Cloud Volumes ONTAP文档

Cloud Volumes ONTAP

NetApp
March 10, 2026

目录

Cloud Volumes ONTAP文档

发行说明

Cloud Volumes ONTAP的新功能

了解NetApp Console中Cloud Volumes ONTAP管理的新功能。

本页描述的增强功能特定于通过控制台管理Cloud Volumes ONTAP 。要了解Cloud Volumes ONTAP软件本身的新功能， "转到Cloud Volumes ONTAP发行说明" 。

2026 年 3 月 10 日

能够管理 **Cloud Volumes ONTAP** 的 **Console** 代理设置

现在，即使失去连接或代理设置不正确，也可以在 NetApp Console 代理上管理 Cloud Volumes ONTAP 的代理设置。以前，如果 Console 代理在 20 分钟内无法连接到 Cloud Volumes ONTAP，它将使用默认设置覆盖您的手动代理设置。这导致通信失败，包括 AutoSupport 消息问题。若要保留现有系统的代理设置，请运行以下 API 调用：

```
PUT /occm/config
```

在请求正文中包含以下参数：

```
{
  "proxyMode": "No_Overwrites"
}
```

默认模式为标准模式，这意味着如果 Console 代理在 20 分钟内无法连接到 Cloud Volumes ONTAP，它将使用默认设置覆盖您的代理设置。

"配置可修改的 NetApp Console 参数"

2026 年 2 月 26 日

支持用于私有模式部署的 **Google Infrastructure Manager**

Cloud Volumes ONTAP 9.16.1 及更高版本现在支持 "Google Cloud Infrastructure Manager" (IM) 而不是 "Cloud Deployment Manager" (DM) 用于 Google Cloud 中的新私有模式部署。Google 将在不久的将来弃用 Deployment Manager 作为基础架构服务，转而使用更高级的 Infrastructure Manager。

从 2026 年 2 月 25 日开始，Cloud Volumes ONTAP 使用 Infrastructure Manager 进行新的和现有的专用模式部署。下表介绍了您的基本工作流程：

场景	操作	代理的新 **API**	代理的新权限	适用于 **Cloud Volumes ONTAP** 的全新 **Google Cloud API**	文档资源
私有模式下的现有代理和现有部署	通过从 NetApp 支持站点下载安装程序，然后在主机上手动安装代理，升级到最新版本的 NetApp Console 代理，以便它可以使用 Infrastructure Manager API。然后，将现有的 Cloud Volumes ONTAP 系统转换为使用 Infrastructure Manager。	• 云基础架构管理器 API • Cloud Quotas API • Cloud Build API	Console 发行版列出的所有权限： • "2025 年 12 月 8 日" • "2026 年 2 月 09 日" • cloudbuild.workerpools.get • cloudbuild.workerpools.get	• https://cloudbuild.googleapis.com/v1 • https://www.googleapis.com/upload/storage/v1 • https://config.googleapis.com/v1	"为 Google Cloud Infrastructure Manager 配置现有的 Cloud Volumes ONTAP 部署"
新代理和新部署	创建新代理，并在专用模式下部署新的 Cloud Volumes ONTAP 系统。				• "从 Google Cloud 创建 Console 代理" • "私人模式部署的快速入门"

在专用模式部署中，您需要对 Cloud Volumes ONTAP 进行一些配置更改才能开始使用 Infrastructure Manager。请参阅 "适用于专用模式部署的 Infrastructure Manager 配置"。

相关链接

- "NetApp Console Agent 4.2.0 发行说明"

- "Google Cloud Infrastructure Manager 所需的权限"

2026 年 2 月 19 日

Azure 支持的新区域

您现在可以在以下区域的 Azure 中的单个和多个可用区域中部署Cloud Volumes ONTAP 9.12.1 GA 及更高版本。这包括对单节点和高可用性 (HA) 部署的支持。

- 日本西部 (japanwest)
- 印度尼西亚中部 (indonesiacentral)

有关所有地区的列表，请参阅 "Azure 下的全球区域地图"。

2026 年 2 月 17 日

Cloud Volumes ONTAP 支持下一代 **Google Cloud** 虚拟机

借助 9.18.1，NetApp 将新的 Cloud Volumes ONTAP 部署从 N2 虚拟机过渡到下一代 Google Cloud C3 系列虚拟机，以获得更快、更具可扩展性的体验。现在，您可以在 Google Cloud 中部署 Cloud Volumes ONTAP 9.18.1 及更高版本时利用 C3 系列虚拟机。C3 系列机器通过使用 Google Virtual NIC (gVNIC) 和 Hyperdisk Balanced 磁盘，确保密集型工作负载的动态性能，从而提供更高的性能和更高的容量限制。

目前，Cloud Volumes ONTAP 仅在单节点部署中支持 C3 系列。

如果您的 Cloud Volumes ONTAP 系统运行 9.18.1 或更高版本，则用于轻松部署单节点的预配置包将自动使用 C3 虚拟机，同时使您能够根据工作负载需求自定义 IOPS 和吞吐量参数。同样，在创建聚合时，您可以添加 Hyperdisk Balanced 磁盘，以在 Google Cloud 中实现更好的性能和可扩展性。此外，您可以为默认 Flash Cache 支持选择 C3 系列计算机的 LSSD 变体。

将卷添加到聚合时，无法更改 C3 VM 的磁盘类型，因为 C3 仅支持 Hyperdisk Balanced 磁盘。同样，将具有 N2 VM 类型的系统复制到 C3 VM 时，磁盘类型默认设置为 Hyperdisk Balanced。

"Google Cloud 中 Cloud Volumes ONTAP 支持的配置"

"Google 文档：C3 机器系列"

Azure 中 **Cloud Volumes ONTAP** 的 **VNet** 安全性

Azure 单个和多个可用区域中的 Cloud Volumes ONTAP 9.18.1 及更高版本部署支持 Azure Virtual Network (VNet) 加密，作为其分层安全策略的一部分来保护传输中的数据。Cloud Volumes ONTAP 利用 Azure 的本机数据报传输层安全性 (DTLS) 协议来保护 ONTAP 节点、管理接口和其他 Azure 服务之间的通信，防止拦截和未经授权的访问。这种网络级加密是对 ONTAP 内置存储和静态数据保护的补充，可为您的数据提供端到端的安全性。

"用于 Azure VNet 加密的网络"

2026 年 2 月 12 日

在 **Azure** 中支持 **Ebdsv5** 和 **E104ids_v5** 虚拟机

从 Cloud Volumes ONTAP 9.18.1 开始，您可以部署 Ebdsv5 和 E104ids_v5 虚拟机，用于单节点和高可用性 (HA) 部署和升级。

Azure 虚拟机 Eb 系列中的 Ebdsv5 VM 针对更高的远程存储性能进行了优化。您可以将这些 VM 用于内存密集型和 I/O 密集型企业工作负载，例如关系数据库、内存分析和其他要求苛刻的关键业务应用程序。

E104ids_v5 是一个隔离的 VM 实例，可帮助您更好地处理计划的维护窗口。与 E80ids_v4 相比，它提供了更高的磁盘吞吐量和 IOPS，以及更好的整体网络性能。

"Azure 中Cloud Volumes ONTAP支持的配置"

"Azure 文档：Edsv5 尺寸系列"

2026 年 2 月 10 日

Cloud Volumes ONTAP 9.18.1 GA

您现在可以使用 NetApp Console 在 AWS、Azure 和 Google Cloud 中部署和管理 Cloud Volumes ONTAP 9.18.1 的 General Availability (GA) 版本。

"了解有关此版本Cloud Volumes ONTAP的更多信息" 。

2026 年 2 月 9 日

支持 **Google Cloud Infrastructure Manager**

Cloud Volumes ONTAP 9.16.1 及更高版本现在支持 "Google Cloud Infrastructure Manager" (IM) 而不是 "Cloud Deployment Manager" (DM) 用于 Google Cloud 中的新部署。Google 将在不久的将来弃用 Deployment Manager 作为基础架构服务，转而使用更高级的 Infrastructure Manager。

从 2026 年 2 月 9 日开始，Cloud Volumes ONTAP 使用 Infrastructure Manager 进行新的和现有的部署。下表为您解释了一些工作流程：

场景	操作	代理的新 **API**	代理的新权限	适用于 **Cloud Volumes ONTAP** 的全新 **Google Cloud API**	文档资源
现有代理和现有 Cloud Volumes ONTAP 部署	将新的 API 和权限添加到现有代理并转换现有 Cloud Volumes ONTAP 系统。	• 云基础架构管理器 API • Cloud Quotas API	Console 发行版列出的所有权限： • "2025 年 12 月 8 日" • "2026 年 2 月 09 日"	https://www.googleapis.com/upload/storage/v1 https://config.googleapis.com/v1	"为 Google Cloud Infrastructure Manager 配置现有的 Cloud Volumes ONTAP 部署"
现有代理和新的 Cloud Volumes ONTAP 部署	向现有代理添加新的 API 和权限，并部署新的 Cloud Volumes ONTAP 系统。	• 云基础架构管理器 API • Cloud Quotas API	Console 发行版列出的所有权限： • "2025 年 12 月 8 日" • "2026 年 2 月 09 日"	新部署的所有步骤	"在 Google Cloud 中开始使用 Cloud Volumes ONTAP"

场景	操作	代理的新 **API**	代理的新权限	适用于 **Cloud Volumes ONTAP** 的全新 **Google Cloud API**	文档资源
新代理和新部署	创建新代理并部署新的 Cloud Volumes ONTAP 系统。				• "从 Google Cloud 创建 Console 代理" • "在 Google Cloud 中开始使用 Cloud Volumes ONTAP"

现在，部署 Cloud Volumes ONTAP 以自动使用 Infrastructure Manager，或者通过运行转换工具将 Deployment Manager 中的现有部署切换到 Infrastructure Manager。转换是一次性过程，之后您的系统将开始使用 Infrastructure Manager。有关运行转换工具的说明，请参阅 "为 Google Cloud Infrastructure Manager 配置现有的 Cloud Volumes ONTAP 部署"。

使用 Infrastructure Manager 的 Cloud Volumes ONTAP 系统使用 Google Cloud Storage 存储桶在第一次部署的区域中存储数据和记录，以存储部署记录，这些记录可重复用于后续部署。您可能需要为这些存储桶支付额外费用，但不要编辑或删除存储桶或其内容：

- `gs://netapp-cvo-infrastructure-manager-<project id>`：适用于 ONTAP 版本和用于新 Cloud Volumes ONTAP 部署的 SVM Terraform 模板。在其中， `dm-to-im-convert` 存储桶包含 Cloud Volumes ONTAP Terraform 文件。
- `<gcp project number>-<region>-blueprint-config`：用于存储 Google Cloud Terraform 工件。

相关链接

- "在 Google Cloud 中开始使用 Cloud Volumes ONTAP"
- "NetApp Console Agent 4.2.0 发行说明"
- "Google Cloud Infrastructure Manager 所需的权限"

2026年1月12日

Cloud Volumes ONTAP的首选计费方式

现在您可以选择一种首选的计费方式来计算您的Cloud Volumes ONTAP使用量和超额费用。自 2025 年 6 月 25 日起，自带许可证 (BYOL) 许可模式将不再提供， NetApp已在NetApp Console的“许可和订阅”部分添加了首选的计费方式。您可以选择使用年度市场订阅进行计费和超额费用结算，或者选择现有的 BYOL 模式作为首选方案。这样，您可以灵活选择最适合您组织财务战略和使用模式的充电方式。

"计费偏好和超额费用"。

2025年12月10日

提升 **Azure** 中 **Premium SSD v2** 磁盘性能的能力

现在，您可以通过修改 IOPS 和吞吐量参数来提高 Azure 中 Premium SSD v2 托管磁盘的性能。利用此功能，您可以根据工作负载需求优化系统的存储性能。

"在 Azure 中管理Cloud Volumes ONTAP的 Premium SSD v2 磁盘性能"。

Essentials 许可证超额收费简化

对于Cloud Volumes ONTAP市场年度合同/私有报价，Essentials 许可证的超额使用计算现在与自带许可证 (BYOL) 套餐保持一致。此前，超出部分按基本套餐的每小时市场价格计费。现在，如果您的市场年度合同包含多个 Essentials 套餐， NetApp Console会将 Essentials 套餐的超额费用计入您订阅中价格更高的 Essentials 套餐的可用容量。这简化了 Essentials 套餐的超额费用计算，并确保从 BYOL 许可模式平稳过渡到订阅模式。

"Essentials许可证超额费用如何收取"

支持 **Azure Edsv6** 尺寸系列

从Cloud Volumes ONTAP 9.17.1 开始，您可以通过NetApp Console为新的Cloud Volumes ONTAP实例部署 Azure Edsv6 系列虚拟机。 Cloud Volumes ONTAP 9.17.1 及更高版本将仅支持新部署的第二代虚拟机。这些第二代机器与最新技术兼容，例如统一可扩展固件接口 (UEFI)、Azure Boost 系统和 NVMe。它们非常适合内存密集型系统和需要快速本地存储的应用，例如数据库服务器和分析引擎。

"Azure 中Cloud Volumes ONTAP支持的配置"

2025年11月10日

增强的 **NVMe-TCP** 支持

以前，在 NVMe-TCP 上部署Cloud Volumes ONTAP实例时，您必须在部署之前手动获取和应用 NVMe 许可证。通过此次更新， Cloud Volumes ONTAP现在会在部署期间自动安装所需的 NVMe 许可证，从而简化设置过程。

对于缺少许可证的现有 NVMe-TCP 部署， Cloud Volumes ONTAP会自动应用许可证。您必须重启系统才能使许可证生效。

更多信息请参见 "Cloud Volumes ONTAP支持的客户端协议：NVMe-TCP"。

2025年10月17日

Azure 中的Cloud Volumes ONTAP现已仅限于最新支持版本

现在，通过NetApp Console在 Azure 中部署和升级Cloud Volumes ONTAP仅限于最新支持的版本。这确保了与 Microsoft 支持的最新一代硬件的兼容性，并提供最新的功能和安全增强功能。控制台将提示您升级到支持的版本。

有关更多详细信息，请参阅：

- 部署： "Cloud Volumes ONTAP部署支持的ONTAP版本"
- 升级： "Azure 支持的升级路径"

2025年10月6日

BlueXP现在是NetApp Console

NetApp Console建立在增强和重组的BlueXP基础之上，可在企业级内部和云环境中集中管理NetApp存储和NetApp Data Services，提供实时洞察、更快的工作流程和简化的管理，并且高度安全且合规。

有关更改的详细信息，请参阅 "NetApp Console发行说明"。

简化 AWS 中的Cloud Volumes ONTAP部署

现在，您可以使用快速部署方法在 AWS 中部署Cloud Volumes ONTAP，适用于单节点和高可用性 (HA) 配置。与高级方法相比，此简化流程减少了步骤数，在单个页面上自动设置默认值，并最大限度地减少了导航，使部署更快、更容易。

有关更多信息，请参阅 "使用快速部署在 AWS 中部署Cloud Volumes ONTAP" 。

2025年9月4日

Cloud Volumes ONTAP 9.17.1 RC

您现在可以使用BlueXP在 Azure 和 Google Cloud 中部署和管理Cloud Volumes ONTAP 9.17.1 的候选版本 1。但此版本尚不支持在AWS中部署和升级。

"了解有关此版本Cloud Volumes ONTAP的更多信息"。

2025年8月11日

优化许可证的可用性终止

从 2025 年 8 月 11 日开始， Cloud Volumes ONTAP Optimized 许可证将被弃用，并且将不再可在 Azure 和 Google Cloud 市场中以即用即付 (PAYGO) 订阅的方式购买或续订。如果您拥有现有的包含优化许可证的年度合同，则可以继续使用该许可证，直到合同结束。当您的优化许可证到期时，您可以选择BlueXP中的Cloud Volumes ONTAP Essentials 或 Professional 许可证。

但是，可以通过 API 添加或更新优化许可证。

有关许可包的信息，请参阅 "Cloud Volumes ONTAP许可"。

有关切换到不同充电方式的信息，请参阅 "管理基于容量的许可"。

2025年7月14日

支持透明代理

除了现有的显式代理连接之外， BlueXP现在还支持透明代理服务器。创建或修改BlueXP连接器时，您可以配置透明代理服务器来安全地管理往返于Cloud Volumes ONTAP 的网络流量。

有关在Cloud Volumes ONTAP中使用代理服务器的更多信息，请参阅：

- "用于支持 AWS 中的连接器代理的网络配置"
- "用于支持 Azure 中的连接器代理的网络配置"
- "用于支持 Google Cloud 中的连接器代理的网络配置"

Azure 中的**Cloud Volumes ONTAP**支持新的 **VM** 类型

从Cloud Volumes ONTAP 9.13.1 开始，L8s_v3 作为 Azure 单个和多个可用区域中的 VM 类型受到支持，适用于新的和现有的高可用性 (HA) 对部署。

有关详细信息，请参阅https://docs.netapp.com/us-en/cloud-volumes-ontap-relnotes/reference-configs-azure.html["Azure 中支持的配置"^] 。

2025年6月25日

Cloud Volumes ONTAP的 **BYOL** 许可可用性受限

自 2025 年 6 月 25 日起， NetApp已限制Cloud Volumes ONTAP的自带许可证 (BYOL) 许可模式。此限制适用于 AWS、Azure 和 Google Cloud 中的所有客户和Cloud Volumes ONTAP部署。唯一的例外是美国公共部门客户和中国区域部署。

NetApp支持和服务将持续到您的 BYOL 合同到期，但已过期的许可证将无法续订或延长。BYOL许可证到期后，您必须将其替换为通过云市场订阅购买的基于容量的许可证。通过超大规模市场购买的基于容量的许可模式可以简化许可体验并带来更大的业务优势。请联系您的NetApp客户团队或客户成功代表，讨论您的转换方案。

欲了解更多信息，请参阅此客户公报： "CPC-00661： Cloud Volumes ONTAP BYOL 政策变更" 。

2025年5月29日

为**Cloud Volumes ONTAP 9.15.1** 启用私有模式部署

您现在可以在 AWS、Azure 和 Google Cloud 中以私有模式部署Cloud Volumes ONTAP 9.15.1。 Cloud Volumes ONTAP 9.15.1 的单节点和高可用性 (HA) 部署均启用私有模式。

有关私有模式部署的更多信息，请参阅https://docs.netapp.com/us-en/bluexp-setup-admin/concept-modes.html#restricted-mode["了解BlueXP部署模式"^]。

2025年5月12日

在BlueXP中发现通过 Azure 市场进行的部署

BlueXP现在能够发现通过 Azure 市场直接部署的Cloud Volumes ONTAP系统。这意味着您现在可以在BlueXP中将这些系统作为工作环境添加和管理，就像任何其他Cloud Volumes ONTAP系统一样。

"从 Azure 市场部署Cloud Volumes ONTAP"

2025年4月16日

Azure 支持的新区域

您现在可以在以下区域的 Azure 中的单个和多个可用区域中部署Cloud Volumes ONTAP 9.12.1 GA 及更高版本。这包括对单节点和高可用性 (HA) 部署的支持。

- 西班牙中部
- 墨西哥中央

有关所有地区的列表，请参阅 "Azure 下的全球区域地图"。

2025年4月14日

通过 Google Cloud 中的 API 自动创建存储虚拟机

您现在可以使用BlueXP API 在 Google Cloud 中自动创建存储虚拟机。您一直在Cloud Volumes ONTAP高可用性 (HA) 配置中使用此功能，现在您也可以在单节点部署中使用它。通过使用BlueXP API，您可以在 Google Cloud 环境中轻松创建、重命名和删除其他数据服务存储虚拟机，而无需手动配置所需的网络接口、LIF 和管理 LIF。这种自动化简化了管理存储虚拟机的过程。

"在 Google Cloud 中管理Cloud Volumes ONTAP的数据服务存储虚拟机"

2025年4月3日

AWS 中Cloud Volumes ONTAP 9.13.1 对中国区域的支持

您现在可以在中国区域的 AWS 中部署Cloud Volumes ONTAP 9.13.1。这包括对单节点和高可用性 (HA) 部署的支持。仅支持直接从NetApp购买的许可证。

有关区域可用性，请参阅 "Cloud Volumes ONTAP的全球区域地图"。

2025年3月28日

为Cloud Volumes ONTAP 9.14.1 启用私有模式部署

您现在可以在 AWS、Azure 和 Google Cloud 中以私有模式部署Cloud Volumes ONTAP 9.14.1。 Cloud Volumes ONTAP 9.14.1 的单节点和高可用性 (HA) 部署均启用私有模式。

有关私有模式部署的更多信息，请参阅https://docs.netapp.com/us-en/bluexp-setup-admin/concept-modes.html#restricted-mode["了解BlueXP部署模式"^]。

2025年3月12日

Azure 中支持多可用区域部署的新区域

以下区域现在支持 Azure 中适用于Cloud Volumes ONTAP 9.12.1 GA 及更高版本的 HA 多可用区域部署：

- 美国中部
- US Gov Virginia（美国政府地区 - 弗吉尼亚州）

有关所有地区的列表，请参阅 "Azure 下的全球区域地图"。

2025年3月10日

通过 **Azure** 中的 **API** 自动创建存储虚拟机

您现在可以使用BlueXP API 在 Azure 中为Cloud Volumes ONTAP创建、重命名和删除其他数据服务存储虚拟机。如果您需要使用存储虚拟机进行管理，则使用 API 可以自动执行存储虚拟机的创建过程，包括所需网络接口、LIF 和管理 LIF 的配置。

"管理 Azure 中Cloud Volumes ONTAP的数据服务存储虚拟机"

2025年3月6日

Cloud Volumes ONTAP 9.16.1 正式版

您现在可以使用BlueXP在 Azure 和 Google Cloud 中部署和管理Cloud Volumes ONTAP 9.16.1 通用可用性版本。但此版本尚不支持在AWS中部署和升级。

"了解此版本Cloud Volumes ONTAP中包含的新功能" 。

2025年3月3日

Azure 对新西兰北部地区的支持

Azure 现已支持新西兰北部地区的Cloud Volumes ONTAP 9.12.1 GA 及更高版本的单节点和高可用性 (HA) 配置。请注意，此区域不支持 Lsv3 实例类型。

有关所有受支持区域的列表，请参阅 "Azure 下的全球区域地图"。

2025年2月18日

介绍 **Azure** 市场直接部署

您现在可以利用 Azure 市场直接部署功能，直接从 Azure 市场轻松快速地部署Cloud Volumes ONTAP 。使用这种简化的方法，您可以在您的环境中探索Cloud Volumes ONTAP的核心特性和功能，而无需设置BlueXP Connector 或满足通过BlueXP部署Cloud Volumes ONTAP所需的其他入职标准。

- "了解 Azure 中的Cloud Volumes ONTAP部署选项"
- "从 Azure 市场部署Cloud Volumes ONTAP"

2025年2月10日

已启用用户身份验证，可从**BlueXP**访问系统管理器

作为BlueXP管理员，您现在可以为从BlueXP访问ONTAP系统管理器的ONTAP用户激活身份验证。您可以通过编辑BlueXP连接器设置来启用此选项。此选项适用于标准模式和私人模式。

"使用系统管理器管理Cloud Volumes ONTAP" 。

BlueXP Advanced View 重命名为 **System Manager**

通过ONTAP系统管理器从BlueXP对Cloud Volumes ONTAP进行高级管理的选项已从 **Advanced View** 重命名为 **System Manager**。

"使用系统管理器管理Cloud Volumes ONTAP" 。

引入使用**BlueXP digital wallet**管理许可证的更简单方法

现在，您可以通过使用BlueXP digital wallet中改进的导航点来体验简化的Cloud Volumes ONTAP许可证管理：

- 通过*管理>Licenses and subscriptions>概述/直接许可证*选项卡轻松访问您的Cloud Volumes ONTAP许可证信息。
- 单击“概览”选项卡中 Cloud Volume ONTAP面板上的“查看”以全面了解基于容量的许可证。此高级视图提供有关您的许可证和订阅的详细信息。
- 如果您更喜欢以前的界面，您可以单击“切换到旧视图”按钮按类型查看许可证详细信息并修改许可证的收费方式。

"管理基于容量的许可证" 。

2024年12月9日

已更新 **Azure** 支持的虚拟机列表，以符合最佳实践

在 Azure 中部署Cloud Volumes ONTAP的新实例时， BlueXP上不再可选择 DS_v2 和 Es_v3 机器系列。这些系列将仅在较旧的现有系统中保留和支持。从 9.12.1 版本开始，Azure 仅支持Cloud Volumes ONTAP的新部署。我们建议您切换到 Es_v4 或任何其他与Cloud Volumes ONTAP 9.12.1 及更高版本兼容的系列。但是，DS_v2 和 Es_v3 系列机器将可用于通过 API 进行的新部署。

"Azure 中支持的配置"

2024年11月11日

基于节点的许可证的可用性终止

NetApp已计划终止提供 (EOA) 和终止支持 (EOS) Cloud Volumes ONTAP基于节点的许可。从 2024 年 11 月 11 日起，基于节点的许可证的有限可用性已终止。基于节点的许可支持将于 2024 年 12 月 31 日结束。在基于节点的许可证 EOA 之后，您应该使用BlueXP许可证转换工具过渡到基于容量的许可证。

对于年度或长期承诺， NetApp建议您在 EOA 日期或许可证到期日之前联系您的NetApp代表，以确保过渡的先决条件到位。如果您没有Cloud Volumes ONTAP节点的长期合同，并且根据按需付费 (PAYGO) 订阅运行您的系

统，那么在 EOS 日期之前规划您的转换非常重要。对于长期合同和 PAYGO 订阅，您都可以使用BlueXP许可证转换工具进行无缝转换。

"基于节点的许可证的可用性终止" "将Cloud Volumes ONTAP基于节点的许可证转换为基于容量的许可证"

从**BlueXP**中删除基于节点的部署

使用基于节点的许可证部署Cloud Volumes ONTAP系统的选项在BlueXP上已弃用。除少数特殊情况外，您不能对任何云提供商的Cloud Volumes ONTAP部署使用基于节点的许可证。

NetApp认识到符合合同义务和运营需求的以下独特许可要求，并将在这些情况下继续支持基于节点的许可证：

- 美国公共部门客户
- 私有模式下的部署
- AWS 中国区Cloud Volumes ONTAP部署
- 如果您拥有有效、未过期的按节点自带许可证（BYOL 许可证）

"基于节点的许可证的可用性终止"

在 **Azure Blob** 存储上为**Cloud Volumes ONTAP**数据添加冷层

BlueXP现在允许您选择冷层来存储 Azure Blob 存储上的非活动容量层数据。在现有的热层和冷层中添加冷层可为您提供更实惠的存储选项并提高成本效率。

"Azure 中的数据分层"

限制 **Azure** 存储帐户公共访问的选项

您现在可以选择限制对 Azure 中Cloud Volumes ONTAP系统的存储帐户的公共访问。通过禁用访问，您可以保护您的私有 IP 地址不被泄露，即使在同一个 VNet 内，也需要遵守您组织的安全策略。此选项还会禁用Cloud Volumes ONTAP系统的数据分层，并且适用于单节点和高可用性对。

"安全组规则" 。

部署**Cloud Volumes ONTAP**后启用 **WORM**

现在，您可以使用BlueXP在现有的Cloud Volumes ONTAP系统上激活一次写入、多次读取 (WORM) 存储。此功能为您提供了在工作环境中启用 WORM 的灵活性，即使在创建期间未启用 WORM。一旦启用，您就无法禁用 WORM。

"在Cloud Volumes ONTAP工作环境中启用 WORM"

2024年10月25日

已更新 **Google Cloud** 支持的虚拟机列表，以符合最佳实践

在 Google Cloud 中部署Cloud Volumes ONTAP的新实例时， BlueXP上不再可选择 n1 系列机器。n1 系列机器将保留，并且仅在较旧的现有系统中得到支持。从 9.8 版本开始，Google Cloud 才支持Cloud Volumes ONTAP的新部署。我们建议您切换到与Cloud Volumes ONTAP 9.8 及更高版本兼容的 n2 系列机器类型。然而，n1 系列机器将可用于通过 API 执行的新部署。

"Google Cloud 中支持的配置" 。

私有模式下对 **Amazon Web Services** 的本地区域支持

BlueXP现在支持私有模式下的Cloud Volumes ONTAP高可用性 (HA) 部署的 AWS 本地区域。之前仅限于标准模式的支持现已扩展到包括私人模式。

在受限模式下使用BlueXP时不支持 AWS 本地区域。

有关具有 HA 部署的 AWS 本地区域的更多信息，请参阅"AWS 本地区域"。

2024年10月7日

增强用户升级版本选择的体验

从此版本开始，当您尝试使用BlueXP通知升级Cloud Volumes ONTAP，您将收到有关使用默认、最新和兼容版本的指导。此外，现在您可以选择与您的Cloud Volumes ONTAP实例兼容的最新补丁或主要版本，或者手动输入要升级的版本。

"升级Cloud Volumes ONTAP软件"

2024年9月9日

WORM 和 **ARP** 功能不再收费

WORM（一次写入多次读取）和 ARP（自主勒索软件保护）的内置数据保护和安全功能将通过Cloud Volumes ONTAP许可证免费提供。新的定价模式适用于 AWS、Azure 和 Google Cloud 的新旧 BYOL 和 PAYGO/市场订阅。基于容量和基于节点的许可证都将包含所有配置的 ARP 和 WORM，包括单节点和高可用性 (HA) 对，无需额外费用。

简化的定价为您带来以下好处：

- 当前包含 WORM 和 ARP 的帐户将不再对这些功能收取费用。今后，您的账单将仅收取容量使用费，就像此次变更之前一样。 WORM 和 ARP 将不再包含在您未来的账单中。
- 如果您当前的帐户不包含这些功能，您现在可以免费选择 WORM 和 ARP。
- 所有针对新账户的Cloud Volumes ONTAP产品均不收取 WORM 和 ARP 费用。

了解有关这些功能的更多信息：

- "为Cloud Volumes ONTAP启用NetApp勒索软件防护解决方案"
- "WORM存储"

2024年8月23日

AWS 现已支持加拿大西部地区

AWS 现已支持加拿大西部地区的Cloud Volumes ONTAP 9.12.1 GA 及更高版本。

有关所有地区的列表，请参阅 "AWS 下的全球区域地图"。

2024年8月22日

Cloud Volumes ONTAP 9.15.1 正式版

BlueXP现在可以在 AWS、Azure 和 Google Cloud 中部署和管理Cloud Volumes ONTAP 9.15.1 通用可用性版本。

"了解此版本Cloud Volumes ONTAP中包含的新功能" 。

2024年8月8日

Edge Cache 许可包已弃用

Edge Cache 基于容量的许可包将不再适用于Cloud Volumes ONTAP的未来部署。但是，您可以使用 API 来实现此功能。

Azure 中闪存缓存的最低版本支持

在 Azure 中配置 Flash Cache 所需的最低Cloud Volumes ONTAP版本是 9.13.1 GA。您只能使用ONTAP 9.13.1 GA 及更高版本在 Azure 中的Cloud Volumes ONTAP系统上部署 Flash Cache。

有关支持的配置，请参阅 "Azure 中支持的配置"。

市场订阅的免费试用已弃用

云提供商市场中按使用量付费订阅的 30 天自动免费试用或评估许可证将不再在Cloud Volumes ONTAP中提供。任何类型的市场订阅（PAYGO 或年度合同）的收费将从首次使用时激活，没有任何免费试用期。

2024年6月10日

Cloud Volumes ONTAP 9.15.0

BlueXP现在可以在 AWS、Azure 和 Google Cloud 中部署和管理Cloud Volumes ONTAP 9.15.0。

"了解此版本Cloud Volumes ONTAP中包含的新功能" 。

2024年5月17日

Amazon Web Services 本地区域支持

Cloud Volumes ONTAP HA 部署现已支持 AWS 本地区域。 AWS 本地区域是一种基础设施部署，其中存储、计算、数据库和其他精选 AWS 服务位于大城市和工业区附近。

> 在标准模式下使用BlueXP时支持 AWS 本地区域。目前，在受限模式或私有模式下使用BlueXP时不支持 AWS 本地区域。

有关具有 HA 部署的 AWS 本地区域的更多信息，请参阅 "AWS 本地区域"。

2024年4月23日

Azure 中支持多可用区域部署的新区域

以下区域现在支持 Azure 中适用于Cloud Volumes ONTAP 9.12.1 GA 及更高版本的 HA 多可用区域部署：

- 德国中西部
- 波兰中部
- 美国西部 3
- 以色列中心
- 意大利北部
- 加拿大中部

有关所有地区的列表，请参阅 "Azure 下的全球区域地图"。

Google Cloud 现已支持约翰内斯堡地区

约翰内斯堡地区(`africa-south1`Google Cloud 的Cloud Volumes ONTAP 9.12.1 GA 及更高版本现已支持区域。

有关所有地区的列表，请参阅 "Google Cloud 下的全球区域地图"。

不再支持卷模板和标签

您无法再从模板创建卷或编辑卷的标签。这些操作与BlueXP修复服务相关，但该服务已不再可用。

2024年3月8日

Amazon Instant Metadata Service v2 支持

在 AWS 中， Cloud Volumes ONTAP、Mediator 和 Connector 现在支持 Amazon Instant Metadata Service v2 (IMDSv2) 的所有功能。 IMDSv2 提供了增强的针对漏洞的保护。之前仅支持 IMDSv1。

如果您的安全策略需要，您可以将 EC2 实例配置为使用 IMDSv2。有关说明，请参阅 "用于管理现有连接器的BlueXP设置和管理文档"。

2024年3月5日

Cloud Volumes ONTAP 9.14.1 正式版

BlueXP现在可以在 AWS、Azure 和 Google Cloud 中部署和管理Cloud Volumes ONTAP 9.14.1 通用可用性版本。

"了解此版本Cloud Volumes ONTAP中包含的新功能" 。

2024年2月2日

Azure 中对 Edv5 系列 VM 的支持

从 9.14.1 版本开始， Cloud Volumes ONTAP现在支持以下 Edv5 系列虚拟机。

- E4ds_v5
- E8ds_v5
- E20s_v5
- E32ds_v5
- E48ds_v5
- E64ds_v5

"Azure 中支持的配置"

2024年1月16日

BlueXP中的补丁版本

BlueXP中仅提供针对Cloud Volumes ONTAP最新三个版本的补丁版本。

"升级Cloud Volumes ONTAP"

2024年1月8日

适用于 **Azure** 多可用区域的新 **VM**

从Cloud Volumes ONTAP 9.13.1 开始，以下 VM 类型支持 Azure 多个可用区域，用于新的和现有的高可用性对部署：

- L16s_v3
- L32s_v3
- L48s_v3
- L64s_v3

"Azure 中支持的配置"

2023年12月6日

Cloud Volumes ONTAP 9.14.1 RC1

BlueXP现在可以在 AWS、Azure 和 Google Cloud 中部署和管理Cloud Volumes ONTAP 9.14.1。

"了解此版本Cloud Volumes ONTAP中包含的新功能" 。

FlexVol volume最大限制为 **300 TiB**

现在，您可以使用 System Manager 和ONTAP CLI（从Cloud Volumes ONTAP 9.12.1 P2 和 9.13.0 P2 开始）以及在BlueXP （从Cloud Volumes ONTAP 9.13.1 开始）中创建最大大小为 300 TiB 的FlexVol volume。

- "AWS 中的存储限制"
- "Azure 中的存储限制"
- "Google Cloud 中的存储限制"

2023年12月5日

引入了以下变化。

Azure 中的新区域支持

单一可用区域区域支持
以下区域现在支持 Azure 中适用于Cloud Volumes ONTAP 9.12.1 GA 及更高版本的高可用性单可用区部署：

- 特拉维夫
- 米兰

多可用区域支持
以下区域现在支持 Azure 中适用于Cloud Volumes ONTAP 9.12.1 GA 及更高版本的高可用性多可用区部署：

- 印度中部
- 挪威东部
- 瑞士北部
- 南非北部
- 阿拉伯联合酋长国北部

有关所有地区的列表，请参阅 "Azure 下的全球区域地图"。

2023年11月10日

连接器 3.9.35 版本引入了以下更改。

Google Cloud 现已支持柏林地区

Google Cloud for Cloud Volumes ONTAP 9.12.1 GA 及更高版本现已支持柏林地区。

有关所有地区的列表，请参阅 "Google Cloud 下的全球区域地图"。

2023年11月8日

连接器 3.9.35 版本引入了以下更改。

AWS 现已支持特拉维夫地区

AWS 现已支持特拉维夫地区的Cloud Volumes ONTAP 9.12.1 GA 及更高版本。

有关所有地区的列表，请参阅 "AWS 下的全球区域地图"。

2023年11月1日

连接器 3.9.34 版本引入了以下更改。

Google Cloud 现已支持沙特阿拉伯地区

Google Cloud for Cloud Volumes ONTAP和 Connector for Cloud Volumes ONTAP 9.12.1 GA 及更高版本现已支持沙特阿拉伯地区。

有关所有地区的列表，请参阅 "Google Cloud 下的全球区域地图"。

2023年10月23日

连接器 3.9.34 版本引入了以下更改。

Azure 中支持 HA 多可用区部署的新区域

Azure 中的以下区域现在支持Cloud Volumes ONTAP 9.12.1 GA 及更高版本的高可用性多可用区部署：

- 澳大利亚东部
- 东亚
- 法国中部
- 北欧
- 卡塔尔中央
- 瑞典中央
- 西欧
- 美国西部 2

有关支持多个可用区的所有区域的列表，请参阅 "Azure 下的全球区域地图"。

2023年10月6日

连接器 3.9.34 版本引入了以下更改。

Cloud Volumes ONTAP 9.14.0

BlueXP现在可以在 AWS、Azure 和 Google Cloud 中部署和管理Cloud Volumes ONTAP 9.14.0 通用可用性版本。

"了解此版本Cloud Volumes ONTAP中包含的新功能" 。

2023年9月10日

连接器 3.9.33 版本引入了以下更改。

Azure 中对 Lsv3 系列 VM 的支持

从 9.13.1 版本开始，Azure 中的Cloud Volumes ONTAP现在支持 L48s_v3 和 L64s_v3 实例类型，用于在单个和多个可用区域中具有共享托管磁盘的单节点和高可用性对部署。这些实例类型支持 Flash Cache。

"查看 Azure 中Cloud Volumes ONTAP支持的配置" "查看 Azure 中Cloud Volumes ONTAP的存储限制"

2023年7月30日

连接器 3.9.32 版本引入了以下更改。

Google Cloud 中的 Flash Cache 和高写入速度支持

可以在 Google Cloud for Cloud Volumes ONTAP 9.13.1 及更高版本中单独启用闪存和高写入速度。所有受支持的实例类型均具有高写入速度。以下实例类型支持 Flash Cache：

- n2-标准-16
- n2-标准-32
- n2-标准-48
- n2-标准-64

您可以在单节点和高可用性对部署中单独或一起使用这些功能。

"在 Google Cloud 中启动Cloud Volumes ONTAP"

使用情况报告增强功能

现在可以对使用报告中显示的信息进行各种改进。以下是使用情况报告的增强功能：

- TiB 单位现在包含在列名中。
- 现在包含一个用于序列号的新“节点”字段。
- 存储虚拟机使用情况报告下现在包含一个新的“工作负载类型”列。
- 工作环境名称现在包含在存储虚拟机和卷使用报告中。
- 卷类型“文件”现在标记为“主（读/写）”。
- 卷类型“辅助”现在标记为“辅助 (DP)”。

有关使用情况报告的更多信息，请参阅 "下载使用情况报告"。

2023年7月26日

连接器 3.9.31 版本引入了以下更改。

Cloud Volumes ONTAP 9.13.1 正式版

BlueXP现在可以在 AWS、Azure 和 Google Cloud 中部署和管理Cloud Volumes ONTAP 9.13.1 通用可用性版本。

"了解此版本Cloud Volumes ONTAP中包含的新功能" 。

2023年7月2日

连接器 3.9.31 版本引入了以下更改。

支持 **Azure** 中的 **HA** 多可用区域部署

Azure 中的日本东部和韩国中部现在支持Cloud Volumes ONTAP 9.12.1 GA 及更高版本的 HA 多可用区域部署。

有关支持多个可用区的所有区域的列表，请参阅 "Azure 下的全球区域地图"。

自主勒索软件防护支持

Cloud Volumes ONTAP现已支持自主勒索软件防护 (ARP)。 Cloud Volumes ONTAP版本 9.12.1 及更高版本提供 ARP 支持。

要了解有关 ARP 与Cloud Volumes ONTAP 的更多信息，请参阅 "自主勒索软件防护"。

2023年6月26日

连接器 3.9.30 版本引入了以下更改。

Cloud Volumes ONTAP 9.13.1 RC1

BlueXP现在可以在 AWS、Azure 和 Google Cloud 中部署和管理Cloud Volumes ONTAP 9.13.1。

"了解此版本Cloud Volumes ONTAP中包含的新功能" 。

2023年6月4日

连接器 3.9.30 版本引入了以下更改。

Cloud Volumes ONTAP升级版本选择器更新

通过升级Cloud Volumes ONTAP页面，您现在可以选择升级到最新可用的Cloud Volumes ONTAP版本或旧版本。

要了解有关通过BlueXP升级Cloud Volumes ONTAP 的更多信息，请参阅 "升级Cloud Volumes ONTAP"。

2023年5月7日

连接器 3.9.29 版本引入了以下更改。

Google Cloud 现已支持卡塔尔地区

Google Cloud for Cloud Volumes ONTAP和 Connector for Cloud Volumes ONTAP 9.12.1 GA 及更高版本现已支持卡塔尔地区。

Azure 现已支持瑞典中部地区

Azure 现已支持瑞典中部地区的Cloud Volumes ONTAP以及Cloud Volumes ONTAP 9.12.1 GA 及更高版本的连

接器。

支持 **Azure** 澳大利亚东部的 **HA** 多可用性区域部署

Azure 中的澳大利亚东部区域现在支持Cloud Volumes ONTAP 9.12.1 GA 及更高版本的 HA 多可用区域部署。

充电使用情况明细

现在，您可以了解订阅基于容量的许可证时需要支付的费用。可以从BlueXP中的数字钱包下载以下类型的使用情况报告。使用情况报告提供您的订阅的容量详细信息，并告诉您如何为Cloud Volumes ONTAP订阅中的资源付费。可下载的报告可以轻松地与他人共享。

- Cloud Volumes ONTAP软件包使用情况
- 高级用法
- 存储虚拟机使用情况
- 卷使用情况

有关更多信息，请参阅 "管理基于容量的许可证" 。

现在，无需订阅市场即可访问**BlueXP**并显示通知

现在，只要您在没有市场订阅的情况下访问BlueXP中的Cloud Volumes ONTAP，就会显示一条通知。通知指出“此工作环境的市场订阅必须符合Cloud Volumes ONTAP条款和条件。”

AWS IAM 策略中为 **HA** 中介器添加了新权限

这些新的 AWS 权限已添加到Cloud Volumes ONTAP高可用性 (HA) 环境中 HA 中介器的 IAM 策略中：

- sts：AssumeRole
- ec2:描述子网

2023年4月4日

对 **AWS** 中国区域的支持

从Cloud Volumes ONTAP 9.12.1 GA 开始，AWS 现在支持中国地区，如下所示。

- 支持单节点系统。
- 支持直接从NetApp购买的许可证。

有关区域可用性，请参阅 "Cloud Volumes ONTAP的全球区域地图"。

2023年4月3日

连接器 3.9.28 版本引入了以下更改。

Google Cloud 现已支持都灵地区

Google Cloud for Cloud Volumes ONTAP和 Connector for Cloud Volumes ONTAP 9.12.1 GA 及更高版本现已支持都灵地区。

BlueXP digital wallet增强功能

BlueXP digital wallet现在显示您通过市场私人优惠购买的许可容量。

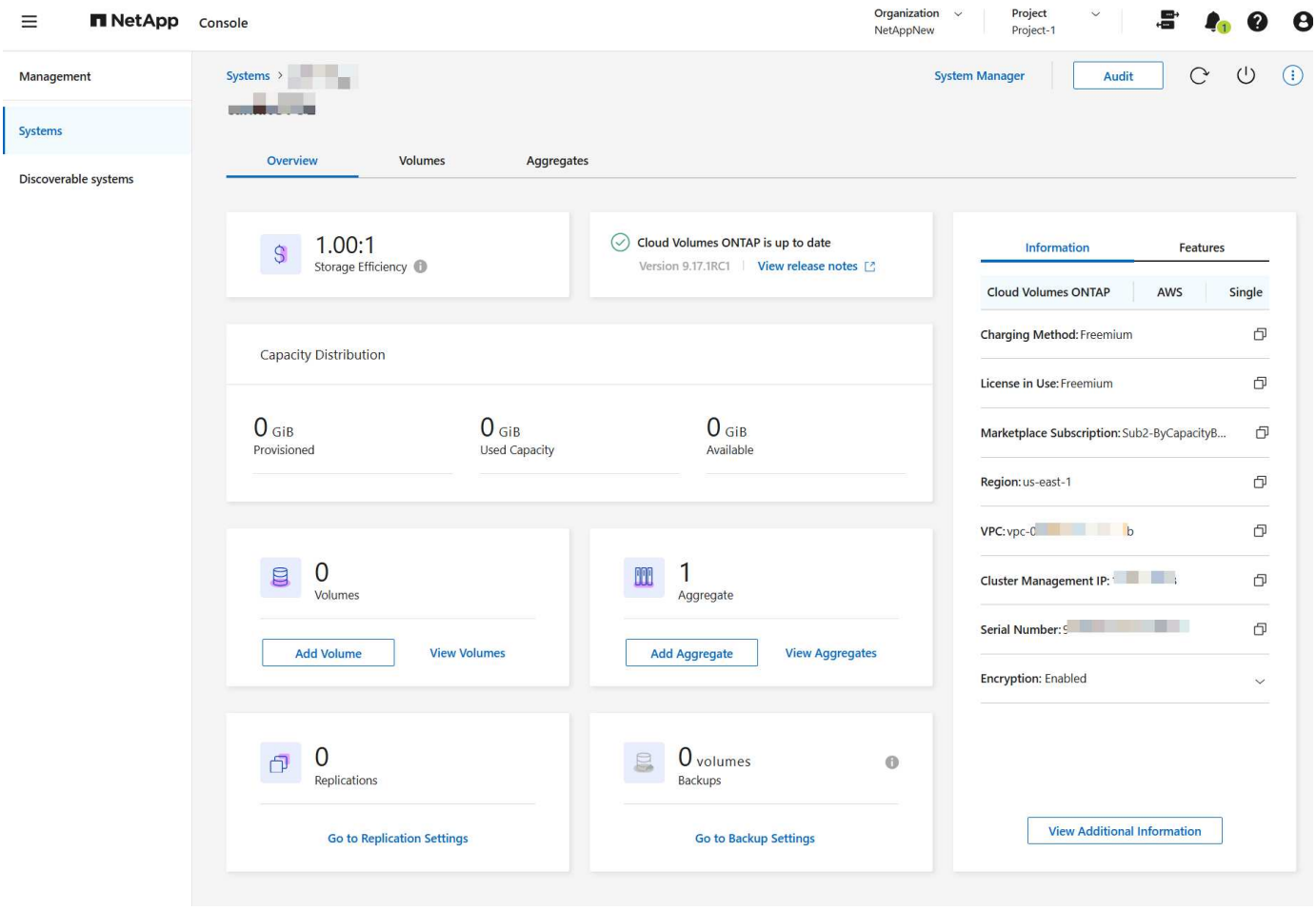
"了解如何查看账户中已消耗的容量" 。

支持在卷创建期间进行注释

此版本使您能够在使用 API 创建Cloud Volumes ONTAP FlexGroup卷或FlexVol volume时发表评论。

BlueXP用户界面针对Cloud Volumes ONTAP概览、卷和聚合页面进行了重新设计

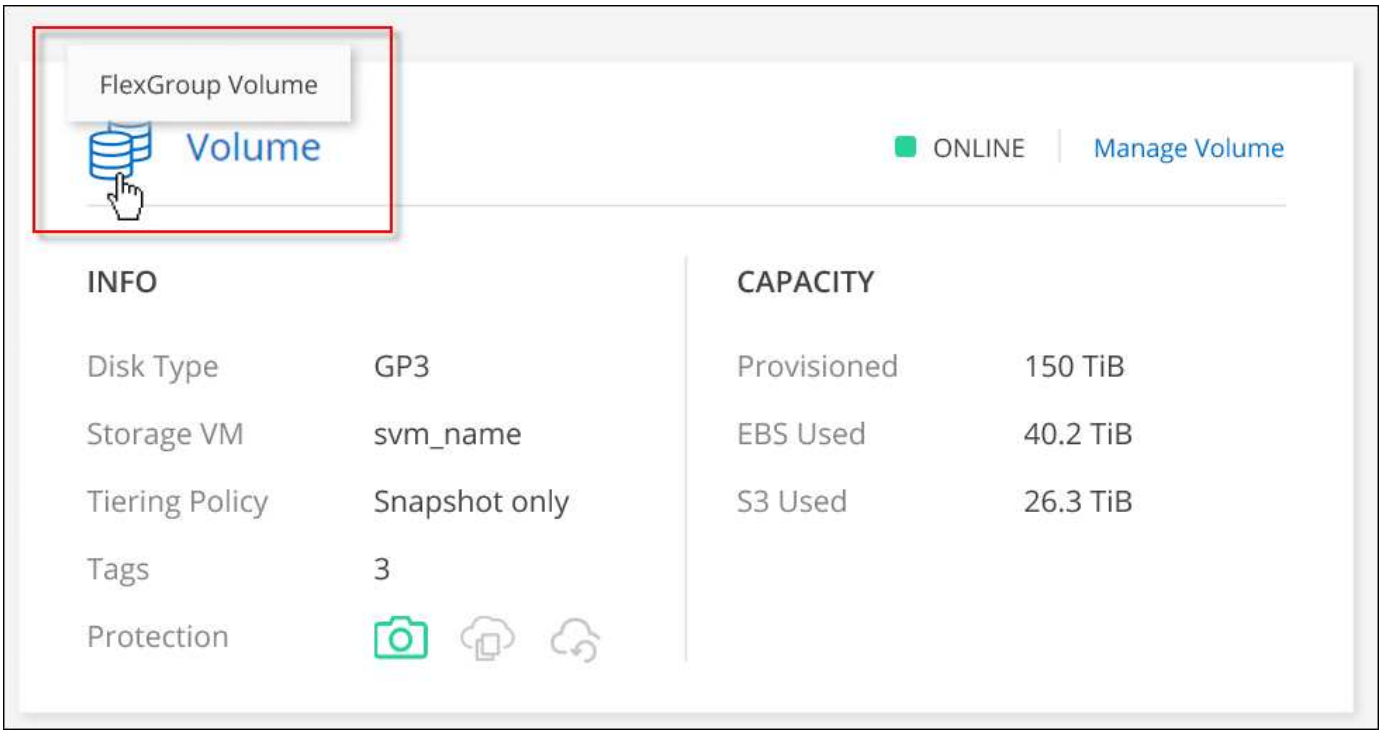
BlueXP现在重新设计了Cloud Volumes ONTAP概览、卷和聚合页面的用户界面。基于图块的设计在每个图块中呈现更全面的信息，以获得更好的用户体验。



可通过Cloud Volumes ONTAP查看FlexGroup Volumes

现在可以通过BlueXP中重新设计的卷磁贴查看通过ONTAP System Manager 或ONTAP CLI 直接创建的FlexGroup卷。与为FlexVol卷提供的信息相同， BlueXP通过专用卷图块提供已创建的FlexGroup卷的详细信息。

目前，您只能查看BlueXP下的现有FlexGroup卷。 BlueXP中创建FlexGroup卷的功能尚不可用，但计划在未来版本中提供。



"了解有关查看已创建的FlexGroup卷的更多信息。"

2023年3月13日

Azure 对中国区域的支持

现在，中国北方 3 区域支持在 Azure 中单节点部署Cloud Volumes ONTAP 9.12.1 GA 和 9.13.0 GA。这些地区仅支持直接从NetApp购买的许可证（BYOL 许可证）。

仅 9.12.1 GA 和 9.13.0 GA 支持在中国区域全新部署Cloud Volumes ONTAP 。您可以将这些版本升级到Cloud Volumes ONTAP的更高补丁和版本。如果您想在中国地区部署更高版本的Cloud Volumes ONTAP ，请联系NetApp支持。

有关区域可用性，请参阅 "Cloud Volumes ONTAP的全球区域地图"。

2023年3月5日

连接器 3.9.27 版本引入了以下更改。

Cloud Volumes ONTAP 9.13.0

BlueXP现在可以在 AWS、Azure 和 Google Cloud 中部署和管理Cloud Volumes ONTAP 9.13.0。

"了解此版本Cloud Volumes ONTAP中包含的新功能" 。

Azure 中的 16 TiB 和 32 TiB 支持

Cloud Volumes ONTAP现在支持 16 TiB 和 32 TiB 磁盘大小，用于在 Azure 中的托管磁盘上运行的高可用性部署。

详细了解 "Azure 中支持的磁盘大小"。

MTEKM 许可证

多租户加密密钥管理 (MTEKM) 许可证现在包含在运行 9.12.1 GA 或更高版本的新旧Cloud Volumes ONTAP系统中。

多租户外部密钥管理使单个存储虚拟机 (SVM) 能够在使用NetApp卷加密时通过 KMIP 服务器维护自己的密钥。

"了解如何使用NetApp加密解决方案加密卷" 。

支持无互联网环境

现在，任何与互联网完全隔离的云环境都支持Cloud Volumes ONTAP 。这些环境仅支持基于节点的许可（BYOL）。不支持基于容量的许可。首先，手动安装 Connector 软件，登录到 Connector 上运行的BlueXP控制台，将您的 BYOL 许可证添加到BlueXP digital wallet，然后部署Cloud Volumes ONTAP。

- "在没有互联网访问的位置安装连接器"
- "访问连接器上的BlueXP控制台"
- "添加未分配的许可证"

Google Cloud 中的 Flash Cache 和高写入速度

现在， Cloud Volumes ONTAP 9.13.0 版本的选定实例可以支持闪存、高写入速度和 8,896 字节的高最大传输单元 (MTU)。

详细了解 "Google Cloud 许可证支持的配置"。

2023年2月5日

连接器 3.9.26 版本引入了以下更改。

在 AWS 中创建置放群组

现在可以使用新的配置设置来通过 AWS HA 单可用区 (AZ) 部署创建放置组。现在您可以选择绕过失败的放置组创建并允许 AWS HA 单可用区部署成功完成。

有关如何配置置放群组创建设置的详细信息，请参阅 "为 AWS HA 单可用区配置置放群组创建"。

私有 DNS 区域配置更新

现在可以使用新的配置设置，以便您在使用 Azure Private Links 时避免在私有 DNS 区域和虚拟网络之间创建链接。默认情况下启用创建。

"向BlueXP提供有关 Azure 私有 DNS 的详细信息"

WORM存储和数据分层

现在，创建Cloud Volumes ONTAP 9.8 系统或更高版本时，您可以同时启用数据分层和 WORM 存储。使用 WORM 存储启用数据分层允许您将数据分层到云中的对象存储。

"了解 WORM 存储。"

2023年1月1日

连接器 3.9.25 版本引入了以下更改。

Google Cloud 中提供的许可包

Google Cloud Marketplace 中为Cloud Volumes ONTAP提供优化和基于 Edge Cache 容量的许可包，可作为即用即付产品或年度合同使用。

参考 "Cloud Volumes ONTAP许可"。

Cloud Volumes ONTAP的默认配置

多租户加密密钥管理 (MTEKM) 许可证不再包含在新的Cloud Volumes ONTAP部署中。

有关随Cloud Volumes ONTAP自动安装的ONTAP功能许可证的更多信息，请参阅 "Cloud Volumes ONTAP的默认配置"。

2022年12月15日

Cloud Volumes ONTAP 9.12.0

BlueXP现在可以在 AWS 和 Google Cloud 中部署和管理Cloud Volumes ONTAP 9.12.0。

"了解此版本Cloud Volumes ONTAP中包含的新功能" 。

2022年12月8日

Cloud Volumes ONTAP 9.12.1

BlueXP现在可以部署和管理Cloud Volumes ONTAP 9.12.1，其中包括对新功能和额外云提供商区域的支持。

"了解此版本Cloud Volumes ONTAP中包含的新功能"

2022年12月4日

连接器 3.9.24 版本引入了以下更改。

WORM + 云备份现在可在Cloud Volumes ONTAP创建期间使用

现在可以在Cloud Volumes ONTAP创建过程中激活一次写入、多次读取 (WORM) 和云备份功能。

Google Cloud 现已支持以色列地区

Google Cloud for Cloud Volumes ONTAP和 Connector for Cloud Volumes ONTAP 9.11.1 P3 及更高版本现已支持以色列地区。

2022年11月15日

连接器 3.9.23 版本引入了以下更改。

Google Cloud 中的**ONTAP S3** 许可证

现在，在 Google Cloud Platform 中运行 9.12.1 或更高版本的新版和现有Cloud Volumes ONTAP系统均包含ONTAP S3 许可证。

"ONTAP文档：了解如何配置和管理 S3 对象存储服务"

2022年11月6日

连接器 3.9.23 版本引入了以下更改。

在 **Azure** 中移动资源组

现在，您可以将工作环境从同一 Azure 订阅中的一个资源组移动到 Azure 中的另一个资源组。

有关更多信息，请参阅 "移动资源组" 。

NDMP 副本认证

NDMP-copy 现已通过认证，可与 Cloud Volume ONTAP一起使用。

有关如何配置和使用 NDMP 的信息，请参阅 "ONTAP文档：NDMP 配置概述"。

Azure 的托管磁盘加密支持

已添加新的 Azure 权限，现在允许您在创建时加密所有托管磁盘。

有关此新功能的更多信息，请参阅 "设置Cloud Volumes ONTAP以在 Azure 中使用客户管理的密钥"。

2022年9月18日

连接器 3.9.22 版本引入了以下更改。

数字钱包增强功能

- 数字钱包现在显示优化 I/O 许可包的摘要以及您帐户中Cloud Volumes ONTAP系统的预配置 WORM 容量。

  这些详细信息可以帮助您更好地了解收费方式以及是否需要购买额外的容量。

  "了解如何查看账户中已消耗的容量" 。

- 您现在可以从一种充电方式更改为优化充电方式。

"了解如何更改充电方式" 。

优化成本和性能

您现在可以直接从 Canvas 优化Cloud Volumes ONTAP系统的成本和性能。

选择工作环境后，您可以选择“优化成本和性能”选项来更改Cloud Volumes ONTAP的实例类型。选择较小规模的实例可以帮助您降低成本，而更改为较大规模的实例可以帮助您优化性能。

[选择Cloud Volumes ONTAP系统后，可从 Canvas 中获取“优化成本和性能”选项的屏幕截图。]

AutoSupport 通知

如果Cloud Volumes ONTAP系统无法发送AutoSupport消息， BlueXP现在将生成通知。通知中包含一个链接，您可以使用该链接来解决网络问题。

2022年7月31日

连接器 3.9.21 版本引入了以下更改。

MTEKM 许可证

多租户加密密钥管理 (MTEKM) 许可证现在包含在运行 9.11.1 或更高版本的新旧Cloud Volumes ONTAP系统中。

多租户外部密钥管理使单个存储虚拟机 (SVM) 能够在使用NetApp卷加密时通过 KMIP 服务器维护自己的密钥。

"了解如何使用NetApp加密解决方案加密卷" 。

代理服务器

如果没有可用的出站互联网连接来发送AutoSupport消息， BlueXP现在会自动配置您的Cloud Volumes ONTAP系统以使用连接器作为代理服务器。

AutoSupport主动监控系统的健康状况并向NetApp技术支持发送消息。

唯一的要求是确保连接器的安全组允许通过端口 3128 进行入站连接。部署连接器后，您需要打开此端口。

更改充电方式

您现在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 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 包。此功能可通过数字钱包获得。

"了解如何更改充电方式" 。

安全组增强

当您创建Cloud Volumes ONTAP工作环境时，用户界面现在允许您选择是否希望预定义安全组仅允许所选网络内的流量（推荐）或所有网络内的流量。

[屏幕截图显示了选择安全组时工作环境向导中可用的“允许内部流量”选项。]

2022年7月18日

Azure 中的新许可包

当您通过 Azure 市场订阅付款时，Azure 中的Cloud Volumes ONTAP可以使用两个新的基于容量的许可包：

- 优化：分别支付配置容量和 I/O 操作的费用
- **Edge Cache**：许可 "Cloud Volumes 边缘缓存"

"了解有关这些许可包的更多信息" 。

2022年7月3日

连接器 3.9.20 版本引入了以下更改。

数字钱包

数字钱包现在显示您帐户中消耗的总容量以及许可包消耗的容量。这可以帮助您了解收费方式以及是否需要购买额外的容量。

[显示基于容量的许可证的数字钱包页面的屏幕截图。该页面概述了您帐户中已消耗的容量，然后按许可包细分了已消耗的容量。]

弹性卷增强

现在，从用户界面创建Cloud Volumes ONTAP工作环境时， BlueXP支持 Amazon EBS Elastic Volumes 功能。使用 gp3 或 io1 磁盘时，弹性卷功能默认启用。您可以根据您的存储需求选择初始容量，并在部署Cloud Volumes ONTAP后进行修改。

"了解有关 AWS 弹性卷支持的更多信息" 。

AWS 中的ONTAP S3 许可证

现在，在 AWS 中运行 9.11.0 或更高版本的新版和现有Cloud Volumes ONTAP系统均包含ONTAP S3 许可证。

"ONTAP文档：了解如何配置和管理 S3 对象存储服务"

新的 Azure 云区域支持

从 9.10.1 版本开始，Azure West US 3 区域现在支持Cloud Volumes ONTAP 。

"查看Cloud Volumes ONTAP支持区域的完整列表"

Azure 中的ONTAP S3 许可证

现在，在 Azure 中运行 9.9.1 或更高版本的新版和现有Cloud Volumes ONTAP系统均包含ONTAP S3 许可证。

"ONTAP文档：了解如何配置和管理 S3 对象存储服务"

2022年6月7日

连接器 3.9.19 版本引入了以下更改。

Cloud Volumes ONTAP 9.11.1

BlueXP现在可以部署和管理Cloud Volumes ONTAP 9.11.1，其中包括对新功能和额外云提供商区域的支持。

"了解此版本Cloud Volumes ONTAP中包含的新功能"

新的高级视图

如果您需要对Cloud Volumes ONTAP执行高级管理，则可以使用ONTAP System Manager（它是ONTAP系统提供的管理界面）来执行此操作。我们已将系统管理器界面直接包含在BlueXP中，这样您无需离开BlueXP即可进行高级管理。

此高级视图可作为Cloud Volumes ONTAP 9.10.0 及更高版本的预览版使用。我们计划在即将发布的版本中完善这种体验并增加增强功能。请使用产品内聊天向我们发送反馈。

"了解有关高级视图的更多信息" 。

支持 **Amazon EBS** 弹性卷

通过Cloud Volumes ONTAP聚合支持 Amazon EBS Elastic Volumes 功能可提供更好的性能和额外的容量，同时使BlueXP能够根据需要自动增加底层磁盘容量。

从 *new* Cloud Volumes ONTAP 9.11.0 系统以及 gp3 和 io1 EBS 磁盘类型开始，可以支持弹性卷。

"了解有关弹性卷支持的更多信息" 。

请注意，对弹性卷的支持需要为连接器授予新的 AWS 权限：

```
"ec2:DescribeVolumesModifications",
"ec2:ModifyVolume",
```

确保为您添加到BlueXP 的每组 AWS 凭证提供这些权限。 "查看最新的 AWS 连接器策略" 。

支持在共享 **AWS** 子网中部署 **HA** 对

Cloud Volumes ONTAP 9.11.1 包括对 AWS VPC 共享的支持。此版本的连接器使您能够在使用 API 时在 AWS 共享子网中部署 HA 对。

"了解如何在共享子网中部署 HA 对" 。

使用服务端点时网络访问受限

当使用 VNet 服务端点在Cloud Volumes ONTAP和存储帐户之间建立连接时， BlueXP现在会限制网络访问。如果您禁用 Azure Private Link 连接， BlueXP将使用服务端点。

"了解有关 Azure Private Link 与Cloud Volumes ONTAP连接的更多信息" 。

支持在 **Google Cloud** 中创建存储虚拟机

从 9.11.1 版本开始，Google Cloud 中的Cloud Volumes ONTAP现在支持多个存储虚拟机。从此版本的连接器开始， BlueXP允许您使用 API 在 Google Cloud 中的Cloud Volumes ONTAP HA 对上创建存储虚拟机。

要支持创建存储虚拟机，需要为连接器授予新的 Google Cloud 权限：

```
- compute.instanceGroups.get
- compute.addresses.get
```

请注意，必须使用 ONTAP CLI 或 System Manager 在单节点系统上创建存储 VM。

- "详细了解 Google Cloud 中的存储虚拟机限制"
- "了解如何在 Google Cloud 中为Cloud Volumes ONTAP创建数据服务存储虚拟机"

2022年5月2日

连接器 3.9.18 版本引入了以下更改。

Cloud Volumes ONTAP 9.11.0

BlueXP现在可以部署和管理Cloud Volumes ONTAP 9.11.0。

"了解此版本Cloud Volumes ONTAP中包含的新功能" 。

增强调解员升级

当BlueXP升级 HA 对的中介器时，它会在删除启动磁盘之前验证是否有新的中介器映像可用。此更改可确保升级过程不成功时中介仍可继续成功运行。

K8s 选项卡已删除

K8s 选项卡在之前的版本中已被弃用，现在已被删除。

Azure 年度合同

现在可以通过年度合同在 Azure 中使用 Essentials 和 Professional 套餐。您可以联系NetApp销售代表购买年度合同。该合同在 Azure 市场中以私人优惠形式提供。

NetApp与您共享私人优惠后，您可以在创建工作环境期间从 Azure 市场订阅时选择年度计划。

"了解有关许可的更多信息" 。

S3 Glacier 即时检索

现在，您可以将分层数据存储在 Amazon Simple Storage Service (Amazon S3) Glacier Instant Retrieval 存储类中。

"了解如何更改分层数据的存储类别" 。

连接器所需的新 **AWS** 权限

在单个可用区 (AZ) 中部署 HA 对时，现在需要以下权限来创建 AWS 分布置放群组：

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

现在需要这些权限来优化BlueXP创建放置组的方式。

确保为您添加到BlueXP 的每组 AWS 凭证提供这些权限。 "查看最新的 AWS 连接器策略" 。

新的 **Google Cloud** 区域支持

从 9.10.1 版本开始，以下 Google Cloud 区域现在支持Cloud Volumes ONTAP：

- 德里 (asia-south2)
- 墨尔本 (australia-southeast2)
- 米兰 (europe-west8) - 仅限单节点
- 圣地亚哥 (southamerica-west1) - 仅限单节点

"查看Cloud Volumes ONTAP支持区域的完整列表"

Google Cloud 支持 **n2-standard-16**

从 9.10.1 版本开始，Google Cloud 中的Cloud Volumes ONTAP现在支持 n2-standard-16 机器类型。

"查看 Google Cloud 中Cloud Volumes ONTAP支持的配置"

Google Cloud 防火墙政策的增强功能

- 当您在 Google Cloud 中创建Cloud Volumes ONTAP HA 对时， BlueXP现在将显示 VPC 中所有现有的防火墙策略。

  以前， BlueXP不会显示 VPC-1、VPC-2 或 VPC-3 中没有目标标签的任何策略。

- 现在，在 Google Cloud 中创建 Cloud Volumes ONTAP 单节点系统时，您可以选择是否希望预定义的防火墙策略仅允许所选 VPC 内的流量（推荐）或所有 VPC。

Google Cloud 服务帐户的增强功能

当您选择与Cloud Volumes ONTAP一起使用的 Google Cloud 服务帐户时， BlueXP现在会显示与每个服务帐户关联的电子邮件地址。查看电子邮件地址可以更容易区分同名的服务帐户。

[服务帐户字段的屏幕截图]

2022年4月3日

系统管理器链接已删除

我们删除了之前在Cloud Volumes ONTAP工作环境中可用的系统管理器链接。

您仍然可以通过在与Cloud Volumes ONTAP系统连接的 Web 浏览器中输入集群管理 IP 地址来连接到系统管理器。 "了解有关连接到系统管理器的更多信息" 。

WORM存储收费

现在，优惠特价已经过期，您现在需要为使用 WORM 存储付费。根据 WORM 卷的总配置容量按小时收费。这适用于新的和现有的Cloud Volumes ONTAP系统。

"了解 WORM 存储的定价" 。

2022年2月27日

连接器 3.9.16 版本引入了以下更改。

重新设计的卷向导

我们最近推出的创建新卷向导现在可在从“高级分配”选项在特定聚合上创建卷时使用。

"了解如何在特定聚合上创建卷" 。

2022年2月9日

市场更新

- 现在，所有云提供商市场均提供 Essentials 套餐和 Professional 套餐。

  这些按容量收费的方法使您能够按小时付费或直接从云提供商处购买年度合同。您仍然可以选择直接从NetApp购买按容量许可证。

  如果您在云市场中已有订阅，那么您也会自动订阅这些新产品。部署新的Cloud Volumes ONTAP工作环境时，您可以选择按容量收费。

  如果您是新客户， BlueXP会在您创建新的工作环境时提示您订阅。

- 所有云提供商市场的按节点许可均已弃用，并且不再适用于新订户。这包括年度合同和小时订阅（探索、标准和高级）。

  此收费方式仍适用于拥有有效订阅的现有客户。

"了解有关Cloud Volumes ONTAP许可选项的更多信息" 。

2022年2月6日

交换未分配的许可证

如果您有未分配的基于节点的Cloud Volumes ONTAP许可证且尚未使用，您现在可以将其转换为 Cloud Backup 许可证、Cloud Data Sense 许可证或 Cloud Tiering 许可证来交换该许可证。

此操作将撤销Cloud Volumes ONTAP许可证，并为该服务创建具有相同到期日期的等值美元许可证。

"了解如何交换未分配的基于节点的许可证" 。

2022年1月30日

连接器 3.9.15 版本引入了以下更改。

重新设计的许可选择

我们重新设计了创建新的Cloud Volumes ONTAP工作环境时的许可选择屏幕。这些变化凸显了 2021 年 7 月推出的按容量收费方法，并支持通过云提供商市场推出的即将推出的产品。

数字钱包更新

我们通过将Cloud Volumes ONTAP许可证整合到一个选项卡中来更新*数字钱包*。

2022年1月2日

连接器 3.9.14 版本引入了以下更改。

支持其他 **Azure VM** 类型

从 9.10.1 版本开始， Cloud Volumes ONTAP现在支持 Microsoft Azure 中的以下 VM 类型：

- E4ds_v4
- E8ds_v4
- E32ds_v4
- E48ds_v4

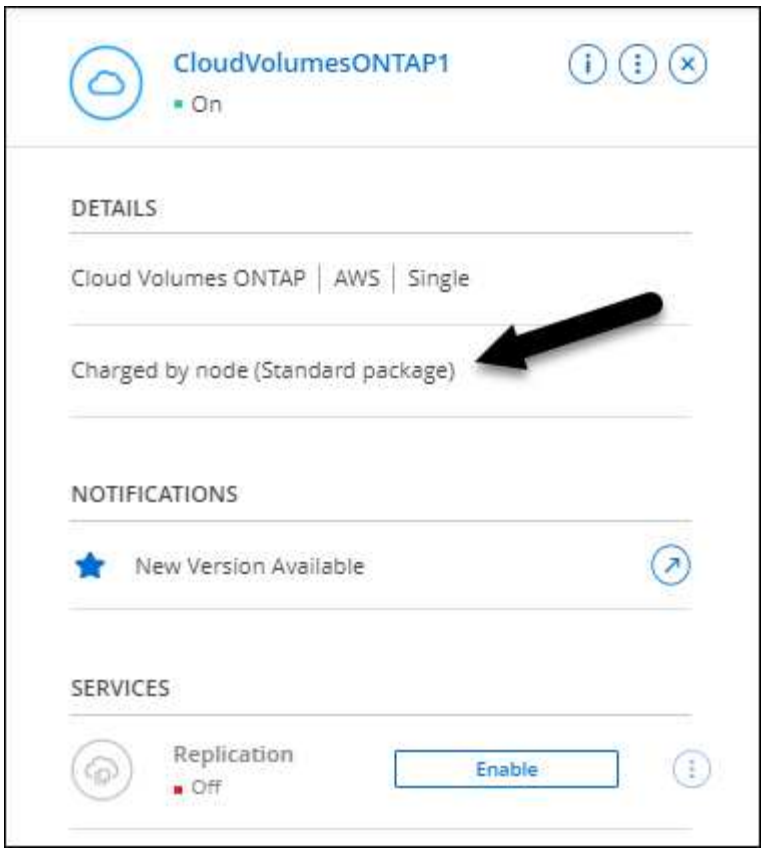
前往 "Cloud Volumes ONTAP发行说明"有关支持的配置的更多详细信息。

FlexClone收费更新

如果你使用 "基于容量的许可证"对于Cloud Volumes ONTAP，您不再需要为FlexClone卷使用的容量付费。

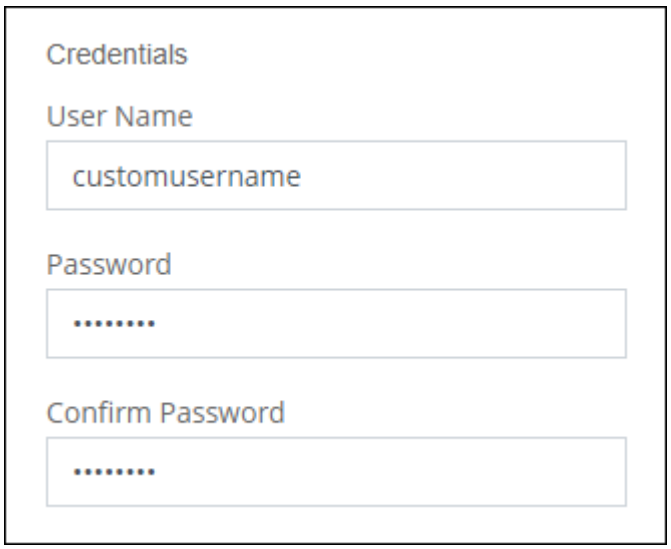
充电方式现已显示

BlueXP现在在 Canvas 的右侧面板中显示每个Cloud Volumes ONTAP工作环境的收费方式。



选择你的用户名

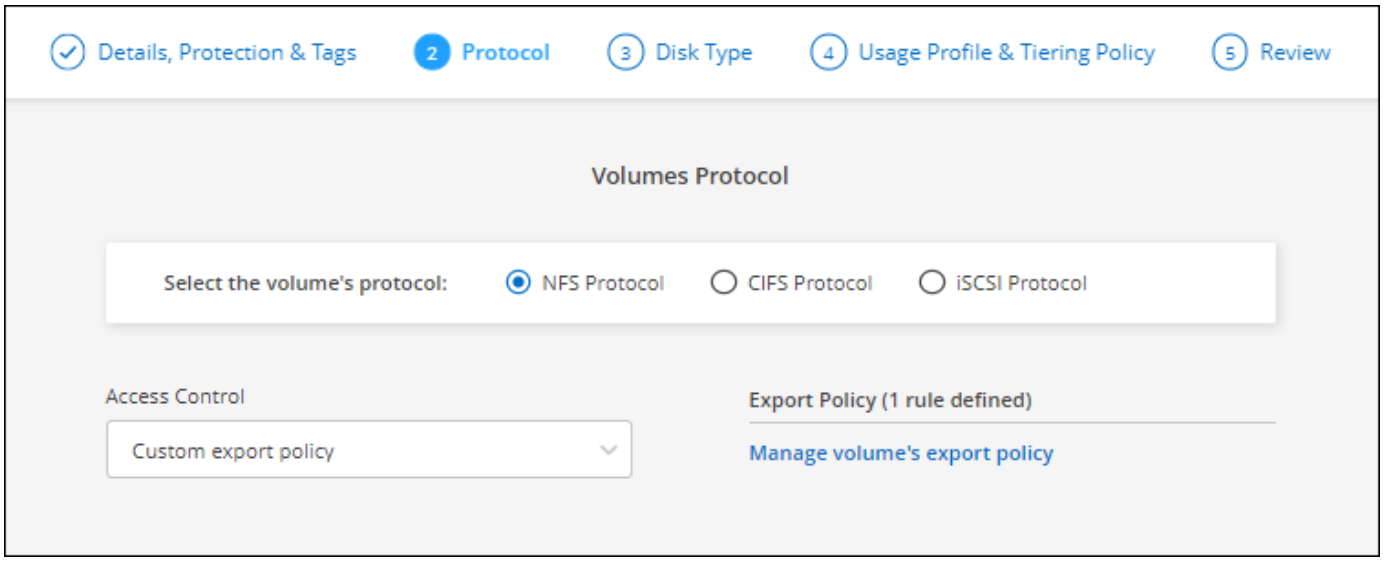
当您创建Cloud Volumes ONTAP工作环境时，您现在可以选择输入您的首选用户名，而不是默认的管理员用户名。



卷创建增强功能

我们对卷创建做了一些增强：

- 我们重新设计了创建卷向导，以便于使用。
- 您现在可以为 NFS 选择自定义导出策略。



2021年11月28日

连接器 3.9.13 版本引入了以下更改。

Cloud Volumes ONTAP 9.10.1

BlueXP现在可以部署和管理Cloud Volumes ONTAP 9.10.1。

"了解此版本Cloud Volumes ONTAP中包含的新功能" 。

NetApp Keystone订阅

您现在可以使用Keystone订阅来支付Cloud Volumes ONTAP HA 对的费用。

Keystone订阅是一种按需付费的订阅式服务，为那些喜欢 OpEx 消费模式而非前期资本支出或租赁的用户提供无缝的混合云体验。

您可以从BlueXP部署的所有新版本的Cloud Volumes ONTAP均支持Keystone订阅。

- "了解有关NetApp Keystone订阅的更多信息" 。
- "了解如何在BlueXP中开始使用Keystone订阅" 。

新的 AWS 区域支持

Cloud Volumes ONTAP现已在 AWS 亚太地区（大阪）区域（ap-northeast-3）获得支持。

端口减少

对于单节点系统和 HA 对，端口 8023 和 49000 不再在 Azure 中的 Cloud Volumes ONTAP 系统上打开。

此更改适用于从 Connector 3.9.13 版本开始的_new_ Cloud Volumes ONTAP系统。

2021年10月4日

连接器 3.9.11 版本引入了以下更改。

Cloud Volumes ONTAP 9.10.0

BlueXP现在可以部署和管理Cloud Volumes ONTAP 9.10.0。

"了解此版本Cloud Volumes ONTAP中包含的新功能" 。

减少部署时间

当启用正常写入速度时，我们减少了在 Microsoft Azure 或 Google Cloud 中部署Cloud Volumes ONTAP工作环境所需的时间。现在部署时间平均缩短了 3-4 分钟。

2021年9月2日

连接器 3.9.10 版本引入了以下更改。

Azure 中的客户管理加密密钥

使用以下方式在 Azure 中的Cloud Volumes ONTAP上自动加密数据 "Azure 存储服务加密"使用 Microsoft 管理的密钥。但现在您可以通过完成以下步骤来使用您自己的客户管理的加密密钥：

