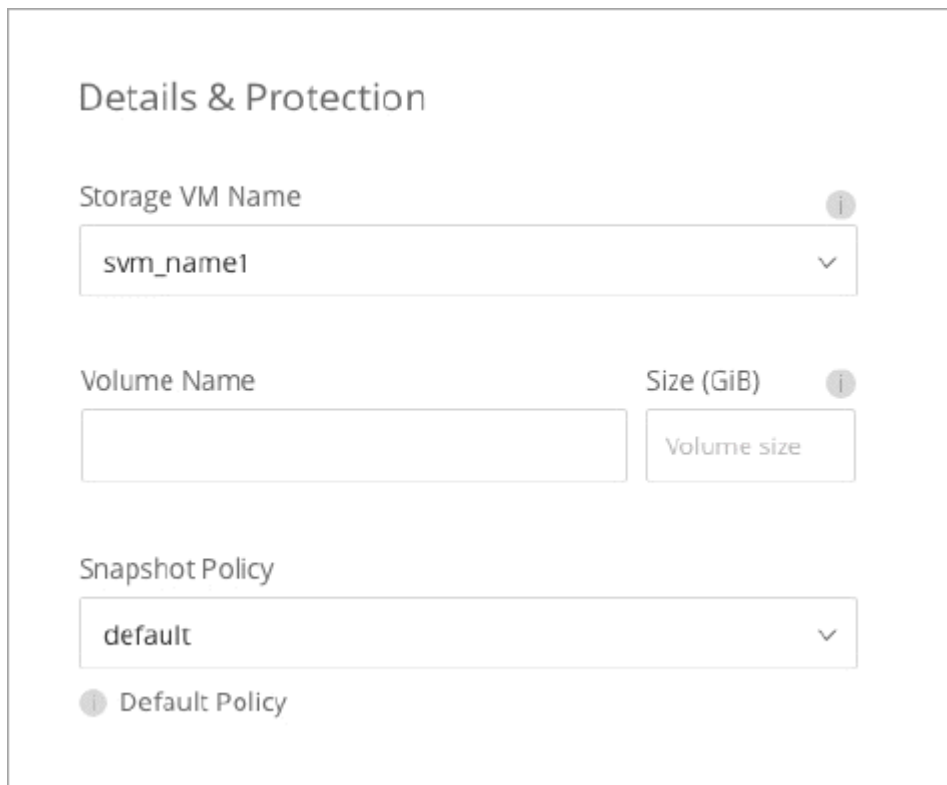
支持的 Storage VM 数量

某些配置支持多个Storage VM。转至 "[《Cloud Volumes ONTAP 发行说明》](#)" 验证您的 Cloud Volumes ONTAP 版本支持的 Storage VM 数量。

使用多个 Storage VM

BlueXP支持您通过System Manager或CLI创建的任何其他Storage VM。

例如，下图显示了在创建卷时如何选择 Storage VM。



The screenshot shows a configuration interface titled "Details & Protection". It contains the following elements:

- Storage VM Name:** A dropdown menu with "svm_name1" selected and a downward arrow.
- Volume Name:** An empty text input field.
- Size (GiB):** A text input field with "Volume size" written inside.
- Snapshot Policy:** A dropdown menu with "default" selected and a downward arrow.
- Default Policy:** A label with an information icon (i) next to it.

下图显示了在将卷复制到其他系统时如何选择 Storage VM。

Destination Volume Name
volume_copy

Destination Storage VM Name
svm_name1

Destination Aggregate
Automatically select the best aggregate

修改默认 **Storage VM** 的名称

BlueXP会自动为其为Cloud Volumes ONTAP 创建的单个Storage VM命名。如果您有严格的命名标准、则可以在System Manager、命令行界面或API中修改Storage VM的名称。例如，您可能希望此名称与您为 ONTAP 集群命名 Storage VM 的方式一致。

在 **AWS** 中为 **Cloud Volumes ONTAP** 创建提供数据的 **Storage VM**

Storage VM 是在 ONTAP 中运行的虚拟机，可为客户端提供存储和数据服务。您可能会将其识别为 *svm* 或 *vserver*。默认情况下，Cloud Volumes ONTAP 配置有一个 Storage VM，但某些配置支持额外的 Storage VM。

要创建其他提供数据的 Storage VM，您需要在 AWS 中分配 IP 地址，然后根据 Cloud Volumes ONTAP 配置运行 ONTAP 命令。

支持的 **Storage VM** 数量

从 9.7 版开始，特定 Cloud Volumes ONTAP 配置支持多个 Storage VM。转至 "[《Cloud Volumes ONTAP 发行说明》](#)" 验证您的 Cloud Volumes ONTAP 版本支持的 Storage VM 数量。

所有其他 Cloud Volumes ONTAP 配置均支持一个提供数据的 Storage VM 和一个用于灾难恢复的目标 Storage VM。如果源 Storage VM 发生中断，您可以激活目标 Storage VM 以进行数据访问。

验证配置限制

每个 EC2 实例支持每个网络接口的最大专用 IPv4 地址数。在 AWS 中为新 Storage VM 分配 IP 地址之前，您需要验证此限制。

步骤

1. 转到 "[《Cloud Volumes ONTAP 发行说明》](#) 中的 "存储限制" 部分"。
2. 确定实例类型中每个接口的最大 IP 地址数。

3. 请记住此数字，因为在 AWS 中分配 IP 地址时，您将在下一节中需要此数字。

在 AWS 中分配 IP 地址

在为新 Storage VM 创建 LIF 之前，必须将专用 IPv4 地址分配给 AWS 中的端口 e0a。

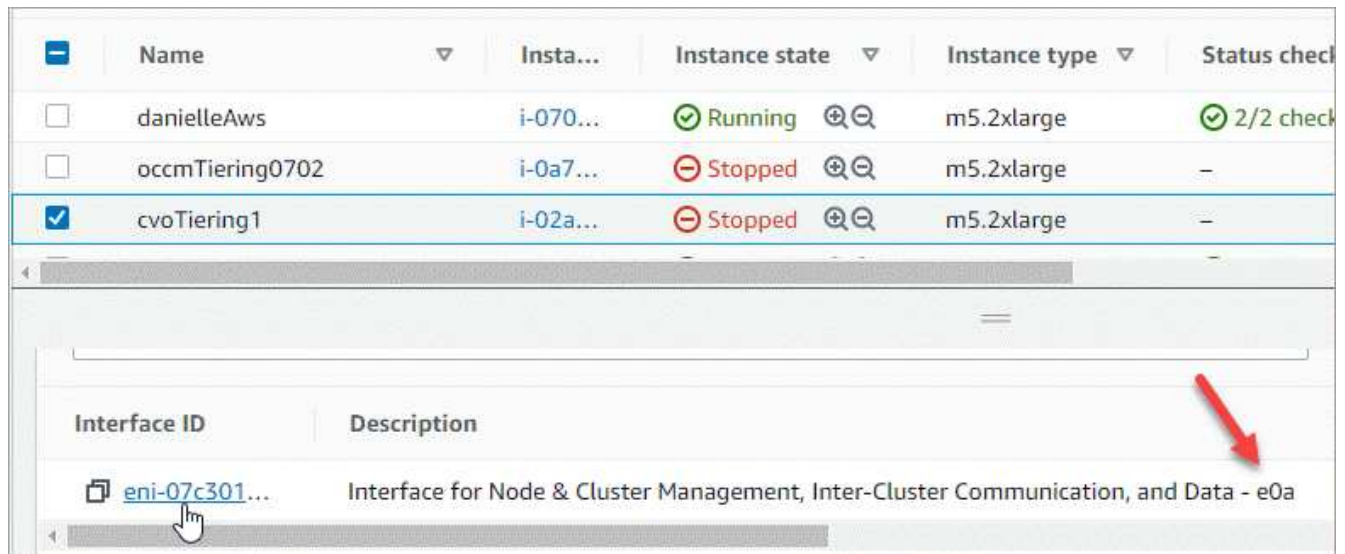
请注意，Storage VM 的可选管理 LIF 需要在单节点系统上和单个 AZ 中的 HA 对上使用专用 IP 地址。此管理 LIF 可连接到 SnapCenter 等管理工具。

步骤

1. 登录到 AWS 并打开 EC2 服务。
2. 选择 Cloud Volumes ONTAP 实例并单击 * 网络连接 *。

如果要在 HA 对上创建 Storage VM，请选择节点 1。

3. 向下滚动到 * 网络接口 *，然后单击端口 e0a 的 * 接口 ID*。



4. 选择网络接口，然后单击 * 操作 > 管理 IP 地址 *。
5. 展开 e0a 的 IP 地址列表。
6. 验证 IP 地址：
 - a. 计算已分配 IP 地址的数量，以确认此端口是否有空间可供其他 IP 使用。
您应已在此页面上一节中确定每个接口支持的最大 IP 地址数。
 - b. 可选：转到 Cloud Volumes ONTAP 的命令行界面并运行 * 网络接口 show* 以确认这些 IP 地址中的每个地址均已使用。

如果某个 IP 地址未使用，则可以将其与新的 Storage VM 结合使用。

7. 返回 AWS 控制台，单击 * 分配新 IP 地址 *，根据新 Storage VM 所需的数量分配其他 IP 地址。

- 单节点系统：需要一个未使用的二级专用 IP。

如果要在 Storage VM 上创建管理 LIF，则需要可选的二级专用 IP。

- 一个 AZ 中的 HA 对：节点 1 上需要一个未使用的二级专用 IP。

如果要在 Storage VM 上创建管理 LIF，则需要可选的二级专用 IP。

- 多个 AZs 中的 HA 对：每个节点需要一个未使用的二级专用 IP。

8. 如果要在单个 AZ 中为 HA 对分配 IP 地址，请启用 * 允许重新分配二级专用 IPv4 地址 *。
9. 单击 * 保存 *。
10. 如果您的 HA 对位于多个 AZs 中，则需要对节点 2 重复这些步骤。

在单节点系统上创建 **Storage VM**

以下步骤将在单节点系统上创建新的 Storage VM。创建 NAS LIF 需要一个专用 IP 地址，如果要创建管理 LIF，则需要另一个可选专用 IP 地址。

步骤

1. 创建 Storage VM 和指向 Storage VM 的路由。

```
vserver create -rootvolume-security-style unix -rootvolume root_svm_2  
-snapshot-policy default -vserver svm_2 -aggregate aggr1
```

```
network route create -destination 0.0.0.0/0 -vserver svm_2 -gateway  
subnet_gateway
```

2. 创建 NAS LIF。

```
network interface create -auto-revert true -vserver svm_2 -service  
-policy default-data-files -home-port e0a -address private_ip_x -netmask  
node1Mask -lif ip_nas_2 -home-node cvo-node
```

其中 *private_ip_x* 是 e0a 上未使用的二级专用 IP。

3. 可选：创建 Storage VM 管理 LIF。

```
network interface create -auto-revert true -vserver svm_2 -service  
-policy default-management -home-port e0a -address private_ip_y -netmask  
node1Mask -lif ip_svm_mgmt_2 -home-node cvo-node
```

其中 *private_ip_y* 是 e0a 上另一个未使用的二级专用 IP。

4. 将一个或多个聚合分配给 Storage VM。

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

之所以需要执行此步骤，是因为新的 Storage VM 需要至少访问一个聚合，然后才能在 Storage VM 上创建卷。

在一个 AZ 中的 HA 对上创建一个 Storage VM

以下步骤将在一个 AZ 中的 HA 对上创建一个新的 Storage VM。创建 NAS LIF 需要一个专用 IP 地址，如果要创建管理 LIF，则需要另一个可选专用 IP 地址。

这两个 LIF 都在节点 1 上分配。如果发生故障，专用 IP 地址可以在节点之间移动。

步骤

1. 创建 Storage VM 和指向 Storage VM 的路由。

```
vserver create -rootvolume-security-style unix -rootvolume root_svm_2  
-snapshot-policy default -vserver svm_2 -aggregate aggr1
```

```
network route create -destination 0.0.0.0/0 -vserver svm_2 -gateway  
subnet_gateway
```

2. 在节点 1 上创建 NAS LIF。

```
network interface create -auto-revert true -vserver svm_2 -service  
-policy default-data-files -home-port e0a -address private_ip_x -netmask  
node1Mask -lif ip_nas_2 -home-node cvo-node1
```

其中 *private_ip_x* 是 CVO-node1 的 e0a 上未使用的二级专用 IP。如果发生接管，可以将此 IP 地址重新定位到 CVO-node2 的 e0a，因为服务策略 *default-data-files* 指示 IP 可以迁移到配对节点。

3. 可选：在节点 1 上创建 Storage VM 管理 LIF。

```
network interface create -auto-revert true -vserver svm_2 -service  
-policy default-management -home-port e0a -address private_ip_y -netmask  
node1Mask -lif ip_svm_mgmt_2 -home-node cvo-node1
```

其中 *private_ip_y* 是 e0a 上另一个未使用的二级专用 IP。

4. 将一个或多个聚合分配给 Storage VM。

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

之所以需要执行此步骤，是因为新的 Storage VM 需要至少访问一个聚合，然后才能在 Storage VM 上创建卷。

5. 如果您运行的是 Cloud Volumes ONTAP 9.11.1 或更高版本，请修改此 Storage VM 的网络服务策略。

需要修改服务，因为它可以确保 Cloud Volumes ONTAP 可以使用 iSCSI LIF 进行出站管理连接。

```
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service data-fpolicy-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ad-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-dns-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ldap-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-nis-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-ad-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-dns-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-ldap-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-nis-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-ad-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-dns-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-ldap-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-nis-client
```

在多个 AZs 中的 HA 对上创建一个 Storage VM

以下步骤将在多个 AZs 中的 HA 对上创建一个新的 Storage VM。

NAS LIF 需要 *float* IP 地址，而管理 LIF 则可选。这些浮动 IP 地址不要求您在 AWS 中分配私有 IP。而是在 AWS 路由表中自动配置浮动 IP，以指向同一 VPC 中特定节点的 ENI。

要使浮动 IP 与 ONTAP 配合使用，必须在每个节点上的每个 Storage VM 上配置一个专用 IP 地址。这一点反映

在以下步骤中，在节点 1 和节点 2 上创建 iSCSI LIF。

步骤

1. 创建 Storage VM 和指向 Storage VM 的路由。

```
vserver create -rootvolume-security-style unix -rootvolume root_svm_2  
-snapshot-policy default -vserver svm_2 -aggregate aggr1
```

```
network route create -destination 0.0.0.0/0 -vserver svm_2 -gateway  
subnet_gateway
```

2. 在节点 1 上创建 NAS LIF。

```
network interface create -auto-revert true -vserver svm_2 -service  
-policy default-data-files -home-port e0a -address floating_ip -netmask  
node1Mask -lif ip_nas_floating_2 -home-node cvo-node1
```

- 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。192.168.209.27 是一个示例浮动 IP 地址。"[了解有关选择浮动 IP 地址的更多信息](#)"。
- `-service-policy default-data-files` 表示 IP 可以迁移到配对节点。

3. 可选：在节点 1 上创建 Storage VM 管理 LIF。

```
network interface create -auto-revert true -vserver svm_2 -service  
-policy default-management -home-port e0a -address floating_ip -netmask  
node1Mask -lif ip_svm_mgmt_2 -home-node cvo-node1
```

4. 在节点 1 上创建 iSCSI LIF。

```
network interface create -vserver svm_2 -service-policy default-data-  
blocks -home-port e0a -address private_ip -netmask node1Mask -lif  
ip_node1_iscsi_2 -home-node cvo-node1
```

- 要支持 Storage VM 中浮动 IP 的 LIF 迁移，需要使用此 iSCSI LIF。它不必是 iSCSI LIF，但不能配置为在节点之间迁移。
- `-service-policy default-data-block` 表示 IP 地址不会在节点之间迁移。
- `private_ip` 是 CVO_node1 的 eth0（e0a）上未使用的二级专用 IP 地址。

5. 在节点 2 上创建 iSCSI LIF。

```
network interface create -vserver svm_2 -service-policy default-data-  
blocks -home-port e0a -address private_ip -netmaskNode2Mask -lif  
ip_node2_iscsi_2 -home-node cvo-node2
```

- 要支持 Storage VM 中浮动 IP 的 LIF 迁移，需要使用此 iSCSI LIF。它不必是 iSCSI LIF，但不能配置为在节点之间迁移。
- `-service-policy default-data-block` 表示 IP 地址不会在节点之间迁移。
- `private_ip` 是 CVO_node2 的 eth0（e0a）上未使用的二级专用 IP 地址。

6. 将一个或多个聚合分配给 Storage VM。

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

之所以需要执行此步骤，是因为新的 Storage VM 需要至少访问一个聚合，然后才能在 Storage VM 上创建卷。

7. 如果您运行的是 Cloud Volumes ONTAP 9.11.1 或更高版本，请修改此 Storage VM 的网络服务策略。

需要修改服务，因为它可以确保 Cloud Volumes ONTAP 可以使用 iSCSI LIF 进行出站管理连接。

```

network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service data-fpolicy-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ad-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-dns-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ldap-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-nis-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-ad-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-dns-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-ldap-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-nis-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-ad-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-dns-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-ldap-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-nis-client

```

在 Azure 中为 Cloud Volumes ONTAP 创建提供数据的 Storage VM

Storage VM 是在 ONTAP 中运行的虚拟机，可为客户端提供存储和数据服务。您可能会将其识别为 *svm* 或 *vserver*。默认情况下，Cloud Volumes ONTAP 配置有一个 Storage VM，但在 Azure 中运行 Cloud Volumes ONTAP 时，支持其他 Storage VM。

要创建其他提供数据的 Storage VM，您需要在 Azure 中分配 IP 地址，然后运行 ONTAP 命令来创建 Storage VM 和数据 LIF。

支持的 Storage VM 数量

从 9.9.0 版开始，特定 Cloud Volumes ONTAP 配置支持多个 Storage VM。转至 "[《Cloud Volumes ONTAP 发行说明》](#)" 验证您的 Cloud Volumes ONTAP 版本支持的 Storage VM 数量。

所有其他 Cloud Volumes ONTAP 配置均支持一个提供数据的 Storage VM 和一个用于灾难恢复的目标 Storage VM。如果源 Storage VM 发生中断，您可以激活目标 Storage VM 以进行数据访问。

在 Azure 中分配 IP 地址

在创建 Storage VM 和分配 LIF 之前，您需要在 Azure 中分配 IP 地址。

单节点系统

在创建 Storage VM 并分配 LIF 之前，必须在 Azure 中将 IP 地址分配给 nic0。

您需要为数据 LIF 访问创建一个 IP 地址，并为 Storage VM （SVM）管理 LIF 创建另一个可选 IP 地址。此管理 LIF 可连接到 SnapCenter 等管理工具。