1. 从 Azure 创建一个密钥保管库，然后在该保管库中生成一个密钥。
2. 从BlueXP中，使用 API 创建使用密钥的Cloud Volumes ONTAP工作环境。

"了解有关这些步骤的更多信息" 。

2021年7月7日

连接器 3.9.8 版本引入了以下更改。

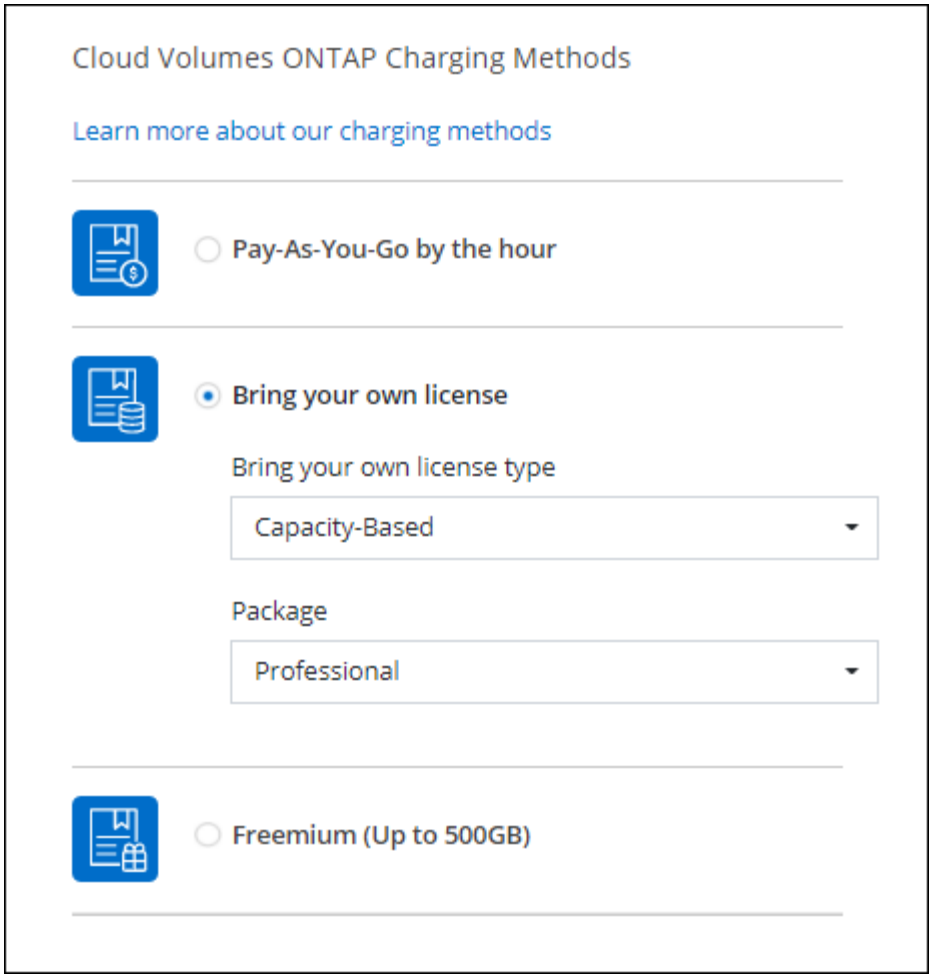
新的充电方式

Cloud Volumes ONTAP有新的计费方式。

- 基于容量的 **BYOL**：基于容量的许可证使您能够按 TiB 容量支付Cloud Volumes ONTAP费用。该许可证与您的NetApp帐户相关联，只要您的许可证提供足够的容量，您就可以创建多个Cloud Volumes ONTAP系统。基于容量的许可以包的形式提供，可以是_Essentials_ 或_Professional_。
- 免费增值服务：免费增值服务使您能够免费使用NetApp的所有Cloud Volumes ONTAP功能（仍需支付云提供商费用）。每个系统的配置容量限制为 500 GiB，并且没有支持合同。您最多可以拥有 10 个免费增值系统。

  "了解有关这些许可选项的更多信息" 。

  以下是您可以选择的充电方法的示例：



WORM 存储可供一般使用

一次写入，多次读取 (WORM) 存储不再处于预览阶段，现在可以通过Cloud Volumes ONTAP供一般使用。 "了解有关 WORM 存储的更多信息" 。

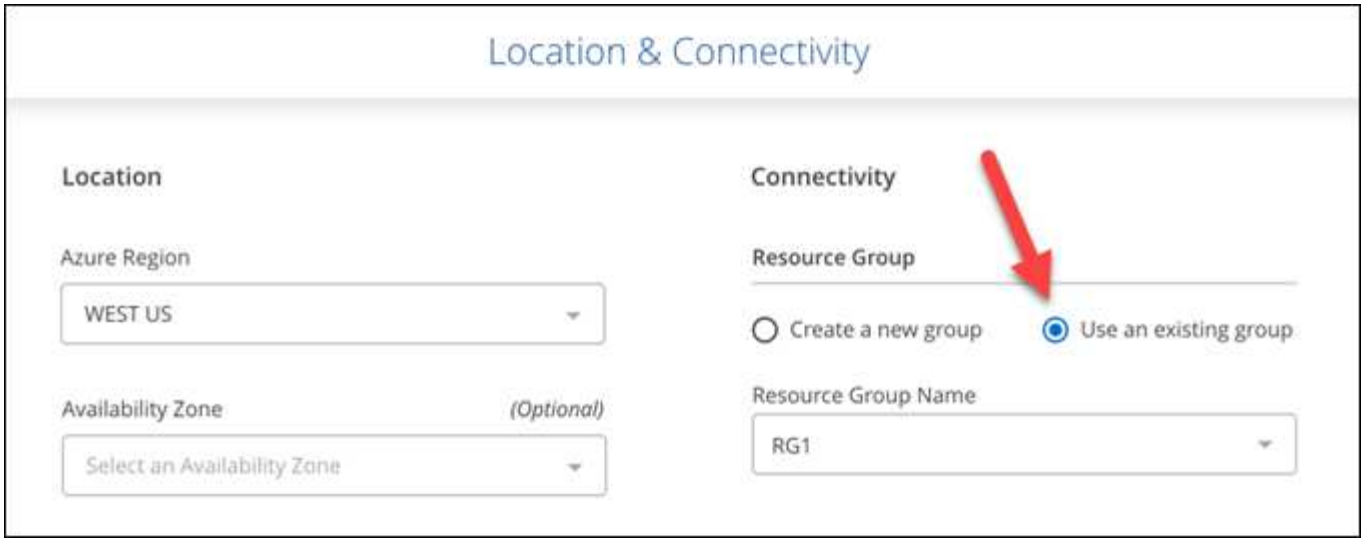
AWS 中对 **m5dn.24xlarge** 的支持

从 9.9.1 版本开始， Cloud Volumes ONTAP现在支持 m5dn.24xlarge 实例类型，并具有以下收费方式：PAYGO Premium、自带许可证 (BYOL) 和 Freemium。

"查看 AWS 中Cloud Volumes ONTAP支持的配置" 。

选择现有的 **Azure** 资源组

在 Azure 中创建Cloud Volumes ONTAP系统时，您现在可以选择为 VM 及其相关资源选择一个现有资源组。



如果部署失败或删除，以下权限使BlueXP能够从资源组中删除Cloud Volumes ONTAP资源：

```
"Microsoft.Network/privateEndpoints/delete",
"Microsoft.Compute/availabilitySets/delete",
```

确保向添加到BlueXP 的每组 Azure 凭据提供这些权限。 "查看 Azure 的最新连接器策略" 。

Azure 现已禁用 **Blob** 公共访问

作为一项安全增强功能， BlueXP现在在为Cloud Volumes ONTAP创建存储帐户时禁用 **Blob** 公共访问。

Azure Private Link 增强功能

默认情况下， BlueXP现在在新的Cloud Volumes ONTAP系统的启动诊断存储帐户上启用 Azure Private Link 连接。

这意味着Cloud Volumes ONTAP的所有存储帐户现在都将使用私有链接。

"了解有关使用 Azure Private Link 和Cloud Volumes ONTAP 的更多信息" 。

Google Cloud 中的平衡持久磁盘

从 9.9.1 版本开始， Cloud Volumes ONTAP现在支持平衡持久磁盘 (pd-balanced)。

这些 SSD 通过提供较低的每 GiB IOPS 来平衡性能和成本。

Google Cloud 不再支持 **custom-4-16384**

新的Cloud Volumes ONTAP系统不再支持 custom-4-16384 机器类型。

如果您现有的系统正在此机器类型上运行，您可以继续使用它，但我们建议切换到 n2-standard-4 机器类型。

"查看 Google Cloud 中Cloud Volumes ONTAP支持的配置"。

2021年5月30日

连接器 3.9.7 版本引入了以下更改。

AWS 中的新专业套餐

新的专业套餐使您能够使用 AWS Marketplace 的年度合同捆绑Cloud Volumes ONTAP和Cloud Backup Service。按 TiB 付款。此订阅不允许您备份本地数据。

如果您选择此付款方式，您可以通过 EBS 磁盘和分层到 S3 对象存储（单节点或 HA）为每个Cloud Volumes ONTAP系统配置最多 2 PiB。

前往 "AWS Marketplace 页面"查看定价详情并前往 "Cloud Volumes ONTAP发行说明"了解有关此许可选项的更多信息。

AWS 中 EBS 卷上的标签

BlueXP现在在创建新的Cloud Volumes ONTAP工作环境时向 EBS 卷添加标签。这些标签是在部署Cloud Volumes ONTAP之后创建的。

如果您的组织使用服务控制策略 (SCP) 来管理权限，则此更改会有所帮助。

自动分层策略的最短冷却期

如果您使用自动分层策略在卷上启用了数据分层，则现在可以使用 API 调整最短冷却期。

"了解如何调整最短冷却时间。"

增强自定义导出策略

当您创建新的 NFS 卷时， BlueXP现在会按升序显示自定义导出策略，使您更容易找到所需的导出策略。

删除旧的云快照

BlueXP现在会删除在部署Cloud Volumes ONTAP系统时以及每次关闭电源时创建的根和启动磁盘的旧云快照。根卷和启动卷仅保留最近的两个快照。

此增强功能通过删除不再需要的快照来帮助降低云提供商的成本。

请注意，连接器需要新的权限才能删除 Azure 快照。 "查看 Azure 的最新连接器策略" 。

```
"Microsoft.Compute/snapshots/delete"
```

2021年5月24日

Cloud Volumes ONTAP 9.9.1

BlueXP现在可以部署和管理Cloud Volumes ONTAP 9.9.1。

"了解此版本Cloud Volumes ONTAP中包含的新功能" 。

2021年4月11日

连接器 3.9.5 版本引入了以下更改。

逻辑空间报告

BlueXP现在可以在其为Cloud Volumes ONTAP创建的初始存储 VM 上启用逻辑空间报告。

当逻辑报告空间时， ONTAP会报告卷空间，以便存储效率功能节省的所有物理空间也被报告为已使用。

AWS 中对 **gp3** 磁盘的支持

从 9.7 版本开始， Cloud Volumes ONTAP现在支持_通用 SSD (gp3)_ 磁盘。gp3 磁盘是成本最低的 SSD，可在广泛的工作负载中平衡成本和性能。

"在 AWS 中调整系统大小" 。

AWS 不再支持冷 **HDD** 磁盘

Cloud Volumes ONTAP不再支持 Cold HDD (sc1) 磁盘。

Azure 存储帐户的 **TLS 1.2**

当BlueXP在 Azure 中为Cloud Volumes ONTAP创建存储帐户时，该存储帐户的 TLS 版本现在为 1.2 版。

2021年3月8日

连接器 3.9.4 版本引入了以下更改。

Cloud Volumes ONTAP 9.9.0

BlueXP现在可以部署和管理Cloud Volumes ONTAP 9.9.0。

"了解此版本Cloud Volumes ONTAP中包含的新功能" 。

支持 **AWS C2S** 环境

您现在可以在 AWS 商业云服务 (C2S) 环境中部署Cloud Volumes ONTAP 9.8。

"在 AWS Secret Cloud 或 AWS Top Secret Cloud 中部署Cloud Volumes ONTAP" 。

使用客户管理的 **CMK** 进行 **AWS** 加密

BlueXP始终允许您使用 AWS 密钥管理服务 (KMS) 加密Cloud Volumes ONTAP数据。从Cloud Volumes ONTAP 9.9.0 开始，如果您选择客户管理的 CMK，则 EBS 磁盘上的数据和分层到 S3 的数据都会被加密。以前，只有 EBS 数据会被加密。

请注意，您需要为Cloud Volumes ONTAP IAM 角色提供使用 CMK 的访问权限。

"了解有关使用Cloud Volumes ONTAP设置 AWS KMS 的更多信息" 。

对 **Azure DoD** 的支持

您现在可以在 Azure 国防部 (DoD) 影响级别 6 (IL6) 中部署Cloud Volumes ONTAP 9.8。

Google Cloud 中的 **IP** 地址减少

我们减少了 Google Cloud 中Cloud Volumes ONTAP 9.8 及更高版本所需的 IP 地址数量。默认情况下，需要的 IP 地址少一个（我们将集群间 LIF 与节点管理 LIF 统一起来）。您还可以选择在使用 API 时跳过创建 SVM 管理 LIF，这将减少对额外 IP 地址的需求。

"详细了解 Google Cloud 中的 IP 地址要求" 。

Google Cloud 中的共享 **VPC** 支持

在 Google Cloud 中部署Cloud Volumes ONTAP HA 对时，您现在可以为 VPC-1、VPC-2 和 VPC-3 选择共享 VPC。以前，只有 VPC-0 可以成为共享 VPC。 Cloud Volumes ONTAP 9.8 及更高版本支持此更改。

"详细了解 Google Cloud 网络要求" 。

2021年1月4日

连接器 3.9.2 版本引入了以下更改。

AWS Outposts

几个月前，我们宣布Cloud Volumes ONTAP已获得 Amazon Web Services (AWS) Outposts Ready 认证。今天，我们很高兴地宣布，我们已经通过 AWS Outposts 验证了BlueXP和Cloud Volumes ONTAP 。

如果您有 AWS Outpost，则可以通过在工作环境向导中选择 Outpost VPC 在该 Outpost 中部署Cloud Volumes ONTAP 。体验与驻留在 AWS 中的任何其他 VPC 相同。请注意，您需要首先在 AWS Outpost 中部署连接器。

需要指出的是，存在一些限制：

- 目前仅支持单节点Cloud Volumes ONTAP系统
- 可与Cloud Volumes ONTAP一起使用的 EC2 实例仅限于 Outpost 中可用的实例
- 目前仅支持通用 SSD（gp2）

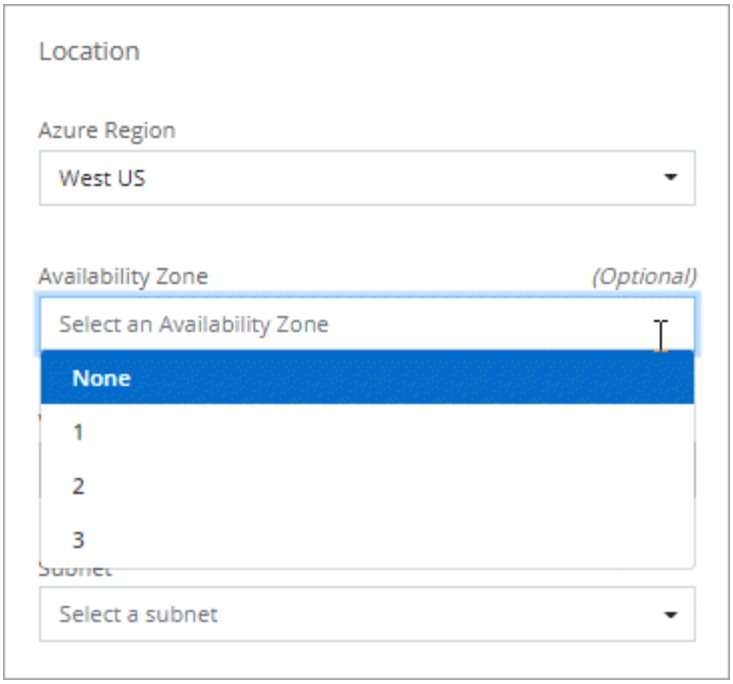
受支持的 **Azure** 区域中的 **Ultra SSD VNVRAM**

现在，当您将 E32s_v3 VM 类型与单节点系统一起使用时，Cloud Volumes ONTAP 可以将 Ultra SSD 用作 VNVRAM "在任何受支持的 Azure 区域中"。

VNVRAM 提供更好的写入性能。

在 **Azure** 中选择一个可用性区域

您现在可以选择要部署单节点Cloud Volumes ONTAP系统的可用区域。如果您不选择 AZ， BlueXP将为您选择一个。



Google Cloud 中的更大磁盘

Cloud Volumes ONTAP 现在支持 Google Cloud 中的 64 TB 磁盘。

由于 Google Cloud 的限制，仅使用磁盘的最大系统容量仍为 256 TB。

Google Cloud 中的新机器类型

Cloud Volumes ONTAP现在支持以下机器类型：

- n2-standard-4 带有 Explore 许可证和 BYOL
- n2-standard-8 具有标准许可证和 BYOL
- 具有 Premium 许可证和 BYOL 的 n2-standard-32

2020年11月3日

连接器 3.9.0 版本引入了以下变化。

适用于**Cloud Volumes ONTAP** 的**Azure Private Link**

默认情况下， BlueXP现在启用Cloud Volumes ONTAP及其关联存储帐户之间的 Azure Private Link 连接。专用链接可保护 Azure 中端点之间的连接。

- "了解有关 Azure Private Links 的更多信息"
- "了解有关使用 Azure Private Link 和Cloud Volumes ONTAP 的更多信息"

已知限制

已知限制标识了该产品的此版本不支持或不能与其正确互操作的平台、设备或功能。仔细

审查这些限制。

这些限制特定于NetApp Console中的Cloud Volumes ONTAP管理。要查看Cloud Volumes ONTAP软件本身的限制， "转到Cloud Volumes ONTAP发行说明" 。

控制台不支持创建**FlexGroup**卷

虽然Cloud Volumes ONTAP支持FlexGroup卷，但控制台目前不支持创建FlexGroup卷。如果您从ONTAP系统管理器或ONTAP CLI 创建FlexGroup卷，则应将控制台中的容量管理模式设置为 `Manual`。 `Automatic`模式可能无法与FlexGroup卷正常配合使用。

我们计划在未来的版本中提供在控制台中创建FlexGroup卷的功能。

控制台不支持带有**Cloud Volumes ONTAP** 的**S3**

虽然 Cloud Volumes ONTAP 支持 S3 作为横向扩展存储的选项，但 Console 不为此功能提供任何管理功能。使用 CLI 是从 Cloud Volumes ONTAP 配置 S3 客户端访问的最佳实践。有关详细信息，请参阅 "ONTAP S3 配置电源指南"。

"详细了解 Cloud Volumes ONTAP 对 ONTAP S3 和其他客户端协议的支持"。

控制台不支持存储虚拟机的灾难恢复

控制台不提供存储虚拟机 (SVM) 灾难恢复的任何设置或编排支持。您必须使用ONTAP系统管理器或ONTAP CLI。

"了解有关 SVM 灾难恢复的更多信息" 。

Cloud Volumes ONTAP发行说明

Cloud Volumes ONTAP的发行说明提供了特定于版本的信息。版本中的新功能、支持的配置、存储限制以及任何可能影响产品功能的已知限制或问题。

"转至Cloud Volumes ONTAP发行说明"

开始使用

了解Cloud Volumes ONTAP

Cloud Volumes ONTAP使您能够优化云存储成本和性能，同时增强数据保护、安全性和合规性。

Cloud Volumes ONTAP是一款纯软件存储设备，可在云中运行ONTAP数据管理软件。它提供具有以下主要功能的企业级存储：

- 存储效率

  利用内置数据重复数据删除、数据压缩、精简配置和克隆来最大限度地降低存储成本。

- 高可用性

  确保云环境出现故障时企业的可靠性和持续运行。

- 数据保护

  Cloud Volumes ONTAP利用 NetApp 业界领先的复制技术SnapMirror将本地数据复制到云端，以便轻松获得可用于多种用例的辅助副本。

  Cloud Volumes ONTAP还与NetApp Backup and Recovery集成，提供备份和恢复功能，以保护和长期存档您的云数据。

  "了解有关备份和恢复的更多信息"

- 数据分层

  按需在高性能和低性能存储池之间切换，无需使应用程序离线。

- 应用程序一致性

  使用NetApp SnapCenter确保NetApp Snapshot 副本的一致性。

  "了解有关SnapCenter的更多信息"

- 数据安全

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

- 隐私合规控制

  与NetApp Data Classification集成可帮助您了解数据环境并识别敏感数据。

  "了解有关数据分类的更多信息"

Cloud Volumes ONTAP中包含ONTAP功能的许可证。

"查看支持的Cloud Volumes ONTAP配置"

"了解有关Cloud Volumes ONTAP 的更多信息"

Cloud Volumes ONTAP部署支持的ONTAP版本

当您添加Cloud Volumes ONTAP系统时， NetApp Console可让您从多个不同的ONTAP版本中进行选择。

除此处列出的版本外，Cloud Volumes ONTAP 的其他版本不可用于新部署。此处版本中的修补程序或通用（通用可用性）版本表示可用于部署的基本版本。有关可用修补程序的详细信息，请参阅每个版本的 "版本化发行说明"。

有关升级的信息，请参阅 "支持的升级路径"。

AWS

单节点

- 9.18.1
- 9.17.1 P1
- 9.16.1
- 9.15.1
- 9.15.0 P1
- 9.14.1
- 9.14.1
- 9.14.0
- 9.13.1
- 9.12.1
- 9.12.1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9.8
- 9.7 P5
- 9.5 P6

HA 对

- 9.18.1
- 9.17.1 P1
- 9.16.1
- 9.15.1

- 9.15.0 P1
- 9.14.1
- 9.14.1
- 9.14.0
- 9.13.1
- 9.12.1
- 9.12.1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9.8
- 9.7 P5
- 9.5 P6

Azure

单节点

- 9.18.1
- 9.17.1 P1
- 9.16.1 P3
- 9.15.1 P10
- 9.14.1 P13
- 9.13.1 P16
- 9.12.1 P18

HA 对

- 9.18.1
- 9.17.1 P1
- 9.16.1 P3
- 9.15.1 P10
- 9.14.1 P13
- 9.13.1 P16
- 9.12.1 P18

Google Cloud

单节点

- 9.18.1
- 9.17.1 P1

- 9.16.1
- 9.15.1
- 9.15.0 P1
- 9.14.1
- 9.14.1
- 9.14.0
- 9.13.1
- 9.12.1
- 9.12.1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9.8
- 9.7 P5

HA 对

- 9.18.1
- 9.17.1 P1
- 9.16.1
- 9.15.1
- 9.15.0 P1
- 9.14.1
- 9.14.1
- 9.14.0
- 9.13.1
- 9.12.1
- 9.12.1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9.8

开始使用 **Amazon Web Services**

AWS 中的**Cloud Volumes ONTAP**快速入门

只需几个步骤即可开始在 AWS 中使用Cloud Volumes ONTAP 。

1 创建控制台代理

如果你没有 "控制台代理"但是，您需要创建一个。 "了解如何在 AWS 中创建控制台代理" 。

请注意，如果您想在没有互联网访问的子网中部署Cloud Volumes ONTAP ，则需要手动安装控制台代理并访问在该控制台代理上运行的NetApp Console用户界面。 "了解如何在没有互联网访问的地方手动安装控制台代理" 。

2 规划您的配置

控制台提供符合您的工作负载要求的预配置包，或者您可以创建自己的配置。如果您选择自己的配置，您应该了解可用的选项。"了解更多" 。

3 设置网络

1. 确保您的 VPC 和子网将支持控制台代理和Cloud Volumes ONTAP之间的连接。
2. 为NetApp AutoSupport启用从目标 VPC 的出站互联网访问。

   如果您在没有互联网访问的位置部署Cloud Volumes ONTAP，则不需要执行此步骤。
3. 设置 Amazon Simple Storage Service (Amazon S3) 服务的 VPC 端点。

   如果您想将冷数据从Cloud Volumes ONTAP到低成本对象存储，则需要 VPC 端点。

"了解有关网络要求的更多信息" 。

4 设置 **AWS KMS**

如果您想将 Amazon 加密与Cloud Volumes ONTAP结合使用，则需要确保存在有效的客户主密钥 (CMK)。您还需要通过添加以_密钥用户_身份向控制台代理提供权限的 IAM 角色来修改每个 CMK 的密钥策略。"了解更多" 。

5 使用控制台启动**Cloud Volumes ONTAP**

单击“添加系统”，选择您想要部署的系统类型，然后完成向导中的步骤。"阅读分步说明" 。

相关链接

- "为 AWS 创建控制台代理"
- "从 AWS Marketplace 创建控制台代理"
- "在本地安装并设置控制台代理"
- "控制台代理的 AWS 权限"

在 **AWS** 中规划您的**Cloud Volumes ONTAP**配置

在 AWS 中部署Cloud Volumes ONTAP时，您可以选择符合您的工作负载要求的预配置系

统，也可以创建自己的配置。如果您选择自己的配置，您应该了解可用的选项。

选择**Cloud Volumes ONTAP**许可证

Cloud Volumes ONTAP有多种许可选项。每个选项都可以让您选择符合您需求的消费模式。

- "了解Cloud Volumes ONTAP的许可选项"
- "了解如何设置许可"

选择支持的区域

大多数 AWS 区域都支持Cloud Volumes ONTAP 。 "查看支持区域的完整列表" 。

必须先启用较新的 AWS 区域，然后才能在这些区域中创建和管理资源。 "AWS 文档：了解如何启用区域" 。

选择受支持的本地区域

选择本地区域是可选的。包括新加坡在内的一些 AWS 本地区域支持Cloud Volumes ONTAP 。 AWS 中的Cloud Volumes ONTAP仅支持单个可用区域中的高可用性 (HA) 模式。不支持单节点部署。

> Cloud Volumes ONTAP不支持 AWS 本地区域中的数据分层和云分层。此外，不支持具有未符合Cloud Volumes ONTAP资格的实例的本地区域。例如迈阿密，它不能用作本地区域，因为它只有不受支持且不合格的 Gen6 实例。

"AWS 文档：查看本地区域的完整列表" 。必须先启用本地区域，然后才能在这些区域中创建和管理资源。

"AWS 文档：AWS 本地区域入门" 。

选择支持的实例

Cloud Volumes ONTAP支持多种实例类型，具体取决于您选择的许可证类型。

"AWS 中Cloud Volumes ONTAP支持的配置"

了解存储限制

Cloud Volumes ONTAP系统的原始容量限制与许可证相关。额外的限制会影响聚合和卷的大小。在规划配置时您应该注意这些限制。

"AWS 中Cloud Volumes ONTAP的存储限制"

在 **AWS** 中调整系统大小

调整Cloud Volumes ONTAP系统的大小可以帮助您满足性能和容量要求。选择实例类型、磁盘类型和磁盘大小时，您应该注意几个关键点：

实例类型

- 将您的工作负载要求与每个 EC2 实例类型的最大吞吐量和 IOPS 相匹配。
- 如果多个用户同时向系统写入数据，请选择具有足够 CPU 来管理请求的实例类型。

- 如果您有一个主要用于读取的应用程序，那么请选择具有足够 RAM 的系统。
  - "AWS 文档：Amazon EC2 实例类型"
  - "AWS 文档：Amazon EBS 优化实例"

EBS 磁盘类型

从高层次来看，EBS 磁盘类型之间的差异如下。要了解有关 EBS 磁盘用例的更多信息，请参阅 "AWS 文档：EBS 卷类型"。

- 通用 *SSD (gp3)* 磁盘是成本最低的 SSD，可在广泛的工作负载中平衡成本和性能。性能以 IOPS 和吞吐量来定义。Cloud Cloud Volumes ONTAP 9.7 及更高版本支持 gp3 磁盘。

  当您选择 gp3 磁盘时， NetApp Console会填写默认 IOPS 和吞吐量值，这些值根据所选磁盘大小提供与 gp2 磁盘相当的性能。您可以增加这些值以更高的成本获得更好的性能，但我们不支持较低的值，因为这会导致性能下降。简而言之，坚持默认值或增加默认值。不要降低它们。 "AWS 文档：了解有关 gp3 磁盘及其性能的更多信息" 。

  请注意， Cloud Volumes ONTAP支持带有 gp3 磁盘的 Amazon EBS Elastic Volumes 功能。"了解有关弹性卷支持的更多信息" 。

- 通用 *SSD (gp2)* 磁盘可在广泛的工作负载中平衡成本和性能。性能以 IOPS 来定义。
- *Provisioned IOPS SSD (io1)* 磁盘适用于需要以较高成本获得最高性能的关键应用程序。

  请注意， Cloud Volumes ONTAP支持带有 io1 磁盘的 Amazon EBS Elastic Volumes 功能。"了解有关弹性卷支持的更多信息" 。

- 吞吐量优化 *HDD (st1)* 磁盘适用于需要以较低价格实现快速、一致吞吐量的频繁访问的工作负载。

  如果您的 Cloud Volumes ONTAP 系统位于 AWS Local Zone 中，则不支持到 Amazon Simple Storage Service (Amazon S3) 的数据分层，因为在 Local Zone 之外访问 Amazon S3 存储桶涉及更高的延迟并影响 Cloud Volumes ONTAP 活动。

EBS 磁盘大小

如果您选择的配置不支持"Amazon EBS 弹性卷功能"，那么您需要在启动Cloud Volumes ONTAP系统时选择初始磁盘大小。之后，您可以"让控制台为您管理系统容量"，但如果你想"自己创建聚合"，请注意以下事项：

- 聚合中的所有磁盘必须具有相同的大小。
- EBS 磁盘的性能与磁盘大小相关。该大小决定了 SSD 磁盘的基线 IOPS 和最大突发持续时间以及 HDD 磁盘的基线和突发吞吐量。
- 最终，您应该选择能够提供您所需的_持续性能_的磁盘大小。
- 即使您确实选择了更大的磁盘（例如，六个 4 TiB 磁盘），您也可能无法获得所有的 IOPS，因为 EC2 实例可能会达到其带宽限制。

  有关 EBS 磁盘性能的更多详细信息，请参阅 "AWS 文档：EBS 卷类型"。

  如上所述，支持 Amazon EBS Elastic Volumes 功能的Cloud Volumes ONTAP配置不支持选择磁盘大小。"了解有关弹性卷支持的更多信息" 。

查看默认系统磁盘

除了用户数据的存储之外，控制台还购买了Cloud Volumes ONTAP系统数据（启动数据、根数据、核心数据和NVRAM）的云存储。出于规划目的，在部署Cloud Volumes ONTAP之前查看这些详细信息可能会有所帮助。

"查看 AWS 中Cloud Volumes ONTAP系统数据的默认磁盘" 。

控制台代理还需要系统磁盘。 "查看控制台代理默认配置的详细信息" 。

准备在 **AWS Outpost** 中部署**Cloud Volumes ONTAP**

如果您有 AWS Outpost，则可以通过在部署过程中选择 Outpost VPC 在该 Outpost 中部署Cloud Volumes ONTAP 。体验与驻留在 AWS 中的任何其他 VPC 相同。请注意，您需要首先在 AWS Outpost 中部署控制台代理。

需要指出的是，存在一些限制：

- 目前仅支持单节点Cloud Volumes ONTAP系统
- 可与Cloud Volumes ONTAP一起使用的 EC2 实例仅限于 Outpost 中可用的实例
- 目前仅支持通用 SSD（gp2）

收集网络信息

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

单个可用区中的单个节点或 **HA** 对

AWS 信息	你的价值
地区	
VPC	
子网	
安全组（如果使用您自己的）	

多个可用区中的 **HA** 对

AWS 信息	你的价值
地区	
VPC	
安全组（如果使用您自己的）	
节点 1 可用区	
节点 1 子网	
节点 2 可用区	
节点 2 子网	

AWS 信息	你的价值
中介可用区域	
调解器子网	
中介者的密钥对	
集群管理网口浮动IP地址	
节点 1 上数据的浮动 IP 地址	
节点 2 上数据的浮动 IP 地址	
浮动 IP 地址的路由表	

选择写入速度

控制台使您能够选择Cloud Volumes ONTAP的写入速度设置。在选择写入速度之前，您应该了解正常设置和高设置之间的差异以及使用高写入速度时的风险和建议。"了解有关写入速度的更多信息"。

选择卷使用情况配置文件

ONTAP包含多种存储效率功能，可以减少您所需的总存储量。在控制台中创建卷时，您可以选择启用这些功能的配置文件或禁用这些功能的配置文件。您应该了解有关这些功能的更多信息，以帮助您决定使用哪个配置文件。

NetApp存储效率功能具有以下优势：

精简配置

向主机或用户提供比物理存储池中实际拥有的更多的逻辑存储。不是预先分配存储空间，而是在写入数据时动态地将存储空间分配给每个卷。

重复数据删除

通过定位相同的数据块并将其替换为对单个共享块的引用来提高效率。该技术通过消除驻留在同一卷中的冗余数据块来减少存储容量要求。

数据压缩

通过压缩主存储、辅助存储和归档存储卷内的数据来减少存储数据所需的物理容量。

设置网络

为Cloud Volumes ONTAP设置 AWS 网络

NetApp Console负责设置Cloud Volumes ONTAP的网络组件，例如 IP 地址、网络掩码和路由。您需要确保可以访问出站互联网、有足够的私有 IP 地址、有正确的连接等等。

一般要求

确保您已满足 AWS 中的以下要求。

Cloud Volumes ONTAP节点的出站互联网访问

Cloud Volumes ONTAP系统需要出站互联网访问才能访问外部端点以实现各种功能。如果这些端点在具有严格安全要求的环境中被阻止， Cloud Volumes ONTAP将无法正常运行。

控制台代理联系多个端点以进行日常操作。有关所用端点的信息，请参阅 "查看从控制台代理联系的端点"和 "准备使用控制台的网络"。

Cloud Volumes ONTAP端点

Cloud Volumes ONTAP使用这些端点与各种服务进行通信。

端点	适用于	目的	部署模式	端点不可用时的影响
\ https://netapp-cloud-account.auth0.com	身份验证	用于控制台中的身份验证。	标准和限制模式。	用户身份验证失败，以下服务仍然不可用： • Cloud Volumes ONTAP服务 • ONTAP 服务 • 协议和代理服务
\ https://api.bluexp.netapp.com/tenancy	租户	用于从控制台检索Cloud Volumes ONTAP资源以授权资源和用户。	标准和限制模式。	Cloud Volumes ONTAP资源和用户未获得授权。
\ https://mysupport.netapp.com/aods/asupmessage \ https://mysupport.netapp.com/asupprod/post/1.0/postAsup	AutoSupport	用于将AutoSupport遥测数据发送给NetApp支持。	标准和限制模式。	AutoSupport信息仍未送达。
AWS 服务的确切商业端点（后缀为 `amazonaws.com`）取决于您使用的 AWS 区域。请参阅 "AWS 文档了解详细信息"。	• 云形成 • 弹性计算云（EC2） • 身份和访问管理 (IAM) • 密钥管理服务（KMS） • 安全令牌服务 (STS) • Amazon Simple Storage Service (S3)	与 AWS 服务通信。	标准和私人模式。	Cloud Volumes ONTAP无法与 AWS 服务通信以在 AWS 中执行特定操作。

端点	适用于	目的	部署模式	端点不可用时的影响
AWS 服务的具体政府端点取决于您使用的 AWS 区域。端点后缀为 `amazonaws.com` 和 `c2s.ic.gov`。参考 "AWS 开发工具包"和 "AWS 文档"了解更多信息。	• 云形成 • 弹性计算云（EC2） • 身份和访问管理(IAM) • 密钥管理服务（KMS） • 安全令牌服务(STS) • 简单存储服务（S3）	与 AWS 服务通信。	限制模式。	Cloud Volumes ONTAP无法与 AWS 服务通信以在 AWS 中执行特定操作。

HA 中介器的出站互联网访问

HA 中介实例必须具有与 AWS EC2 服务的出站连接，以便它可以协助存储故障转移。为了提供连接，您可以添加公共 IP 地址、指定代理服务器或使用手动选项。

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

NetApp Console代理的网络代理配置

您可以使用NetApp Console代理的代理服务器配置来启用来自Cloud Volumes ONTAP 的出站互联网访问。控制台支持两种类型的代理：

- 显式代理：来自Cloud Volumes ONTAP 的出站流量使用在控制台代理的代理配置期间指定的代理服务器的 HTTP 地址。管理员可能还配置了用户凭据和根 CA 证书以进行额外的身份验证。Cloud Volumes ONTAP显式代理有可用的根 CA 证书，请确保使用 "ONTAP CLI：安全证书安装"命令。
- 透明代理：网络配置为通过控制台代理的代理自动路由来自Cloud Volumes ONTAP 的出站流量。设置透明代理时，管理员只需要提供用于从Cloud Volumes ONTAP进行连接的根 CA 证书，而不是代理服务器的 HTTP 地址。确保使用以下方式获取相同的根 CA 证书并将其上传到您的Cloud Volumes ONTAP系统 "ONTAP CLI：安全证书安装"命令。

有关配置代理服务器的信息，请参阅 "配置控制台代理以使用代理服务器"。

私有 **IP** 地址

控制台会自动为Cloud Volumes ONTAP分配所需数量的私有 IP 地址。您需要确保您的网络有足够的可用私有 IP 地址。

Console 为 Cloud Volumes ONTAP 分配的 LIF 数量取决于您是部署单节点系统还是 HA 对。LIF 是与物理端口关联的 IP 地址。

单节点系统的 **IP** 地址

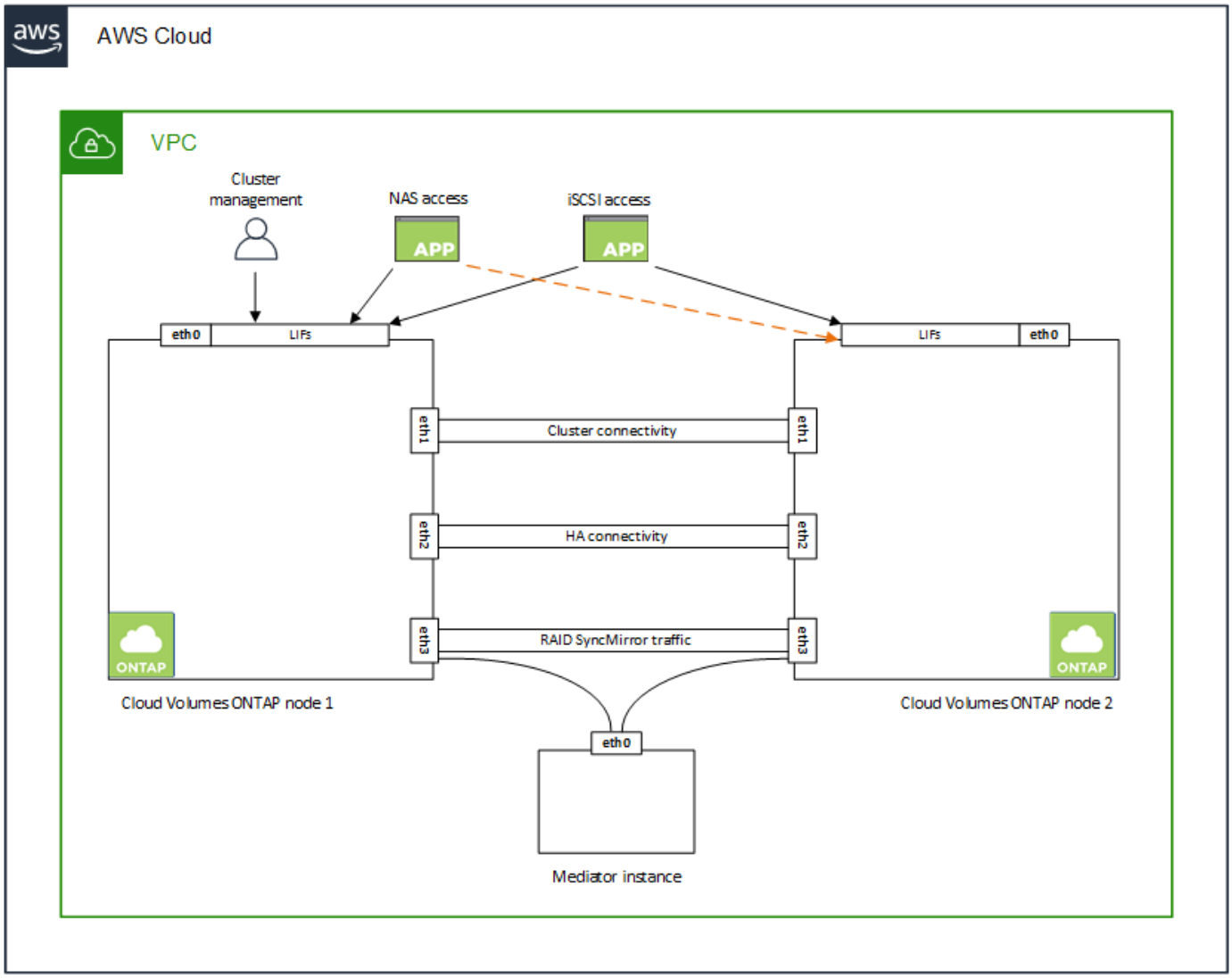
Console 为单节点系统分配 6 个 IP 地址。

下表提供了与每个私有 IP 地址关联的 LIF 的详细信息。

LIF	目的
集群管理	整个集群（HA 对）的行政管理。
节点管理	节点的行政管理。
集群间	跨集群通信、备份和复制。
NAS数据	通过 NAS 协议进行客户端访问。
iSCSI 数据	通过 iSCSI 协议进行客户端访问。系统还将其用于其他重要的网络工作流程。此 LIF 是必需的，不应删除。
存储虚拟机管理	存储虚拟机管理 LIF 与SnapCenter等管理工具一起使用。

HA 对的 **IP** 地址

HA 对比单节点系统需要更多的 IP 地址。这些 IP 地址分布在不同的以太网接口上，如下图所示：



HA 对所需的私有 IP 地址数量取决于您选择的部署模型。在单个 AWS 可用区 (AZ) 中部署的 HA 对需要 15 个私有 IP 地址，而在多个 AZ 中部署的 HA 对需要 13 个私有 IP 地址。

下表提供了与每个私有 IP 地址关联的 LIF 的详细信息。

LIF	接口	节点	目的
集群管理	eth0	节点 1	整个集群（HA 对）的行政管理。
节点管理	eth0	节点 1 和节点 2	节点的行政管理。
集群间	eth0	节点 1 和节点 2	跨集群通信、备份和复制。
NAS数据	eth0	节点 1	通过 NAS 协议进行客户端访问。
iSCSI 数据	eth0	节点 1 和节点 2	通过 iSCSI 协议进行客户端访问。系统还将其用于其他重要的网络工作流程。这些 LIF 是必需的，不应删除。
集群连接	eth1	节点 1 和节点 2	使节点能够相互通信并在集群内移动数据。
HA 连接	eth2	节点 1 和节点 2	发生故障转移时两个节点之间的通信。
RSM iSCSI 流量	eth3	节点 1 和节点 2	RAID SyncMirror iSCSI 流量，以及两个Cloud Volumes ONTAP节点和中介之间的通信。
调解器	eth0	调解器	节点和中介之间的通信通道，用于协助存储接管和归还过程。

LIF	接口	节点	目的
节点管理	eth0	节点 1 和节点 2	节点的行政管理。
集群间	eth0	节点 1 和节点 2	跨集群通信、备份和复制。
iSCSI 数据	eth0	节点 1 和节点 2	通过 iSCSI 协议进行客户端访问。这些 LIF 还管理节点之间浮动 IP 地址的迁移。这些 LIF 是必需的，不应删除。
集群连接	eth1	节点 1 和节点 2	使节点能够相互通信并在集群内移动数据。
HA 连接	eth2	节点 1 和节点 2	发生故障转移时两个节点之间的通信。
RSM iSCSI 流量	eth3	节点 1 和节点 2	RAID SyncMirror iSCSI 流量，以及两个Cloud Volumes ONTAP节点和中介之间的通信。
调解器	eth0	调解器	节点和中介之间的通信通道，用于协助存储接管和归还过程。

当部署在多个可用区时，多个 LIF 与"浮动IP地址"，这不计入 AWS 私有 IP 限制。

安全组

您不需要创建安全组，因为控制台会为您完成此操作。如果您需要使用自己的，请参阅"安全组规则"。

正在寻找有关控制台代理的信息？ "查看控制台代理的安全组规则"

数据分层连接

如果要将 EBS 作为性能层，将 Amazon S3 作为容量层，则必须确保 Cloud Volumes ONTAP 具有到 S3 的连接。提供此连接的最佳方法是创建到 S3 服务的 VPC 端点。有关说明，请参阅 "AWS 文档：创建网关终端节点"。

创建 VPC 端点时，请确保选择与Cloud Volumes ONTAP实例相对应的区域、VPC 和路由表。您还必须修改安全组以添加允许流量到 S3 端点的出站 HTTPS 规则。否则， Cloud Volumes ONTAP无法连接到 S3 服务。

如果您遇到任何问题，请参阅 "AWS Support 知识中心：为什么我无法使用网关 VPC 终端节点连接到 S3 存储桶？"

与**ONTAP**系统的连接

要在 AWS 中的Cloud Volumes ONTAP系统和其他网络中的ONTAP系统之间复制数据，您必须在 AWS VPC 和其他网络（例如您的公司网络）之间建立 VPN 连接。有关说明，请参阅 "AWS 文档：设置 AWS VPN 连接"。

CIFS 的 **DNS** 和 **Active Directory**

如果您想要配置 CIFS 存储，则必须在 AWS 中设置 DNS 和 Active Directory，或者将您的本地设置扩展到 AWS。

DNS 服务器必须为 Active Directory 环境提供名称解析服务。您可以配置 DHCP 选项集以使用默认 EC2 DNS 服务器，该服务器不能是 Active Directory 环境使用的 DNS 服务器。

有关说明，请参阅 "AWS 文档：AWS 云上的 Active Directory 域服务：快速入门参考部署"。

VPC共享

从 9.11.1 版本开始，AWS 通过 VPC 共享支持Cloud Volumes ONTAP HA 对。 VPC 共享使您的组织能够与其他 AWS 账户共享子网。要使用此配置，您必须设置您的 AWS 环境，然后使用 API 部署 HA 对。

"了解如何在共享子网中部署 HA 对" 。

多可用区中 **HA** 对的要求

其他 AWS 网络要求适用于使用多个可用区 (AZ) 的Cloud Volumes ONTAP HA 配置。在启动 HA 对之前，您应该查看这些要求，因为在添加Cloud Volumes ONTAP系统时必须在控制台中输入网络详细信息。

要了解 HA 对的工作原理，请参阅"高可用性对"。

可用区域

此 HA 部署模型使用多个 AZ 来确保数据的高可用性。您应该为每个Cloud Volumes ONTAP实例和中介实例使用专用 AZ，这为 HA 对之间提供了通信通道。

每个可用区都应该有一个子网。

用于 **NAS** 数据和集群/**SVM** 管理的浮动 **IP** 地址

多个可用区中的 HA 配置使用浮动 IP 地址，如果发生故障，这些地址会在节点之间迁移。它们无法从 VPC 外部本机访问，除非您"设置 AWS 中转网关"。

一个浮动 IP 地址用于集群管理，一个用于节点 1 上的 NFS/CIFS 数据，一个用于节点 2 上的 NFS/CIFS 数

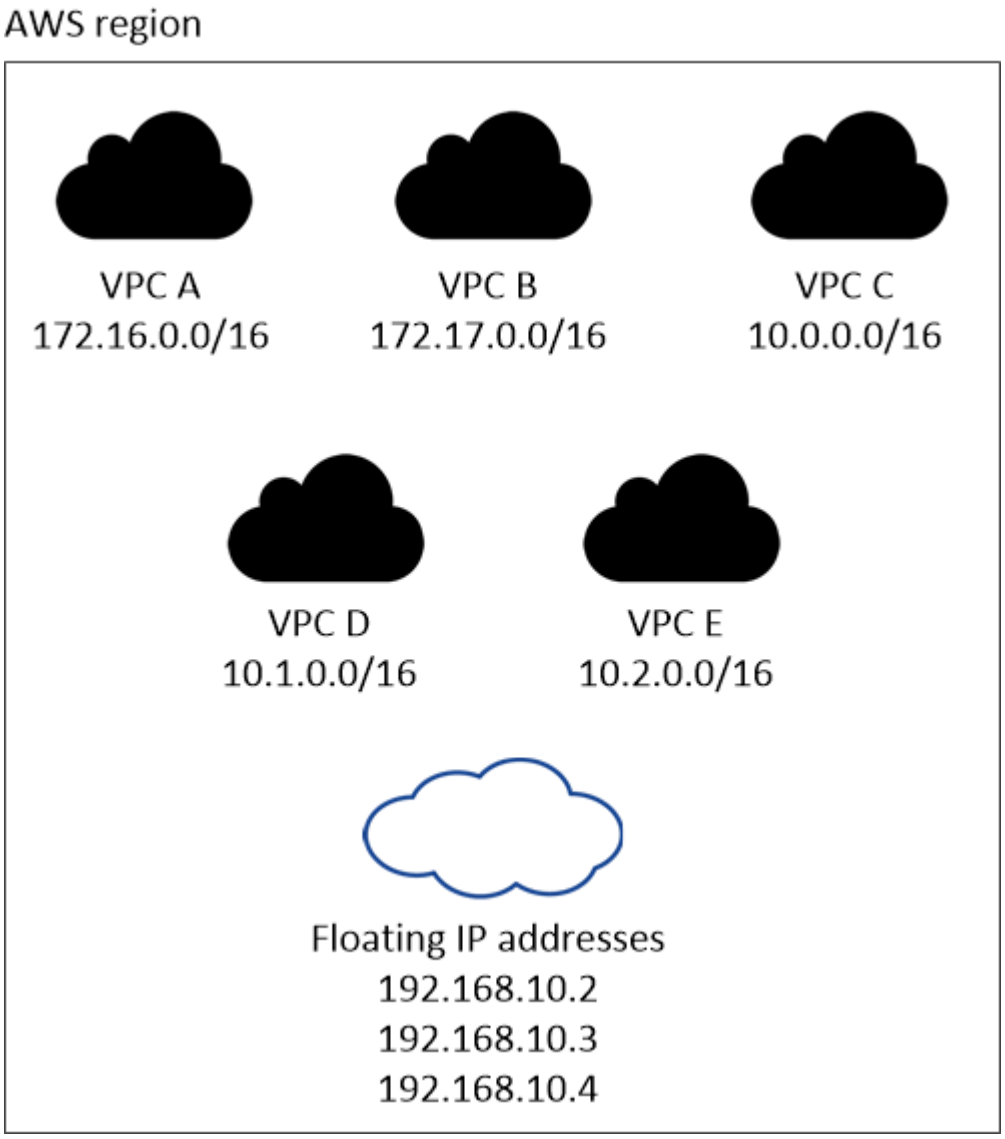
据。用于 SVM 管理的第四个浮动 IP 地址是可选的。

如果您将SnapDrive for Windows 或SnapCenter与 HA 对一起使用，则 SVM 管理 LIF 需要浮动 IP 地址。

添加Cloud Volumes ONTAP HA 系统时，需要输入浮动 IP 地址。控制台在启动系统时将 IP 地址分配给 HA 对。

浮动 IP 地址必须位于您部署 HA 配置的 AWS 区域中的所有 VPC 的 CIDR 块之外。将浮动 IP 地址视为您所在区域的 VPC 之外的逻辑子网。

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



控制台会自动创建静态 IP 地址，用于 iSCSI 访问和来自 VPC 外部客户端的 NAS 访问。您不需要满足这些类型的 IP 地址的任何要求。

中转网关，用于从 **VPC** 外部启用浮动 **IP** 访问

如果需要的话，"设置 AWS 中转网关"允许从 HA 对所在的 VPC 外部访问 HA 对的浮动 IP 地址。

路由表

指定浮动 IP 地址后，系统将提示您选择应包含浮动 IP 地址路由的路由表。这使得客户端可以访问 HA 对。

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

例如，您可能有两个与不同路由表关联的子网。如果您选择路由表 A，而不是路由表 B，则与路由表 A 关联的子网中的客户端可以访问 HA 对，但与路由表 B 关联的子网中的客户端则不能访问。

有关路由表的更多信息，请参阅 "AWS 文档：路由表"。

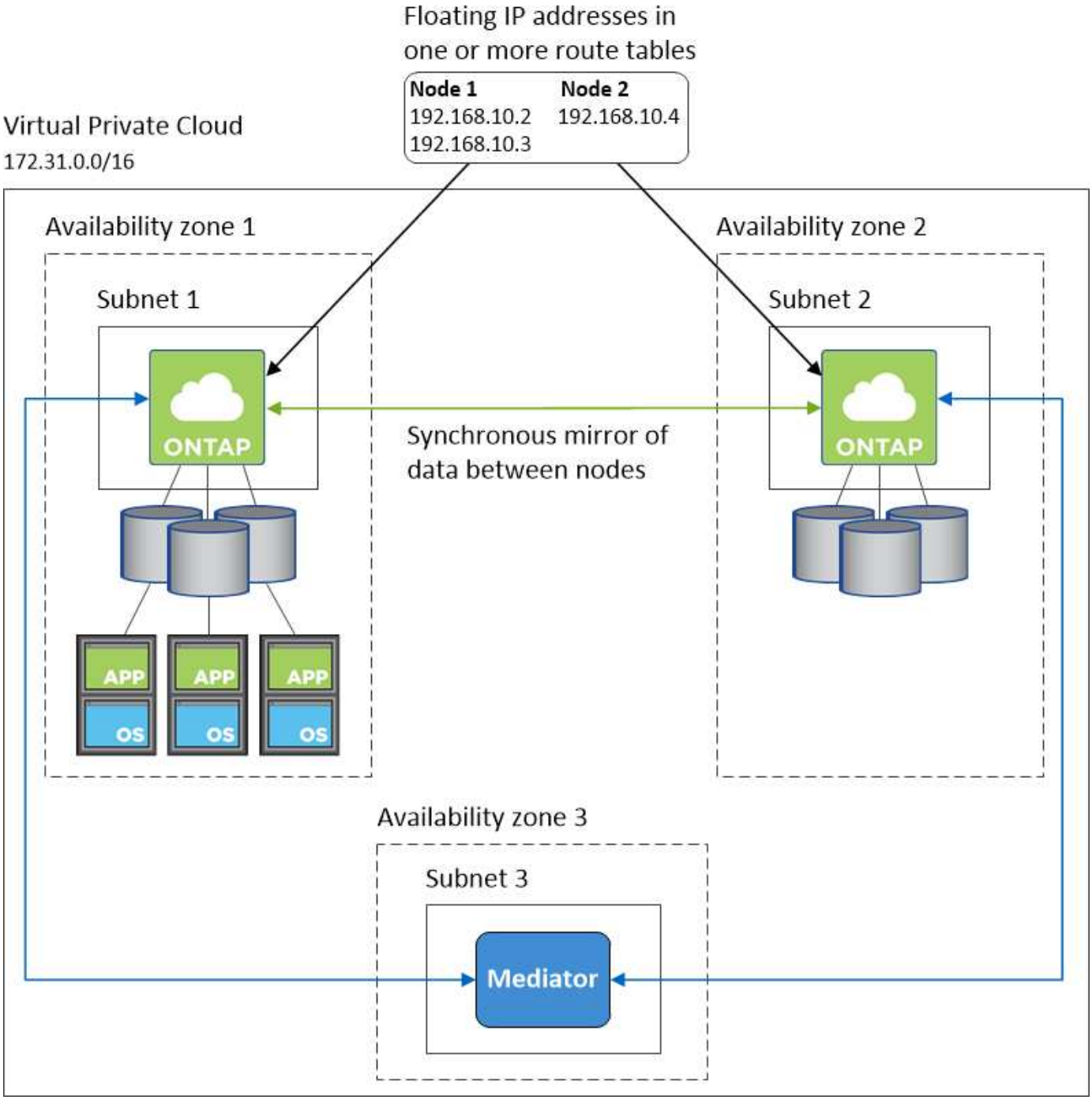
连接到**NetApp**管理工具

要将NetApp管理工具与多个 AZ 中的 HA 配置一起使用，您有两种连接选项：

1. 在不同的 VPC 中部署NetApp管理工具，并"设置 AWS 中转网关"。网关允许从 VPC 外部访问集群管理接口的浮动 IP 地址。
2. 在同一 VPC 中部署NetApp管理工具，并使用与 NAS 客户端类似的路由配置。

HA 配置示例

下图说明了多个可用区中的 HA 对特有的网络组件：三个可用区、三个子网、浮动 IP 地址和一个路由表。



控制台代理的要求

如果您尚未创建控制台代理，则应查看网络要求。

- "查看控制台代理的网络要求"
- "AWS 中的安全组规则"

相关主题

- "验证Cloud Volumes ONTAP 的AutoSupport设置"
- "了解ONTAP内部端口" 。

为**Cloud Volumes ONTAP HA** 对设置 **AWS** 传输网关

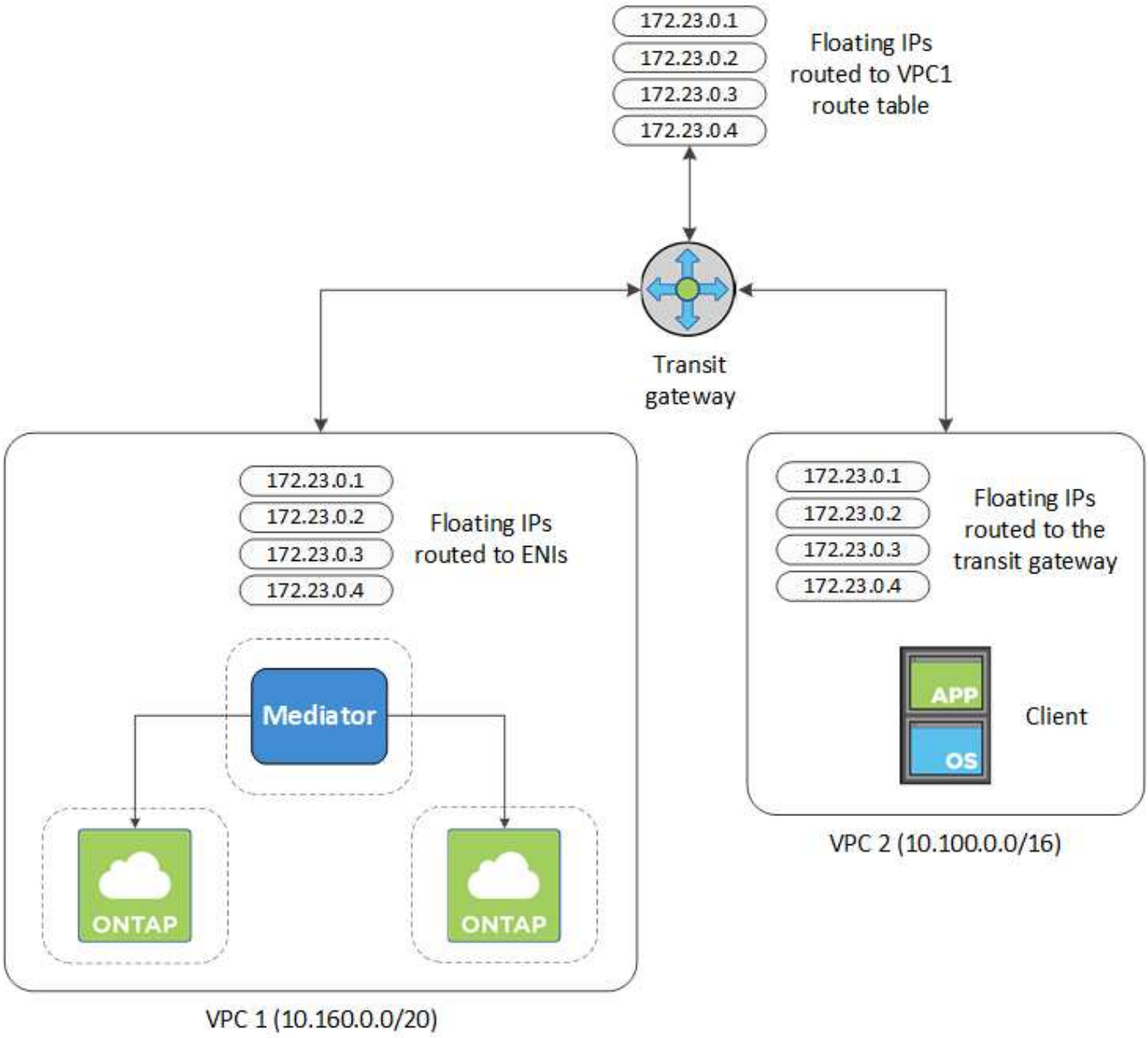
设置 AWS 中转网关以允许访问 HA 对的"浮动IP地址"来自 HA 对所在的 VPC 外部。

当Cloud Volumes ONTAP HA 配置分布在多个 AWS 可用区时，需要浮动 IP 地址才能从 VPC 内部访问 NAS 数据。当发生故障时，这些浮动 IP 地址可以在节点之间迁移，但无法从 VPC 外部进行本机访问。单独的私有 IP 地址提供从 VPC 外部的数据访问，但它们不提供自动故障转移。

集群管理接口和可选的 SVM 管理 LIF 也需要浮动 IP 地址。

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

下面是一个显示通过中转网关连接的两个 VPC 的示例。 HA 系统位于一个 VPC 中，而客户端位于另一个 VPC 中。然后，您可以使用浮动 IP 地址在客户端上安装 NAS 卷。

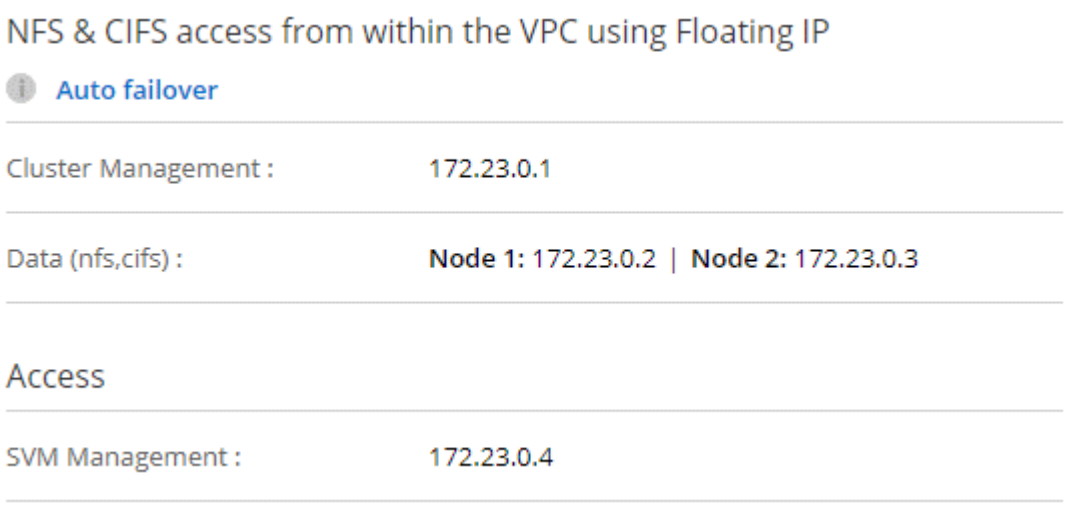


以下步骤说明如何设置类似的配置。

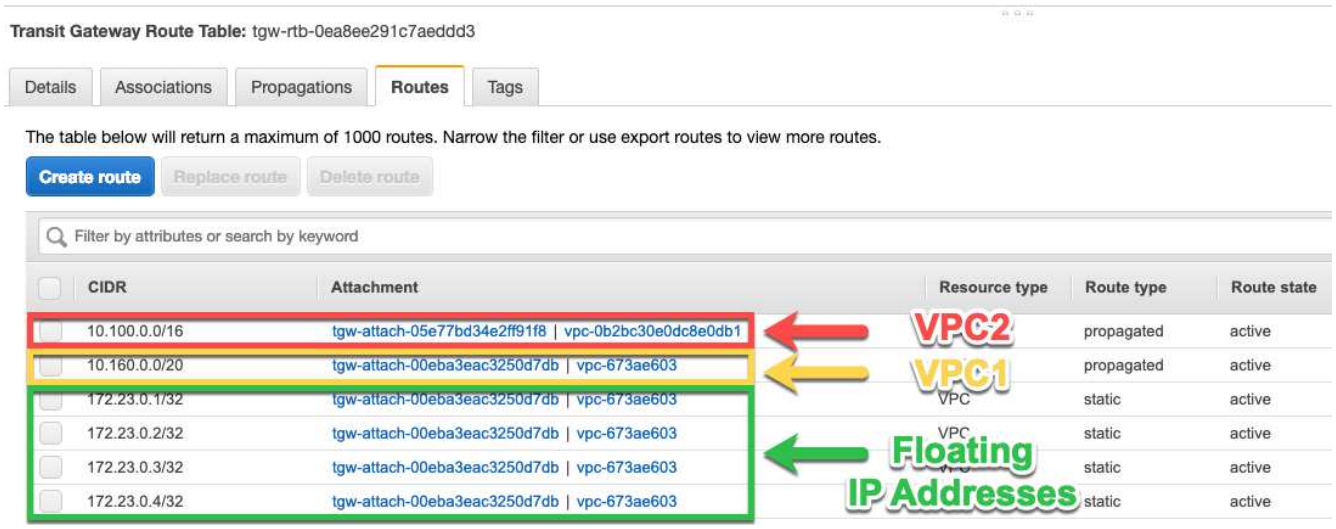
步骤

1. "创建中转网关并将 VPC 附加到该网关" 。
2. 将 VPC 与传输网关路由表关联。
   a. 在 **VPC** 服务中，单击 **Transit Gateway Route Tables**。
   b. 选择路由表。
   c. 单击*关联*，然后选择*创建关联*。
   d. 选择要关联的附件（VPC），然后单击*创建关联*。
3. 通过指定 HA 对的浮动 IP 地址在传输网关的路由表中创建路由。

   您可以在NetApp Console的系统信息页面上找到浮动 IP 地址。以下是一个例子：



   以下示例图显示了中转网关的路由表。它包括到两个 VPC 的 CIDR 块的路由和Cloud Volumes ONTAP使用的四个浮动 IP 地址。

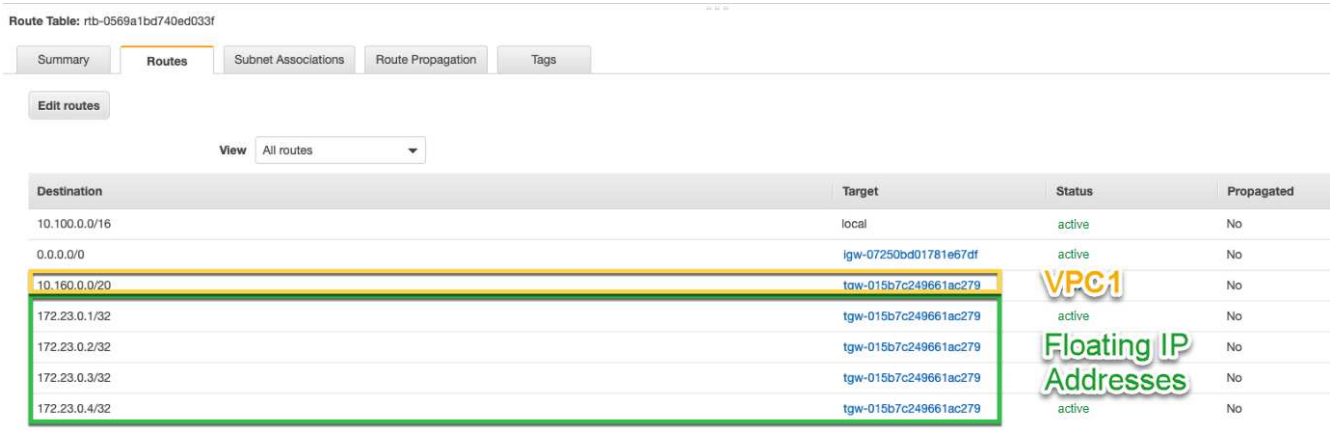


4. 修改需要访问浮动IP地址的VPC的路由表。

a. 为浮动IP地址添加路由条目。

b. 将路由条目添加到 HA 对所在 VPC 的 CIDR 块。

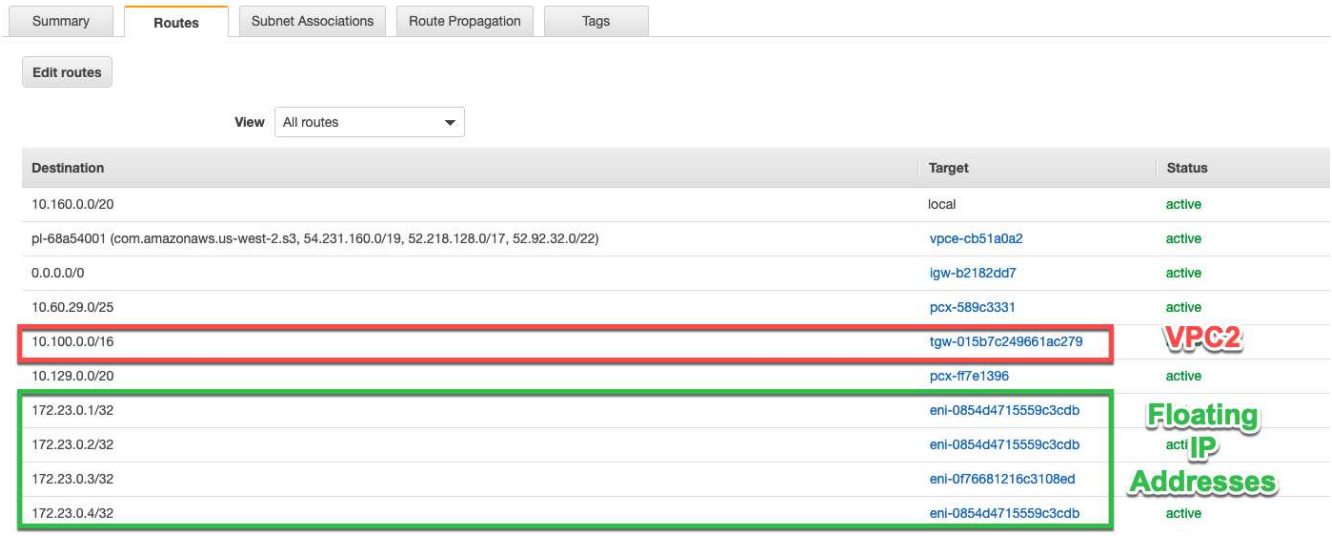
下面的示例图显示了 VPC 2 的路由表，其中包括到 VPC 1 的路由和浮动 IP 地址。



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

这一步很重要，因为它完成了 VPC 之间的路由。

以下示例图像显示了 VPC 1 的路由表。它包括到浮动 IP 地址和客户端所在的 VPC 2 的路由。控制台在部署 HA 对时会自动将浮动 IP 添加到路由表中。



6. 将安全组设置更新为 VPC 的所有流量。

a. 在虚拟私有云下，单击*子网*。

b. 单击“路由表”选项卡，为 HA 对的其中一个浮动 IP 地址选择所需的环境。

c. 单击“安全组”。

d. 选择*编辑入站规则*。

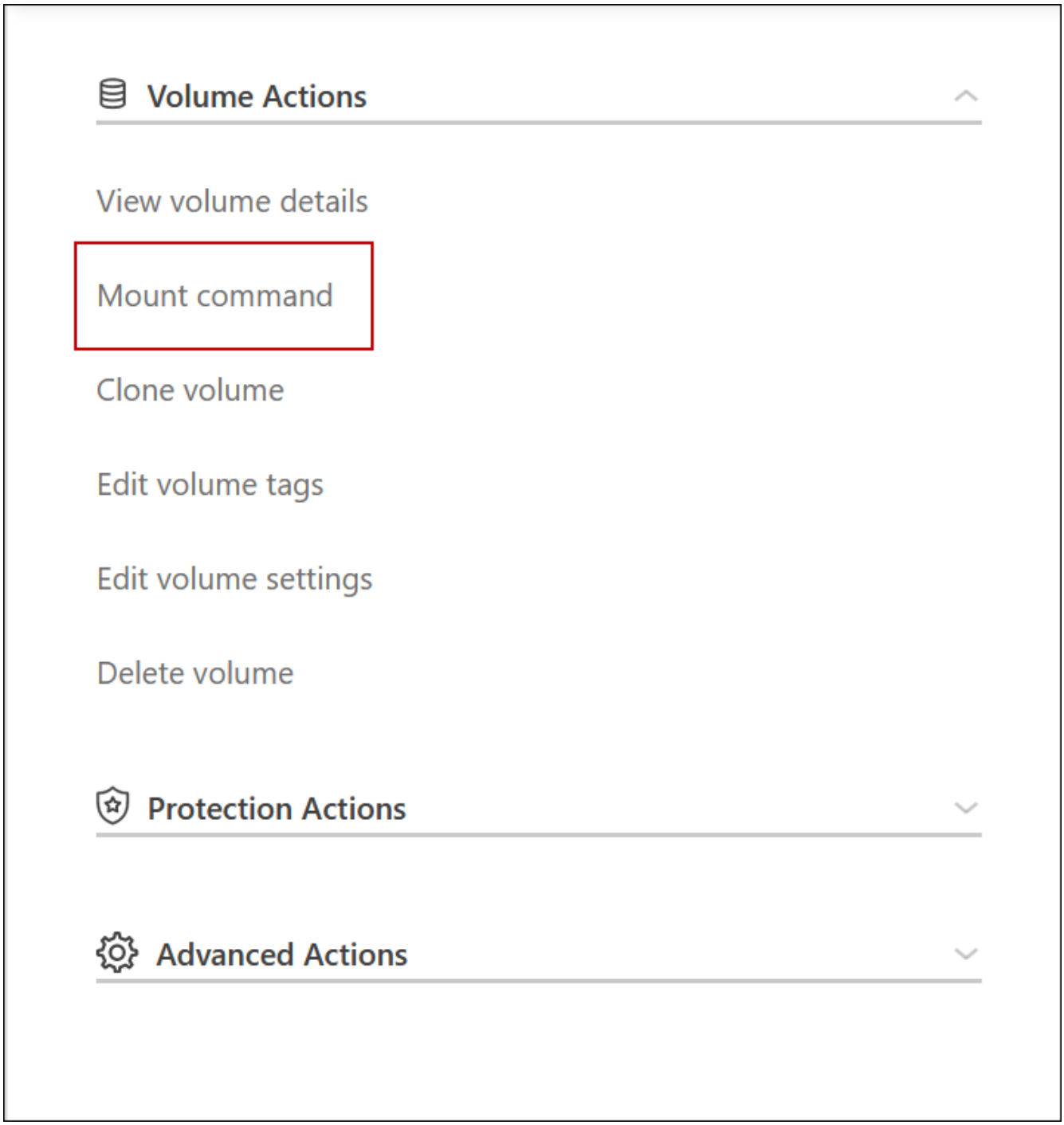
e. 单击“添加规则”。

f. 在类型下，选择*所有流量*，然后选择 VPC IP 地址。

g. 单击“保存规则”以应用更改。

7. 使用浮动 IP 地址将卷挂载到客户端。

   您可以通过控制台中“管理卷”面板下的“**Mount Command**”选项在控制台中找到正确的 IP 地址。



8. 如果您正在挂载 NFS 卷，请配置导出策略以匹配客户端 VPC 的子网。

   "了解如何编辑卷" 。

相关链接

- "AWS 中的高可用性对"
- "AWS 中Cloud Volumes ONTAP的网络要求"

在 **AWS** 共享子网中部署**Cloud Volumes ONTAP HA** 对

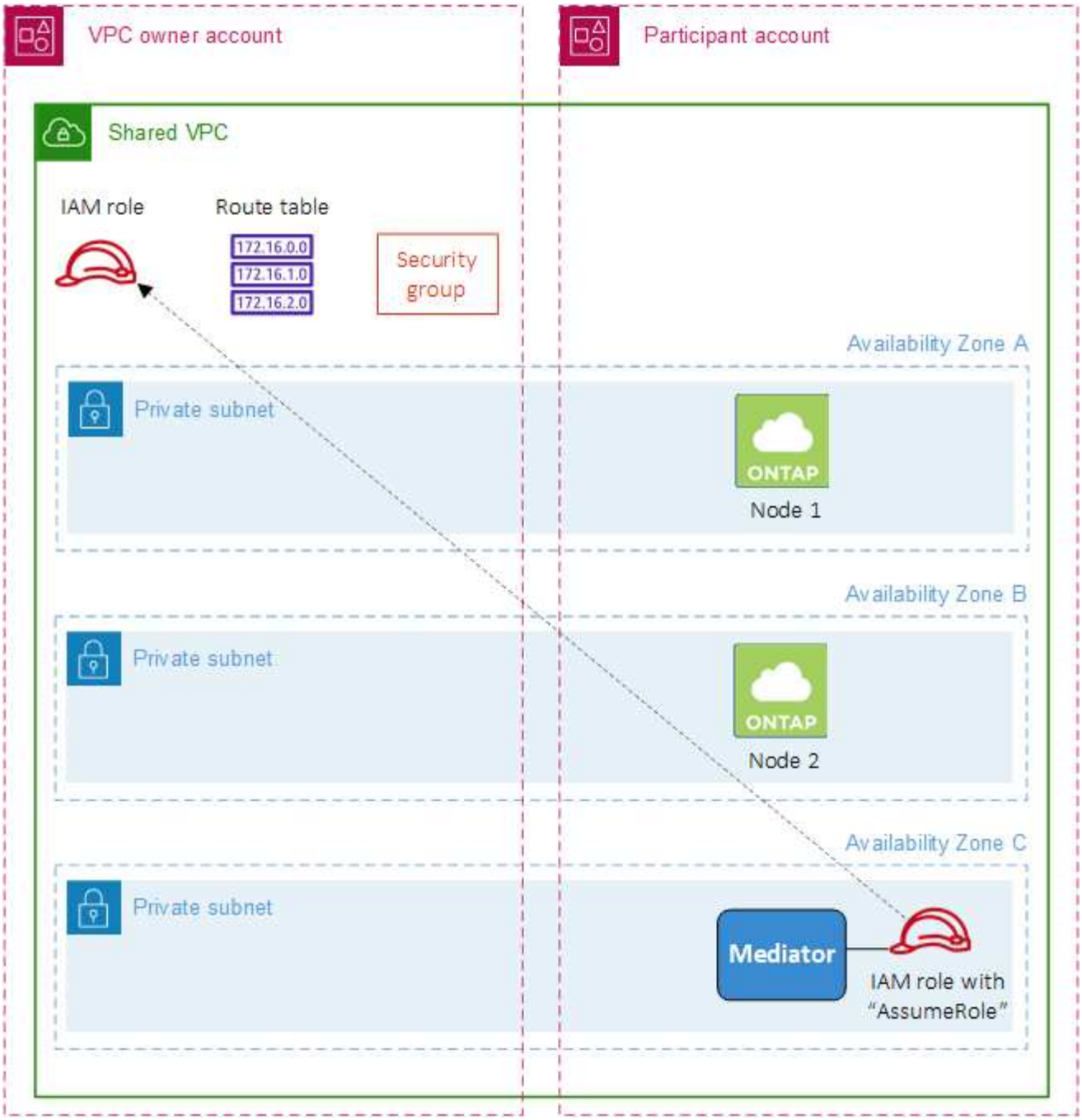
从 9.11.1 版本开始，AWS 通过 VPC 共享支持Cloud Volumes ONTAP HA 对。 VPC 共享使您的组织能够与其他 AWS 账户共享子网。要使用此配置，您必须设置您的 AWS 环境，然后使用 API 部署 HA 对。

和 "VPC共享"， Cloud Volumes ONTAP HA 配置分布在两个帐户中：

- VPC 所有者账户，拥有网络（VPC、子网、路由表和Cloud Volumes ONTAP安全组）
- 参与者账户，其中 EC2 实例部署在共享子网中（这包括两个 HA 节点和中介者）

对于跨多个可用区部署的Cloud Volumes ONTAP HA 配置，HA 中介需要特定权限才能写入 VPC 所有者帐户中的路由表。您需要通过设置调解员可以承担的 IAM 角色来提供这些权限。

下图显示了此部署所涉及的组件：



按照以下步骤所述，您需要与参与者账户共享子网，然后在 VPC 所有者账户中创建 IAM 角色和安全组。

当您创建Cloud Volumes ONTAP系统时， NetApp Console会自动创建 IAM 角色并将其附加到中介器。此角色承担您在 VPC 所有者账户中创建的 IAM 角色，以便对与 HA 对关联的路由表进行更改。

步骤

1. 与参与者账户共享 VPC 所有者账户中的子网。

   此步骤是在共享子网中部署 HA 对所必需的。

   "AWS 文档：共享子网"

2. 在 VPC 所有者账户中，为Cloud Volumes ONTAP创建一个安全组。

"请参阅Cloud Volumes ONTAP的安全组规则" 。请注意，您不需要为 HA 中介创建安全组。控制台会为您完成该操作。

3. 在 VPC 所有者账户中，创建一个包含以下权限的 IAM 角色：

```
Action": [
                "ec2:AssignPrivateIpAddresses",
                "ec2:CreateRoute",
                "ec2:DeleteRoute",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeVpcs",
                "ec2:ReplaceRoute",
                "ec2:UnassignPrivateIpAddresses"
```

4. 使用 API 创建新的Cloud Volumes ONTAP系统。

   请注意，您必须指定以下字段：

   - “安全组 ID”

     “securityGroupId”字段应指定您在 VPC 所有者帐户中创建的安全组（请参阅上面的步骤 2）。

   - “haParams”对象中的“assumeRoleArn”

     “assumeRoleArn”字段应包括您在 VPC 所有者账户中创建的 IAM 角色的 ARN（请参阅上面的步骤 3）。

     例如：

```
"haParams": {
     "assumeRoleArn":
"arn:aws:iam::642991768967:role/mediator_role_assume_fromdev"
}
```

+
"了解Cloud Volumes ONTAP API"

在 **AWS** 单可用区中为**Cloud Volumes ONTAP HA** 对配置放置组创建

如果放置组创建失败，AWS 单可用区 (AZ) 中的Cloud Volumes ONTAP高可用性 (HA) 部署可能会失败并回滚。如果Cloud Volumes ONTAP节点和中介实例不可用，则放置组的创建也会失败，并且部署会回滚。为了避免这种情况，您可以修改配置，以便即使放置组创建失败也能完成部署。

绕过回滚过程后， Cloud Volumes ONTAP部署过程成功完成，并通知您放置组创建未完成。

步骤

1. 使用 SSH 连接到NetApp Console代理主机并登录。
2. 导航至 `/opt/application/netapp/cloudmanager/docker_occm/data`。
3. 编辑 `app.conf`通过改变 `rollback-on-placement-group-failure`参数 `false`。该参数的默认值是 `true`。

```
{
    "occm" : {
        "aws" : {
            "rollback-on-placement-group-failure" : false
        }
    }
}
```

4. 保存文件并注销控制台代理。您不需要重新启动控制台代理。

Cloud Volumes ONTAP的 **AWS** 安全组入站和出站规则

NetApp Console创建 AWS 安全组，其中包括Cloud Volumes ONTAP成功运行所需的入站和出站规则。您可能希望参考端口以进行测试，或者您更喜欢使用自己的安全组。

Cloud Volumes ONTAP规则

Cloud Volumes ONTAP的安全组需要入站和出站规则。

入站规则

添加Cloud Volumes ONTAP系统并选择预定义安全组时，您可以选择允许以下之一内的流量：

- 仅限选定的 **VPC**：入站流量的来源是Cloud Volumes ONTAP系统的 VPC 子网范围和控制台代理所在的 VPC 子网范围。这是推荐的选项。
- 所有 **VPC**：入站流量的来源是 0.0.0.0/0 IP 范围。

协议	端口	目的
所有 ICMP	全部	对实例执行 ping 操作
HTTP	80	使用集群管理 LIF 的 IP 地址通过 HTTP 访问ONTAP System Manager Web 控制台
HTTPS	443	使用集群管理 LIF 的 IP 地址与控制台代理建立连接并通过 HTTPS 访问ONTAP System Manager Web 控制台
SSH	22	通过 SSH 访问集群管理 LIF 或节点管理 LIF 的 IP 地址
TCP	111	NFS 的远程过程调用
TCP	139	CIFS 的 NetBIOS 服务会话
TCP	161-162	简单网络管理协议

协议	端口	目的
TCP	445	使用 NetBIOS 框架的 TCP 上的 Microsoft SMB/CIFS
TCP	635	NFS 挂载
TCP	749	Kerberos
TCP	2049	NFS 服务器守护进程
TCP	3260	通过 iSCSI 数据 LIF 进行 iSCSI 访问
TCP	4045	NFS 锁守护进程
TCP	4046	NFS 网络状态监视器
TCP	10000	使用 NDMP 备份
TCP	11104	SnapMirror集群间通信会话的管理
TCP	11105	使用集群间 LIF 进行SnapMirror数据传输
UDP	111	NFS 的远程过程调用
UDP	161-162	简单网络管理协议
UDP	635	NFS 挂载
UDP	2049	NFS 服务器守护进程
UDP	4045	NFS 锁守护进程
UDP	4046	NFS 网络状态监视器
UDP	4049	NFS rquotad 协议

出站规则

Cloud Volumes ONTAP的预定义安全组打开所有出站流量。如果可以接受，请遵循基本的出站规则。如果您需要更严格的规则，请使用高级出站规则。

基本出站规则

Cloud Volumes ONTAP的预定义安全组包括以下出站规则。

协议	端口	目的
所有 ICMP	全部	所有出站流量
所有 TCP	全部	所有出站流量
所有 UDP	全部	所有出站流量

高级出站规则

如果您需要对出站流量制定严格的规则，则可以使用以下信息仅打开Cloud Volumes ONTAP出站通信所需的端口。

源是Cloud Volumes ONTAP系统上的接口（IP 地址）。

服务	协议	端口	源	目标	目的
Active Directory	TCP	88	节点管理 LIF	Active Directory 林	Kerberos V 身份验证
	UDP	137	节点管理 LIF	Active Directory 林	NetBIOS 名称服务
	UDP	138	节点管理 LIF	Active Directory 林	NetBIOS 数据报服务
	TCP	139	节点管理 LIF	Active Directory 林	NetBIOS 服务会话
	TCP 和 UDP	389	节点管理 LIF	Active Directory 林	LDAP
	TCP	445	节点管理 LIF	Active Directory 林	使用 NetBIOS 框架的 TCP 上的 Microsoft SMB/CIFS
	TCP	464	节点管理 LIF	Active Directory 林	Kerberos V 更改和设置密码（SET_CHANGE）
	UDP	464	节点管理 LIF	Active Directory 林	Kerberos 密钥管理
	TCP	749	节点管理 LIF	Active Directory 林	Kerberos V 更改和设置密码（RPCSEC_GSS）
	TCP	88	数据 LIF（NFS 、CIFS、iSCSI）	Active Directory 林	Kerberos V 身份验证
	UDP	137	数据 LIF（NFS 、CIFS）	Active Directory 林	NetBIOS 名称服务
	UDP	138	数据 LIF（NFS 、CIFS）	Active Directory 林	NetBIOS 数据报服务
	TCP	139	数据 LIF（NFS 、CIFS）	Active Directory 林	NetBIOS 服务会话
	TCP 和 UDP	389	数据 LIF（NFS 、CIFS）	Active Directory 林	LDAP
	TCP	445	数据 LIF（NFS 、CIFS）	Active Directory 林	使用 NetBIOS 框架的 TCP 上的 Microsoft SMB/CIFS
	TCP	464	数据 LIF（NFS 、CIFS）	Active Directory 林	Kerberos V 更改和设置密码（SET_CHANGE）
	UDP	464	数据 LIF（NFS 、CIFS）	Active Directory 林	Kerberos 密钥管理
	TCP	749	数据 LIF（NFS 、CIFS）	Active Directory 林	Kerberos V 更改和设置密码（RPCSEC_GSS）
AutoSupport	HTTPS	443	节点管理 LIF	mysupport.netapp.com	AutoSupport （默认为 HTTPS）
	HTTP	80	节点管理 LIF	mysupport.netapp.com	AutoSupport （仅当传输协议从 HTTPS 更改为 HTTP 时）
	TCP	3128	节点管理 LIF	控制台代理	如果出站互联网连接不可用，则通过控制台代理上的代理服务器发送AutoSupport消息

服务	协议	端口	源	目标	目的
备份到S3	TCP	5010	集群间 LIF	备份端点或恢复端点	备份到 S3 功能的备份和还原操作
集群	所有流量	所有流量	一个节点上的所有LIF	另一个节点上的所有LIF	集群间通信（仅限Cloud Volumes ONTAP HA）
	TCP	3000	节点管理 LIF	HA介导者	ZAPI 调用（仅限Cloud Volumes ONTAP HA）
	ICMP	1	节点管理 LIF	HA介导者	保持活动状态（仅限Cloud Volumes ONTAP HA）
配置备份	HTTP	80	节点管理 LIF	http://<控制台代理 IP地址>/occm/offboxconfig	将配置备份发送到控制台代理。"ONTAP 文档"
DHCP	UDP	68	节点管理 LIF	DHCP	首次设置的 DHCP 客户端
DHCP服务	UDP	67	节点管理 LIF	DHCP	DHCP 服务器
DNS	UDP	53	节点管理 LIF 和数据 LIF（NFS、CIFS）	DNS	DNS
NDMP	TCP	18600-18699	节点管理 LIF	目标服务器	NDMP 拷贝
SMTP	TCP	25	节点管理 LIF	邮件服务器	SMTP 警报，可用于AutoSupport
SNMP	TCP	161	节点管理 LIF	监控服务器	通过 SNMP 陷阱进行监控
	UDP	161	节点管理 LIF	监控服务器	通过 SNMP 陷阱进行监控
	TCP	162	节点管理 LIF	监控服务器	通过 SNMP 陷阱进行监控
	UDP	162	节点管理 LIF	监控服务器	通过 SNMP 陷阱进行监控
SnapMirror	TCP	11104	集群间 LIF	ONTAP集群间 LIF	SnapMirror集群间通信会话的管理
	TCP	11105	集群间 LIF	ONTAP集群间 LIF	SnapMirror数据传输
系统日志	UDP	514	节点管理 LIF	系统日志服务器	Syslog 转发消息

HA 调解器外部安全组的规则

Cloud Volumes ONTAP HA 中介的预定义外部安全组包括以下入站和出站规则。

入站规则

HA 中介的预定义安全组包括以下入站规则。

协议	端口	源	目的
TCP	3000	控制台代理的 CIDR	通过控制台代理访问 RESTful API

出站规则

HA 中介的预定义安全组打开所有出站流量。如果可以接受，请遵循基本的出站规则。如果您需要更严格的规则，请使用高级出站规则。

基本出站规则

HA 中介的预定义安全组包括以下出站规则。

协议	端口	目的
所有 TCP	全部	所有出站流量
所有 UDP	全部	所有出站流量

高级出站规则

如果您需要对出站流量制定严格的规则，则可以使用以下信息仅打开 HA 中介器出站通信所需的端口。

协议	端口	目标	目的
HTTP	80	AWS EC2 实例上的控制台代理的 IP 地址	下载中介器的升级版本
HTTPS	443	ec2.amazonaws.com	协助存储故障转移
UDP	53	ec2.amazonaws.com	协助存储故障转移

您可以创建从目标子网到 AWS EC2 服务的接口 VPC 端点，而不是打开端口 443 和 53。

HA 配置内部安全组的规则

Cloud Volumes ONTAP HA 配置的预定义内部安全组包括以下规则。该安全组支持 HA 节点之间以及中介与节点之间的通信。

控制台始终创建此安全组。您没有选择使用自己的。

入站规则

预定义安全组包括以下入站规则。

协议	端口	目的
所有流量	全部	HA 中介器和 HA 节点之间的通信

出站规则

预定义安全组包括以下出站规则。

协议	端口	目的
所有流量	全部	HA 中介器和 HA 节点之间的通信

控制台代理的规则

"查看控制台代理的安全组规则"

设置Cloud Volumes ONTAP以在 AWS 中使用客户管理的密钥

如果您想将 Amazon 加密与Cloud Volumes ONTAP一起使用，则需要设置 AWS 密钥管理服务 (KMS)。

步骤

1. 确保存在有效的客户主密钥 (CMK)。

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

   "AWS 文档：客户主密钥 (CMK)"

2. 通过添加以_密钥用户_身份向控制台提供权限的 IAM 角色来修改每个 CMK 的密钥策略。

   将身份和访问管理 (IAM) 角色添加为关键用户，可授予控制台使用 CMK 与Cloud Volumes ONTAP 的权限。

   "AWS 文档：编辑密钥"

3. 如果 CMK 位于不同的 AWS 账户中，请完成以下步骤：

   a. 从 CMK 所在的账户进入 KMS 控制台。

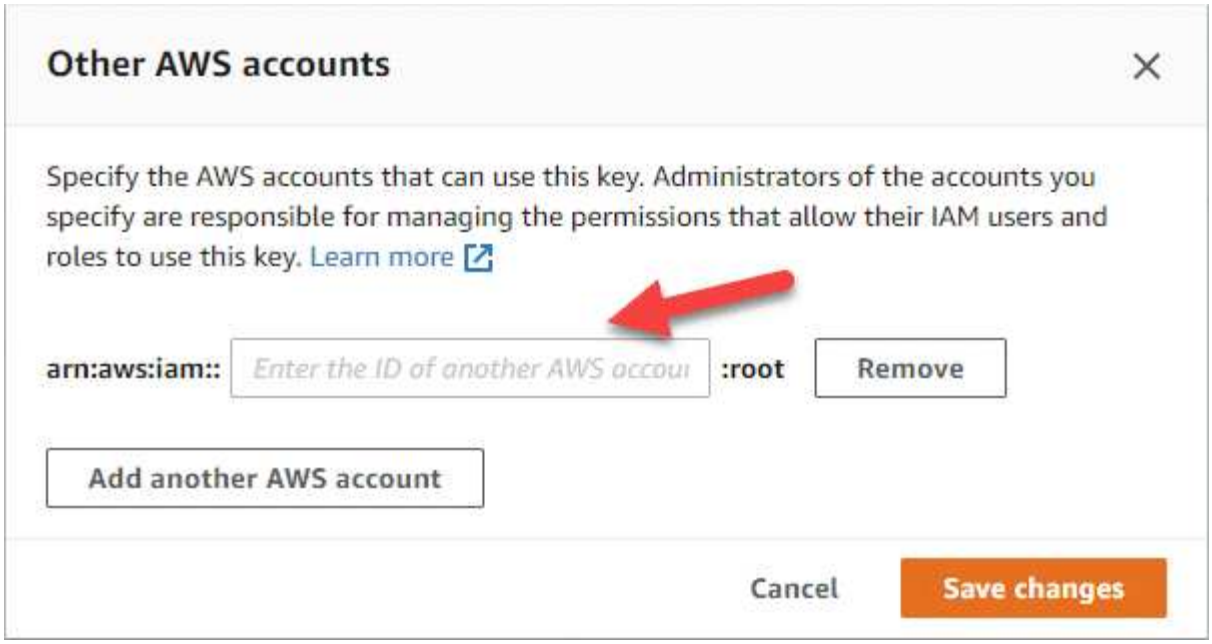
   b. 选择键。

   c. 在“常规配置”窗格中，复制密钥的 ARN。

      创建Cloud Volumes ONTAP系统时，您需要向控制台提供 ARN。

   d. 在 其他 **AWS** 账户 窗格中，添加为控制台提供权限的 AWS 账户。

      通常，这是部署控制台的帐户。如果 AWS 中未安装控制台，请使用您向控制台提供 AWS 访问密钥的帐户。



e. 现在切换到为控制台提供权限的 AWS 账户并打开 IAM 控制台。

f. 创建包含下面列出的权限的 IAM 策略。

g. 将策略附加到向控制台提供权限的 IAM 角色或 IAM 用户。

以下策略提供控制台使用来自外部 AWS 账户的 CMK 所需的权限。请务必修改“资源”部分中的区域和帐户 ID。

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

+
有关此过程的更多详细信息，请参阅 "AWS 文档：允许其他账户中的用户使用 KMS 密钥"。

4. 如果您使用的是客户管理的 CMK，请通过将Cloud Volumes ONTAP IAM 角色添加为_密钥用户_来修改 CMK 的密钥策略。

   如果您在 Cloud Volumes ONTAP 上启用了数据分层并希望加密存储在 Amazon Simple Storage Service

(Amazon S3) 存储桶中的数据，则需要执行此步骤。

您需要在部署Cloud Volumes ONTAP之后执行此步骤，因为 IAM 角色是在创建Cloud Volumes ONTAP系统时创建的。 （当然，您可以选择使用现有的Cloud Volumes ONTAP IAM 角色，因此可以先执行此步骤。）

"AWS 文档：编辑密钥"

为Cloud Volumes ONTAP节点设置 AWS IAM 角色

必须将具有所需权限的 AWS 身份和访问管理 (IAM) 角色附加到每个Cloud Volumes ONTAP节点。对于 HA 调解员来说也是如此。最简单的方法是让NetApp Console为您创建 IAM 角色，但您也可以使用自己的角色。

此任务是可选的。当您创建Cloud Volumes ONTAP系统时，默认选项是让控制台为您创建 IAM 角色。如果您企业的安全策略要求您自己创建 IAM 角色，请按照以下步骤操作。

AWS Secret Cloud 需要提供您自己的 IAM 角色。"了解如何在 C2S 中部署Cloud Volumes ONTAP" 。

步骤

1. 转到 AWS IAM 控制台。
2. 创建包含以下权限的 IAM 策略：
    - Cloud Volumes ONTAP节点的基本策略

标准区域

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Action": "s3:ListAllMyBuckets",
            "Resource": "arn:aws:s3:::*",
            "Effect": "Allow"
        }, {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws:s3:::fabric-pool-*",
            "Effect": "Allow"
        }, {
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject"
            ],
            "Resource": "arn:aws:s3:::fabric-pool-*",
            "Effect": "Allow"
        }
    ]
}
```

GovCloud（美国）区域

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Action": "s3:ListAllMyBuckets",
        "Resource": "arn:aws-us-gov:s3:::*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": "arn:aws-us-gov:s3:::fabric-pool-*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:GetObject",
            "s3:PutObject",
            "s3:DeleteObject"
        ],
        "Resource": "arn:aws-us-gov:s3:::fabric-pool-*",
        "Effect": "Allow"
    }]
}
```

绝密地区

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Action": "s3:ListAllMyBuckets",
        "Resource": "arn:aws-iso:s3:::*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": "arn:aws-iso:s3:::fabric-pool-*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:GetObject",
            "s3:PutObject",
            "s3:DeleteObject"
        ],
        "Resource": "arn:aws-iso:s3:::fabric-pool-*",
        "Effect": "Allow"
    }]
}
```

秘密区域

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Action": "s3:ListAllMyBuckets",
        "Resource": "arn:aws-iso-b:s3:::*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": "arn:aws-iso-b:s3:::fabric-pool-*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:GetObject",
            "s3:PutObject",
            "s3:DeleteObject"
        ],
        "Resource": "arn:aws-iso-b:s3:::fabric-pool-*",
        "Effect": "Allow"
    }]
}
```

- Cloud Volumes ONTAP节点的备份策略

  如果您计划将NetApp Backup and Recovery与Cloud Volumes ONTAP系统一起使用，则节点的 IAM 角色必须包括下面显示的第二个策略。

标准区域

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws:s3:::netapp-backup*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:ListAllMyBuckets",
                "s3:PutObjectTagging",
                "s3:GetObjectTagging",
                "s3:RestoreObject",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetObjectRetention",
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutObjectRetention"
            ],
            "Resource": "arn:aws:s3:::netapp-backup*/*",
            "Effect": "Allow"
        }
    ]
}
```

GovCloud（美国）区域

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws-us-gov:s3:::netapp-backup*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:ListAllMyBuckets",
                "s3:PutObjectTagging",
                "s3:GetObjectTagging",
                "s3:RestoreObject",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetObjectRetention",
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutObjectRetention"
            ],
            "Resource": "arn:aws-us-gov:s3:::netapp-backup*/*",
            "Effect": "Allow"
        }
    ]
}
```

绝密地区

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws-iso:s3:::netapp-backup*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:ListAllMyBuckets",
                "s3:PutObjectTagging",
                "s3:GetObjectTagging",
                "s3:RestoreObject",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetObjectRetention",
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutObjectRetention"
            ],
            "Resource": "arn:aws-iso:s3:::netapp-backup*/*",
            "Effect": "Allow"
        }
    ]
}
```

秘密区域

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws-iso-b:s3:::netapp-backup*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:ListAllMyBuckets",
                "s3:PutObjectTagging",
                "s3:GetObjectTagging",
                "s3:RestoreObject",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetObjectRetention",
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutObjectRetention"
            ],
            "Resource": "arn:aws-iso-b:s3:::netapp-backup*/*",
            "Effect": "Allow"
        }
    ]
}
```

- HA介导者

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:AssignPrivateIpAddresses",
                "ec2:CreateRoute",
                "ec2:DeleteRoute",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeVpcs",
                "ec2:ReplaceRoute",
                "ec2:UnassignPrivateIpAddresses",
                "sts:AssumeRole",
                "ec2:DescribeSubnets"
            ],
            "Resource": "*"
        }
    ]
}
```

3. 创建一个 IAM 角色并将您创建的策略附加到该角色。

结果

现在，您拥有可以在创建新的Cloud Volumes ONTAP系统时选择的 IAM 角色。

更多信息

- "AWS 文档：创建 IAM 策略"
- "AWS 文档：创建 IAM 角色"

在 AWS 中设置Cloud Volumes ONTAP许可

在您决定要对Cloud Volumes ONTAP使用哪种许可选项后，需要执行几个步骤才能在创建新系统时选择该许可选项。

免费增值

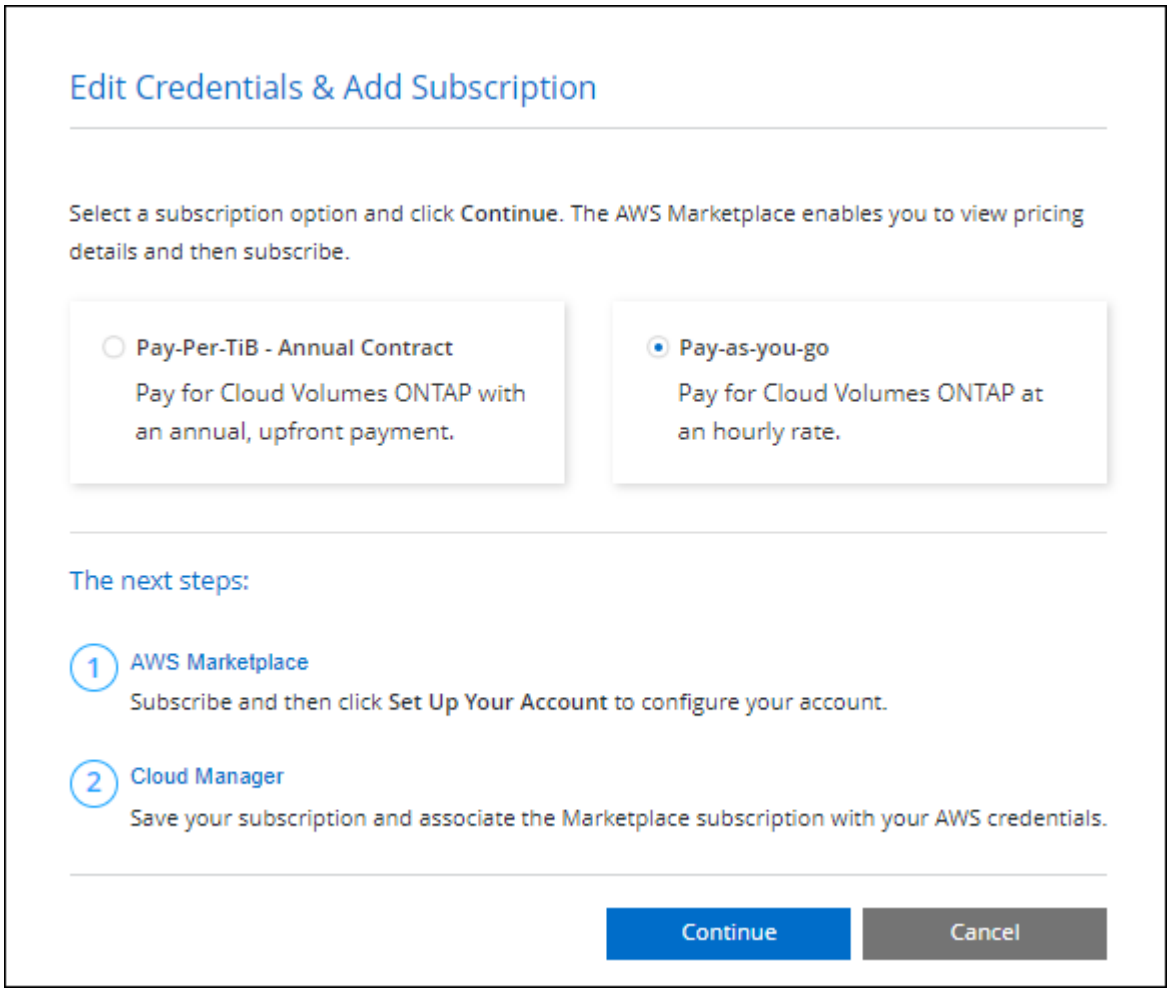
选择免费增值服务，免费使用Cloud Volumes ONTAP，最高可提供 500 GiB 的配置容量。"了解有关免费增值服务的更多信息" 。

步骤

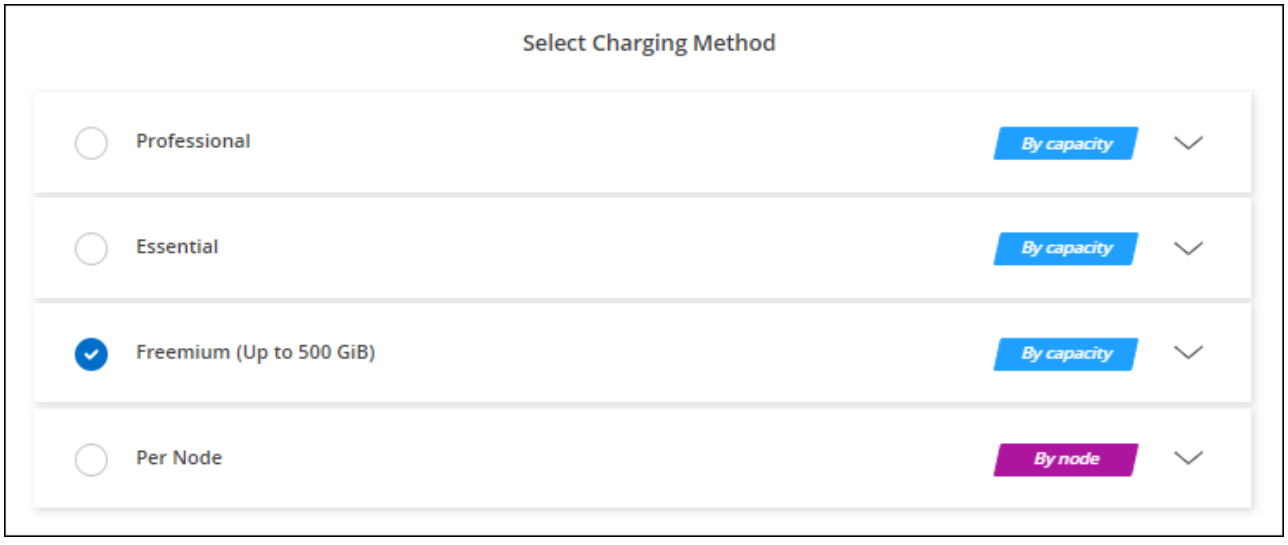
1. 从NetApp Console的左侧导航菜单中，选择“存储”>“管理”。
2. 在*系统*页面上，单击*添加系统*并按照步骤操作。
    a. 在“详细信息和凭证”页面上，单击“编辑凭证”>“添加订阅”，然后按照提示订阅 AWS Marketplace 中的即

用即付服务。

除非您超过 500 GiB 的预配置容量，否则您无需通过市场订阅付费，此时系统将自动转换为"基本套餐"。



a. 返回控制台后，到达收费方式页面时选择“免费增值”。



"查看在 AWS 中启动Cloud Volumes ONTAP 的分步说明" 。

基于容量的许可证

基于容量的许可使您能够按 TiB 容量支付Cloud Volumes ONTAP费用。基于容量的许可以_包_的形式提供：Essentials 包或 Professional 包。

Essentials 和 Professional 套餐提供以下几种消费模式或购买选项：

- 从NetApp购买的许可证（自带许可证 (BYOL)）
- AWS Marketplace 的按小时付费 (PAYGO) 订阅
- 来自 AWS Marketplace 的年度合同

"了解有关基于容量的许可的更多信息" 。

以下部分介绍了如何开始使用每种消费模型。

BYOL

通过从NetApp购买许可证 (BYOL) 进行预付款，以便在任何云提供商处部署Cloud Volumes ONTAP系统。

已限制 BYOL 许可证的购买、延期和续订。有关更多信息，请参阅 "Cloud Volumes ONTAP的 BYOL 许可可用性受限" 。

步骤

1. "联系NetApp销售人员获取许可证"
2. "将您的NetApp支持站点帐户添加到控制台"

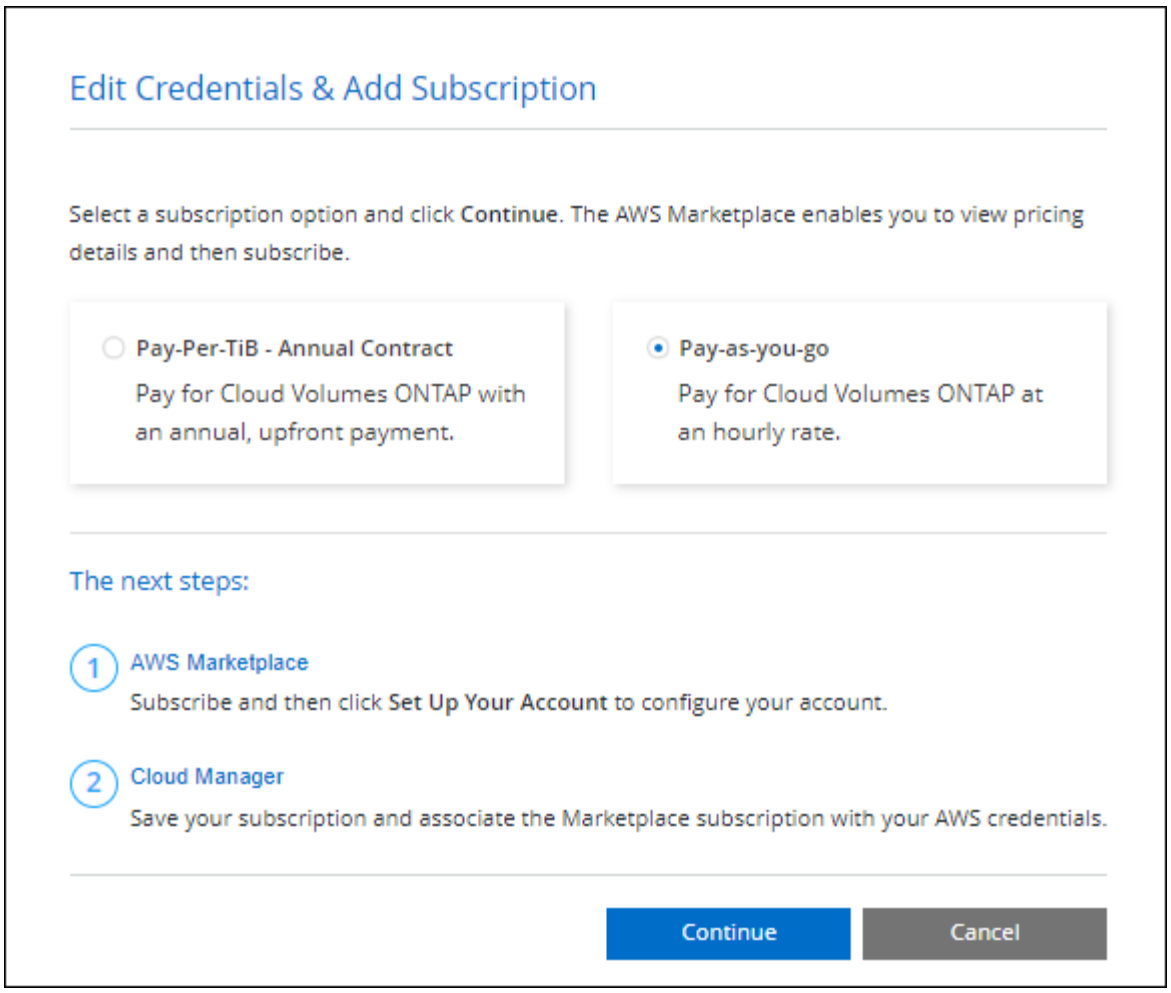
   控制台会自动查询 NetApp 的许可服务，以获取与您的NetApp支持站点帐户相关的许可证的详细信息。如果没有错误，控制台会自动将许可证添加到控制台。

   您必须先从控制台获取许可证，然后才能将其与Cloud Volumes ONTAP一起使用。如果需要的话，你可以"手动将许可证添加到控制台"。

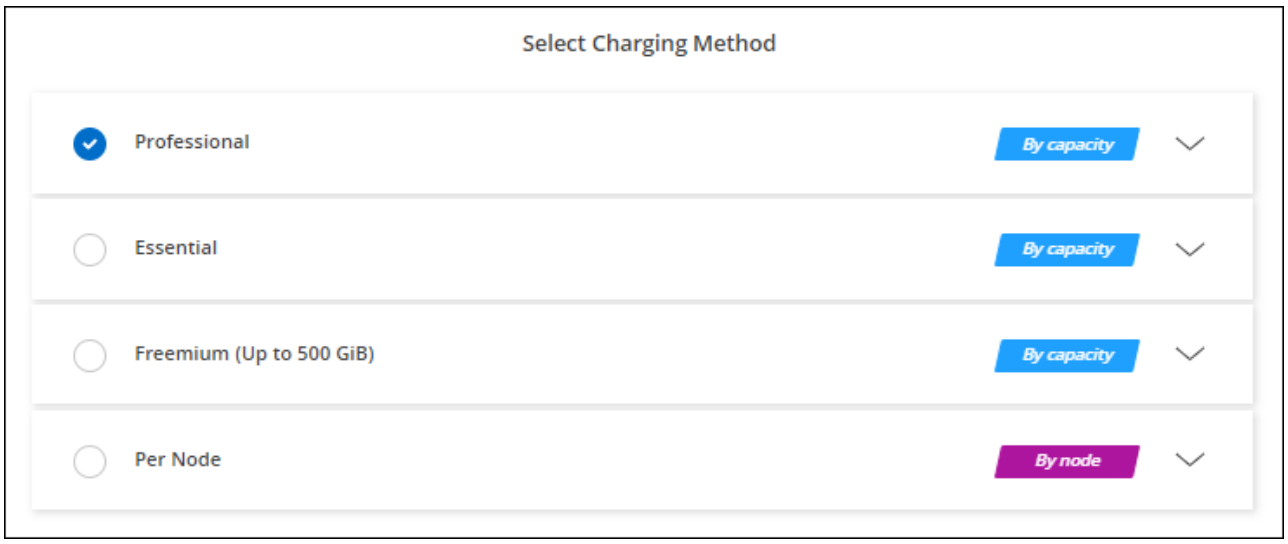
3. 在控制台的“系统”页面上，单击“添加系统”并按照步骤操作。

   a. 在“详细信息和凭证”页面上，单击“编辑凭证”>“添加订阅”，然后按照提示订阅 AWS Marketplace 中的即用即付服务。

      始终会先向您从NetApp购买的许可证收费，但如果您超出许可容量或许可证期限到期，则会按照市场上的小时费率向您收费。



a. 返回控制台后，在进入收费方式页面时选择基于容量的套餐。



"查看在 AWS 中启动Cloud Volumes ONTAP 的分步说明" 。

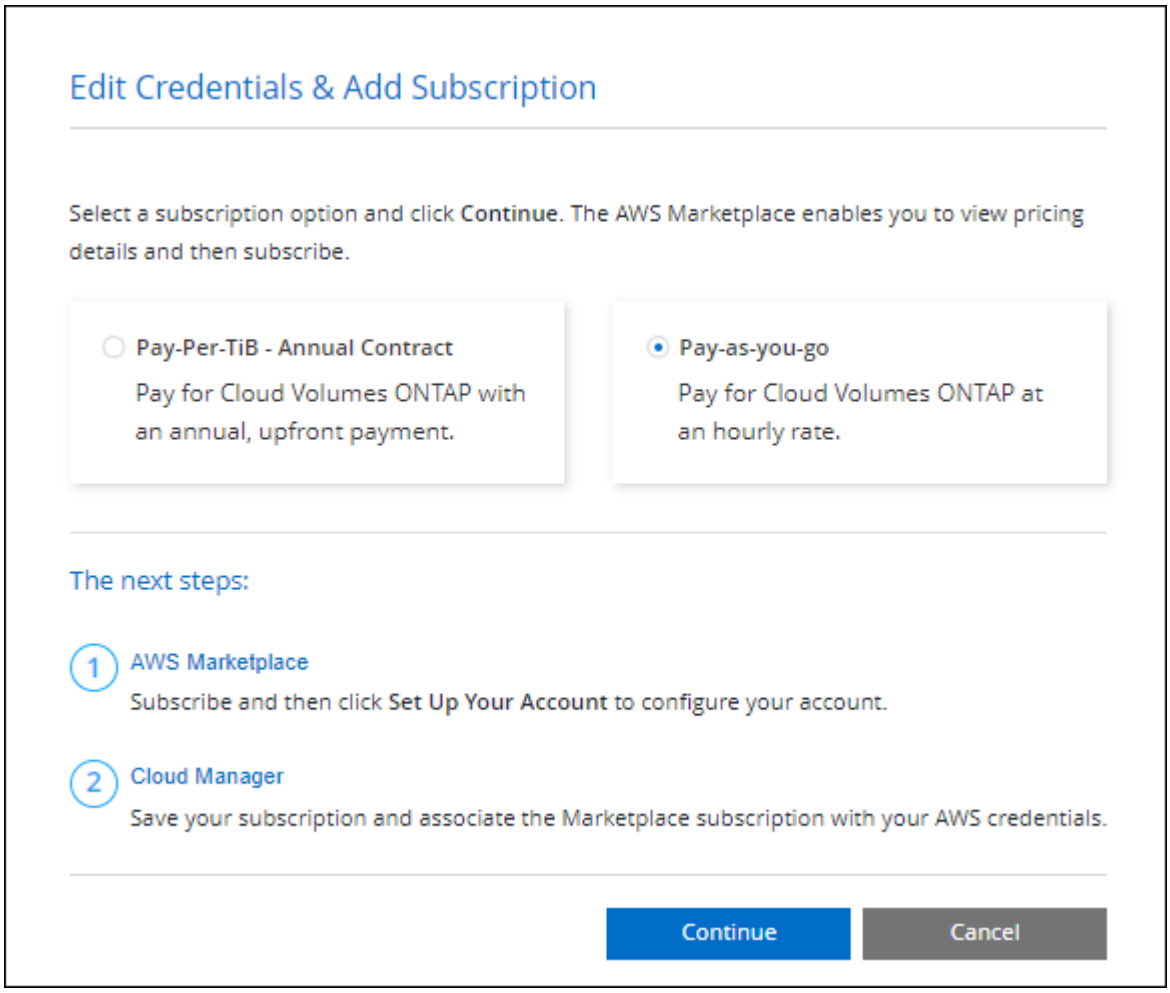
PAYGO 订阅

通过订阅云提供商市场提供的服务按小时付费。

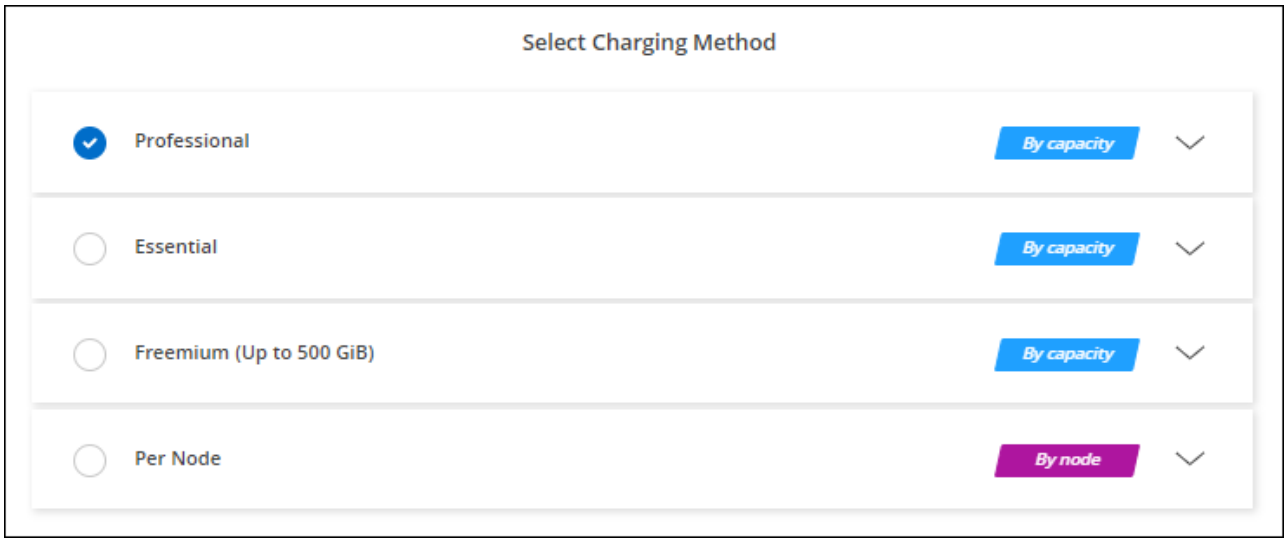
当您创建Cloud Volumes ONTAP系统时，控制台会提示您订阅 AWS Marketplace 中提供的协议。然后将该订阅与系统关联以进行收费。您可以使用相同的订阅来获取其他Cloud Volumes ONTAP系统。

步骤

1. 从左侧导航菜单中，选择“存储”>“管理”。
2. 在*系统*页面上，单击*添加系统*并按照步骤操作。
   a. 在“详细信息和凭证”页面上，单击“编辑凭证”>“添加订阅”，然后按照提示订阅 AWS Marketplace 中的即用即付服务



   b. 返回控制台后，在进入收费方式页面时选择基于容量的套餐。



"查看在 AWS 中启动Cloud Volumes ONTAP 的分步说明" 。

您可以从“设置”>“凭证”页面管理与您的 AWS 账户关联的 AWS Marketplace 订阅。 "了解如何管理您的 AWS 账户和订阅"

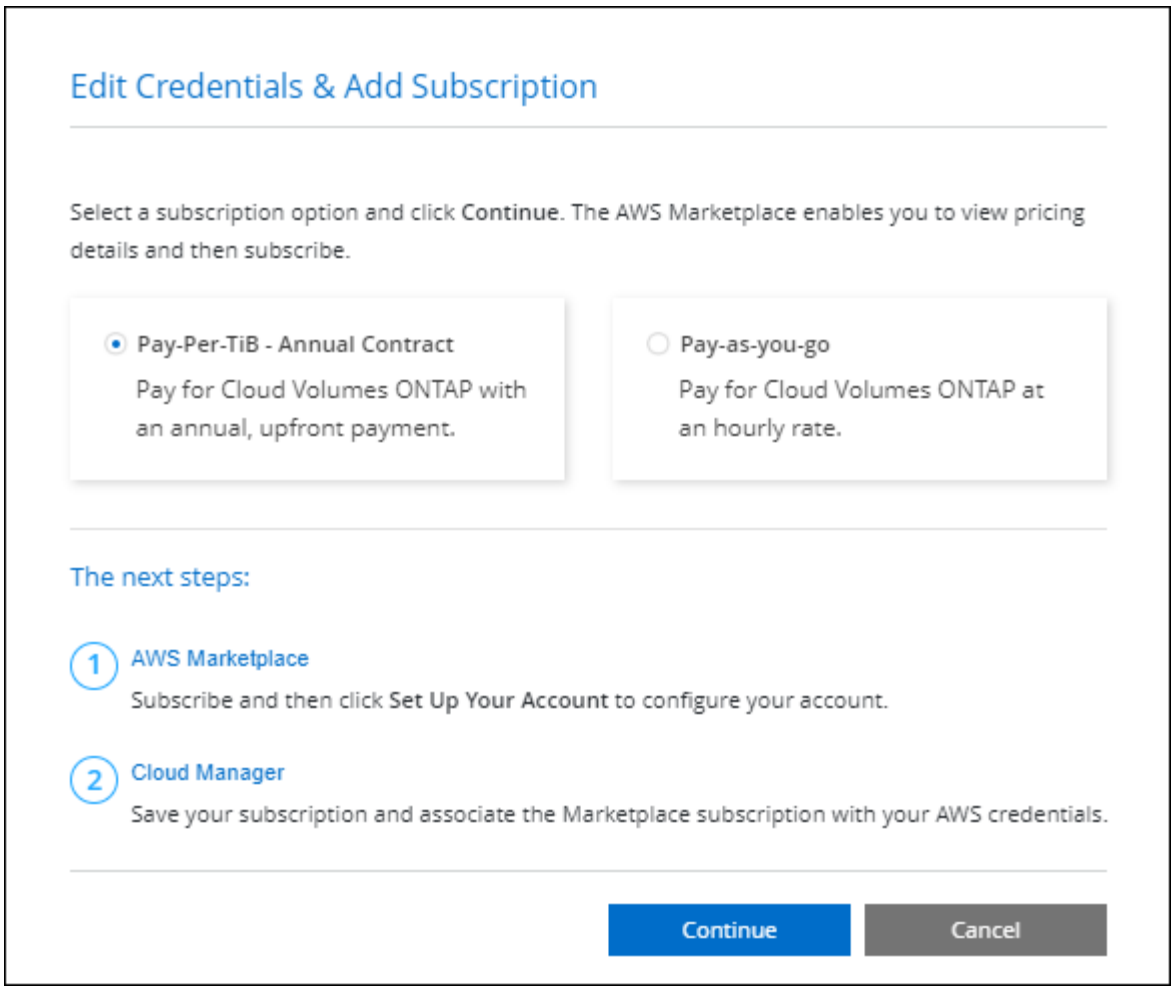
年度合同

从云提供商的市场购买年度合同，按年付款。

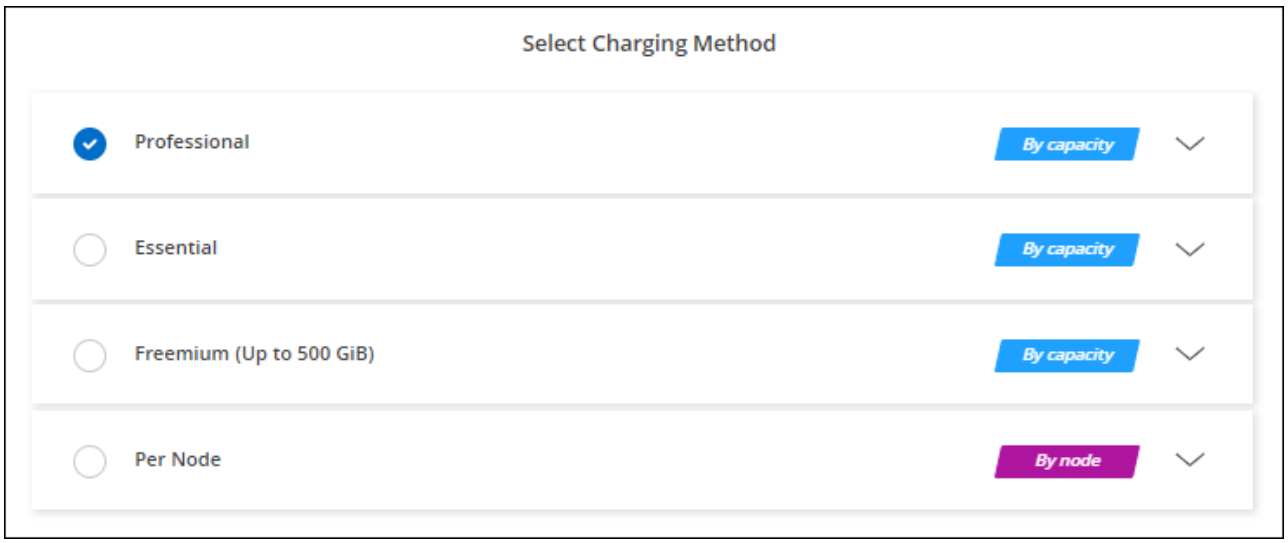
与按小时订阅类似，控制台会提示您订阅 AWS Marketplace 中提供的年度合同。

步骤

1. 在*系统*页面上，单击*添加系统*并按照步骤操作。
   a. 在*详细信息和凭证*页面上，单击*编辑凭证 > 添加订阅*，然后按照提示在 AWS Marketplace 中订阅年度合同。



b. 返回控制台后，在进入收费方式页面时选择基于容量的套餐。



"查看在 AWS 中启动Cloud Volumes ONTAP 的分步说明" 。

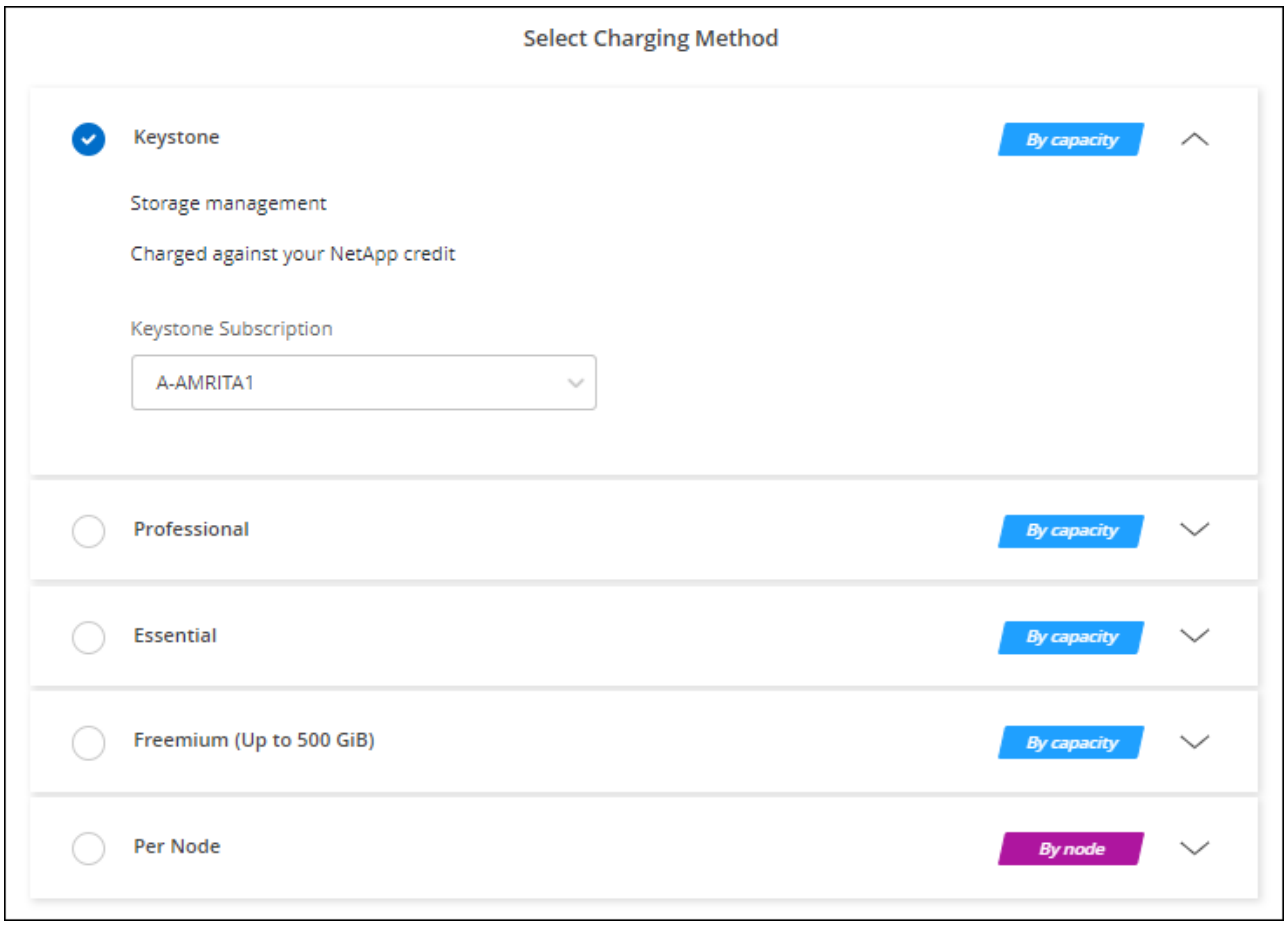
Keystone订阅

Keystone订阅是一种按需付费的订阅式服务。"了解有关NetApp Keystone订阅的更多信息" 。

步骤

1. 如果您尚未订阅， "联系NetApp"
2. 联系NetApp 为您的用户帐户授权一个或多个Keystone订阅。
3. NetApp授权您的帐户后，"链接您的订阅以用于Cloud Volumes ONTAP" 。
4. 在*系统*页面上，单击*添加系统*并按照步骤操作。

    a. 当提示选择收费方式时，选择Keystone Subscription 收费方式。



"查看在 AWS 中启动Cloud Volumes ONTAP 的分步说明" 。

基于节点的许可证

基于节点的许可证是Cloud Volumes ONTAP的上一代许可证。基于节点的许可证可以从NetApp (BYOL) 处购买，并且仅在特定情况下才可以续订许可证。有关信息，请参阅：

- "基于节点的许可证的可用性终止"
- "基于节点的许可证的可用性终止"
- "将基于节点的许可证转换为基于容量的许可证"

使用快速部署在 **AWS** 中部署**Cloud Volumes ONTAP**

您可以使用快速部署方法在 AWS 中部署Cloud Volumes ONTAP，适用于单节点和高可用性 (HA) 配置。与先进的方法相比，这种简化的流程减少了部署步骤。它还通过在单个页面上自动设置默认值并最小化导航来提供更清晰的工作流程。

开始之前

您需要以下内容才能从NetApp Console在 AWS 中添加Cloud Volumes ONTAP系统。

- 已启动并正在运行的控制台代理。
  - 你应该有一个 "与您的项目或工作区关联的控制台代理"。
  - "您应该准备好让控制台代理始终处于运行状态" 。
- 了解您想要使用的配置。

  您应该已经做好准备，选择配置并从管理员处获取 AWS 网络信息。有关详细信息，请参阅"规划您的Cloud Volumes ONTAP配置"。
- 了解设置Cloud Volumes ONTAP许可所需的条件。

  "了解如何设置许可" 。
- CIFS 配置的 DNS 和 Active Directory。

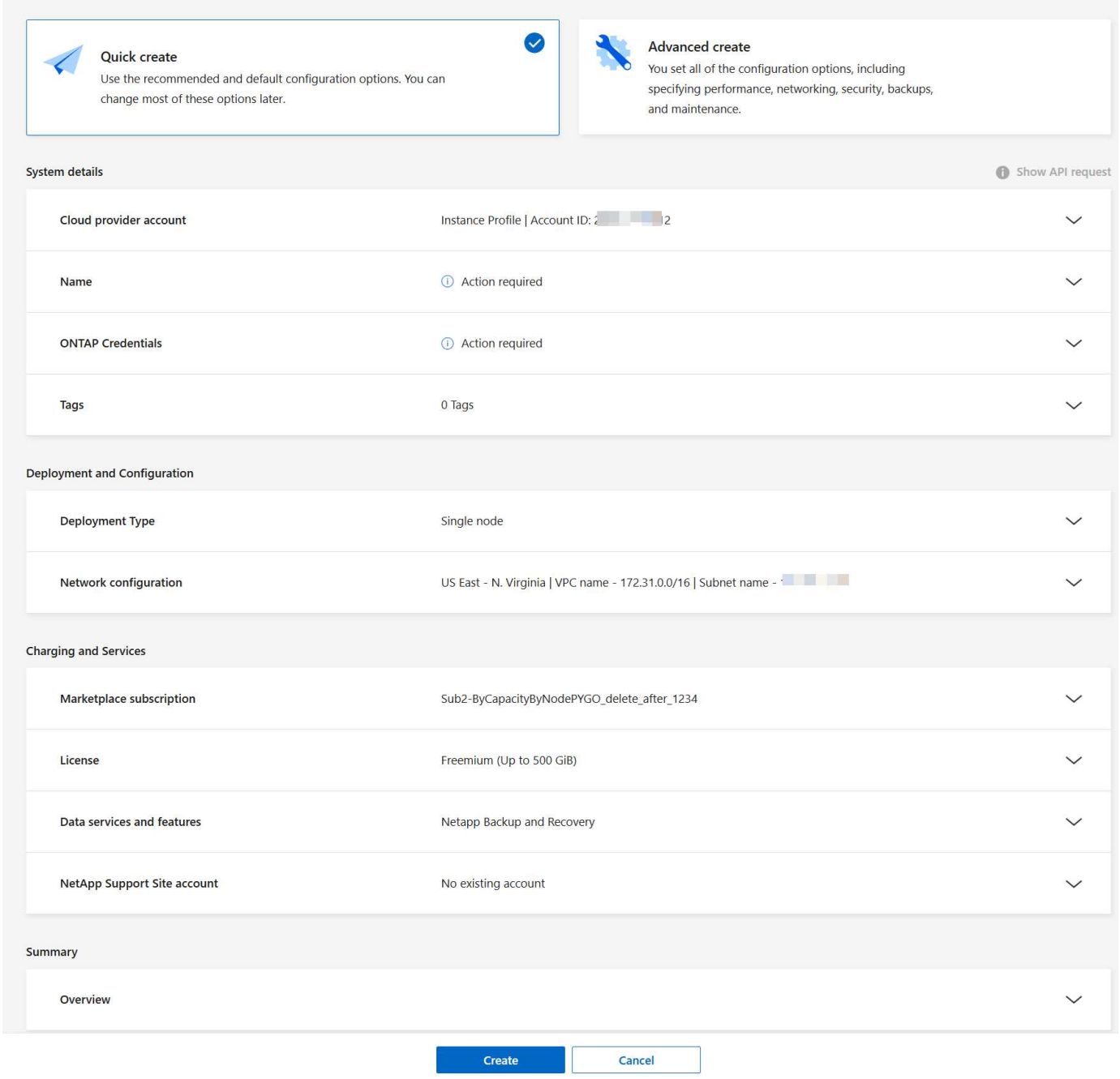
  有关详细信息，请参阅"AWS 中Cloud Volumes ONTAP的网络要求"。

关于此任务

创建Cloud Volumes ONTAP系统后， NetApp Console会立即在指定的 VPC 中启动测试实例以验证连接性。如果成功，控制台会立即终止实例，然后开始部署系统。如果控制台无法验证连接，则系统创建失败。测试实例可以是 `t2.nano`（对于默认 VPC 租赁）或 `m3.medium`（适用于专用 VPC 租赁）。

步骤

1. 从左侧导航菜单中，选择“存储”>“管理”。
2. 在 Canvas 页面上，单击 添加系统 并按照提示进行操作。
3. 选择 **Amazon Web Services** > * Cloud Volumes ONTAP* > 添加新。默认情况下选择*快速创建*选项。



系统详细信息

1. 云提供商帐户：帐户详细信息将根据您选择的控制台代理自动填充。如果您有多个帐户，请选择要使用的帐户。如果控制台代理不可用，系统将提示您 "创建控制台代理"。
2. 名称：系统名称。控制台使用系统（集群）名称来命名Cloud Volumes ONTAP系统和 Amazon EC2 实例。如果您选择该选项，它还会使用该名称作为预定义安全组的前缀。
3. * ONTAP凭据* 这些是Cloud Volumes ONTAP集群管理员帐户的凭据。您可以使用这些凭据通过ONTAP System Manager 或ONTAP CLI 连接到Cloud Volumes ONTAP 。您可以保留默认的_admin_用户名，也可以将其更改为自定义用户名。
4. 标签 AWS 标签是您的 AWS 资源的元数据。控制台将标签添加到Cloud Volumes ONTAP实例以及与该实例关联的每个 AWS 资源。创建Cloud Volumes ONTAP系统时，您可以从用户界面添加最多 15 个标签，然后可以在创建后添加更多标签。请注意，创建系统时，API 不会将您限制为四个标签。有关标签的信息，请参阅 "AWS 文档：标记您的 Amazon EC2 资源"。

部署和配置

1. 部署类型：选择您要使用的部署类型，单节点、单个可用区 (AZ) 中的高可用性 (HA) 或多个 AZ 中的 HA。
2. 网络配置：输入您在 "AWS 工作表"。
   a. **AWS** 区域：默认选择关联云账户的、拥有子网资源的 VPC 所在区域。
   b. **VPC**：输入具有子网的 AWS 区域的 VPC。如果没有子网，则选择 VPC 的默认值。
   c. 子网：您只能为 VPC 选择一个子网，以用于单节点部署或单 AZ 中的 HA 部署。

高可用性

如果您选择了 HA 配置，请输入以下信息：

单可用区高可用性

1. 调解器访问：指定调解器访问信息。调解器是一个单独的实例，用于监控 HA 对的健康状况并在发生故障时提供仲裁。提供密钥对名称以使中介实例能够连接到 AWS EC2 服务，并选择连接方法。

多个可用区中的高可用性

1. 可用区域和中介：选择每个节点的可用区域 (AZ) 以及要部署Cloud Volumes ONTAP HA 对的中介和相应子网。
2. 浮动 **IP**：如果您选择多个 AZ，请为 NFS 和 CIFS 服务以及集群和 SVM 管理指定浮动 IP 地址。 IP 地址必须位于该区域内所有 VPC 的 CIDR 块之外。有关更多详细信息，请参阅"多个可用区中Cloud Volumes ONTAP HA 的 AWS 网络要求"。
3. 调解器访问：指定调解器访问信息。调解器是一个单独的实例，用于监控 HA 对的健康状况并在发生故障时提供仲裁。提供密钥对名称以使中介实例能够连接到 AWS EC2 服务，并选择连接方法。
4. 路由表：如果您选择了多个 AZ，请选择包含到浮动 IP 地址的路由的路由表。如果您有多个路由表，则选择正确的路由表非常重要。否则，某些客户端可能无法访问Cloud Volumes ONTAP HA 对。有关路由表的更多信息，请参阅 "AWS 文档：路由表"。

充电和服务

1. 市场订阅：选择您想要与此Cloud Volumes ONTAP系统一起使用的 AWS 市场订阅。
2. 许可证：选择您想要与此Cloud Volumes ONTAP系统一起使用的许可证类型。您可以从专业版、基本版和高级版许可证中进行选择。有关不同许可证的信息，请参阅"了解Cloud Volumes ONTAP许可证"。
3. 数据服务和功能：保持服务启用或禁用您不想与Cloud Volumes ONTAP一起使用的服务。
   - "了解有关NetApp分类的更多信息"
   - "了解有关NetApp Backup and Recovery的更多信息"
   - "了解Cloud Volumes ONTAP上的 WORM 存储"

   如果您想利用 WORM 和数据分层，则必须禁用备份和恢复并部署版本 9.8 或更高版本的Cloud Volumes ONTAP系统。

   - * NetApp支持站点帐户*：如果您有多个帐户，请选择要使用的帐户。

摘要

检查或编辑您输入的详细信息，然后单击*创建*。

部署过程完成后，请勿修改 AWS 云门户中系统生成的Cloud Volumes ONTAP配置，尤其是系统标签。对这些配置所做的任何更改都可能导致意外行为或数据丢失。

相关链接

- "规划您的Cloud Volumes ONTAP配置"
- "使用高级部署在 AWS 中部署Cloud Volumes ONTAP"

在 AWS 中启动Cloud Volumes ONTAP

您可以在单系统配置中启动Cloud Volumes ONTAP ，也可以在 AWS 中以 HA 对的形式启动 Cloud Volumes ONTAP。此方法提供了高级部署体验，与快速部署方法相比，它提供了更多的配置选项和灵活性。

开始之前

开始之前您需要以下内容。

- 已启动并正在运行的控制台代理。
  - 你应该有一个 "与您的系统关联的控制台代理"。
  - "您应该准备好让控制台代理始终处于运行状态" 。
- 了解您想要使用的配置。

  您应该已经做好准备，选择配置并从管理员处获取 AWS 网络信息。有关详细信息，请参阅"规划您的Cloud Volumes ONTAP配置"。
- 了解设置Cloud Volumes ONTAP许可所需的条件。

  "了解如何设置许可" 。
- CIFS 配置的 DNS 和 Active Directory。

  有关详细信息，请参阅"AWS 中Cloud Volumes ONTAP的网络要求"。

在 AWS 中启动单节点Cloud Volumes ONTAP系统

如果您想在 AWS 中启动Cloud Volumes ONTAP ，则需要在NetApp Console中创建一个新系统。

关于此任务

创建系统后，控制台会立即在指定的 VPC 中启动测试实例以验证连接性。如果成功，控制台将立即终止实例，然后开始部署Cloud Volumes ONTAP系统。如果无法验证连接，系统创建将失败。测试实例可以是 `t2.nano`（对于默认 VPC 租赁）或 `m3.medium`（适用于专用 VPC 租赁）。

步骤

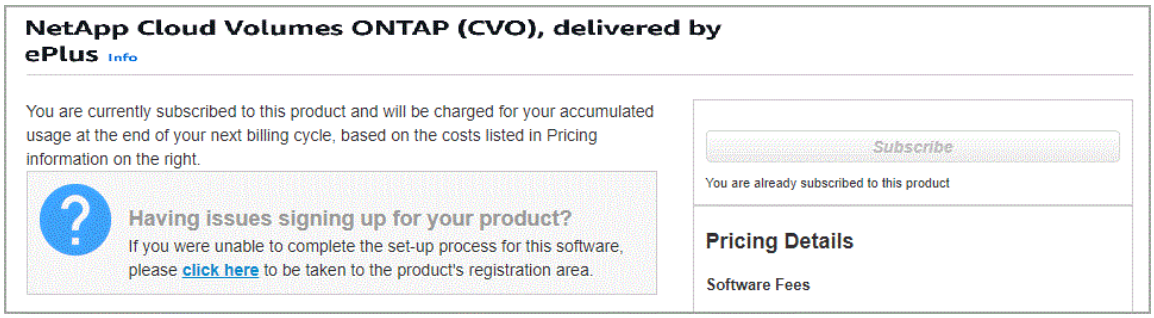
1. 从左侧导航菜单中，选择“存储”>“管理”。
2. 在*系统*页面上，单击*添加系统*并按照提示进行操作。
3. 选择 **Amazon Web Services** 和 * Cloud Volumes ONTAP Single Node*。

4. 选择*高级创建*。由于默认选择了*快速创建*模式，您可能会看到一条有关默认值的消息。单击“继续”。
5. 如果出现提示， "创建控制台代理" 。
6. 详细信息和凭证：可选择更改 AWS 凭证和订阅，输入系统名称，根据需要添加标签，然后输入密码。

   此页面中的某些字段是不言自明的。下表描述了您可能需要指导的字段：

字段	描述
系统名称	控制台使用系统名称来命名Cloud Volumes ONTAP系统和 Amazon EC2 实例。如果您选择该选项，它还会使用该名称作为预定义安全组的前缀。
添加标签	AWS 标签是您的 AWS 资源的元数据。控制台将标签添加到Cloud Volumes ONTAP实例以及与该实例关联的每个 AWS 资源。创建系统时，您可以从用户界面添加最多四个标签，然后可以在创建系统后添加更多标签。请注意，创建系统时，API 不会将您限制为四个标签。有关标签的信息，请参阅 "AWS 文档：标记您的 Amazon EC2 资源"。
用户名和密码	这些是Cloud Volumes ONTAP集群管理员帐户的凭据。您可以使用这些凭据通过ONTAP System Manager 或ONTAP CLI 连接到Cloud Volumes ONTAP 。保留默认的_admin_用户名或将其更改为自定义用户名。
编辑凭证	选择与您要部署此系统的帐户关联的 AWS 凭证。您还可以将 AWS 市场订阅与此Cloud Volumes ONTAP系统关联起来使用。点击“添加订阅”将所选凭证与新的 AWS 市场订阅关联。订阅可以是年度合同，也可以是按小时付费的Cloud Volumes ONTAP 。https://docs.netapp.com/us-en/bluexp-setup-admin/task-adding-aws-accounts.html["了解如何向NetApp Console添加其他 AWS 凭证"^] 。

   如果多个 IAM 用户在同一个 AWS 账户中工作，则每个用户都需要订阅。第一个用户订阅后，AWS 市场会通知后续用户他们已经订阅，如下图所示。当 AWS 账户有订阅时，每个 IAM 用户都需要将自己与该订阅关联起来。如果您看到下面显示的消息，请单击“单击此处”链接转到控制台网站并完成该过
   程。



7. 服务：保持服务启用或禁用您不想与Cloud Volumes ONTAP一起使用的单个服务。
   - "了解有关NetApp Data Classification的更多信息"
   - "了解有关NetApp Backup and Recovery的更多信息"

   如果您想使用 WORM 和数据分层，则必须禁用备份和恢复并部署版本 9.8 或更高版本的Cloud Volumes ONTAP系统。

8. 位置和连接：输入您在 "AWS 工作表"。

下表描述了您可能需要指导的字段：

字段	描述
VPC	如果您有 AWS Outpost，则可以通过选择 Outpost VPC 在该 Outpost 中部署单节点Cloud Volumes ONTAP系统。体验与驻留在 AWS 中的任何其他 VPC 相同。
生成的安全组	如果您让控制台为您生成安全组，则需要选择如何允许流量： • 如果您选择*仅限选定的 VPC*，则入站流量的来源是选定 VPC 的子网范围和控制台代理所在 VPC 的子网范围。这是推荐的选项。 • 如果您选择*所有 VPC*，则入站流量的来源是 0.0.0.0/0 IP 范围。
使用现有的安全组	如果您使用现有的防火墙策略，请确保它包含所需的规则。"了解Cloud Volumes ONTAP的防火墙规则" 。

9. 数据加密：选择无数据加密或 AWS 管理加密。

   对于 AWS 管理的加密，您可以从您的账户或其他 AWS 账户中选择不同的客户主密钥 (CMK)。

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

   "了解如何为Cloud Volumes ONTAP设置 AWS KMS" 。

   "了解有关受支持的加密技术的更多信息" 。

10. 收费方式和 **NSS** 帐户：指定您想要在此系统中使用的收费选项，然后指定NetApp支持站点帐户。
    - "了解Cloud Volumes ONTAP的许可选项" 。
    - "了解如何设置许可" 。
11. * Cloud Volumes ONTAP配置*（仅限年度 AWS 市场合同）：查看默认配置并单击*继续*或单击*更改配置*以选择您自己的配置。

    如果保留默认配置，则只需要指定一个卷，然后审核并批准该配置。

12. 预配置包：选择其中一个包以快速启动Cloud Volumes ONTAP，或单击*更改配置*以选择您自己的配置。

    如果您选择其中一个包，那么您只需要指定一个卷，然后审核并批准配置。

13. **IAM** 角色：最好保留默认选项，让控制台为您创建角色。

    如果您希望使用自己的政策，则必须满足"Cloud Volumes ONTAP节点的策略要求"。

14. 许可：根据需要更改Cloud Volumes ONTAP版本并选择实例类型和实例租赁。

    如果所选版本有较新的候选版本、通用版本或补丁版本，则控制台在创建系统时会将系统更新到该版本。例如，如果您选择Cloud Volumes ONTAP 9.13.1 并且 9.13.1 P4 可用，则会发生更新。更新不会从一个版本发生到另一个版本 - 例如，从 9.13 到 9.14。

15. 底层存储资源：选择磁盘类型，配置底层存储，并选择是否保持数据分层启用。

请注意以下事项：

- 磁盘类型适用于初始卷（和聚合）。您可以为后续卷（和聚合）选择不同的磁盘类型。
- 如果您选择 gp3 或 io1 磁盘，控制台将使用 AWS 中的弹性卷功能根据需要自动增加底层存储磁盘容量。您可以根据您的存储需求选择初始容量，并在部署Cloud Volumes ONTAP后进行修改。"了解有关 AWS 弹性卷支持的更多信息" 。
- 如果您选择 gp2 或 st1 磁盘，则可以为初始聚合中的所有磁盘以及使用简单配置选项时控制台创建的任何其他聚合选择磁盘大小。您可以使用高级分配选项创建使用不同磁盘大小的聚合。
- 您可以在创建或编辑卷时选择特定的卷分层策略。
- 如果您禁用数据分层，则可以在后续聚合上启用它。

  "了解数据分层的工作原理" 。

16. 写入速度和 **WORM**：

    a. 如果需要，选择*正常*或*高*写入速度。

       "了解有关写入速度的更多信息" 。

    b. 如果需要，请激活一次写入、多次读取 (WORM) 存储。

       如果为Cloud Volumes ONTAP 9.7 及更低版本启用了数据分层，则无法启用 WORM。启用 WORM 和分层后，恢复或降级到Cloud Volumes ONTAP 9.8 的操作将被阻止。

    "了解有关 WORM 存储的更多信息" 。

    a. 如果您激活 WORM 存储，请选择保留期限。

17. 创建卷：输入新卷的详细信息或单击*跳过*。

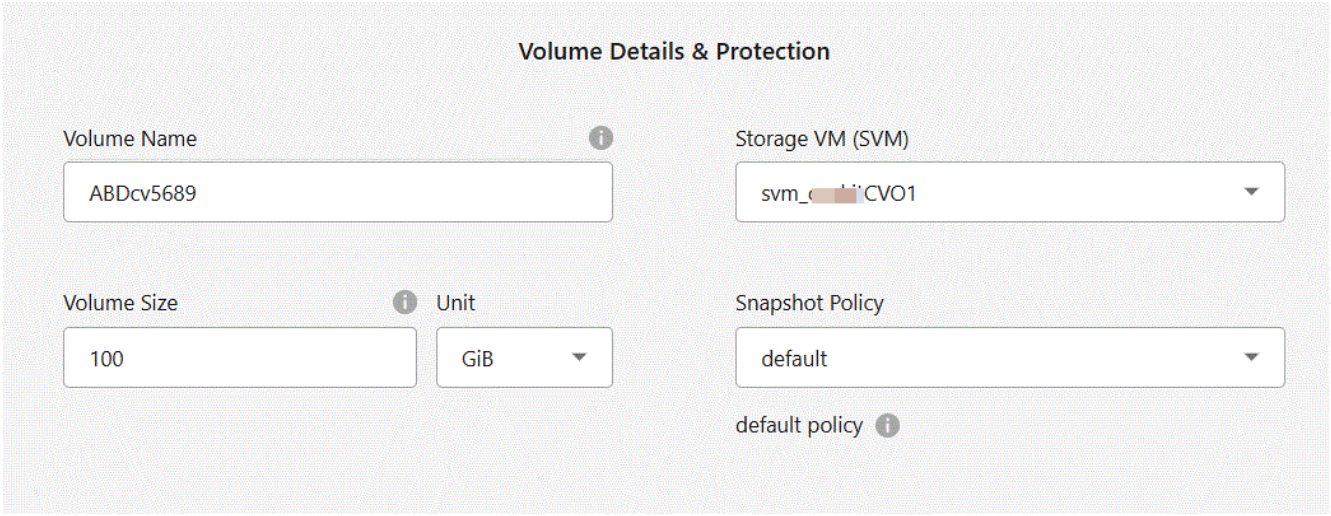
    "了解支持的客户端协议和版本" 。

    此页面中的某些字段是不言自明的。下表描述了您可能需要指导的字段：

字段	描述
大小	您可以输入的最大大小很大程度上取决于您是否启用精简配置，这使您能够创建比当前可用的物理存储更大的卷。
访问控制（仅适用于 NFS）	导出策略定义了子网中可以访问卷的客户端。默认情况下，控制台输入一个提供对子网中所有实例的访问权限的值。
权限和用户/组（仅适用于 CIFS）	这些字段使您能够控制用户和组对共享的访问级别（也称为访问控制列表或 ACL）。您可以指定本地或域 Windows 用户或组，或者 UNIX 用户或组。如果指定域 Windows 用户名，则必须使用域\用户名格式包含用户的域。
Snapshot 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 副本是时间点文件系统映像，它不会影响性能并且只需要最少的存储空间。您可以选择默认策略或无策略。对于瞬态数据，您可能选择无：例如，对于 Microsoft SQL Server，请选择 tempdb。
高级选项（仅适用于 NFS）	为卷选择一个 NFS 版本：NFSv3 或 NFSv4。

字段	描述
启动器组和 IQN（仅适用于 iSCSI）	iSCSI 存储目标称为 LUN（逻辑单元），并作为标准块设备呈现给主机。启动器组是 iSCSI 主机节点名称表，用于控制哪些启动器可以访问哪些 LUN。iSCSI 目标通过标准以太网网络适配器 (NIC)、带有软件启动器的 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。当您创建 iSCSI 卷时，控制台会自动为您创建一个 LUN。我们通过为每个卷创建一个 LUN 来简化操作，因此无需进行任何管理。创建卷后，"使用 IQN 从主机连接到 LUN" 。

下图显示了卷创建向导的第一页：



18. **CIFS** 设置：如果您选择了 CIFS 协议，请设置 CIFS 服务器。

字段	描述
DNS 主 IP 地址和辅助 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 服务器必须包含定位 CIFS 服务器将加入的域的 Active Directory LDAP 服务器和域控制器所需的服务位置记录 (SRV)。
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 域内指定组织单位 (OU) 的 Windows 帐户的名称和密码。
CIFS 服务器 NetBIOS 名称	AD 域中唯一的 CIFS 服务器名称。
组织单位	AD 域内与 CIFS 服务器关联的组织单位。默认值为 CN=Computers。如果将 AWS Managed Microsoft AD 配置为Cloud Volumes ONTAP 的AD 服务器，则应在此字段中输入 **OU=Computers,OU=corp**。
DNS 域	Cloud Volumes ONTAP存储虚拟机 (SVM) 的 DNS 域。大多数情况下，该域与 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。如果您需要使用不同的地址配置 NTP 服务器，那么您应该使用 API。请参阅 "NetApp Console自动化文档"了解详情。请注意，只有在创建 CIFS 服务器时才能配置 NTP 服务器。创建 CIFS 服务器后，它不可配置。

19. 使用情况配置文件、磁盘类型和分层策略：选择是否要启用存储效率功能，并在需要时编辑卷分层策略。

    更多信息，请参阅"了解卷使用情况"，"数据分层概述" ， 和 "KB：CVO 支持哪些内联存储效率功能？"

20. 审核并批准：审核并确认您的选择。
    a. 查看有关配置的详细信息。
    b. 单击“更多信息”以查看有关支持和控制台将购买的 AWS 资源的详细信息。
    c. 选中*我明白…*复选框。
    d. 单击“开始”。

结果

控制台启动Cloud Volumes ONTAP实例。您可以在*审计*页面上跟踪进度。

如果您在启动Cloud Volumes ONTAP实例时遇到任何问题，请查看失败消息。您也可以选择系统并单击*重新创建环境*。

如需更多帮助，请访问 "NetApp Cloud Volumes ONTAP支持"。

> 部署过程完成后，请勿修改 AWS 云门户中系统生成的Cloud Volumes ONTAP配置，尤其是系统标签。对这些配置所做的任何更改都可能导致意外行为或数据丢失。

完成后

- 如果您配置了 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共享并创建文件。
- 如果要将配额应用于卷，请使用ONTAP系统管理器或ONTAP CLI。

  配额使您能够限制或跟踪用户、组或 qtree 使用的磁盘空间和文件数量。

在 **AWS** 中启动**Cloud Volumes ONTAP HA** 对

如果您想在 AWS 中启动Cloud Volumes ONTAP HA 对，则需要在控制台中创建一个 HA 系统。

局限性

目前，AWS Outposts 不支持 HA 对。

关于此任务

创建Cloud Volumes ONTAP系统后，控制台会立即在指定的 VPC 中启动测试实例以验证连接性。如果成功，控制台将立即终止实例，然后开始部署Cloud Volumes ONTAP系统。如果无法验证连接，系统创建将失败。测试实例可以是 `t2.nano`（对于默认 VPC 租赁）或 `m3.medium`（适用于专用 VPC 租赁）。

步骤

1. 从左侧导航菜单中，选择“存储”>“管理”。
2. 在*系统*页面上，单击*添加系统*并按照提示进行操作。
3. 选择 **Amazon Web Services** 和 * Cloud Volumes ONTAP HA*。

   一些 AWS 本地区域可用。

您必须先启用本地区域并在 AWS 账户的本地区域中创建子网，然后才能使用 AWS 本地区域。按照*选择加入 AWS 本地区域*和*将您的 Amazon VPC 扩展到本地区域*中的步骤操作"AWS 教程“开始使用 AWS 本地区域部署低延迟应用程序"。

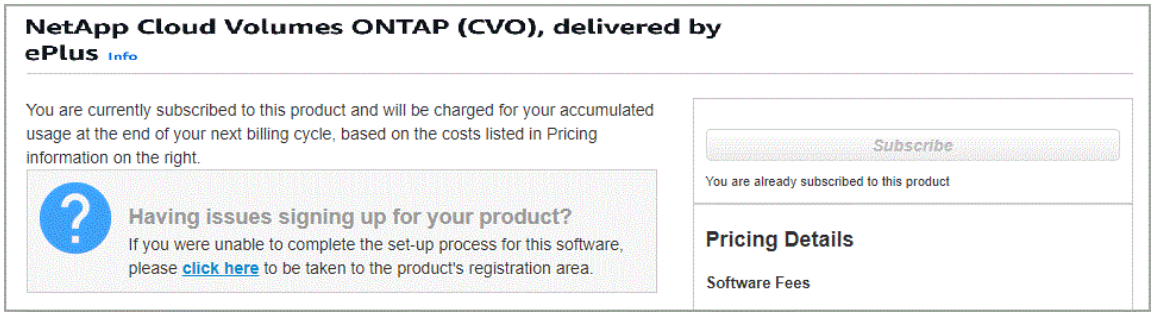
如果您运行的是控制台代理 3.9.36 或更低版本，则需要添加 `DescribeAvailabilityZones`AWS EC2 控制台中 AWS 角色的权限。

4. 详细信息和凭证：可选择更改 AWS 凭证和订阅，输入系统名称，根据需要添加标签，然后输入密码。

   此页面中的某些字段是不言自明的。下表描述了您可能需要指导的字段：

字段	描述
系统名称	控制台使用系统名称来命名Cloud Volumes ONTAP系统和 Amazon EC2 实例。如果您选择该选项，它还会使用该名称作为预定义安全组的前缀。
添加标签	AWS 标签是您的 AWS 资源的元数据。控制台将标签添加到Cloud Volumes ONTAP实例以及与该实例关联的每个 AWS 资源。创建系统时，您可以从用户界面添加最多四个标签，然后可以在创建系统后添加更多标签。请注意，创建系统时，API 不会将您限制为四个标签。有关标签的信息，请参阅 "AWS 文档：标记您的 Amazon EC2 资源"。
用户名和密码	这些是Cloud Volumes ONTAP集群管理员帐户的凭据。您可以使用这些凭据通过ONTAP System Manager 或ONTAP CLI 连接到Cloud Volumes ONTAP 。保留默认的_admin_用户名或将其更改为自定义用户名。
编辑凭证	选择要用于此Cloud Volumes ONTAP系统的 AWS 凭证和市场订阅。点击“添加订阅”将所选凭证与新的 AWS 市场订阅关联。订阅可以是年度合同，也可以是按小时付费的Cloud Volumes ONTAP 。如果您直接从NetApp购买了许可证（自带许可证 (BYOL)），则无需 AWS 订阅。NetApp已限制 BYOL 许可证的购买、延期和续订。有关更多信息，请参阅 "Cloud Volumes ONTAP的 BYOL 许可可用性受限" 。https://docs.netapp.com/us-en/bluexp-setup-admin/task-adding-aws-accounts.html["了解如何向控制台添加其他 AWS 凭证"^] 。

如果多个 IAM 用户在同一个 AWS 账户中工作，则每个用户都需要订阅。第一个用户订阅后，AWS 市场会通知后续用户他们已经订阅，如下图所示。当 AWS 账户有订阅时，每个 IAM 用户都需要将自己与该订阅关联起来。如果您看到下面显示的消息，请单击“单击此处”链接转到控制台网站并完成该过
程。



5. 服务：保持服务启用或禁用您不想在此Cloud Volumes ONTAP系统中使用的单个服务。
   - "了解有关NetApp Data Classification的更多信息"
   - "了解有关备份和恢复的更多信息"

如果您想使用 WORM 和数据分层，则必须禁用备份和恢复并部署版本 9.8 或更高版本的Cloud Volumes ONTAP系统。

6. **HA** 部署模型：选择 HA 配置。

   有关部署模型的概述，请参阅"适用于 AWS 的Cloud Volumes ONTAP HA"。

7. 位置和连接（单个可用区 (AZ)）或*区域和 VPC*（多个 AZ）：输入您在 AWS 工作表中记录的网络信息。

   下表描述了您可能需要指导的字段：

字段	描述
生成的安全组	如果您让控制台为您生成安全组，则需要选择如何允许流量： • 如果您选择*仅限选定的 VPC*，则入站流量的来源是选定 VPC 的子网范围和控制台代理所在 VPC 的子网范围。这是推荐的选项。 • 如果您选择*所有 VPC*，则入站流量的来源是 0.0.0.0/0 IP 范围。
使用现有的安全组	如果您使用现有的防火墙策略，请确保它包含所需的规则。"了解Cloud Volumes ONTAP的防火墙规则" 。

8. 连接和 **SSH** 身份验证：选择 HA 对和中介的连接方法。
9. 浮动 **IP**：如果您选择多个 AZ，请指定浮动 IP 地址。

   IP 地址必须位于该区域内所有 VPC 的 CIDR 块之外。有关更多详细信息，请参阅"多个可用区中Cloud Volumes ONTAP HA 的 AWS 网络要求"。

10. 路由表：如果您选择了多个 AZ，请选择应包含到浮动 IP 地址的路由的路由表。

    如果您有多个路由表，那么选择正确的路由表非常重要。否则，某些客户端可能无法访问Cloud Volumes ONTAP HA 对。有关路由表的更多信息，请参阅 "AWS 文档：路由表"。

11. 数据加密：选择无数据加密或 AWS 管理加密。

    对于 AWS 管理的加密，您可以从您的账户或其他 AWS 账户中选择不同的客户主密钥 (CMK)。

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

    "了解如何为Cloud Volumes ONTAP设置 AWS KMS" 。

    "了解有关受支持的加密技术的更多信息" 。

12. 收费方式和 **NSS** 帐户：指定您想要在此系统中使用的收费选项，然后指定NetApp支持站点帐户。
    - "了解Cloud Volumes ONTAP的许可选项" 。
    - "了解如何设置许可" 。
13. * Cloud Volumes ONTAP配置*（仅限年度 AWS Marketplace 合同）：查看默认配置并单击*继续*或单击*更改配置*以选择您自己的配置。

如果保留默认配置，则只需要指定一个卷，然后审核并批准该配置。

14. 预配置包（按小时或仅限 BYOL）：选择其中一个包以快速启动Cloud Volumes ONTAP，或单击*更改配置*以选择您自己的配置。

    如果您选择其中一个包，那么您只需要指定一个卷，然后审核并批准配置。

15. **IAM** 角色：最好保留默认选项，让控制台为您创建角色。

    如果您希望使用自己的政策，则必须满足"Cloud Volumes ONTAP节点和 HA 调解器的策略要求"。

16. 许可：根据需要更改Cloud Volumes ONTAP版本并选择实例类型和实例租赁。

    如果所选版本有较新的候选版本、通用版本或补丁版本，则控制台在创建系统时会将系统更新到该版本。例如，如果您选择Cloud Volumes ONTAP 9.13.1 并且 9.13.1 P4 可用，则会发生更新。更新不会从一个版本发生到另一个版本 - 例如，从 9.13 到 9.14。

17. 底层存储资源：选择磁盘类型，配置底层存储，并选择是否保持数据分层启用。

    请注意以下事项：

    - 磁盘类型适用于初始卷（和聚合）。您可以为后续卷（和聚合）选择不同的磁盘类型。
    - 如果您选择 gp3 或 io1 磁盘，控制台将使用 AWS 中的弹性卷功能根据需要自动增加底层存储磁盘容量。您可以根据您的存储需求选择初始容量，并在部署Cloud Volumes ONTAP后进行修改。"了解有关 AWS 弹性卷支持的更多信息" 。
    - 如果您选择 gp2 或 st1 磁盘，则可以为初始聚合中的所有磁盘以及使用简单配置选项时控制台创建的任何其他聚合选择磁盘大小。您可以使用高级分配选项创建使用不同磁盘大小的聚合。
    - 您可以在创建或编辑卷时选择特定的卷分层策略。
    - 如果您禁用数据分层，则可以在后续聚合上启用它。

      "了解数据分层的工作原理" 。

18. 写入速度和 **WORM**：

    a. 如果需要，选择*正常*或*高*写入速度。

       "了解有关写入速度的更多信息" 。

    b. 如果需要，请激活一次写入、多次读取 (WORM) 存储。

       如果为Cloud Volumes ONTAP 9.7 及更低版本启用了数据分层，则无法启用 WORM。启用 WORM 和分层后，恢复或降级到Cloud Volumes ONTAP 9.8 的操作将被阻止。

    "了解有关 WORM 存储的更多信息" 。

    a. 如果您激活 WORM 存储，请选择保留期限。

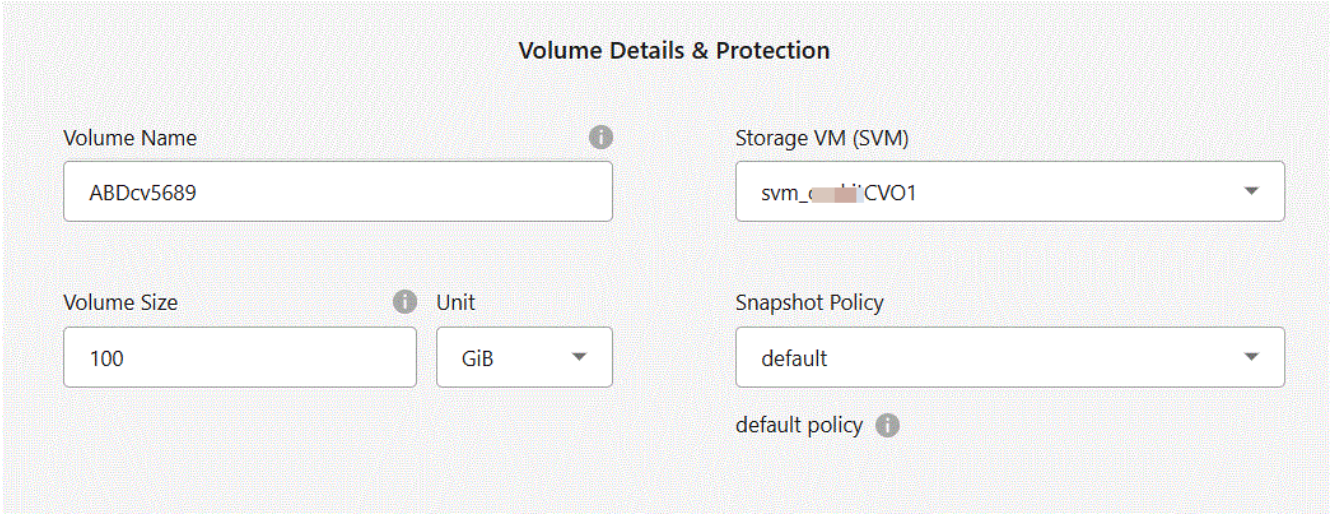
19. 创建卷：输入新卷的详细信息或单击*跳过*。

    "了解支持的客户端协议和版本" 。

此页面中的某些字段是不言自明的。下表描述了您可能需要指导的字段：

字段	描述
大小	您可以输入的最大大小很大程度上取决于您是否启用精简配置，这使您能够创建比当前可用的物理存储更大的卷。
访问控制（仅适用于 NFS）	导出策略定义了子网中可以访问卷的客户端。默认情况下，控制台输入一个提供对子网中所有实例的访问权限的值。
权限和用户/组（仅适用于 CIFS）	这些字段使您能够控制用户和组对共享的访问级别（也称为访问控制列表或 ACL）。您可以指定本地或域 Windows 用户或组，或者 UNIX 用户或组。如果指定域 Windows 用户名，则必须使用域\用户名格式包含用户的域。
Snapshot 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 副本是时间点文件系统映像，它不会影响性能并且只需要最少的存储空间。您可以选择默认策略或无策略。对于瞬态数据，您可能选择无：例如，对于 Microsoft SQL Server，请选择 tempdb。
高级选项（仅适用于 NFS）	为卷选择一个 NFS 版本：NFSv3 或 NFSv4。
启动器组和 IQN（仅适用于 iSCSI）	iSCSI 存储目标称为 LUN（逻辑单元），并作为标准块设备呈现给主机。启动器组是 iSCSI 主机节点名称表，用于控制哪些启动器可以访问哪些 LUN。iSCSI 目标通过标准以太网网络适配器 (NIC)、带有软件启动器的 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。当您创建 iSCSI 卷时，控制台会自动为您创建一个 LUN。我们通过为每个卷创建一个 LUN 来简化操作，因此无需进行任何管理。创建卷后，"使用 IQN 从主机连接到 LUN" 。

下图显示了卷创建向导的第一页：



20. **CIFS** 设置：如果您选择了 CIFS 协议，请设置 CIFS 服务器。

字段	描述
DNS 主 IP 地址和辅助 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 服务器必须包含定位 CIFS 服务器将加入的域的 Active Directory LDAP 服务器和域控制器所需的服务位置记录 (SRV)。

字段	描述
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 域内指定组织单位 (OU) 的 Windows 帐户的名称和密码。
CIFS 服务器 NetBIOS 名称	AD 域中唯一的 CIFS 服务器名称。
组织单位	AD 域内与 CIFS 服务器关联的组织单位。默认值为 CN=Computers。如果将 AWS Managed Microsoft AD 配置为Cloud Volumes ONTAP 的AD 服务器，则应在此字段中输入 **OU=Computers,OU=corp**。
DNS 域	Cloud Volumes ONTAP存储虚拟机 (SVM) 的 DNS 域。大多数情况下，该域与 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。如果您需要使用不同的地址配置 NTP 服务器，那么您应该使用 API。请参阅 "NetApp Console自动化文档"了解详情。请注意，只有在创建 CIFS 服务器时才能配置 NTP 服务器。创建 CIFS 服务器后，它不可配置。

21. 使用情况配置文件、磁盘类型和分层策略：选择是否要启用存储效率功能，并在需要时编辑卷分层策略。

    更多信息，请参阅"选择卷使用情况配置文件"和"数据分层概述"。

22. 审核并批准：审核并确认您的选择。
    a. 查看有关配置的详细信息。
    b. 单击“更多信息”以查看有关支持和控制台将购买的 AWS 资源的详细信息。
    c. 选中*我明白…*复选框。
    d. 单击“开始”。

结果

控制台启动Cloud Volumes ONTAP HA 对。您可以在*审计*页面上跟踪进度。

如果您在启动 HA 对时遇到任何问题，请查看失败消息。您也可以选择系统并单击重新创建环境。

如需更多帮助，请访问 "NetApp Cloud Volumes ONTAP支持"。

完成后

- 如果您配置了 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共享并创建文件。
- 如果要将配额应用于卷，请使用ONTAP系统管理器或ONTAP CLI。

  配额使您能够限制或跟踪用户、组或 qtree 使用的磁盘空间和文件数量。

> 部署过程完成后，请勿修改 AWS 云门户中系统生成的Cloud Volumes ONTAP配置，尤其是系统标签。对这些配置所做的任何更改都可能导致意外行为或数据丢失。

相关链接

- "规划您的Cloud Volumes ONTAP配置"
- "使用快速部署在 AWS 中部署Cloud Volumes ONTAP"

在 AWS Secret Cloud 或 AWS Top Secret Cloud 中部署Cloud Volumes ONTAP

与标准 AWS 区域NetApp Console，您可以在"AWS 秘密云"并且在"AWS 顶级机密云"部署Cloud Volumes ONTAP，为您的云存储提供企业级功能。 AWS Secret Cloud 和 Top Secret Cloud 是特定于美国情报界的封闭区域；本页上的说明仅适用于 AWS Secret Cloud 和 Top Secret Cloud 区域用户。

开始之前

在开始之前，请查看 AWS Secret Cloud 和 Top Secret Cloud 中支持的版本，并了解控制台中的私有模式。

- 查看 AWS Secret Cloud 和 Top Secret Cloud 中支持的以下版本：
  - Cloud Volumes ONTAP 9.12.1 P2
  - 控制台代理版本 3.9.32

    需要控制台代理才能在 AWS 中部署和管理Cloud Volumes ONTAP 。您将从安装在控制台代理实例上的软件登录到控制台。 AWS Secret Cloud 和 Top Secret Cloud 不支持控制台的 SaaS 网站。
- 了解私人模式

  在 AWS Secret Cloud 和 Top Secret Cloud 中，控制台以_私有模式_运行。在私人模式下，控制台与 SaaS 层没有连接。您可以通过可以访问控制台代理的本地基于 Web 的应用程序来访问控制台。

  要了解有关隐私模式工作原理的更多信息，请参阅"控制台中的私有部署模式"。

步骤 **1**：设置网络

设置您的 AWS 网络，以便Cloud Volumes ONTAP可以正常运行。

步骤

1. 选择要在其中启动控制台代理实例和Cloud Volumes ONTAP实例的 VPC 和子网。
2. 确保您的 VPC 和子网将支持控制台代理和Cloud Volumes ONTAP之间的连接。
3. 设置 Amazon Simple Storage Service (Amazon S3) 服务的 VPC 端点。

   如果您想将冷数据从Cloud Volumes ONTAP到低成本对象存储，则需要 VPC 端点。

步骤 **2**：设置权限

设置 IAM 策略和角色，为控制台代理和Cloud Volumes ONTAP提供在 AWS Secret Cloud 或 Top Secret Cloud 中执行操作所需的权限。

您需要针对以下各项制定 IAM 策略和 IAM 角色：

- 控制台代理实例

- Cloud Volumes ONTAP实例
- 对于 HA 对， Cloud Volumes ONTAP HA 中介实例（如果您要部署 HA 对）

步骤

1. 转到 AWS IAM 控制台并单击 策略。
2. 为控制台代理实例创建策略。

> 您创建这些策略来支持 AWS 环境中的 S3 存储桶。稍后创建存储桶时，请确保存储桶名称以 `fabric-pool-`。此要求适用于 AWS Secret Cloud 和 Top Secret Cloud 区域。

秘密区域

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:RunInstances",
                "ec2:ModifyInstanceAttribute",
                "ec2:DescribeRouteTables",
                "ec2:DescribeImages",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DescribeVolumes",
                "ec2:ModifyVolumeAttribute",
                "ec2:DeleteVolume",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:DescribeSecurityGroups",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateNetworkInterface",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DeleteNetworkInterface",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeDhcpOptions",
                "ec2:CreateSnapshot",
                "ec2:DeleteSnapshot",
                "ec2:DescribeSnapshots",
                "ec2:GetConsoleOutput",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeRegions",
                "ec2:DeleteTags",
                "ec2:DescribeTags",
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackEvents",
                "cloudformation:ValidateTemplate",
```

```
                "iam:PassRole",
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:PutRolePolicy",
                "iam:ListInstanceProfiles",
                "iam:CreateInstanceProfile",
                "iam:DeleteRolePolicy",
                "iam:AddRoleToInstanceProfile",
                "iam:RemoveRoleFromInstanceProfile",
                "iam:DeleteInstanceProfile",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:ListAllMyBuckets",
                "kms:List*",
                "kms:Describe*",
                "ec2:AssociateIamInstanceProfile",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:DescribeInstanceAttribute",
                "ec2:CreatePlacementGroup",
                "ec2:DeletePlacementGroup"
            ],
            "Resource": "*"
        },
        {
            "Sid": "fabricPoolPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions"
            ],
            "Resource": [
                "arn:aws-iso-b:s3:::fabric-pool*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances",
```

```
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/WorkingEnvironment": "*"
                }
            },
            "Resource": [
                "arn:aws-iso-b:ec2:*:*:instance/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws-iso-b:ec2:*:*:volume/*"
            ]
        }
    ]
}
```