步骤

1. 登录到 Azure 门户并打开 * 虚拟机 * 服务。
2. 单击 Cloud Volumes ONTAP VM 的名称。
3. 单击 * 网络连接 *。
4. 单击 nic0 的网络接口名称。
5. 在 * 设置 * 下，单击 * IP 配置 *。
6. 单击 * 添加 *。
7. 输入 IP 配置的名称，选择 * 动态 *，然后单击 * 确定 *。
8. 单击刚刚创建的 IP 配置的名称，将 * 分配 * 更改为 * 静态 *，然后单击 * 保存 *。

最好使用静态 IP 地址，因为静态 IP 可确保 IP 地址不会更改，这有助于防止应用程序发生不必要的中断。

如果要创建 SVM 管理 LIF，请重复这些步骤以创建其他 IP 地址。

完成后

复制刚刚创建的专用 IP 地址。在为新 Storage VM 创建 LIF 时，您需要指定这些 IP 地址。

HA对

如何为 HA 对分配 IP 地址取决于您使用的存储协议。

iSCSI

在创建 Storage VM 和分配 LIF 之前，必须在 Azure 中将 iSCSI IP 地址分配给 nic0。iSCSI 的 IP 分配给 nic0，而不是负载均衡器，因为 iSCSI 使用 ALUA 进行故障转移。

您需要创建以下 IP 地址：

- 一个 IP 地址，用于从节点 1 访问 iSCSI 数据 LIF
- 一个用于从节点2访问iSCSI数据LIF的IP地址
- Storage VM（SVM）管理 LIF 的可选 IP 地址

此管理 LIF 可连接到 SnapCenter 等管理工具。

步骤

1. 登录到 Azure 门户并打开 * 虚拟机 * 服务。
2. 单击节点 1 的 Cloud Volumes ONTAP VM 的名称。
3. 单击 * 网络连接 *。
4. 单击 nic0 的网络接口名称。
5. 在 * 设置 * 下，单击 * IP 配置 *。
6. 单击 * 添加 *。
7. 输入 IP 配置的名称，选择 * 动态 *，然后单击 * 确定 *。
8. 单击刚刚创建的 IP 配置的名称，将 * 分配 * 更改为 * 静态 *，然后单击 * 保存 *。

最好使用静态 IP 地址，因为静态 IP 可确保 IP 地址不会更改，这有助于防止应用程序发生不必要的中断。

9. 在节点 2 上重复上述步骤。
10. 如果要创建 SVM 管理 LIF，请在节点 1 上重复这些步骤。

NFS

用于 NFS 的 IP 地址会在负载均衡器中分配，以便在发生故障转移事件时，IP 地址可以迁移到另一个节点。

您需要创建以下 IP 地址：

- 一个 IP 地址，用于从节点 1 访问 NAS 数据 LIF
- 一个用于从节点2访问NAS数据LIF的IP地址
- Storage VM（SVM）管理 LIF 的可选 IP 地址

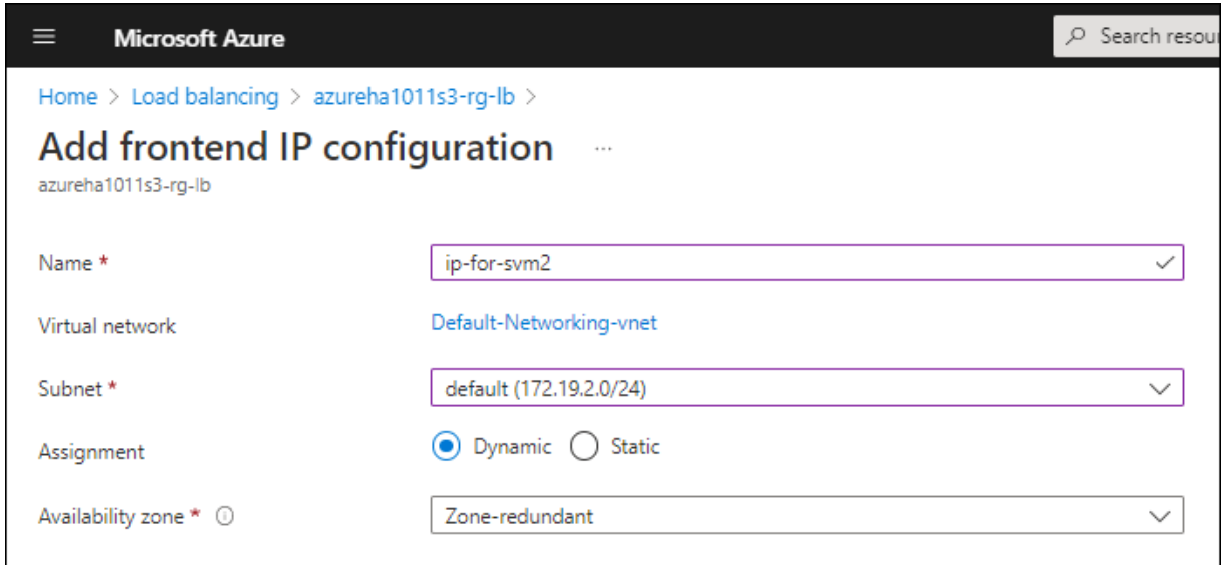
DNS通信需要iSCSI LIF。为此，我们使用了 iSCSI LIF，因为它不会在故障转移时迁移。

此管理 LIF 可连接到 SnapCenter 等管理工具。

步骤

1. 在 Azure 门户中，打开 * 负载均衡器 * 服务。

2. 单击 HA 对的负载均衡器的名称。
3. 为从节点 1 访问数据 LIF 创建一个前端 IP 配置，为从节点 2 访问数据 LIF 创建另一个前端 IP 配置，并为 Storage VM （SVM）管理 LIF 创建另一个可选前端 IP 。
 - a. 在 * 设置 * 下，单击 * 前端 IP 配置 * 。
 - b. 单击 * 添加 * 。
 - c. 输入前端IP的名称、选择Cloud Volumes ONTAP HA对的子网、并保留*动态*选项、在具有可用性区域的区域中、保留*区域冗余*选项、以确保在区域发生故障时IP地址仍然可用。



The screenshot shows the 'Add frontend IP configuration' page in the Microsoft Azure portal. The breadcrumb navigation is 'Home > Load balancing > azureha1011s3-rg-lb >'. The title is 'Add frontend IP configuration' with a three-dot menu icon. Below the title is the resource name 'azureha1011s3-rg-lb'. The form contains the following fields:

- Name ***: A text input field containing 'ip-for-svm2' with a checkmark icon on the right.
- Virtual network**: A dropdown menu showing 'Default-Networking-vnet'.
- Subnet ***: A dropdown menu showing 'default (172.19.2.0/24)' with a downward arrow icon.
- Assignment**: Two radio buttons, 'Dynamic' (which is selected) and 'Static'.
- Availability zone ***: A dropdown menu showing 'Zone-redundant' with a downward arrow icon.

- d. 单击刚刚创建的前端 IP 配置的名称，将 * 分配 * 更改为 * 静态 * ，然后单击 * 保存 * 。

最好使用静态 IP 地址，因为静态 IP 可确保 IP 地址不会更改，这有助于防止应用程序发生不必要的中断。

4. 为刚刚创建的每个前端 IP 添加运行状况探测。
 - a. 在负载均衡器的 * 设置 * 下，单击 * 运行状况探针 * 。
 - b. 单击 * 添加 * 。
 - c. 输入运行状况探测的名称，并输入介于 63005 和 65000 之间的端口号。保留其他字段的默认值。

端口号必须介于 63005 和 65000 之间，这一点很重要。例如，如果要创建三个运行状况探测，则可以输入端口号为 63005 ， 63006 和 63007 的探测。



Home > Load balancers > azureha1011s3-rg-lb >

Add health probe ...

azureha1011s3-rg-lb

Name *	<input type="text" value="svm2-health-probe1"/>	✓
Protocol *	<input type="text" value="TCP"/>	▼
Port * ⓘ	<input type="text" value="63005"/>	✓
Interval * ⓘ	<input type="text" value="5"/>	seconds
Unhealthy threshold * ⓘ	<input type="text" value="2"/>	consecutive failures
Used by ⓘ	Not used	

5. 为每个前端 IP 创建新的负载均衡规则。
 - a. 在负载均衡器的 * 设置 * 下，单击 * 负载均衡规则 *。
 - b. 单击 * 添加 * 并输入所需信息：
 - * 名称 *：输入规则的名称。
 - * IP 版本 *：选择 * IPv4 *。
 - * 前端 IP 地址 *：选择刚刚创建的前端 IP 地址之一。
 - * 高可用性端口 *：启用此选项。
 - * 后端池 *：保留已选择的默认后端池。
 - * 运行状况探测 *：选择为选定前端 IP 创建的运行状况探测。
 - * 会话持久性 *：选择 * 无 *。
 - * 浮动 IP*：选择 * 已启用 *。

Add load balancing rule

chandanaTcpRst3-rg-lb

i A load balancing rule distributes incoming traffic that is sent to a selected IP address and port combination across a group of backend pool instances. Only backend instances that the health probe considers healthy receive new traffic.

Name *
jimmy_new_rule ✓

IP Version *
 IPv4 IPv6

Frontend IP address * ⓘ
10.1.0.156 (dataAFIP) ▼

HA Ports ⓘ

Backend pool ⓘ
backendPool (2 virtual machines) ▼

Health probe ⓘ
dataAProbe (TCP:63002) ▼

Session persistence ⓘ
None ▼

Floating IP ⓘ
 Disabled Enabled

6. 确保 Cloud Volumes ONTAP 的网络安全组规则允许负载均衡器为在上述步骤 4 中创建的运行状况探测发送 TCP 探测。请注意，默认情况下允许这样做。

SMB

用于 SMB 数据的 IP 地址会在负载均衡器中分配，以便在发生故障转移事件时，IP 地址可以迁移到另一个节点。

您需要在负载均衡器中创建以下 IP 地址：

- 一个 IP 地址，用于从节点 1 访问 NAS 数据 LIF
- 一个用于从节点 2 访问 NAS 数据 LIF 的 IP 地址
- 每个 VM 各自 NIC 0 中节点 1 上的 iSCSI LIF 的一个 IP 地址
- 节点 2 上的 iSCSI LIF 使用一个 IP 地址

DNS 和 SMB 通信需要 iSCSI LIF。为此，我们使用了 iSCSI LIF，因为它不会在故障转移时迁移。

- Storage VM（SVM）管理 LIF 的可选 IP 地址

此管理 LIF 可连接到 SnapCenter 等管理工具。

步骤

1. 在 Azure 门户中，打开 * 负载均衡器 * 服务。
2. 单击 HA 对的负载均衡器的名称。
3. 仅为数据和SVM LIF创建所需数量的前端IP配置：



只能在NIC0下为每个相应的SVM创建前端IP。有关如何将IP地址添加到SVM NIC0的详细信息、请参见第7步[[hyperlink](#)]

- a. 在 * 设置 * 下，单击 * 前端 IP 配置 *。
- b. 单击 * 添加 *。
- c. 输入前端IP的名称、选择Cloud Volumes ONTAP HA对的子网、并保留*动态*选项、在具有可用性区域的区域中、保留*区域冗余*选项、以确保在区域发生故障时IP地址仍然可用。

The screenshot shows the 'Add frontend IP configuration' page in the Microsoft Azure portal. The breadcrumb navigation is 'Home > Load balancing > azureha1011s3-rg-lb >'. The title is 'Add frontend IP configuration' with a three-dot menu icon. Below the title is the resource name 'azureha1011s3-rg-lb'. The form contains the following fields:

- Name ***: A text input field containing 'ip-for-svm2' with a checkmark icon on the right.
- Virtual network**: A dropdown menu showing 'Default-Networking-vnet'.
- Subnet ***: A dropdown menu showing 'default (172.19.2.0/24)' with a downward arrow icon.
- Assignment**: Two radio buttons, 'Dynamic' (selected) and 'Static'.
- Availability zone ***: A dropdown menu showing 'Zone-redundant' with a downward arrow icon and an information icon.

- d. 单击刚刚创建的前端 IP 配置的名称，将 * 分配 * 更改为 * 静态 *，然后单击 * 保存 *。

最好使用静态 IP 地址，因为静态 IP 可确保 IP 地址不会更改，这有助于防止应用程序发生不必要的中断。

4. 为刚刚创建的每个前端 IP 添加运行状况探测。
 - a. 在负载均衡器的 * 设置 * 下，单击 * 运行状况探针 *。
 - b. 单击 * 添加 *。
 - c. 输入运行状况探测的名称，并输入介于 63005 和 65000 之间的端口号。保留其他字段的默认值。

端口号必须介于 63005 和 65000 之间，这一点很重要。例如，如果要创建三个运行状况探测，则可以输入端口号为 63005，63006 和 63007 的探测。



Home > Load balancers > azureha1011s3-rg-lb >

Add health probe ...

azureha1011s3-rg-lb

Name *	<input type="text" value="svm2-health-probe1"/>	✓
Protocol *	<input type="text" value="TCP"/>	▼
Port * ⓘ	<input type="text" value="63005"/>	✓
Interval * ⓘ	<input type="text" value="5"/>	seconds
Unhealthy threshold * ⓘ	<input type="text" value="2"/>	consecutive failures
Used by ⓘ	Not used	

5. 为每个前端 IP 创建新的负载均衡规则。
 - a. 在负载均衡器的 * 设置 * 下，单击 * 负载均衡规则 *。
 - b. 单击 * 添加 * 并输入所需信息：
 - * 名称 *：输入规则的名称。
 - * IP 版本 *：选择 * IPv4 *。
 - * 前端 IP 地址 *：选择刚刚创建的前端 IP 地址之一。
 - * 高可用性端口 *：启用此选项。
 - * 后端池 *：保留已选择的默认后端池。
 - * 运行状况探测 *：选择为选定前端 IP 创建的运行状况探测。
 - * 会话持久性 *：选择 * 无 *。
 - * 浮动 IP*：选择 * 已启用 *。

Add load balancing rule

chandanaTcpRst3-rg-lb

i A load balancing rule distributes incoming traffic that is sent to a selected IP address and port combination across a group of backend pool instances. Only backend instances that the health probe considers healthy receive new traffic.

Name *
jimmy_new_rule ✓

IP Version *
 IPv4 IPv6

Frontend IP address * ⓘ
10.1.0.156 (dataAFIP) ▼

HA Ports ⓘ

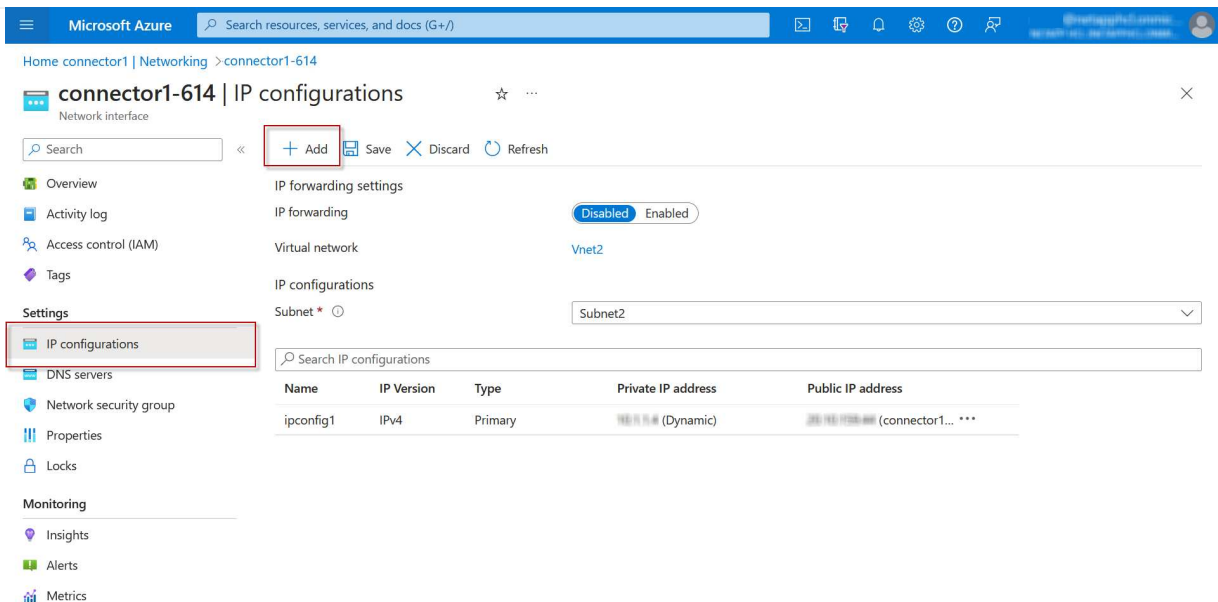
Backend pool ⓘ
backendPool (2 virtual machines) ▼