绝密地区

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:RunInstances",
                "ec2:ModifyInstanceAttribute",
                "ec2:DescribeRouteTables",
                "ec2:DescribeImages",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DescribeVolumes",
                "ec2:ModifyVolumeAttribute",
                "ec2:DeleteVolume",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:DescribeSecurityGroups",
```

```
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateNetworkInterface",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DeleteNetworkInterface",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeDhcpOptions",
                "ec2:CreateSnapshot",
                "ec2:DeleteSnapshot",
                "ec2:DescribeSnapshots",
                "ec2:GetConsoleOutput",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeRegions",
                "ec2:DeleteTags",
                "ec2:DescribeTags",
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackEvents",
                "cloudformation:ValidateTemplate",
                "iam:PassRole",
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:PutRolePolicy",
                "iam:ListInstanceProfiles",
                "iam:CreateInstanceProfile",
                "iam:DeleteRolePolicy",
                "iam:AddRoleToInstanceProfile",
                "iam:RemoveRoleFromInstanceProfile",
                "iam:DeleteInstanceProfile",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:ListAllMyBuckets",
                "kms:List*",
                "kms:Describe*",
                "ec2:AssociateIamInstanceProfile",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:DescribeInstanceAttribute",
                "ec2:CreatePlacementGroup",
```

```
                "ec2:DeletePlacementGroup"
            ],
            "Resource": "*"
        },
        {
            "Sid": "fabricPoolPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions"
            ],
            "Resource": [
                "arn:aws-iso:s3:::fabric-pool*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances",
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/WorkingEnvironment": "*"
                }
            },
            "Resource": [
                "arn:aws-iso:ec2:*:*:instance/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws-iso:ec2:*:*:volume/*"
            ]
        }
```

```
        ]
}
```

3. 为Cloud Volumes ONTAP创建策略。

秘密区域

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Action": "s3:ListAllMyBuckets",
        "Resource": "arn:aws-iso-b:s3:::*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": "arn:aws-iso-b:s3:::fabric-pool-*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:GetObject",
            "s3:PutObject",
            "s3:DeleteObject"
        ],
        "Resource": "arn:aws-iso-b:s3:::fabric-pool-*",
        "Effect": "Allow"
    }]
}
```

绝密地区

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Action": "s3:ListAllMyBuckets",
        "Resource": "arn:aws-iso:s3:::*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": "arn:aws-iso:s3:::fabric-pool-*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:GetObject",
            "s3:PutObject",
            "s3:DeleteObject"
        ],
        "Resource": "arn:aws-iso:s3:::fabric-pool-*",
        "Effect": "Allow"
    }]
}
```

对于 HA 对，如果您计划部署Cloud Volumes ONTAP HA 对，请为 HA 中介创建策略。

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:AssignPrivateIpAddresses",
                "ec2:CreateRoute",
                "ec2:DeleteRoute",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeVpcs",
                "ec2:ReplaceRoute",
                "ec2:UnassignPrivateIpAddresses"
            ],
            "Resource": "*"
        }
    ]
}
```

4. 创建角色类型为 Amazon EC2 的 IAM 角色并附加您在前面步骤中创建的策略。

   创建角色：

   与策略类似，您应该为控制台代理设置一个 IAM 角色，为Cloud Volumes ONTAP节点设置一个 IAM 角色。对于 HA 对：与策略类似，您应该为控制台代理设置一个 IAM 角色，为Cloud Volumes ONTAP节点设置一个 IAM 角色，为 HA 中介设置一个 IAM 角色（如果您想要部署 HA 对）。

   选择角色：

   启动控制台代理实例时，必须选择控制台代理 IAM 角色。当您从控制台创建Cloud Volumes ONTAP系统时，您可以选择Cloud Volumes ONTAP的 IAM 角色。对于 HA 对，您可以在创建Cloud Volumes ONTAP系统时选择Cloud Volumes ONTAP和 HA 中介的 IAM 角色。

步骤 3：设置 AWS KMS

如果您想要将 Amazon 加密与Cloud Volumes ONTAP结合使用，请确保满足 AWS 密钥管理服务 (KMS) 的要求。

步骤

1. 确保您的账户或其他 AWS 账户中存在有效的客户主密钥 (CMK)。

   CMK 可以是 AWS 管理的 CMK 或客户管理的 CMK。

2. 如果 CMK 位于与您计划部署Cloud Volumes ONTAP 的账户不同的 AWS 账户中，则需要获取该密钥的 ARN。

   创建Cloud Volumes ONTAP系统时，您需要向控制台提供 ARN。

3. 将实例的 IAM 角色添加到 CMK 的密钥用户列表中。

这授予控制台使用 CMK 和Cloud Volumes ONTAP 的权限。

步骤 4：安装控制台代理并设置控制台

在开始使用控制台在 AWS 中部署Cloud Volumes ONTAP之前，您必须安装并设置控制台代理。它使控制台能够管理公共云环境（包括Cloud Volumes ONTAP）内的资源和流程。

步骤

1. 获取由证书颁发机构 (CA) 签名的、采用隐私增强邮件 (PEM) Base-64 编码 X.509 格式的根证书。请查阅您所在组织的政策和程序以获取证书。

   对于 AWS Secret Cloud 区域，您应该上传 `NSS Root CA 2`证书，对于 Top Secret Cloud，`Amazon Root CA 4`证书。确保仅上传这些证书而不是整个链。证书链文件较大，上传可能会失败。如果您有其他证书，您可以稍后上传，如下一步所述。

   您需要在设置过程中上传证书。控制台通过 HTTPS 向 AWS 发送请求时使用受信任的证书。

2. 启动控制台代理实例：
   a. 转到控制台的 AWS Intelligence Community Marketplace 页面。
   b. 在“自定义启动”选项卡上，选择从 EC2 控制台启动实例的选项。
   c. 按照提示配置实例。

      配置实例时请注意以下事项：

      - 我们推荐 t3.xlarge。
      - 您必须选择在设置权限时创建的 IAM 角色。
      - 您应该保留默认存储选项。
      - 控制台代理所需的连接方法如下：SSH、HTTP 和 HTTPS。
3. 从与实例有连接的主机设置控制台：
   a. 打开网络浏览器并输入 https://ipaddress其中 ipaddress 是安装控制台代理的 Linux 主机的 IP 地址。
   b. 指定用于连接 AWS 服务的代理服务器。
   c. 上传您在步骤 1 中获得的证书。
   d. 按照提示设置新系统。
      - 系统详细信息：输入控制台代理的名称和您的公司名称。
      - 创建管理员用户：为系统创建管理员用户。

        该用户帐户在系统本地运行。无法通过控制台连接到 auth0 服务。

      - 审核：审核详细信息，接受许可协议，然后选择*设置*。
   e. 要完成 CA 签名证书的安装，请从 EC2 控制台重新启动控制台代理实例。
4. 控制台代理重新启动后，使用您在安装向导中创建的管理员用户帐户登录。

步骤 **5**：（可选）安装私有模式证书

对于 AWS Secret Cloud 和 Top Secret Cloud 区域，此步骤是可选的，并且仅当您除了上一步中安装的根证书之外还有其他证书时才需要执行此步骤。

步骤

1. 列出现有安装的证书。
   a. 要收集 occm 容器 docker id（标识名称“ds-occm-1”），请运行以下命令：

   ```
   docker ps
   ```

   b. 要进入 occm 容器，请运行以下命令：

   ```
   docker exec -it <docker-id> /bin/sh
   ```

   c. 要从“TRUST_STORE_PASSWORD”环境变量收集密码，请运行以下命令：

   ```
   env
   ```

   d. 要列出信任库中所有已安装的证书，请运行以下命令并使用上一步收集的密码：

   ```
   keytool -list -v -keystore occm.truststore
   ```

2. 添加证书。
   a. 要收集 occm 容器 docker id（标识名称“ds-occm-1”），请运行以下命令：

   ```
   docker ps
   ```

   b. 要进入 occm 容器，请运行以下命令：

   ```
   docker exec -it <docker-id> /bin/sh
   ```

   将新的证书文件保存在里面。

   c. 要从“TRUST_STORE_PASSWORD”环境变量收集密码，请运行以下命令：

   ```
   env
   ```

   d. 要将证书添加到信任库，请运行以下命令并使用上一步中的密码：

```
keytool -import -alias <alias-name> -file <certificate-file-name>
-keystore occm.truststore
```

e. 要检查证书是否已安装，请运行以下命令：

```
keytool -list -v -keystore occm.truststore -alias <alias-name>
```

f. 要退出 occm 容器，请运行以下命令：

```
exit
```

g. 要重置 occm 容器，请运行以下命令：

```
docker restart <docker-id>
```

步骤 **6**：向控制台添加许可证

如果您从NetApp购买了许可证，则需要将其添加到控制台，以便在创建新的Cloud Volumes ONTAP系统时选择该许可证。在将这些许可证与新的Cloud Volumes ONTAP系统关联之前，它们将保持未分配状态。

步骤

1. 从左侧导航菜单中，选择*Licenses and subscriptions*。
2. 在 * Cloud Volumes ONTAP* 面板上，选择 查看。
3. 在 * Cloud Volumes ONTAP* 选项卡上，选择 许可证**>**基于节点的许可证。
4. 单击“未分配”。
5. 单击“添加未分配的许可证”。
6. 输入许可证的序列号或上传许可证文件。
7. 如果您还没有许可证文件，则需要从 netapp.com 手动上传许可证文件。
   a. 前往"NetApp许可证文件生成器"并使用您的NetApp支持站点凭据登录。
   b. 输入您的密码，选择您的产品，输入序列号，确认您已阅读并接受隐私政策，然后单击*提交*。
   c. 选择您是否希望通过电子邮件或直接下载接收 serialnumber.NLF JSON 文件。
8. 单击“添加许可证”。

结果

控制台会将许可证添加为未分配状态，直到您将其与新的Cloud Volumes ONTAP系统关联。您可以在左侧导航菜单的 **Licenses and subscriptions> Cloud Volumes ONTAP >** 查看 **>** 许可证 下看到许可证。

步骤 7：从控制台启动Cloud Volumes ONTAP

您可以通过在控制台中创建新系统来在 AWS Secret Cloud 和 Top Secret Cloud 中启动Cloud Volumes ONTAP 实例。

开始之前

对于 HA 对，需要密钥对来启用对 HA 中介的基于密钥的 SSH 身份验证。

步骤

1. 在“系统”页面上，单击“添加系统”。
2. 在“创建”下，选择Cloud Volumes ONTAP。

   对于 HA：在 创建 下，选择Cloud Volumes ONTAP或Cloud Volumes ONTAP HA。

3. 完成向导中的步骤以启动Cloud Volumes ONTAP系统。

> 通过向导进行选择时，请不要选择*服务*下的*数据感知与合规性*和*备份到云*。在*预配置包*下，仅选择*更改配置*，并确保您没有选择任何其他选项。 AWS Secret Cloud 和 Top Secret Cloud 区域不支持预配置包，如果选择，您的部署将失败。

在多个可用区中部署**Cloud Volumes ONTAP HA** 的注意事项

完成 HA 对向导时请注意以下事项。

- 在多个可用区 (AZ) 中部署Cloud Volumes ONTAP HA 时，您应该配置一个传输网关。有关说明，请参阅"设置 AWS 中转网关"。
- 由于发布时 AWS Top Secret Cloud 中只有两个可用可用区，因此请按如下方式部署配置：
  - 节点 1：可用区 A
  - 节点 2：可用区 B
  - 调解员：可用区域 A 或 B

在单节点和 **HA** 节点中部署**Cloud Volumes ONTAP** 的注意事项

完成向导时请注意以下事项：

- 您应该保留默认选项以使用生成的安全组。

  预定义的安全组包含Cloud Volumes ONTAP成功运行所需的规则。如果您有使用自己的需求，可以参考下面的安全组部分。

- 您必须选择在准备 AWS 环境时创建的 IAM 角色。
- 底层 AWS 磁盘类型适用于初始Cloud Volumes ONTAP卷。

  您可以为后续卷选择不同的磁盘类型。

- AWS 磁盘的性能与磁盘大小相关。

  您应该选择能够提供所需持续性能的磁盘大小。有关 EBS 性能的更多详细信息，请参阅 AWS 文档。

- 磁盘大小是系统上所有磁盘的默认大小。

> 如果您稍后需要不同的大小，则可以使用高级分配选项来创建使用特定大小磁盘的聚合。

结果

Cloud Volumes ONTAP实例已启动。您可以在*审计*页面跟踪进度。

步骤 8：安装数据分层的安全证书

您需要手动安装安全证书才能在 AWS Secret Cloud 和 Top Secret Cloud 区域中启用数据分层。

开始之前

1. 创建 S3 存储桶。

> 确保存储桶名称带有前缀 `fabric-pool-.`例如 `fabric-pool-testbucket。

2. 保留您安装的根证书 `step 4`便利。

步骤

1. 复制您安装的根证书中的文本 `step 4`。
2. 使用 CLI 安全地连接到Cloud Volumes ONTAP系统。
3. 安装根证书。您可能需要按 `ENTER`多次键入：

```
security certificate install -type server-ca -cert-name <certificate-
name>
```

4. 出现提示时，输入复制的整个文本，包括 `----- BEGIN CERTIFICATE -----`到 `----- END CERTIFICATE -----`。
5. 保留 CA 签名的数字证书的副本以供将来参考。
6. 保留 CA 名称和证书序列号。
7. 为 AWS Secret Cloud 和 Top Secret Cloud 区域配置对象存储： `set -privilege advanced -confirmations off`
8. 运行此命令来配置对象存储。

> 所有 Amazon 资源名称 (ARN) 都应以 `-iso-b`， 例如 `arn:aws-iso-b`。例如，如果资源需要具有区域的 ARN，对于 Top Secret Cloud，请使用以下命名约定 `us-iso-b`对于 `-server`旗帜。对于 `AWS Secret Cloud`，使用 `us-iso-b-1`。

```
storage aggregate object-store config create -object-store-name
<S3Bucket> -provider-type AWS_S3 -auth-type EC2-IAM -server <s3.us-iso-
b-1.server_name> -container-name <fabric-pool-testbucket> -is-ssl
-enabled true -port 443
```

9. 验证对象存储是否已成功创建： `storage aggregate object-store show -instance`
10. 将对象存储附加到聚合。对于每个新的聚合体都应重复此操作： `storage aggregate object-store attach -aggregate <aggr1> -object-store-name <S3Bucket>`

开始使用 Microsoft Azure

了解 Azure 中的Cloud Volumes ONTAP部署选项

NetApp提供了两种在 Azure 上部署Cloud Volumes ONTAP 的选项。 Cloud Volumes ONTAP传统上依赖NetApp Console进行部署和编排。从Cloud Volumes ONTAP 9.16.1 开始，您可以利用 Azure 市场直接部署，这是一个简化的过程，可以访问有限但仍然强大的Cloud Volumes ONTAP功能和选项。

当您直接从 Azure 市场部署Cloud Volumes ONTAP时，您无需设置控制台代理或满足通过控制台部署Cloud Volumes ONTAP所需的其他安全和入职标准。从 Azure 市场，您只需单击几下即可快速部署Cloud Volumes ONTAP ，并在您的环境中探索其核心特性和功能。

在 Azure 市场完成部署后，您可以在控制台中发现这些系统。发现后，您可以将它们作为Cloud Volumes ONTAP系统进行管理，并利用所有控制台功能。请参阅"在控制台中发现已部署的系统" 。

以下是两个选项之间的功能比较。请注意，通过 Azure 市场部署的独立实例的功能在控制台中被发现时会发生变化。

	Azure 市场	**NetApp Console**
入职培训	更短、更简单，直接部署所需的准备工作最少	更长的入职流程，包括控制台代理的安装
支持的虚拟机 **(VM)** 类型	Eds_v5 和 Ls_v3 实例类型	全方位的 VM 类型。https://docs.netapp.com/us-en/cloud-volumes-ontap-relnotes/reference-configs-azure.html["Azure 中支持的配置"^]
执照	免费许可证	任何基于容量的许可证。"Cloud Volumes ONTAP许可"
* NetApp支持*	不包括	根据许可证类型可用
容量	最多 500 GiB	可通过配置扩展
部署模型	单可用区（AZ）高可用（HA）模式部署	所有支持的配置，包括单节点和 HA 模式、单 AZ 和多 AZ 部署
支持的磁盘类型	高级 SSD v2 托管磁盘	更广泛的支持。"Cloud Volumes ONTAP的默认配置"
写入速度（快速写入模式）	不支持	根据您的配置，支持。"了解Cloud Volumes ONTAP中的写入速度" 。
编排功能	不可用	根据许可证类型，可通过NetApp Console获取

	Azure 市场	NetApp Console
支持的存储虚拟机数量	每个部署一个	根据您的配置，多个存储虚拟机。"支持的存储虚拟机数量"
更改实例类型	不支持	支持
* FabricPool分层*	不支持	支持

相关链接

- Azure 市场直接部署："从 Azure 市场部署Cloud Volumes ONTAP"
- 通过控制台部署："Azure 中的Cloud Volumes ONTAP快速入门"
- "NetApp Console文档"

开始使用NetApp Console

Azure 中的Cloud Volumes ONTAP快速入门

只需几个步骤即可开始使用Cloud Volumes ONTAP for Azure。


创建控制台代理

如果你没有 "控制台代理"但是，您需要创建一个。 "了解如何在 Azure 中创建控制台代理"

请注意，如果您想在没有互联网访问的子网中部署Cloud Volumes ONTAP ，则需要手动安装控制台代理并访问在该控制台代理上运行的NetApp Console。 "了解如何在没有互联网访问的地方手动安装控制台代理"


规划您的配置

控制台提供符合您的工作负载要求的预配置包，或者您可以创建自己的配置。如果您选择自己的配置，您应该了解可用的选项。有关信息，请参阅"在 Azure 中规划Cloud Volumes ONTAP配置"。


设置网络

1. 确保您的 VNet 和子网将支持控制台代理和Cloud Volumes ONTAP之间的连接。
2. 为NetApp AutoSupport启用从目标 VPC 的出站互联网访问。

   如果您在没有互联网访问的位置部署Cloud Volumes ONTAP，则不需要执行此步骤。

"了解有关网络要求的更多信息" 。


启动Cloud Volumes ONTAP

单击“添加系统”，选择您想要部署的系统类型，然后完成向导中的步骤。"阅读分步说明" 。

相关链接

- "从控制台创建控制台代理"

- "从 Azure 市场创建控制台代理"
- "在 Linux 主机上安装控制台代理软件"
- "控制台如何处理权限"

在 **Azure** 中规划**Cloud Volumes ONTAP**配置

在 Azure 中部署Cloud Volumes ONTAP时，您可以选择符合您的工作负载要求的预配置系统，也可以创建自己的配置。如果您选择自己的配置，您应该了解可用的选项。

选择**Cloud Volumes ONTAP**许可证

Cloud Volumes ONTAP有多种许可选项。每个选项都可以让您选择符合您需求的消费模式。

- "了解Cloud Volumes ONTAP的许可选项"
- "了解如何设置许可"

选择支持的区域

大多数 Microsoft Azure 区域都支持Cloud Volumes ONTAP 。 "查看支持区域的完整列表" 。

选择受支持的 **VM** 类型

Cloud Volumes ONTAP支持多种 VM 类型，具体取决于您选择的许可证类型。

"Azure 中Cloud Volumes ONTAP支持的配置"

了解存储限制

Cloud Volumes ONTAP系统的原始容量限制与许可证相关。额外的限制会影响聚合和卷的大小。在规划配置时您应该注意这些限制。

"Azure 中Cloud Volumes ONTAP的存储限制"

在 **Azure** 中调整系统大小

调整Cloud Volumes ONTAP系统的大小可以帮助您满足性能和容量要求。选择 VM 类型、磁盘类型和磁盘大小时，您应该注意几个关键点：

虚拟机类型

查看受支持的虚拟机类型 "Cloud Volumes ONTAP发行说明"然后查看有关每种受支持的 VM 类型的详细信息。请注意，每种 VM 类型都支持特定数量的数据磁盘。

- "Azure 文档：通用虚拟机大小"
- "Azure 文档：内存优化虚拟机大小"

具有单节点系统的 **Azure** 磁盘类型

为Cloud Volumes ONTAP创建卷时，您需要选择Cloud Volumes ONTAP用作磁盘的底层云存储。

单节点系统可以使用以下类型的 Azure 托管磁盘：

- 高级 *SSD* 托管磁盘 以更高的成本为 I/O 密集型工作负载提供高性能。
- 与高级 SSD 托管磁盘相比，高级 *SSD v2* 托管磁盘 以更低的成本提供更高的性能和更低的延迟。
- _标准 SSD 托管磁盘_为需要低 IOPS 的工作负载提供一致的性能。
- 如果您不需要高 IOPS 并且想要降低成本，那么“标准 HDD 托管磁盘”是一个不错的选择。

有关这些磁盘用例的更多详细信息，请参阅 "Microsoft Azure 文档：Azure 中有哪些磁盘类型？"。

具有 **HA** 对的 **Azure** 磁盘类型

HA 系统使用高级 SSD 共享托管磁盘，它们都以更高的成本为 I/O 密集型工作负载提供高性能。 9.12.1 版本之前创建的 HA 部署使用高级页面 blob。

Azure 磁盘大小

启动Cloud Volumes ONTAP实例时，您必须选择聚合的默认磁盘大小。 NetApp Console将此磁盘大小用于初始聚合，以及使用简单配置选项时创建的任何其他聚合。您可以通过以下方式创建使用不同于默认磁盘大小的聚合："使用高级分配选项" 。

聚合中的所有磁盘必须具有相同的大小。

选择磁盘大小时，您应该考虑几个因素。磁盘大小会影响您支付的存储费用、您可以在聚合中创建的卷的大小、 Cloud Volumes ONTAP可用的总容量以及存储性能。

Azure Premium Storage 的性能与磁盘大小相关。更大的磁盘可提供更高的 IOPS 和吞吐量。例如，选择 1 TiB 磁盘可以提供比 500 GiB 磁盘更好的性能，但成本更高。

标准存储的磁盘大小之间没有性能差异。您应该根据所需的容量来选择磁盘大小。

请参阅 Azure 了解按磁盘大小划分的 IOPS 和吞吐量：

- "Microsoft Azure：托管磁盘定价"
- "Microsoft Azure：Page Blob 定价"

查看默认系统磁盘

除了用户数据的存储之外，控制台还购买了Cloud Volumes ONTAP系统数据（启动数据、根数据、核心数据和NVRAM）的云存储。出于规划目的，在部署Cloud Volumes ONTAP之前查看这些详细信息可能会有所帮助。

"查看 Azure 中Cloud Volumes ONTAP系统数据的默认磁盘" 。

控制台代理还需要系统磁盘。 "查看控制台代理默认配置的详细信息" 。

收集网络信息

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

Azure 信息	你的价值
地区	

Azure 信息	你的价值
虚拟网络 (VNet)	
子网	
网络安全组（如果使用您自己的）	

选择写入速度

控制台使您能够选择Cloud Volumes ONTAP的写入速度设置。在选择写入速度之前，您应该了解正常设置和高设置之间的差异以及使用高写入速度时的风险和建议。"了解有关写入速度的更多信息"。

选择卷使用情况配置文件

ONTAP包含多种存储效率功能，可以减少您所需的总存储量。在控制台中创建卷时，您可以选择启用这些功能的配置文件或禁用这些功能的配置文件。您应该了解有关这些功能的更多信息，以帮助您决定使用哪个配置文件。

NetApp存储效率功能具有以下优势：

精简配置

向主机或用户提供比物理存储池中实际拥有的更多的逻辑存储。不是预先分配存储空间，而是在写入数据时动态地将存储空间分配给每个卷。

重复数据删除

通过定位相同的数据块并将其替换为对单个共享块的引用来提高效率。该技术通过消除驻留在同一卷中的冗余数据块来减少存储容量要求。

数据压缩

通过压缩主存储、辅助存储和归档存储卷内的数据来减少存储数据所需的物理容量。

为**Cloud Volumes ONTAP**设置 **Azure** 网络

NetApp Console负责设置Cloud Volumes ONTAP的网络组件，例如 IP 地址、网络掩码和路由。您需要确保可以访问出站互联网、有足够的私有 IP 地址、有正确的连接等等。

Cloud Volumes ONTAP的要求

Azure 中必须满足以下网络要求。

出站互联网访问

Cloud Volumes ONTAP系统需要出站互联网访问才能访问外部端点以实现各种功能。如果这些端点在具有严格安全要求的环境中被阻止， Cloud Volumes ONTAP将无法正常运行。

控制台代理还联系多个端点以进行日常操作。有关端点的信息，请参阅 "查看从控制台代理联系的端点"和 "准备使用控制台的网络"。

Cloud Volumes ONTAP端点

Cloud Volumes ONTAP使用这些端点与各种服务进行通信。

端点	适用于	目的	部署模式	不可用时的影响
\ https://netapp-cloud-account.auth0.com	身份验证	用于控制台中的身份验证。	标准和限制模式。	用户身份验证失败，以下服务仍然不可用： • Cloud Volumes ONTAP服务 • ONTAP 服务 • 协议和代理服务
https://vault.azure.net	密钥保管库	用于在使用客户管理密钥 (CMK) 时从 Azure Key Vault 检索客户端密钥。	标准、受限和私人模式。	Cloud Volumes ONTAP服务不可用。
\ https://api.bluexp.netapp.com/tenancy	租户	用于从控制台检索Cloud Volumes ONTAP资源以授权资源和用户。	标准和限制模式。	Cloud Volumes ONTAP资源和用户未获得授权。
\ https://mysupport.netapp.com/aods/asupmessage \ https://mysupport.netapp.com/asupprod/post/1.0/postAsup	AutoSupport	用于将AutoSupport遥测数据发送给NetApp支持。	标准和限制模式。	AutoSupport信息仍未送达。
\ https://management.azure.com \ https://login.microsoftonline.com \ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://core.windows.net	公共区域	与 Azure 服务通信。	标准、受限和私人模式。	Cloud Volumes ONTAP无法与 Azure 服务通信以对 Azure 中的控制台执行特定操作。
\ https://management.chinacloudapi.cn \ https://login.chinacloudapi.cn \ https://blob.core.chinacloudapi.cn \ https://core.chinacloudapi.cn	中国区	与 Azure 服务通信。	标准、受限和私人模式。	Cloud Volumes ONTAP无法与 Azure 服务通信以对 Azure 中的控制台执行特定操作。

端点	适用于	目的	部署模式	不可用时的影响
\ https://management.microsoftazure.de \ https://login.microsoftonline.de \ https://blob.core.cloudapi.de \ https://core.cloudapi.de	德国地区	与 Azure 服务通信。	标准、受限和私人模式。	Cloud Volumes ONTAP无法与 Azure 服务通信以对 Azure 中的控制台执行特定操作。
\ https://management.usgovcloudapi.net \ https://login.microsoftonline.us \ https://blob.core.usgovcloudapi.net \ https://core.usgovcloudapi.net	政府区域	与 Azure 服务通信。	标准、受限和私人模式。	Cloud Volumes ONTAP无法与 Azure 服务通信以对 Azure 中的控制台执行特定操作。
\ https://management.azure.microsoft.scloud \ https://login.microsoftonline.microsoft.scloud \ https://blob.core.microsoft.scloud \ https://core.microsoft.scloud	政府国防部地区	与 Azure 服务通信。	标准、受限和私人模式。	Cloud Volumes ONTAP无法与 Azure 服务通信以对 Azure 中的控制台执行特定操作。

NetApp Console代理的网络代理配置

您可以使用NetApp Console代理的代理服务器配置来启用来自Cloud Volumes ONTAP 的出站互联网访问。控制台支持两种类型的代理：

- 显式代理：来自Cloud Volumes ONTAP 的出站流量使用在控制台代理的代理配置期间指定的代理服务器的 HTTP 地址。管理员可能还配置了用户凭据和根 CA 证书以进行额外的身份验证。Cloud Volumes ONTAP显式代理有可用的根 CA 证书，请确保使用 "ONTAP CLI：安全证书安装"命令。
- 透明代理：网络配置为通过控制台代理的代理自动路由来自Cloud Volumes ONTAP 的出站流量。设置透明代理时，管理员只需要提供用于从Cloud Volumes ONTAP进行连接的根 CA 证书，而不是代理服务器的 HTTP 地址。确保使用以下方式获取相同的根 CA 证书并将其上传到您的Cloud Volumes ONTAP系统 "ONTAP CLI：安全证书安装"命令。

有关配置代理服务器的信息，请参阅 "配置控制台代理以使用代理服务器"。

IP 地址

控制台会自动为 Azure 中的Cloud Volumes ONTAP分配所需数量的私有 IP 地址。您需要确保您的网络有足够的可用私有 IP 地址。

为 Cloud Volumes ONTAP 分配的 LIF 数量取决于您是部署单节点系统还是 HA 对。LIF 是与物理端口关联的 IP 地址。像 SnapCenter 这样的管理工具需要 SVM 管理 LIF。

> iSCSI LIF 通过 iSCSI 协议提供客户端访问，并被系统用于其他重要的网络工作流程。这些 LIF 是必需的，不应删除。

单节点系统的 **IP** 地址

Console 为单节点系统分配 5 或 6 个 IP 地址：

- 集群管理IP
- 节点管理 IP
- SnapMirror的集群间 IP
- NFS/CIFS IP
- iSCSI IP

> iSCSI IP 通过 iSCSI 协议提供客户端访问。系统还将其用于其他重要的网络工作流程。此 LIF 是必需的，不应删除。

- SVM 管理（可选 - 默认未配置）

HA 对的 **IP** 地址

控制台在部署期间将 IP 地址分配给 4 个 NIC（每个节点）。

请注意，Console 在 HA 对上创建 SVM 管理 LIF，但不在 Azure 中的单节点系统上创建。

NIC0

- 节点管理 IP
- 集群间 IP
- iSCSI IP

> iSCSI IP 通过 iSCSI 协议提供客户端访问。系统还将其用于其他重要的网络工作流程。此 LIF 是必需的，不应删除。

NIC1

- 集群网络IP

NIC2

- 集群互连 IP (HA IC)

NIC3

- Pageblob NIC IP（磁盘访问）

NIC3 仅适用于使用页 Blob 存储的 HA 部署。

上述 IP 地址在故障转移事件中不会迁移。

此外，还配置了 4 个前端 IP（FIP）以在故障转移事件时进行迁移。这些前端 IP 位于负载均衡器中。

- 集群管理IP
- NodeA 数据 IP (NFS/CIFS)
- NodeB数据IP（NFS/CIFS）
- SVM 管理 IP

与 **Azure** 服务的安全连接

默认情况下，控制台启用 Azure 专用链接，用于Cloud Volumes ONTAP和 Azure 页 Blob 存储帐户之间的连接。

在大多数情况下，您无需执行任何操作 - 控制台会为您管理 Azure 专用链接。但是如果您使用 Azure 私有 DNS，则需要编辑配置文件。您还应该了解 Azure 中控制台代理的位置要求。

如果您的业务需要，您还可以禁用专用链接连接。如果禁用该链接，控制台会将Cloud Volumes ONTAP配置为使用服务端点。

"了解有关将 Azure Private Links 或服务端点与Cloud Volumes ONTAP结合使用的更多信息" 。

用于 **Azure VNet** 加密的网络

Cloud Volumes ONTAP 支持 "Azure 虚拟网络 (VNet) 加密"对 VNet 内部或跨对等 VNet 的 VM 到 VM 流量进行加密。此功能在 Azure VNet 层配置，独立于 Cloud Volumes ONTAP 拓扑（单节点或 HA）。

只需确保在虚拟机的 NIC 上启用加速网络，并在启用该功能之前查看 Azure VNet 加密要求和限制即可。不应修改 NetApp 托管负载平衡器对象。

"Azure 文档：VNet 加密和 Accelerated Networking"。

与其他**ONTAP**系统的连接

要在 Azure 中的Cloud Volumes ONTAP系统和其他网络中的ONTAP系统之间复制数据，您必须在 Azure VNet 和其他网络（例如您的公司网络）之间建立 VPN 连接。

有关说明，请参阅 "Microsoft Azure 文档：在 Azure 门户中创建站点到站点连接"。

HA 互连端口

Cloud Volumes ONTAP HA 对包括 HA 互连，这使得每个节点能够持续检查其伙伴节点是否正常运行，并为对方的非易失性存储器镜像日志数据。 HA 互连使用 TCP 端口 10006 进行通信。

默认情况下，HA 互连 LIF 之间的通信是开放的，并且此端口没有安全组规则。但是，如果您在 HA 互连 LIF 之间创建防火墙，则需要确保 TCP 流量对端口 10006 开放，以便 HA 对可以正常运行。

Azure 资源组中只有一个 HA 对

您必须为在 Azure 中部署的每个Cloud Volumes ONTAP HA 对使用一个专用资源组。一个资源组中仅支持一个 HA 对。

如果您尝试在 Azure 资源组中部署第二个Cloud Volumes ONTAP HA 对，控制台会遇到连接问题。

安全组规则

控制台创建 Azure 安全组，其中包括Cloud Volumes ONTAP成功运行的入站和出站规则。 "查看控制台代理的安全组规则" 。

Cloud Volumes ONTAP的 Azure 安全组需要打开适当的端口以进行节点之间的内部通信。 "了解ONTAP内部端口" 。

我们不建议修改预定义的安全组或使用自定义安全组。但是，如果必须这样做，请注意，部署过程要求Cloud Volumes ONTAP系统在其自己的子网内拥有完全访问权限。部署完成后，如果决定修改网络安全组，请确保保持集群端口和 HA 网络端口开放。这确保了Cloud Volumes ONTAP集群内的无缝通信（节点之间的任意通信）。

单节点系统的入站规则

添加Cloud Volumes ONTAP系统并选择预定义安全组时，您可以选择允许以下之一内的流量：

- 仅限选定的 **VNet**：入站流量的来源是Cloud Volumes ONTAP系统的 VNet 子网范围和控制台代理所在的 VNet 子网范围。这是推荐的选项。
- 所有 **VNets**：入站流量的来源是 0.0.0.0/0 IP 范围。
- 已禁用：此选项限制对您的存储帐户的公共网络访问，并禁用Cloud Volumes ONTAP系统的数据分层。如果由于安全法规和政策，您的私有 IP 地址即使在同一个 VNet 内也不应该暴露，那么建议使用此选项。

优先级和名称	端口和协议	来源和目的地	描述
1000 入站_ssh	22 TCP	任意到任意	通过 SSH 访问集群管理 LIF 或节点管理 LIF 的 IP 地址
1001 入站 http	80 TCP	任意到任意	使用集群管理 LIF 的 IP 地址通过 HTTP 访问ONTAP System Manager Web 控制台
1002 inbound_111_tcp	111 TCP	任意到任意	NFS 的远程过程调用
1003 inbound_111_udp	111 UDP	任意到任意	NFS 的远程过程调用
1004 inbound_139	139 TCP	任意到任意	CIFS 的 NetBIOS 服务会话
1005 入站_161-162 _tcp	161-162 TCP	任意到任意	简单网络管理协议
1006 入站_161-162 _udp	161-162 UDP	任意到任意	简单网络管理协议

优先级和名称	端口和协议	来源和目的地	描述
1007 inbound_443	443 TCP	任意到任意	使用集群管理 LIF 的 IP 地址与控制台代理建立连接并通过 HTTPS 访问ONTAP System Manager Web 控制台
1008 inbound_445	445 TCP	任意到任意	使用 NetBIOS 框架的 TCP 上的 Microsoft SMB/CIFS
1009 inbound_635_tcp	635 TCP	任意到任意	NFS 挂载
1010 inbound_635_udp	635 UDP	任意到任意	NFS 挂载
1011 inbound_749	749 TCP	任意到任意	Kerberos
1012 inbound_2049_tcp	2049 TCP	任意到任意	NFS 服务器守护进程
1013 inbound_2049_udp	2049 UDP	任意到任意	NFS 服务器守护进程
1014 inbound_3260	3260 TCP	任意到任意	通过 iSCSI 数据 LIF 进行 iSCSI 访问
1015 入站_4045-4046_tcp	4045-4046 TCP	任意到任意	NFS 锁定守护进程和网络状态监视器
1016 入站_4045-4046_udp	4045-4046 UDP	任意到任意	NFS 锁定守护进程和网络状态监视器
1017 inbound_10000	10000 TCP	任意到任意	使用 NDMP 备份
1018 入站_11104-11105	11104-11105 TCP	任意到任意	SnapMirror数据传输
3000 入站拒绝 _所有_tcp	任意端口 TCP	任意到任意	阻止所有其他 TCP 入站流量
3001 入站拒绝 _所有 udp	任意端口 UDP	任意到任意	阻止所有其他 UDP 入站流量
65000 允许 VnetInBound	任意端口任意协议	虚拟网络到虚拟网络	来自 VNet 内部的入站流量
65001 允许 Azure 负载均衡器入站	任意端口任意协议	AzureLoadBalancer 到任意	来自 Azure 标准负载均衡器的数据流量
65500 拒绝所有入站	任意端口任意协议	任意到任意	阻止所有其他入站流量

HA 系统的入站规则

添加Cloud Volumes ONTAP系统并选择预定义安全组时，您可以选择允许以下之一内的流量：

- 仅限选定的 **VNet**：入站流量的来源是Cloud Volumes ONTAP系统的 VNet 子网范围和控制台代理所在的 VNet 子网范围。这是推荐的选项。
- 所有 **VNets**：入站流量的来源是 0.0.0.0/0 IP 范围。

HA 系统的入站规则少于单节点系统，因为入站数据流量通过 Azure Standard Load Balancer。因此，应打开来自 Load Balancer 的流量，如"AllowAzureLoadBalancerInBound"规则中所示。

- 已禁用：此选项限制对您的存储帐户的公共网络访问，并禁用Cloud Volumes ONTAP系统的数据分层。如果

由于安全法规和政策，您的私有 IP 地址即使在同一个 VNet 内也不应该暴露，那么建议使用此选项。

优先级和名称	端口和协议	来源和目的地	描述
100 inbound_443	443 任何协议	任意到任意	使用集群管理 LIF 的 IP 地址与控制台代理建立连接并通过 HTTPS 访问ONTAP System Manager Web 控制台
101 inbound_111_tcp	111 任何协议	任意到任意	NFS 的远程过程调用
102 inbound_2049_tcp	2049 任何协议	任意到任意	NFS 服务器守护进程
111 入站_ssh	22 任何协议	任意到任意	通过 SSH 访问集群管理 LIF 或节点管理 LIF 的 IP 地址
121 inbound_53	53 任何协议	任意到任意	DNS 和 CIFS
65000 允许 VnetInBound	任意端口任意协议	虚拟网络到虚拟网络	来自 VNet 内部的入站流量
65001 允许 Azure 负载均衡器入站	任意端口任意协议	AzureLoadBalancer 到任意	来自 Azure 标准负载均衡器的数据流量
65500 拒绝所有入站	任意端口任意协议	任意到任意	阻止所有其他入站流量

出站规则

Cloud Volumes ONTAP的预定义安全组打开所有出站流量。如果可以接受，请遵循基本的出站规则。如果您需要更严格的规则，请使用高级出站规则。

基本出站规则

Cloud Volumes ONTAP的预定义安全组包括以下出站规则。

端口	协议	目的
全部	所有 TCP	所有出站流量
全部	所有 UDP	所有出站流量

高级出站规则

如果您需要对出站流量制定严格的规则，则可以使用以下信息仅打开Cloud Volumes ONTAP出站通信所需的端口。

源是Cloud Volumes ONTAP系统上的接口（IP 地址）。

服务	端口	协议	源	目标	目的
Active Directory	88	TCP	节点管理 LIF	Active Directory 林	Kerberos V 身份验证
	137	UDP	节点管理 LIF	Active Directory 林	NetBIOS 名称服务
	138	UDP	节点管理 LIF	Active Directory 林	NetBIOS 数据报服务
	139	TCP	节点管理 LIF	Active Directory 林	NetBIOS 服务会话
	389	TCP 和 UDP	节点管理 LIF	Active Directory 林	LDAP
	445	TCP	节点管理 LIF	Active Directory 林	使用 NetBIOS 框架的 TCP 上的 Microsoft SMB/CIFS
	464	TCP	节点管理 LIF	Active Directory 林	Kerberos V 更改和设置密码（SET_CHANGE）
	464	UDP	节点管理 LIF	Active Directory 林	Kerberos 密钥管理
	749	TCP	节点管理 LIF	Active Directory 林	Kerberos V 更改和设置密码（RPCSEC_GSS）
	88	TCP	数据 LIF（NFS 、CIFS、iSCSI）	Active Directory 林	Kerberos V 身份验证
	137	UDP	数据 LIF（NFS 、CIFS）	Active Directory 林	NetBIOS 名称服务
	138	UDP	数据 LIF（NFS 、CIFS）	Active Directory 林	NetBIOS 数据报服务
	139	TCP	数据 LIF（NFS 、CIFS）	Active Directory 林	NetBIOS 服务会话
	389	TCP 和 UDP	数据 LIF（NFS 、CIFS）	Active Directory 林	LDAP
	445	TCP	数据 LIF（NFS 、CIFS）	Active Directory 林	使用 NetBIOS 框架的 TCP 上的 Microsoft SMB/CIFS
	464	TCP	数据 LIF（NFS 、CIFS）	Active Directory 林	Kerberos V 更改和设置密码（SET_CHANGE）
	464	UDP	数据 LIF（NFS 、CIFS）	Active Directory 林	Kerberos 密钥管理
	749	TCP	数据 LIF（NFS 、CIFS）	Active Directory 林	Kerberos V 更改和设置密码（RPCSEC_GSS）
AutoSupport	HTTPS	443	节点管理 LIF	mysupport.netapp.com	AutoSupport （默认为 HTTPS）
	HTTP	80	节点管理 LIF	mysupport.netapp.com	AutoSupport （仅当传输协议从 HTTPS 更改为 HTTP 时）
	TCP	3128	节点管理 LIF	控制台代理	如果出站互联网连接不可用，则通过控制台代理上的代理服务器发送AutoSupport消息

服务	端口	协议	源	目标	目的
配置备份	HTTP	80	节点管理 LIF	http://<控制台代理 IP 地址>/occm/offboxconfig	将配置备份发送到控制台代理。"ONTAP 文档" 。
DHCP	68	UDP	节点管理 LIF	DHCP	首次设置的 DHCP 客户端
DHCP服务	67	UDP	节点管理 LIF	DHCP	DHCP 服务器
DNS	53	UDP	节点管理 LIF 和数据 LIF（NFS、CIFS）	DNS	DNS
NDMP	18600-18699	TCP	节点管理 LIF	目标服务器	NDMP 拷贝
SMTP	25	TCP	节点管理 LIF	邮件服务器	SMTP 警报，可用于AutoSupport
SNMP	161	TCP	节点管理 LIF	监控服务器	通过 SNMP 陷阱进行监控
	161	UDP	节点管理 LIF	监控服务器	通过 SNMP 陷阱进行监控
	162	TCP	节点管理 LIF	监控服务器	通过 SNMP 陷阱进行监控
	162	UDP	节点管理 LIF	监控服务器	通过 SNMP 陷阱进行监控
SnapMirror	11104	TCP	集群间 LIF	ONTAP集群间 LIF	SnapMirror集群间通信会话的管理
	11105	TCP	集群间 LIF	ONTAP集群间 LIF	SnapMirror数据传输
系统日志	514	UDP	节点管理 LIF	系统日志服务器	Syslog 转发消息

控制台代理的要求

如果您尚未创建控制台代理，您也应该查看控制台代理的网络要求。

- "查看控制台代理的网络要求"
- "Azure 中的安全组规则"

相关主题

- "验证Cloud Volumes ONTAP 的AutoSupport设置"
- "了解ONTAP内部端口" 。

设置**Cloud Volumes ONTAP**以在 **Azure** 中使用客户管理的密钥

使用带有 Microsoft 管理密钥的 Azure 存储服务加密，数据在 Azure 中的Cloud Volumes ONTAP上自动加密。但是您可以按照本页上的步骤使用您自己的加密密钥。

数据加密概述

Cloud Volumes ONTAP数据在 Azure 中自动使用 "Azure 存储服务加密"。默认实现使用 Microsoft 管理的密钥。无需设置。

如果您想将客户管理的密钥与Cloud Volumes ONTAP一起使用，则需要完成以下步骤：

1. 从 Azure 创建一个密钥保管库，然后在该保管库中生成一个密钥。
2. 从NetApp Console，使用 API 创建使用密钥的Cloud Volumes ONTAP系统。

数据如何加密

控制台使用磁盘加密集，从而可以通过托管磁盘而不是页面 blob 来管理加密密钥。任何新的数据磁盘也使用相同的磁盘加密集。较低版本将使用 Microsoft 管理的密钥，而不是客户管理的密钥。

创建配置为使用客户管理密钥的Cloud Volumes ONTAP系统后， Cloud Volumes ONTAP数据将按如下方式加密。

Cloud Volumes ONTAP配置	用于密钥加密的系统磁盘	用于密钥加密的数据磁盘
单节点	• 引导 • 核 • NVRAM	• 根 • 数据
具有页 Blob 的 Azure HA 单可用性区域	• 引导 • 核 • NVRAM	无
具有共享托管磁盘的 Azure HA 单可用性区域	• 引导 • 核 • NVRAM	• 根 • 数据
具有共享托管磁盘的 Azure HA 多个可用性区域	• 引导 • 核 • NVRAM	• 根 • 数据

Cloud Volumes ONTAP的所有 Azure 存储帐户均使用客户管理的密钥加密。如果您想在创建存储帐户期间对其进行加密，则必须在Cloud Volumes ONTAP创建请求中创建并提供资源的 ID。这适用于所有类型的部署。如果您不提供，存储帐户仍将被加密，但控制台首先使用 Microsoft 管理的密钥加密创建存储帐户，然后更新存储帐户以使用客户管理的密钥。

Cloud Volumes ONTAP中的密钥轮换

配置加密密钥时，必须使用 Azure 门户来设置并启用自动密钥轮换。创建并启用新版本的加密密钥可确保Cloud Volumes ONTAP可以自动检测并使用最新的密钥版本进行加密，从而确保您的数据保持安全而无需人工干预。

有关配置密钥和设置密钥轮换的信息，请参阅以下 Microsoft Azure 文档主题：

- "在 Azure Key Vault 中配置加密密钥自动轮换"
- "Azure PowerShell - 启用客户管理的密钥"

配置密钥后，请确保已选择 "启用自动旋转"，以便Cloud Volumes ONTAP可以在之前的密钥过期时使用新的密钥。如果您未在 Azure 门户上启用此选项， Cloud Volumes ONTAP将无法自动检测新密钥，这可能会导致存储配置问题。

创建用户分配的托管标识

您可以选择创建称为用户分配的托管标识的资源。这样做可以让您在创建Cloud Volumes ONTAP系统时加密您的存储帐户。我们建议在创建密钥保管库和生成密钥之前创建此资源。

该资源具有以下 ID： `userassignedidentity` 。

步骤

1. 在 Azure 中，转到 Azure 服务并选择 托管标识。
2. 单击“创建”。
3. 提供以下详细信息：
   - 订阅：选择订阅。我们建议选择与控制台代理的订阅相同的订阅。
   - 资源组：使用现有资源组或创建一个新的资源组。
   - 区域：可选，选择与控制台代理相同的区域。
   - 名称：输入资源的名称。
4. （可选）添加标签。
5. 单击“创建”。

创建密钥保管库并生成密钥

密钥保管库必须位于您计划创建Cloud Volumes ONTAP系统的同一 Azure 订阅和区域中。

如果你创建了用户分配的托管标识，在创建密钥保管库时，还应该为密钥保管库创建访问策略。

步骤

1. "在 Azure 订阅中创建密钥保管库" 。

   请注意密钥保管库的以下要求：

   - 密钥保管库必须与Cloud Volumes ONTAP系统位于同一区域。
   - 应启用以下选项：
     - 软删除（此选项默认启用，但不能禁用）
     - 清除保护
     - 用于卷加密的 **Azure Disk Encryption**（适用于单节点系统、多个区域中的 HA 对和 HA 单 AZ 部署）

       使用 Azure 客户管理加密密钥的前提是为密钥保管库启用 Azure 磁盘加密。
   - 如果创建了用户分配的托管标识，则应启用以下选项：
     - 保险库访问政策

2. 如果选择了“保管库访问策略”，请单击“创建”为密钥保管库创建访问策略。如果没有，请跳至步骤 3。
   a. 选择以下权限：
      - 得到
      - 列表
      - 解密
      - 加密
      - 解开密钥
      - 包装键
      - 核实
      - 符号
   b. 选择用户分配的托管标识（资源）作为主体。
   c. 审查并创建访问策略。
3. "在密钥保管库中生成密钥" 。

   请注意以下密钥要求：

   - 密钥类型必须是*RSA*。
   - 建议的 RSA 密钥大小为 **2048**，但也支持其他大小。

创建使用加密密钥的系统

创建密钥保管库并生成加密密钥后，您可以创建配置为使用该密钥的新Cloud Volumes ONTAP系统。这些步骤通过使用 API 来支持。

所需权限

如果要在单节点Cloud Volumes ONTAP系统中使用客户管理密钥，请确保控制台代理具有以下权限：

```
"Microsoft.Compute/diskEncryptionSets/read",
"Microsoft.Compute/diskEncryptionSets/write",
"Microsoft.Compute/diskEncryptionSets/delete"
"Microsoft.KeyVault/vaults/deploy/action",
"Microsoft.KeyVault/vaults/read",
"Microsoft.KeyVault/vaults/accessPolicies/write",
"Microsoft.ManagedIdentity/userAssignedIdentities/assign/action"
```

"查看最新的权限列表"

步骤

1. 使用以下 API 调用获取 Azure 订阅中的密钥保管库列表。

   对于 HA 对： `GET /azure/ha/metadata/vaults`

对于单节点： `GET /azure/vsa/metadata/vaults`

记下*名称*和*资源组*。您需要在下一步中指定这些值。

"了解有关此 API 调用的更多信息"。

2. 使用以下 API 调用获取保管库中的密钥列表。

对于 HA 对： `GET /azure/ha/metadata/keys-vault`

对于单节点： `GET /azure/vsa/metadata/keys-vault`

记下*keyName*。您需要在下一步中指定该值（以及保险库名称）。

"了解有关此 API 调用的更多信息"。

3. 使用以下 API 调用创建Cloud Volumes ONTAP系统。

a. 对于 HA 对：

`POST /azure/ha/working-environments`

请求主体必须包含以下字段：

```
"azureEncryptionParameters": {
                "key": "keyName",
                "vaultName": "vaultName"
}
```

包括 `"userAssignedIdentity": " userAssignedIdentityId"`如果您创建此资源是为了用于存储帐户加密，则字段。

"了解有关此 API 调用的更多信息"。

b. 对于单节点系统：

`POST /azure/vsa/working-environments`

请求主体必须包含以下字段：

```
"azureEncryptionParameters": {
                "key": "keyName",
                "vaultName": "vaultName"
}
```

包括 `"userAssignedIdentity": " userAssignedIdentityId"`如果您创建此资源是为了用于存储帐户加密，则字段。

"了解有关此 API 调用的更多信息" 。

结果

您有一个新的Cloud Volumes ONTAP系统，该系统配置为使用客户管理的密钥进行数据加密。

在 **Azure** 中设置**Cloud Volumes ONTAP**许可

在您决定要对Cloud Volumes ONTAP使用哪种许可选项后，需要执行几个步骤才能在创建新系统时选择该许可选项。

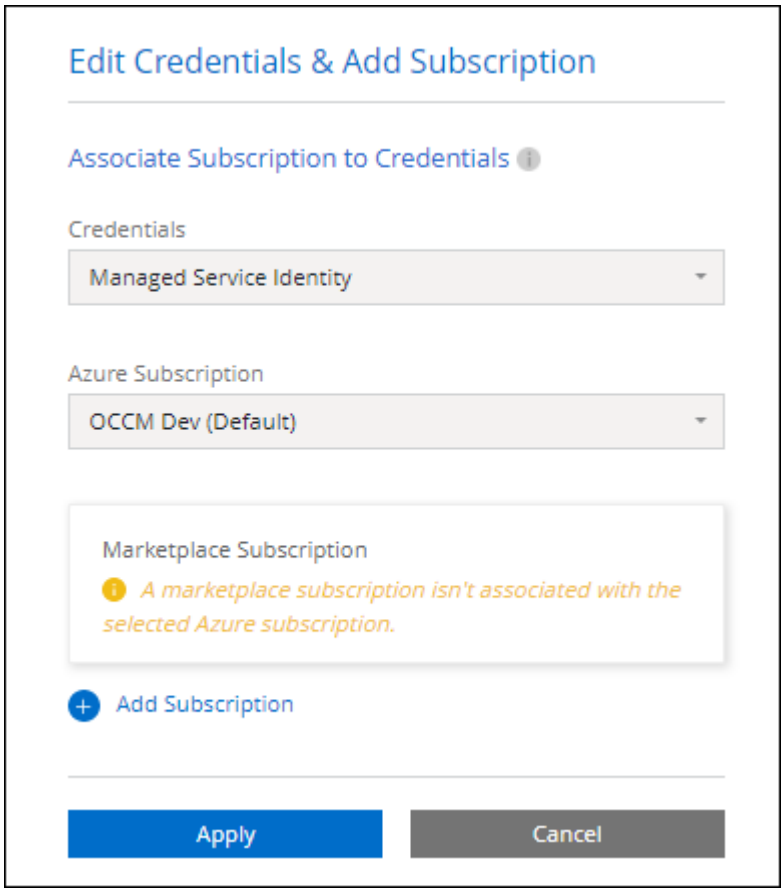
免费增值

选择免费增值服务，免费使用Cloud Volumes ONTAP，最高可提供 500 GiB 的配置容量。"了解有关免费增值服务的更多信息" 。

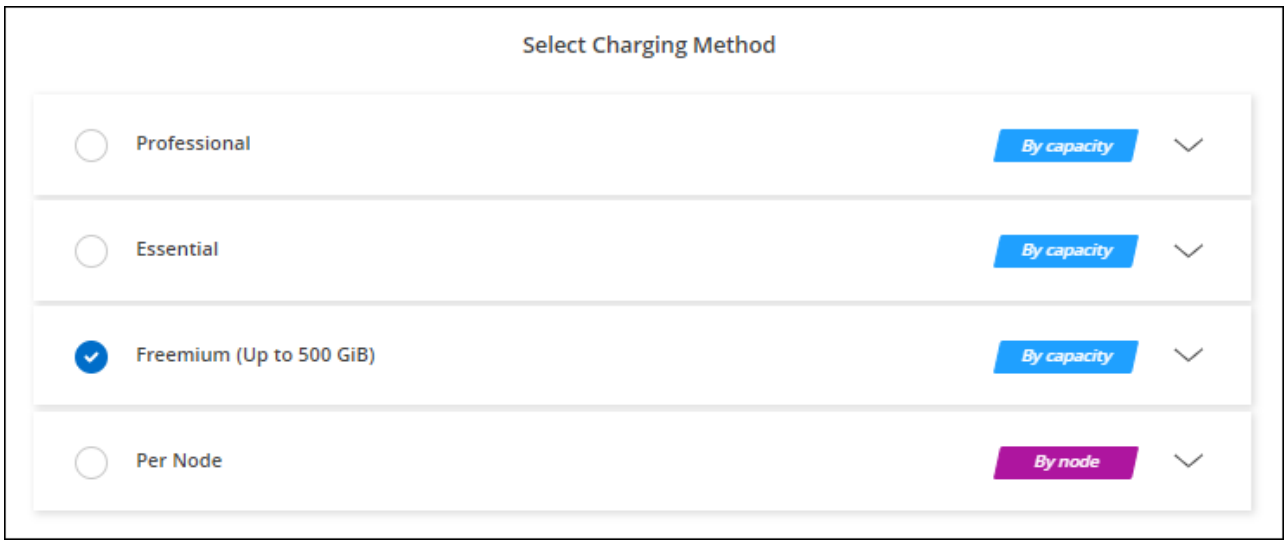
步骤

1. 从NetApp Console的左侧导航菜单中，选择“存储”>“管理”。
2. 在*系统*页面上，单击*添加系统*并按照步骤操作。
   a. 在“详细信息和凭据”页面上，单击“编辑凭据”>“添加订阅”，然后按照提示订阅 Azure 市场中的即用即付产品。

      除非您超过 500 GiB 的预配置容量，否则您无需通过市场订阅付费，此时系统将自动转换为"基本套餐"。



a. 返回控制台后，到达收费方式页面时选择“免费增值”。



"查看在 Azure 中启动Cloud Volumes ONTAP 的分步说明" 。

基于容量的许可证

基于容量的许可使您能够按 TiB 容量支付Cloud Volumes ONTAP费用。基于容量的许可以_包_的形式提供：Essentials 包或 Professional 包。

Essentials 和 Professional 套餐提供以下几种消费模式或购买选项：

- 从NetApp购买的许可证（自带许可证 (BYOL)）
- Azure 市场提供的按小时付费 (PAYGO) 订阅
- 年度合同

"了解有关基于容量的许可的更多信息" 。

以下部分介绍了如何开始使用每种消费模型。

BYOL

通过从NetApp购买许可证 (BYOL) 进行预付款，以便在任何云提供商处部署Cloud Volumes ONTAP系统。

已限制 BYOL 许可证的购买、延期和续订。有关更多信息，请参阅 "Cloud Volumes ONTAP的 BYOL 许可可用性受限" 。

步骤

1. "联系NetApp销售人员获取许可证"
2. "将您的NetApp支持站点帐户添加到控制台"

   控制台会自动查询 NetApp 的许可服务，以获取与您的NetApp支持站点帐户相关的许可证的详细信息。如果没有错误，控制台会自动将许可证添加到控制台。

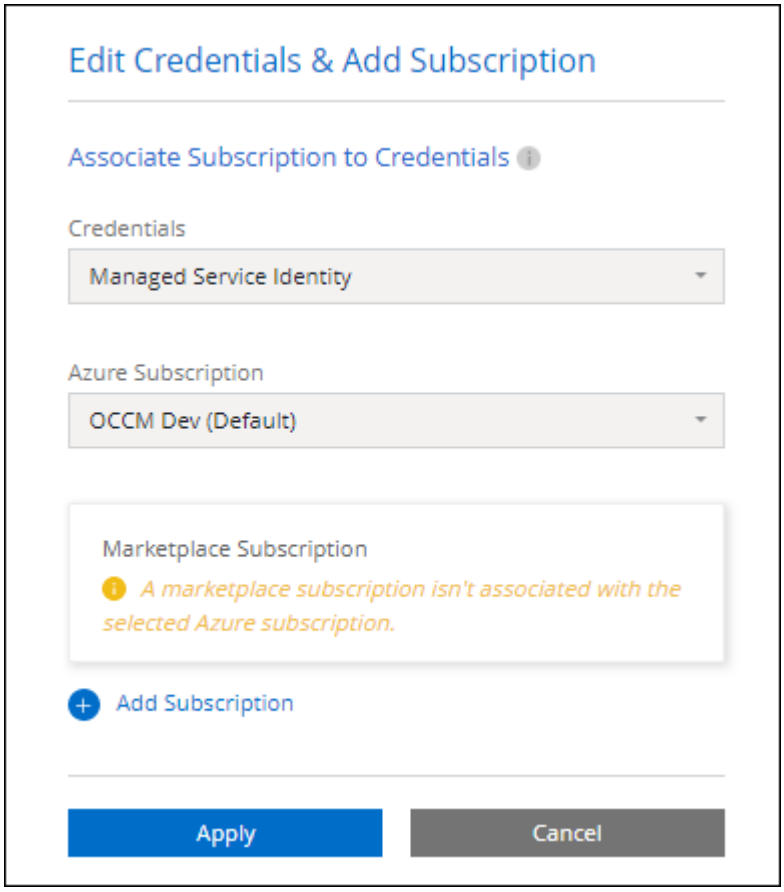
   您必须先从控制台获取许可证，然后才能将其与Cloud Volumes ONTAP一起使用。如果需要的话，你可以"

手动将许可证添加到控制台"。

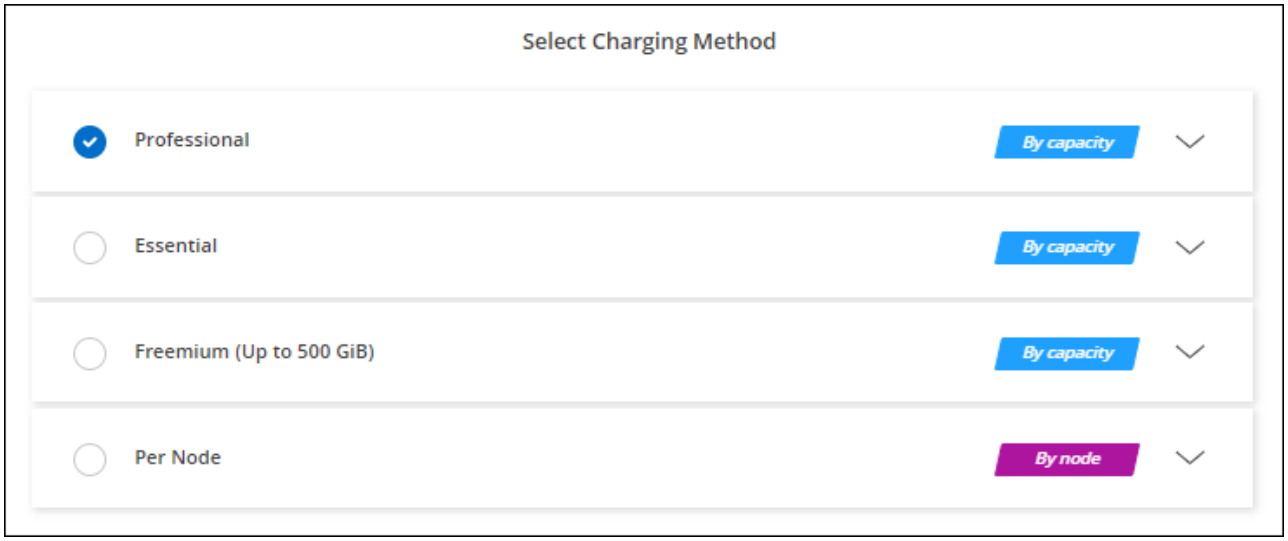
3. 在*系统*页面上，单击*添加系统*并按照步骤操作。

   a. 在“详细信息和凭据”页面上，单击“编辑凭据”>“添加订阅”，然后按照提示订阅 Azure 市场中的即用即付产品。

      始终会先向您从NetApp购买的许可证收费，但如果您超出许可容量或许可证期限到期，则会按照市场上的小时费率向您收费。



   a. 返回控制台后，在进入收费方式页面时选择基于容量的套餐。



"查看在 Azure 中启动Cloud Volumes ONTAP 的分步说明" 。

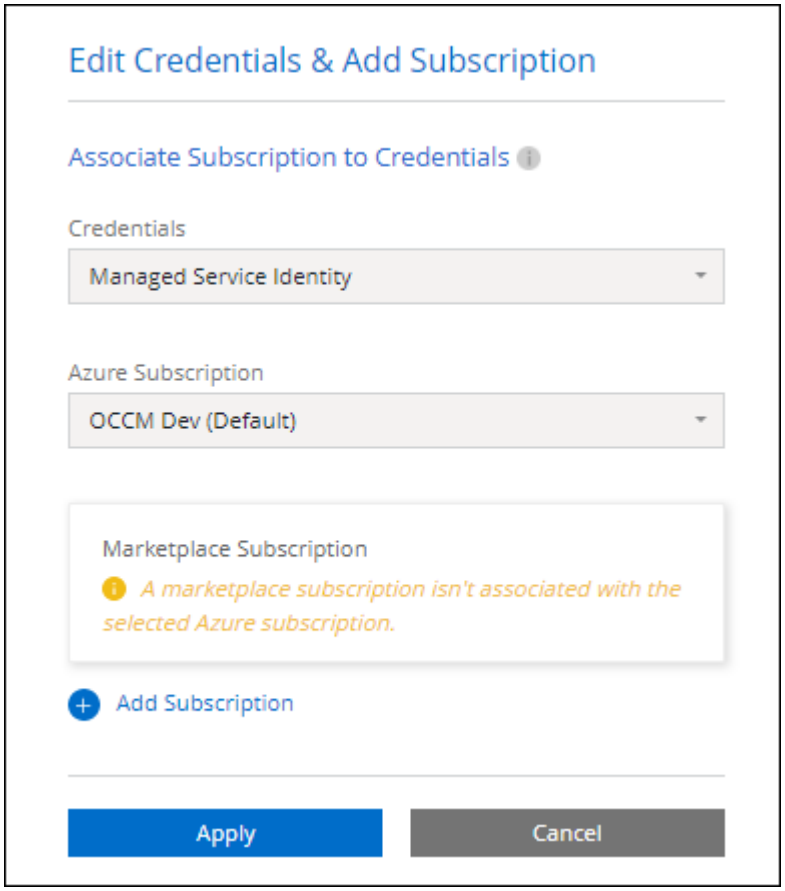
PAYGO 订阅

通过订阅云提供商市场提供的服务按小时付费。

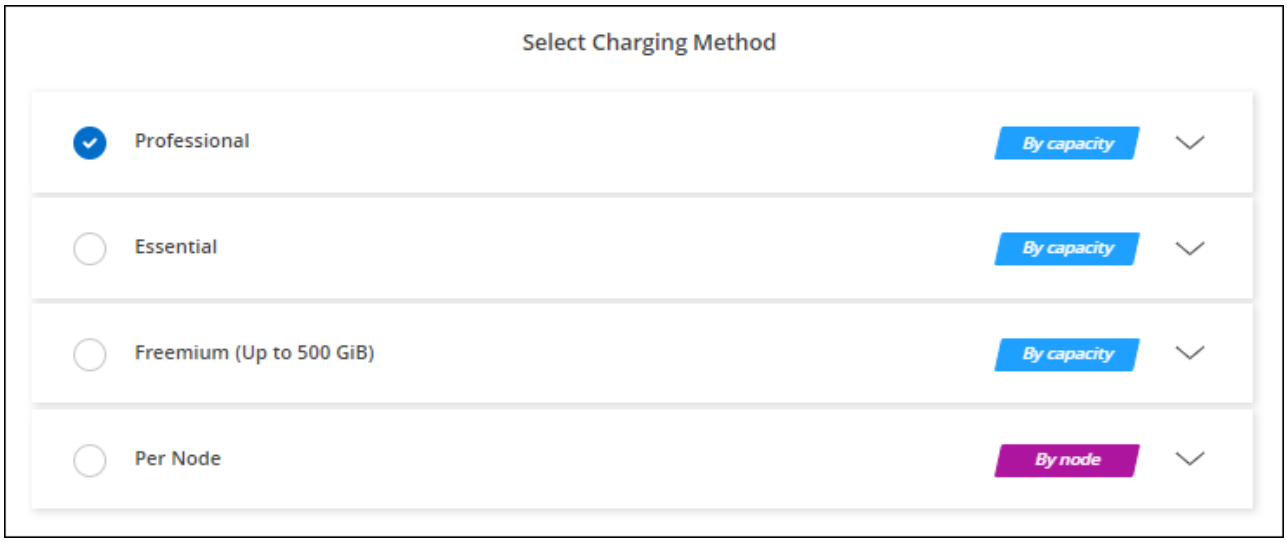
当您创建Cloud Volumes ONTAP系统时，控制台会提示您订阅 Azure 市场中提供的协议。然后将该订阅与系统关联以进行收费。您可以将同一订阅用于其他系统。

步骤

1. 从左侧导航菜单中，选择“存储”>“管理”。
2. 在*系统*页面上，单击*添加系统*并按照步骤操作。
   a. 在“详细信息和凭据”页面上，单击“编辑凭据”>“添加订阅”，然后按照提示订阅 Azure 市场中的即用即付产品。



   b. 返回控制台后，在进入收费方式页面时选择基于容量的套餐。



"查看在 Azure 中启动Cloud Volumes ONTAP 的分步说明" 。

您可以从“设置”>“凭据”页面管理与您的 Azure 帐户关联的 Azure 市场订阅。 "了解如何管理 Azure 帐户和订阅"

年度合同

通过购买年度合同每年支付Cloud Volumes ONTAP 的费用。

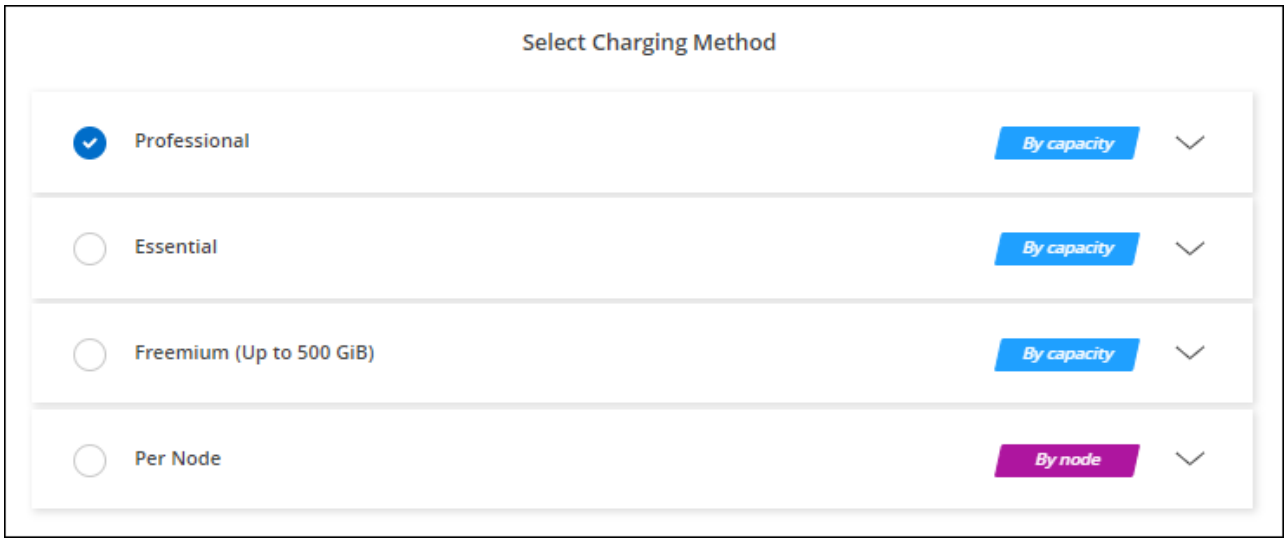
步骤

1. 联系您的NetApp销售代表购买年度合同。

   该合同在 Azure 市场中以私人优惠的形式提供。

   NetApp与您分享私人优惠后，您可以在系统创建期间从 Azure 市场订阅时选择年度计划。

2. 在*系统*页面上，单击*添加系统*并按照步骤操作。
   a. 在“详细信息和凭据”页面上，单击“编辑凭据”>“添加订阅”>“继续”。
   b. 在 Azure 门户中，选择与您的 Azure 帐户共享的年度计划，然后单击“订阅”。
   c. 返回控制台后，在进入收费方式页面时选择基于容量的套餐。



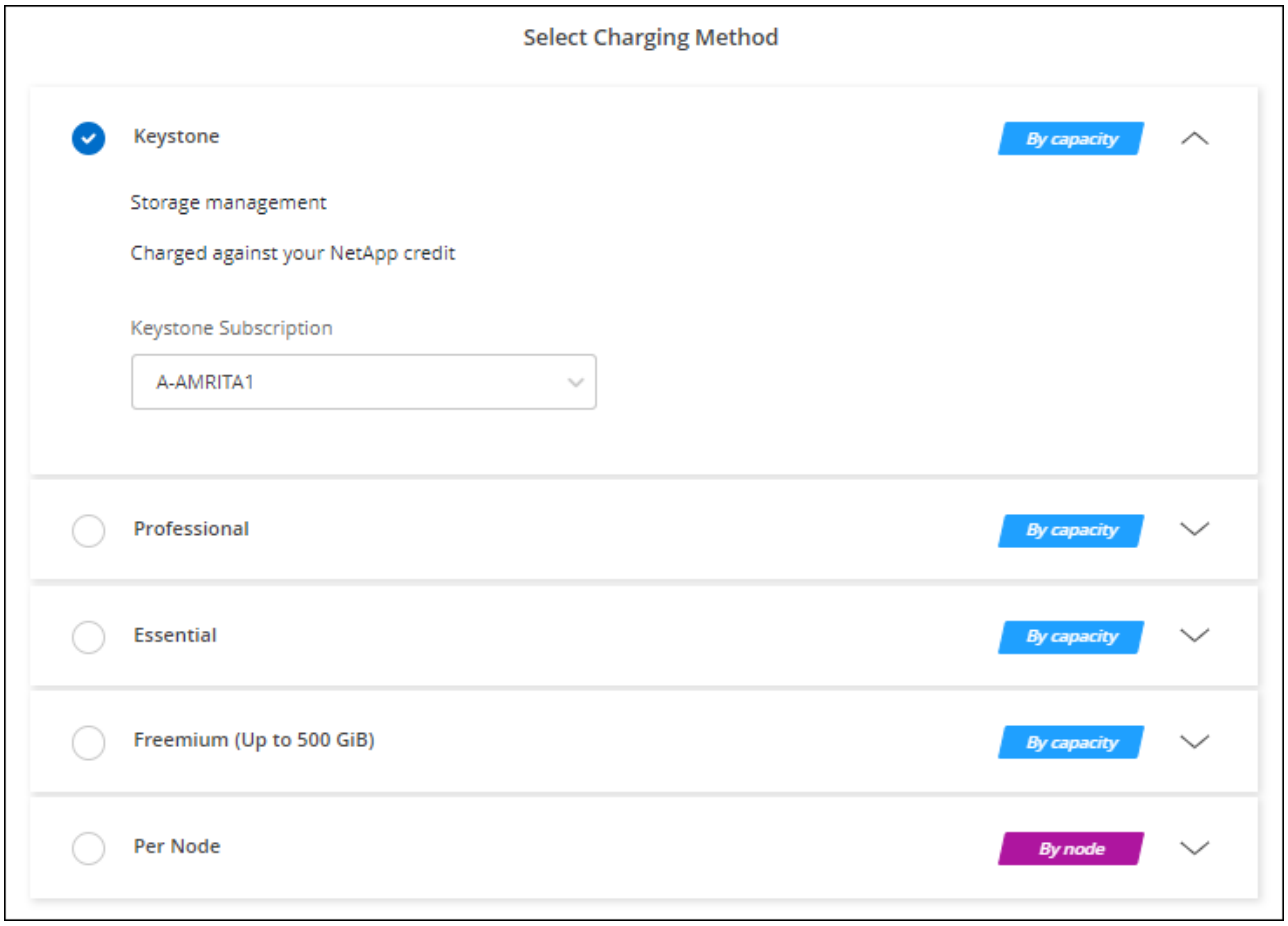
"查看在 Azure 中启动Cloud Volumes ONTAP 的分步说明" 。

Keystone订阅

Keystone订阅是一种按需付费的订阅式服务。"了解有关NetApp Keystone订阅的更多信息" 。

步骤

1. 如果您尚未订阅， "联系NetApp"
2. 联系NetApp 以在控制台中授权您的用户帐户拥有一个或多个Keystone订阅。
3. NetApp授权您的帐户后，"链接您的订阅以用于Cloud Volumes ONTAP" 。
4. 在*系统*页面上，单击*添加系统*并按照步骤操作。
    a. 当提示选择收费方式时，选择Keystone Subscription 收费方式。



"查看在 Azure 中启动Cloud Volumes ONTAP 的分步说明" 。

基于节点的许可证

基于节点的许可证是Cloud Volumes ONTAP的上一代许可证。基于节点的许可证可以从NetApp (BYOL) 处购买，并且仅在特定情况下才可以续订许可证。有关信息，请参阅：

- "基于节点的许可证的可用性终止"
- "基于节点的许可证的可用性终止"
- "将基于节点的许可证转换为基于容量的许可证"

在 **Azure** 中为**Cloud Volumes ONTAP**启用高可用性模式

您应该启用 Microsoft Azure 的高可用性 (HA) 模式，以减少计划外故障转移时间，并为 Cloud Volumes ONTAP 启用 NFSv4 支持。如果启用此模式，您的 Cloud Volumes ONTAP HA 节点可以在 CIFS 和 NFSv4 客户端上的计划外故障转移期间实现较低（60 秒）的恢复时间目标 (RTO)。

从Cloud Volumes ONTAP 9.10.1 开始，我们减少了在 Microsoft Azure 中运行的Cloud Volumes ONTAP HA 对的计划外故障转移时间，并增加了对 NFSv4 的支持。要使这些增强功能可用于Cloud Volumes ONTAP，您需要在 Azure 订阅上启用高可用性功能。

关于此任务

当需要在 Azure 订阅上启用此功能时，NetApp Console 会提示您这些详细信息。请注意以下事项：

- 您的Cloud Volumes ONTAP HA 对的高可用性没有问题。此 Azure 功能与ONTAP协同工作，以减少客户端观察到的因计划外故障转移事件导致的 NFS 协议应用程序中断时间。
- 启用此功能不会对Cloud Volumes ONTAP HA 对造成破坏。
- 在您的 Azure 订阅上启用此功能不会给其他虚拟机带来问题。
- Cloud Volumes ONTAP在 CIFS 和 NFS 客户端上的集群和 SVM 管理 LIF 故障转移期间使用内部 Azure 负载均衡器。
- 启用 HA 模式后，控制台每 12 小时扫描一次系统以更新内部 Azure 负载均衡器规则。

步骤

具有 *Owner* 权限的 Azure 用户可以从 Azure CLI 启用该功能。

1. "从 Azure 门户访问 Azure Cloud Shell"
2. 注册高可用性模式功能：

```
az account set -s AZURE_SUBSCRIPTION_NAME_OR_ID
az feature register --name EnableHighAvailabilityMode --namespace
Microsoft.Network
az provider register -n Microsoft.Network
```

3. （可选）验证该功能现在是否已注册：

```
az feature show --name EnableHighAvailabilityMode --namespace
Microsoft.Network
```

Azure CLI 应返回类似于以下内容的结果：

```
{
  "id": "/subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-
xxxxxxxxxxxx/providers/Microsoft.Features/providers/Microsoft.Network/fe
atures/EnableHighAvailabilityMode",
  "name": "Microsoft.Network/EnableHighAvailabilityMode",
  "properties": {
    "state": "Registered"
  },
  "type": "Microsoft.Features/providers/features"
}
```

相关链接

1. "Microsoft Azure 文档：高可用性端口概述"

2. "Microsoft Azure 文档：Azure CLI 入门"

在 **Azure** 中为**Cloud Volumes ONTAP**启用 **VMOrchestratorZonalMultiFD**

要在本地冗余存储 (LRS) 单可用区 (AZ) 中部署虚拟机实例，您应该激活 Microsoft `Microsoft.Compute/VMOrchestratorZonalMultiFD`您的订阅功能。在高可用性 (HA) 模式下，此功能有助于在同一可用区域内的不同故障域中部署节点。

除非您激活此功能，否则不会发生区域部署，并且之前的 LRS 非区域部署将生效。

有关在单个可用区域中部署虚拟机的信息，请参阅"Azure 中的高可用性对"。

以具有“所有者”权限的用户身份执行以下步骤：

步骤

1. 从 Azure 门户访问 Azure Cloud Shell。欲了解更多信息，请参阅 "Microsoft Azure 文档：Azure Cloud Shell 入门"。
2. 注册 `Microsoft.Compute/VMOrchestratorZonalMultiFD`通过运行以下命令来启用此功能：

   ```
   az 帐户设置 -s <Azure_subscription_name_or_ID> az 功能注册 --name VMOrchestratorZonalMultiFD --namespace Microsoft.Compute
   ```

3. 验证注册状态及输出样例：

   ```
   az feature show -n VMOrchestratorZonalMultiFD --namespace Microsoft.Compute { “id”：“/subscriptions/<ID>/providers/Microsoft.Features/providers/Microsoft.Compute/features/VMOrchestratorZonalMultiFD”， “name”：“Microsoft.Compute/VMOrchestratorZonalMultiFD”， “properties”：{ “state”：“Registered” }，“type”：“Microsoft.Features/providers/features” }
   ```

在 **Azure** 中启动**Cloud Volumes ONTAP**

您可以通过在 NetApp Console 中创建 Cloud Volumes ONTAP 系统来在 Azure 中启动单节点系统或 HA 对。

开始之前

开始之前您需要以下内容。

- 已启动并正在运行的控制台代理。
  - 你应该有一个 "与您的系统关联的控制台代理"。
  - "您应该准备好让控制台代理始终处于运行状态" 。
- 了解您想要使用的配置。

  您应该有一个配置计划，并且从管理员那里获得必要的 Azure 网络详细信息。有关详细信息，请参阅"规划您的Cloud Volumes ONTAP配置" 。

- 了解设置Cloud Volumes ONTAP许可所需的条件。

  "了解如何设置许可" 。

关于此任务

当控制台在 Azure 中创建Cloud Volumes ONTAP系统时，它会创建多个 Azure 对象，例如资源组、网络接口和存储帐户。您可以在向导结束时查看资源摘要。

> 数据丢失的可能性
>
> 最佳做法是为每个Cloud Volumes ONTAP系统使用一个新的专用资源组。
>
> 由于存在数据丢失的风险，不建议在现有的共享资源组中部署Cloud Volumes ONTAP 。虽然控制台可以在部署失败或删除的情况下从共享资源组中删除Cloud Volumes ONTAP资源，但 Azure 用户可能会意外从共享资源组中删除Cloud Volumes ONTAP资源。

在 **Azure** 中启动单节点**Cloud Volumes ONTAP**系统

如果要在 Azure 中启动单节点 Cloud Volumes ONTAP 系统，需要在 Console 中创建单节点系统。

步骤

1. 从左侧导航菜单中，选择“存储”>“管理”。
2. 在*系统*页面上，单击*添加系统*并按照提示进行操作。
3. 选择位置：选择*Microsoft Azure*和* Cloud Volumes ONTAP单节点*。
4. 如果出现提示， "创建控制台代理" 。
5. 详细信息和凭据：可选择更改 Azure 凭据和订阅，指定群集名称，根据需要添加标签，然后指定凭据。

   下表描述了您可能需要指导的字段：

字段	描述
系统名称	控制台使用系统名称来命名Cloud Volumes ONTAP系统和 Azure 虚拟机。如果您选择该选项，它还会使用该名称作为预定义安全组的前缀。
资源组标签	标签是 Azure 资源的元数据。当您在此字段中输入标签时，控制台会将它们添加到与Cloud Volumes ONTAP系统关联的资源组中。创建系统时，您可以从用户界面添加最多四个标签，然后可以在创建系统后添加更多标签。请注意，创建系统时，API 不会将您限制为四个标签。有关标签的信息，请参阅 "Microsoft Azure 文档：使用标签来组织您的 Azure 资源"。
用户名和密码	这些是Cloud Volumes ONTAP集群管理员帐户的凭据。您可以使用这些凭据通过ONTAP System Manager 或ONTAP CLI 连接到Cloud Volumes ONTAP 。保留默认的_admin_用户名或将其更改为自定义用户名。
编辑凭证	您可以选择不同的 Azure 凭据和不同的 Azure 订阅来与此Cloud Volumes ONTAP系统一起使用。您需要将 Azure 市场订阅与选定的 Azure 订阅关联，以便部署即用即付的Cloud Volumes ONTAP系统。 "了解如何添加凭证" 。

6. 服务：启用或禁用您想要或不想与Cloud Volumes ONTAP一起使用的单个服务。
   - "了解有关NetApp Data Classification的更多信息"

- "了解有关NetApp Backup and Recovery的更多信息"

> 如果您想使用 WORM 和数据分层，则必须禁用备份和恢复并部署版本 9.8 或更高版本的Cloud Volumes ONTAP系统。

7. 位置：选择区域、可用区域、VNet 和子网，然后选中复选框以确认控制台代理和目标位置之间的网络连接。

> 对于中国区域，仅Cloud Volumes ONTAP 9.12.1 GA 和 9.13.0 GA 支持单节点部署。您可以将这些版本升级到Cloud Volumes ONTAP的更高补丁和版本，如下所示"Azure 中支持"。如果您想在中国地区部署更高版本的Cloud Volumes ONTAP ，请联系NetApp支持。中国地区仅支持直接从NetApp购买的许可证，不提供市场订阅。

8. 连接：选择一个新的或现有的资源组，然后选择是否使用预定义的安全组或使用您自己的安全组。

   下表描述了您可能需要指导的字段：

字段	描述
资源组	为Cloud Volumes ONTAP创建新的资源组或使用现有的资源组。最佳做法是为Cloud Volumes ONTAP使用新的专用资源组。虽然可以在现有的共享资源组中部署Cloud Volumes ONTAP ，但由于存在数据丢失的风险，因此不建议这样做。请参阅上面的警告以了解更多详细信息。 如果您使用的 Azure 帐户具有 "所需权限"，如果部署失败或删除，控制台会从资源组中删除Cloud Volumes ONTAP资源。
生成的安全组	如果您让控制台为您生成安全组，则需要选择如何允许流量： • 如果选择*仅限选定的 VNet*，则入站流量的来源是选定 VNet 的子网范围和控制台代理所在的 VNet 的子网范围。这是推荐的选项。 • 如果选择“所有 **VNets**”，则入站流量的来源是 0.0.0.0/0 IP 范围。
使用现有的	如果您选择现有的安全组，则它必须满足Cloud Volumes ONTAP要求。"查看默认安全组" 。

9. 收费方式和 **NSS** 帐户：指定您想要在此系统中使用的收费选项，然后指定NetApp支持站点帐户。
   - "了解Cloud Volumes ONTAP的许可选项" 。
   - "了解如何设置许可" 。
10. 预配置包：选择其中一个包来快速部署Cloud Volumes ONTAP系统，或者单击*创建我自己的配置*。

    如果您选择其中一个套餐，您只需指定一个卷，然后审核并批准配置。

11. 许可：如果需要，更改Cloud Volumes ONTAP版本，并选择虚拟机类型。

> 如果所选版本有较新的候选版本、通用版本或补丁版本，则BlueXP会在创建工作环境时将系统更新到该版本。例如，如果您选择Cloud Volumes ONTAP 9.16.1 P3 并且 9.16.1 P4 可用，则会发生更新。更新不会从一个版本发生到另一个版本 - 例如，从 9.15 到 9.16。

12. 从 **Azure** 市场订阅：如果控制台无法启用Cloud Volumes ONTAP的编程部署，您将看到此页面。按照屏幕上列出的步骤操作。请参阅 "以编程方式部署 Marketplace 产品"了解更多信息。
13. 底层存储资源：选择初始聚合的设置：磁盘类型、每个磁盘的大小以及是否应启用数据分层到 Blob 存储。

    请注意以下事项：

    - 如果在 VNet 中禁用了对您的存储帐户的公共访问，则您无法在Cloud Volumes ONTAP系统中启用数据分层。有关信息，请参阅"安全组规则"。
    - 磁盘类型适用于初始卷。您可以为后续卷选择不同的磁盘类型。
    - 磁盘大小适用于初始聚合中的所有磁盘以及使用简单配置选项时控制台创建的任何其他聚合。您可以使用高级分配选项创建使用不同磁盘大小的聚合。

      有关选择磁盘类型和大小的帮助，请参阅"在 Azure 中调整系统大小"。

    - 您可以在创建或编辑卷时选择特定的卷分层策略。
    - 如果您禁用数据分层，则可以在后续聚合上启用它。

      "了解有关数据分层的更多信息" 。

14. 写入速度和 **WORM**：

    a. 如果需要，选择*正常*或*高*写入速度。

       "了解有关写入速度的更多信息" 。

    b. 如果需要，请激活一次写入、多次读取 (WORM) 存储。

       此选项仅适用于某些 VM 类型。要了解受支持的 VM 类型，请参阅"HA 对许可证支持的配置"。

       如果为Cloud Volumes ONTAP 9.7 及更低版本启用了数据分层，则无法启用 WORM。启用 WORM 和分层后，恢复或降级到Cloud Volumes ONTAP 9.8 的操作将被阻止。

    "了解有关 WORM 存储的更多信息" 。

    a. 如果您激活 WORM 存储，请选择保留期限。
15. 创建卷：输入新卷的详细信息或单击*跳过*。

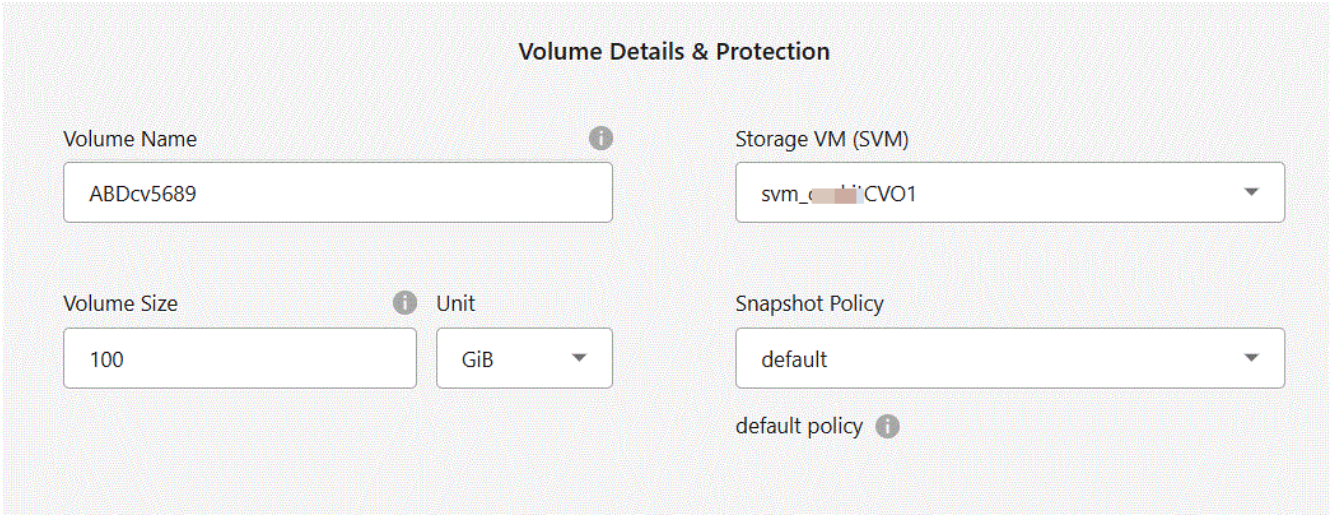
    "了解支持的客户端协议和版本" 。

    此页面中的某些字段是不言自明的。下表描述了您可能需要指导的字段：

字段	描述
大小	您可以输入的最大大小很大程度上取决于您是否启用精简配置，这使您能够创建比当前可用的物理存储更大的卷。
访问控制（仅适用于 NFS）	导出策略定义了子网中可以访问卷的客户端。默认情况下，控制台输入一个提供对子网中所有实例的访问权限的值。

字段	描述
权限和用户/组（仅适用于 CIFS）	这些字段使您能够控制用户和组对共享的访问级别（也称为访问控制列表或 ACL）。您可以指定本地或域 Windows 用户或组，或者 UNIX 用户或组。如果指定域 Windows 用户名，则必须使用域\用户名格式包含用户的域。
Snapshot 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 副本是时间点文件系统映像，它不会影响性能并且只需要最少的存储空间。您可以选择默认策略或无策略。对于瞬态数据，您可能选择无：例如，对于 Microsoft SQL Server，请选择 tempdb。
高级选项（仅适用于 NFS）	为卷选择一个 NFS 版本：NFSv3 或 NFSv4。
启动器组和 IQN（仅适用于 iSCSI）	iSCSI 存储目标称为 LUN（逻辑单元），并作为标准块设备呈现给主机。启动器组是 iSCSI 主机节点名称表，用于控制哪些启动器可以访问哪些 LUN。iSCSI 目标通过标准以太网网络适配器 (NIC)、带有软件启动器的 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。当您创建 iSCSI 卷时，控制台会自动为您创建一个 LUN。我们通过为每个卷创建一个 LUN 来简化操作，因此无需进行任何管理。创建卷后，"使用 IQN 从主机连接到 LUN" 。

下图显示了卷创建向导的第一页：



16. **CIFS** 设置：如果您选择了 CIFS 协议，请设置 CIFS 服务器。

字段	描述
DNS 主 IP 地址和辅助 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 服务器必须包含定位 CIFS 服务器将加入的域的 Active Directory LDAP 服务器和域控制器所需的服务位置记录 (SRV)。
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 域内指定组织单位 (OU) 的 Windows 帐户的名称和密码。
CIFS 服务器 NetBIOS 名称	AD 域中唯一的 CIFS 服务器名称。

字段	描述
组织单位	AD 域内与 CIFS 服务器关联的组织单位。默认值为 CN=Computers。要将 Azure AD 域服务配置为Cloud Volumes ONTAP 的AD 服务器，您应该在此字段中输入 **OU=AADDC Computers** 或 **OU=AADDC Users** 。https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou["Azure 文档：在 Azure AD 域服务托管域中创建组织单位 (OU)"^]
DNS 域	Cloud Volumes ONTAP存储虚拟机 (SVM) 的 DNS 域。大多数情况下，该域与 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。如果您需要使用不同的地址配置 NTP 服务器，那么您应该使用 API。请参阅 "NetApp Console自动化文档"了解详情。请注意，只有在创建 CIFS 服务器时才能配置 NTP 服务器。创建 CIFS 服务器后，它不可配置。

17. 使用情况配置文件、磁盘类型和分层策略：选择是否要启用存储效率功能并更改卷分层策略（如果需要）。

    更多信息，请参阅"了解卷使用情况"和"数据分层概述"。

18. 审核并批准：审核并确认您的选择。
    a. 查看有关配置的详细信息。
    b. 单击“更多信息”以查看有关支持和控制台将购买的 Azure 资源的详细信息。
    c. 选中*我明白…*复选框。
    d. 单击“开始”。

结果

控制台部署Cloud Volumes ONTAP系统。您可以在审核页面上跟踪进度。

如果您在部署Cloud Volumes ONTAP系统时遇到任何问题，请查看失败消息。您也可以选择系统并单击*重新创建环境*。

如需更多帮助，请访问 "NetApp Cloud Volumes ONTAP支持"。

部署过程完成后，请勿修改 Azure 门户中系统生成的Cloud Volumes ONTAP配置，尤其是系统标签。对这些配置所做的任何更改都可能导致意外行为或数据丢失。

完成后

- 如果您配置了 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共享并创建文件。
- 如果要将配额应用于卷，请使用ONTAP系统管理器或ONTAP CLI。

  配额使您能够限制或跟踪用户、组或 qtree 使用的磁盘空间和文件数量。

在 **Azure** 中启动**Cloud Volumes ONTAP HA** 对

如果您想在 Azure 中启动Cloud Volumes ONTAP HA 对，则需要在控制台中创建一个 HA 系统。

步骤

1. 从左侧导航菜单中，选择“存储”>“管理”。
2. 在*系统*页面上，单击*添加系统*并按照提示进行操作。
3. 如果出现提示， "创建控制台代理" 。
4. 详细信息和凭据：可选择更改 Azure 凭据和订阅，指定群集名称，根据需要添加标签，然后指定凭据。

   下表描述了您可能需要指导的字段：

字段	描述
系统名称	控制台使用系统名称来命名Cloud Volumes ONTAP系统和 Azure 虚拟机。如果您选择该选项，它还会使用该名称作为预定义安全组的前缀。
资源组标签	标签是 Azure 资源的元数据。当您在此字段中输入标签时，控制台会将它们添加到与Cloud Volumes ONTAP系统关联的资源组中。创建系统时，您可以从用户界面添加最多四个标签，然后可以在创建系统后添加更多标签。请注意，创建系统时，API 不会将您限制为四个标签。有关标签的信息，请参阅 "Microsoft Azure 文档：使用标签来组织您的 Azure 资源"。
用户名和密码	这些是Cloud Volumes ONTAP集群管理员帐户的凭据。您可以使用这些凭据通过ONTAP System Manager 或ONTAP CLI 连接到Cloud Volumes ONTAP 。保留默认的_admin_用户名或将其更改为自定义用户名。
编辑凭证	您可以选择不同的 Azure 凭据和不同的 Azure 订阅来与此Cloud Volumes ONTAP系统一起使用。您需要将 Azure 市场订阅与选定的 Azure 订阅关联，以便部署即用即付的Cloud Volumes ONTAP系统。 "了解如何添加凭证" 。

5. 服务：根据您是否要将各个服务与Cloud Volumes ONTAP一起使用来启用或禁用它们。
   - "了解有关NetApp Data Classification的更多信息"
   - "了解有关NetApp Backup and Recovery的更多信息"

   如果您想使用 WORM 和数据分层，则必须禁用备份和恢复并部署版本 9.8 或更高版本的Cloud Volumes ONTAP系统。

6. **HA**部署模型：
   a. 选择*单个可用区*或*多个可用区*。
      - 对于单个可用区域，请选择 Azure 区域、可用区域、VNet 和子网。

        从Cloud Volumes ONTAP 9.15.1 开始，您可以在 Azure 中的单个可用区域 (AZ) 中以 HA 模式部署虚拟机 (VM) 实例。您需要选择支持此部署的区域和地域。如果区域或地域不支持区域部署，则遵循之前LRS的非区域部署模式。要了解共享托管磁盘支持的配置，请参阅"具有共享托管磁盘的 HA 单可用区域配置"。

      - 对于多个可用区域，请选择区域、VNet、子网、节点 1 的区域以及节点 2 的区域。

   b. 选中*我已验证网络连接…*复选框。
7. 连接：选择一个新的或现有的资源组，然后选择是否使用预定义的安全组或使用您自己的安全组。

   下表描述了您可能需要指导的字段：

字段	描述
资源组	为Cloud Volumes ONTAP创建新的资源组或使用现有的资源组。最佳做法是为Cloud Volumes ONTAP使用新的专用资源组。虽然可以在现有的共享资源组中部署Cloud Volumes ONTAP ，但由于存在数据丢失的风险，因此不建议这样做。请参阅上面的警告以了解更多详细信息。 您必须为在 Azure 中部署的每个Cloud Volumes ONTAP HA 对使用专用资源组。一个资源组中仅支持一个 HA 对。如果您尝试在 Azure 资源组中部署第二个Cloud Volumes ONTAP HA 对，控制台会遇到连接问题。 如果您使用的 Azure 帐户具有 "所需权限"，如果部署失败或删除，控制台会从资源组中删除Cloud Volumes ONTAP资源。
生成的安全组	如果您让控制台为您生成安全组，则需要选择如何允许流量： • 如果选择*仅限选定的 VNet*，则入站流量的来源是选定 VNet 的子网范围和控制台代理所在的 VNet 的子网范围。这是推荐的选项。 • 如果选择“所有 **VNets**”，则入站流量的来源是 0.0.0.0/0 IP 范围。
使用现有的	如果您选择现有的安全组，则它必须满足Cloud Volumes ONTAP要求。"查看默认安全组" 。

8. 收费方式和 **NSS** 帐户：指定您想要在此系统中使用的收费选项，然后指定NetApp支持站点帐户。
   - "了解Cloud Volumes ONTAP的许可选项" 。
   - "了解如何设置许可" 。
9. 预配置包：选择其中一个包来快速部署Cloud Volumes ONTAP系统，或者单击*更改配置*。

   如果您选择其中一个套餐，您只需指定一个卷，然后审核并批准配置。
10. 许可：根据需要更改Cloud Volumes ONTAP版本并选择虚拟机类型。

    如果所选版本有较新的候选版本、通用版本或补丁版本，则控制台在创建系统时会将其更新到该版本。例如，如果您选择Cloud Volumes ONTAP 9.13.1 并且 9.13.1 P4 可用，则会发生更新。更新不会从一个版本发生到另一个版本 — 例如，从 9.13 到 9.14。
11. 从 **Azure** 市场订阅：如果控制台无法启用Cloud Volumes ONTAP的编程部署，请按照以下步骤操作。
12. 底层存储资源：选择初始聚合的设置：磁盘类型、每个磁盘的大小以及是否应启用数据分层到 Blob 存储。

    请注意以下事项：
    - 磁盘大小适用于初始聚合中的所有磁盘以及使用简单配置选项时控制台创建的任何其他聚合。您可以使用高级分配选项创建使用不同磁盘大小的聚合。

      有关选择磁盘大小的帮助，请参阅"在 Azure 中调整系统大小"。
    - 如果在 VNet 中禁用了对您的存储帐户的公共访问，则您无法在Cloud Volumes ONTAP系统中启用数据分层。有关信息，请参阅"安全组规则"。

- 您可以在创建或编辑卷时选择特定的卷分层策略。
- 如果您禁用数据分层，则可以在后续聚合上启用它。

  "了解有关数据分层的更多信息" 。

- 从Cloud Volumes ONTAP 9.15.0P1 开始，Azure 页面 blob 不再支持新的高可用性对部署。如果您当前在现有的高可用性对部署中使用 Azure 页 Blob，则可以迁移到 Edsv4 系列 VM 和 Edsv5 系列 VM 中较新的 VM 实例类型。

  "详细了解 Azure 中支持的配置" 。

13. 写入速度和 **WORM**：

    a. 如果需要，选择*正常*或*高*写入速度。

       "了解有关写入速度的更多信息" 。

    b. 如果需要，请激活一次写入、多次读取 (WORM) 存储。

       此选项仅适用于某些 VM 类型。要了解受支持的 VM 类型，请参阅"HA 对许可证支持的配置"。

       如果为Cloud Volumes ONTAP 9.7 及更低版本启用了数据分层，则无法启用 WORM。启用 WORM 和分层后，恢复或降级到Cloud Volumes ONTAP 9.8 的操作将被阻止。

    "了解有关 WORM 存储的更多信息" 。

    a. 如果您激活 WORM 存储，请选择保留期限。

14. 与存储和 **WORM** 的安全通信：选择是否启用与 Azure 存储帐户的 HTTPS 连接，并激活一次写入、多次读取 (WORM) 存储（如果需要）。

    HTTPS 连接从Cloud Volumes ONTAP 9.7 HA 对到 Azure 页面 blob 存储帐户。请注意，启用此选项可能会影响写入性能。创建系统后，您无法更改设置。

    "了解有关 WORM 存储的更多信息" 。

    如果启用了数据分层，则无法启用 WORM。

    "了解有关 WORM 存储的更多信息" 。

15. 创建卷：输入新卷的详细信息或单击*跳过*。

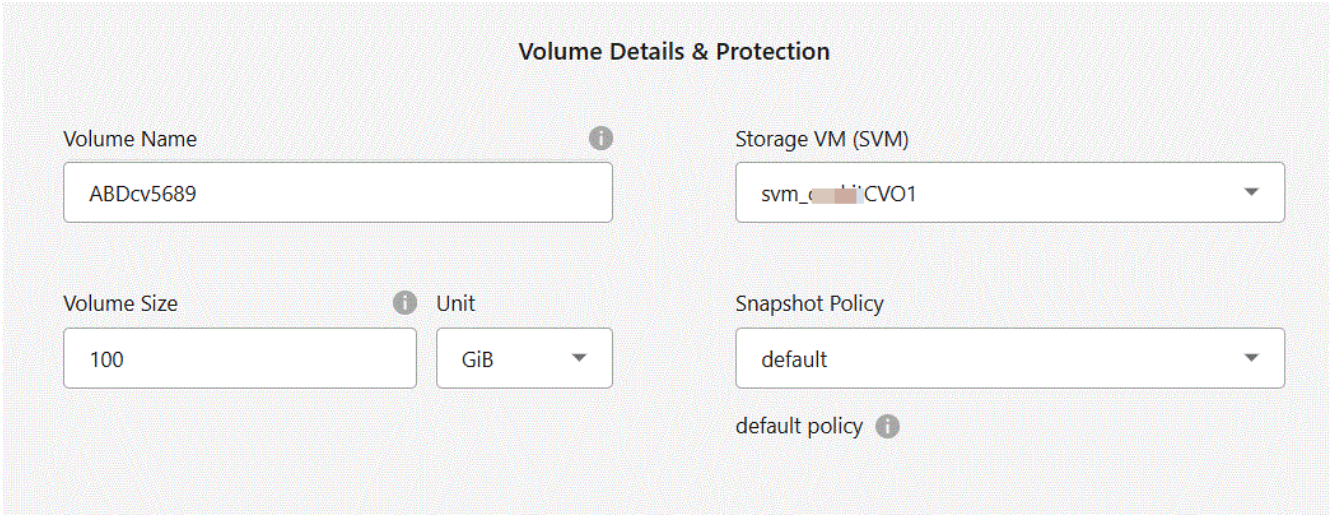
    "了解支持的客户端协议和版本" 。

    此页面中的某些字段是不言自明的。下表描述了您可能需要指导的字段：

字段	描述
大小	您可以输入的最大大小很大程度上取决于您是否启用精简配置，这使您能够创建比当前可用的物理存储更大的卷。
访问控制（仅适用于 NFS）	导出策略定义了子网中可以访问卷的客户端。默认情况下，控制台输入一个提供对子网中所有实例的访问权限的值。

字段	描述
权限和用户/组（仅适用于 CIFS）	这些字段使您能够控制用户和组对共享的访问级别（也称为访问控制列表或 ACL）。您可以指定本地或域 Windows 用户或组，或者 UNIX 用户或组。如果指定域 Windows 用户名，则必须使用域\用户名格式包含用户的域。
Snapshot 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 副本是时间点文件系统映像，它不会影响性能并且只需要最少的存储空间。您可以选择默认策略或无策略。对于瞬态数据，您可能选择无：例如，对于 Microsoft SQL Server，请选择 tempdb。
高级选项（仅适用于 NFS）	为卷选择一个 NFS 版本：NFSv3 或 NFSv4。
启动器组和 IQN（仅适用于 iSCSI）	iSCSI 存储目标称为 LUN（逻辑单元），并作为标准块设备呈现给主机。启动器组是 iSCSI 主机节点名称表，用于控制哪些启动器可以访问哪些 LUN。iSCSI 目标通过标准以太网网络适配器 (NIC)、带有软件启动器的 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。当您创建 iSCSI 卷时，控制台会自动为您创建一个 LUN。我们通过为每个卷创建一个 LUN 来简化操作，因此无需进行任何管理。创建卷后，"使用 IQN 从主机连接到 LUN" 。

下图显示了卷创建向导的第一页：



16. **CIFS** 设置：如果您选择了 CIFS 协议，请设置 CIFS 服务器。

字段	描述
DNS 主 IP 地址和辅助 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 服务器必须包含定位 CIFS 服务器将加入的域的 Active Directory LDAP 服务器和域控制器所需的服务位置记录 (SRV)。
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 域内指定组织单位 (OU) 的 Windows 帐户的名称和密码。
CIFS 服务器 NetBIOS 名称	AD 域中唯一的 CIFS 服务器名称。

字段	描述
组织单位	AD 域内与 CIFS 服务器关联的组织单位。默认值为 CN=Computers。要将 Azure AD 域服务配置为Cloud Volumes ONTAP 的AD 服务器，您应该在此字段中输入 **OU=AADDC Computers** 或 **OU=AADDC Users** 。https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou["Azure 文档：在 Azure AD 域服务托管域中创建组织单位 (OU)"^]
DNS 域	Cloud Volumes ONTAP存储虚拟机 (SVM) 的 DNS 域。大多数情况下，该域与 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。如果您需要使用不同的地址配置 NTP 服务器，那么您应该使用 API。请参阅 "NetApp Console自动化文档"了解详情。请注意，只有在创建 CIFS 服务器时才能配置 NTP 服务器。创建 CIFS 服务器后，它不可配置。

17. 使用情况配置文件、磁盘类型和分层策略：选择是否要启用存储效率功能并更改卷分层策略（如果需要）。

    更多信息，请参阅"选择卷使用情况配置文件"，"数据分层概述" ， 和 "KB：CVO 支持哪些内联存储效率功能？ "

18. 审核并批准：审核并确认您的选择。

    a. 查看有关配置的详细信息。

    b. 单击“更多信息”以查看有关支持和控制台将购买的 Azure 资源的详细信息。

    c. 选中*我明白…*复选框。

    d. 单击“开始”。

结果

控制台部署Cloud Volumes ONTAP系统。您可以在审核页面上跟踪进度。

如果您在部署Cloud Volumes ONTAP系统时遇到任何问题，请查看失败消息。您也可以选择系统并单击*重新创建环境*。

如需更多帮助，请访问 "NetApp Cloud Volumes ONTAP支持"。

完成后

- 如果您配置了 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共享并创建文件。
- 如果要将配额应用于卷，请使用ONTAP系统管理器或ONTAP CLI。

  配额使您能够限制或跟踪用户、组或 qtree 使用的磁盘空间和文件数量。

> 部署过程完成后，请勿修改 Azure 门户中系统生成的Cloud Volumes ONTAP配置，尤其是系统标签。对这些配置所做的任何更改都可能导致意外行为或数据丢失。

相关链接

*"在 Azure 中规划Cloud Volumes ONTAP配置" *"从 Azure 市场在 Azure 中部署Cloud Volumes ONTAP"

验证 **Azure** 平台映像

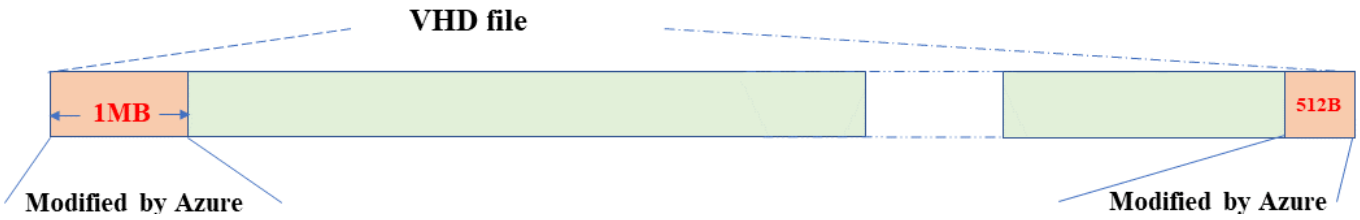
针对**Cloud Volumes ONTAP** 的**Azure** 市场映像验证

Azure 映像验证符合增强的NetApp安全要求。验证图像文件是一个简单的过程。但是，Azure 映像签名验证需要特别注意 Azure VHD 映像文件，因为它在 Azure 市场中被更改了。

Cloud Volumes ONTAP 9.15.0 及更高版本支持 Azure 映像验证。

Azure 对已发布 **VHD** 文件的更改

VHD 文件开头的 1 MB（1048576 字节）和结尾的 512 字节已被 Azure 修改。 NetApp对剩余的 VHD 文件进行签名。



在示例中，VHD 文件为 10GB。 NetApp签名的部分标记为绿色（10 GB - 1 MB - 512 字节）。

相关链接

- "页面错误博客：如何使用 OpenSSL 进行签名和验证"
- "使用 Azure Marketplace 映像为 Azure Stack Edge Pro GPU 创建 VM 映像 | Microsoft Learn"
- "使用 Azure CLI 将托管磁盘导出/复制到存储帐户 | Microsoft Learn"
- "Azure Cloud Shell 快速入门 - Bash | Microsoft Learn"
- "如何安装 Azure CLI | Microsoft Learn"
- "az 存储 blob 副本 | Microsoft Learn"
- "使用 Azure CLISign in— 登录和身份验证 | Microsoft Learn"

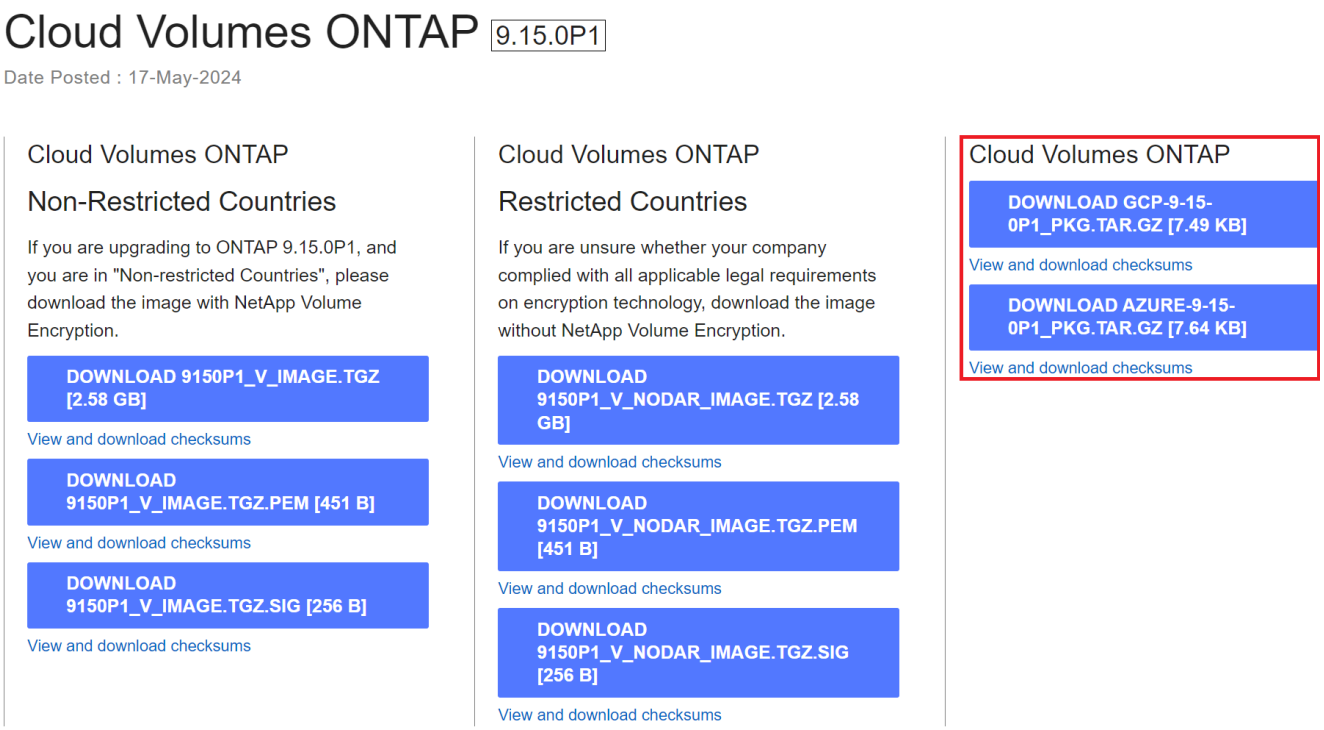
下载适用于**Cloud Volumes ONTAP** 的**Azure** 映像文件

您可以从 "NetApp 支持站点"。

tar.gz 文件包含图像签名验证所需的文件。除了 *tar.gz* 文件之外，您还应该下载图像的 *checksum* 文件。校验和文件包含 `md5`和 `sha256`*tar.gz* 文件的校验和。

步骤

1. 前往 "NetApp支持站点上的Cloud Volumes ONTAP产品页面"并从*下载*部分下载所需的软件版本。
2. 在Cloud Volumes ONTAP下载页面上，单击 Azure 映像的可下载文件并下载 *tar.gz* 文件。



3. 在 Linux 上，运行 `md5sum AZURE-<version>_PKG.TAR.GZ`。

   在 macOS 上，运行 `sha256sum AZURE-<version>_PKG.TAR.GZ`。

4. 验证 `md5sum`和 `sha256sum`值与下载的 Azure 映像中的值匹配。
5. 在 Linux 和 macOS 上，使用以下命令提取 *tar.gz* 文件 `tar -xzf`命令。

   解压后的 *tar.gz* 文件包含摘要（*.sig*）文件、公钥证书（*.pem*）文件和链证书（*.pem*）文件。

   提取 **tar.gz** 文件后的示例输出：

```
$ ls cert/ -l
-rw-r----- 1 netapp netapp  384 May  13 13:00 9.15.0P1_azure_digest.sig
-rw-r----- 1 netapp netapp 2365 May  13 13:00 Certificate-
9.15.0P1_azure.pem
-rw-r----- 1 netapp netapp 8537 May  13 13:00 Certificate-Chain-
9.15.0P1_azure.pem
-rw-r----- 1 netapp netapp 8537 May  13 13:00 version_readme
```

从 **Azure** 市场导出**Cloud Volumes ONTAP**的 **VHD** 映像

一旦 VHD 映像发布到 Azure 云，它就不再由NetApp管理。相反，已发布的图像被放置在 Azure 市场上。当映像在 Azure 市场上暂存和发布时，Azure 会修改 VHD 开头的 1 MB 和结尾的 512 字节。要验证VHD文件的签名，需要从Azure市场导出Azure修改后的VHD镜像。

开始之前

确保您的系统上安装了 Azure CLI，或者可以通过 Azure 门户使用 Azure Cloud Shell。有关如何安装 Azure CLI 的详细信息，请参阅 "Microsoft 文档：如何安装 Azure CLI"。

步骤

1. 使用 *version_readme* 文件的内容将系统上的Cloud Volumes ONTAP版本映射到 Azure 市场映像版本。Cloud Volumes ONTAP版本由 `buildname`Azure 市场镜像版本表示为 `version`在版本映射中。

   在以下示例中， Cloud Volumes ONTAP版本 `9.15.0P1`映射到 `Azure` 市场映像版本 `9150.01000024.05090105`。此 Azure 市场镜像版本稍后用于设置镜像 URN。

   ```
   [
    "buildname": "9.15.0P1",
       "publisher": "netapp",
        "version": "9150.01000024.05090105"

   ]
   ```

2. 确定要创建虚拟机的区域。区域名称用作 `locName`设置市场图像的 URN 时的变量。要列出可用区域，请运行以下命令：

   ```
   az account list-locations -o table
   ```

   在此表中，区域名称出现在 `Name`场地。

   ```
   $ az account list-locations -o table
   DisplayName               Name                 RegionalDisplayName
   ------------------------  -------------------
   -------------------------------------
   East US                   eastus               (US) East US
   East US 2                 eastus2              (US) East US 2
   South Central US          southcentralus       (US) South Central US
   ...
   ```

3. 查看下表中相应Cloud Volumes ONTAP版本和 VM 部署类型的 SKU 名称。 SKU 名称用作 `skuName`设置市场图像的 URN 时的变量。

   例如，所有采用Cloud Volumes ONTAP 9.15.0 的单节点部署都应使用 `ontap_cloud_byol`作为 SKU 名称。

* Cloud Volumes ONTAP版本*	通过虚拟机部署	**SKU** 名称
9.17.1 及更高版本	Azure 市场	ontap_cloud_direct_gen2
9.17.1 及更高版本	NetApp Console	ontap_cloud_gen2
9.16.1	Azure 市场	ontap_cloud_direct
9.16.1	控制台	ontap_cloud

9.15.1	控制台	ontap_cloud
9.15.0	控制台，单节点部署	ontap_cloud_byol
9.15.0	控制台、高可用性 (HA) 部署	ontap_cloud_byol_ha

4. 映射ONTAP版本和 Azure 市场映像后，使用 Azure Cloud Shell 或 Azure CLI 从 Azure 市场导出 VHD 文件。

使用 **Linux** 上的 **Azure Cloud Shell** 导出 **VHD** 文件

从 Azure Cloud Shell，将市场映像导出到 VHD 文件（例如，*9150.01000024.05090105.vhd*），然后将其下载到本地 Linux 系统。执行以下步骤从 Azure 市场获取 VHD 映像。

步骤

1. 设置市场图像的 URN 和其他参数。 URN 格式为 `<publisher>:<offer>:<sku>:<version>`。或者，您可以列出NetApp市场图像来确认正确的图像版本。

```
PS /home/user1> $urn="netapp:netapp-ontap-
cloud:ontap_cloud_byol:9150.01000024.05090105"
PS /home/user1> $locName="eastus2"
PS /home/user1> $pubName="netapp"
PS /home/user1> $offerName="netapp-ontap-cloud"
PS /home/user1> $skuName="ontap_cloud_byol"
PS /home/user1> Get-AzVMImage -Location $locName -PublisherName $pubName
-Offer $offerName -Sku $skuName |select version
...
141.20231128
9.141.20240131
9.150.20240213
9150.01000024.05090105
...
```

2. 从市场映像创建一个具有匹配映像版本的新托管磁盘：

```
PS /home/user1> $diskName = “9150.01000024.05090105-managed-disk"
PS /home/user1> $diskRG = “fnf1”
PS /home/user1> az disk create -g $diskRG -n $diskName --image-reference
$urn
PS /home/user1> $sas = az disk grant-access --duration-in-seconds 3600
--access-level Read --name $diskName --resource-group $diskRG
PS /home/user1> $diskAccessSAS = ($sas | ConvertFrom-Json)[0].accessSas
```

3. 将 VHD 文件从托管磁盘导出到 Azure 存储。创建具有适当访问级别的容器。在这个例子中，我们使用了一个名为 `vm-images`和 `Container`访问级别。从 Azure 门户获取存储帐户访问密钥：存储帐户 **> *examplesaname* >** 访问密钥 **> *key1* > *key* >** 显示 **> <copy>**

```
PS /home/user1> $storageAccountName = “examplesaname”
PS /home/user1> $containerName = “vm-images”
PS /home/user1> $storageAccountKey = "<replace with the above access
key>"
PS /home/user1> $destBlobName = “9150.01000024.05090105.vhd”
PS /home/user1> $destContext = New-AzureStorageContext
-StorageAccountName $storageAccountName -StorageAccountKey
$storageAccountKey
PS /home/user1> Start-AzureStorageBlobCopy -AbsoluteUri $diskAccessSAS
-DestContainer $containerName -DestContext $destContext -DestBlob
$destBlobName
PS /home/user1> Get-AzureStorageBlobCopyState –Container $containerName
–Context $destContext -Blob $destBlobName
```

4. 将生成的图像下载到您的 Linux 系统。使用 `wget`下载VHD文件的命令：

```
wget <URL of filename/Containers/vm-images/9150.01000024.05090105.vhd>
```

URL 遵循标准格式。为了实现自动化，您可以获取如下所示的 URL 字符串。或者，您可以使用 Azure CLI `az`命令来获取 URL。示例 URL：https://examplesaname.bluexpinfraprod.eastus2.data.azurecr.io/vm-images/9150.01000024.05090105.vhd[]

5. 清理托管磁盘

```
PS /home/user1> Revoke-AzDiskAccess -ResourceGroupName $diskRG -DiskName
$diskName
PS /home/user1> Remove-AzDisk -ResourceGroupName $diskRG -DiskName
$diskName
```

使用 **Linux** 上的 **Azure CLI** 导出 **VHD** 文件

使用本地 Linux 系统的 Azure CLI 将市场映像导出到 VHD 文件。

步骤

1. 登录到 Azure CLI 并列出市场图像：

```
% az login --use-device-code
```

2. 要登录，请使用网络浏览器打开页面 https://microsoft.com/devicelogin并输入验证码。

```
% az vm image list --all --publisher netapp --offer netapp-ontap-cloud
--sku ontap_cloud_byol
...
{
"architecture": "x64",
"offer": "netapp-ontap-cloud",
"publisher": "netapp",
"sku": "ontap_cloud_byol",
"urn": "netapp:netapp-ontap-
cloud:ontap_cloud_byol:9150.01000024.05090105",
"version": "9150.01000024.05090105"
},
...
```

3. 从具有匹配映像版本的市场映像创建新的托管磁盘。

```
% export urn="netapp:netapp-ontap-
cloud:ontap_cloud_byol:9150.01000024.05090105"
% export diskName="9150.01000024.05090105-managed-disk"
% export diskRG="new_rg_your_rg"
% az disk create -g $diskRG -n $diskName --image-reference $urn
% az disk grant-access --duration-in-seconds 3600 --access-level Read
--name $diskName --resource-group $diskRG
{
  "accessSas": "https://md-
xxxxxx.bluexpinfraprod.eastus2.data.azurecr.io/xxxxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxx&sigxxxxxxxxxxxxxxxxxxxxxxx"
}
% export diskAccessSAS="https://md-
xxxxxx.bluexpinfraprod.eastus2.data.azurecr.io/xxxxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xx-xx-xx&sigxxxxxxxxxxxxxxxxxxxxxxx"
```

为了使该过程自动化，需要从标准输出中提取 SAS。请参阅相应文档以获取指导。

4. 从托管磁盘导出 VHD 文件。

   a. 创建具有适当访问级别的容器。在此示例中，名为 `vm-images`和 `Container`使用访问级别。

   b. 从 Azure 门户获取存储帐户访问密钥：存储帐户 **> *examplesaname* >** 访问密钥 **> *key1* > *key* >** 显示 **> *<copy>***

      您还可以使用 `az`此步骤的命令。

```
% export storageAccountName="examplesaname"
% export containerName="vm-images"
% export storageAccountKey="xxxxxxxxxx"
% export destBlobName="9150.01000024.05090105.vhd"

% az storage blob copy start --source-uri $diskAccessSAS --destination
-container $containerName --account-name $storageAccountName --account
-key $storageAccountKey --destination-blob $destBlobName

{
  "client_request_id": "xxxx-xxxx-xxxx-xxxx-xxxx",
  "copy_id": "xxxx-xxxx-xxxx-xxxx-xxxx",
  "copy_status": "pending",
  "date": "2022-11-02T22:02:38+00:00",
  "etag": "\"0xXXXXXXXXXXXXXXXX\"",
  "last_modified": "2022-11-02T22:02:39+00:00",
  "request_id": "xxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx",
  "version": "2020-06-12",
  "version_id": null
}
```

5. 检查 blob 副本的状态。

```
% az storage blob show --name $destBlobName --container-name
$containerName --account-name $storageAccountName

....
    "copy": {
      "completionTime": null,
      "destinationSnapshot": null,
      "id": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxx",
      "incrementalCopy": null,
      "progress": "10737418752/10737418752",
      "source": "https://md-
xxxxxx.bluexpinfraprod.eastus2.data.azurecr.io/xxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx",
      "status": "success",
      "statusDescription": null
    },
....
```

6. 将生成的图像下载到您的 Linux 服务器。

```
wget <URL of file examplesaname/Containers/vm-
images/9150.01000024.05090105.vhd>
```

URL 遵循标准格式。为了实现自动化，您可以获取如下所示的 URL 字符串。或者，您可以使用 Azure CLI `az`命令来获取 URL。示例 URL：https://examplesaname.bluexpinfraprod.eastus2.data.azurecr.io/vm-images/9150.01000024.05090105.vhd[]

7. 清理托管磁盘

```
az disk revoke-access --name $diskName --resource-group $diskRG
az disk delete --name $diskName --resource-group $diskRG --yes
```

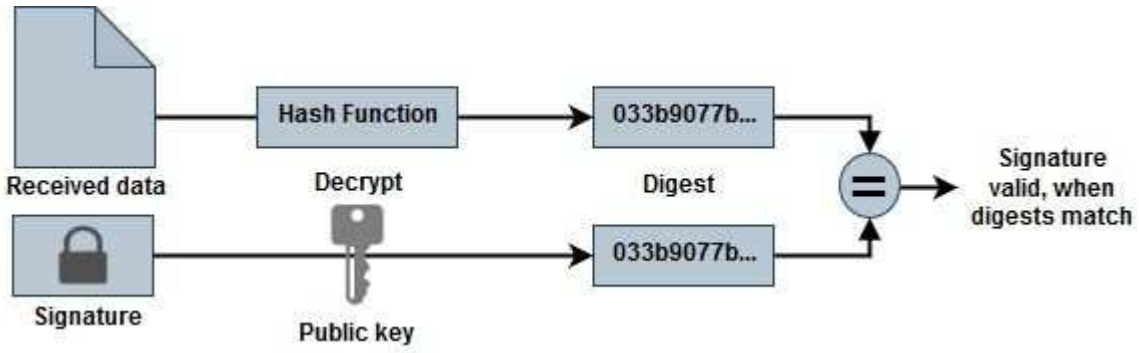
验证文件签名

针对**Cloud Volumes ONTAP** 的**Azure** 市场映像签名验证

Azure 映像验证过程通过剥离 VHD 文件的开头 1 MB 和结尾 512 字节，然后应用哈希函数来生成摘要文件。为了匹配签名程序，使用_sha256_进行散列。

文件签名验证工作流程摘要

以下是文件签名验证工作流程的概述。



- 从下载 Azure 映像 "NetApp 支持站点"并提取摘要（.sig）文件、公钥证书（.pem）文件和链证书（.pem）文件。请参阅"下载 Azure 映像摘要文件"了解更多信息。
- 信任链的验证。
- 从公钥证书（.pem）中提取公钥（.pub）。
- 使用提取的公钥解密摘要文件。
- 将结果与从图像文件中删除开头 1 MB 和结尾 512 字节后创建的临时文件的新生成的摘要进行比较。此步骤通过使用 OpenSSL 命令行工具执行。 OpenSSL CLI 工具会在文件匹配成功或失败时显示相应的消息。

```
openssl dgst -verify <public_key> -keyform <form> <hash_function>
-signature <digest_file> -binary <temporary_file>
```

在 Linux 上验证导出的 VHD 文件签名包括验证信任链、编辑文件和验证签名。

步骤

1. 从下载 Azure 映像文件 "NetApp 支持站点"并提取摘要（.sig）文件、公钥证书（.pem）文件和链证书（.pem）文件。

   参考 "下载 Azure 映像摘要文件"了解更多信息。

2. 验证信任链。

```
% openssl verify -CAfile Certificate-Chain-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem: OK
```

3. 删除 VHD 文件开头的 1 MB（1,048,576 字节）和结尾的 512 字节。使用时 `tail`， 这 `-c +K`选项从文件的第 `K` 个字节生成字节。因此，它将 `1048577` 传递给 `tail -c`。

```
% tail -c +1048577 ./9150.01000024.05090105.vhd > ./sign.tmp.tail
% head -c -512 ./sign.tmp.tail > sign.tmp
% rm ./sign.tmp.tail
```

4. 使用 OpenSSL 从证书中提取公钥，并使用签名文件和公钥验证剥离的文件（sign.tmp）。

   命令提示符根据验证显示指示成功或失败的消息。

```
% openssl x509 -pubkey -noout -in ./Certificate-9.15.0P1_azure.pem >
./Code-Sign-Cert-Public-key.pub

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./sign.tmp
Verification OK

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./another_file_from_nowhere.tmp
Verification Failure
```

5. 清理工作区。

```
% rm ./9150.01000024.05090105.vhd ./sign.tmp
% rm *.sig *.pub *.pem
```

在 Linux 上验证导出的 VHD 文件签名包括验证信任链、编辑文件和验证签名。

步骤

1. 从下载 Azure 映像文件 "NetApp 支持站点"并提取摘要（.sig）文件、公钥证书（.pem）文件和链证书（.pem）文件。

   参考 "下载 Azure 映像摘要文件"了解更多信息。

2. 验证信任链。

```
% openssl verify -CAfile Certificate-Chain-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem: OK
```

3. 删除 VHD 文件开头的 1MB（1,048,576 字节）和结尾的 512 字节。使用时 `tail`， 这 `-c +K`选项从文件的第 `K` 个字节生成字节。因此，它将 `1048577` 传递给 `tail -c`。请注意，在 macOS 上，tail 命令可能需要大约十分钟才能完成。

```
% tail -c +1048577 ./9150.01000024.05090105.vhd > ./sign.tmp.tail
% head -c -512 ./sign.tmp.tail > sign.tmp
% rm ./sign.tmp.tail
```

4. 使用 OpenSSL 从证书中提取公钥，并使用签名文件和公钥验证剥离的文件（sign.tmp）。命令提示符根据验证显示指示成功或失败的消息。

```
% openssl x509 -pubkey -noout -in ./Certificate-9.15.0P1_azure.pem >
./Code-Sign-Cert-Public-key.pub

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./sign.tmp
Verified OK

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./another_file_from_nowhere.tmp
Verification Failure
```

5. 清理工作区。

```
% rm ./9150.01000024.05090105.vhd ./sign.tmp
% rm *.sig *.pub *.pem
```

从 Azure 市场部署Cloud Volumes ONTAP

您可以使用 Azure 市场直接部署来快速轻松地部署Cloud Volumes ONTAP。从 Azure 市场，您只需单击几下即可快速部署Cloud Volumes ONTAP ，并在您的环境中探索其核心特性和功能。

有关该产品的更多信息，请参阅"了解NetApp Console和市场中的Cloud Volumes ONTAP产品"。

关于此任务

使用 Azure 市场直接部署部署的Cloud Volumes ONTAP系统具有这些属性。请注意，通过 Azure 市场部署的独立实例的功能在NetApp Console中被发现时会发生变化。

- 最新的Cloud Volumes ONTAP版本（9.16.1 或更高版本）。
- Cloud Volumes ONTAP的免费许可证，限制为 500 GiB 的配置容量。此许可证不包括NetApp支持，并且没有到期日期。
- 两个节点在单个可用区 (AZ) 中以高可用性 (HA) 模式配置，并配置默认序列号。存储虚拟机（存储 VM）部署在"灵活的编排模式"。
- 默认创建的实例的聚合。
- 预置容量为 500 GiB 的高级 SSD v2 托管磁盘，以及根磁盘和数据磁盘。
- 部署了一个数据存储虚拟机，具有 NFS、CIFS、iSCSI 和 NVMe/TCP 数据服务。您不能添加任何额外的数据存储虚拟机。
- 为 NFS、CIFS (SMB)、iSCSI、自主勒索软件防护 (ARP)、 SnapLock和SnapMirror安装许可证。
- "ONTAP温度敏感存储效率 (TSSE)"、卷加密和外部密钥管理默认启用。
- 不支持以下功能：
  - FabricPool分层
  - 更改存储虚拟机类型
  - 快速写入模式

开始之前

- 确保您拥有有效的 Azure 市场订阅。
- 确保您满足"单个可用区内的高可用性部署"在 Azure 中。请参阅"为Cloud Volumes ONTAP设置 Azure 网络"。
- 您需要分配以下 Azure 角色之一才能部署Cloud Volumes ONTAP：
  - 这 `contributor`具有默认权限的角色。欲了解更多信息，请参阅 "Microsoft Azure 文档：Azure 内置角色"。
  - 具有以下权限的自定义 RBAC 角色。欲了解更多信息，请参阅 "Azure 文档：Azure 自定义角色"。

“权限”：[{“操作”：[“Microsoft.AAD/register/action”
，“Microsoft.Resources/subscriptions/resourceGroups/write”
，“Microsoft.Network/loadBalancers/write”，“Microsoft.ClassicCompute/virtualMachines/write”
，“Microsoft.Compute/capacityReservationGroups/deploy/action”
，“Microsoft.ClassicCompute/virtualMachines/networkInterfaces/associatedNetworkSecurityGroups/write”，“Microsoft.Network/networkInterfaces/write”
，“Microsoft.Compute/virtualMachines/write”
，“Microsoft.Compute/virtualMachines/extensions/write”
，“Microsoft.Resources/deployments/validate/action”
，“Microsoft.Resources/subscriptions/resourceGroups/read”
，“Microsoft.Network/virtualNetworks/write”，“Microsoft.Network/virtualNetworks/read”
，“Microsoft.Network/networkSecurityGroups/write”，
“Microsoft.Network/networkSecurityGroups/read”、“Microsoft.Compute/disks/write”、“Microsoft.Compute/virtualMachineScaleSets/write”、“Microsoft.Resources/deployments/write”、“Microsoft.Network/virtualNetworks/subnets/read”、“Microsoft.Network/virtualNetworks/subnets/write”]、“notActions”：[]、“dataActions”：[]、“notDataActions”：[] }]

如果您已将资源提供程序“Microsoft.storage”注册到您的订阅，那么您不需要 `Microsoft.AAD/register/action`允许。欲了解更多信息，请参阅 "Azure 文档：Azure 存储权限"。