Health probe ⓘ
dataProbe (TCP:63002) ▼

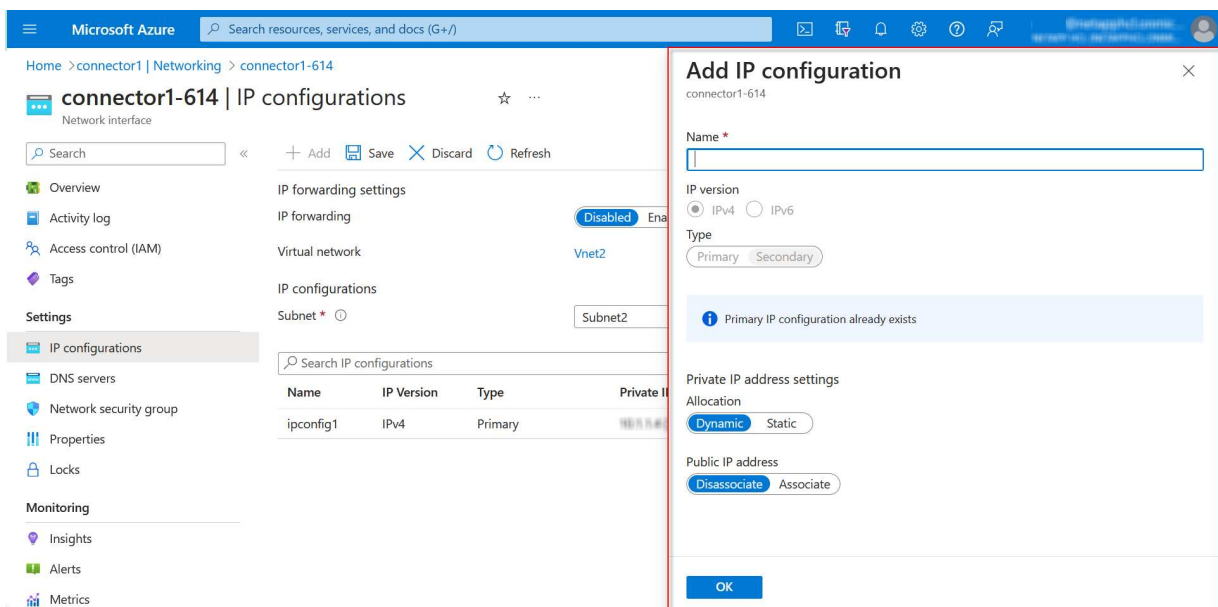
Session persistence ⓘ
None ▼

Floating IP ⓘ
 Disabled Enabled

6. 确保 Cloud Volumes ONTAP 的网络安全组规则允许负载均衡器为在上述步骤 4 中创建的运行状况探测发送 TCP 探测。请注意，默认情况下允许这样做。
7. 对于 iSCSI LIF、请为 NIC0 添加 IP 地址。
 - a. 单击 Cloud Volumes ONTAP VM 的名称。
 - b. 单击 * 网络连接 *。
 - c. 单击 nic0 的网络接口名称。
 - d. 在设置下、单击* IP配置*。
 - e. 单击 * 添加 *。



f. 输入IP配置的名称、选择动态、然后单击*确定*。



g. 单击刚刚创建的IP配置的名称、将"Assignment"更改为"Static"、然后单击*保存*。



最好使用静态 IP 地址，因为静态 IP 可确保 IP 地址不会更改，这有助于防止应用程序发生不必要的中断。

完成后

复制刚刚创建的专用 IP 地址。在为新 Storage VM 创建 LIF 时，您需要指定这些 IP 地址。

创建 Storage VM 和 LIF

在 Azure 中分配 IP 地址后，您可以在单节点系统或 HA 对上创建新的 Storage VM 。

单节点系统

如何在单节点系统上创建 Storage VM 和 LIF 取决于所使用的存储协议。

iSCSI

按照以下步骤创建新的 Storage VM 以及所需的 LIF 。

步骤

1. 创建 Storage VM 和指向 Storage VM 的路由。

```
vserver create -vserver <svm-name> -subtype default -rootvolume  
<root-volume-name> -rootvolume-security-style unix
```

```
network route create -destination 0.0.0.0/0 -vserver <svm-name>  
-gateway <ip-of-gateway-server>
```

2. 创建数据 LIF ：

```
network interface create -vserver <svm-name> -home-port e0a -address  
<iscsi-ip-address> -netmask-length <# of mask bits> -lif <lif-name>  
-home-node <name-of-nodel> -data-protocol iscsi
```

3. 可选：创建 Storage VM 管理 LIF 。

```
network interface create -vserver <svm-name> -lif <lif-name> -role  
data -data-protocol none -address <svm-mgmt-ip-address> -netmask  
-length <length> -home-node <name-of-nodel> -status-admin up  
-failover-policy system-defined -firewall-policy mgmt -home-port e0a  
-auto-revert false -failover-group Default
```

4. 将一个或多个聚合分配给 Storage VM 。

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

之所以需要执行此步骤，是因为新的 Storage VM 需要至少访问一个聚合，然后才能在 Storage VM 上创建卷。

NFS

按照以下步骤创建新的 Storage VM 以及所需的 LIF 。

步骤

1. 创建 Storage VM 和指向 Storage VM 的路由。

```
vserver create -vserver <svm-name> -subtype default -rootvolume  
<root-volume-name> -rootvolume-security-style unix
```

```
network route create -destination 0.0.0.0/0 -vserver <svm-name>  
-gateway <ip-of-gateway-server>
```

2. 创建数据 LIF :

```
network interface create -vserver <svm-name> -lif <lif-name> -role  
data -data-protocol cifs,nfs -address <nas-ip-address> -netmask  
-length <length> -home-node <name-of-node1> -status-admin up  
-failover-policy disabled -firewall-policy data -home-port e0a -auto  
-revert true -failover-group Default
```

3. 可选: 创建 Storage VM 管理 LIF 。

```
network interface create -vserver <svm-name> -lif <lif-name> -role  
data -data-protocol none -address <svm-mgmt-ip-address> -netmask  
-length <length> -home-node <name-of-node1> -status-admin up  
-failover-policy system-defined -firewall-policy mgmt -home-port e0a  
-auto-revert false -failover-group Default
```

4. 将一个或多个聚合分配给 Storage VM 。

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

之所以需要执行此步骤，是因为新的 Storage VM 需要至少访问一个聚合，然后才能在 Storage VM 上创建卷。

SMB

按照以下步骤创建新的 Storage VM 以及所需的 LIF 。

步骤

1. 创建 Storage VM 和指向 Storage VM 的路由。

```
vserver create -vserver <svm-name> -subtype default -rootvolume  
<root-volume-name> -rootvolume-security-style unix
```

```
network route create -destination 0.0.0.0/0 -vserver <svm-name>
-gateway <ip-of-gateway-server>
```

2. 创建数据 LIF :

```
network interface create -vserver <svm-name> -lif <lif-name> -role
data -data-protocol cifs,nfs -address <nas-ip-address> -netmask
-length <length> -home-node <name-of-node1> -status-admin up
-failover-policy disabled -firewall-policy data -home-port e0a -auto
-revert true -failover-group Default
```

3. 可选: 创建 Storage VM 管理 LIF 。

```
network interface create -vserver <svm-name> -lif <lif-name> -role
data -data-protocol none -address <svm-mgmt-ip-address> -netmask
-length <length> -home-node <name-of-node1> -status-admin up
-failover-policy system-defined -firewall-policy mgmt -home-port e0a
-auto-revert false -failover-group Default
```

4. 将一个或多个聚合分配给 Storage VM 。

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

之所以需要执行此步骤，是因为新的 Storage VM 需要至少访问一个聚合，然后才能在 Storage VM 上创建卷。

HA对

如何在 HA 对上创建 Storage VM 和 LIF 取决于所使用的存储协议。

iSCSI

按照以下步骤创建新的 Storage VM 以及所需的 LIF 。

步骤

1. 创建 Storage VM 和指向 Storage VM 的路由。

```
vserver create -vserver <svm-name> -subtype default -rootvolume  
<root-volume-name> -rootvolume-security-style unix
```

```
network route create -destination 0.0.0.0/0 -vserver <svm-name>  
-gateway <ip-of-gateway-server>
```

2. 创建数据 LIF ：

- a. 使用以下命令在节点 1 上创建 iSCSI LIF 。

```
network interface create -vserver <svm-name> -home-port e0a  
-address <iscsi-ip-address> -netmask-length <# of mask bits> -lif  
<lif-name> -home-node <name-of-node1> -data-protocol iscsi
```

- b. 使用以下命令在节点2上创建iSCSI LIF。

```
network interface create -vserver <svm-name> -home-port e0a  
-address <iscsi-ip-address> -netmask-length <# of mask bits> -lif  
<lif-name> -home-node <name-of-node2> -data-protocol iscsi
```

3. 可选：在节点 1 上创建 Storage VM 管理 LIF 。

```
network interface create -vserver <svm-name> -lif <lif-name> -role  
data -data-protocol none -address <svm-mgmt-ip-address> -netmask  
-length <length> -home-node <name-of-node1> -status-admin up  
-failover-policy system-defined -firewall-policy mgmt -home-port e0a  
-auto-revert false -failover-group Default
```

此管理 LIF 可连接到 SnapCenter 等管理工具。

4. 将一个或多个聚合分配给 Storage VM 。

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

之所以需要执行此步骤，是因为新的 Storage VM 需要至少访问一个聚合，然后才能在 Storage VM 上创建卷。

5. 如果您运行的是Cloud Volumes ONTAP 9.11.1或更高版本、请修改此Storage VM的网络服务策略。
 - a. 输入以下命令以访问高级模式。

```
::> set adv -con off
```

需要修改服务、因为它可以确保Cloud Volumes ONTAP 可以使用iSCSI LIF进行出站管理连接。

```
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service data-fpolicy-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ad-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-dns-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ldap-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-nis-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-ad-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-dns-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-ldap-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-nis-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-ad-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-dns-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-ldap-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-nis-client
```

NFS

按照以下步骤创建新的 Storage VM 以及所需的 LIF 。

步骤

1. 创建 Storage VM 和指向 Storage VM 的路由。

```
vserver create -vserver <svm-name> -subtype default -rootvolume  
<root-volume-name> -rootvolume-security-style unix
```

```
network route create -destination 0.0.0.0/0 -vserver <svm-name>  
-gateway <ip-of-gateway-server>
```

2. 创建数据 LIF :

a. 使用以下命令在节点 1 上创建 NAS LIF 。

```
network interface create -vserver <svm-name> -lif <lif-name>  
-role data -data-protocol cifs,nfs -address <nfs-cifs-ip-address>  
-netmask-length <length> -home-node <name-of-node1> -status-admin  
up -failover-policy system-defined -firewall-policy data -home  
-port e0a -auto-revert true -failover-group Default -probe-port  
<port-number-for-azure-health-probe1>
```

b. 使用以下命令在节点2上创建NAS LIF。

```
network interface create -vserver <svm-name> -lif <lif-name>  
-role data -data-protocol cifs,nfs -address <nfs-cifs-ip-address>  
-netmask-length <length> -home-node <name-of-node2> -status-admin  
up -failover-policy system-defined -firewall-policy data -home  
-port e0a -auto-revert true -failover-group Default -probe-port  
<port-number-for-azure-health-probe2>
```

3. 创建iSCSI LIF以提供DNS通信:

a. 使用以下命令在节点 1 上创建 iSCSI LIF 。

```
network interface create -vserver <svm-name> -home-port e0a  
-address <iscsi-ip-address> -netmask-length <# of mask bits> -lif  
<lif-name> -home-node <name-of-node1> -data-protocol iscsi
```

b. 使用以下命令在节点2上创建iSCSI LIF。

```
network interface create -vserver <svm-name> -home-port e0a
-address <iscsi-ip-address> -netmask-length <# of mask bits> -lif
<lif-name> -home-node <name-of-node2> -data-protocol iscsi
```

4. 可选：在节点 1 上创建 Storage VM 管理 LIF 。

```
network interface create -vserver <svm-name> -lif <lif-name> -role
data -data-protocol none -address <svm-mgmt-ip-address> -netmask
-length <length> -home-node <name-of-node1> -status-admin up
-failover-policy system-defined -firewall-policy mgmt -home-port e0a
-auto-revert false -failover-group Default -probe-port <port-number-
for-azure-health-probe3>
```

此管理 LIF 可连接到 SnapCenter 等管理工具。

5. 可选：在节点 1 上创建 Storage VM 管理 LIF 。

```
network interface create -vserver <svm-name> -lif <lif-name> -role
data -data-protocol none -address <svm-mgmt-ip-address> -netmask
-length <length> -home-node <name-of-node1> -status-admin up
-failover-policy system-defined -firewall-policy mgmt -home-port e0a
-auto-revert false -failover-group Default -probe-port <port-number-
for-azure-health-probe3>
```

此管理 LIF 可连接到 SnapCenter 等管理工具。

6. 将一个或多个聚合分配给 Storage VM 。

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

之所以需要执行此步骤，是因为新的 Storage VM 需要至少访问一个聚合，然后才能在 Storage VM 上创建卷。

7. 如果您运行的是 Cloud Volumes ONTAP 9.11.1 或更高版本，请修改此 Storage VM 的网络服务策略。

- a. 输入以下命令以访问高级模式。

```
::> set adv -con off
```

需要修改服务，因为它可以确保 Cloud Volumes ONTAP 可以使用 iSCSI LIF 进行出站管理连接。


```

network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service data-fpolicy-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ad-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-dns-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ldap-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-nis-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-ad-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-dns-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-ldap-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-nis-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-ad-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-dns-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-ldap-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-nis-client

```

SMB

按照以下步骤创建新的 Storage VM 以及所需的 LIF 。

步骤

1. 创建 Storage VM 和指向 Storage VM 的路由。

```

vserver create -vserver <svm-name> -subtype default -rootvolume
<root-volume-name> -rootvolume-security-style unix

```

```

network route create -destination 0.0.0.0/0 -vserver <svm-name>
-gateway <ip-of-gateway-server>

```

2. 创建 NAS 数据 LIF :

- a. 使用以下命令在节点 1 上创建 NAS LIF 。

```
network interface create -vserver <svm-name> -lif <lif-name>
-role data -data-protocol cifs,nfs -address <nfs-cifs-ip-address>
-netmask-length <length> -home-node <name-of-node1> -status-admin
up -failover-policy system-defined -firewall-policy data -home
-port e0a -auto-revert true -failover-group Default -probe-port
<port-number-for-azure-health-probe1>
```

- b. 使用以下命令在节点2上创建NAS LIF。

```
network interface create -vserver <svm-name> -lif <lif-name>
-role data -data-protocol cifs,nfs -address <nfs-cifs-ip-address>
-netmask-length <length> -home-node <name-of-node2> -status-admin
up -failover-policy system-defined -firewall-policy data -home
-port e0a -auto-revert true -failover-group Default -probe-port
<port-number-for-azure-health-probe2>
```

3. 创建iSCSI LIF以提供DNS通信:

- a. 使用以下命令在节点 1 上创建 iSCSI LIF 。

```
network interface create -vserver <svm-name> -home-port e0a
-address <iscsi-ip-address> -netmask-length <# of mask bits> -lif
<lif-name> -home-node <name-of-node1> -data-protocol iscsi
```

- b. 使用以下命令在节点2上创建iSCSI LIF。

```
network interface create -vserver <svm-name> -home-port e0a
-address <iscsi-ip-address> -netmask-length <# of mask bits> -lif
<lif-name> -home-node <name-of-node2> -data-protocol iscsi
```

4. 可选: 在节点 1 上创建 Storage VM 管理 LIF 。

```
network interface create -vserver <svm-name> -lif <lif-name> -role
data -data-protocol none -address <svm-mgmt-ip-address> -netmask
-length <length> -home-node <name-of-node1> -status-admin up
-failover-policy system-defined -firewall-policy mgmt -home-port e0a
-auto-revert false -failover-group Default -probe-port <port-number-
for-azure-health-probe3>
```

此管理 LIF 可连接到 SnapCenter 等管理工具。

5. 将一个或多个聚合分配给 Storage VM 。

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

之所以需要执行此步骤，是因为新的 Storage VM 需要至少访问一个聚合，然后才能在 Storage VM 上创建卷。

6. 如果您运行的是 Cloud Volumes ONTAP 9.11.1 或更高版本、请修改此 Storage VM 的网络服务策略。
 - a. 输入以下命令以访问高级模式。

```
::> set adv -con off
```

需要修改服务、因为它可以确保 Cloud Volumes ONTAP 可以使用 iSCSI LIF 进行出站管理连接。

```

network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service data-fpolicy-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ad-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-dns-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ldap-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-nis-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-ad-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-dns-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-ldap-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-nis-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-ad-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-dns-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-ldap-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-nis-client

```

下一步是什么？

在 HA 对上创建 Storage VM 后，最好等待 12 小时，然后再在该 SVM 上配置存储。从 Cloud Volumes ONTAP 9.10.1 版开始，BlueXP 会每 12 小时扫描一次 HA 对的负载均衡器设置。如果存在新的 SVM，则 BlueXP 将启用一个设置，以缩短计划外故障转移时间。

在 Google Cloud 中为 Cloud Volumes ONTAP 创建数据服务 Storage VM

Storage VM 是在 ONTAP 中运行的虚拟机，可为客户端提供存储和数据服务。您可能会将其识别为 *svm* 或 *vserver*。默认情况下，Cloud Volumes ONTAP 配置有一个 Storage VM，但某些配置支持额外的 Storage VM。

支持的 **Storage VM** 数量

从9.11.1版开始、Google Cloud中的特定Cloud Volumes ONTAP 配置支持多个Storage VM。转至 "[《 Cloud Volumes ONTAP 发行说明》](#)" 验证您的 Cloud Volumes ONTAP 版本支持的 Storage VM 数量。

所有其他 Cloud Volumes ONTAP 配置均支持一个提供数据的 Storage VM 和一个用于灾难恢复的目标 Storage VM。如果源 Storage VM 发生中断，您可以激活目标 Storage VM 以进行数据访问。

创建**Storage VM**

如果许可证支持、您可以在单节点系统或HA对上创建多个Storage VM。请注意、您必须使用BlueXP API在HA对上创建Storage VM、而可以使用CLI或System Manager在单节点系统上创建Storage VM。

单节点系统

以下步骤将使用命令行界面在单节点系统上创建新的Storage VM。创建数据LIF需要一个专用IP地址、如果要创建管理LIF、则需要另一个可选专用IP地址。

步骤

1. 在Google Cloud中、转至Cloud Volumes ONTAP 实例并为每个LIF添加一个IP地址到nic0。

Edit network interface

Network *
default

Subnetwork *
default IPv4 (10.138.0.0/20)

i To use IPv6, you need an IPv6 subnet range. [LEARN MORE](#)

IP stack type

IPv4 (single-stack)

IPv4 and IPv6 (dual-stack)

Primary internal IP
gpcvo-vm-ip-nic0-nodemgmt (10.138.0.46)

Alias IP ranges

Subnet range 1 Primary (10.138.0.0/20)	Alias IP range 1 * 10.138.0.25/32
Subnet range 2 Primary (10.138.0.0/20)	Alias IP range 2 * 10.138.0.23/32
Subnet range 3 Primary (10.138.0.0/20)	Alias IP range 3 * 10.138.0.21/32
Subnet range 4 Primary (10.138.0.0/20)	Alias IP range 4 * 10.138.0.31/32

+ ADD IP RANGE

External IPv4 address
None

如果要在Storage VM上创建管理LIF、则需要一个数据LIF的IP地址和另一个可选IP地址。

"[Google Cloud文档：向现有实例添加别名IP范围](#)"

2. 创建 Storage VM 和指向 Storage VM 的路由。

```
vserver create -vserver <svm-name> -subtype default -rootvolume <root-volume-name> -rootvolume-security-style unix
```

```
network route create -destination 0.0.0.0/0 -vserver <svm-name> -gateway <ip-of-gateway-server>
```

3. 通过指定在Google Cloud中添加的IP地址来创建数据LIF。

iSCSI

```
network interface create -vserver <svm-name> -home-port e0a -address <iscsi-ip-address> -lif <lif-name> -home-node <name-of-node1> -data -protocol iscsi
```

NFS 或 SMB

```
network interface create -vserver <svm-name> -lif <lif-name> -role data -data-protocol cifs,nfs -address <nfs-ip-address> -netmask -length <length> -home-node <name-of-node1> -status-admin up -failover-policy disabled -firewall-policy data -home-port e0a -auto -revert true -failover-group Default
```