步骤

1. 从 Azure 市场网站搜索NetApp产品。
2. 选择* NetApp Cloud Volumes ONTAP direct*。
3. 单击“创建”以启动部署向导。
4. 选择一个计划。 *计划*列表通常显示Cloud Volumes ONTAP的最新版本。
5. 在“基本信息”选项卡中，提供以下详细信息：
   - 订阅：选择订阅。部署将与订阅号挂钩。
   - 资源组：使用现有资源组或创建一个新的资源组。资源组有助于在Cloud Volumes ONTAP系统的单个组内分配所有资源，例如磁盘和存储虚拟机。
   - 区域：选择支持在单个 AZ 中部署 Azure HA 的区域。您只会看到列表中可用的区域。
   - 大小：为支持的 Premium SSD v2 托管磁盘选择存储 VM 大小。
   - 区域：为您选择的地区选择一个区域。
   - 管理员密码：设置密码。部署完成后，您可以使用此管理员密码登录系统。
   - 确认密码：再次输入相同的密码进行确认。
     - 在“网络”选项卡中，添加虚拟网络和子网，或从列表中选择它们。

       为了遵守 Microsoft Azure 限制，您应该在设置新的虚拟网络时创建一个新的子网。同样，如果您选择现有网络，则应该选择现有子网。

     - 要选择预定义的网络安全组，请选择“是”。选择“否”以分配具有必要流量规则的预定义 Azure 网络安全组。有关详细信息，请参阅"Azure 的安全组规则" 。

- 在“高级”选项卡中确认是否已设置此部署所需的两个 Azure 功能。参考"为Cloud Volumes ONTAP单可用区部署启用 Azure 功能"和"在 Azure 中为Cloud Volumes ONTAP启用高可用性模式"。
- 您可以在“标签”选项卡中为资源或资源组定义名称和值对。
- 在“**Review + create**”选项卡中，查看详细信息并开始部署。

完成后

选择通知图标即可查看部署进度。部署Cloud Volumes ONTAP后，您可以查看列出的可供操作的存储虚拟机。

一旦可以访问，请使用ONTAP系统管理器或ONTAP CLI 通过您设置的管理员凭据登录到存储虚拟机。此后，您可以创建卷、LUN 或共享并开始利用Cloud Volumes ONTAP的存储功能。

解决部署问题

直接通过 Azure 市场部署的Cloud Volumes ONTAP系统不包括NetApp的支持。如果部署过程中出现任何问题，您可以独立排除故障并解决。

步骤

1. 在 Azure 市场网站上，转到 启动诊断 **>** 串行日志。
2. 下载并调查串行日志。
3. 请参阅产品文档和知识库 (KB) 文章以进行故障排除。
   - "Azure 市场文档"
   - "NetApp文档"
   - "NetApp知识库文章"

在控制台中发现已部署的系统

您可以发现使用 Azure 市场直接部署部署的Cloud Volumes ONTAP系统，并在控制台中的 系统 页面上对其进行管理。控制台代理发现系统、添加系统并应用必要的许可证，并为这些系统解锁控制台的全部功能。保留具有 PSSD v2 托管磁盘的单个 AZ 中的原始 HA 配置，并且系统注册到与原始部署相同的 Azure 订阅和资源组。

关于此任务

在发现使用 Azure 市场直接部署部署的Cloud Volumes ONTAP系统时，控制台代理将执行以下任务：

- 将发现系统的免费许可证替换为常规的基于容量的许可证"免费增值许可证"。
- 保留已部署系统的现有功能，并添加控制台的附加功能，例如数据保护、数据管理和安全功能。
- 使用 NFS、CIFS (SMB)、iSCSI、ARP、 SnapLock和SnapMirror的新ONTAP许可证替换节点上已安装的许可证。
- 将通用节点序列号转换为唯一序列号。
- 根据需要为资源分配新的系统标签。
- 将实例的动态 IP 地址转换为静态 IP 地址。
- 启用以下功能"FabricPool分层"，"AutoSupport" ， 和"一次写入多次读取"（WORM）存储。您可以在需要时从控制台激活这些功能。
- 将实例注册到用于发现它们的 NSS 帐户。

- 启用容量管理功能"自动和手动模式"对于已发现的系统。

开始之前

确保在 Azure 市场上部署已完成。仅当部署完成且可供发现时，控制台代理才能发现系统。

步骤

在控制台中，您可以按照标准程序来发现现有系统。请参阅"将现有的Cloud Volumes ONTAP系统添加到控制台"。

> 在发现过程中，您可能会看到失败消息，但您可以忽略它们，直到发现过程完成。在发现期间，请勿修改 Azure 市场门户中系统生成的Cloud Volumes ONTAP配置，尤其是系统标签。对这些配置所做的任何更改都可能导致意外的系统行为。

完成后

发现完成后，您可以在控制台中的“系统”页面上查看列出的系统。您可以执行各种管理任务，例如"扩大总量"，"添加卷"，"配置额外的存储虚拟机"， 和"更改实例类型"。

相关链接

有关创建存储的更多信息，请参阅ONTAP文档：

- "为 NFS 创建卷"
- "为 iSCSI 创建 LUN"
- "为 CIFS 创建共享"

开始使用 Google Cloud

Google Cloud 中的Cloud Volumes ONTAP快速入门

只需几个步骤即可在 Google Cloud 中开始使用Cloud Volumes ONTAP 。

1 创建控制台代理

如果你没有 "控制台代理"但是，你需要创建一个。 "了解如何在 Google Cloud 中创建控制台代理"

请注意，如果您想在没有互联网访问的子网中部署Cloud Volumes ONTAP ，则需要手动安装控制台代理并访问在该控制台代理上运行的NetApp Console。 "了解如何在没有互联网访问的地方手动安装控制台代理"

2 规划您的配置

控制台提供符合您的工作负载要求的预配置包，或者您可以创建自己的配置。如果您选择自己的配置，您应该了解可用的选项。

"了解有关规划配置的更多信息" 。

3 设置网络

1. 确保您的 VPC 和子网将支持控制台代理和Cloud Volumes ONTAP之间的连接。
2. 如果您计划启用数据分层， "为私有 Google 访问配置Cloud Volumes ONTAP子网" 。
3. 如果您正在部署 HA 对，请确保您有四个 VPC，每个 VPC 都有自己的子网。
4. 如果您使用共享 VPC，请向控制台代理服务帐户提供_计算网络用户_角色。
5. 为NetApp AutoSupport启用从目标 VPC 的出站互联网访问。

   如果您在没有互联网访问的位置部署Cloud Volumes ONTAP，则不需要执行此步骤。

"了解有关网络要求的更多信息" 。


设置服务帐户

Cloud Volumes ONTAP需要 Google Cloud 服务帐户来实现两个目的。第一个是当你启用"数据分层"将冷数据分层到 Google Cloud 中的低成本对象存储。第二个是当你启用 "NetApp Backup and Recovery"将卷备份到低成本的对象存储。

您可以设置一个服务帐户并将其用于两种用途。服务帐户必须具有*存储管理员*角色。

"阅读分步说明" 。


启用 **Google Cloud API**

"在项目中启用 Google Cloud API"。 "这些 API"，您可能已经在创建 Console 代理时启用了这些功能，这些功能是在 Google Cloud 中部署 Cloud Volumes ONTAP 所必需的。


使用控制台启动**Cloud Volumes ONTAP**

单击“添加系统”，选择您想要部署的系统类型，然后完成向导中的步骤。"阅读分步说明" 。

相关链接

- "创建控制台代理"
- "在 Linux 主机上安装控制台代理软件"
- "控制台代理的 Google Cloud 权限"

在 **Google Cloud** 中规划您的**Cloud Volumes ONTAP**配置

在 Google Cloud 中部署Cloud Volumes ONTAP时，您可以选择符合您的工作负载要求的预配置系统，也可以创建自己的配置。如果您选择自己的配置，您应该了解可用的选项。

选择**Cloud Volumes ONTAP**许可证

Cloud Volumes ONTAP有多种许可选项。每个选项都可以让您选择符合您需求的消费模式。

- "了解Cloud Volumes ONTAP的许可选项"

- "了解如何设置许可"

选择支持的区域

大多数 Google Cloud 区域都支持Cloud Volumes ONTAP 。 "查看支持区域的完整列表" 。

选择支持的机器类型

Cloud Volumes ONTAP支持多种机器类型，具体取决于您选择的许可证类型。

"Google Cloud 中 Cloud Volumes ONTAP 支持的配置"

了解存储限制

Cloud Volumes ONTAP系统的原始容量限制与许可证相关。额外的限制会影响聚合和卷的大小。在规划配置时您应该注意这些限制。

"Google Cloud 中 Cloud Volumes ONTAP 的存储限制"

在 **Google Cloud** 中调整系统大小

调整Cloud Volumes ONTAP系统的大小可以帮助您满足性能和容量要求。在选择机器类型、磁盘类型和磁盘大小时，您应该注意几个关键点：

机器类型

请查看支持的机器类型。 "Cloud Volumes ONTAP发行说明"然后查看谷歌提供的关于每种受支持机器类型的详细信息。将您的工作负载要求与机器类型的 vCPU 和内存数量相匹配。请注意，每个 CPU 核心都会提高网络性能。

请参阅以下内容以了解更多详细信息：

- "Google Cloud 文档：N1 标准机器类型"
- "Google Cloud 文档：性能"

磁盘类型

为Cloud Volumes ONTAP创建卷时，您需要选择Cloud Volumes ONTAP用于磁盘的底层云存储。磁盘类型可以是以下任意一种：

- 区域 *SSD* 持久磁盘：SSD 持久磁盘最适合需要高随机 IOPS 率的工作负载。
- 区域平衡持久磁盘：这些 SSD 通过提供每 GB 较低的 IOPS 来平衡性能和成本。
- 区域标准持久磁盘：标准持久磁盘经济实惠，可以处理顺序读/写操作。

欲了解更多详情，请参阅 "Google Cloud 文档：区域持久磁盘（标准和 SSD）"。

磁盘大小

部署Cloud Volumes ONTAP系统时，您需要选择初始磁盘大小。之后，您可以让NetApp Console为您管理系统的容量，但如果您想自己构建聚合，请注意以下事项：

- 聚合中的所有磁盘必须具有相同的大小。

- 确定所需的空间，同时考虑性能。
- 持久磁盘的性能会随着磁盘大小和系统可用的 vCPU 数量自动扩展。

  请参阅以下内容以了解更多详细信息：

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

查看默认系统磁盘

除了用户数据的存储之外，控制台还购买了Cloud Volumes ONTAP系统数据（启动数据、根数据、核心数据和NVRAM）的云存储。出于规划目的，在部署Cloud Volumes ONTAP之前查看这些详细信息可能会有所帮助。

- "查看 Google Cloud 中Cloud Volumes ONTAP系统数据的默认磁盘" 。
- "Google Cloud 文档：云配额概述"

  Google Cloud Compute Engine 对资源使用实施配额，因此您应确保在部署Cloud Volumes ONTAP之前尚未达到限制。

控制台代理还需要系统磁盘。 "查看控制台代理默认配置的详细信息" 。

收集网络信息

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

单节点系统的网络信息

Google Cloud 信息	你的价值
地区	
分区	
VPC 网络	
子网	
防火墙策略（如果使用您自己的）	

多个区域中 **HA** 对的网络信息

Google Cloud 信息	你的价值
地区	
节点 1 的区域	
节点 2 的区域	
调解员区域	
VPC-0 和子网	

Google Cloud 信息	你的价值
VPC-1 和子网	
VPC-2 和子网	
VPC-3 和子网	
防火墙策略（如果使用您自己的）	

单个区域中 **HA** 对的网络信息

Google Cloud 信息	你的价值
地区	
分区	
VPC-0 和子网	
VPC-1 和子网	
VPC-2 和子网	
VPC-3 和子网	
防火墙策略（如果使用您自己的）	

选择写入速度

控制台可让您选择Cloud Volumes ONTAP的写入速度设置，但 Google Cloud 中的高可用性 (HA) 对除外。在选择写入速度之前，您应该了解正常设置和高设置之间的差异以及使用高写入速度时的风险和建议。"了解有关写入速度的更多信息" 。

选择卷使用情况配置文件

ONTAP包含多种存储效率功能，可以减少您所需的总存储量。在控制台中创建卷时，您可以选择启用这些功能的配置文件或禁用这些功能的配置文件。您应该了解有关这些功能的更多信息，以帮助您决定使用哪个配置文件。

NetApp存储效率功能具有以下优势：

精简配置

向主机或用户提供比物理存储池中实际拥有的更多的逻辑存储。不是预先分配存储空间，而是在写入数据时动态地将存储空间分配给每个卷。

重复数据删除

通过定位相同的数据块并将其替换为对单个共享块的引用来提高效率。该技术通过消除驻留在同一卷中的冗余数据块来减少存储容量要求。

数据压缩

通过压缩主存储、辅助存储和归档存储卷内的数据来减少存储数据所需的物理容量。

为Cloud Volumes ONTAP设置 Google Cloud 网络

NetApp Console负责设置Cloud Volumes ONTAP的网络组件，例如 IP 地址、网络掩码和路由。您需要确保可以访问出站互联网、有足够的私有 IP 地址、有正确的连接等等。

如果你想部署 HA 对，你应该"了解 HA 对在 Google Cloud 中的工作原理"。

Cloud Volumes ONTAP的要求

Google Cloud 必须满足以下要求。

特定于单节点系统的要求

如果要部署单节点系统，请确保网络满足以下要求。

一个 VPC

单节点系统需要一个虚拟私有云 (VPC)。

私有 IP 地址

对于 Google Cloud 中的单节点系统，Console 将私有 IP 地址分配给以下内容：

- 节点
- 集群
- Storage VM
- 数据 NAS LIF
- 数据 iSCSI LIF

如果您使用 API 部署Cloud Volumes ONTAP并指定以下标志，则可以跳过创建存储虚拟机 (SVM) 管理 LIF：

```
skipSvmManagementLif: true
```

LIF 是与物理端口关联的 IP 地址。 SnapCenter等管理工具需要存储虚拟机 (SVM) 管理 LIF。

HA 对的特定要求

如果您要部署 HA 对，请确保您的网络满足以下要求。

一个或多个区域

您可以通过在多个区域或单个区域中部署 HA 配置来确保数据的高可用性。创建 HA 对时，控制台会提示您选择多个区域或单个区域。

- 多区域（推荐）

  跨三个区域部署 HA 配置可确保当一个区域内发生故障时数据仍然可用。请注意，与使用单个区域相比，写入性能略低，但差别很小。

- 单区

  在单个区域中部署时， Cloud Volumes ONTAP HA 配置使用分散放置策略。此策略可确保 HA 配置免受区域内单点故障的影响，而无需使用单独的区域来实现故障隔离。

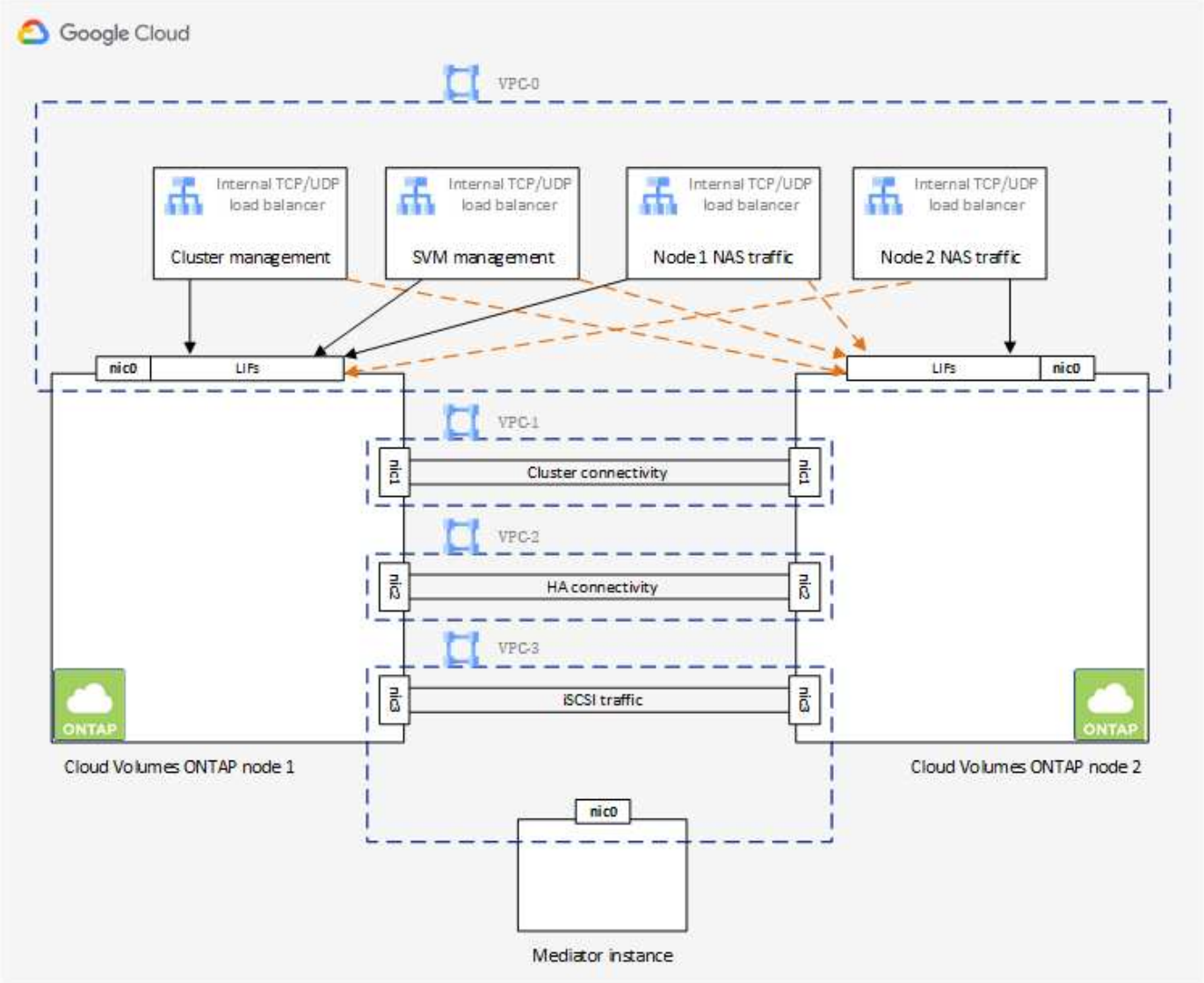
  这种部署模型确实降低了您的成本，因为区域之间没有数据流出费用。

四个虚拟私有云

HA 配置需要四个虚拟私有云 (VPC)。需要四个 VPC，因为 Google Cloud 要求每个网络接口位于单独的 VPC 网络中。

创建 HA 对时，控制台会提示您选择四个 VPC：

- VPC-0 用于数据和节点的入站连接
- VPC-1、VPC-2 和 VPC-3 用于节点和 HA 中介之间的内部通信



子网

每个 VPC 都需要一个私有子网。

如果将控制台代理放置在 VPC-0 中，则需要在子网上启用私有 Google 访问权限以访问 API 并启用数据分层。

这些 VPC 中的子网必须具有不同的 CIDR 范围。它们不能有重叠的 CIDR 范围。

私有 **IP** 地址

控制台会自动为 Google Cloud 中的Cloud Volumes ONTAP分配所需数量的私有 IP 地址。您需要确保您的网络有足够的可用私有地址。

为 Cloud Volumes ONTAP 分配的 LIF 数量取决于您是部署单节点系统还是 HA 对。LIF 是与物理端口关联的 IP 地址。像 SnapCenter 这样的管理工具需要 SVM 管理 LIF。

- 单节点 Console 为单节点系统分配 4 个 IP 地址：
  - 节点管理 LIF
  - 集群管理 LIF
  - iSCSI 数据 LIF

    iSCSI LIF 通过 iSCSI 协议提供客户端访问，并被系统用于其他重要的网络工作流程。这些 LIF 是必需的，不应删除。

  - NAS LIF

    如果您使用 API 部署Cloud Volumes ONTAP并指定以下标志，则可以跳过创建存储虚拟机 (SVM) 管理 LIF：

```
skipSvmManagementLif: true
```

- **HA** 对 控制台为 HA 对分配 12-13 个 IP 地址：
  - 2 个节点管理 LIF (e0a)
  - 1 集群管理 LIF (e0a)
  - 2 个 iSCSI LIF (e0a)

    iSCSI LIF 通过 iSCSI 协议提供客户端访问，并被系统用于其他重要的网络工作流程。这些 LIF 是必需的，不应删除。

  - 1 或 2 个 NAS LIF (e0a)
  - 2 个集群 LIF (e0b)
  - 2 个 HA 互连 IP 地址 (e0c)
  - 2 个 RSM iSCSI IP 地址（e0d）

    如果您使用 API 部署Cloud Volumes ONTAP并指定以下标志，则可以跳过创建存储虚拟机 (SVM) 管理 LIF：

```
skipSvmManagementLif: true
```

内部负载均衡器

控制台创建四个 Google Cloud 内部负载均衡器（TCP/UDP），用于管理传入Cloud Volumes ONTAP HA 对的流量。您无需进行任何设置。我们将其列为一项要求只是为了告知您网络流量并减轻任何安全问题。

一个负载均衡器用于集群管理，一个用于存储虚拟机 (SVM) 管理，一个用于到节点 1 的 NAS 流量，最后一个用于到节点 2 的 NAS 流量。

每个负载均衡器的设置如下：

- 一个共享的私有 IP 地址
- 一次全球健康检查

  默认情况下，健康检查使用的端口为63001、63002、63003。

- 一个区域 TCP 后端服务
- 一个区域 UDP 后端服务
- 一条 TCP 转发规则
- 一条 UDP 转发规则
- 全局访问已禁用

  尽管默认情况下禁用全局访问，但支持在部署后启用它。我们禁用它是因为跨区域流量会有明显更高的延迟。我们希望确保您不会因为意外的跨区域坐骑而产生负面体验。启用此选项是为了满足您的业务需求。

共享 **VPC**

Google Cloud 共享 VPC 和独立 VPC 均支持Cloud Volumes ONTAP和控制台代理。

对于单节点系统，VPC 可以是共享 VPC 或独立 VPC。

对于 HA 对，需要四个 VPC。每个 VPC 可以是共享的，也可以是独立的。例如，VPC-0 可以是共享 VPC，而 VPC-1、VPC-2 和 VPC-3 可以是独立 VPC。

共享 VPC 使您能够跨多个项目配置和集中管理虚拟网络。您可以在_主机项目_中设置共享 VPC 网络，并在_服务项目_中部署控制台代理和Cloud Volumes ONTAP虚拟机实例。

"Google Cloud 文档：共享 VPC 概览" 。

"查看控制台代理部署中涵盖的所需共享 VPC 权限"

VPC 中的数据包镜像

"数据包镜像"必须在部署Cloud Volumes ONTAP的 Google Cloud 子网中禁用。

出站互联网访问

Cloud Volumes ONTAP系统需要出站互联网访问才能访问外部端点以实现各种功能。如果这些端点在具有严格

安全要求的环境中被阻止， Cloud Volumes ONTAP将无法正常运行。

控制台代理还联系多个端点以进行日常操作。有关端点的信息，请参阅 "查看从控制台代理联系的端点"和 "准备使用控制台的网络"。

Cloud Volumes ONTAP端点

Cloud Volumes ONTAP使用这些端点与各种服务进行通信。

端点	适用于	目的	部署模式	端点不可用时的影响
\ https://netapp-cloud-account.auth0.com	身份验证	用于控制台中的身份验证。	标准和限制模式。	用户身份验证失败，以下服务仍然不可用： • Cloud Volumes ONTAP服务 • ONTAP 服务 • 协议和代理服务
\ https://api.bluexp.netapp.com/tenancy	租户	用于从控制台检索Cloud Volumes ONTAP资源以授权资源和用户。	标准和限制模式。	Cloud Volumes ONTAP资源和用户未获得授权。
\ https://mysupport.netapp.com/aods/asupmessage \ https://mysupport.netapp.com/asupprod/post/1.0/postAsup	AutoSupport	用于将AutoSupport遥测数据发送给NetApp支持。	标准和限制模式。	AutoSupport信息仍未送达。

端点	适用于	目的	部署模式	端点不可用时的影响
https://cloudbuild.googleapis.com/v1 （仅适用于私有模式部署） https://cloudkms.googleapis.com/v1 https://cloudresourcemanager.googleapis.com/v1/projects https://compute.googleapis.com/compute/v1 https://www.googleapis.com/compute/beta https://www.googleapis.com/compute/v1/projects/ https://www.googleapis.com/deploymentmanager/v2/projects https://www.googleapis.com/storage/v1 https://www.googleapis.com/upload/storage/v1 https://config.googleapis.com/v1 https://iam.googleapis.com/v1 https://storage.googleapis.com/storage/v1	Google Cloud（商业用途）。	与 Google Cloud 服务通信。	标准、受限和私人模式。	Cloud Volumes ONTAP无法与 Google Cloud 服务通信以对 Google Cloud 中的控制台执行特定操作。

与其他网络中的**ONTAP**系统的连接

要在 Google Cloud 中的Cloud Volumes ONTAP系统和其他网络中的ONTAP系统之间复制数据，您必须在 VPC 和其他网络（例如您的公司网络）之间建立 VPN 连接。

"Google Cloud 文档：Cloud VPN 概览" 。

防火墙规则

控制台创建 Google Cloud 防火墙规则，其中包括Cloud Volumes ONTAP成功运行所需的入站和出站规则。您可能希望参考端口以进行测试，或者您更喜欢使用自己的防火墙规则。

Cloud Volumes ONTAP的防火墙规则需要入站和出站规则。如果您正在部署 HA 配置，这些是 VPC-0 中Cloud Volumes ONTAP的防火墙规则。

请注意，HA 配置需要两组防火墙规则：

- 针对 VPC-0 中的 HA 组件的一组规则。这些规则允许对Cloud Volumes ONTAP进行数据访问。

- 针对 VPC-1、VPC-2 和 VPC-3 中的 HA 组件的另一组规则。这些规则对于 HA 组件之间的入站和出站通信开放。了解更多 。

正在寻找有关控制台代理的信息？ "查看控制台代理的防火墙规则"

入站规则

添加Cloud Volumes ONTAP系统时，您可以在部署期间选择预定义防火墙策略的源过滤器：

- 仅限选定的 **VPC**：入站流量的源过滤器是Cloud Volumes ONTAP系统的 VPC 子网范围和控制台代理所在的 VPC 子网范围。这是推荐的选项。
- 所有 **VPC**：入站流量的源过滤器是 0.0.0.0/0 IP 范围。

如果您使用自己的防火墙策略，请确保添加所有需要与Cloud Volumes ONTAP通信的网络，同时还要确保添加两个地址范围以允许内部 Google 负载均衡器正常运行。这些地址是 130.211.0.0/22 和 35.191.0.0/16。欲了解更多信息，请参阅 "Google Cloud 文档：负载均衡器防火墙规则"。

协议	端口	目的
所有 ICMP	全部	对实例执行 ping 操作
HTTP	80	使用集群管理 LIF 的 IP 地址通过 HTTP 访问ONTAP System Manager Web 控制台
HTTPS	443	使用集群管理 LIF 的 IP 地址与控制台代理建立连接并通过 HTTPS 访问ONTAP System Manager Web 控制台
SSH	22	通过 SSH 访问集群管理 LIF 或节点管理 LIF 的 IP 地址
TCP	111	NFS 的远程过程调用
TCP	139	CIFS 的 NetBIOS 服务会话
TCP	161-162	简单网络管理协议
TCP	445	使用 NetBIOS 框架的 TCP 上的 Microsoft SMB/CIFS
TCP	635	NFS 挂载
TCP	749	Kerberos
TCP	2049	NFS 服务器守护进程
TCP	3260	通过 iSCSI 数据 LIF 进行 iSCSI 访问
TCP	4045	NFS 锁守护进程
TCP	4046	NFS 网络状态监视器
TCP	10000	使用 NDMP 备份
TCP	11104	SnapMirror集群间通信会话的管理
TCP	11105	使用集群间 LIF 进行SnapMirror数据传输
TCP	63001-63050	负载平衡探测端口以确定哪个节点是健康的（仅 HA 对需要）
UDP	111	NFS 的远程过程调用

协议	端口	目的
UDP	161-162	简单网络管理协议
UDP	635	NFS 挂载
UDP	2049	NFS 服务器守护进程
UDP	4045	NFS 锁守护进程
UDP	4046	NFS 网络状态监视器
UDP	4049	NFS rquotad 协议

出站规则

Cloud Volumes ONTAP的预定义安全组打开所有出站流量。如果可以接受，请遵循基本的出站规则。如果您需要更严格的规则，请使用高级出站规则。

基本出站规则

Cloud Volumes ONTAP的预定义安全组包括以下出站规则。

协议	端口	目的
所有 ICMP	全部	所有出站流量
所有 TCP	全部	所有出站流量
所有 UDP	全部	所有出站流量

高级出站规则

如果您需要对出站流量制定严格的规则，则可以使用以下信息仅打开Cloud Volumes ONTAP出站通信所需的端口。 Cloud Volumes ONTAP集群使用以下端口来调节节点流量。

源是Cloud Volumes ONTAP系统的接口（IP 地址）。

服务	协议	端口	源	目标	目的
Active Directory	TCP	88	节点管理 LIF	Active Directory 林	Kerberos V 身份验证
	UDP	137	节点管理 LIF	Active Directory 林	NetBIOS 名称服务
	UDP	138	节点管理 LIF	Active Directory 林	NetBIOS 数据报服务
	TCP	139	节点管理 LIF	Active Directory 林	NetBIOS 服务会话
	TCP 和 UDP	389	节点管理 LIF	Active Directory 林	LDAP
	TCP	445	节点管理 LIF	Active Directory 林	使用 NetBIOS 框架的 TCP 上的 Microsoft SMB/CIFS
	TCP	464	节点管理 LIF	Active Directory 林	Kerberos V 更改和设置密码（SET_CHANGE）
	UDP	464	节点管理 LIF	Active Directory 林	Kerberos 密钥管理
	TCP	749	节点管理 LIF	Active Directory 林	Kerberos V 更改和设置密码（RPCSEC_GSS）
	TCP	88	数据 LIF（NFS、CIFS、iSCSI）	Active Directory 林	Kerberos V 身份验证
	UDP	137	数据 LIF（NFS、CIFS）	Active Directory 林	NetBIOS 名称服务
	UDP	138	数据 LIF（NFS、CIFS）	Active Directory 林	NetBIOS 数据报服务
	TCP	139	数据 LIF（NFS、CIFS）	Active Directory 林	NetBIOS 服务会话
	TCP 和 UDP	389	数据 LIF（NFS、CIFS）	Active Directory 林	LDAP
	TCP	445	数据 LIF（NFS、CIFS）	Active Directory 林	使用 NetBIOS 框架的 TCP 上的 Microsoft SMB/CIFS
	TCP	464	数据 LIF（NFS、CIFS）	Active Directory 林	Kerberos V 更改和设置密码（SET_CHANGE）
	UDP	464	数据 LIF（NFS、CIFS）	Active Directory 林	Kerberos 密钥管理
	TCP	749	数据 LIF（NFS、CIFS）	Active Directory 林	Kerberos V 更改和设置密码（RPCSEC_GSS）
AutoSupport	HTTPS	443	节点管理 LIF	mysupport.netapp.com	AutoSupport （默认为 HTTPS）
	HTTP	80	节点管理 LIF	mysupport.netapp.com	AutoSupport （仅当传输协议从 HTTPS 更改为 HTTP 时）
	TCP	3128	节点管理 LIF	控制台代理	如果出站互联网连接不可用，则通过控制台代理上的代理服务器发送AutoSupport消息

服务	协议	端口	源	目标	目的
配置备份	HTTP	80	节点管理 LIF	http://<控制台代理 IP 地址>/occm/offboxconfig	将配置备份发送到控制台代理。"ONTAP 文档"
DHCP	UDP	68	节点管理 LIF	DHCP	首次设置的 DHCP 客户端
DHCP服务	UDP	67	节点管理 LIF	DHCP	DHCP 服务器
DNS	UDP	53	节点管理 LIF 和数据 LIF（NFS、CIFS）	DNS	DNS
NDMP	TCP	18600-18699	节点管理 LIF	目标服务器	NDMP 拷贝
SMTP	TCP	25	节点管理 LIF	邮件服务器	SMTP 警报，可用于AutoSupport
SNMP	TCP	161	节点管理 LIF	监控服务器	通过 SNMP 陷阱进行监控
	UDP	161	节点管理 LIF	监控服务器	通过 SNMP 陷阱进行监控
	TCP	162	节点管理 LIF	监控服务器	通过 SNMP 陷阱进行监控
	UDP	162	节点管理 LIF	监控服务器	通过 SNMP 陷阱进行监控
SnapMirror	TCP	11104	集群间 LIF	ONTAP集群间 LIF	SnapMirror集群间通信会话的管理
	TCP	11105	集群间 LIF	ONTAP集群间 LIF	SnapMirror数据传输
系统日志	UDP	514	节点管理 LIF	系统日志服务器	Syslog 转发消息

VPC-1、**VPC-2** 和 **VPC-3** 的规则

在 Google Cloud 中，HA 配置部署在四个 VPC 中。 VPC-0 中的 HA 配置所需的防火墙规则是上面列出的Cloud Volumes ONTAP。

同时，为 VPC-1、VPC-2 和 VPC-3 中的实例创建的预定义防火墙规则支持通过所有协议和端口进行入站通信。这些规则支持 HA 节点之间的通信。

从 HA 节点到 HA 中介的通信通过端口 3260（iSCSI）进行。

> 为了使新的 Google Cloud HA 对部署实现较高的写入速度，VPC-1、VPC-2 和 VPC-3 需要至少 8,896 字节的最大传输单元 (MTU)。如果您选择将现有的 VPC-1、VPC-2 和 VPC-3 升级到 8,896 字节的 MTU，则必须在配置过程中关闭使用这些 VPC 的所有现有 HA 系统。

适用于专用模式部署的 **Infrastructure Manager** 配置

如果要在私有模式下部署 Cloud Volumes ONTAP 9.16.1 或更高版本，则需要进行一些配置更改，以便 Cloud Volumes ONTAP 可以使用 Google Cloud Infrastructure Manager 作为部署服务，而不是 Google 最终将弃用的 Deployment Manager。

开始之前

- 确保您的 Cloud Volumes ONTAP 系统为 9.16.1 或更高版本。如果不是，请升级您的系统。有关说明，请参阅 "升级Cloud Volumes ONTAP"。
- 请确保已启用 Google Cloud API。请参阅 "启用 Google Cloud API"。
- 确保已启用 Cloud Build API。请参阅 "在此处启用 Cloud Build API"。
- 验证 Console 代理的服务帐户是否具有所有标准权限。此外，请确保服务帐户具有 `cloudbuild.workerpools.get`和 `cloudbuild.workerpools.list`权限。请参阅 "控制台代理的 Google Cloud 权限"。

步骤

1. 在与 Cloud Volumes ONTAP 部署相同的区域中使用此配置创建专用工作者池。有关创建专用工作者池的信息，请参阅 "Google Cloud 文档：创建和管理私有池"和 "Google Cloud Build 定价"。

   工作进程池必须具有以下配置：

   - 机器类型：e2-medium
   - 磁盘大小：100 GB
   - 分配外部 IP：False
   - 网络：Default 或 private。
   - 配置为访问 "Google APIs"的子网。执行以下步骤以确保子网可以访问 Google API：
     i. 确保子网的 "Private Google Access" 已打开。
     ii. 转到 **VPC Network level > Private Service Access Tab > Allocated IP ranges for services**。
     iii. 选择 分配 **IP** 范围 ，并为与 Google Compute Service 的私有连接分配内部 IP 范围。
     iv. 在 **Private connection to services** 上，选择 **Create Connection**。
     v. 选择 **Connected service producer = Google Cloud Platform**。
     vi. 为您在上一步中创建的专用连接 IP 范围分配配额。
2. 部署此工作者池并使其运行以进行 Cloud Volumes ONTAP 管理。Google Cloud 使用此工作者池在隔离环境中运行所有 Terraform 操作。
3. 在私有模式下部署 Cloud Volumes ONTAP 时，请在 **GCP Worker Pool** 字段中选择此工作池的名称。有关说明，请参阅 "在 Google Cloud 中启动Cloud Volumes ONTAP"。

控制台代理的要求

如果您尚未创建控制台代理，则应查看网络要求。

- "查看控制台代理的网络要求"
- "Google Cloud 中的防火墙规则"

支持控制台代理的网络配置

您可以使用为控制台代理配置的代理服务器来启用来自Cloud Volumes ONTAP 的出站互联网访问。控制台支持两种类型的代理：

- 显式代理：来自Cloud Volumes ONTAP 的出站流量使用控制台代理代理配置期间指定的代理服务器的

HTTP 地址。控制台代理管理员可能还配置了用户凭据和根 CA 证书以进行额外的身份验证。Cloud Volumes ONTAP显式代理有可用的根 CA 证书，请确保使用 "ONTAP CLI：安全证书安装"命令。

- 透明代理：网络配置为通过控制台代理代理自动路由来自Cloud Volumes ONTAP 的出站流量。设置透明代理时，控制台代理管理员仅需要提供用于从Cloud Volumes ONTAP进行连接的根 CA 证书，而不是代理服务器的 HTTP 地址。确保使用以下方式获取相同的根 CA 证书并将其上传到您的Cloud Volumes ONTAP系统 "ONTAP CLI：安全证书安装"命令。

有关为控制台代理配置代理服务器的信息，请参阅 "配置控制台代理以使用代理服务器"。

在 **Google Cloud** 中为**Cloud Volumes ONTAP**配置网络标签

在控制台代理的透明代理配置期间，管理员为 Google Cloud 添加网络标签。您需要获取并手动添加Cloud Volumes ONTAP配置的相同网络标签。此标签对于代理服务器正常运行是必需的。

1. 在 Google Cloud Console 中，找到 Cloud Volumes ONTAP 系统。
2. 转到*详细信息>网络>网络标签*。
3. 添加用于控制台代理的标签并保存配置。

相关主题

- "验证Cloud Volumes ONTAP 的AutoSupport设置"
- "了解ONTAP内部端口" 。

设置 **VPC** 服务控制以在 **Google Cloud** 中部署**Cloud Volumes ONTAP**

当选择使用 VPC 服务控制锁定您的 Google Cloud 环境时，您应该了解NetApp Console和Cloud Volumes ONTAP如何与 Google Cloud API 交互，以及如何配置您的服务边界以部署控制台和Cloud Volumes ONTAP。

VPC 服务控制使您能够控制对受信任边界之外的 Google 管理服务的访问，阻止来自不受信任位置的数据访问，并降低未经授权的数据传输风险。 "详细了解 Google Cloud VPC 服务控制" 。

NetApp服务如何与 **VPC** 服务控制进行通信

控制台直接与 Google Cloud API 通信。这可以从 Google Cloud 外部的外部 IP 地址触发（例如，来自 api.services.cloud.netapp.com），也可以从 Google Cloud 内部分配给控制台代理的内部地址触发。

根据控制台代理的部署方式，您的服务边界可能需要做出某些例外。

图片

Cloud Volumes ONTAP 和 Console 都使用来自 Google Cloud 中由 NetApp 管理的项目的映像。如果您的组织具有阻止使用未在组织内托管的映像的策略，这可能会影响 Console 代理和 Cloud Volumes ONTAP 的部署。

您可以使用手动安装方法手动部署控制台代理，但Cloud Volumes ONTAP还需要从NetApp项目中提取图像。您必须提供允许列表才能部署控制台代理和Cloud Volumes ONTAP。

部署控制台代理

部署控制台代理的用户需要能够引用 projectId 为 *netapp-cloudmanager* 且项目编号为 *14190056516* 中托管的图像。

- 控制台服务帐户需要引用服务项目中托管在 projectId *netapp-cloudmanager* 中的图像和项目编号 *14190056516*。
- 默认 Google API 服务代理的服务帐户需要引用服务项目中 projectId *netapp-cloudmanager* 和项目编号 *14190056516* 中托管的图像。

下面定义了使用 VPC 服务控制拉取这些图像所需的规则示例。

VPC 服务控制边界策略

策略允许对 VPC Service Controls 规则集进行例外。有关策略的详细信息，请访问 "Google Cloud VPC Service Controls Policy 文档"。

要设置控制台所需的策略，请导航到您组织内的 VPC 服务控制边界并添加以下策略。这些字段应与 VPC 服务控制策略页面中给出的选项相匹配。还要注意，*所有*规则都是必需的，并且规则集中应该使用*OR*参数。

入口规则

```
From:
    Identities:
        [User Email Address]
    Source > All sources allowed
To:
    Projects =
        [Service Project]
    Services =
        Service name: iam.googleapis.com
          Service methods: All actions
        Service name: compute.googleapis.com
          Service methods:All actions
```

或

```
From:
    Identities:
        [User Email Address]
    Source > All sources allowed
To:
    Projects =
        [Host Project]
    Services =
        Service name: compute.googleapis.com
          Service methods: All actions
```

或

```
From:
    Identities:
        [Service Project Number]@cloudservices.gserviceaccount.com
    Source > All sources allowed
To:
    Projects =
        [Service Project]
        [Host Project]
    Services =
        Service name: compute.googleapis.com
        Service methods: All actions
```

出口规则

```
From:
    Identities:
        [Service Project Number]@cloudservices.gserviceaccount.com
To:
    Projects =
        14190056516
    Service =
        Service name: compute.googleapis.com
        Service methods: All actions
```

上面列出的项目编号是NetApp用于存储控制台代理和Cloud Volumes ONTAP 的图像的项目*netapp-cloudmanager*。

为**Cloud Volumes ONTAP**创建 **Google Cloud** 服务帐号

Cloud Volumes ONTAP需要 Google Cloud 服务帐户来实现两个目的。第一个是当你启用"数据分层"将冷数据分层到 Google Cloud 中的低成本对象存储。第二个是当你启用"NetApp Backup and Recovery"将卷备份到低成本的对象存储。

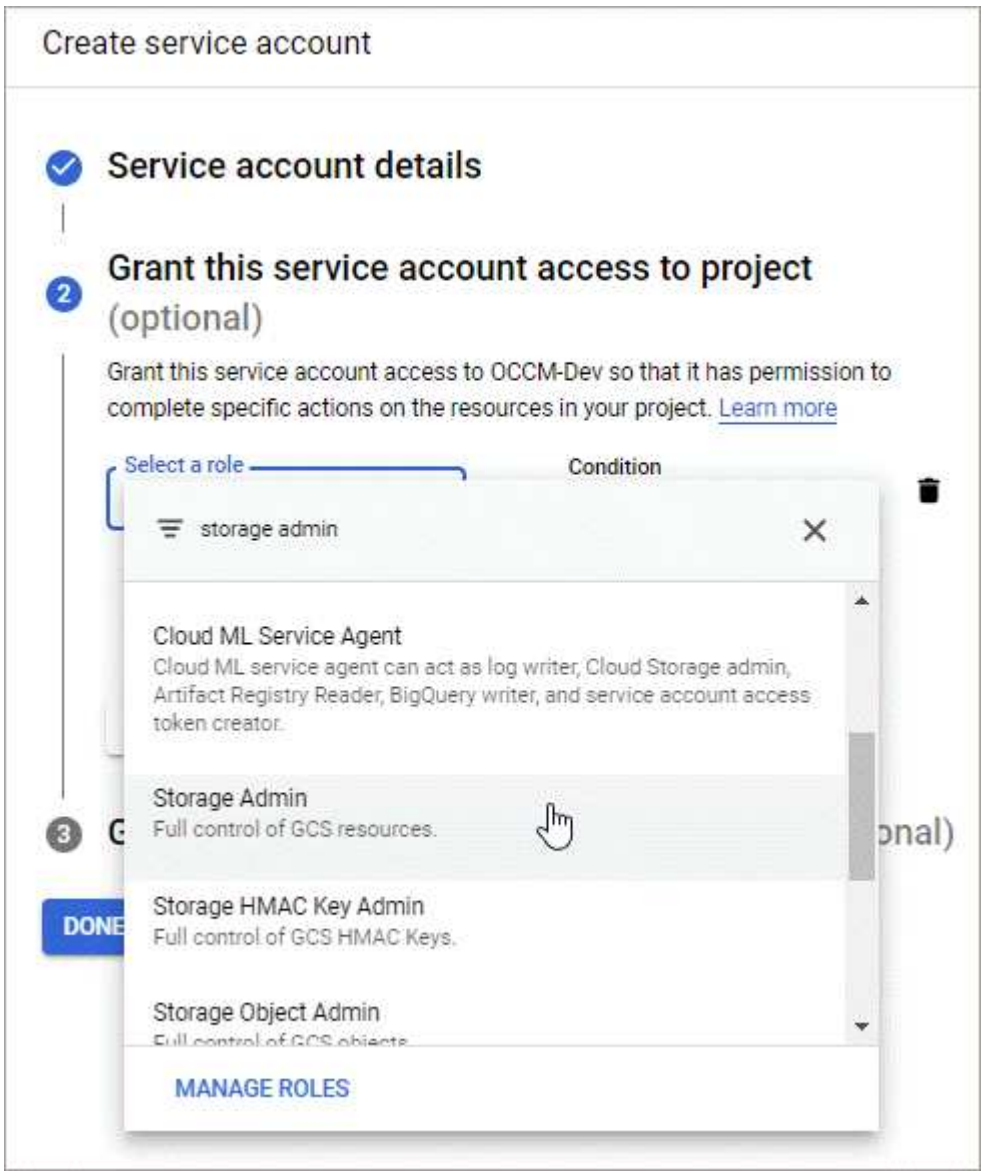
Cloud Volumes ONTAP使用服务帐户来访问和管理一个用于分层数据的存储桶以及另一个用于备份的存储桶。

您可以设置一个服务帐户并将其用于两种用途。服务帐户必须具有*存储管理员*角色。

步骤

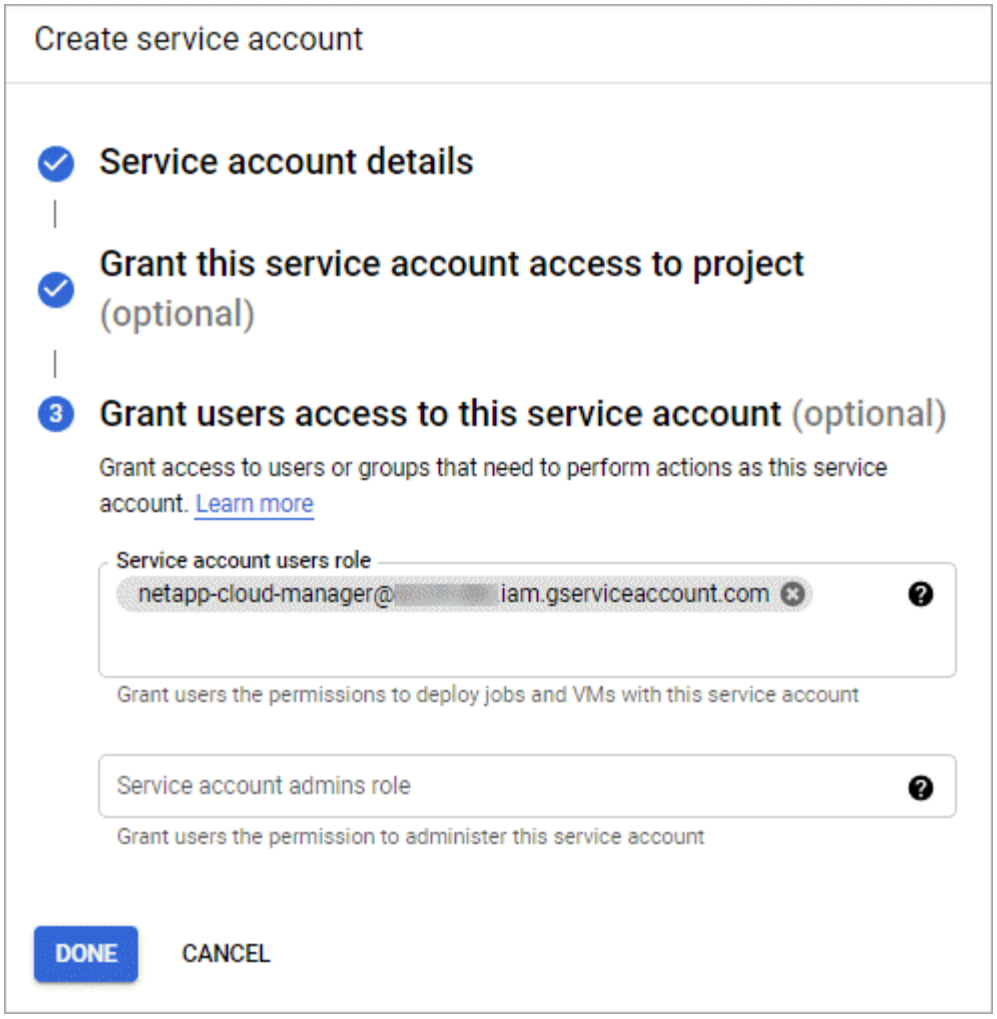
1. 在 Google Cloud Console 中， "前往服务帐户页面"。
2. 选择您的项目。
3. 单击*创建服务帐户*并提供所需信息。
    a. 服务帐户详细信息：输入名称和描述。

b. 授予此服务帐户访问项目的权限：选择*存储管理员*角色。



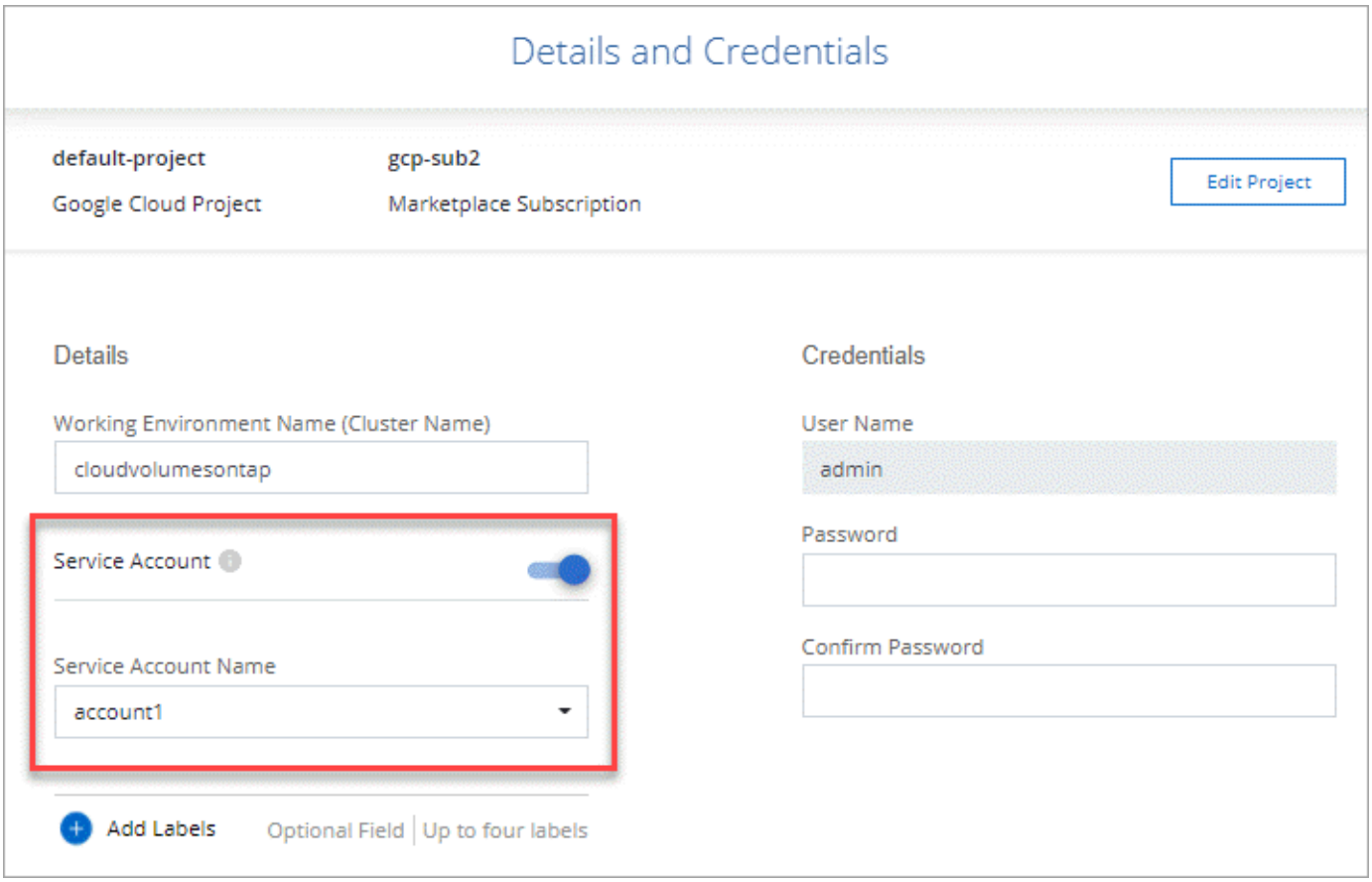
c. 授予用户访问此服务帐户的权限：将控制台代理服务帐户作为_服务帐户用户_添加到此新服务帐户。

此步骤仅对于数据分层是必需的。备份和恢复不需要它。



下一步是什么?

稍后创建Cloud Volumes ONTAP系统时，您需要选择服务帐户。



将客户管理的加密密钥与Cloud Volumes ONTAP结合使用

虽然 Google Cloud Storage 始终会在将数据写入磁盘之前对其进行加密，但您可以使用 API 创建使用_客户管理加密密钥_的Cloud Volumes ONTAP系统。这些是您使用云密钥管理服务在 GCP 中生成和管理的密钥。

步骤

1. 确保控制台代理服务帐户在存储密钥的项目中具有项目级别的正确权限。

   权限已在以下文件中提供： "默认的服务帐户权限"但如果您使用其他项目来管理云密钥服务，则可能无法应用此功能。

   权限如下：

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

2. 确保 "Google Compute Engine 服务代理"对密钥具有 Cloud KMS 加密器/解密器权限。

   服务帐户的名称使用以下格式：“service-[service_project_number]@compute-system.iam.gserviceaccount.com”。

"Google Cloud 文档：将 IAM 与 Cloud KMS 结合使用 - 授予资源角色"

3. 通过调用 get 命令获取密钥的“id” `/gcp/vsa/metadata/gcp-encryption-keys` API 调用或通过在 GCP 控制台中的键上选择“复制资源名称”。
4. 如果使用客户管理的加密密钥并将数据分层到对象存储， NetApp Console会尝试使用用于加密持久磁盘的相同密钥。但您首先需要启用 Google Cloud Storage 存储桶才能使用密钥：

   a. 按照以下步骤查找 Google Cloud Storage 服务代理 "Google Cloud 文档：获取云存储服务代理"。

   b. 导航到加密密钥并为 Google Cloud Storage 服务代理分配 Cloud KMS Encrypter/Decrypter 权限。

   有关详细信息，请参阅 "Google Cloud 文档：使用客户管理的加密密钥"

5. 创建系统时，请将 "gcpEncryption" 参数与 API 请求一起使用。

   例子

```
"gcpEncryptionParameters": {
    "key": "projects/project-1/locations/us-east4/keyRings/keyring-
1/cryptoKeys/generatedkey1"
  }
```

请参阅 "NetApp Console自动化文档"有关使用“GcpEncryption”参数的更多详细信息。

在 Google Cloud 中设置Cloud Volumes ONTAP许可

在您决定要对Cloud Volumes ONTAP使用哪种许可选项后，需要执行几个步骤才能在创建新系统时选择该许可选项。

免费增值

选择免费增值服务，免费使用Cloud Volumes ONTAP，最高可提供 500 GiB 的配置容量。"了解有关免费增值服务的更多信息" 。

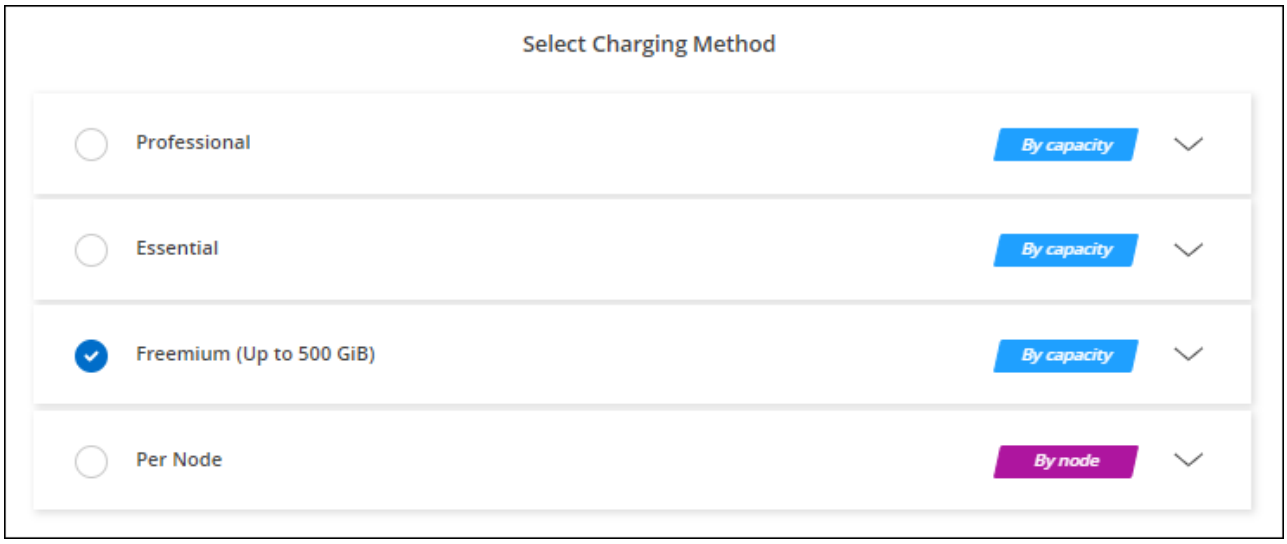
步骤

1. 从左侧导航菜单中，选择“存储”>“管理”。
2. 在“系统”页面上，单击“添加系统”并按照NetApp Console中的步骤进行操作。

   a. 在*详细信息和凭据*页面上，单击*编辑凭据>添加订阅*，然后按照提示订阅 Google Cloud Marketplace 中的即用即付产品。

      除非您超过 500 GiB 的预配置容量，否则您无需通过市场订阅付费，此时系统将自动转换为"基本套餐"。

   b. 返回控制台后，到达收费方式页面时选择“免费增值”。



"查看在 Google Cloud 中启动Cloud Volumes ONTAP 的分步说明" 。

基于容量的许可证

基于容量的许可使您能够按 TiB 容量支付Cloud Volumes ONTAP费用。基于容量的许可以_包_的形式提供：Essentials 或 Professional 包。

Essentials 和 Professional 套餐提供以下几种消费模式或购买选项：

- 从NetApp购买的许可证（自带许可证 (BYOL)）
- Google Cloud Marketplace 的按小时付费 (PAYGO) 订阅
- 年度合同

"了解有关基于容量的许可的更多信息" 。

以下部分介绍了如何开始使用每种消费模型。

BYOL

通过从NetApp购买许可证 (BYOL) 进行预付款，以便在任何云提供商处部署Cloud Volumes ONTAP系统。

已限制 BYOL 许可证的购买、延期和续订。有关更多信息，请参阅 "Cloud Volumes ONTAP的 BYOL 许可可用性受限" 。

步骤

1. "联系NetApp销售人员获取许可证"
2. "将您的NetApp支持站点帐户添加到NetApp Console"

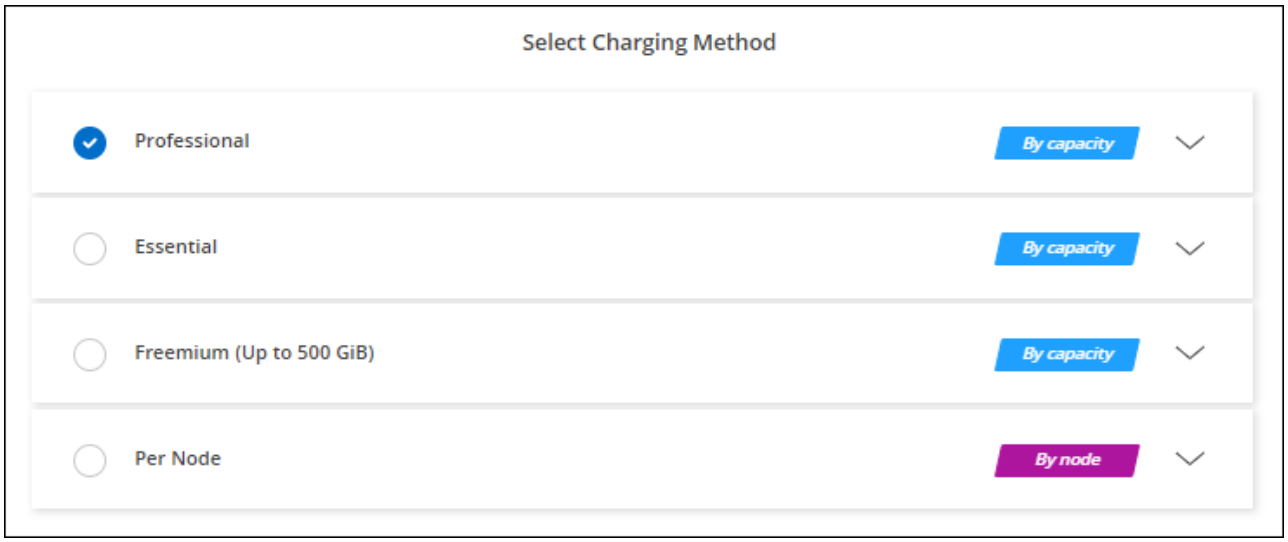
   控制台会自动查询 NetApp 的许可服务，以获取与您的NetApp支持站点帐户相关的许可证的详细信息。如果没有错误，控制台将添加许可证。

   您必须先从控制台获取许可证，然后才能将其与Cloud Volumes ONTAP一起使用。如果需要的话，你可以"手动将许可证添加到控制台"。

3. 在*系统*页面上，单击*添加系统*并按照步骤操作。
    a. 在*详细信息和凭据*页面上，单击*编辑凭据>添加订阅*，然后按照提示订阅 Google Cloud Marketplace 中的即用即付产品。

        始终会先向您从NetApp购买的许可证收费，但如果您超出许可容量或许可证期限到期，则会按照市场上的小时费率向您收费。

    b. 返回控制台后，在进入收费方式页面时选择基于容量的套餐。



"查看在 Google Cloud 中启动Cloud Volumes ONTAP 的分步说明" 。

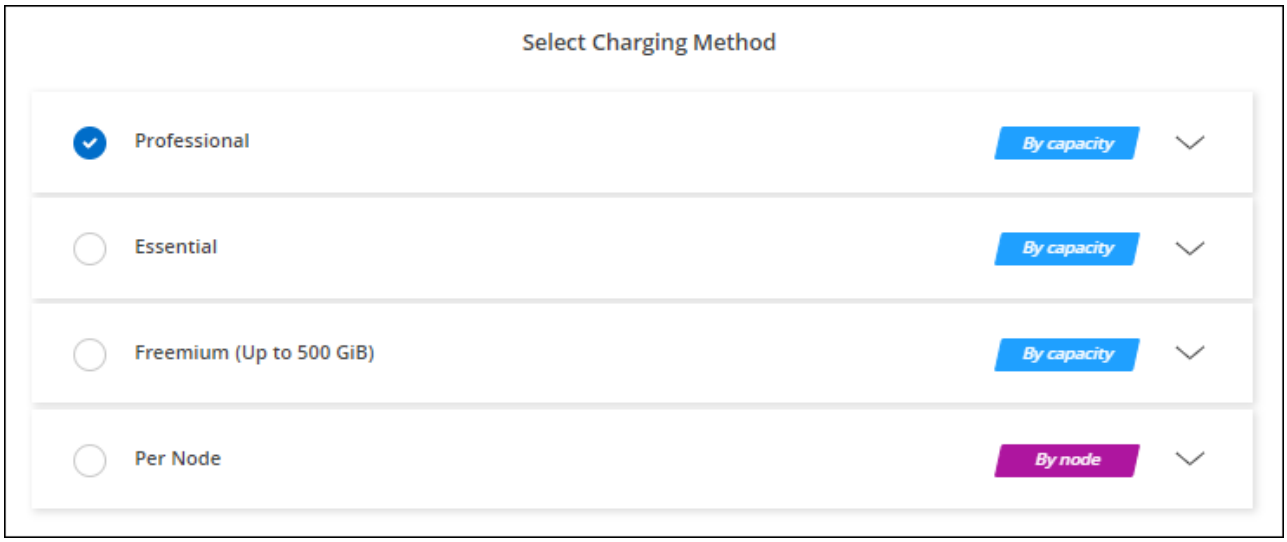
PAYGO 订阅

通过订阅云提供商市场提供的服务按小时付费。

当您创建Cloud Volumes ONTAP系统时，控制台会提示您订阅 Google Cloud Marketplace 中提供的协议。然后将该订阅与系统关联以进行收费。您可以将同一订阅用于其他系统。

步骤

1. 从左侧导航菜单中，选择“存储”>“管理”。
2. 在*系统*页面上，单击*添加系统*并按照步骤操作。
    a. 在*详细信息和凭据*页面上，单击*编辑凭据>添加订阅*，然后按照提示订阅 Google Cloud Marketplace 中的即用即付产品。
    b. 返回控制台后，在进入收费方式页面时选择基于容量的套餐。



"查看在 Google Cloud 中启动Cloud Volumes ONTAP 的分步说明" 。

您可以从“设置”>“凭据”页面管理与您的帐户关联的 Google Cloud Marketplace 订阅。 "了解如何管理您的 Google Cloud 凭据和订阅"

年度合同

通过购买年度合同每年支付Cloud Volumes ONTAP 的费用。

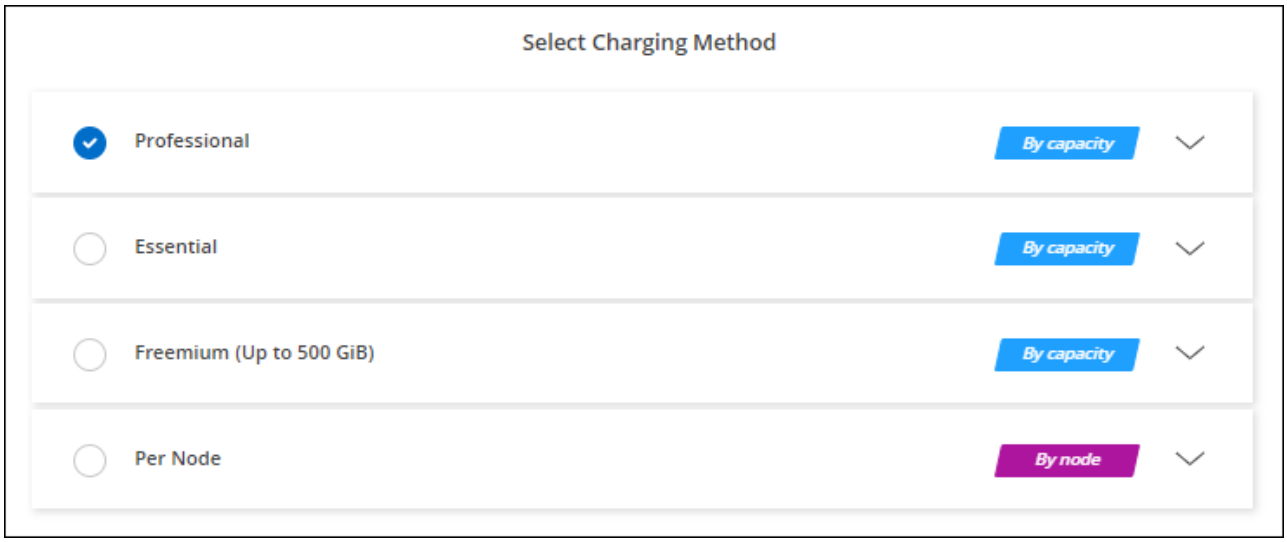
步骤

1. 联系您的NetApp销售代表购买年度合同。

   该合同在 Google Cloud Marketplace 中以私人优惠形式提供。

   NetApp与您分享私人优惠后，您可以在系统创建期间从 Google Cloud Marketplace 订阅时选择年度计划。

2. 在*系统*页面上，单击*添加系统*并按照步骤操作。
   a. 在*详细信息和凭据*页面上，单击*编辑凭据>添加订阅*，然后按照提示在 Google Cloud Marketplace 中订阅年度计划。
   b. 在 Google Cloud 中，选择与您的帐户共享的年度计划，然后单击*订阅*。
   c. 返回控制台后，在进入收费方式页面时选择基于容量的套餐。



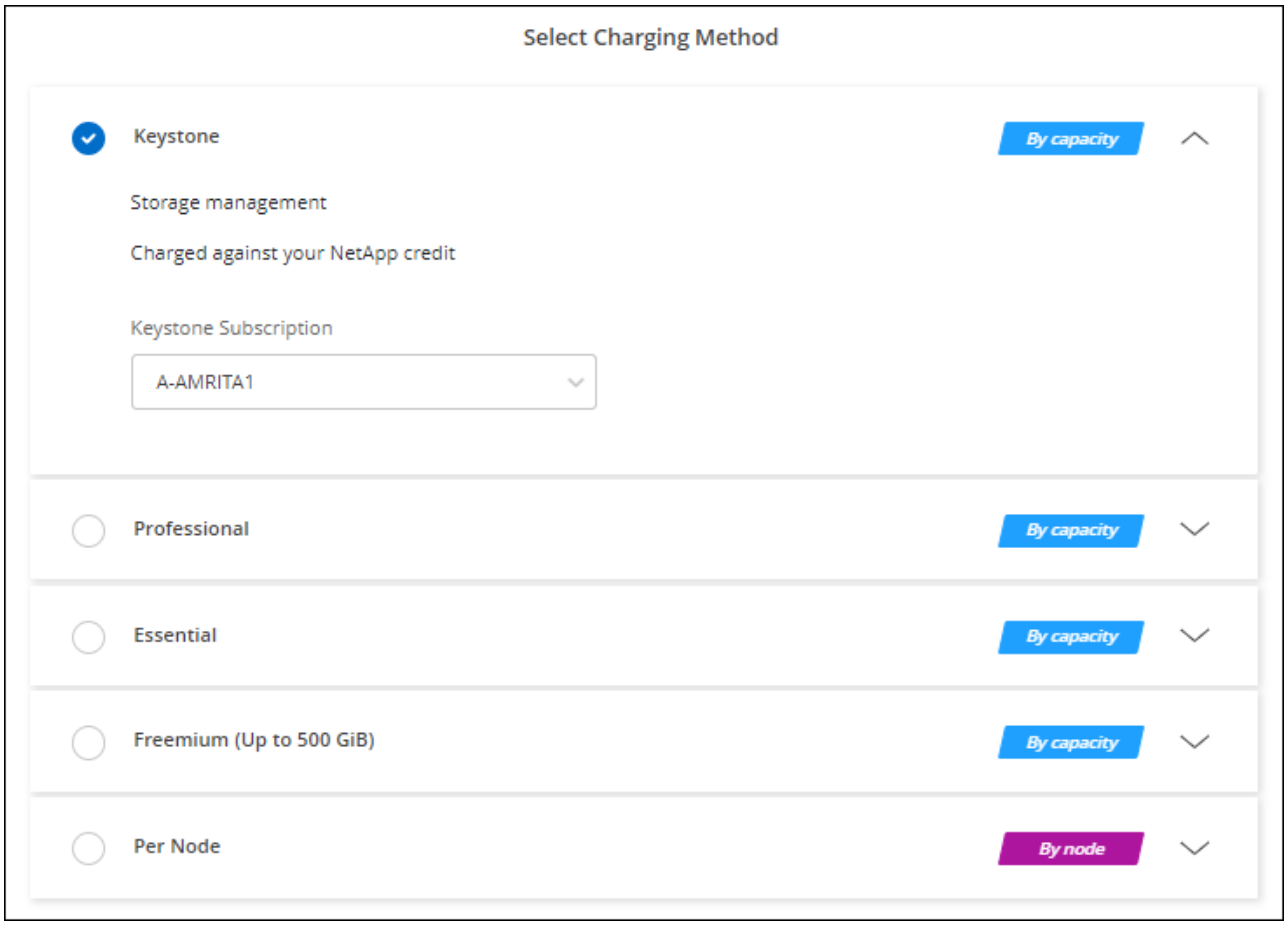
"查看在 Google Cloud 中启动Cloud Volumes ONTAP 的分步说明" 。

Keystone订阅

Keystone订阅是一种按需付费的订阅式服务。"了解有关NetApp Keystone订阅的更多信息" 。

步骤

1. 如果您尚未订阅， "联系NetApp"
2. 联系NetApp 授权您的控制台用户帐户拥有一个或多个Keystone订阅。
3. NetApp授权您的帐户后，"链接您的订阅以用于Cloud Volumes ONTAP" 。
4. 在*系统*页面上，单击*添加系统*并按照步骤操作。
    a. 当提示选择收费方式时，选择Keystone Subscription 收费方式。



"查看在 Google Cloud 中启动Cloud Volumes ONTAP 的分步说明" 。

基于节点的许可证

基于节点的许可证是Cloud Volumes ONTAP的上一代许可证。基于节点的许可证可以从NetApp (BYOL) 处购买，并且仅在特定情况下才可以续订许可证。有关信息，请参阅：

- "基于节点的许可证的可用性终止"
- "基于节点的许可证的可用性终止"
- "将基于节点的许可证转换为基于容量的许可证"

在 Google Cloud 中启动Cloud Volumes ONTAP

您可以在单节点配置中启动Cloud Volumes ONTAP ，也可以在 Google Cloud 中以 HA 对的形式启动 Cloud Volumes ONTAP。

开始之前

开始之前您需要以下内容。

- 已启动且正在运行的 NetApp Console 代理。
  - 你应该有一个 "与您的系统关联的控制台代理"。

- "您应该准备好让控制台代理始终处于运行状态" 。
- 与控制台代理关联的服务帐户 "应该具有所需的权限"

- 了解您想要使用的配置。

  您应该已经做好准备，选择配置并从管理员处获取 Google Cloud 网络信息。有关详细信息，请参阅"规划您的Cloud Volumes ONTAP配置"。

- 了解设置Cloud Volumes ONTAP许可所需的条件。

  "了解如何设置许可" 。

- Google Cloud API 应该 "在您的项目中启用"：
  - 云部署管理器 V2 API
  - 云日志 API
  - 云资源管理器 API
  - 计算引擎 API
  - 身份和访问管理 (IAM) API

在 **Google Cloud** 中启动单节点系统

在NetApp Console中创建一个系统以在 Google Cloud 中启动Cloud Volumes ONTAP 。

步骤

1. 从左侧导航菜单中，选择“存储”>“管理”。
2. 在*系统*页面上，单击*添加系统*并按照提示进行操作。
3. 选择位置：选择*Google Cloud*和* Cloud Volumes ONTAP*。
4. 如果出现提示， "创建控制台代理" 。
5. 详细信息和凭证：选择一个项目，指定一个集群名称，可选地选择一个服务帐户，可选地添加标签，然后指定凭证。

   下表描述了您可能需要指导的字段：

字段	描述
系统名称	控制台使用系统名称来命名Cloud Volumes ONTAP系统和 Google Cloud VM 实例。如果您选择该选项，它还会使用该名称作为预定义安全组的前缀。
服务帐户名称	如果你打算使用"数据分层"或者 "NetApp Backup and Recovery"使用Cloud Volumes ONTAP，则需要启用*服务帐户*并选择具有预定义存储管理员角色的服务帐户。"了解如何创建服务帐号" 。
添加标签	标签是您的 Google Cloud 资源的元数据。控制台将标签添加到Cloud Volumes ONTAP系统以及与该系统关联的 Google Cloud 资源。创建系统时，您可以从用户界面添加最多四个标签，然后可以在创建系统后添加更多标签。请注意，创建系统时，API 不会将您限制为四个标签。有关标签的信息，请参阅 "Google Cloud 文档：标记资源"。

字段	描述
用户名和密码	这些是Cloud Volumes ONTAP集群管理员帐户的凭据。您可以使用这些凭据通过ONTAP System Manager 或ONTAP CLI 连接到Cloud Volumes ONTAP 。保留默认的_admin_用户名或将其更改为自定义用户名。
编辑项目	选择您希望Cloud Volumes ONTAP驻留的项目。默认项目是控制台所在的项目。 如果您在下拉列表中没有看到任何其他项目，则表示您尚未将服务帐户与其他项目关联。转到 Google Cloud Console，打开 IAM 服务，然后选择项目。将具有用于 Console 的角色的服务帐户添加到该项目。您需要为每个项目重复此步骤。 这是您为控制台设置的服务帐户，"如本页所述" 。 单击“添加订阅”将选定的凭据与订阅关联。 要创建按使用量付费的Cloud Volumes ONTAP系统，您需要从 Google Cloud 市场选择与Cloud Volumes ONTAP订阅相关联的 Google Cloud 项目。参考 "将市场订阅与 Google Cloud 凭据关联"。

6. 服务：选择您想要在此系统上使用的服务。为了选择备份和恢复，或使用NetApp Cloud Tiering，您必须在步骤 3 中指定服务帐户。

   如果您想使用 WORM 和数据分层，则必须禁用备份和恢复并部署版本 9.8 或更高版本的Cloud Volumes ONTAP系统。

7. 位置和连接：为您的系统选择 Google Cloud 区域和区域，选择防火墙策略，并确认网络连接到 Google Cloud 存储以进行数据分层。

   下表描述了您可能需要指导的字段：

字段	描述
连接验证	要将冷数据分层到 Google Cloud Storage 存储桶，必须为Cloud Volumes ONTAP所在的子网配置私有 Google Access。有关说明，请参阅 "Google Cloud 文档：配置私有 Google 访问权限"。
生成的防火墙策略	如果您让控制台为您生成防火墙策略，则需要选择如何允许流量： • 如果您选择*仅限选定的 VPC*，则入站流量的源过滤器是选定 VPC 的子网范围和控制台代理所在 VPC 的子网范围。这是推荐的选项。 • 如果您选择*所有 VPC*，则入站流量的源过滤器是 0.0.0.0/0 IP 范围。
使用现有的防火墙策略	如果您使用现有的防火墙策略，请确保它包含所需的规则："了解Cloud Volumes ONTAP的防火墙规则"

8. 收费方式和 **NSS** 帐户：指定您想要在此系统中使用的收费选项，然后指定NetApp支持站点帐户：
   - "了解Cloud Volumes ONTAP的许可选项"

- "了解如何设置许可"

9. 预配置的软件包：选择其中一个软件包以快速部署 Cloud Volumes ONTAP 系统，或单击*创建我自己的配置*。预配置的软件包因所选 Cloud Volumes ONTAP 版本而异。例如，对于 Cloud Volumes ONTAP 9.18.1 及更高版本，Console 显示包含 C3 VM 的软件包，包括 Hyperdisk Balanced 磁盘。您可以根据工作负载需求修改配置，例如 IOPS 和吞吐量参数。

   如果您选择其中一个套餐，您只需指定一个卷，然后审核并批准配置。

10. 许可：根据需要更改Cloud Volumes ONTAP版本并选择机器类型。

    如果所选版本有较新的候选版本、通用版本或补丁版本，则控制台在创建系统时会将其更新到该版本。例如，如果您选择Cloud Volumes ONTAP 9.13.1 并且 9.13.1 P4 可用，则会发生更新。更新不会从一个版本发生到另一个版本 — 例如，从 9.13 到 9.14。

11. 底层存储资源：选择初始聚合的设置：磁盘类型和每个磁盘的大小。

    磁盘类型适用于初始卷。您可以为后续卷选择不同的磁盘类型。

    磁盘大小适用于初始聚合中的所有磁盘以及使用简单配置选项时控制台创建的任何其他聚合。您可以使用高级分配选项创建使用不同磁盘大小的聚合。

    有关选择磁盘类型和大小的帮助，请参阅"在 Google Cloud 中调整系统大小"。

12. 闪存缓存、写入速度和 **WORM**：

    a. 如果需要，启用 **Flash Cache** 或选择*普通*或*高*写入速度。

       详细了解 "Flash Cache" 和 "写入速度"。

       通过*高*写入速度选项可实现高写入速度和更高的 8,896 字节最大传输单元 (MTU)。此外，8,896 的更高 MTU 要求选择 VPC-1、VPC-2 和 VPC-3 进行部署。有关 VPC-1、VPC-2 和 VPC-3 的更多信息，请参阅 "VPC-1、VPC-2 和 VPC-3 的规则"。

    b. 如果需要，请激活一次写入、多次读取 (WORM) 存储。

       如果为Cloud Volumes ONTAP 9.7 及更低版本启用了数据分层，则无法启用 WORM。启用 WORM 和分层后，恢复或降级到Cloud Volumes ONTAP 9.8 的操作将被阻止。

    "了解有关 WORM 存储的更多信息" 。

    a. 如果您激活 WORM 存储，请选择保留期限。

13. **Google Cloud Platform** 中的数据分层：选择是否在初始聚合上启用数据分层，为分层数据选择存储类，然后选择具有预定义存储管理员角色的服务帐户（ Cloud Volumes ONTAP 9.7 或更高版本所需），或选择 Google Cloud 帐户（ Cloud Volumes ONTAP 9.6 所需）。

    请注意以下事项：

    - 控制台在Cloud Volumes ONTAP实例上设置服务帐户。此服务帐户提供将数据分层到 Google Cloud Storage 存储桶的权限。请确保将控制台代理服务帐户添加为分层服务帐户的用户，否则，您无法从控制台中选择它。

- 如需添加 Google Cloud 帐户的帮助，请参阅 "使用 9.6 设置和添加 Google Cloud 帐户以进行数据分层"。
- 您可以在创建或编辑卷时选择特定的卷分层策略。
- 如果您禁用数据分层，则可以在后续聚合上启用它，但您需要关闭系统并从 Google Cloud Console 添加服务帐户。

  "了解有关数据分层的更多信息" 。

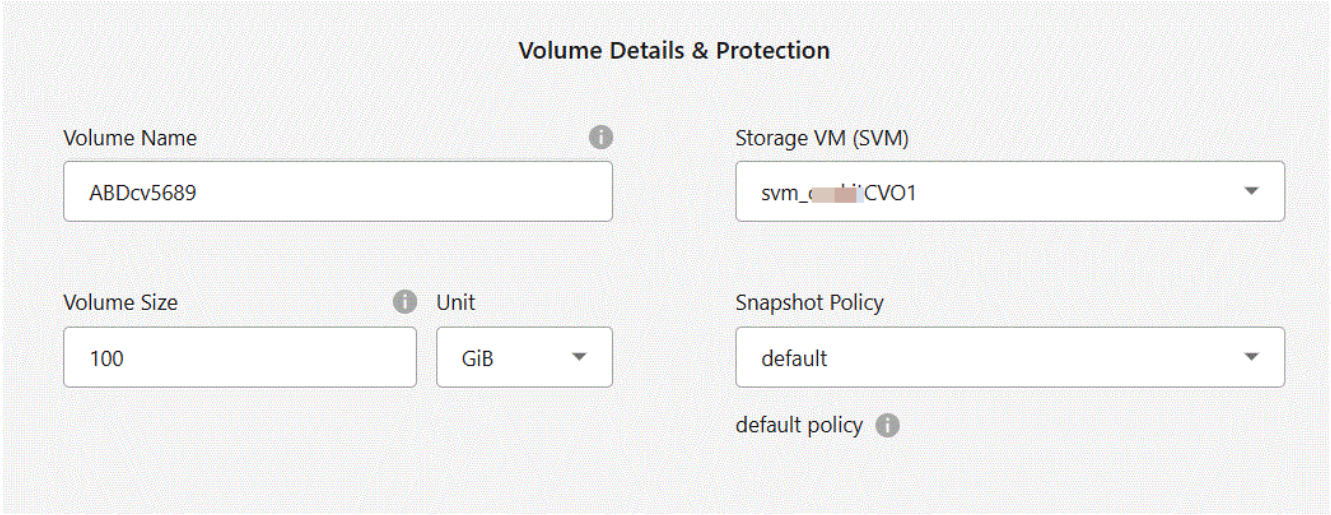
14. 创建卷：输入新卷的详细信息或单击*跳过*。

    "了解支持的客户端协议和版本" 。

    此页面中的某些字段是不言自明的。下表描述了您可能需要指导的字段：

字段	描述
大小	您可以输入的最大大小很大程度上取决于您是否启用精简配置，这使您能够创建比当前可用的物理存储更大的卷。
访问控制（仅适用于 NFS）	导出策略定义了子网中可以访问卷的客户端。默认情况下，控制台输入一个提供对子网中所有实例的访问权限的值。
权限和用户/组（仅适用于 CIFS）	这些字段使您能够控制用户和组对共享的访问级别（也称为访问控制列表或 ACL）。您可以指定本地或域 Windows 用户或组，或者 UNIX 用户或组。如果指定域 Windows 用户名，则必须使用域\用户名格式包含用户的域。
Snapshot 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 副本是时间点文件系统映像，它不会影响性能并且只需要最少的存储空间。您可以选择默认策略或无策略。对于瞬态数据，您可能选择无：例如，对于 Microsoft SQL Server，请选择 tempdb。
高级选项（仅适用于 NFS）	为卷选择一个 NFS 版本：NFSv3 或 NFSv4。
启动器组和 IQN（仅适用于 iSCSI）	iSCSI 存储目标称为 LUN（逻辑单元），并作为标准块设备呈现给主机。启动器组是 iSCSI 主机节点名称表，用于控制哪些启动器可以访问哪些 LUN。iSCSI 目标通过标准以太网网络适配器 (NIC)、带有软件启动器的 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。当您创建 iSCSI 卷时，控制台会自动为您创建一个 LUN。我们通过为每个卷创建一个 LUN 来简化操作，因此无需进行任何管理。创建卷后，"使用 IQN 从主机连接到 LUN" 。

    下图显示了卷创建向导的第一页：



15. **CIFS** 设置：如果您选择了 CIFS 协议，请设置 CIFS 服务器。

字段	描述
DNS 主 IP 地址和辅助 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 服务器必须包含定位 CIFS 服务器将加入的域的 Active Directory LDAP 服务器和域控制器所需的服务位置记录 (SRV)。如果您正在配置 Google 管理的 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 域内指定组织单位 (OU) 的 Windows 帐户的名称和密码。
CIFS 服务器 NetBIOS 名称	AD 域中唯一的 CIFS 服务器名称。
组织单位	AD 域内与 CIFS 服务器关联的组织单位。默认值为 CN=Computers。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** 。https://cloud.google.com/managed-microsoft-ad/docs/manage-active-directory-objects#organizational_units["Google Cloud 文档：Google Managed Microsoft AD 中的组织单位"^]
DNS 域	Cloud Volumes ONTAP存储虚拟机 (SVM) 的 DNS 域。大多数情况下，该域与 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。如果您需要使用不同的地址配置 NTP 服务器，那么您应该使用 API。欲了解更多信息，请参阅 "NetApp Console自动化文档"了解详情。请注意，只有在创建 CIFS 服务器时才能配置 NTP 服务器。创建 CIFS 服务器后，它不可配置。

16. 使用情况配置文件、磁盘类型和分层策略：选择是否要启用存储效率功能并更改卷分层策略（如果需要）。

    更多信息，请参阅"选择卷使用情况配置文件"，"数据分层概述" ， 和 "KB：CVO 支持哪些内联存储效率功能？"

17. 审核并批准：审核并确认您的选择。

    a. 查看有关配置的详细信息。

b. 点击*更多信息*查看有关支持和控制台将购买的 Google Cloud 资源的详细信息。

c. 选中*我明白…*复选框。

d. 单击“开始”。

结果

控制台部署Cloud Volumes ONTAP系统。您可以在*审核*页面上跟踪进度。

如果您在部署Cloud Volumes ONTAP系统时遇到任何问题，请查看失败消息。您也可以选择系统并单击*重新创建环境*。

如需更多帮助，请访问 "NetApp Cloud Volumes ONTAP支持"。

完成后

- 如果您配置了 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共享并创建文件。
- 如果要将配额应用于卷，请使用ONTAP系统管理器或ONTAP CLI。

  配额使您能够限制或跟踪用户、组或 qtree 使用的磁盘空间和文件数量。

部署流程完成后，请勿修改 Google Cloud 门户中系统生成的 Cloud Volumes ONTAP 配置，例如系统标签以及 Google Cloud 资源中设置的标签。对这些配置进行的任何更改都可能导致意外行为或数据丢失。

在 **Google Cloud** 中启动 **HA** 对

在控制台中创建一个系统以在 Google Cloud 中启动Cloud Volumes ONTAP 。

步骤

1. 从左侧导航菜单中，选择“存储”>“管理”。
2. 在*系统*页面上，单击*存储>系统*并按照提示进行操作。
3. 选择位置：选择*Google Cloud*和* Cloud Volumes ONTAP HA*。
4. 详细信息和凭证：选择一个项目，指定一个集群名称，可选地选择一个服务帐户，可选地添加标签，然后指定凭证。

   下表描述了您可能需要指导的字段：

字段	描述
系统名称	控制台使用系统名称来命名Cloud Volumes ONTAP系统和 Google Cloud VM 实例。如果您选择该选项，它还会使用该名称作为预定义安全组的前缀。
服务帐户名称	如果您打算使用"NetApp Cloud Tiering"或者 "备份和恢复"服务，您需要启用*服务帐户*开关，然后选择具有预定义存储管理员角色的服务帐户。
添加标签	标签是您的 Google Cloud 资源的元数据。控制台将标签添加到Cloud Volumes ONTAP系统以及与该系统关联的 Google Cloud 资源。创建系统时，您可以从用户界面添加最多四个标签，然后可以在创建系统后添加更多标签。请注意，创建系统时，API 不会将您限制为四个标签。有关标签的信息，请参阅 "Google Cloud 文档：标记资源"。

字段	描述
用户名和密码	这些是Cloud Volumes ONTAP集群管理员帐户的凭据。您可以使用这些凭据通过ONTAP System Manager 或ONTAP CLI 连接到Cloud Volumes ONTAP 。保留默认的_admin_用户名或将其更改为自定义用户名。
编辑项目	选择要让 Cloud Volumes ONTAP 驻留的项目。 如果您在下拉列表中没有看到任何其他项目，则表示您尚未将服务帐户与其他项目关联。转到 Google Cloud Console，打开 IAM 服务，然后选择项目。将具有用于 Console 的角色的服务帐户添加到该项目。您需要为每个项目重复此步骤。 这是您为控制台设置的服务帐户，"如本页所述" 。 单击“添加订阅”将选定的凭据与订阅关联。 要创建按使用量付费的Cloud Volumes ONTAP系统，您需要从 Google Cloud Marketplace 中选择与Cloud Volumes ONTAP订阅相关联的 Google Cloud 项目。参考 "将市场订阅与 Google Cloud 凭据关联"。

5. 服务：选择您想要在此系统上使用的服务。要选择备份和恢复，或使用NetApp Cloud Tiering，您必须在步骤 3 中指定服务帐户。

   如果您想使用 WORM 和数据分层，则必须禁用备份和恢复并部署版本 9.8 或更高版本的Cloud Volumes ONTAP系统。

6. **HA Deployment Models**：为 HA 配置选择多个区域（推荐）或单个区域。然后选择一个区域和可用区。

   "了解有关 HA 部署模型的更多信息" 。

7. 连接性：为 HA 配置选择四个不同的 VPC，每个 VPC 中选择一个子网，然后选择一个防火墙策略。

   "了解有关网络要求的更多信息" 。

   下表描述了您可能需要指导的字段：

字段	描述
生成的策略	如果您让控制台为您生成防火墙策略，则需要选择如何允许流量： • 如果您选择*仅限选定的 VPC*，则入站流量的源过滤器是选定 VPC 的子网范围和控制台代理所在 VPC 的子网范围。这是推荐的选项。 • 如果您选择*所有 VPC*，则入站流量的源过滤器是 0.0.0.0/0 IP 范围。
使用现有的	如果您使用现有的防火墙策略，请确保它包含所需的规则。"了解Cloud Volumes ONTAP的防火墙规则" 。

8. 收费方式和 **NSS** 帐户：指定您想要在此系统中使用的收费选项，然后指定NetApp支持站点帐户。
   - "了解Cloud Volumes ONTAP的许可选项" 。

- "了解如何设置许可" 。

9. 预配置包：选择其中一个包来快速部署Cloud Volumes ONTAP系统，或者单击*创建我自己的配置*。

   如果您选择其中一个套餐，您只需指定一个卷，然后审核并批准配置。

10. 许可：根据需要更改Cloud Volumes ONTAP版本并选择机器类型。

    > 如果所选版本有较新的候选版本、通用版本或补丁版本，则控制台在创建系统时会将其更新到该版本。例如，如果您选择Cloud Volumes ONTAP 9.13.1 并且 9.13.1 P4 可用，则会发生更新。更新不会从一个版本发生到另一个版本 - 例如，从 9.13 到 9.14。

11. 底层存储资源：选择初始聚合的设置：磁盘类型和每个磁盘的大小。

    磁盘类型适用于初始卷。您可以为后续卷选择不同的磁盘类型。

    磁盘大小适用于初始聚合中的所有磁盘以及使用简单配置选项时控制台创建的任何其他聚合。您可以使用高级分配选项创建使用不同磁盘大小的聚合。

    有关选择磁盘类型和大小的帮助，请参阅"在 Google Cloud 中调整系统大小"。

12. 闪存缓存、写入速度和 **WORM**：

    a. 如果需要，启用 **Flash Cache** 或选择*普通*或*高*写入速度。

       详细了解 "Flash Cache" 和 "写入速度"。

       > 通过 n2-standard-16、n2-standard-32、n2-standard-48 和 n2-standard-64 实例类型的高 写入速度选项，可以获得高写入速度和更高的 8,896 字节的最大传输单元 (MTU)。此外，8,896 的更高 MTU 要求选择 VPC-1、VPC-2 和 VPC-3 进行部署。高写入速度和 8,896 的 MTU 取决于功能，无法在配置的实例中单独禁用。有关 VPC-1、VPC-2 和 VPC-3 的更多信息，请参阅 "VPC-1、VPC-2 和 VPC-3 的规则"。

    b. 如果需要，请激活一次写入、多次读取 (WORM) 存储。

       如果为Cloud Volumes ONTAP 9.7 及更低版本启用了数据分层，则无法启用 WORM。启用 WORM 和分层后，恢复或降级到Cloud Volumes ONTAP 9.8 的操作将被阻止。

    "了解有关 WORM 存储的更多信息" 。

    a. 如果您激活 WORM 存储，请选择保留期限。

13. **Google Cloud** 中的数据分层：选择是否在初始聚合上启用数据分层，为分层数据选择存储类，然后选择具有预定义存储管理员角色的服务帐户。

    请注意以下事项：

    - 控制台在Cloud Volumes ONTAP实例上设置服务帐户。此服务帐户提供将数据分层到 Google Cloud Storage 存储桶的权限。请确保将控制台代理服务帐户添加为分层服务帐户的用户，否则，您无法从控制台中选择它。
    - 您可以在创建或编辑卷时选择特定的卷分层策略。
    - 如果您禁用数据分层，则可以在后续聚合上启用它，但您需要关闭系统并从 Google Cloud Console 添加

服务帐户。

"了解有关数据分层的更多信息"。

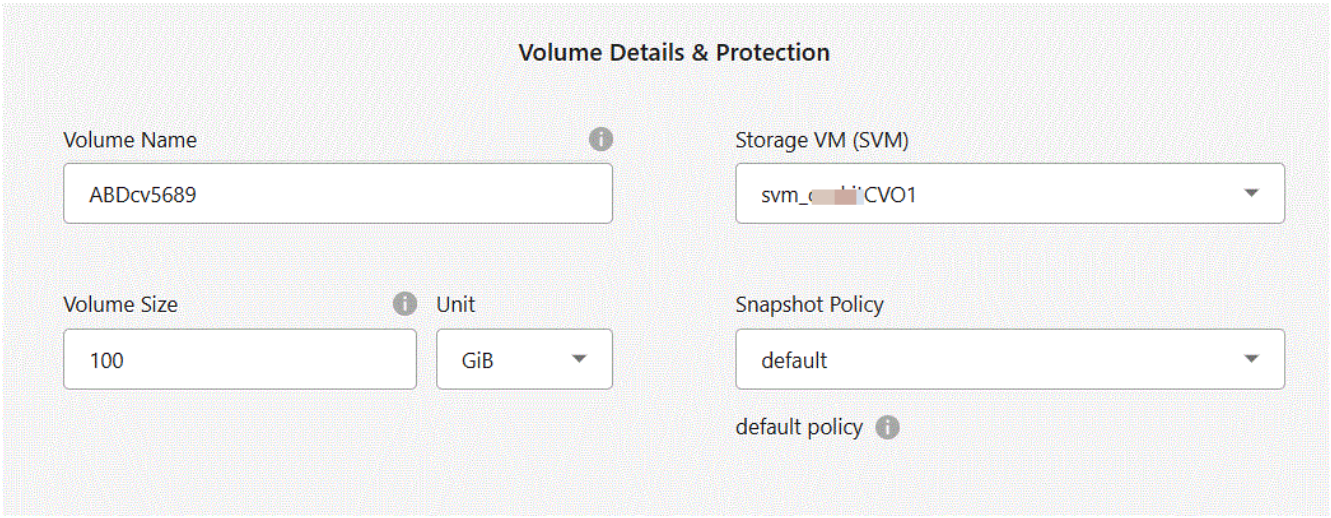
14. 创建卷：输入新卷的详细信息或单击*跳过*。

"了解支持的客户端协议和版本"。

此页面中的某些字段是不言自明的。下表描述了您可能需要指导的字段：

字段	描述
大小	您可以输入的最大大小很大程度上取决于您是否启用精简配置，这使您能够创建比当前可用的物理存储更大的卷。
访问控制（仅适用于 NFS）	导出策略定义了子网中可以访问卷的客户端。默认情况下，控制台输入一个提供对子网中所有实例的访问权限的值。
权限和用户/组（仅适用于 CIFS）	这些字段使您能够控制用户和组对共享的访问级别（也称为访问控制列表或 ACL）。您可以指定本地或域 Windows 用户或组，或者 UNIX 用户或组。如果指定域 Windows 用户名，则必须使用域\用户名格式包含用户的域。
Snapshot 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 副本是时间点文件系统映像，它不会影响性能并且只需要最少的存储空间。您可以选择默认策略或无策略。对于瞬态数据，您可能选择无：例如，对于 Microsoft SQL Server，请选择 tempdb。
高级选项（仅适用于 NFS）	为卷选择一个 NFS 版本：NFSv3 或 NFSv4。
启动器组和 IQN（仅适用于 iSCSI）	iSCSI 存储目标称为 LUN（逻辑单元），并作为标准块设备呈现给主机。启动器组是 iSCSI 主机节点名称表，用于控制哪些启动器可以访问哪些 LUN。iSCSI 目标通过标准以太网网络适配器 (NIC)、带有软件启动器的 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。当您创建 iSCSI 卷时，控制台会自动为您创建一个 LUN。我们通过为每个卷创建一个 LUN 来简化操作，因此无需进行任何管理。创建卷后，"使用 IQN 从主机连接到 LUN"。

下图显示了卷创建向导的第一页：



15. **CIFS** 设置：如果您选择了 CIFS 协议，请设置 CIFS 服务器。

字段	描述
DNS 主 IP 地址和辅助 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 服务器必须包含定位 CIFS 服务器将加入的域的 Active Directory LDAP 服务器和域控制器所需的服务位置记录 (SRV)。如果您正在配置 Google 管理的 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 域内指定组织单位 (OU) 的 Windows 帐户的名称和密码。
CIFS 服务器 NetBIOS 名称	AD 域中唯一的 CIFS 服务器名称。
组织单位	AD 域内与 CIFS 服务器关联的组织单位。默认值为 CN=Computers。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** 。https://cloud.google.com/managed-microsoft-ad/docs/manage-active-directory-objects#organizational_units["Google Cloud 文档：Google Managed Microsoft AD 中的组织单位"^]
DNS 域	Cloud Volumes ONTAP存储虚拟机 (SVM) 的 DNS 域。大多数情况下，该域与 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。如果您需要使用不同的地址配置 NTP 服务器，那么您应该使用 API。请参阅 "NetApp Console自动化文档"了解详情。请注意，只有在创建 CIFS 服务器时才能配置 NTP 服务器。创建 CIFS 服务器后，它不可配置。

16. 使用情况配置文件、磁盘类型和分层策略：选择是否要启用存储效率功能并更改卷分层策略（如果需要）。

    更多信息，请参阅"选择卷使用情况配置文件"，"数据分层概述" ， 和 "KB：CVO 支持哪些内联存储效率功能？ "

17. 审核并批准：审核并确认您的选择。
    a. 查看有关配置的详细信息。
    b. 点击*更多信息*查看有关支持和控制台将购买的 Google Cloud 资源的详细信息。
    c. 选中*我明白…*复选框。
    d. 单击“开始”。

结果

控制台部署Cloud Volumes ONTAP系统。您可以在*审核*页面上跟踪进度。

如果您在部署Cloud Volumes ONTAP系统时遇到任何问题，请查看失败消息。您也可以选择系统并单击*重新创建环境*。

如需更多帮助，请访问 "NetApp Cloud Volumes ONTAP支持"。

完成后

- 如果您配置了 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共享并创建文件。
- 如果要将配额应用于卷，请使用ONTAP系统管理器或ONTAP CLI。

  配额使您能够限制或跟踪用户、组或 qtree 使用的磁盘空间和文件数量。

部署流程完成后，请勿修改 Google Cloud 门户中系统生成的 Cloud Volumes ONTAP 配置，例如系统标签以及 Google Cloud 资源中设置的标签。对这些配置进行的任何更改都可能导致意外行为或数据丢失。

相关链接

- "在 Google Cloud 中规划Cloud Volumes ONTAP配置"

Google Cloud Platform 图像验证

了解如何在**Cloud Volumes ONTAP**中验证 **Google Cloud** 映像

Google Cloud 映像验证符合增强的NetApp安全要求。已经对生成图像的脚本进行了更改，以便使用专门为此任务生成的私钥对图像进行签名。您可以使用 Google Cloud 的签名摘要和公共证书来验证 Google Cloud 映像的完整性，该证书可通过以下方式下载 "国家安全局"针对特定版本。

Cloud Volumes ONTAP软件版本 9.13.0 或更高版本支持 Google Cloud 映像验证。

将 **Google Cloud** 映像转换为**Cloud Volumes ONTAP** 的原始格式

用于部署新实例、升级或在现有映像中使用的映像将通过以下方式与客户端共享 "NetApp支持站点 (NSS)"。已签名的摘要和证书可通过 NSS 门户下载。确保您下载的摘要和证书与NetApp支持共享的图像对应的正确版本。例如，9.13.0 图像将具有 9.13.0 签名摘要和 NSS 上可用的证书。

为什么需要这一步？

无法直接下载来自 Google Cloud 的图片。为了根据签名的摘要和证书验证图像，您需要有一种机制来比较两个文件并下载图像。为此，您必须将图像导出/转换为 disk.raw 格式，并将结果保存在 Google Cloud 的存储桶中。在此过程中，disk.raw 文件被压缩并压缩。

用户/服务帐户需要权限才能执行以下操作：

- 访问 Google 存储桶
- 写入 Google 存储桶
- 创建云构建作业（在导出过程中使用）
- 访问所需图像
- 创建导出图像任务

要验证图像，必须将其转换为 disk.raw 格式，然后下载。

使用 **Google Cloud** 命令行导出 **Google Cloud** 镜像

将图像导出到云存储的首选方法是使用 "gcloud compute images export 命令"。此命令获取提供的图像并将其转换为 disk.raw 文件，然后对其进行 tar 和 gzip 压缩。生成的文件保存在目标URL，然后可以下载进行验证。

用户/帐户必须具有访问和写入所需存储桶、导出图像和云构建（Google 用于导出图像）的权限才能执行此操作。

使用 **gcloud** 导出 **Google Cloud** 镜像

点击显示

```
$ gcloud compute images export \
    --destination-uri DESTINATION_URI \
    --image IMAGE_NAME

# For our example:
$ gcloud compute images export \
    --destination-uri gs://vsa-dev-bucket1/example-user-exportimage-
gcp-demo \
    --image example-user-20230120115139


## DEMO ##
# Step 1 - Optional: Checking access and listing objects in the
destination bucket
$ gsutil ls gs://example-user-export-image-bucket/

# Step 2 - Exporting the desired image to the bucket
$ gcloud compute images export --image example-user-export-image-demo
--destination-uri gs://example-user-export-image-bucket/export-
demo.tar.gz
Created [https://cloudbuild.googleapis.com/v1/projects/example-demo-
project/locations/us-central1/builds/xxxxxxxxxxxx].
Logs are available at [https://console.cloud.google.com/cloud-
build/builds;region=us-central1/xxxxxxxxxxxx?project=xxxxxxxxxxxx].
[image-export]: 2023-01-25T18:13:48Z Fetching image "example-user-
export-image-demo" from project "example-demo-project".
[image-export]: 2023-01-25T18:13:49Z Validating workflow
[image-export]: 2023-01-25T18:13:49Z Validating step "setup-disks"
[image-export]: 2023-01-25T18:13:49Z Validating step "image-export-
export-disk"
[image-export.image-export-export-disk]: 2023-01-25T18:13:49Z
Validating step "setup-disks"
[image-export.image-export-export-disk]: 2023-01-25T18:13:49Z
Validating step "run-image-export-export-disk"
[image-export.image-export-export-disk]: 2023-01-25T18:13:50Z
Validating step "wait-for-inst-image-export-export-disk"
[image-export.image-export-export-disk]: 2023-01-25T18:13:50Z
Validating step "copy-image-object"
[image-export.image-export-export-disk]: 2023-01-25T18:13:50Z
Validating step "delete-inst"
[image-export]: 2023-01-25T18:13:51Z Validation Complete
[image-export]: 2023-01-25T18:13:51Z Workflow Project: example-demo-
project
[image-export]: 2023-01-25T18:13:51Z Workflow Zone: us-central1-c
```

```
[image-export]: 2023-01-25T18:13:51Z Workflow GCSPath: gs://example-
demo-project-example-bkt-us/
[image-export]: 2023-01-25T18:13:51Z Example scratch path:
https://console.cloud.google.com/storage/browser/example-demo-project-
example-bkt-us/example-image-export-20230125-18:13:49-r88px
[image-export]: 2023-01-25T18:13:51Z Uploading sources
[image-export]: 2023-01-25T18:13:51Z Running workflow
[image-export]: 2023-01-25T18:13:51Z Running step "setup-disks"
(CreateDisks)
[image-export.setup-disks]: 2023-01-25T18:13:51Z CreateDisks: Creating
disk "disk-image-export-image-export-r88px".
[image-export]: 2023-01-25T18:14:02Z Step "setup-disks" (CreateDisks)
successfully finished.
[image-export]: 2023-01-25T18:14:02Z Running step "image-export-export-
disk" (IncludeWorkflow)
[image-export.image-export-export-disk]: 2023-01-25T18:14:02Z Running
step "setup-disks" (CreateDisks)
[image-export.image-export-export-disk.setup-disks]: 2023-01-
25T18:14:02Z CreateDisks: Creating disk "disk-image-export-export-disk-
image-export-image-export--r88px".
[image-export.image-export-export-disk]: 2023-01-25T18:14:02Z Step
"setup-disks" (CreateDisks) successfully finished.
[image-export.image-export-export-disk]: 2023-01-25T18:14:02Z Running
step "run-image-export-export-disk" (CreateInstances)
[image-export.image-export-export-disk.run-image-export-export-disk]:
2023-01-25T18:14:02Z CreateInstances: Creating instance "inst-image-
export-export-disk-image-export-image-export--r88px".
[image-export.image-export-export-disk]: 2023-01-25T18:14:08Z Step
"run-image-export-export-disk" (CreateInstances) successfully finished.
[image-export.image-export-export-disk.run-image-export-export-disk]:
2023-01-25T18:14:08Z CreateInstances: Streaming instance "inst-image-
export-export-disk-image-export-image-export--r88px" serial port 1
output to https://storage.cloud.google.com/example-demo-project-
example-bkt-us/example-image-export-20230125-18:13:49-r88px/logs/inst-
image-export-export-disk-image-export-image-export--r88px-serial-
port1.log
[image-export.image-export-export-disk]: 2023-01-25T18:14:08Z Running
step "wait-for-inst-image-export-export-disk" (WaitForInstancesSignal)
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:08Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
watching serial port 1, SuccessMatch: "ExportSuccess", FailureMatch:
["ExportFailed:"] (this is not an error), StatusMatch: "GCEExport:".
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
```

```
StatusMatch found: "GCEExport: <serial-output key:'source-size-gb'
value:'10'>"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Running export tool."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Disk /dev/sdb is 10 GiB, compressed size
will most likely be much smaller."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Beginning export process..."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Copying \"/dev/sdb\" to gs://example-
demo-project-example-bkt-us/example-image-export-20230125-18:13:49-
r88px/outs/image-export-export-disk.tar.gz."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Using \"/root/upload\" as the buffer
prefix, 1.0 GiB as the buffer size, and 4 as the number of workers."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Creating gzipped image of \"/dev/sdb\"."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Read 1.0 GiB of 10 GiB (212 MiB/sec),
total written size: 992 MiB (198 MiB/sec)"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:59Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Read 8.0 GiB of 10 GiB (237 MiB/sec),
total written size: 1.5 GiB (17 MiB/sec)"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Finished creating gzipped image of
\"/dev/sdb\" in 48.956433327s [213 MiB/s] with a compression ratio of
6."
```

```
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Finished export in  48.957347731s"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: <serial-output key:'target-size-gb'
value:'2'>"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
SuccessMatch found "ExportSuccess"
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Step
"wait-for-inst-image-export-export-disk" (WaitForInstancesSignal)
successfully finished.
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Running
step "copy-image-object" (CopyGCSObjects)
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Running
step "delete-inst" (DeleteResources)
[image-export.image-export-export-disk.delete-inst]: 2023-01-
25T18:15:19Z DeleteResources: Deleting instance "inst-image-export-
export-disk".
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Step
"copy-image-object" (CopyGCSObjects) successfully finished.
[image-export.image-export-export-disk]: 2023-01-25T18:15:34Z Step
"delete-inst" (DeleteResources) successfully finished.
[image-export]: 2023-01-25T18:15:34Z Step "image-export-export-disk"
(IncludeWorkflow) successfully finished.
[image-export]: 2023-01-25T18:15:34Z Serial-output value -> source-
size-gb:10
[image-export]: 2023-01-25T18:15:34Z Serial-output value -> target-
size-gb:2
[image-export]: 2023-01-25T18:15:34Z Workflow "image-export" cleaning
up (this may take up to 2 minutes).
[image-export]: 2023-01-25T18:15:35Z Workflow "image-export" finished
cleanup.

# Step 3 - Validating the image was successfully exported
$ gsutil ls gs://example-user-export-image-bucket/
gs://example-user-export-image-bucket/export-demo.tar.gz


# Step 4 - Download the exported image
$ gcloud storage cp gs://BUCKET_NAME/OBJECT_NAME SAVE_TO_LOCATION
```

```
$ gcloud storage cp gs://example-user-export-image-bucket/export-
demo.tar.gz CVO_GCP_Signed_Digest.tar.gz
Copying gs://example-user-export-image-bucket/export-demo.tar.gz to
file://CVO_GCP_Signed_Digest.tar.gz
  Completed files 1/1 | 1.5GiB/1.5GiB | 185.0MiB/s

Average throughput: 213.3MiB/s
$ ls -l
total 1565036
-rw-r--r-- 1 example-user example-user 1602589949 Jan 25 18:44
CVO_GCP_Signed_Digest.tar.gz
```

解压压缩文件

```
# Extracting files from the digest
$ tar -xf CVO_GCP_Signed_Digest.tar.gz
```

有关如何通过 Google Cloud 导出图像的更多信息，请参阅 "Google Cloud 文档：导出图像"。

图像签名验证

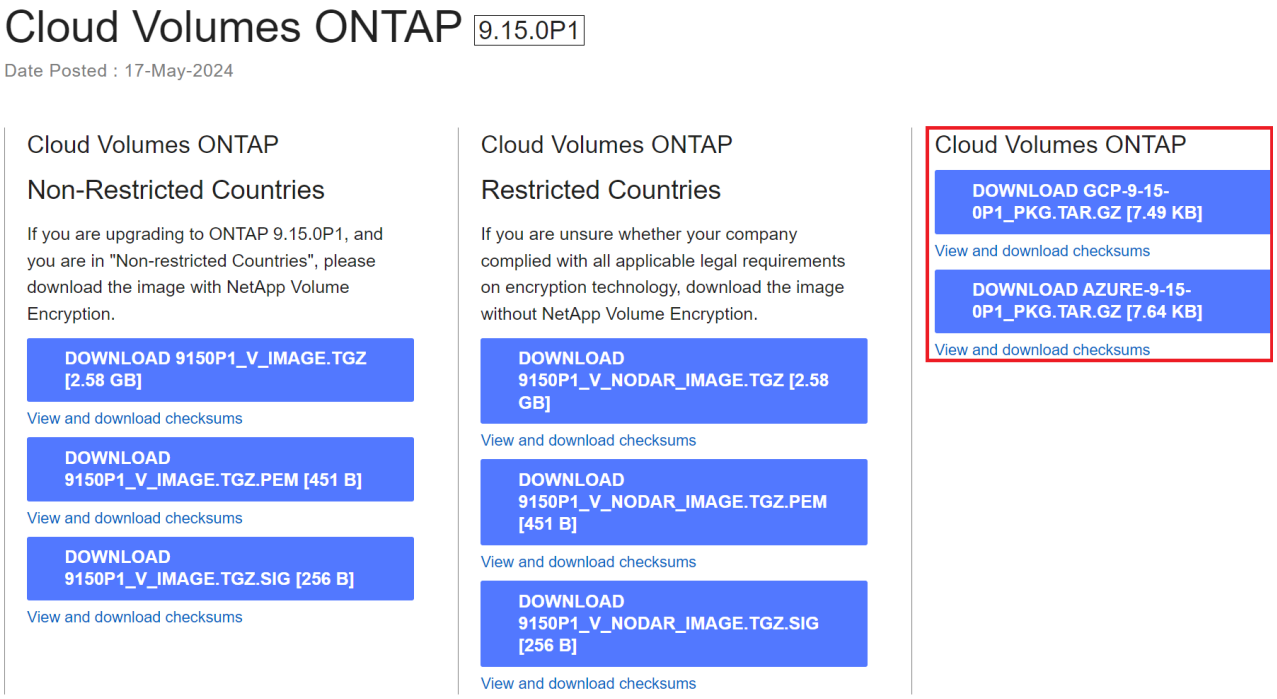
Cloud Volumes ONTAP的 Google Cloud 映像签名验证

要验证导出的 Google Cloud 签名映像，您必须从 NSS 下载映像摘要文件以验证 disk.raw 文件和摘要文件内容。

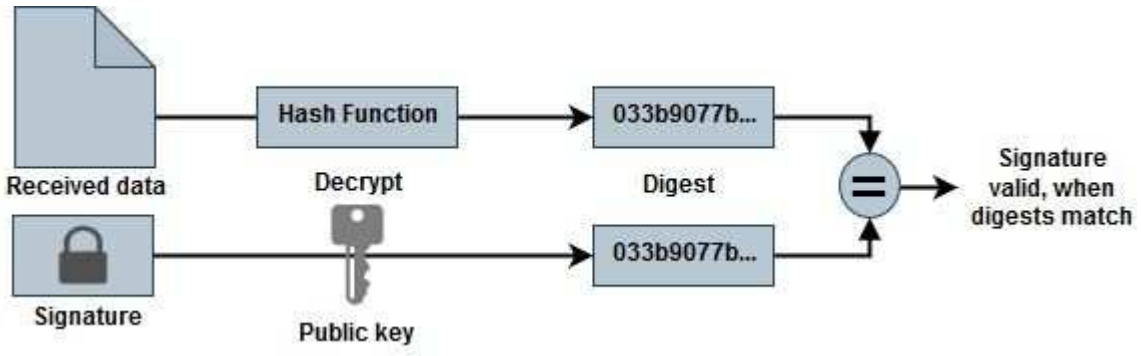
签名图像验证工作流程摘要

以下是 Google Cloud 签名图像验证工作流程的概述。

- 从 "国家安全局"，下载包含以下文件的 Google Cloud 存档：
  - 签名摘要（.sig）
  - 包含公钥的证书（.pem）
  - 证书链（.pem）



- 下载转换后的 disk.raw 文件
- 使用证书链验证证书
- 使用包含公钥的证书验证签名的摘要
  - 使用公钥解密签名的摘要，以提取图像文件的摘要
  - 创建下载的 disk.raw 文件的摘要
  - 比较两个摘要文件进行验证



使用 **OpenSSL** 验证**Cloud Volumes ONTAP**的 **Google Cloud** 映像 **disk.raw** 文件

您可以通过以下方式验证 Google Cloud 下载的 disk.raw 文件与摘要文件内容 "国家安全局"使用 OpenSSL。

用于验证图像的 OpenSSL 命令与 Linux、macOS 和 Windows 机器兼容。

步骤

1. 使用 OpenSSL 验证证书。

点击显示

```
# Step 1 - Optional, but recommended: Verify the certificate using
OpenSSL

# Step 1.1 - Copy the Certificate and certificate chain to a
directory
$ openssl version
LibreSSL 3.3.6
$ ls -l
total 48
-rw-r--r--@ 1 example-user  engr  8537 Jan 19 15:42 Certificate-
Chain-GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  engr  2365 Jan 19 15:42 Certificate-GCP-
CVO-20230119-0XXXXX.pem

# Step 1.2 - Get the OSCP URL
$ oscp_url=$(openssl x509 -noout -ocsp_uri -in <Certificate-
Chain.pem>)
$ oscp_url=$(openssl x509 -noout -ocsp_uri -in Certificate-Chain-
GCP-CVO-20230119-0XXXXX.pem)
$ echo $oscp_url
http://ocsp.entrust.net

# Step 1.3 - Generate an OCSP request for the certificate
$ openssl ocsp -issuer <Certificate-Chain.pem> -CAfile <Certificate-
Chain.pem> -cert <Certificate.pem> -reqout <request.der>
$ openssl ocsp -issuer Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem
-CAfile Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem -cert
Certificate-GCP-CVO-20230119-0XXXXX.pem -reqout req.der

# Step 1.4 - Optional: Check the new file "req.der" has been
generated
$ ls -l
total 56
-rw-r--r--@ 1 example-user  engr  8537 Jan 19 15:42 Certificate-
Chain-GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  engr  2365 Jan 19 15:42 Certificate-GCP-
CVO-20230119-0XXXXX.pem
-rw-r--r--  1 example-user  engr   120 Jan 19 16:50 req.der

# Step 1.5 - Connect to the OCSP Manager using openssl to send the
OCSP request
$ openssl ocsp -issuer <Certificate-Chain.pem> -CAfile <Certificate-
Chain.pem> -cert <Certificate.pem> -url ${ocsp_url} -resp_text
-respout <response.der>
```

```
$ openssl ocsp -issuer Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem
-CAfile Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem -cert
Certificate-GCP-CVO-20230119-0XXXXX.pem  -url ${ocsp_url} -resp_text
-respout resp.der
OCSP Response Data:
    OCSP Response Status: successful (0x0)
    Response Type: Basic OCSP Response
    Version: 1 (0x0)
    Responder Id: C = US, O = "Entrust, Inc.", CN = Entrust Extended
Validation Code Signing CA - EVCS2
    Produced At: Jan 19 15:14:00 2023 GMT
    Responses:
    Certificate ID:
      Hash Algorithm: sha1
      Issuer Name Hash: 69FA640329AB84E27220FE0927647B8194B91F2A
      Issuer Key Hash: CE894F8251AA15A28462CA312361D261FBF8FE78
      Serial Number: 5994B3D01D26D594BD1D0FA7098C6FF5
    Cert Status: good
    This Update: Jan 19 15:00:00 2023 GMT
    Next Update: Jan 26 14:59:59 2023 GMT

    Signature Algorithm: sha512WithRSAEncryption
         0b:b6:61:e4:03:5f:98:6f:10:1c:9a:f7:5f:6f:c7:e3:f4:72:
         f2:30:f4:86:88:9a:b9:ba:1e:d6:f6:47:af:dc:ea:e4:cd:31:
         af:e3:7a:20:35:9e:60:db:28:9c:7f:2e:17:7b:a5:11:40:4f:
         1e:72:f7:f8:ef:e3:23:43:1b:bb:28:1a:6f:c6:9c:c5:0c:14:
         d3:5d:bd:9b:6b:28:fb:94:5e:8a:ef:40:20:72:a4:41:df:55:
         cf:f3:db:1b:39:e0:30:63:c9:c7:1f:38:7e:7f:ec:f4:25:7b:
         1e:95:4c:70:6c:83:17:c3:db:b2:47:e1:38:53:ee:0a:55:c0:
         15:6a:82:20:b2:ea:59:eb:9c:ea:7e:97:aa:50:d7:bc:28:60:
         8c:d4:21:92:1c:13:19:b4:e0:66:cb:59:ed:2e:f8:dc:7b:49:
         e3:40:f2:b6:dc:d7:2d:2e:dd:21:82:07:bb:3a:55:99:f7:59:
         5d:4a:4d:ca:e7:8f:1c:d3:9a:3f:17:7b:7a:c4:57:b2:57:a8:
         b4:c0:a5:02:bd:59:9c:50:32:ff:16:b1:65:3a:9c:8c:70:3b:
         9e:be:bc:4f:f9:86:97:b1:62:3c:b2:a9:46:08:be:6b:1b:3c:
         24:14:59:28:c6:ae:e8:d5:64:b2:f8:cc:28:24:5c:b2:c8:d8:
         5a:af:9d:55:48:96:f6:3e:c6:bf:a6:0c:a4:c0:ab:d6:57:03:
         2b:72:43:b0:6a:9f:52:ef:43:bb:14:6a:ce:66:cc:6c:4e:66:
         17:20:a3:64:e0:c6:d1:82:0a:d7:41:8a:cc:17:fd:21:b5:c6:
         d2:3a:af:55:2e:2a:b8:c7:21:41:69:e1:44:ab:a1:dd:df:6d:
         15:99:90:cc:a0:74:1e:e5:2e:07:3f:50:e6:72:a6:b9:ae:fc:
         44:15:eb:81:3d:1a:f8:17:b6:0b:ff:05:76:9d:30:06:40:72:
         cf:d5:c4:6f:8b:c9:14:76:09:6b:3d:6a:70:2c:5a:c4:51:92:
         e5:cd:84:b6:f9:d9:d5:bc:8d:72:b7:7c:13:9c:41:89:a8:97:
         6f:4a:11:5f:8f:b6:c9:b5:df:00:7e:97:20:e7:29:2e:2b:12:
         77:dc:e2:63:48:87:42:49:1d:fc:d0:94:a8:8d:18:f9:07:85:
```

```
          e4:d0:3e:9a:4a:d7:d5:d0:02:51:c3:51:1c:73:12:96:2d:75:
          22:83:a6:70:5a:4a:2b:f2:98:d9:ae:1b:57:53:3d:3b:58:82:
          38:fc:fa:cb:57:43:3f:3e:7e:e0:6d:5b:d6:fc:67:7e:07:7e:
          fb:a3:76:43:26:8f:d1:42:d6:a6:33:4e:9e:e0:a0:51:b4:c4:
          bc:e3:10:0d:bf:23:6c:4b
WARNING: no nonce in response
Response Verify OK
Certificate-GCP-CVO-20230119-0XXXXX.pem: good
    This Update: Jan 19 15:00:00 2023 GMT
    Next Update: Jan 26 14:59:59 2023 GMT

# Step 1.5 - Optional: Check the response file "response.der" has
been generated. Verify its contents.
$ ls -l
total 64
-rw-r--r--@ 1 example-user  engr  8537 Jan 19 15:42 Certificate-
Chain-GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  engr  2365 Jan 19 15:42 Certificate-GCP-
CVO-20230119-0XXXXX.pem
-rw-r--r--  1 example-user  engr   120 Jan 19 16:50 req.der
-rw-r--r--  1 example-user  engr   806 Jan 19 16:51 resp.der

# Step 1.6 - Verify the chain of trust and expiration dates against
the local host
$ openssl version -d
OPENSSLDIR: "/private/etc/ssl"
$ OPENSSLDIR=$(openssl version -d | cut -d '"' -f2)
$ echo $OPENSSLDIR
/private/etc/ssl

$ openssl verify -untrusted <Certificate-Chain.pem> -CApath <OpenSSL
dir> <Certificate.pem>
$ openssl verify -untrusted Certificate-Chain-GCP-CVO-20230119-
0XXXXX.pem -CApath ${OPENSSLDIR} Certificate-GCP-CVO-20230119-
0XXXXX.pem
Certificate-GCP-CVO-20230119-0XXXXX.pem: OK
```

2. 将下载的 disk.raw 文件、签名和证书放在一个目录中。
3. 使用 OpenSSL 从证书中提取公钥。
4. 使用提取的公钥解密签名并验证下载的 disk.raw 文件的内容。

点击显示

```
# Step 1 - Place the downloaded disk.raw, the signature and the
certificates in a directory
$ ls -l
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-Chain-
GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-GCP-CVO-
20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 GCP_CVO_20230119-
XXXXXX_digest.sig
-rw-r--r--@ 1 example-user  staff  Jan 19 16:39 disk.raw

# Step 2 - Extract the public key from the certificate
$ openssl x509 -pubkey -noout -in (certificate.pem) >
(public_key.pem)
$ openssl x509 -pubkey -noout -in Certificate-GCP-CVO-20230119-
0XXXXX.pem > CVO-GCP-pubkey.pem

$ ls -l
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-Chain-
GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-GCP-CVO-
20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 17:02 CVO-GCP-pubkey.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 GCP_CVO_20230119-
XXXXXX_digest.sig
-rw-r--r--@ 1 example-user  staff  Jan 19 16:39 disk.raw

# Step 3 - Decrypt the signature using the extracted public key and
verify the contents of the downloaded disk.raw
$ openssl dgst -verify (public_key) -keyform PEM -sha256 -signature
(signed digest) -binary (downloaded or obtained disk.raw)
$ openssl dgst -verify CVO-GCP-pubkey.pem -keyform PEM -sha256
-signature GCP_CVO_20230119-XXXXXX_digest.sig -binary disk.raw
Verified OK

# A failed response would look like this
$ openssl dgst -verify CVO-GCP-pubkey.pem -keyform PEM -sha256
-signature GCP_CVO_20230119-XXXXXX_digest.sig -binary
../sample_file.txt
Verification Failure
```

使用Cloud Volumes ONTAP

许可证管理

管理Cloud Volumes ONTAP基于容量的许可

从NetApp Console管理基于容量的许可证，以确保您的NetApp帐户具有足够的容量用于您的Cloud Volumes ONTAP系统。

_基于容量的许可证_使您能够按 TiB 容量支付Cloud Volumes ONTAP 的费用。

您可以从NetApp Console管理基于容量的Cloud Volumes ONTAP许可证。

> 虽然控制台中管理的产品和服务的实际使用情况和计量始终以 GiB 和 TiB 计算，但 GB/GiB 和 TB/TiB 这两个术语可互换使用。这反映在云市场列表、报价、列表描述和其他支持文档中

"了解有关Cloud Volumes ONTAP许可证的更多信息" 。

如何将许可证添加到NetApp Console

从NetApp销售代表处购买许可证后， 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，控制台会自动查询 NetApp 的许可服务，以获取与您的NetApp支持站点帐户相关的许可证的详细信息。如果没有错误，它会添加许可证。

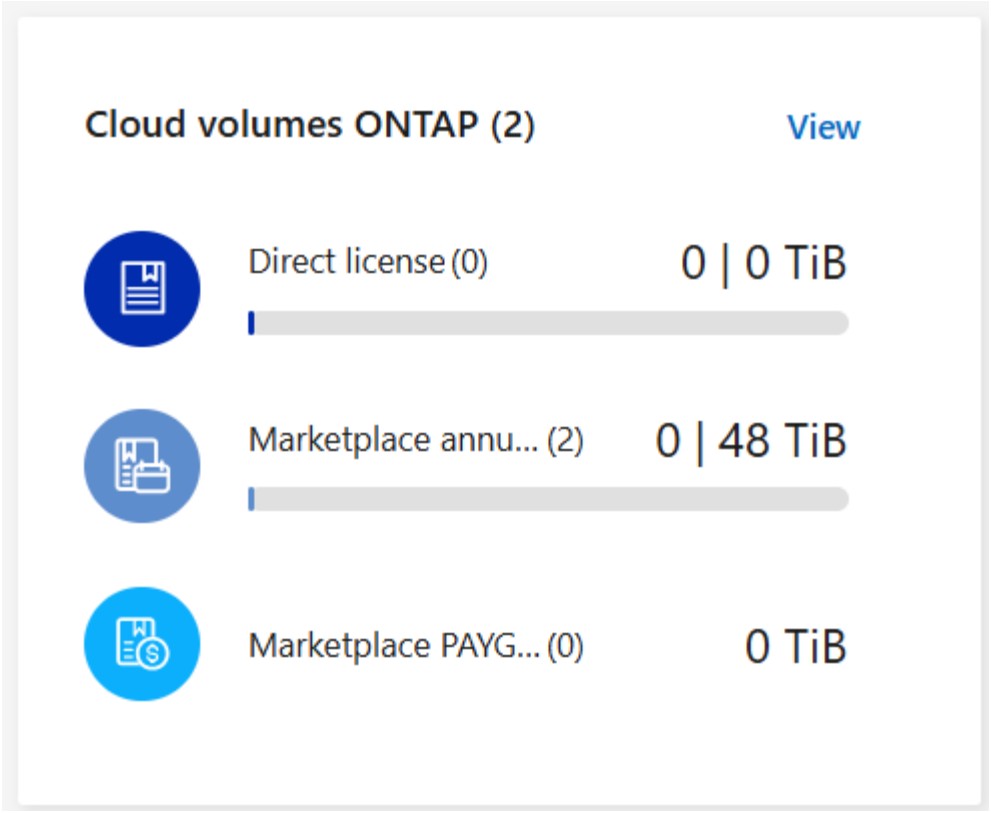
如果控制台无法添加许可证，则需要手动添加它们。例如，如果控制台代理安装在没有互联网访问的位置，则您需要自己添加许可证。 "了解如何将购买的许可证添加到您的帐户" 。

查看您账户中已消耗的容量

控制台显示您帐户中消耗的总容量以及按许可包消耗的容量。这可以帮助您了解收费方式以及是否需要购买额外的容量。

步骤

1. 从左侧导航窗格中，选择“管理”> “Licenses and subscriptions”。
2. 在“概览”选项卡上， Cloud Volumes ONTAP图块显示为您的帐户配置的当前容量。



- _直接许可证_是您的NetApp帐户中所有Cloud Volumes ONTAP系统的总配置容量。收费基于每个卷的配置大小，而不考虑卷内的本地、已用、存储或有效空间。
- _年度合同_是您从NetApp购买的总许可容量（自带许可证 (BYOL) 或市场合同）。
- *PAYGO* 是使用云市场订阅的总配置容量。仅当消耗的容量高于许可容量或控制台中没有可用的 BYOL 许可证时，才使用 PAYGO 收费。

3. 选择“查看”以查看每个许可包所消耗的容量。
4. 选择“许可证”选项卡查看您购买的每个包许可证的详细信息。

   为了更好地了解 Essentials 套件所显示的容量，您应该熟悉充电的工作原理。 "了解 Essentials 套餐的收费" 。

5. 选择“订阅”选项卡来查看按许可证消费模式消耗的容量。此选项卡包括 PAYGO 和年度合同许可证。

   您只会看到与您当前正在查看的组织相关的订阅。

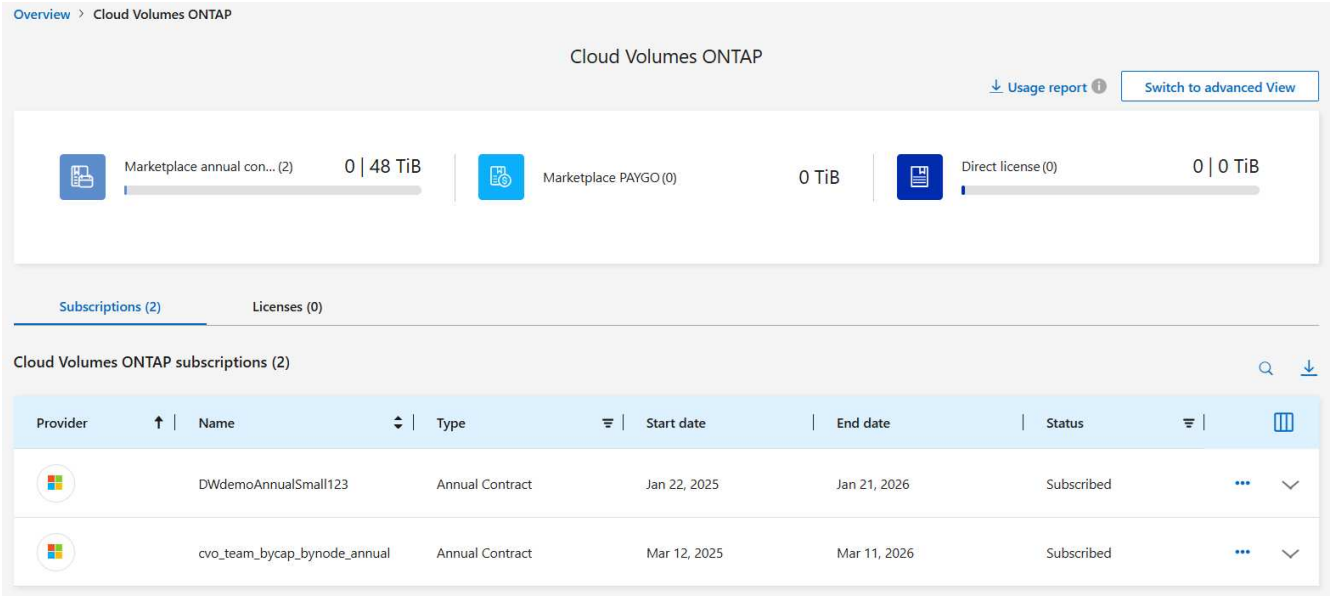
6. 当您查看有关订阅的信息时，您可以与表格中的详细信息进行交互。展开一行可以查看更多详细信息。
   - 选择|||选择表中显示的列。请注意，“期限”和“自动续订”列默认不会出现。自动续订列仅显示 Azure 合同的续订信息。

查看包裹详情

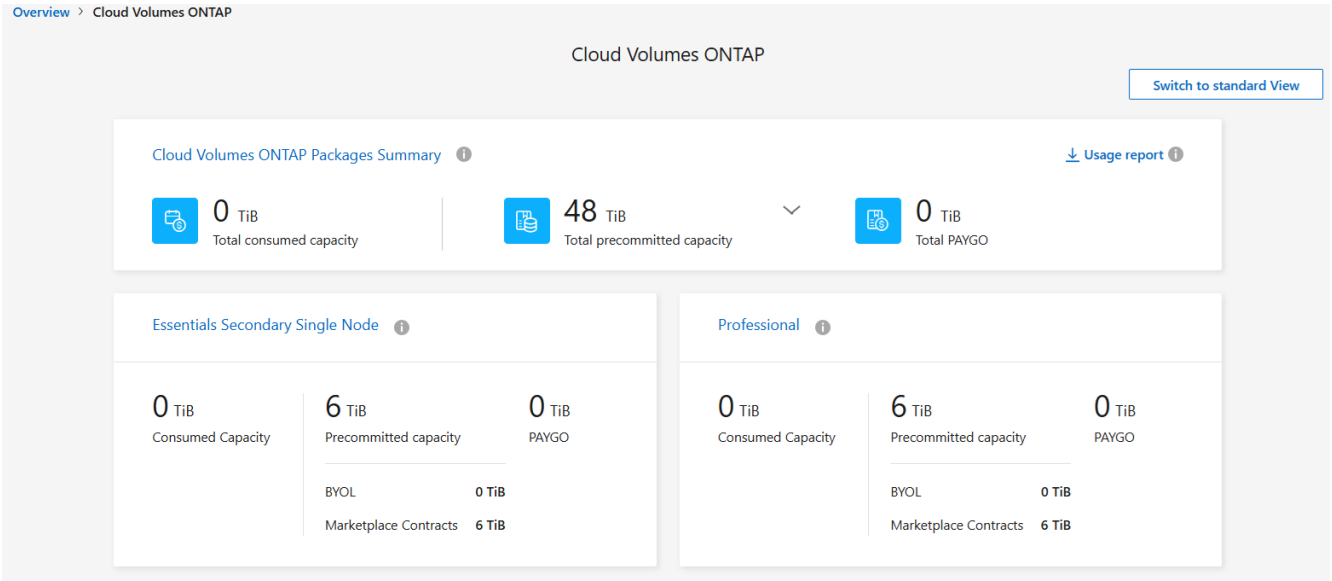
您可以通过在Cloud Volumes ONTAP页面上切换到传统模式来查看每个包使用的容量的详细信息。

1. 从左侧导航窗格中，选择“管理”> “Licenses and subscriptions”。
2. 在“概览”选项卡上， Cloud Volumes ONTAP图块显示为您的帐户配置的当前容量。

3. 选择“查看”以查看每个许可包的配置容量。
4. 选择*切换到高级视图*。



5. 查看您想要查看的包裹的详细信息。



改变充电方式

基于容量的许可以_包_的形式提供。创建Cloud Volumes ONTAP系统时，您可以根据业务需求从多个许可包中进行选择。如果您在创建系统后需求发生变化，您可以随时更改套餐。例如，您可以从 Essentials 包更改为 Professional 包。

"了解有关基于容量的许可包的更多信息" 。

关于此任务

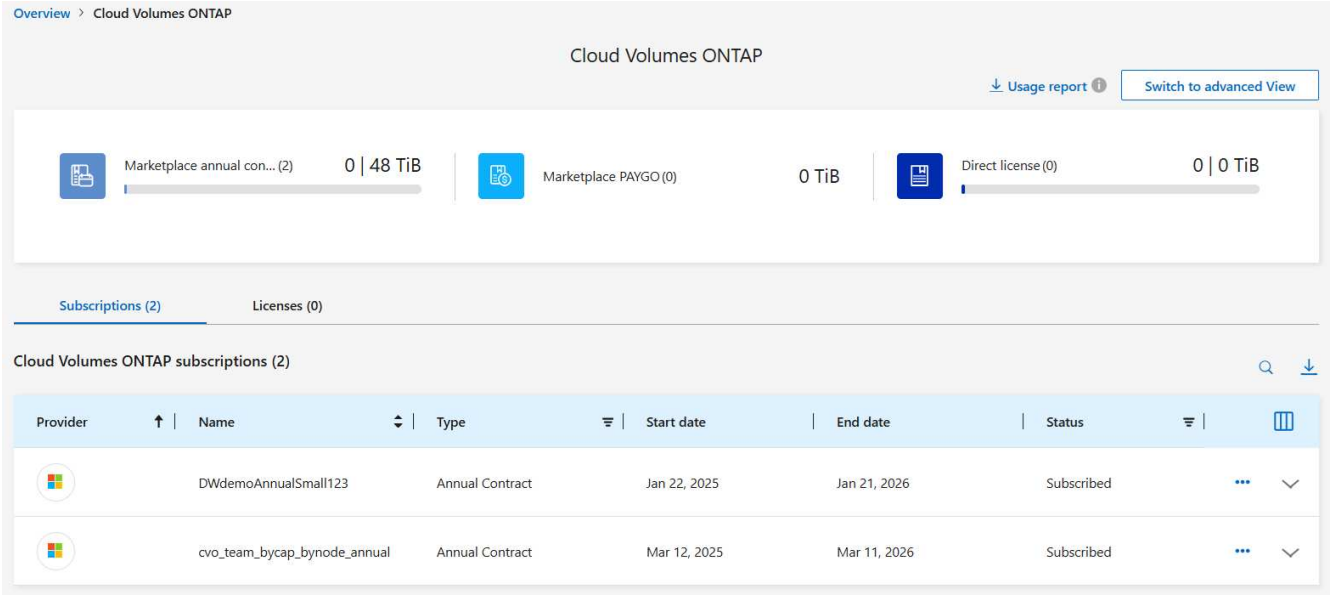
- 更改收费方式不会影响您是通过从NetApp (BYOL) 购买的许可证还是通过云提供商的市场即用即付 (PAYGO) 订阅进行收费。

控制台始终会先尝试根据许可证收费。如果没有许可证，则会根据市场订阅收费。您不必将 BYOL 订阅转换为市场订阅，反之亦然。

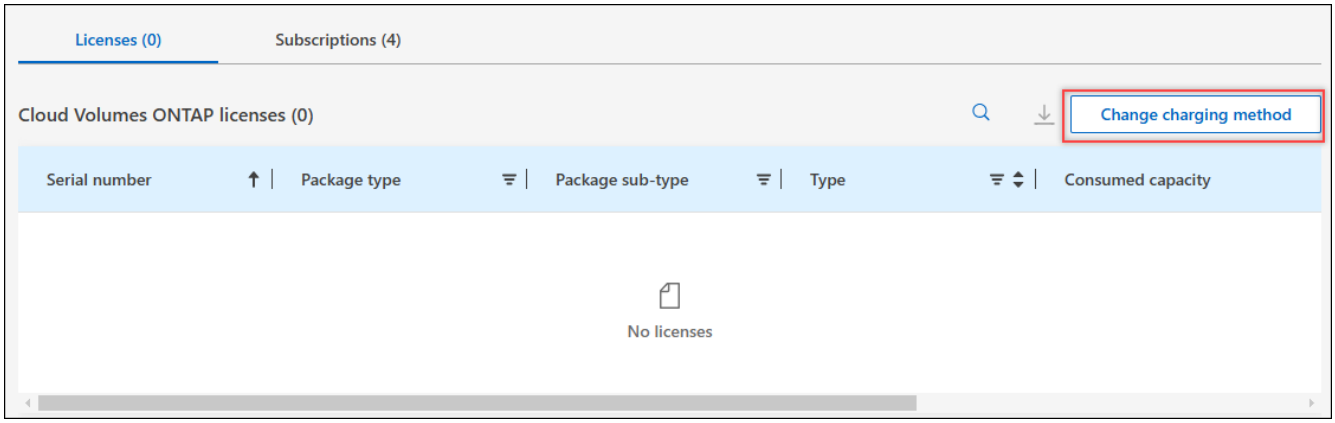
- 如果您拥有来自云提供商市场的私人优惠或合同，则更改为合同中未包含的收费方式将导致对 BYOL（如果您从NetApp购买了许可证）或 PAYGO 收费。

步骤

1. 从左侧导航窗格中，选择“管理”> “Licenses and subscriptions”。
2. 选择“概览”选项卡。
3. 在Cloud Volumes ONTAP图块上，选择 查看。
4. 选择*切换到高级视图*。



5. 向下滚动到*基于容量的许可证*表并选择*更改收费方式*。



6. 在*更改收费方式*弹出窗口中，选择一个Cloud Volumes ONTAP系统，选择新的收费方式，然后确认您了解更改套餐类型将影响服务费用。
7. 选择*更改充电方式*。

下载使用情况报告

您可以从控制台下载四份使用情况报告。这些使用情况报告提供您的订阅的容量详细信息，并告诉您如何为Cloud Volumes ONTAP订阅中的资源付费。可下载的报告捕获某个时间点的数据，并且可以轻松地与他人共享。

以下报告可供下载。显示的容量值以 TiB 为单位。

- 高级用法：此报告包含以下信息：
  - 总消耗容量
  - 预先承诺的总容量
  - 总 BYOL 容量
  - 市场合同总容量
  - PAYGO 总容量
- * Cloud Volumes ONTAP软件包使用情况*：此报告包含每个软件包的以下信息：
  - 总消耗容量
  - 预先承诺的总容量
  - 总 BYOL 容量
  - 市场合同总容量
  - PAYGO 总容量
- 存储虚拟机使用情况：此报告显示收费容量在Cloud Volumes ONTAP系统和存储虚拟机 (SVM) 之间的分配情况。此信息仅在报告中提供。它包含以下信息：
  - 系统 ID 和名称（显示为 UUID）
  - 云
  - NetApp帐户 ID
  - 系统配置
  - SVM 名称
  - 预配置容量
  - 充电容量汇总
  - 市场计费条款
  - Cloud Volumes ONTAP软件包或功能
  - 收费 SaaS 市场订阅名称
  - 收费 SaaS 市场订阅 ID

- 工作负载类型

- 卷使用情况：此报告显示Cloud Volumes ONTAP系统中如何按卷细分收费容量。控制台中的任何屏幕上均不显示此信息。它包括以下信息：
  - 系统 ID 和名称（显示为 UUID）
  - SVN 名称
  - Volume ID
  - 卷类型
  - 卷配置容量

    FlexClone卷不包含在此报告中，因为这些类型的卷不会产生费用。

步骤

1. 从左侧导航窗格中，选择“管理”> “Licenses and subscriptions”。
2. 在*概览*选项卡上，从Cloud Volumes ONTAP图块中选择*查看*。
3. 选择*使用情况报告*。

   使用情况报告下载。

4. 打开下载的文件以访问报告。

通过NetApp Console管理Cloud Volumes ONTAP 的Keystone订阅

通过启用与Cloud Volumes ONTAP一起使用的订阅并请求更改订阅服务级别的承诺容量，在NetApp Console中管理您的Keystone订阅。请求服务级别的额外容量可为Cloud Volumes ONTAP系统提供更多存储空间。

NetApp Keystone是一种灵活的按需付费订阅服务，可为喜欢 OpEx 而非 CapEx 或租赁的客户提供混合云体验。

"了解有关Keystone的更多信息"

授权您的帐户

您需要先联系NetApp授权您的控制台帐户使用Keystone订阅，然后才能在控制台中使用和管理Keystone订阅。

步骤

1. 从NetApp Console菜单中，选择“管理 >Licenses and subscriptions”。
2. 选择* Keystone订阅*。
3. 如果您看到“欢迎使用NetApp Keystone”页面，请向页面上列出的地址发送电子邮件。

   NetApp代表将通过授权您的帐户访问订阅来处理您的请求。

4. 返回“Keystone订阅”选项卡查看您的订阅。

链接订阅

在NetApp授权您的帐户后，您可以链接Keystone订阅以用于Cloud Volumes ONTAP。此操作使用户能够选择订阅作为新Cloud Volumes ONTAP系统的收费方式。

步骤

1. 从NetApp Console菜单中，选择“管理 >Licenses and subscriptions”。
2. 选择* Keystone订阅*。
3. 对于您想要链接的订阅，单击 ••• 并选择*链接*。

结果

订阅现已链接到您的控制台组织或帐户，并可在创建Cloud Volumes ONTAP工作环境时进行选择。

请求更多或更少的承诺容量

如果您想要更改订阅服务级别的承诺容量，您可以直接从控制台向NetApp发送请求。请求服务级别的额外容量可为Cloud Volumes ONTAP系统提供更多存储空间。

步骤

1. 从NetApp Console菜单中，选择“管理 >Licenses and subscriptions”。
2. 选择* Keystone订阅*。
3. 对于要调整容量的订阅，单击 ••• 并选择*查看详细信息和编辑*。
4. 输入一个或多个订阅所请求的承诺容量。
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

您的请求将在 NetApp 系统中创建一张票以供处理。

监控使用情况

Digital Advisor仪表板使您能够监控Keystone订阅使用情况并生成报告。

"了解有关监控订阅使用情况的更多信息"

取消订阅链接

如果您不再想将Keystone订阅与控制台一起使用，您可以取消订阅链接。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NetApp Console菜单中，选择“管理 >Licenses and subscriptions”。
2. 选择* Keystone*。
3. 对于要取消链接的订阅，点击 ••• 并选择*取消链接*。

结果

该订阅已与您的控制台组织或帐户取消链接，并且在创建Cloud Volumes ONTAP工作环境时不再可供选择。

管理Cloud Volumes ONTAP 的基于节点的许可

在NetApp Console中管理基于节点的许可证，以确保每个Cloud Volumes ONTAP系统都具有所需容量的有效许可证。

_基于节点的许可证_是上一代许可模型（不适用于新客户）：

- 从NetApp购买自带许可证 (BYOL)
- 从云提供商的市场购买按小时付费 (PAYGO) 订阅

您可以从NetApp Console管理基于节点的Cloud Volumes ONTAP许可证。

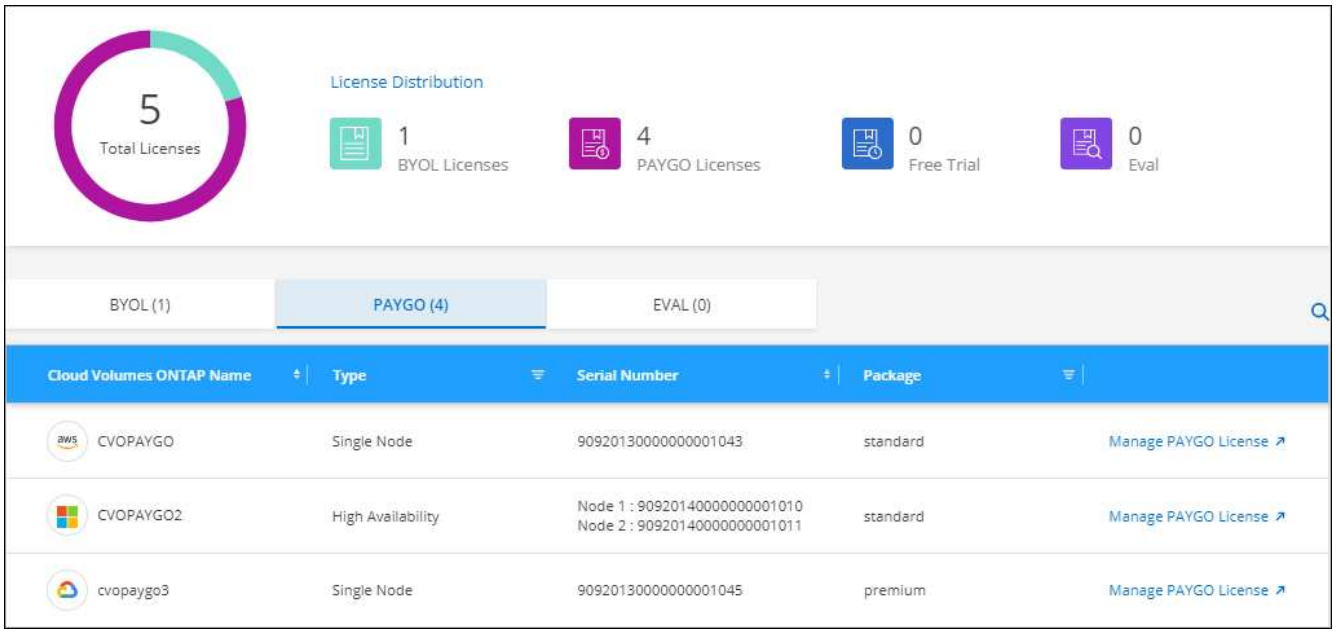
"了解有关Cloud Volumes ONTAP许可证的更多信息" 。

管理 PAYGO 许可证

Licenses and subscriptions菜单，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. 从左侧导航窗格中，选择“管理”> “Licenses and subscriptions”。
2. 选择“概览”选项卡。
3. 在Cloud Volumes ONTAP图块上，选择 查看。
4. 从下拉菜单中选择*基于节点的许可证*。
5. 点击*PAYGO*。
6. 在表格中查看有关每个 PAYGO 许可证的详细信息。



7. 如果需要，单击*管理 PAYGO 许可证*来更改 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您直接从NetApp购买的许可证。

已限制 BYOL 许可证的购买、延期和续订。有关更多信息，请参阅 "Cloud Volumes ONTAP的 BYOL 许可可用性受限" 。

添加未分配的许可证

将基于节点的许可证添加到控制台，以便您在创建新的Cloud Volumes ONTAP系统时可以选择该许可证。控制台将这些许可证标识为_未分配_。

步骤

1. 从左侧导航窗格中，选择“管理”> “Licenses and subscriptions”。
2. 选择“概览”选项卡。
3. 在Cloud Volumes ONTAP图块上，选择 查看。
4. 从下拉菜单中选择*基于节点的许可证*。
5. 单击“未分配”。
6. 单击“添加未分配的许可证”。
7. 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，请参阅下面的部分。

8. 单击“添加许可证”。

结果

控制台添加许可证。在您将许可证与新的Cloud Volumes ONTAP系统关联之前，该许可证将被标识为未分配。此后，许可证将移至“Licenses and subscriptions”中的“BYOL”选项卡。

交换未分配的基于节点的许可证

如果您有未分配的基于节点的Cloud Volumes ONTAP许可证且尚未使用，则可以将其转换为NetApp Backup and Recovery许可证、 NetApp Data Classification许可证或NetApp Cloud Tiering许可证来交换该许可证。

交换许可证将撤销Cloud Volumes ONTAP许可证并为该服务创建等值美元的许可证：

- Cloud Volumes ONTAP HA 对的许可转换为 51 TiB 直接许可证
- Cloud Volumes ONTAP单节点许可转换为 32 TiB 直接许可证

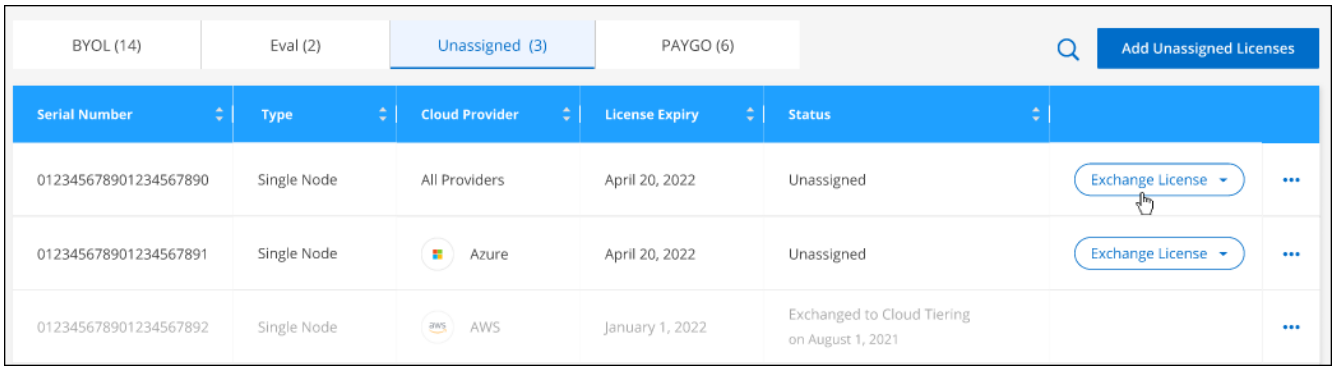
转换后的许可证的到期日期与Cloud Volumes ONTAP许可证相同。

"查看如何交换基于节点的许可证的演练。"

步骤

1. 从左侧导航窗格中，选择“管理”> “Licenses and subscriptions”。
2. 选择“概览”选项卡。

3. 在Cloud Volumes ONTAP图块上，选择 查看。
4. 从下拉菜单中选择*基于节点的许可证*。
5. 单击“未分配”。
6. 单击“交换许可证”。



7. 选择您想要交换许可证的服务。
8. 如果出现提示，请为 HA 对选择一个额外的许可证。
9. 阅读法律同意并点击*同意*。

结果

控制台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”选项卡中查看新的许可证。

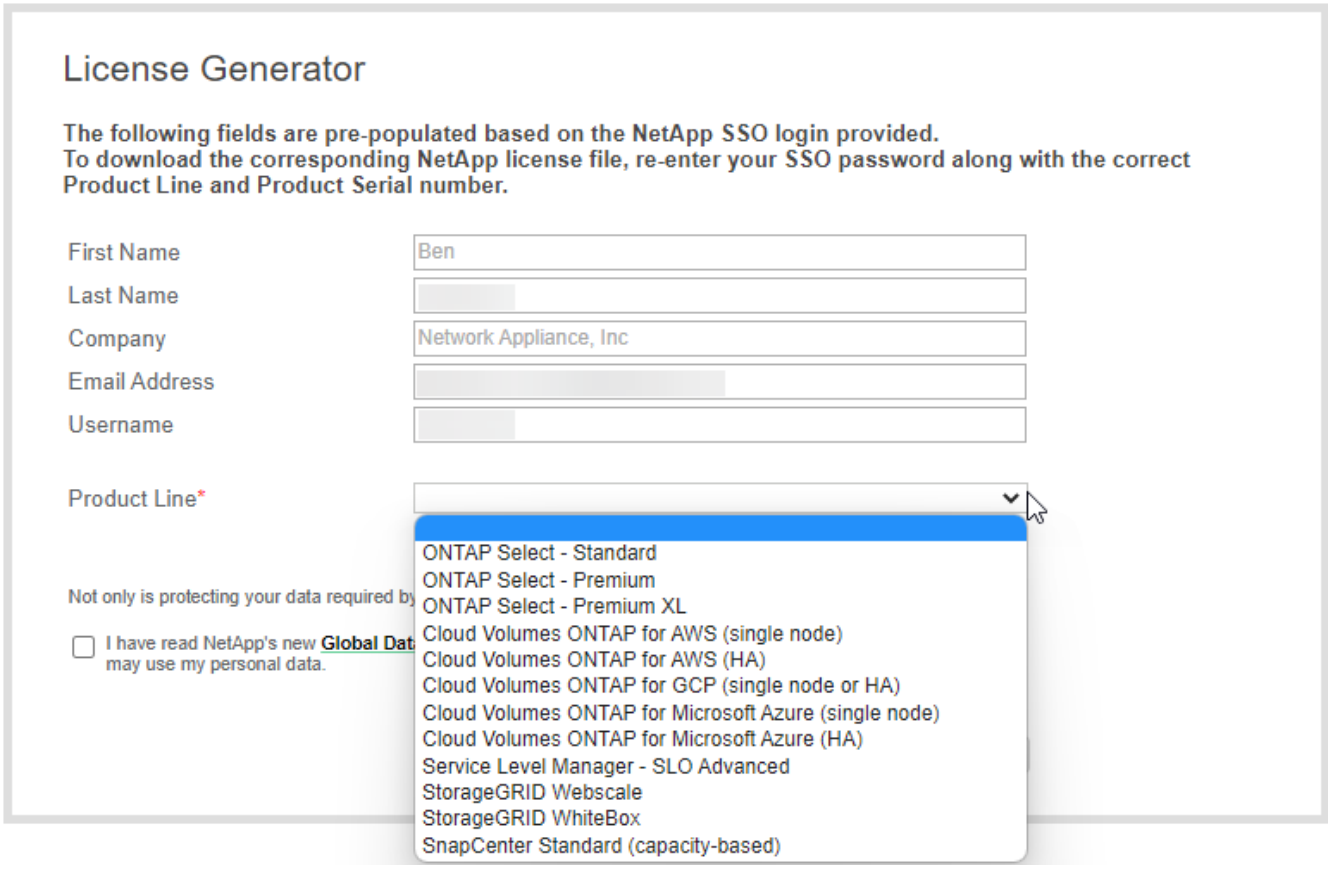
获取系统许可证文件

在大多数情况下，控制台可以使用您的NetApp支持站点帐户自动获取您的许可证文件。但如果不能，那么您将需要手动上传许可证文件。如果您没有许可证文件，您可以从 netapp.com 获取。