4. 可选：通过指定在Google Cloud中添加的IP地址来创建Storage VM管理LIF。

```
network interface create -vserver <svm-name> -lif <lif-name> -role data -data-protocol none -address <svm-mgmt-ip-address> -netmask-length <length> -home-node <name-of-node1> -status-admin up -failover-policy system-defined -firewall-policy mgmt -home-port e0a -auto-revert false -failover-group Default
```

5. 将一个或多个聚合分配给 Storage VM。

```
vserver add-aggregates -vserver <svm-name> -aggregates <aggr1,aggr2>
```

之所以需要执行此步骤，是因为新的 Storage VM 需要至少访问一个聚合，然后才能在 Storage VM 上创建卷。

HA对

您必须使用BlueXP API在Google Cloud中的Cloud Volumes ONTAP 系统上创建Storage VM。需要使用API (而不是System Manager或CLI)、因为BlueXP会为Storage VM配置所需的LIF服务以及出站SMB/CIFS通信所需的iSCSI LIF。

请注意、BlueXP会在Google Cloud中分配所需的IP地址、并创建具有用于SMB/NFS访问的数据LIF和用于出站SMB通信的iSCSI LIF的Storage VM。

所需的Google Cloud权限

连接器需要特定的权限来创建和管理Cloud Volumes ONTAP HA对的Storage VM。所需权限包括在中 ["NetApp提供的策略"](#)。

步骤

1. 使用以下API调用创建Storage VM:

```
POST /occm/api/gcp/ha/working-environments/{WE_ID}/svm/
```

请求正文应包括以下内容:

```
{ "svmName": "myNewSvm1" }
```

管理HA对上的Storage VM

此外、BlueXP API还支持重命名和删除HA对上的Storage VM。

重命名Storage VM

如果需要、您可以随时更改Storage VM的名称。

步骤

1. 使用以下API调用重命名Storage VM:

```
PUT /occm/api/gcp/ha/working-environments/{WE_ID}/svm
```

请求正文应包括以下内容:

```
{  
  "svmNewName": "newSvmName",  
  "svmName": "oldSvmName"  
}
```

删除Storage VM

如果您不再需要Storage VM、可以将其从Cloud Volumes ONTAP 中删除。

步骤

1. 使用以下API调用删除Storage VM:

```
DELETE /occm/api/gcp/ha/working-environments/{WE_ID}/svm/{SVM_NAME}
```

设置SVM灾难恢复

BlueXP不为Storage VM (SVM)灾难恢复提供任何设置或流程编排支持。您必须使用 System Manager 或 CLI 。

如果在两个Cloud Volumes ONTAP系统之间设置SnapMirror SVM复制、则复制必须在两个HA对系统或两个单节点系统之间进行。您不能在HA对和单节点系统之间设置SnapMirror SVM复制。

有关CLI说明、请参阅以下文档。

- "《SVM 灾难恢复准备快速指南》"
- "《SVM 灾难恢复快速指南》"

安全性和数据加密

使用 NetApp 加密解决方案对卷进行加密

Cloud Volumes ONTAP 支持 NetApp 卷加密（NVE）和 NetApp 聚合加密（NAE）。NVE和NAE是基于软件的解决方案、支持FIPS 140-2合规的卷空闲数据加密。"[详细了解这些加密解决方案](#)"。

外部密钥管理器支持 NVE 和 NAE 。

使用AWS密钥管理服务管理密钥

您可以使用 "[AWS的密钥管理服务\(KMS\)](#)" 在部署了Google Cloud Platform的应用程序中保护ONTAP 加密密钥。

可以使用命令行界面或ONTAP REST API启用AWS KMS的密钥管理。

使用KMS时、请注意、默认情况下、数据SVM的LIF用于与云密钥管理端点进行通信。节点管理网络用于与AWS的身份验证服务进行通信。如果集群网络配置不正确，集群将无法正确利用密钥管理服务。

开始之前

- Cloud Volumes ONTAP必须运行9.12.0或更高版本
- 您必须已安装卷加密(VE)许可证和
- 您必须已安装多租户加密密钥管理(MTEKM)许可证。
- 您必须是集群管理员或SVM管理员
- 您必须拥有有效的AWS订阅



您只能为数据SVM配置密钥。

Configuration

AWS

1. 您必须创建 "[授予](#)" 用于管理加密的IAM角色要使用的AWS KMS密钥。IAM角色必须包含一个允许执行以下操作的策略：
 - DescribeKey
 - Encrypt
 - Decrypt要创建授予、请参见 "[AWS文档](#)"。
2. "[将策略添加到相应的IAM角色](#)。" 此策略应支持 DescribeKey, Encrypt, 和 Decrypt 操作。

Cloud Volumes ONTAP

1. 切换到Cloud Volumes ONTAP环境。
2. 切换到高级权限级别：
`set -privilege advanced`
3. 启用AWS密钥管理器：
`security key-manager external aws enable -vserver data_svm_name -region AWS_region -key-id key_ID -encryption-context encryption_context`
4. 出现提示时、输入机密密钥。
5. 确认已正确配置AWS KMS：
`security key-manager external aws show -vserver svm_name`

使用Azure密钥存储管理密钥

您可以使用 "Azure 密钥存储 (AKV)" 保护Azure部署应用程序中的ONTAP 加密密钥。

可使用AKV进行保护 "NetApp 卷加密 (NVE) 密钥" 仅适用于数据SVM。

可以使用命令行界面或ONTAP REST API启用使用AKV的密钥管理。

使用AKV时、请注意、默认情况下、数据SVM LIF用于与云密钥管理端点进行通信。节点管理网络用于与云提供商的身份验证服务(login.microsoftonline.com)进行通信。如果集群网络配置不正确，集群将无法正确利用密钥管理服务。

开始之前

- Cloud Volumes ONTAP 必须运行9.10.1或更高版本
- 已安装卷加密(VE)许可证(已向NetApp支持部门注册的每个Cloud Volumes ONTAP 系统会自动安装NetApp 卷加密许可证)
- 您必须具有多租户加密密钥管理(MT_EK_Mgmt)许可证
- 您必须是集群管理员或SVM管理员
- Active Azure订阅

限制

- 只能在数据SVM上配置AKV

配置过程

概述的步骤将介绍如何向Azure注册Cloud Volumes ONTAP 配置以及如何创建Azure密钥存储和密钥。如果您已完成这些步骤、请确保配置设置正确、尤其是在中 [创建Azure密钥存储](#)、然后继续 [Cloud Volumes ONTAP 配置](#)。

- [Azure应用程序注册](#)
- [创建Azure客户端密钥](#)
- [创建Azure密钥存储](#)
- [创建加密密钥](#)
- [创建Azure Active Directory端点\(仅限HA\)](#)

- [Cloud Volumes ONTAP 配置](#)

Azure应用程序注册

1. 您必须先希望在希望Cloud Volumes ONTAP 用于访问Azure密钥存储的Azure订阅中注册应用程序。在Azure门户中、选择"**应用注册**"。
2. 选择"**新建注册**"。
3. 请为您的应用程序提供一个名称、然后选择支持的应用程序类型。默认的单个租户足以使用Azure密钥存储。选择"**注册**"。
4. 在Azure概述窗口中、选择已注册的应用程序。将"**应用程序(客户端) ID**"和"**目录(租户) ID**"复制到安全位置。注册过程稍后将需要这些许可证。

创建Azure客户端密钥

1. 在Azure密钥存储应用注册的Azure门户中、选择"**证书和密钥**"窗格。
2. 选择"**新建客户端密钥**"。为您的客户端密钥输入一个有意义的名称。NetApp建议使用24个月的到期期限；但是、您的特定云监管策略可能需要其他设置。
3. 单击"**添加**"以创建客户端密钥。复制"**value**"列中列出的机密字符串、并将其存储在安全位置、以供稍后在中使用 [Cloud Volumes ONTAP 配置](#)。离开页面后、不会再显示此机密值。

创建Azure密钥存储

1. 如果您已有Azure密钥存储、则可以将其连接到Cloud Volumes ONTAP 配置；但是、您必须根据此过程中的设置调整访问策略。
2. 在Azure门户中、导航到"**密钥存储**"部分。
3. 单击"**+Create**"(创建)、然后输入所需信息、包括资源组、区域和定价层。此外、输入保留已删除存储的天数、然后在密钥存储上选择"**启用清除保护**"。
4. 选择"**下一步**"以选择访问策略。
5. 选择以下选项：
 - a. 在"**访问配置**"下、选择"**存储访问策略**"。
 - b. 在"**资源访问权限**"下、选择"**用于卷加密的Azure磁盘加密**"。
6. 选择"**+Create**"以添加访问策略。
7. 在"**从模板配置**"下、单击下拉菜单、然后选择"**密钥**"、"**机密**"和"**证书管理**"模板。
8. 选择每个下拉权限菜单(密钥、密钥、证书)、然后选择菜单列表顶部的"**全选**"以选择所有可用权限。您应具备：
 - 密钥权限：已选择20个
 - "**机密权限**"：已选择8个
 - "**证书权限**"：已选择16个

Create an access policy



- 1 **Permissions** 2 Principal 3 Application (optional) 4 Review + create

Configure from a template

Key, Secret, & Certificate Management ▼

Key permissions

Key Management Operations

- Select all
- Get
- List
- Update
- Create
- Import
- Delete
- Recover
- Backup
- Restore

Cryptographic Operations

- Select all
- Decrypt
- Encrypt
- Unwrap Key
- Wrap Key
- Verify
- Sign

Privileged Key Operations

- Select all
- Purge
- Release

Rotation Policy Operations

- Select all
- Rotate
- Get Rotation Policy
- Set Rotation Policy

Secret permissions

Secret Management Operations

- Select all
- Get
- List
- Set
- Delete
- Recover
- Backup
- Restore

Privileged Secret Operations

- Select all
- Purge

Certificate permissions

Certificate Management Operations

- Select all
- Get
- List
- Update
- Create
- Import
- Delete
- Recover
- Backup
- Restore
- Manage Contacts
- Manage Certificate Authorities
- Get Certificate Authorities
- List Certificate Authorities
- Set Certificate Authorities
- Delete Certificate Authorities

Privileged Certificate Operations

- Select all
- Purge

Previous

Next

- 单击"下一步"以选择您在中创建的"*主体"*已注册Azure应用程序 [Azure应用程序注册](#)。选择"*下一步"。



每个策略只能分配一个主体。

Create an access policy

Permissions **Principal** Application (optional) Review + create

Only 1 principal can be assigned per access policy.
Use the new embedded experience to select a principal. The previous popup experience can be accessed here. [Select a principal](#)

Selected item

No item selected

Previous **Next**

- 单击两次"下一步"、直到到达"查看并创建"。然后、单击"*创建"。
- 选择"*下一步"*以进入"*网络连接"*选项。
- 选择适当的网络访问方法或选择"*所有网络"*和"*查看+创建"*以创建密钥存储。(网络访问方法可能由监管策略或您的企业云安全团队规定。)
- 记录密钥存储URI：在您创建的密钥存储中、导航到概述菜单并从右侧列复制"*存储URI"。您需要在后续步骤中使用此功能。

创建加密密钥

- 在为Cloud Volumes ONTAP 创建的密钥存储的菜单中、导航到"*密钥"选项。
- 选择"*生成/导入"*以创建新密钥。
- 将默认选项设置为"*生成"。
- 请提供以下信息：
 - 加密密钥名称

- 密钥类型：RSA
- RSA密钥大小：2048
- Enabled：是

5. 选择"**创建**"以创建加密密钥。
6. 返回到"**密钥**"菜单、然后选择刚刚创建的密钥。
7. 在"**当前版本**"下选择密钥ID以查看密钥属性。
8. 找到"**密钥标识符**"字段。将此URI复制到、但不包括十六进制字符串。

创建**Azure Active Directory**端点(仅限**HA**)

1. 只有在为**HA Cloud Volumes ONTAP** 工作环境配置**Azure**密钥存储时、才需要执行此过程。
2. 在**Azure**门户中、导航到"**虚拟网络**"。
3. 选择部署**Cloud Volumes ONTAP** 工作环境的虚拟网络、然后选择页面左侧的"**子网**"菜单。
4. 从列表中选择**Cloud Volumes ONTAP** 部署的子网名称。
5. 导航到"**服务端点**"标题。在下拉菜单中、选择以下内容：
 - "10.microsoft.AzureActiveDirectory"
 - ***microsoft.KeyVaule**
 - "10.microsoft.Storage"*(可选)

SERVICE ENDPOINTS

Create service endpoint policies to allow traffic to specific azure resources from your virtual network over service endpoints. [Learn more](#)

Services ⓘ

3 selected

Service	Status	
Microsoft.Storage	Succeeded	
Microsoft.AzureActiveDirectory	Succeeded	
Microsoft.KeyVault	Succeeded	

Service endpoint policies

0 selected

SUBNET DELEGATION

Delegate subnet to a service ⓘ

None

NETWORK POLICY FOR PRIVATE ENDPOINTS

The network policy affects all private endpoints in this subnet. To use network security groups, application security groups, or user defined routes to control traffic going to a private endpoint, set the private endpoint network policy to enabled. [Learn more](#)

Private endpoint network policy

Disabled

Save

6. 选择“保存”以捕获设置。

Cloud Volumes ONTAP 配置

1. 使用首选SSH客户端连接到集群管理LIF。
2. 在ONTAP 中进入高级权限模式：

```
set advanced -con off
```

3. 确定所需的数据SVM并验证其DNS配置:

```
vserver services name-service dns show
```

- a. 如果所需数据SVM的DNS条目存在、并且其中包含Azure DNS的条目、则无需执行任何操作。如果不支持、请为指向Azure DNS、专用DNS或内部部署服务器的数据SVM添加DNS服务器条目。此名称应与集群管理SVM的条目匹配:

```
vserver services name-service dns create -vserver SVM_name -domains domain  
-name-servers IP_address
```

- b. 验证是否已为数据SVM创建DNS服务:

```
vserver services name-service dns show
```

4. 使用应用程序注册后保存的客户端ID和租户ID启用Azure密钥存储:

```
security key-manager external azure enable -vserver SVM_name -client-id  
Azure_client_ID -tenant-id Azure_tenant_ID -name Azure_key_vault_name -key-id  
Azure_key_ID
```

5. 检查密钥管理器的状态:

```
security key-manager external azure check
```

输出如下所示:

```
::*> security key-manager external azure check  
  
Vserver: data_svm_name  
Node: akvlab01-01  
  
Category: service_reachability  
Status: OK  
  
Category: ekmip_server  
Status: OK  
  
Category: kms_wrapped_key_status  
Status: UNKNOWN  
Details: No volumes created yet for the vserver. Wrapped KEK status  
will be available after creating encrypted volumes.  
  
3 entries were displayed.
```

如果 `service_reachability` 状态不是 `OK`、SVM无法使用所需的所有连接和权限访问Azure密钥存储服务。确保您的Azure网络策略和路由不会阻止您的专用vNet访问Azure KeyVault公共端点。如果有、请考虑使用Azure私有端点从vNet中访问密钥存储。您可能还需要在SVM上添加静态主机条目、以解析端点的专用IP地址。

。 `kms_wrapped_key_status` 将报告 `UNKNOWN` 初始配置时。其状态将更改为 `OK` 对第一个卷进行加密后。

6. 可选: 创建测试卷以验证NVE的功能。


```
vol create -vserver SVM_name -volume volume_name -aggregate aggr -size size
-state online -policy default
```

如果配置正确、Cloud Volumes ONTAP 将自动创建卷并启用卷加密。

7. 确认卷已正确创建和加密。如果是、则 `-is-encrypted` 参数将显示为 `true`。

```
vol show -vserver SVM_name -fields is-encrypted
```

使用Google的云密钥管理服务管理密钥

您可以使用 "[Google Cloud Platform 的密钥管理服务 \(Cloud KMS\)](#)" 在部署了Google Cloud Platform的应用程序中保护ONTAP 加密密钥。

可以使用命令行界面或ONTAP REST API启用Cloud KMS的密钥管理。

使用Cloud KMS时、请注意、默认情况下、数据SVM的LIF用于与云密钥管理端点进行通信。节点管理网络用于与云提供商的身份验证服务([oauth2.googleapis.com](#))进行通信。如果集群网络配置不正确，集群将无法正确利用密钥管理服务。

开始之前

- Cloud Volumes ONTAP 必须运行9.10.1或更高版本
- 已安装卷加密 (VE) 许可证
- 安装了多租户加密密钥管理(MTEKM)许可证、从Cloud Volumes ONTAP 9.12.1 GA开始。
- 您必须是集群管理员或SVM管理员
- 有效的Google Cloud Platform订阅

限制

- 只能在数据SVM上配置Cloud KMS

Configuration

Google Cloud

1. 在Google Cloud环境中、"[创建对称GCP密钥环和密钥](#)"。
2. 为Cloud Volumes ONTAP 服务帐户创建自定义角色。

```
gcloud iam roles create kmsCustomRole
  --project=<project_id>
  --title=<kms_custom_role_name>
  --description=<custom_role_description>

  --permissions=cloudkms.cryptoKeyVersions.get,cloudkms.cryptoKeyVersions.
list,cloudkms.cryptoKeyVersions.useToDecrypt,cloudkms.cryptoKeyVersions.
useToEncrypt,cloudkms.cryptoKeys.get,cloudkms.keyRings.get,cloudkms.loca
tions.get,cloudkms.locations.list,resourceManager.projects.get
  --stage=GA
```

3. 将自定义角色分配给云KMS密钥和Cloud Volumes ONTAP服务帐户：

```
gcloud kms keys add-iam-policy-binding key_name --keyring key_ring_name
--location key_location --member serviceAccount:_service_account_Name_ --role
projects/customer_project_id/roles/kmsCustomRole
```

4. 下载服务帐户JSON密钥：

```
gcloud iam service-accounts keys create key-file --iam-account=sa-name
@project-id.iam.gserviceaccount.com
```

Cloud Volumes ONTAP

1. 使用首选SSH客户端连接到集群管理LIF。

2. 切换到高级权限级别：

```
set -privilege advanced
```

3. 为数据SVM创建DNS。

```
dns create -domains c.<project>.internal -name-servers server_address -vserver
SVM_name
```

4. 创建CMDK条目：

```
security key-manager external gcp enable -vserver SVM_name -project-id project
-key-ring-name key_ring_name -key-ring-location key_ring_location -key-name
key_name
```

5. 出现提示时、输入GCP帐户中的服务帐户JSON密钥。

6. 确认已启用的进程成功：

```
security key-manager external gcp check -vserver svm_name
```

7. 可选：创建卷以测试加密 `vol create volume_name -aggregate aggregate -vserver vserver_name -size 10G`

故障排除

如果您需要进行故障排除、可以在上述最后两个步骤中结束原始REST API日志：

1. `set d`
2. `systemshell -node node -command tail -f /mroot/etc/log/mlog/kmip2_client.log`

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。借助BlueXP、您可以实施两种NetApp勒索软件解决方案：防范常见勒索软件文件扩展名和自动勒索软件保护(ARP)。这些解决方案为可见性、检测和补救提供了有效的工具。

防止常见勒索软件文件扩展名

通过BlueXP、勒索软件保护设置允许您利用ONTAP FPolicy功能防范常见的勒索软件文件扩展名类型。

步骤

1. 在"画布"页面上、双击您配置为勒索软件保护的系统的名称。
2. 在概述选项卡上、单击功能面板、然后单击*勒索软件保护*旁边的铅笔图标。

Information		Features
Working Environment Tags		Tags 
Scheduled Downtime		Off 
S3 Storage Classes	Standard-Infrequent Access	
Instance Type	m5.xlarge	
Write Speed		Normal 
Ransomware Protection		Off 
Support Registration	Not Registered	
CIFs Setup		

3. 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。

默认 FPolicy 范围会阻止具有以下扩展名的文件：

微型，加密，锁定，加密，加密 crinf，r5a，rxNT，XTbl，R16M01D05，pzdc，好，LOL！，OMG！，RDM，RRK，encryptedRS，crjoker，EnciPhErEd，LeChiffre



当您在Cloud Volumes ONTAP 上激活FPolicy时、BlueXP会创建此范围。此列表基于常见的勒索软件文件类型。您可以使用 Cloud Volumes ONTAP 命令行界面中的 `vserver fpolicy policy scopes` 命令来自定义阻止的文件扩展名。

自主勒索软件保护

Cloud Volumes ONTAP支持自动勒索软件保护(ARP)功能、此功能可对工作负载执行分析、以主动检测可能指示勒索软件攻击的异常活动并发出警告。

与通过提供的文件扩展名保护分开 "勒索软件保护设置", ARP功能使用工作负载分析根据检测到的“异常活动”向用户发出潜在攻击警报。勒索软件保护设置和ARP功能均可结合使用来实现全面的勒索软件保护。

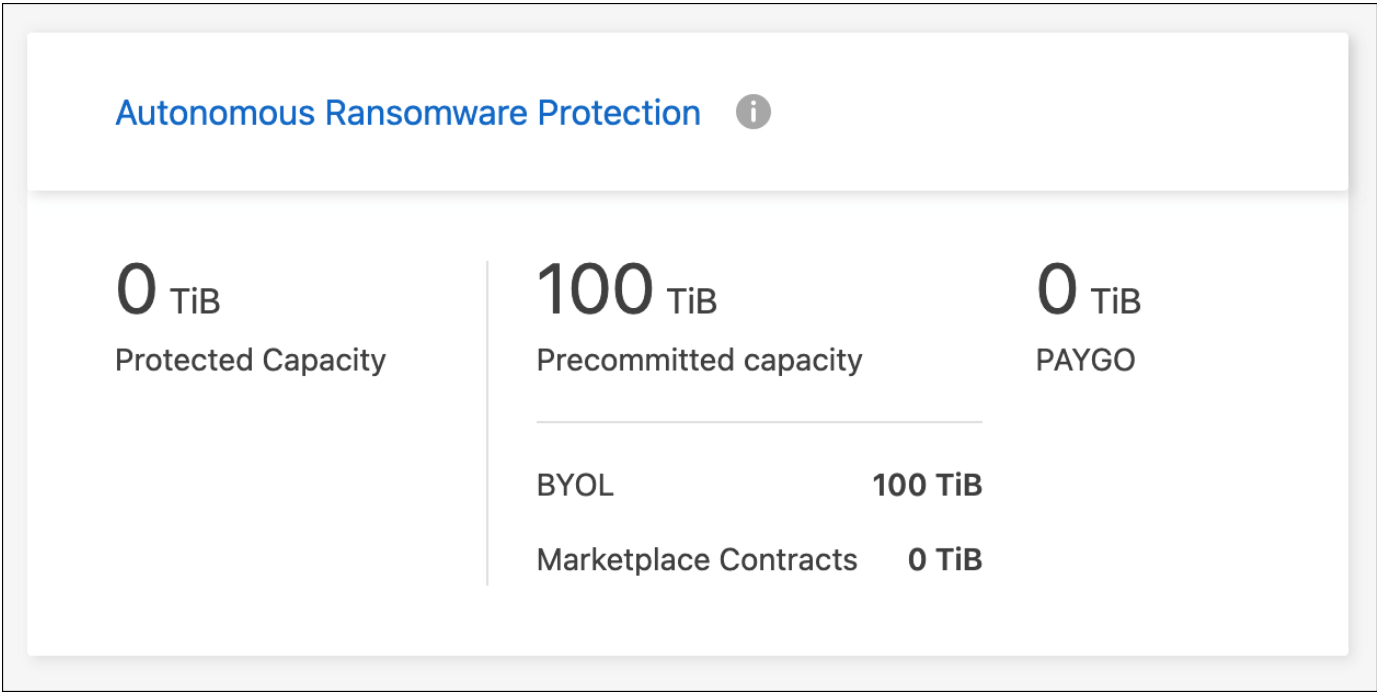
无论是基于节点的许可模式还是基于容量的许可模式、ARP功能都只能与BYOL许可证一起使用(一年期、两年期和三年期)。要购买新的单独附加许可证、以便与Cloud Volumes ONTAP中的ARP功能结合使用、您必须与NetApp销售代表联系。

购买附加许可证并将其添加到电子钱包后、您可以在Cloud Volumes ONTAP中按卷启用ARP。可通过ONTAP系统管理器和ONTAP命令行界面为卷配置ARP。

有关如何使用ONTAP系统管理器和命令行界面启用ARP的详细信息、请参见 "启用自主勒索软件保护"。



如果没有许可证、则不支持使用已获得许可的功能。



系统管理

升级 **Cloud Volumes ONTAP** 软件

从BlueXP升级Cloud Volumes ONTAP 以访问最新的新功能和增强功能。在升级软件之前，您应准备好 Cloud Volumes ONTAP 系统。

升级概述

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

仅从BlueXP升级

必须从BlueXP完成Cloud Volumes ONTAP 升级。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。

如何升级

BlueXP提供了两种升级Cloud Volumes ONTAP 的方法：

- 在工作环境中显示以下升级通知
- 将升级映像放置在HTTPS位置、然后为BlueXP提供URL

支持的升级路径

您可以升级到的 Cloud Volumes ONTAP 版本取决于您当前运行的 Cloud Volumes ONTAP 版本。

当前版本	您可以直接升级到的版本
9.13.0	9.13.1.

当前版本	您可以直接升级到的版本
9.12.1.	9.13.1.
	9.13.0
9.12.2.	9.12.1.
9.11.1.	9.12.1.
	9.12.2.
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

请注意以下事项：

- Cloud Volumes ONTAP 支持的升级路径与内部 ONTAP 集群不同。
- 如果按照工作环境中显示的升级通知进行升级、则BlueXP将提示您升级到遵循这些受支持升级路径的版本。
- 如果通过将升级映像放置在 HTTPS 位置进行升级，请务必遵循以下受支持的升级路径。
- 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，如果您运行的是 9.8 版，并且要升级到 9.10.1 ，则首先需要升级到 9.9.1 版，然后再升级到 9.10.1 版。

- 对于修补程序(P)版本、您可以从一个版本升级到下一个版本的任何P版本。

下面是几个示例：

- 9.13.0 > 9.13.1P15

◦ 9.12.1 > 9.13.1P2

还原或降级

不支持将 Cloud Volumes ONTAP 还原或降级到先前版本。

支持注册

要使用此页面所述的任何方法升级软件，必须向 NetApp 支持部门注册 Cloud Volumes ONTAP。此适用场景既适用于 PAYGO，也适用于 BYOL。您需要 ["手动注册 PAYGO 系统"](#)，而 BYOL 系统默认已注册。



未注册支持的系统仍会收到新版本可用时在BlueXP中显示的软件更新通知。但是，您需要先注册系统，然后才能升级软件。

升级 HA 调解器

在Cloud Volumes ONTAP 升级过程中、BlueXP还会根据需要更新调解器实例。

准备升级

在执行升级之前，您必须验证系统是否已准备就绪，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。

在许多情况下、升级HA对不会造成中断、并且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。

在升级期间、面向会话的协议可能会对某些方面的客户端和应用程序产生发生原因不利影响。有关详细信息、"[请参阅ONTAP文档](#)"

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。



即使BlueXP备份和恢复使用SnapMirror的实施来创建备份文件(称为SnapMirror Cloud)、在升级系统时也不需要暂停备份。

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. 从目标系统登录到 System Manager 。

您可以通过将 Web 浏览器指向集群管理 LIF 的 IP 地址来登录到 System Manager 。您可以在 Cloud Volumes ONTAP 工作环境中找到 IP 地址。



要访问BlueXP的计算机必须与Cloud Volumes ONTAP 建立网络连接。例如、您可能需要从云提供商网络中的跳转主机登录到BlueXP。

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*聚合*选项卡。
2. 在聚合标题下、单击椭圆按钮、然后选择*查看聚合详细信息*。

Aggregate Details	
aggr1	
Overview	Capacity Allocation
Provider Properties	
State	online
Home Node	10.10.10.10
Encryption Type	cloudEncrypted
Volumes	2

3. 如果聚合处于脱机状态，请使用 System Manager 使聚合联机：
 - 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 > 联机 * 。

升级 Cloud Volumes ONTAP

当有新版本可供升级时、BlueXP会向您发出通知。您可以从此通知启动升级过程。有关详细信息，请参见 [从BlueXP通知升级](#)。

使用外部 URL 上的映像执行软件升级的另一种方式。如果BlueXP无法访问S3存储分段来升级软件或为您提供了解决程序、则此选项很有用。有关详细信息，请参见 [从 URL 上提供的映像升级](#)。

从BlueXP通知升级

当有新版本的Cloud Volumes ONTAP 可用时、BlueXP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。

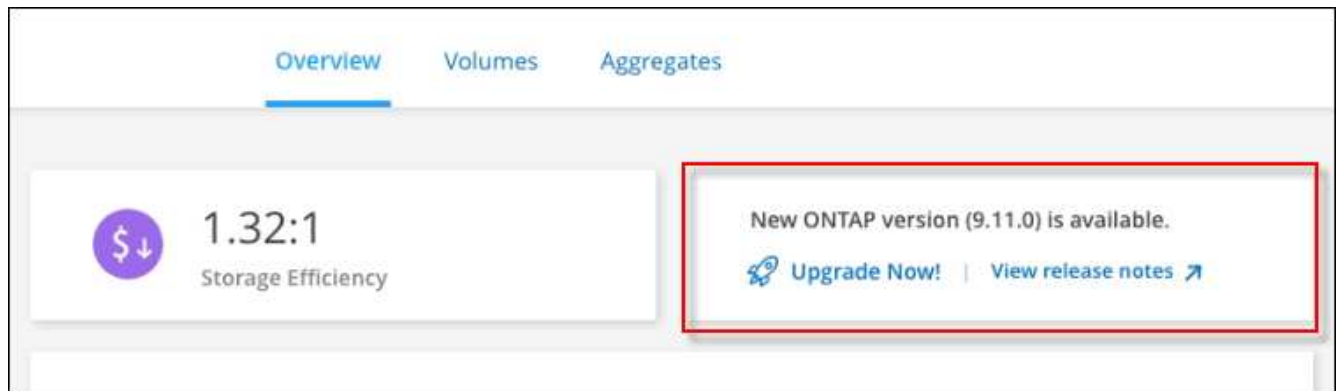
开始之前

Cloud Volumes ONTAP 系统上不得执行诸如卷或聚合创建等BlueXP操作。

步骤

1. 从左侧导航菜单中、选择*存储>画布*。
2. 选择工作环境。

如果有新版本可用、“概述”选项卡将显示一条通知：



3. 如果有新版本、请单击*立即升级！*



在通过BlueXP通知升级Cloud Volumes ONTAP之前、您必须具有NetApp 支持站点 帐户。

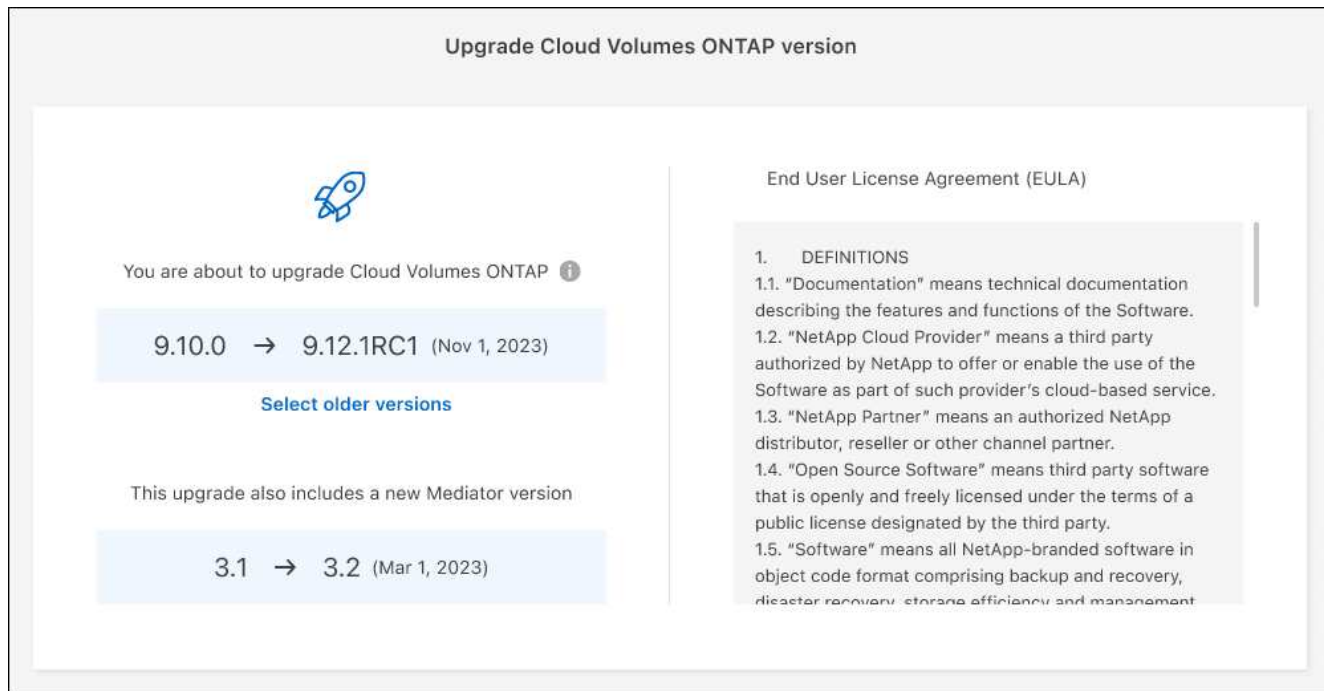
4. 在Upgrade Cloud Volumes ONTAP 页面中、阅读EULA、然后选择*我阅读并批准EULA*。

5. 单击 * 升级 *。



默认情况下、Upgrade Cloud Volumes ONTAP页面会选择要升级的最新可用Cloud Volumes ONTAP版本。如果可用，可以通过单击*选择旧版本*来选择旧版本的Cloud Volumes ONTAP进行升级。

请参见 ["支持的升级路径列表"](#) 根据您当前的Cloud Volumes ONTAP版本选择相应的升级路径。



6. 要检查升级状态，请单击设置图标并选择*Timeline*。

结果

BlueXP开始软件升级。软件更新完成后、您可以对工作环境执行操作。

完成后

如果暂停了 SnapMirror 传输、请使用 System Manager 恢复传输。

从 URL 上提供的映像升级

您可以将Cloud Volumes ONTAP 软件映像放置在连接器或HTTP服务器上、然后从BlueXP启动软件升级。如果BlueXP无法访问S3存储分段来升级软件、您可以使用此选项。

开始之前

- Cloud Volumes ONTAP 系统上不得执行诸如卷或聚合创建等BlueXP操作。
- 如果使用HTTPS托管ONTAP 映像、则升级可能会因缺少证书而导致SSL身份验证问题失败。临时解决策 将生成并安装一个CA签名证书、用于在ONTAP 和BlueXP之间进行身份验证。

请访问NetApp知识库以查看分步说明：

["NetApp知识库：如何将BlueXP配置为HTTPS服务器以托管升级映像"](#)

步骤

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

如果与虚拟网络建立了 VPN 连接，则可以将 Cloud Volumes ONTAP 软件映像放置在自己网络中的 HTTP 服务器上。否则，您必须将文件放置在云中的 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。



默认情况下，预定义的 Cloud Volumes ONTAP 安全组允许出站 HTTP 连接。

3. 从获取软件映像 "[NetApp 支持站点](#)"。
4. 将软件映像复制到 Connector 或 HTTP 服务器上要从中提供文件的目录中。

有两个可用路径。正确的路径取决于您的 Connector 版本。

- /opt/application/netapp/cloudmanager/docker_occm/data/ontap/images/
- /opt/application/netapp/cloudmanager/ontap/images/

5. 在 BlueXP 的工作环境中、单击*。(椭圆图标)*，然后单击*更新 Cloud Volumes ONTAP*。
6. 在“更新 Cloud Volumes ONTAP 版本”页上，输入 URL，然后单击*Change Image*。

如果您已将软件映像复制到上述路径中的 Connector，则应输入以下 URL：

\http: <Connector-private-IP-address><image-file-name>



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

BlueXP 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。

修复使用 Google Cloud NAT 网关时的下载失败问题

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

步骤

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

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

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

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

["了解有关 /ocem/config API 调用的更多信息"](#)。

注册按需购买的系统

Cloud Volumes ONTAP PAYGO 系统附带 NetApp 提供的支持，但您必须先向 NetApp 注册这些系统以激活支持。

要使用任何方法升级 ONTAP 软件，需要向 NetApp 注册 PAYGO 系统 ["本页介绍"](#)。











未注册支持的系统仍会收到新版本可用时在 BlueXP 中显示的软件更新通知。但是，您需要先注册系统，然后才能升级软件。

步骤

1. 如果您尚未将 NetApp 支持站点帐户添加到 BlueXP，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 "画布" 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。

Information	Features
Working Environment Tags	Tags 
Scheduled Downtime	Off 
S3 Storage Classes	Standard-Infrequent Access 
Instance Type	m5.xlarge 
Write Speed	Normal 
Ransomware Protection	Off 
Support Registration	Not Registered 
CIFs Setup	

4. 选择一个 NetApp 支持站点帐户，然后单击 注册。

结果

BlueXP将系统注册到NetApp。

管理 **Cloud Volumes ONTAP** 的状态

您可以从BlueXP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BlueXP配置为在特定时间自动关闭并重新启动系统、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BlueXP会推迟关闭。









传输完成后、BlueXP将关闭系统。

- 此任务会安排 HA 对中两个节点的自动关闭。
- 通过计划的关闭关闭 Cloud Volumes ONTAP 时，不会创建启动磁盘和根磁盘的快照。

只有在执行手动关闭时，才会自动创建快照，如下一节所述。

步骤

1. 在"画布"页面上、双击所需的工作环境。
2. 在概述选项卡上、单击功能面板、然后单击*计划内停机*旁边的铅笔图标。

Information	Features
Working Environment Tags	Tags 
Scheduled Downtime	Off 
S3 Storage Classes	Standard-Infrequent Access 
Instance Type	m5.xlarge 
Write Speed	Normal 
Ransomware Protection	Off 
Support Registration	Not Registered 
CIFs Setup	

3. 指定关机计划:

- 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。
- 指定关闭系统的时间以及关闭系统的时间。

▪ 示例 *

下图显示了一个计划、指示BlueXP在每个星期六的晚上20:00关闭系统(晚上8:00)、持续12小时。BlueXP会在每周一中午12:00重新启动系统

Schedule Downtime

Cloud Manager Time Zone: 17:58 UTC

Select when to turn off your Working Environment:

Turn off every day at 20 : 00 for 12 hours (1-24)
Sun, Mon, Tue, Wed, Thu, Fri, Sat

Turn off every weekdays at 20 : 00 for 12 hours (1-24)
Mon, Tue, Wed, Thu, Fri

Turn off every weekend at 20 : 00 for 12 hours (1-48)
Sat

4. 单击 * 保存 *。

结果

BlueXP将保存此计划。"功能"面板下的相应计划停机行项显示为"开"。

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。



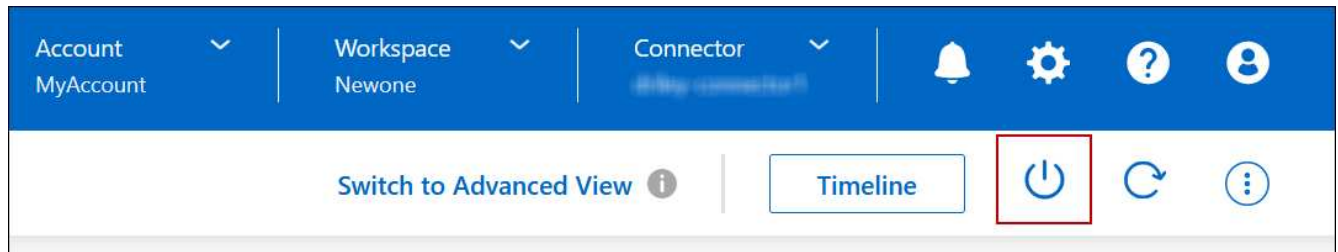
为了降低成本、BlueXP会定期删除根磁盘和启动磁盘的旧快照。对于根磁盘和启动磁盘，只会保留两个最新的快照。

关于此任务

停止HA对时、BlueXP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。



系统会在重新启动时自动创建快照。

使用 NTP 同步系统时间

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。

使用指定 NTP 服务器 "BlueXP API" 或者从用户界面执行此操作 "[创建 CIFS 服务器](#)"。

修改系统写入速度

您可以通过BlueXP为Cloud Volumes ONTAP 选择正常或高写入速度。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。

所有类型的单节点系统和某些HA对配置均支持高写入速度。在中查看支持的配置 "[《 Cloud Volumes ONTAP 发行说明》](#)"









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 系统。这是一个中断过程，需要停机整个系统。

步骤

1. 在"画布"页面上、双击要配置为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。

Information	Features
Working Environment Tags	Tags 
Scheduled Downtime	Off 
S3 Storage Classes	Standard-Infrequent Access 
Instance Type	m5.xlarge 
Write Speed	Normal 
Ransomware Protection	Off 
Support Registration	Not Registered 
CIFs Setup	

3. 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。



从9.13.0版开始、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 的密码

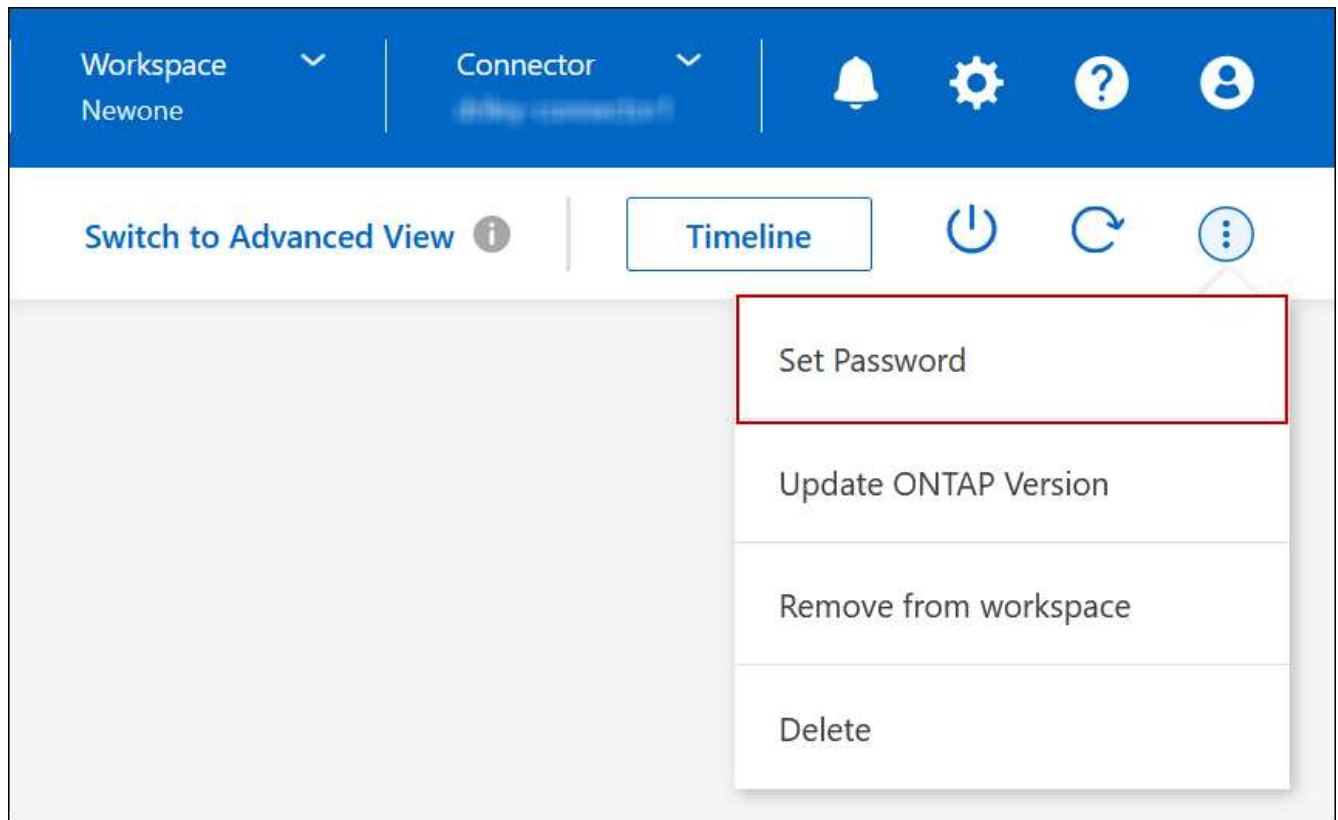
Cloud Volumes ONTAP 包括集群管理员帐户。如果需要、您可以从BlueXP更改此帐户的密码。



不应通过 System Manager 或 CLI 更改管理员帐户的密码。密码不会反映在BlueXP中。因此、BlueXP无法正确监控实例。

步骤

1. 在"画布"页面上、双击Cloud Volumes ONTAP 工作环境的名称。
2. 在BlueXP控制台右上角、单击椭圆图标、然后选择*设置密码*。



新密码必须不同于您使用的最后六个密码之一。

添加，删除或删除系统

将现有Cloud Volumes ONTAP 系统添加到BlueXP

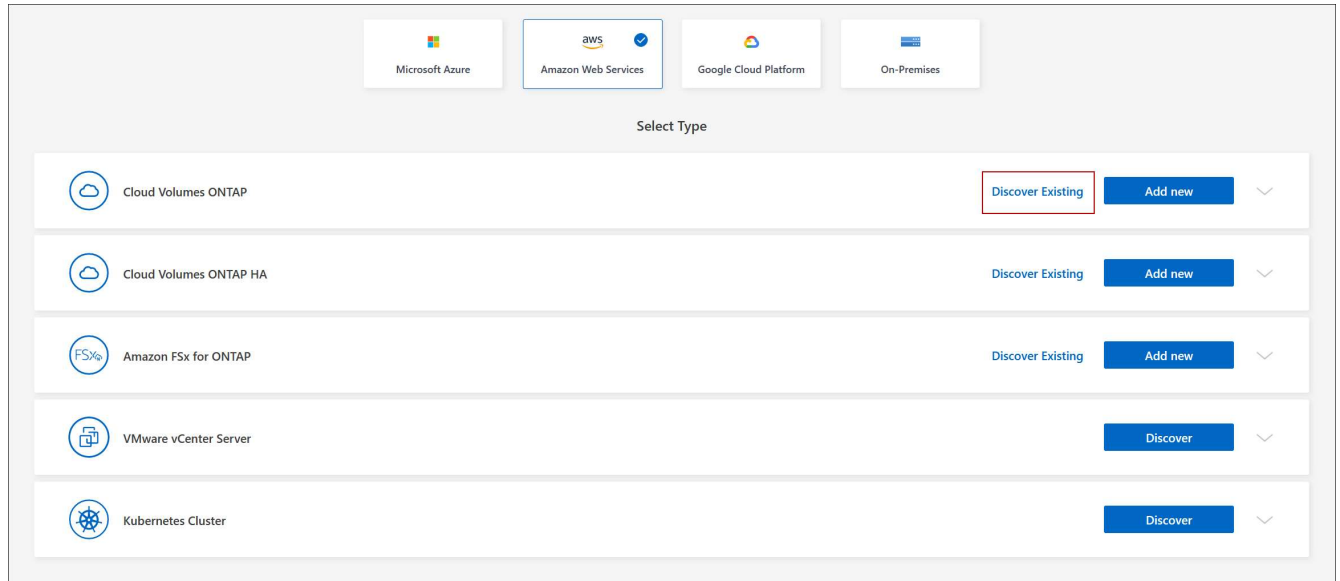
您可以发现现有Cloud Volumes ONTAP 系统并将其添加到BlueXP中。如果您部署了新的BlueXP系统、则可以执行此操作。

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. 从左侧导航菜单中、选择*存储>画布*。
2. 在 "画布" 页面上，单击 * 添加工作环境 * 。
3. 选择系统所在的云提供商。
4. 选择 Cloud Volumes ONTAP 系统的类型。
5. 单击此链接可发现现有系统。



6. 在区域页面上、选择实例运行所在的区域、然后选择实例。
7. 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

BlueXP会将Cloud Volumes ONTAP 实例添加到工作空间中。

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BlueXP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。

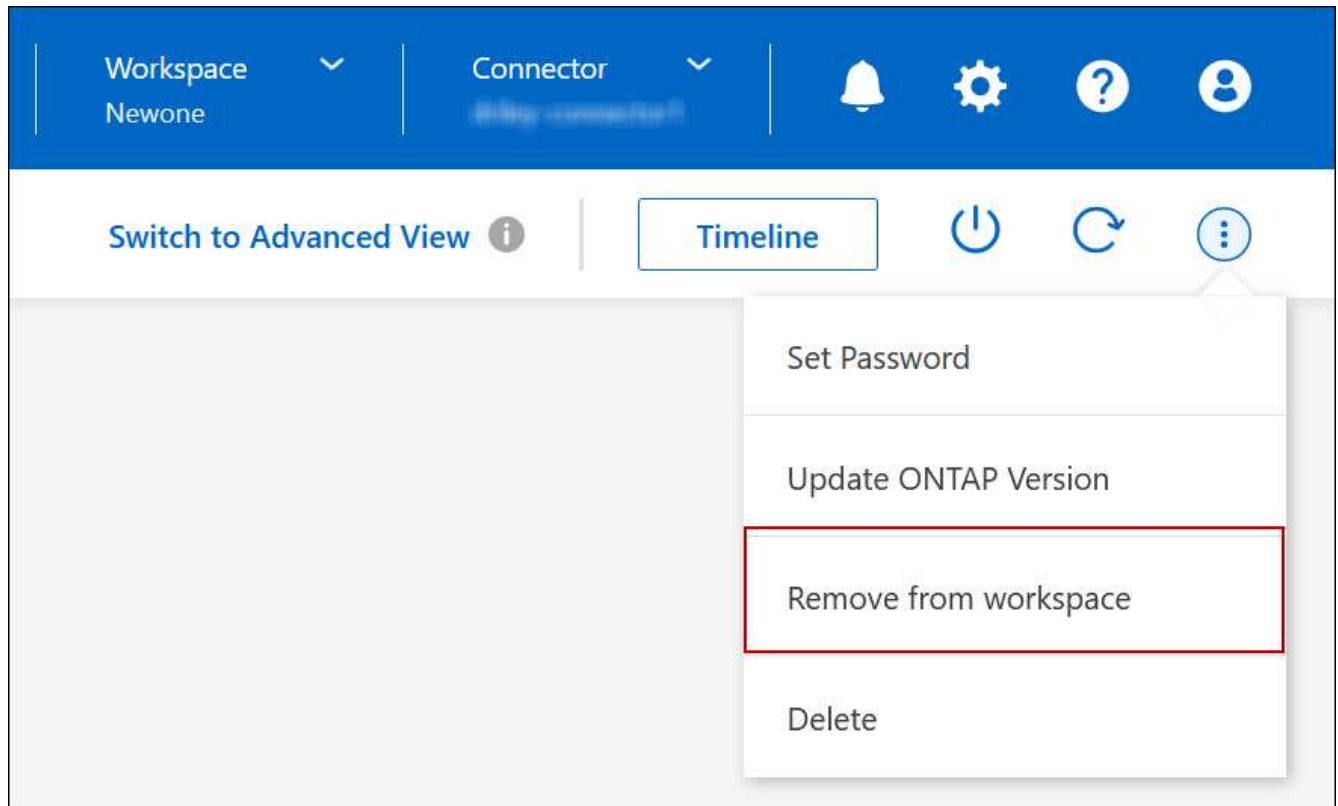
通过从BlueXP中删除工作环境、您可以执行以下操作：

- 在另一个工作空间中重新发现它
- 从另一个BlueXP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"画布"页面上、双击要删除的工作环境。
2. 在BlueXP控制台右上角、单击椭圆图标、然后选择*从工作空间中删除*。



3. 在"Review from Workspace"窗口中、单击*删除*。

结果

BlueXP会删除工作环境。用户可以随时从 " 画布 " 页面重新发现此工作环境。

删除 **Cloud Volumes ONTAP** 系统

您应始终从BlueXP中删除Cloud Volumes ONTAP 系统、而不是从云提供商的控制台中删除。例如，如果您从云提供商终止了已获得许可的 Cloud Volumes ONTAP 实例，则不能将此许可证密钥用于其他实例。要释放许可证、您必须从BlueXP中删除工作环境。

删除工作环境后、BlueXP将终止Cloud Volumes ONTAP 实例并删除磁盘和快照。

删除工作环境时、不会删除由其他服务管理的资源、例如用于BlueXP备份和恢复的备份以及用于BlueXP分类的实例。您需要手动自行删除它们。否则，您将继续收到这些资源的费用。



当BlueXP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. 如果您在工作环境中启用了BlueXP备份和恢复、请确定是否仍需要备份的数据、然后再执行此操作 ["如有必要，删除备份"](#)。

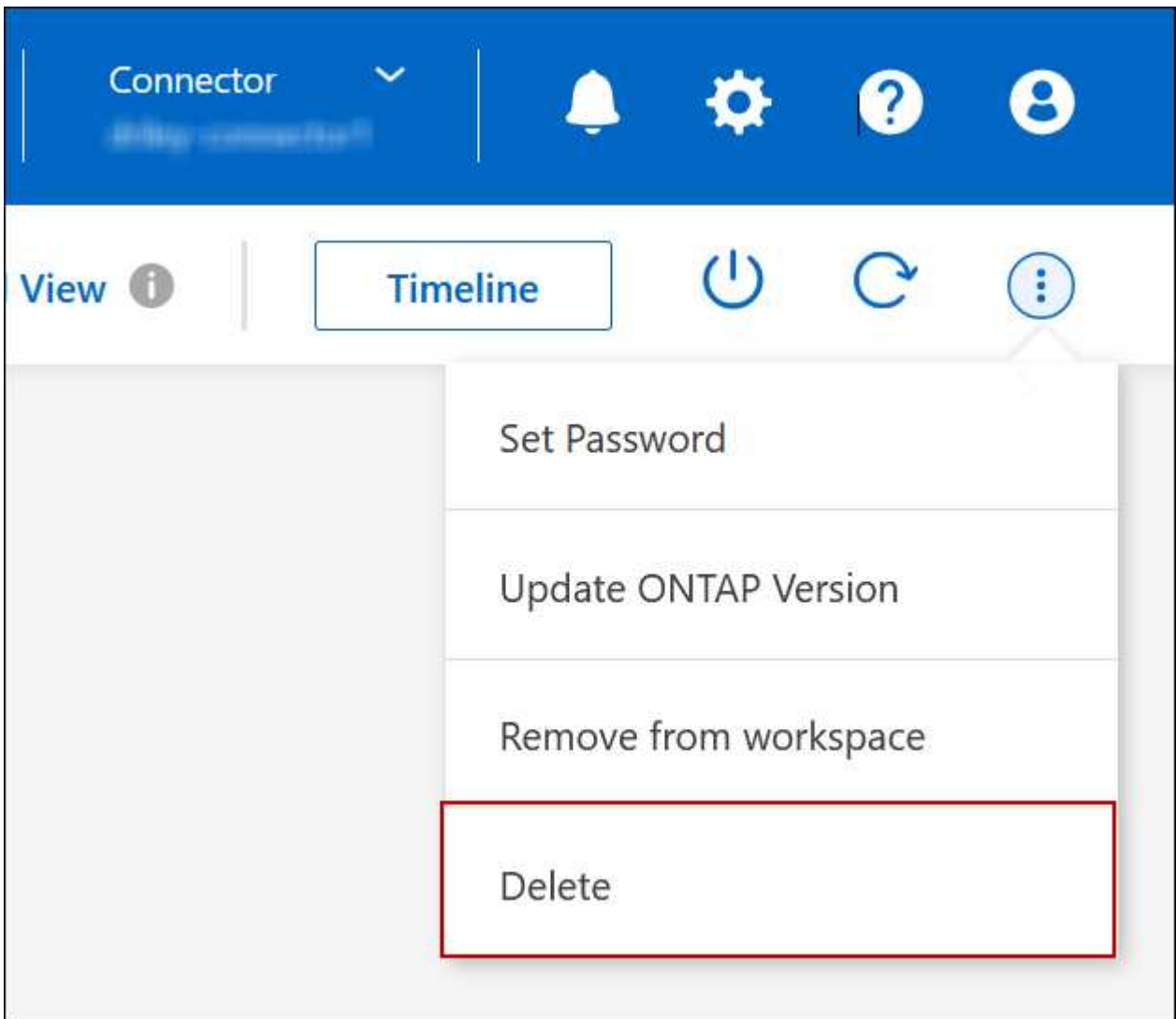
BlueXP备份和恢复在设计上独立于Cloud Volumes ONTAP。在删除Cloud Volumes ONTAP 系统时、BlueXP备份和恢复不会自动删除备份、并且UI中当前不支持在删除系统后删除备份。

2. 如果您在此工作环境中启用了BlueXP分类、并且没有其他工作环境使用此服务、则需要删除此服务的实例。

["了解有关BlueXP分类实例的更多信息"](#)。

3. 删除 Cloud Volumes ONTAP 工作环境。

- a. 在 "画布" 页面上，双击要删除的 Cloud Volumes ONTAP 工作环境的名称。
- b. 在BlueXP控制台右上角、单击椭圆图标、然后选择*删除*。



- c. 在删除工作环境窗口下、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。

AWS管理

更改 Cloud Volumes ONTAP 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的大小不足或过大，则可以随时更改此实例类型。

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）。否则，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。











BlueXP通过启动接管并等待交还来一次妥善更改一个节点。在此过程中，NetApp 的 QA 团队对文件的写入和读取进行了测试，但在客户端上看不到任何问题。随着连接的更改，我们确实看到 I/O 级别重试，但应用程序层克服了 NFS/CIFS 连接的这些短 "重新连接"。

参考

有关AWS中支持的实例类型列表、请参见 ["支持的EC2实例"](#)。

步骤

1. 在"画布"页面上、选择工作环境。
2. 在概述选项卡上、单击功能面板、然后单击*实例类型*旁边的铅笔图标。

Information	Features
Working Environment Tags	Tags 
Scheduled Downtime	Off 
S3 Storage Classes	Standard-Infrequent Access 
Instance Type	m5.xlarge 
Write Speed	Normal 
Ransomware Protection	Off 
Support Registration	Not Registered 
CIFs Setup	

a. 如果您使用的是基于节点的PAYGO许可证、则可以选择通过单击*许可证类型*旁边的铅笔图标来选择其他许可证和实例类型。

3. 选择一个实例类型、选中此复选框以确认您了解此更改的含义、然后单击*更改*。

结果

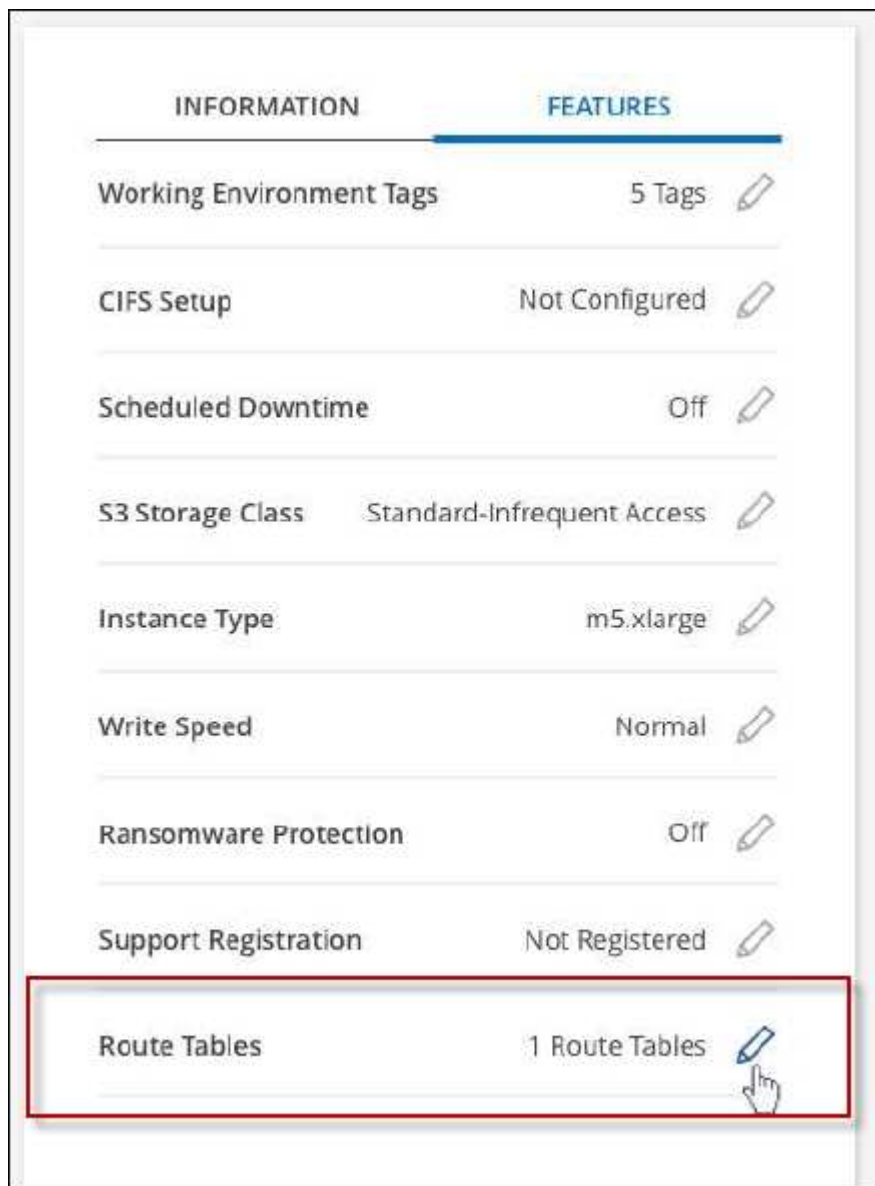
Cloud Volumes ONTAP 会使用新配置重新启动。

更改多个 AZs 中 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 可用性区域（AZs）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，则可以执行此操作。

步骤

1. 在"画布"页面上、选择工作环境。
2. 在概述选项卡上、单击功能面板、然后单击*路由表*旁边的铅笔图标。



3. 修改选定路由表的列表，然后单击 * 保存 *。

结果

BlueXP发送AWS请求以修改路由表。

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的大小不足或过大，则可以随时根据您的需要更改此虚拟机类型。

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）。否则，操作将失败。

["ONTAP 9 文档：用于配置自动交还的命令"](#)

- 更改虚拟机类型可能会影响 Microsoft Azure 服务费用。
- 该操作将重新启动 Cloud Volumes ONTAP 。

对于单节点系统，I/O 中断。

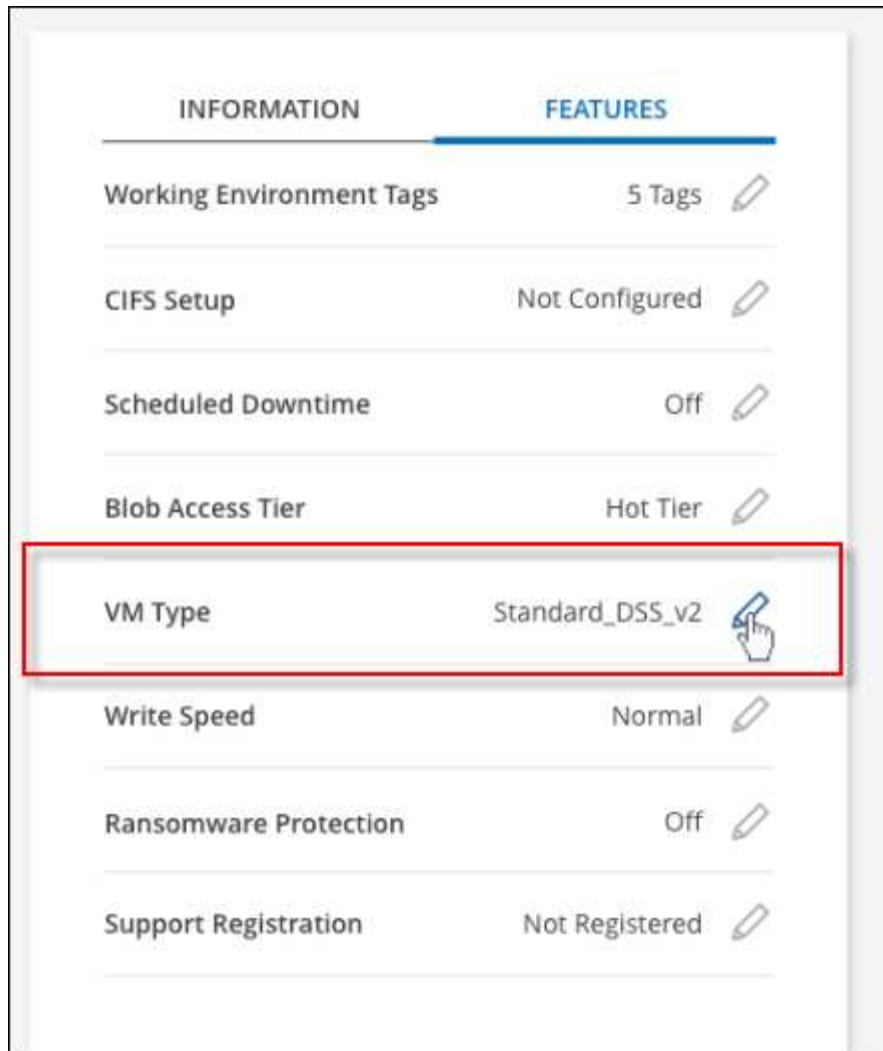
对于 HA 对、更改不会中断。HA 对继续为数据提供服务。



BlueXP通过启动接管并等待交还来一次妥善更改一个节点。在此过程中，NetApp 的 QA 团队对文件的写入和读取进行了测试，但在客户端上看不到任何问题。随着连接的更改，我们确实看到 I/O 级别重试，但应用程序层克服了 NFS/CIFS 连接的这些短 "重新连接"。

步骤

1. 在"画布"页面上、选择工作环境。
2. 在概述选项卡上、单击功能面板、然后单击*虚拟机类型*旁边的铅笔图标。



a. 如果您使用的是基于节点的PAYGO许可证、则可以选择通过单击*许可证类型*旁边的铅笔图标来选择其他许可证和VM类型。

3. 选择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 会使用新配置重新启动。

覆盖Azure中Cloud Volumes ONTAP HA对的CIFS锁定

帐户管理员可以在BlueXP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 CIFS 会话。

关于此任务

Microsoft Azure 会在其虚拟机上计划定期维护事件。在 Cloud Volumes ONTAP HA 对上发生维护事件时， HA 对将启动存储接管。如果在此维护事件期间存在活动的 CIFS 会话，则锁定 CIFS 文件可能会阻止存储交还。

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。



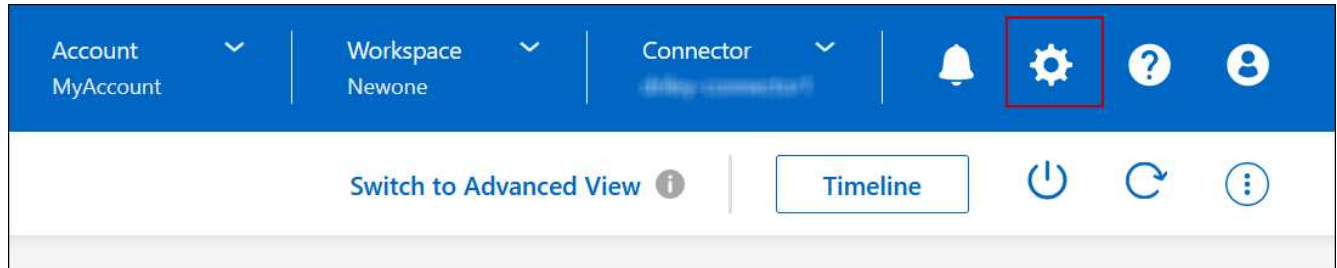
此过程可能会对 CIFS 客户端造成中断。未从 CIFS 客户端提交的数据可能会丢失。

您需要的内容

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

步骤

1. 在BlueXP控制台的右上角、单击设置图标、然后选择*连接器设置*。



2. 在 * Azure * 下，单击 * 适用于 Azure HA 工作环境的 Azure CIFS 锁定 *。
3. 单击复选框以启用此功能，然后单击 * 保存 *。

使用Azure专用链路或服务端点

Cloud Volumes ONTAP 使用Azure专用链路连接到其关联的存储帐户。如果需要、您可以禁用Azure专用链路、而改用服务端点。

概述

默认情况下、BlueXP会为Cloud Volumes ONTAP 与其关联存储帐户之间的连接启用Azure专用链路。Azure Private Link可确保Azure中端点之间的连接安全、并可提供性能优势。

如果需要、您可以将Cloud Volumes ONTAP 配置为使用服务端点、而不是Azure专用链路。

无论采用哪种配置、BlueXP都会始终限制Cloud Volumes ONTAP 与存储帐户之间的连接的网络访问。网络访问仅限于部署了Cloud Volumes ONTAP 的vNet和部署了连接器的vNet。

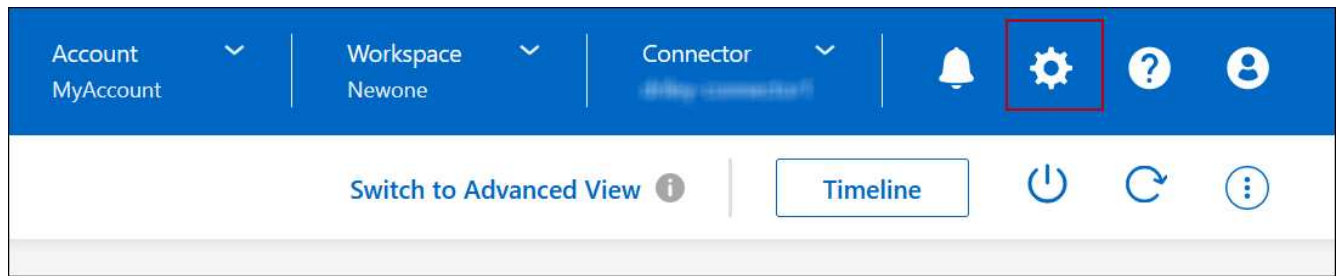
请禁用Azure专用链路并改用服务端点

如果您的企业需要、您可以更改BlueXP中的设置、以便将Cloud Volumes ONTAP 配置为使用服务端点、而不是Azure专用链路。更改此设置将适用场景 添加您创建的新Cloud Volumes ONTAP 系统。仅支持服务端点 "[Azure区域对](#)" 在连接器和Cloud Volumes ONTAP VNets之间。

此连接器应部署在与其管理的 Cloud Volumes ONTAP 系统所在的同一 Azure 区域或中 "[Azure 区域对](#)" 对于 Cloud Volumes ONTAP 系统。

步骤

1. 在BlueXP控制台的右上角、单击设置图标、然后选择*连接器设置*。



2. 在 * Azure * 下，单击 * 使用 Azure 专用链接 *。
3. 取消选择 * Cloud Volumes ONTAP 与存储帐户之间的专用链路连接 *。
4. 单击 * 保存 *。

完成后

如果禁用了 Azure 专用链路、并且 Connector 使用代理服务器、则必须启用直接 API 流量。

["了解如何在 Connector 上启用直接 API 流量"](#)

使用 Azure 专用链路

在大多数情况下、您无需执行任何操作即可使用 Cloud Volumes ONTAP 设置 Azure 专用链路。BlueXP 为您管理 Azure 专用链路。但是、如果您使用现有 Azure 私有 DNS 区域、则需要编辑配置文件。

自定义 DNS 的要求

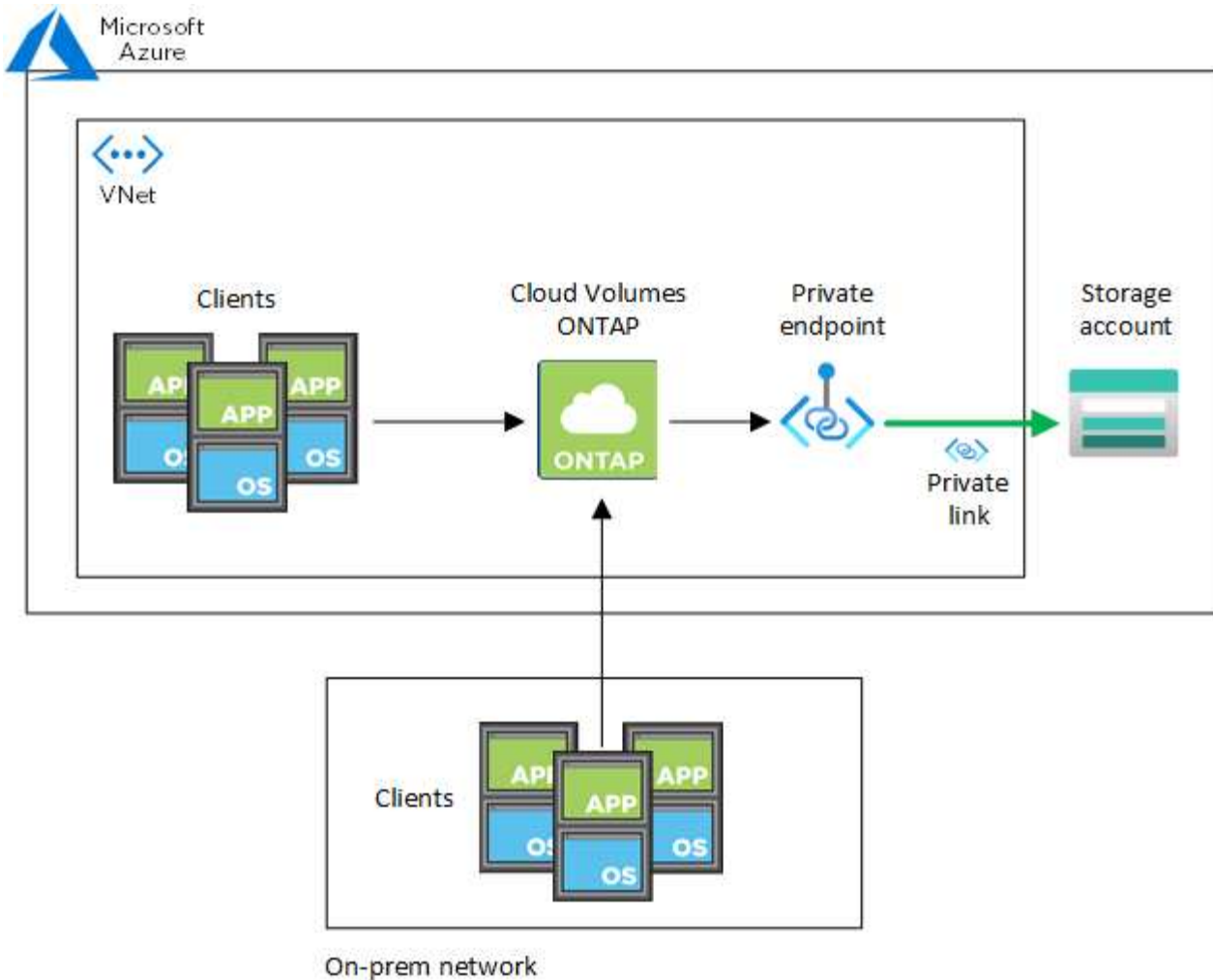
或者、如果您使用自定义 DNS、则需要从自定义 DNS 服务器创建一个条件转发器来访问 Azure 专用 DNS 区域。要了解更多信息、请参见 ["Azure 有关使用 DNS 转发器的文档"](#)。

专用链路连接的工作原理

当 BlueXP 在 Azure 中部署 Cloud Volumes ONTAP 时、它会在资源组中创建一个私有端点。专用端点与 Cloud Volumes ONTAP 的存储帐户关联。因此，对 Cloud Volumes ONTAP 存储的访问会通过 Microsoft 主干网络进行。

如果客户端与 Cloud Volumes ONTAP 位于同一个 vNet 中，位于对等 VNets 中，或者使用专用 VPN 或 ExpressRoute 连接到 VNet，则客户端访问将通过专用链路进行。

以下示例显示了客户端通过同一个 vNet 中的专用链路以及具有专用 VPN 或 ExpressRoute 连接的内部网络进行访问的情况。



如果连接器和Cloud Volumes ONTAP 系统部署在不同的VN中、则必须在部署连接器的vNet与部署Cloud Volumes ONTAP 系统的vNet之间设置vNet对等关系。

向BlueXP提供有关Azure私有DNS的详细信息

如果您使用 "Azure 专用 DNS"，然后您需要修改每个 Connector 上的配置文件。否则、BlueXP无法在Cloud Volumes ONTAP 与其关联存储帐户之间启用Azure专用链路连接。

请注意， DNS 名称必须与 Azure DNS 命名要求匹配 "如 Azure 文档中所示"。

步骤

1. 通过 SSH 连接到 Connector 主机并登录。
2. 导航到以下目录： /opt/application/netapp/cloudmanager/docker_occm/data
3. 通过使用以下关键字值对添加"user-private-dns-zone-settings"参数来编辑app.conf:

```
"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
}
```

应在与"system-id"相同的级别输入参数、如下所示：

```
"system-id" : "<system ID>",
"user-private-dns-zone-settings" : {
```

请注意、只有当专用DNS区域与Connector订阅不同时、才需要使用subscription关键字。

4. 保存文件并注销 Connector 。

不需要重新启动。

启用故障回滚

如果在特定操作中、BlueXP无法创建Azure专用链路、则它将在没有Azure专用链路连接的情况下完成此操作。在创建新的工作环境（单节点或 HA 对）或对 HA 对执行以下操作时，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 时创建新存储帐户。

如果BlueXP无法创建Azure专用链路、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符合公司的安全法规。

如果启用回滚、则BlueXP将停止此操作并回滚此操作中创建的所有资源。

您可以通过API或更新app.conf文件启用回滚。

*通过API*启用回滚

步骤

1. 使用 PUT /occm/config 具有以下请求正文的API调用：

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

*通过更新app.conf启用回滚

步骤

1. 通过 SSH 连接到 Connector 主机并登录。
2. 导航到以下目录： /opt/application/netapp/cloudmanager/docker_occm/data
3. 通过添加以下参数和值来编辑app.conf：

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

。 保存文件并注销 Connector 。

不需要重新启动。

移动资源组

Cloud Volumes ONTAP 支持 Azure 资源组移动、但 workflow 仅在 Azure 控制台中执行。

您可以在同一 Azure 订阅中将工作环境从一个资源组移动到 Azure 中的其他资源组。不支持在不同 Azure 订阅之间移动资源组。

步骤

1. 从*画布*中删除工作环境。

要了解如何删除工作环境、请参见 ["删除 Cloud Volumes ONTAP 工作环境"](#)。

2. 在 Azure 控制台中执行资源组移动。

要完成移动、请参见 ["将资源移动到 Microsoft Azure 文档中的新资源组或订阅"](#)。

3. 在*画布*中、了解工作环境。

4. 在工作环境信息中查找新资源组。

结果

工作环境及其资源 (VM、磁盘、存储帐户、网络接口、快照) 位于新资源组中。

Google Cloud 管理

更改 Cloud Volumes ONTAP 的 Google Cloud 计算机类型

在 Google Cloud 中启动 Cloud Volumes ONTAP 时，您可以从多种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"](#)

- 更改计算机类型可能会影响 Google Cloud 服务费用。
- 该操作将重新启动 Cloud Volumes ONTAP 。

对于单节点系统，I/O 中断。

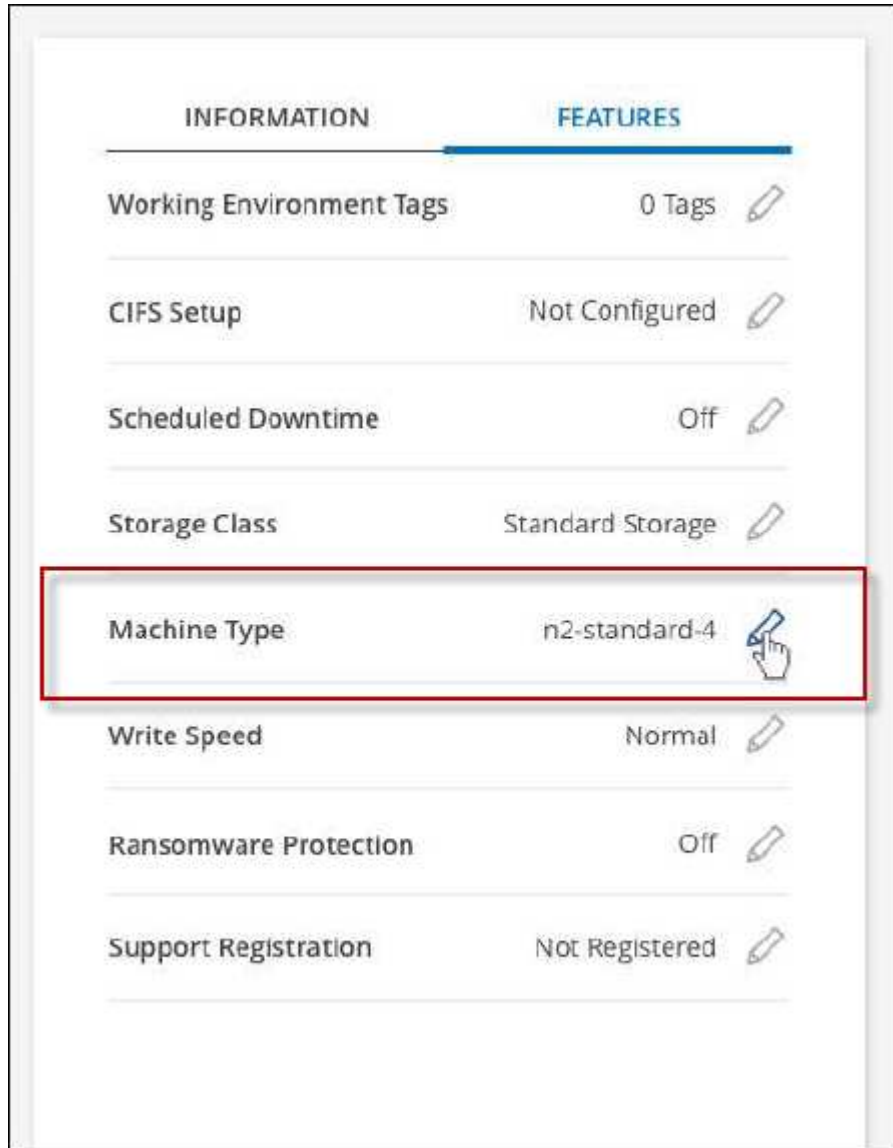
对于 HA 对、更改不会中断。HA 对继续为数据提供服务。



BlueXP通过启动接管并等待交还来一次妥善更改一个节点。在此过程中，NetApp的QA团队对文件的写入和读取进行了测试，但在客户端上看不到任何问题。随着连接的更改，我们确实看到I/O级别重试，但应用程序层克服了NFS/CIFS连接的这些短“重新连接”。

步骤

1. 在“画布”页面上、选择工作环境。
2. 在概述选项卡上、单击功能面板、然后单击*计算机类型*旁边的铅笔图标。



- a. 如果您使用的是基于节点的PAYGO许可证、则可以选择通过单击*许可证类型*旁边的铅笔图标来选择其他许可证和计算机类型。
3. 选择计算机类型、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 会使用新配置重新启动。

使用高级视图管理Cloud Volumes ONTAP

如果您需要对Cloud Volumes ONTAP 执行高级管理、可以使用ONTAP 系统管理器来执行此操作、该管理器是随ONTAP 系统提供的一个管理界面。我们直接在BlueXP中提供了System Manager界面、因此您无需离开BlueXP即可进行高级管理。

此高级视图可作为预览版使用。我们计划改进此体验、并在即将发布的版本中添加增强功能。请通过产品内聊天向我们发送反馈。

功能

通过BlueXP中的高级视图、您可以访问其他管理功能：

- 高级存储管理
管理一致性组、共享、qtree、配额和Storage VM。
- 网络管理
管理IP空间、网络接口、端口集和以太网端口。
- 事件和作业
查看事件日志、系统警报、作业和审核日志。
- 高级数据保护
保护Storage VM、LUN和一致性组。
- 主机管理
设置SAN启动程序组和NFS客户端。

支持的配置

在标准云区域、Cloud Volumes ONTAP 9.10.0及更高版本支持通过System Manager进行高级管理。

在GovCloud地区或无法访问出站Internet的地区不支持System Manager集成。

限制

Cloud Volumes ONTAP 不支持System Manager界面中显示的一些功能：

- BlueXP层
Cloud Volumes ONTAP 不支持BlueXP层服务。创建卷时、必须直接从BlueXP的标准视图设置将数据分层到对象存储。
- 层
System Manager不支持聚合管理(包括本地层和云层)。您必须直接从BlueXP的标准视图管理聚合。

- 固件升级

Cloud Volumes ONTAP 不支持从*集群>设置*页面自动更新固件。

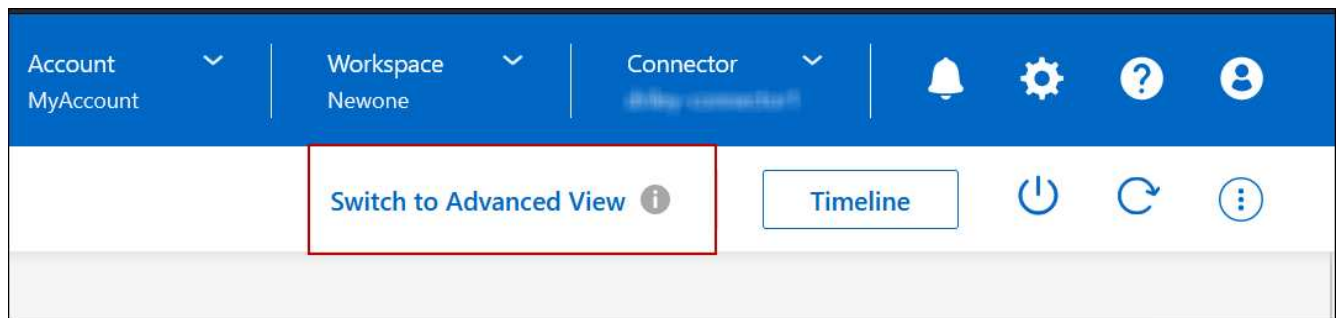
此外、不支持从System Manager进行基于角色的访问控制。

如何开始使用

打开Cloud Volumes ONTAP 工作环境、然后单击高级视图选项。

步骤

1. 从左侧导航菜单中、选择*存储>画布*。
2. 在"画布"页面上、双击Cloud Volumes ONTAP 系统的名称。
3. 在右上角、单击*切换到高级视图*。



4. 如果显示确认消息、请通读该消息并单击*关闭*。
5. 使用System Manager管理Cloud Volumes ONTAP。
6. 如果需要、请单击*切换到标准视图*以通过BlueXP返回到标准管理。

有关使用**System Manager**的帮助

如果在Cloud Volumes ONTAP 中使用System Manager需要帮助、请参见 "[ONTAP 文档](#)" 了解分步说明。以下链接可能会有所帮助：

- "[卷和LUN管理](#)"
- "[网络管理](#)"
- "[数据保护](#)"

从命令行界面管理**Cloud Volumes ONTAP**

Cloud Volumes ONTAP 命令行界面可用于运行所有管理命令，也是执行高级任务或使用命令行界面更自如的理想选择。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、您可能需要从云提供商网络中的跳转主机进行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BlueXP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>画布*。
 - b. 在 "画布 " 页面上，选择 Cloud Volumes ONTAP 系统。
 - c. 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::>
```

系统运行状况和事件

验证 **AutoSupport** 设置

AutoSupport 会主动监控系统的运行状况，并向 NetApp 技术支持发送消息。默认情况下，每个节点都启用了 AutoSupport，以便使用 HTTPS 传输协议向技术支持发送消息。最好验证 AutoSupport 是否可以发送这些消息。

唯一需要的配置步骤是确保 Cloud Volumes ONTAP 具有出站 Internet 连接。有关详细信息，请参阅云提供商的网络要求。

AutoSupport 要求

Cloud Volumes ONTAP 节点需要通过出站Internet访问NetApp AutoSupport、NetApp会主动监控系统运行状况并向NetApp技术支持发送消息。

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>

如果无法通过出站Internet连接发送AutoSupport 消息、则BlueXP会自动将您的Cloud Volumes ONTAP 系统配置为使用Connector作为代理服务器。唯一的要求是确保Connector的安全组允许通过端口3128进行_inbound_连接。部署Connector后、您需要打开此端口。

如果您为Cloud Volumes ONTAP 定义了严格的出站规则、则还需要确保Cloud Volumes ONTAP 安全组允许通过端口3128进行_outout_连接。

确认出站 Internet 访问可用后，您可以测试 AutoSupport 以确保它可以发送消息。有关说明，请参见 "[ONTAP 文档：设置 AutoSupport](#)"。

对AutoSupport 配置进行故障排除

如果出站连接不可用、并且BlueXP无法将您的Cloud Volumes ONTAP 系统配置为使用此连接器作为代理服务器、您将从BlueXP收到一条通知、标题为"<工作环境名称>无法发送AutoSupport 消息"。

您很可能会因为网络问题而收到此消息。

请按照以下步骤解决此问题。

步骤

1. 通过SSH连接到Cloud Volumes ONTAP 系统、以便您可以从命令行界面管理系统。

["了解如何通过SSH连接到Cloud Volumes ONTAP"](#)。

2. 显示 AutoSupport 子系统的详细状态：

```
autosupport check show-details
```

响应应类似于以下内容：

```

Category: smtp
  Component: mail-server
  Status: failed
  Detail: SMTP connectivity check failed for destination:
        mailhost. Error: Could not resolve host -
'mailhost'
  Corrective Action: Check the hostname of the SMTP server

Category: http-https
  Component: http-put-destination
  Status: ok
  Detail: Successfully connected to:
        <https://support.netapp.com/put/AsupPut/>.

  Component: http-post-destination
  Status: ok
  Detail: Successfully connected to:
https://support.netapp.com/asupprod/post/1.0/postAsup.

Category: on-demand
  Component: ondemand-server
  Status: ok
  Detail: Successfully connected to:
        https://support.netapp.com/aods/asupmessage.

Category: configuration
  Component: configuration
  Status: ok
  Detail: No configuration issues found.
5 entries were displayed.

```

如果http-https类别的状态为"ok"、则表示已正确配置AutoSupport、可以发送消息。

3. 如果状态不正确、请验证每个Cloud Volumes ONTAP 节点的代理URL:

```
autosupport show -fields proxy-url
```

4. 如果proxy URL参数为空、请将Cloud Volumes ONTAP 配置为使用Connector作为代理:

```
autosupport modify -proxy-url http://<connector private ip>:3128
```

5. 再次验证AutoSupport 状态:

```
autosupport check show-details
```

6. 如果状态仍为FAILED、请验证Cloud Volumes ONTAP 与连接器之间是否通过端口3128建立连接。

7. 如果在验证是否存在连接后状态ID仍然失败、请通过SSH连接到连接器。

["了解有关连接到Linux VM for the Connector的更多信息"](#)

8. 转至 `/opt/application/netapp/cloudmanager/docker_occm/data/`

9. 打开代理配置文件 `squid.conf`

文件的基本结构如下：

```
http_port 3128
acl localnet src 172.31.0.0/16
acl azure_aws_metadata dst 169.254.169.254

http_access allow localnet
http_access deny azure_aws_metadata
http_access allow localhost
http_access deny all
```

`localnet src`值是Cloud Volumes ONTAP 系统的CIDR。

10. 如果Cloud Volumes ONTAP 系统的CIDR块不在文件中指定的范围内、请按如下所示更新此值或添加新条目：

```
acl cvonet src <cidr>
```

如果添加此新条目、请勿忘记同时添加一个允许条目：

```
http_access allow cvonet
```

以下是一个示例：

```
http_port 3128
acl localnet src 172.31.0.0/16
acl cvonet src 172.33.0.0/16
acl azure_aws_metadata dst 169.254.169.254

http_access allow localnet
http_access allow cvonet
http_access deny azure_aws_metadata
http_access allow localhost
http_access deny all
```

11. 编辑此配置文件后、以`sudo`身份重新启动代理容器：

```
docker restart squid
```

12. 返回到Cloud Volumes ONTAP 命令行界面并验证Cloud Volumes ONTAP 是否可以发送AutoSupport 消息：

```
autosupport check show-details
```

配置EMS

事件管理系统(EMS)可收集并显示有关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 "[ONTAP 文档： EMS 配置概述](#)"。

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。