步骤

1. 前往 "NetApp许可证文件生成器"并使用您的NetApp支持站点凭据登录。
2. 输入您的密码，选择您的产品，输入序列号，确认您已阅读并接受隐私政策，然后单击*提交*。

   例子



3. 选择您是否希望通过电子邮件或直接下载接收 serialnumber.NLF JSON 文件。

更新系统许可证

当您通过联系NetApp代表续订 BYOL 订阅时，控制台会自动从NetApp获取新许可证并将其安装在Cloud Volumes ONTAP系统上。如果控制台无法通过安全的互联网连接访问许可证文件，您可以自行获取该文件，然后手动上传该文件。

步骤

1. 从左侧导航窗格中，选择“管理”> “Licenses and subscriptions”。
2. 选择“概览”选项卡。
3. 在Cloud Volumes ONTAP图块上，选择 查看。
4. 从下拉菜单中选择*基于节点的许可证*。
5. 在 **BYOL** 选项卡中，展开Cloud Volumes ONTAP系统的详细信息。
6. 单击系统许可证旁边的操作菜单，然后选择*更新许可证*。
7. 上传许可证文件（如果您有 HA 对，则上传多个文件）。
8. 单击“更新许可证”。

结果

控制台更新Cloud Volumes ONTAP系统上的许可证。

您可以为Cloud Volumes ONTAP BYOL 系统购买额外的容量许可证，以分配超过 BYOL 系统许可证提供的 368 TiB 的容量。例如，您可以购买一个额外的许可证容量，为Cloud Volumes ONTAP分配最多 736 TiB 的容量。或者您可以购买三个额外的容量许可证以获得高达 1.4 PiB。

可以为单节点系统或 HA 对购买的许可证数量是无限的。

添加容量许可证

通过控制台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. 从左侧导航窗格中，选择“管理”> “Licenses and subscriptions”。
2. 选择“概览”选项卡。
3. 在Cloud Volumes ONTAP图块上，选择 查看。
4. 从下拉菜单中选择*基于节点的许可证*。
5. 在 **BYOL** 选项卡中，展开Cloud Volumes ONTAP系统的详细信息。
6. 单击“添加容量许可证”。
7. 输入序列号或上传许可证文件（如果您有 HA 对，则上传文件）。
8. 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，则需要在控制台中更新许可证。

步骤

1. 从左侧导航窗格中，选择“管理”> “Licenses and subscriptions”。
2. 选择“概览”选项卡。
3. 在Cloud Volumes ONTAP图块上，选择 查看。
4. 从下拉菜单中选择*基于节点的许可证*。
5. 在 **BYOL** 选项卡中，展开Cloud Volumes ONTAP系统的详细信息。
6. 单击容量许可证旁边的操作菜单，然后选择*更新许可证*。
7. 上传许可证文件（如果您有 HA 对，则上传多个文件）。
8. 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，那么您可以随时将其删除。

步骤

1. 从左侧导航窗格中，选择“管理”> “Licenses and subscriptions”。

2. 选择“概览”选项卡。
3. 在Cloud Volumes ONTAP图块上，选择 查看。
4. 从下拉菜单中选择*基于节点的许可证*。
5. 在 **BYOL** 选项卡中，展开Cloud Volumes ONTAP系统的详细信息。
6. 单击容量许可证旁边的操作菜单，然后选择*删除许可证*。
7. 单击“删除”。

PAYGO 和 **BYOL** 之间的变化

不支持将系统从 PAYGO 按节点许可转换为 BYOL 按节点许可（反之亦然）。如果您想在按使用量付费订阅和 BYOL 订阅之间切换，那么您需要部署一个新系统并将数据从现有系统复制到新系统。

步骤

1. 创建一个新的Cloud Volumes ONTAP系统。
2. 对于需要复制的每个卷，在系统之间设置一次性数据复制。

   "了解如何在系统之间复制数据"

3. 通过删除原始系统来终止不再需要的Cloud Volumes ONTAP系统。

   "了解如何删除Cloud Volumes ONTAP系统" 。

相关链接

关联："基于节点的许可证的可用性终止" "将基于节点的许可证转换为基于容量的许可证"

卷和 LUN 管理

在Cloud Volumes ONTAP系统上创建FlexVol volume

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

您可以通过多种方式创建新卷：

- 指定新卷的详细信息，并让控制台为您处理底层数据聚合。了解更多
- 在您选择的数据聚合上创建卷。了解更多
- 在 HA 配置中的第二个节点上创建卷。了解更多

开始之前

关于卷配置的一些注意事项：

- 当您创建 iSCSI 卷时，控制台会自动为您创建一个 LUN。我们通过为每个卷创建一个 LUN 来简化操作，因此无需进行任何管理。创建卷后，"使用 IQN 从主机连接到 LUN" 。
- 您可以从ONTAP系统管理器或ONTAP CLI 创建其他 LUN。

- 如果您想在 AWS 中使用 CIFS，则必须设置 DNS 和 Active Directory。有关详细信息，请参阅"Cloud Volumes ONTAP for AWS 的网络要求"。
- 如果您的Cloud Volumes ONTAP配置支持 Amazon EBS Elastic Volumes 功能，您可能需要"详细了解创建卷时发生的情况"。

创建卷

创建卷的最常见方法是指定所需的卷类型，然后让控制台为您处理磁盘分配。但您也可以选择要在其上创建卷的特定聚合。

步骤

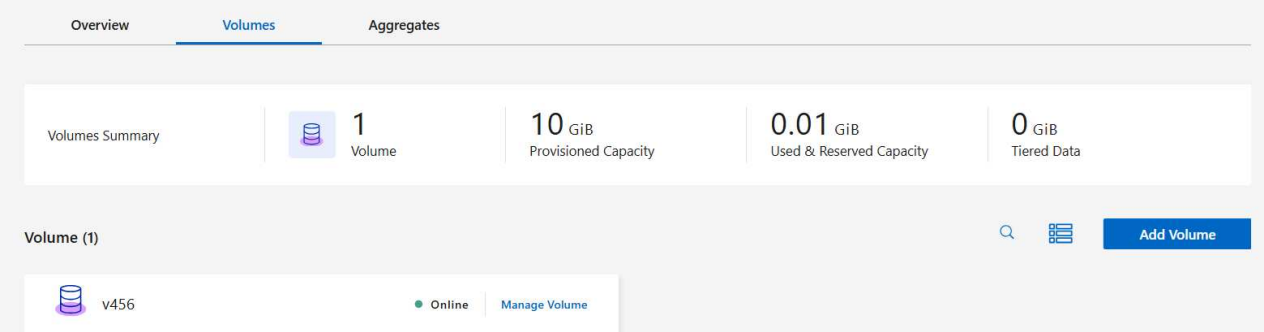
1. 从左侧导航菜单中，选择“存储”>“管理”。
2. 在 **Systems** 页面上，双击要在其上配置FlexVol volume的Cloud Volumes ONTAP系统的名称。

   您可以通过让控制台为您处理磁盘分配来创建卷，或者为卷选择特定的聚合。仅当您对Cloud Volumes ONTAP系统上的数据聚合有充分了解时，才建议选择特定的聚合。

任何聚合

选择“卷”选项卡，然后单击“添加卷”

。

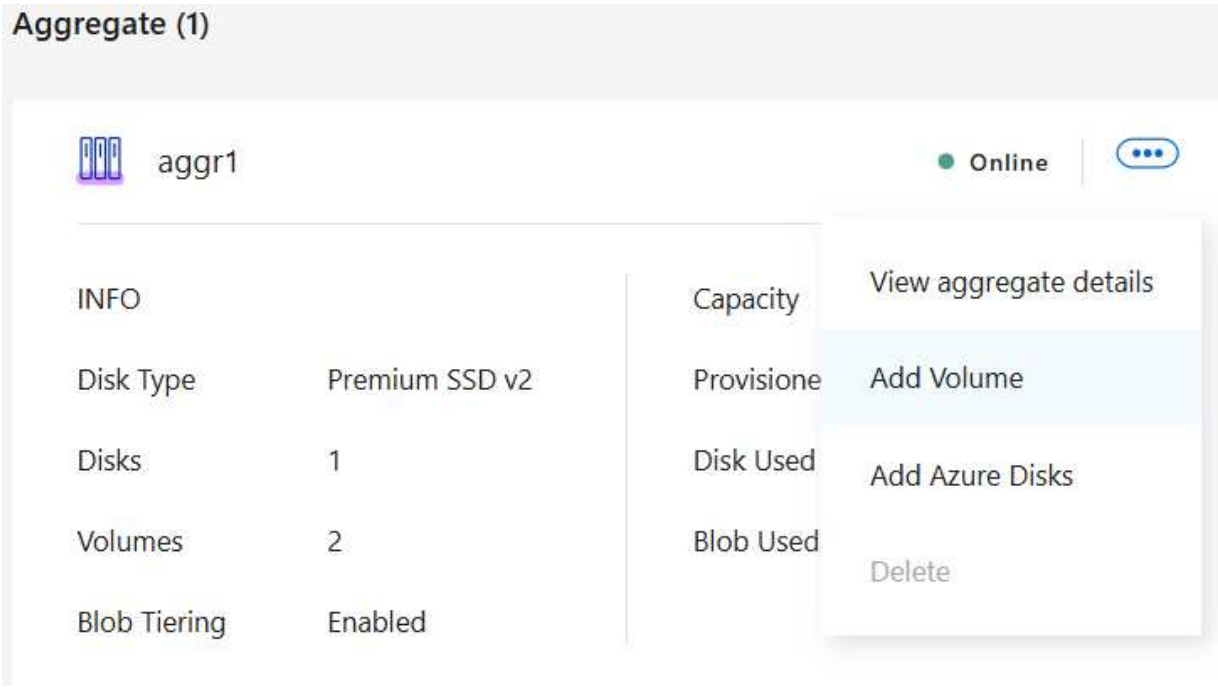


特定骨料

a. 在*聚合*选项卡上，转到所需的聚合并单击 ••• 图标。

b. 选择*添加卷*

。



3. 按照向导中的步骤创建卷。

a. 详细信息、保护和标签：输入有关卷的基本详细信息并选择快照策略。

此页面上的某些字段是不言自明的。以下列表描述了您可能需要指导的字段：

字段	描述
卷名称	您可以为新卷输入的可识别名称。
卷大小	您可以输入的最大大小很大程度上取决于您是否启用精简配置，这使您能够创建比当前可用的物理存储更大的卷。

字段	描述
存储虚拟机 (SVM)	存储虚拟机是在ONTAP内运行的虚拟机，可为您的客户端提供存储和数据服务。您可能知道这是 SVM 或 vserver。 Cloud Volumes ONTAP默认配置一个存储虚拟机，但某些配置支持额外的存储虚拟机。您可以为新卷指定存储虚拟机。
Snapshot 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 副本是时间点文件系统映像，它不会影响性能并且只需要最少的存储空间。您可以选择默认策略或无策略。对于瞬态数据，您可能选择无：例如，对于 Microsoft SQL Server，请选择 tempdb。

b. 协议：为卷选择一个协议（NFS、CIFS 或 iSCSI），然后提供所需的信息。

   如果您选择 CIFS 但未设置服务器，则单击“下一步”后控制台会提示您设置 CIFS 连接。

   "了解支持的客户端协议和版本" 。

   以下部分描述了您可能需要指导的字段。这些描述是按照协议组织的。

NFS

访问控制

选择自定义导出策略以使卷可供客户端使用。

导出策略

定义子网中可以访问卷的客户端。默认情况下，控制台输入一个提供对子网中所有实例的访问权限的值。

CIFS

权限和用户/组

使您能够控制用户和组对 SMB 共享的访问级别（也称为访问控制列表或 ACL）。您可以指定本地或域 Windows 用户或组，或者 UNIX 用户或组。如果指定域 Windows 用户名，则必须使用域\用户名格式包含用户的域。

DNS 主 **IP** 地址和辅助 **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 服务器必须包含定位 CIFS 服务器将加入的域的 Active Directory LDAP 服务器和域控制器所需的服务位置记录 (SRV)。

如果您正在配置 Google 管理的 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 域内指定组织单位 (OU) 的 Windows 帐户的名称和密码。

CIFS 服务器 **NetBIOS** 名称

AD 域中唯一的 CIFS 服务器名称。

组织单位

AD 域内与 CIFS 服务器关联的组织单位。默认值为 CN=Computers。

- 要将 AWS 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=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**。https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou["Azure 文档：在 Azure AD 域服务托管域中创建组织单位 (OU)"^]
- 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**。https://cloud.google.com/managed-microsoft-ad/docs/manage-active-directory-objects#organizational_units["Google Cloud 文档：Google Managed Microsoft AD 中的组织单位"^]

DNS 域

Cloud Volumes ONTAP存储虚拟机 (SVM) 的 DNS 域。大多数情况下，该域与 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。如果您需要使用不同的地址配置 NTP 服务器，那么您应该使用 API。欲了解更多信息，请参阅 "NetApp Console自动化文档"。

请注意，只有在创建 CIFS 服务器时才能配置 NTP 服务器。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），并作为标准块设备呈现给主机。当您创建 iSCSI 卷时，控制台会自动为您创建一个 LUN。我们通过为每个卷创建一个 LUN 来简化操作，因此无需进行任何管理。创建卷后，"使用 IQN 从主机连接到 LUN" 。

发起者组

启动器组 (igroup) 指定哪些主机可以访问存储系统上的指定 LUN

主机启动器 **(IQN)**

iSCSI 目标通过标准以太网网络适配器 (NIC)、带有软件启动器的 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：根据您的性能需求和成本要求为卷选择底层磁盘类型。

   - "在 AWS 中调整系统规模"
     - "在 Azure 中调整系统大小"
     - "在 Google Cloud 中调整系统规模"

4. 使用配置文件和分层策略：选择是否启用或禁用卷上的存储效率功能，然后选择"卷分层策略"。

   ONTAP包含多种存储效率功能，可以减少您所需的总存储量。 NetApp存储效率功能具有以下优势：

   精简配置

   向主机或用户提供比物理存储池中实际拥有的更多的逻辑存储。不是预先分配存储空间，而是在写入数据时动态地将存储空间分配给每个卷。

   重复数据删除

   通过定位相同的数据块并将其替换为对单个共享块的引用来提高效率。该技术通过消除驻留在同一卷中的冗余数据块来减少存储容量要求。

   数据压缩

   通过压缩主存储、辅助存储和归档存储卷内的数据来减少存储数据所需的物理容量。

5. 审核：审核有关卷的详细信息，然后单击*添加*。

结果

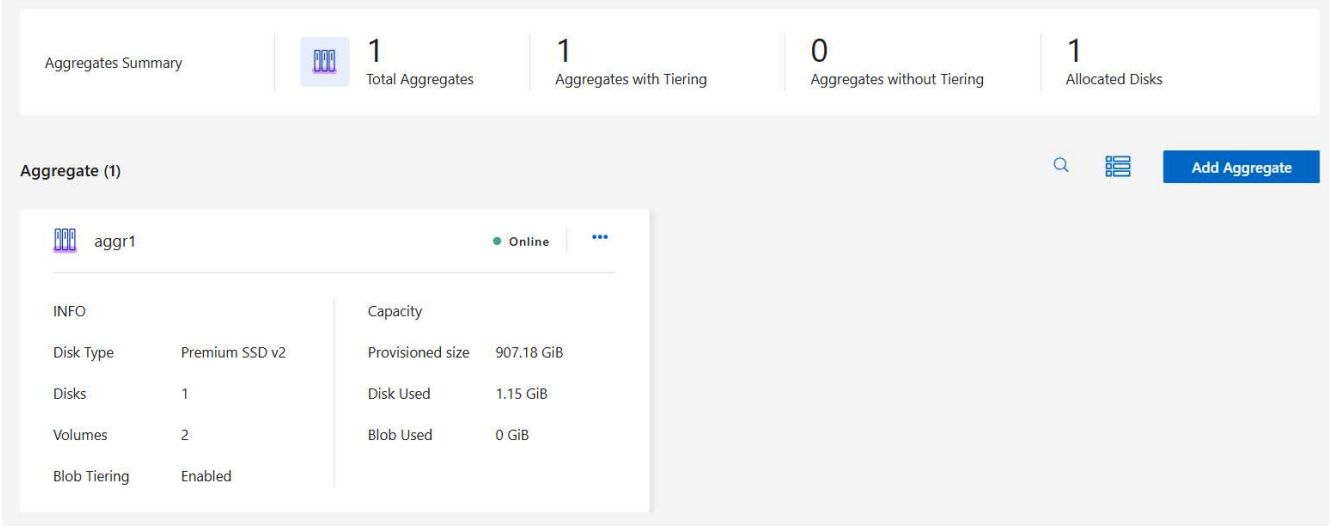
控制台在Cloud Volumes ONTAP系统上创建卷。

在 **HA** 配置中的第二个节点上创建卷

默认情况下，控制台在 HA 配置中的第一个节点上创建卷。如果您需要主动-主动配置，其中两个节点都向客户端提供数据，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”>“管理”。
2. 在“系统”页面上，双击要管理聚合的Cloud Volumes ONTAP系统的名称。
3. 在“聚合”选项卡上，单击“添加聚合”，然后创建聚合。



4. 对于主节点，选择 HA 对中的第二个节点。
5. 控制台创建聚合后，选择它，然后单击*创建卷*。
6. 输入新卷的详细信息，然后单击“创建”。

结果

控制台在 HA 对中的第二个节点上创建卷。

对于在多个 AWS 可用区中部署的 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

如果您配置了 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共享并创建文件。

如果要将配额应用于卷，则必须使用ONTAP系统管理器或ONTAP CLI。配额使您能够限制或跟踪用户、组或 qtree 使用的磁盘空间和文件数量。

管理**Cloud Volumes ONTAP**系统上的卷

您可以在NetApp Console中管理卷和 CIFS 服务器。您还可以移动卷以避免容量问题。

您可以在NetApp Console标准视图中管理卷，也可以通过控制台中包含的ONTAP系统管理器管理卷，以实现高

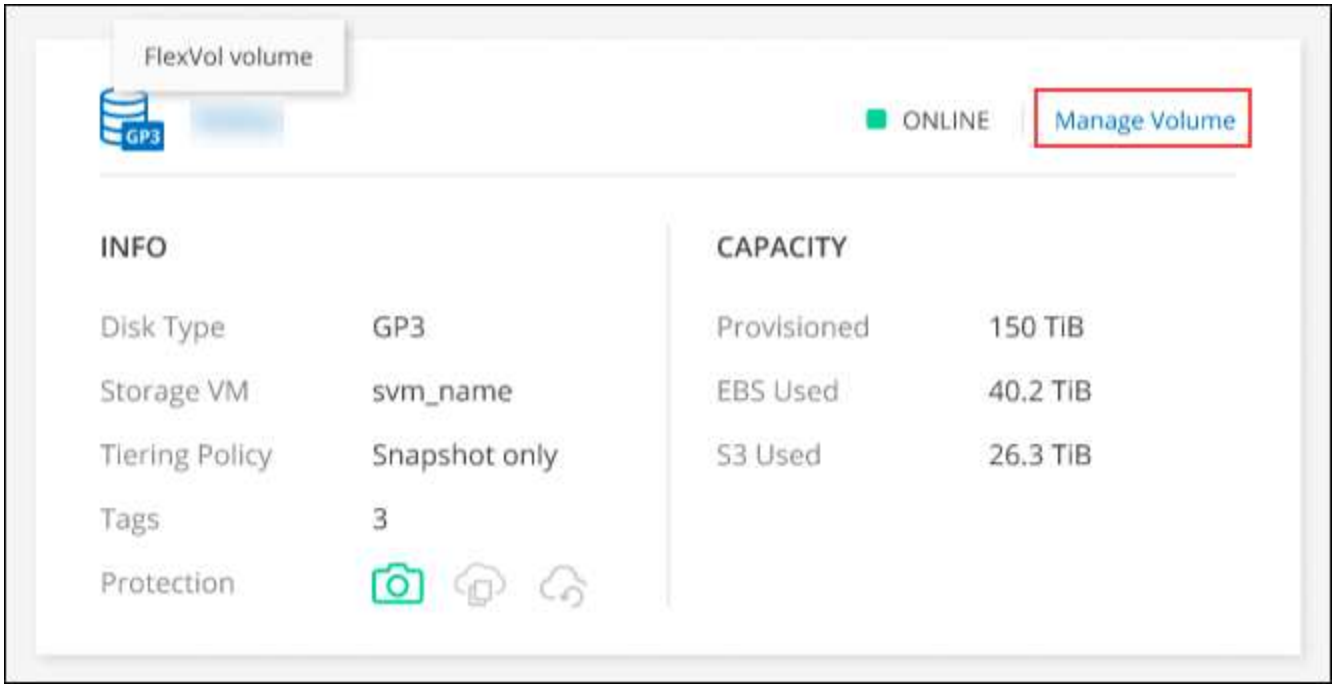
级卷管理。标准视图提供了一组有限的选项来修改您的卷。系统管理器提供高级管理，例如克隆、调整大小、更改反勒索软件、分析、保护和活动跟踪的设置以及跨层移动卷。有关信息，请参阅"使用系统管理器管理Cloud Volumes ONTAP"。

管理卷

通过使用控制台的标准视图，您可以根据存储需求管理卷。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”>“管理”。
2. 在*系统*页面上，双击要管理卷的Cloud Volumes ONTAP系统。
3. 选择“卷”选项卡。



4. 在所需的卷图块上，单击*管理卷*。

任务	操作
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“安装命令”。 b. 单击“复制”。

任务	操作
克隆卷	a. 在“管理卷”面板的“卷操作”下，单击“克隆卷”。 b. 根据需要修改克隆名称，然后单击“克隆”。 此过程会创建一个FlexClone卷。 FlexClone卷是可写的、时间点副本，它节省空间，因为它只使用少量空间来存储元数据，并且仅在更改或添加数据时才消耗额外的空间。 要了解有关FlexClone卷的更多信息，请参阅 "ONTAP 9 逻辑存储管理指南"。
编辑卷（仅限读写卷）	a. 在“管理卷”面板的“卷操作”下，单击“编辑卷设置” b. 修改卷的快照策略、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*。 如果您需要自定义 Snapshot 策略，则可以使用ONTAP System Manager 创建它们。
删除卷	a. 在“管理卷”面板的“卷操作”下，单击“删除卷”。 b. 在“删除卷”窗口下，输入要删除的卷的名称。 c. 再次单击“删除”进行确认。
按需创建 Snapshot 副本	a. 在“管理卷”面板的“保护操作”下，单击“创建 Snapshot 副本”。 b. 如果需要，更改名称，然后单击“创建”。
将数据从 Snapshot 副本还原到新卷	a. 在“管理卷”面板的“保护操作”下，单击“从 Snapshot 副本还原”。 b. 选择一个 Snapshot 副本，输入新卷的名称，然后单击“恢复”。
更改底层磁盘类型	a. 在“管理卷”面板的“高级操作”下，单击“更改磁盘类型”。 b. 选择磁盘类型，然后单击“更改”。 控制台将卷移动到使用所选磁盘类型的现有聚合，或者为该卷创建新的聚合。
更改分层策略	a. 在“管理卷”面板的“高级操作”下，单击“更改分层策略”。 b. 选择不同的策略并单击*更改*。 控制台将卷移动到使用具有分层功能的所选磁盘类型的现有聚合，或者为该卷创建新的聚合。

任务	操作
删除卷	a. 选择一个卷，然后单击“删除”。 b. 在对话框中输入卷的名称。 c. 再次单击“删除”进行确认。

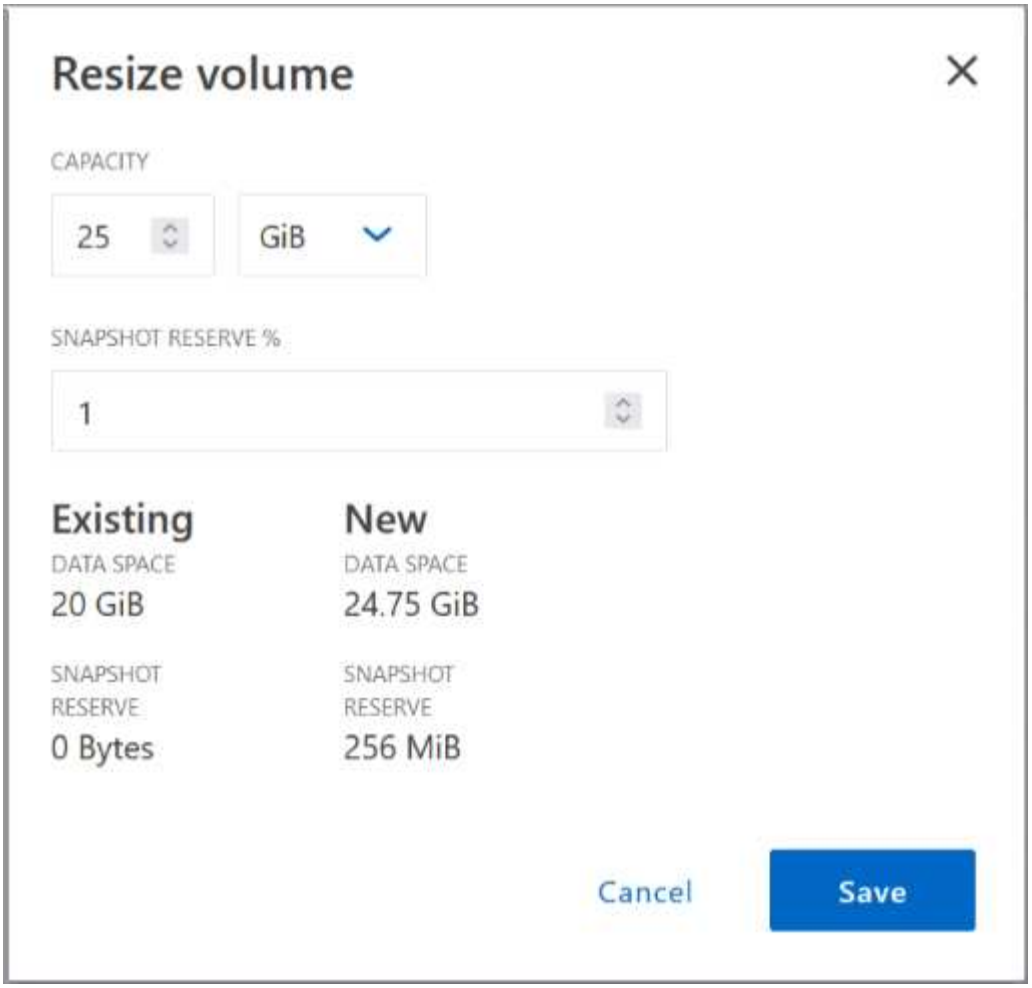
调整卷大小

默认情况下，当卷空间不足时，它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。该值可以在控制台代理的设置中配置。

如果您需要调整卷大小，您可以从控制台中的ONTAP系统管理器进行操作。

步骤

1. 单击系统管理器视图以通过ONTAP系统管理器调整卷大小。请参阅"如何开始" 。
2. 从左侧导航菜单中，选择“存储”>“卷”。
3. 从卷列表中，确定应调整大小的卷。
4. 点击选项图标 。
5. 选择*调整大小*。
6. 在*调整卷大小*屏幕上，根据需要编辑容量和快照预留百分比。您可以将现有的可用空间与修改后的容量进行比较。
7. 单击“保存”。



调整卷大小时，请务必考虑系统的容量限制。前往 "Cloud Volumes ONTAP发行说明"了解更多信息。

修改 **CIFS** 服务器

如果您更改 DNS 服务器或 Active Directory 域，则需要修改Cloud Volumes ONTAP中的 CIFS 服务器，以便它可以继续为客户端提供存储服务。

步骤

1. 从Cloud Volumes ONTAP系统的 **Overview** 选项卡中，单击右侧面板下的 **Feature** 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	操作
选择存储虚拟机 (SVM)	选择 Cloud Volume ONTAP存储虚拟机 (SVM) 显示其配置的 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 域内指定组织单位 (OU) 的 Windows 帐户的名称和密码。

任务	操作
DNS 主 IP 地址和辅助 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 服务器必须包含定位 Active Directory LDAP 服务器和 CIFS 服务器将加入的域的域控制器所需的服务位置记录 (SRV)。ifdef::gcp[] 如果您正在配置 Google Managed Active Directory，则默认情况下可以使用 169.254.169.254 IP 地址访问 AD。endif::gcp[]
DNS 域	Cloud Volumes ONTAP存储虚拟机 (SVM) 的 DNS 域。大多数情况下，该域与 AD 域相同。
CIFS 服务器 NetBIOS 名称	AD 域中唯一的 CIFS 服务器名称。
组织单位	AD 域内与 CIFS 服务器关联的组织单位。默认值为 CN=Computers。 • 要将 AWS 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=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使用更改来更新 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。

您可以在ONTAP系统管理器中移动卷，方法是选择卷和目标聚合、启动卷移动操作以及选择性地监控卷移动作业。使用系统管理器时，卷移动操作会自动完成。

步骤

1. 使用ONTAP系统管理器或ONTAP CLI 将卷移动到聚合。

   在大多数情况下，您可以使用系统管理器来移动卷。

   有关说明，请参阅"《ONTAP 9 卷移动快速指南》"。

当控制台显示“需要操作”消息时移动卷

控制台可能会显示“需要采取措施”消息，表示需要移动卷以避免容量问题，但您需要自行解决问题。如果发生这种情况，您需要确定如何纠正问题，然后移动一个或多个卷。

当聚合已达到 90% 的使用容量时，控制台会显示这些“需要操作”消息。如果启用了数据分层，则当聚合已达到 80% 的已用容量时会显示消息。默认情况下，保留 10% 的可用空间用于数据分层。"了解有关数据分层的可用空间比率的更多信息" 。

步骤

1. [确定如何纠正容量问题] 。
2. 根据您的分析，移动卷以避免容量问题：
   - [将卷移至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] 。

确定如何纠正容量问题

如果控制台无法提供移动卷以避免容量问题的建议，则必须确定需要移动的卷以及是否应将它们移动到同一系统上的另一个聚合或另一个系统。

步骤

1. 查看“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，高级信息应该显示类似如下内容：聚合 aggr1 已达到其容量限制。

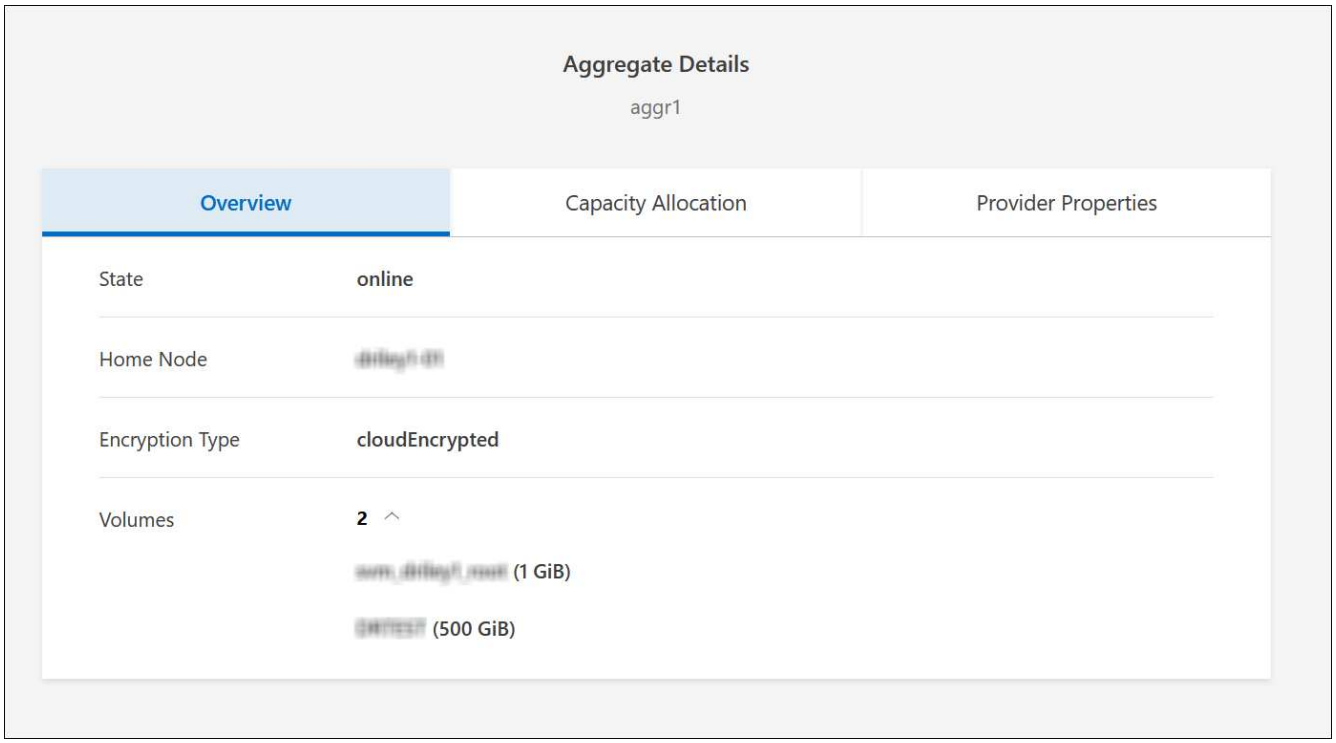
2. 确定要移出聚合的一个或多个卷：

   a. 在Cloud Volumes ONTAP系统中，单击 **Aggregates tab**。

   b. 在聚合图块上，单击 ••• 图标，然后单击*查看汇总详情*。

   c. 在“聚合详细信息”屏幕的“概述”选项卡下，查看每个卷的大小并选择要移出聚合的一个或多个卷。

      您应该选择足够大的卷来释放聚合中的空间，以避免将来出现额外的容量问题。



3. 如果系统尚未达到磁盘限制，则应将卷移动到现有聚合或同一系统上的新聚合。

   有关信息，请参阅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，请执行以下操作之一：
   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。

      有关信息，请参阅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有空间的系统。

      有关信息，请参阅将卷移动到另一个聚合以避免容量问题。

将卷移至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，您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来更正以下“需要操作”消息：

> 移动卷对于避免容量问题是必要的；但是，控制台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. 将源系统拖放到目标系统以执行卷的一次性数据复制。

   有关信息，请参阅"在系统之间复制数据"。

3. 转到“复制状态”页面，然后中断SnapMirror关系，将复制的卷从数据保护卷转换为读/写卷。

   有关信息，请参阅"管理数据复制计划和关系"。

4. 配置数据访问的卷。

   有关配置数据访问目标卷的信息，请参阅"ONTAP 9 卷灾难恢复快速指南"。

5. 删除原始卷。

   有关信息，请参阅"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以避免容量问题。

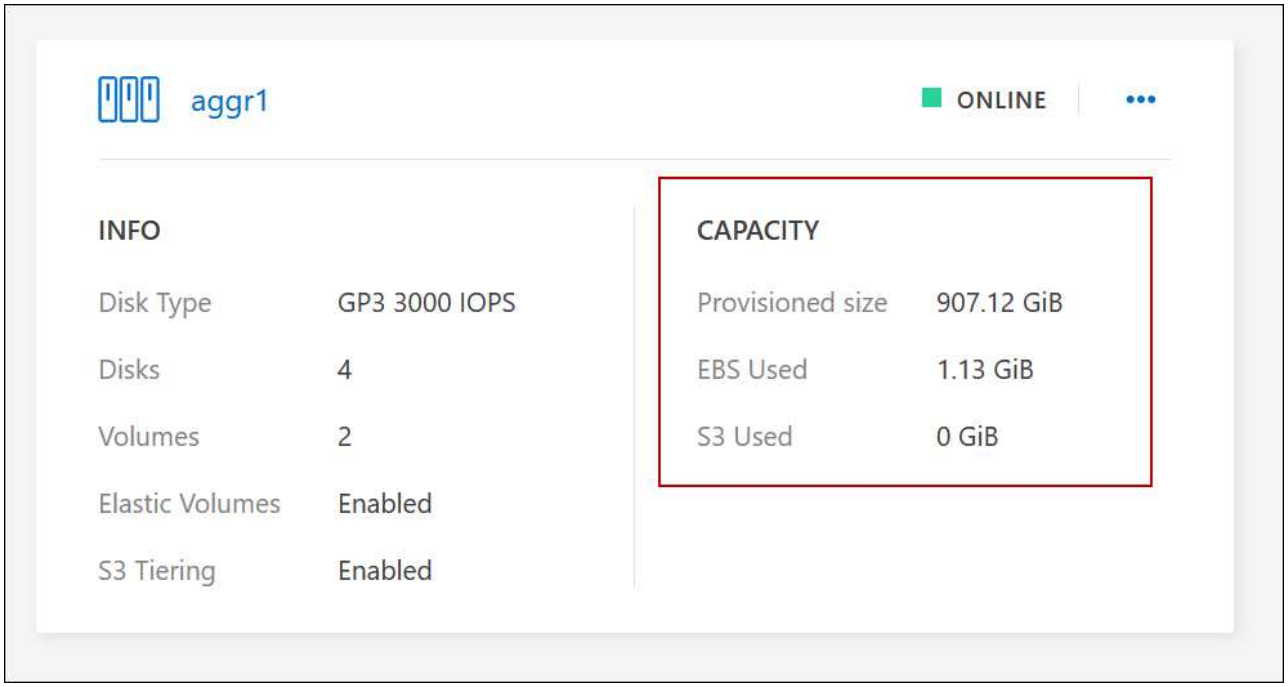
关于此任务

您可以按照此任务中的步骤来更正以下“需要操作”消息：

> 需要移动两个或更多卷以避免容量问题；但是，控制台无法为您执行此操作。

步骤

1. 验证现有聚合是否具有可供您需要移动的卷使用的容量：
   a. 在Cloud Volumes ONTAP系统上，单击 **Aggregates tab**。
   b. 在所需的聚合图块上，单击 ••• 图标，然后*查看聚合详细信息*以查看可用容量（预配置大小减去已用聚合容量）。



2. 如果需要，将磁盘添加到现有聚合：
   a. 选择聚合，然后单击 ••• 图标 > 添加磁盘。
   b. 选择要添加的磁盘数量，然后单击“添加”。
3. 如果没有可用容量的聚合，则创建一个新的聚合。

   有关信息，请参阅"创建聚合"。
4. 使用ONTAP系统管理器或ONTAP CLI 将卷移动到聚合。
5. 在大多数情况下，您可以使用系统管理器来移动卷。

   有关说明，请参阅"《ONTAP 9 卷移动快速指南》"。

交易量变动执行缓慢的原因

如果Cloud Volumes ONTAP满足以下任何条件，则移动卷所需的时间可能会比您预期的要长：

- 该卷是一个克隆。

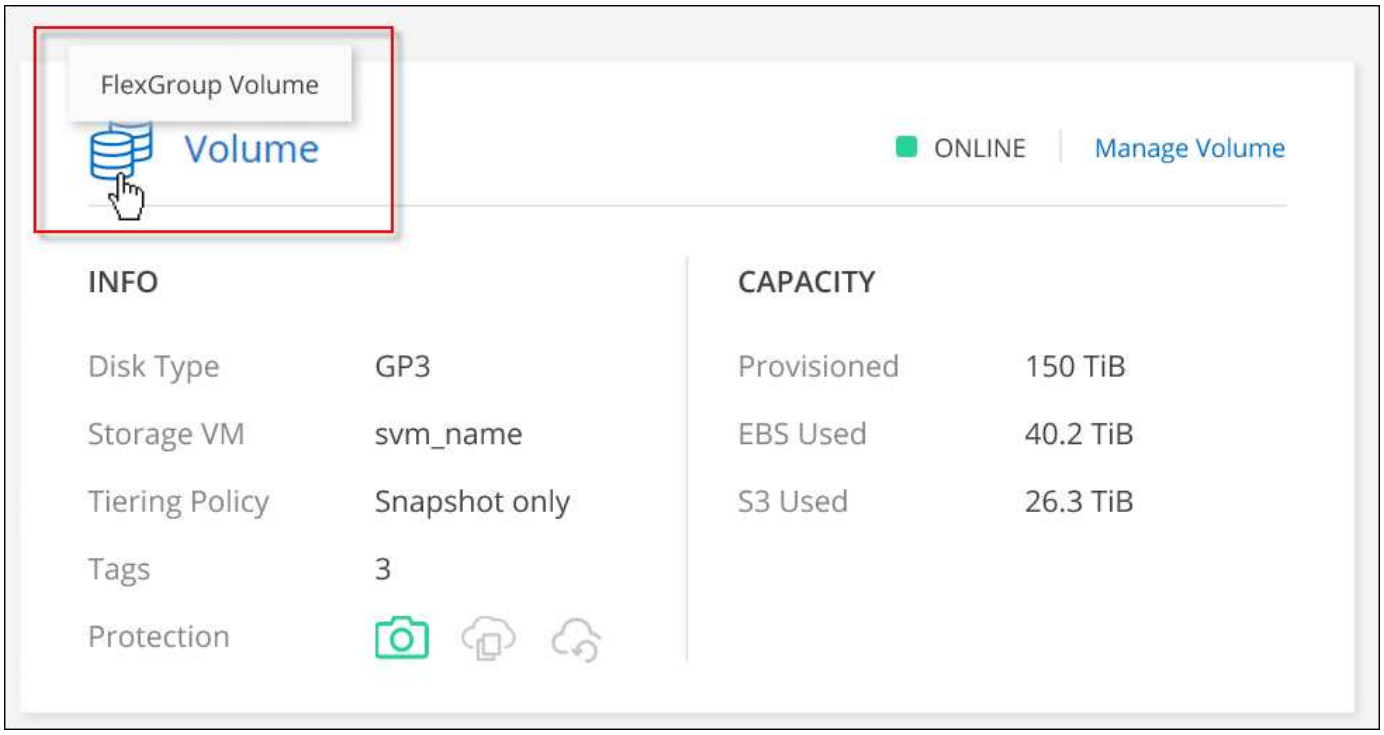
- 该卷是克隆的父卷。
- 源聚合或目标聚合具有单个吞吐量优化 HDD (st1) 磁盘。
- 其中一个聚合使用了较旧的对象命名方案。两个聚合必须使用相同的名称格式。

  如果在 9.4 或更早版本中的聚合上启用了数据分层，则使用较旧的命名方案。

- 源聚合和目标聚合上的加密设置不匹配，或者正在进行重新密钥。
- 在卷移动时指定了 *-tiering-policy* 选项来更改分层策略。
- 在卷移动时指定了 *-generate-destination-key* 选项。

查看**FlexGroup**卷

您可以直接通过控制台中的“卷”选项卡查看通过ONTAP System Manager 或ONTAP CLI 创建的FlexGroup卷。您可以通过专用的 **Volumes** 图块查看 FleGroup 卷的详细信息，并通过图标的悬停文本识别每个FlexGroup卷组。此外，您可以通过卷样式列识别和排序卷列表视图下的FlexGroup卷。



目前，您只能在控制台下查看现有的FlexGroup卷。您无法在控制台中创建FlexGroup卷。

将非活动**Cloud Volumes ONTAP**数据分层到低成本对象存储

您可以通过将用于热数据的 SSD 或 HDD 性能层与用于非活动数据的对象存储容量层相结合来降低Cloud Volumes ONTAP的存储成本。数据分层由FabricPool技术提供支持。有关高级概述，请参阅"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

大多数配置都受支持。如果您拥有运行最新版本的Cloud Volumes ONTAP系统，那么您就可以开始了。"了解更多"。

2 确保**Cloud Volumes ONTAP**与对象存储之间的连接

- 对于 AWS，您需要一个到 Amazon Simple Storage Service (Amazon S3) 的 VPC 端点。了解更多。
- 对于 Azure，只要NetApp Console具有所需的权限，您就不需要执行任何操作。了解更多 。
- 对于 Google Cloud，您需要配置私有 Google Access 子网并设置服务帐户。了解更多 。

3 确保您已启用分层聚合

应在聚合上启用数据分层，以便在卷上启用它。您应该了解新卷和现有卷的要求。了解更多 。

4 创建、修改或复制卷时选择分层策略

当您创建、修改或复制卷时， NetApp Console会提示您选择分层策略。

- "来自读写卷的层数据"
- "来自数据保护卷的分层数据"

> 数据分层不需要什么？
>
> - 您不需要安装功能许可证来启用数据分层。
> - 您不需要为容量层创建对象存储。控制台会为您完成该操作。
> - 您不需要在系统级别启用数据分层。
>
> 控制台在创建系统时为冷数据创建对象存储，只要没有连接或权限问题 。之后，您只需要在卷上启用数据分层（在某些情况下，在聚合体上 ）。

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）或预配置 IOPS SSD（io1）。

> 使用吞吐量优化 HDD (st1) 时，我们不建议将数据分层到对象存储。

- 非活动数据分层存储到 Amazon S3 存储桶。不支持分层到其他提供商。

Azure 中的支持

- Azure 支持数据分层，如下所示：
  - 使用单节点系统的 9.4 版
  - 9.6 版，配备 HA 对
- 性能层可以是高级 SSD 托管磁盘、标准 SSD 托管磁盘或标准 HDD 托管磁盘。
- 非活动数据分层到 Microsoft Azure Blob。不支持分层到其他提供商。

Google Cloud 支持

- 从Cloud Volumes ONTAP 9.6 开始，Google Cloud 支持数据分层。
- 性能层可以是 SSD 持久磁盘、平衡持久磁盘或标准持久磁盘。
- 非活动数据分层存储到 Google Cloud Storage。不支持分层到其他提供商。

功能互操作性

- 数据分层由加密技术支持。
- 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。

将冷数据分层至 Amazon S3 的要求

确保 Cloud Volumes ONTAP 已连接到 Amazon S3。提供此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：创建网关终端节点"。

创建 VPC 端点时，请确保选择与Cloud Volumes ONTAP实例相对应的区域、VPC 和路由表。您还必须修改安全组以添加允许流量到 S3 端点的出站 HTTPS 规则。否则， Cloud Volumes ONTAP无法连接到 S3 服务。

如果您遇到任何问题，请参阅 "AWS Support 知识中心：为什么我无法使用网关 VPC 终端节点连接到 S3 存储桶？"。

将冷数据分层到 Azure Blob 存储的要求

只要控制台具有所需的权限，您就不需要在性能层和容量层之间建立连接。如果控制台代理的自定义角色具有以下权限，则控制台将为您启用 VNet 服务终结点：

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

自定义角色默认包含权限。 "查看控制台代理的 Azure 权限"

将冷数据分层到 Google Cloud Storage 存储桶的要求

- 必须为Cloud Volumes ONTAP所在的子网配置私有 Google Access。有关说明，请参阅 "Google Cloud 文

档：配置私有 Google 访问权限"。

- 必须将服务帐户附加到Cloud Volumes ONTAP。

  "了解如何设置此服务帐号" 。

  创建Cloud Volumes ONTAP系统时，系统会提示您选择此服务帐户。

  如果在部署期间未选择服务帐户，则需要关闭 Cloud Volumes ONTAP，转到 Google Cloud Console，然后将服务帐户附加到 Cloud Volumes ONTAP 实例。然后，您可以按照下一节中的说明启用数据分层。

- 要使用客户管理的加密密钥加密存储桶，请启用 Google Cloud 存储桶以使用该密钥。

  "了解如何将客户管理的加密密钥与Cloud Volumes ONTAP结合使用" 。

实现要求后启用数据分层

只要没有连接或权限问题，控制台就会在创建系统时为冷数据创建对象存储。如果您在创建系统之后才实现上面列出的要求，那么您将需要通过 API 或ONTAP系统管理器手动启用分层，从而创建对象存储。

通过控制台启用分层的功能将在未来的Cloud Volumes ONTAP版本中提供。

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。您应该了解新卷和现有卷的要求。

- 新卷

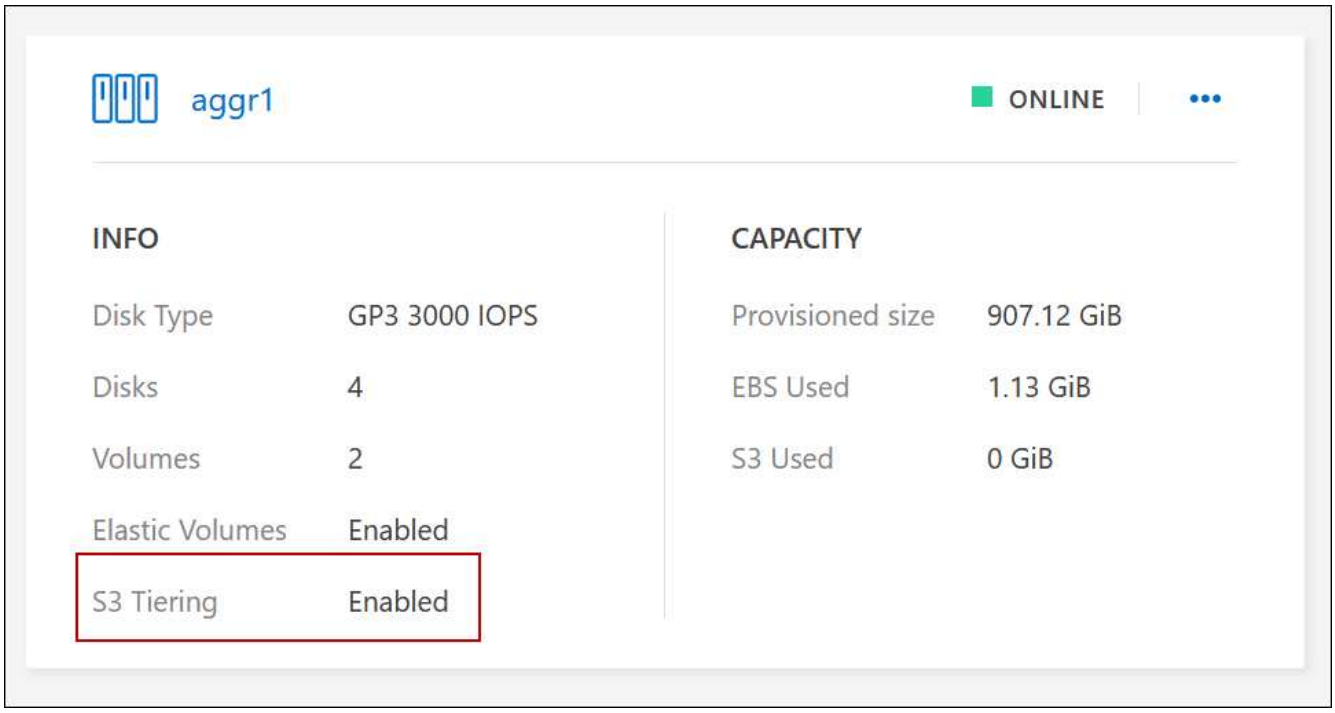
  如果您在新卷上启用数据分层，则无需担心在聚合上启用数据分层。控制台在已启用分层的现有聚合上创建卷，或者如果尚不存在启用数据分层的聚合，则为该卷创建新的聚合。

- 现有卷

  要在现有卷上启用数据分层，请确保在底层聚合上启用它。如果现有聚合上未启用数据分层，则需要使用ONTAP系统管理器将现有聚合附加到对象存储。

确认聚合上是否启用了分层的步骤

1. 从左侧导航菜单中，选择“存储”>“管理”。
2. 打开Cloud Volumes ONTAP系统。
3. 选择“聚合”选项卡并检查聚合上是否启用或禁用分层。



在聚合上启用分层的步骤

1. 在ONTAP系统管理器中，单击 存储 > 层级。
2. 单击聚合的操作菜单并选择*附加云层*。
3. 选择要附加的云层并单击*保存*。

下一步是什么?

您现在可以在新卷和现有卷上启用数据分层，如下一节所述。

来自读写卷的层数据

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，从而释放性能层以存储热数据。

步骤

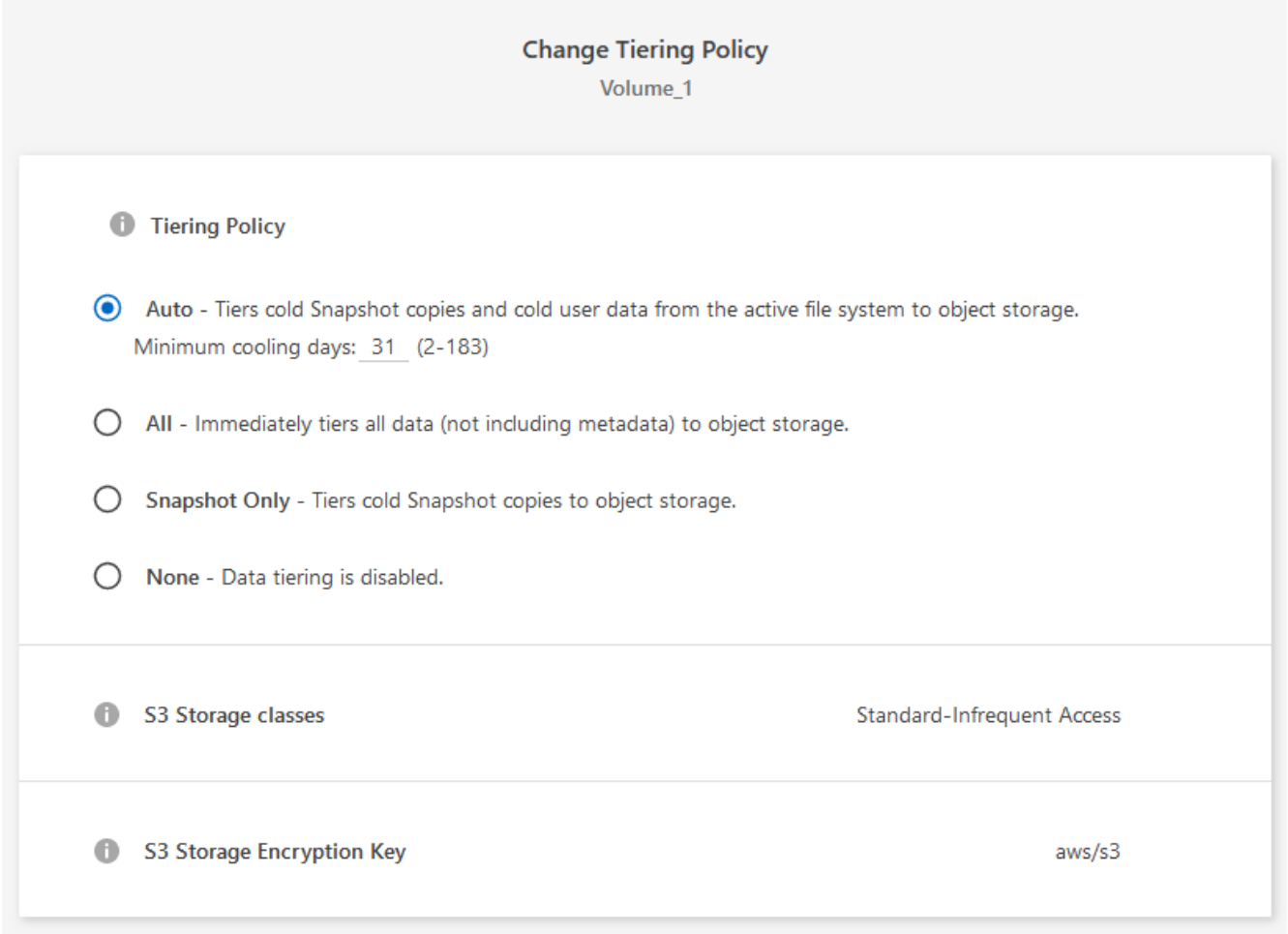
1. 在系统下的*Volumes*选项卡中，创建一个新卷或更改现有卷的层：

任务	操作
创建新卷	单击“添加新卷”。
修改现有卷	选择所需的卷图块，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。

   有关这些政策的描述，请参阅"数据分层概述"。

   例子



如果尚不存在启用数据分层的聚合，则控制台会为卷创建一个新的聚合。

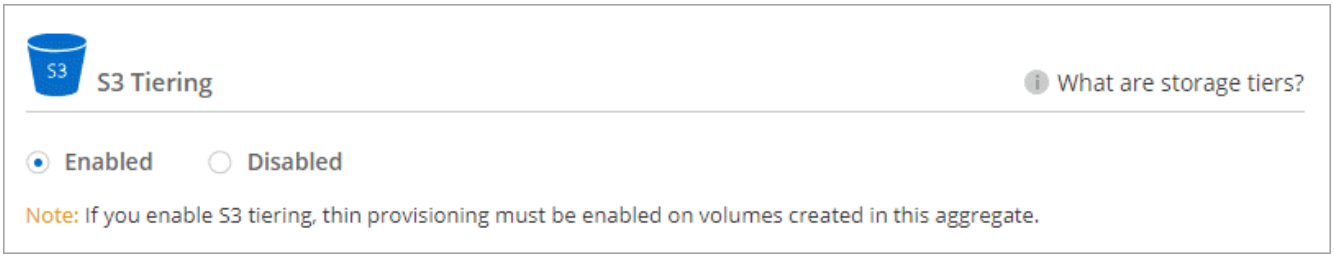
来自数据保护卷的分层数据

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，数据在读取时会逐渐移动到性能层。

步骤

1. 从左侧导航菜单中，选择“存储”>“管理”。
2. 在 系统 页面上，选择包含源卷的Cloud Volumes ONTAP系统，然后将其拖动到要将卷复制到的系统。
3. 按照提示操作，直到到达分层页面并启用数据分层到对象存储。

例子



有关复制数据的帮助，请参阅 "将数据复制到云端或从云端复制数据"。

更改分层数据的存储类别

部署Cloud Volumes ONTAP后，您可以通过更改 30 天未访问的非活动数据的存储类别来降低存储成本。如果您确实访问数据，则访问成本会更高，因此在更改存储类之前必须考虑到这一点。

分层数据的存储类别是系统范围的，而不是每个卷的。

有关受支持的存储类别的信息，请参阅"数据分层概述"。

步骤

1. 在Cloud Volumes ONTAP系统上，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定义了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。默认设置是 10% 的可用空间，但您可以根据需要调整设置。

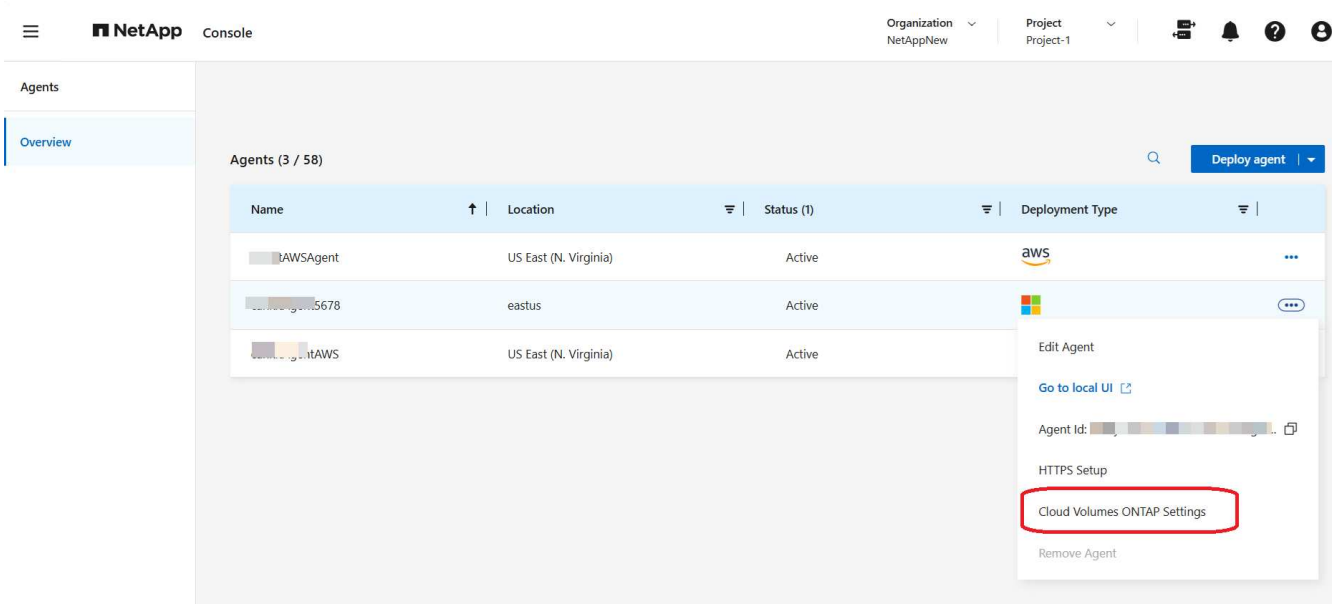
例如，您可以选择少于 10% 的可用空间，以确保您利用所购买的容量。当需要额外容量时，控制台可以为您购买额外的磁盘（直到达到聚合的磁盘限制）。

如果没有足够的空间，那么Cloud Volumes ONTAP就无法移动数据，并且您可能会遇到性能下降的情况。任何改变都应谨慎进行。如果您不确定，请联系NetApp支持寻求指导。

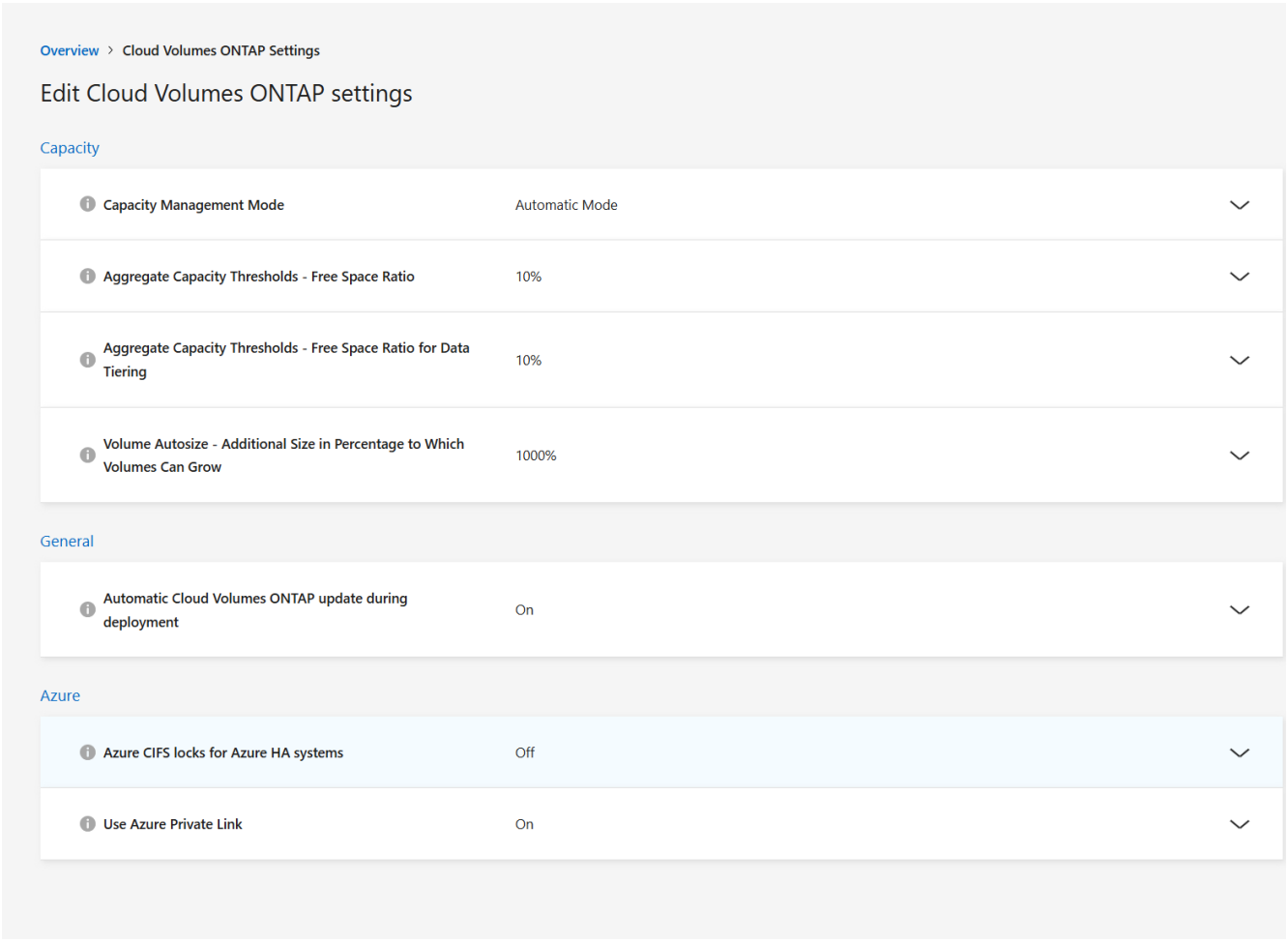
该比率对于灾难恢复场景很重要，因为当从对象存储读取数据时， Cloud Volumes ONTAP会将数据移动到 SSD/HDD 以提供更好的性能。如果没有足够的空间，那么Cloud Volumes ONTAP就无法移动数据。在更改比例时请考虑到这一点，以便满足您的业务需求。

步骤

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



4. 在“容量”下，单击“聚合容量阈值 - 数据分层的可用空间比率”。



5. 根据您的要求更改可用空间比例，然后单击“保存”。

更改自动分层策略的冷却期

如果您使用自动分层策略在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ONTAP CLI 和 API 支持此操作。

冷却期是指卷中的用户数据在被视为“冷”并移动到对象存储之前必须保持不活动的天数。

自动分层策略的默认冷却期为 31 天。您可以按如下方式更改冷却时间：

- 9.8 或更高版本：2 天至 183 天
- 9.7 或更早版本：2 天至 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。

在系统退役时删除 **S3** 存储桶

当您退役环境时，您可以从Cloud Volumes ONTAP系统中删除包含分层数据的 S3 存储桶。

仅当满足以下条件时，您才可以删除 S3 存储桶：

- Cloud Volume ONTAP系统已从控制台中删除。
- 所有对象都从存储桶中删除，并且 S3 存储桶为空。

当您退役Cloud Volumes ONTAP系统时，为该环境创建的 S3 存储桶不会被自动删除。相反，它保持孤立状态以防止任何意外的数据丢失。您可以删除存储桶中的对象，然后移除 S3 存储桶本身，或者保留它以供日后使用。参考 "ONTAP CLI：vserver object-store-server bucket 删除"。

从主机系统连接到**Cloud Volumes ONTAP**上的 **LUN**

当您创建 iSCSI 卷时， NetApp Console会自动为您创建一个 LUN。我们通过为每个卷创建一个 LUN 来简化操作，因此无需进行任何管理。创建卷后，使用 IQN 从主机连接到 LUN。

请注意以下事项：

- 控制台的自动容量管理不适用于 LUN。当它创建 LUN 时，它会禁用自动增长功能。
- 您可以从ONTAP系统管理器或ONTAP CLI 创建其他 LUN。

步骤

1. 从左侧导航菜单中，选择“存储”>“管理”。
2. 在*系统*页面上，双击要管理卷的Cloud Volumes ONTAP系统。
3. 在系统中，选择*Volumes*选项卡。
4. 转到所需的卷图块，然后选择*管理卷*以访问右侧的管理卷面板。
5. 单击*目标 iQN*。
6. 单击“复制”复制 iQN 名称。

7. 建立从主机到 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"

使用Cloud Volumes ONTAP系统上的FlexCache卷加速数据访问

FlexCache卷是一种存储卷，用于缓存从原始（或源）卷读取的 SMB 和 NFS 数据。随后读取缓存数据可以加快对该数据的访问速度。

您可以使用FlexCache卷来加快数据访问速度或卸载访问量大的卷的流量。 FlexCache卷有助于提高性能，特别是当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的系统工作负载。

NetApp Console提供FlexCache卷的管理"NetApp Volume Caching"。

您还可以使用ONTAP CLI 或ONTAP系统管理器来创建和管理FlexCache卷：

- "FlexCache卷实现更快数据访问电源指南"
- "在 System Manager 中创建FlexCache卷"

当源加密时使用FlexCache

在原始卷已加密的Cloud Volumes ONTAP系统上配置FlexCache时，需要执行额外的步骤，以确保FlexCache卷可以正确访问和缓存加密数据。

开始之前

1. 加密设置：确保源卷完全加密且可操作。对于Cloud Volumes ONTAP系统，这涉及与特定于云的密钥管理服务集成。

对于 AWS，这通常意味着使用 AWS 密钥管理服务 (KMS)。有关信息，请参阅"使用 AWS Key Management Service 管理密钥"。

对于 Azure，您需要为NetApp卷加密 (NVE) 设置 Azure Key Vault。有关信息，请参阅"使用 Azure Key Vault 管理密钥"。

对于 Google Cloud，它是 Google Cloud Key Management Service。有关信息，请参阅"使用 Google 的云密钥管理服务管理密钥"。

1. 密钥管理服务：在创建FlexCache卷之前，请验证密钥管理服务是否在Cloud Volumes ONTAP系统上正确配置。此配置对于FlexCache卷解密来自原始卷的数据至关重要。
2. 许可：确认有效的FlexCache许可证可用并在Cloud Volumes ONTAP系统上激活。
3. * ONTAP版本*：确保您的Cloud Volumes ONTAP系统的ONTAP版本支持带有加密卷的FlexCache 。参考最新 "ONTAP发行说明"或兼容性矩阵以获取更多信息。
4. 网络配置：确保网络配置允许原始卷和FlexCache卷之间的无缝通信。这包括云环境中的正确路由和 DNS 解析。

步骤

使用加密源卷在Cloud Volumes ONTAP系统上创建FlexCache卷。有关详细步骤和其他注意事项，请参阅以下部分：

- "FlexCache卷实现更快数据访问电源指南"
- "在 System Manager 中创建FlexCache卷"

聚合管理

为Cloud Volumes ONTAP系统创建聚合

您可以自行创建聚合，也可以让NetApp Console在创建卷时为您创建聚合。自行创建聚合的好处是您可以选择底层磁盘大小，从而可以根据所需的容量或性能调整聚合的大小。

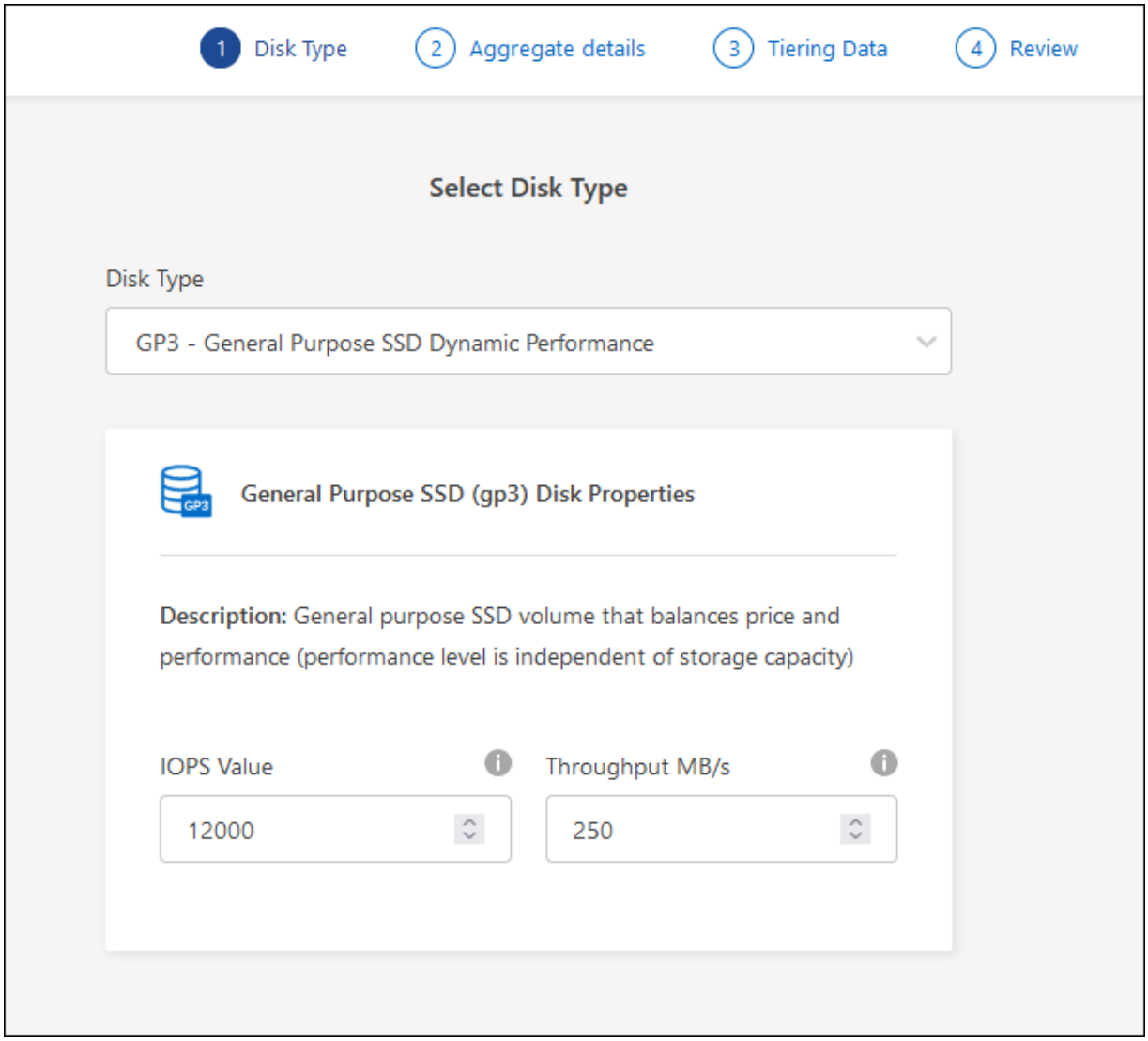
必须直接从控制台创建和删除所有磁盘和聚合。您不应从其他管理工具执行这些操作。这样做会影响系统稳定性，妨碍将来添加磁盘的能力，并可能产生冗余的云提供商费用。

步骤

1. 从左侧导航菜单中，选择“存储”>“管理”。
2. 在“系统”页面上，双击要管理聚合的Cloud Volumes ONTAP系统的名称。
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，请参阅"在 AWS 中规划您的Cloud Volumes ONTAP配置"。
- 如果提示您输入聚合的容量大小，则表示您正在支持 Amazon EBS 弹性卷功能的配置上创建聚合。以下屏幕截图显示了由 gp3 磁盘组成的新聚合的示例。



"了解有关弹性卷支持的更多信息" 。

Azure

有关磁盘类型和磁盘大小的帮助，请参阅"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，请参阅"在 Google Cloud 中规划您的Cloud Volumes ONTAP配置"。

4. 单击“添加”，然后单击“批准并购买”。

管理Cloud Volumes ONTAP集群的聚合

通过添加磁盘、查看有关聚合的信息以及删除聚合来自行管理聚合。

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

开始之前

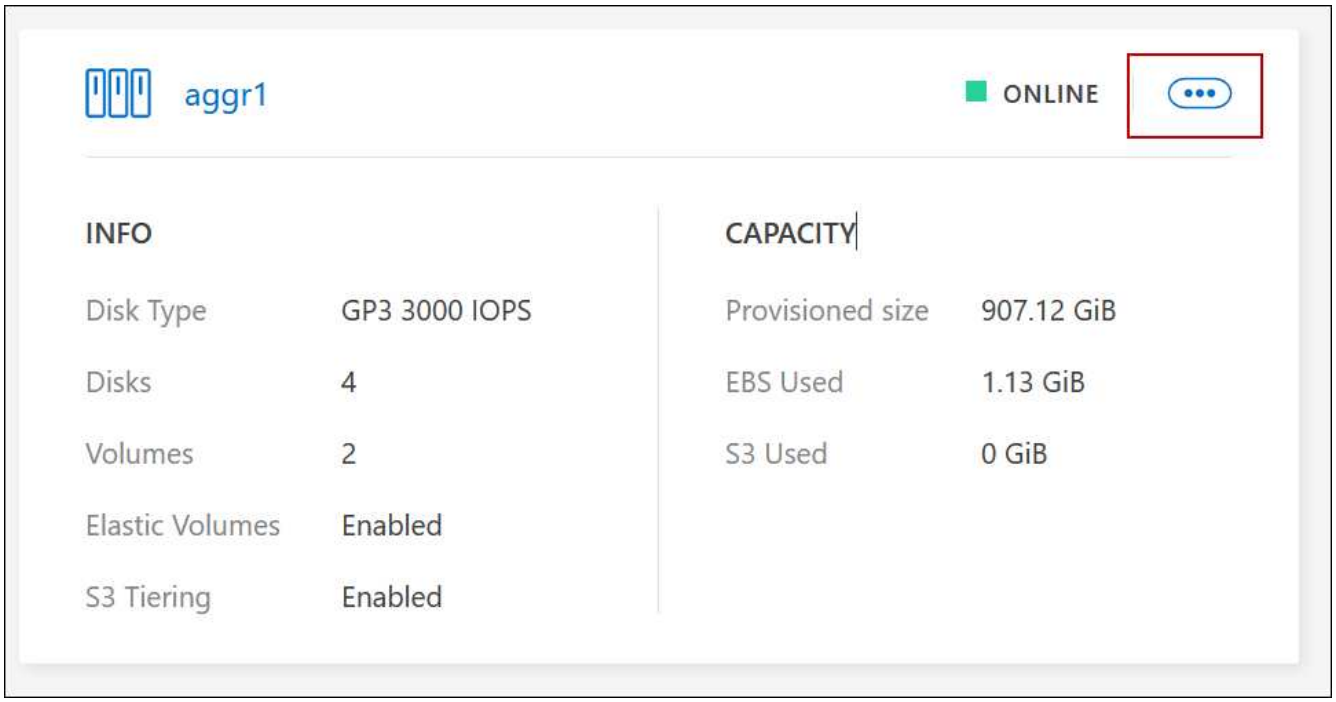
如果要删除聚合，则必须先删除聚合中的卷。

关于此任务

如果聚合空间不足，您可以使用ONTAP系统管理器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”>“管理”。
2. 在 **Systems** 页面上，双击要管理聚合的Cloud Volumes ONTAP系统。
3. 从系统详细信息中，单击“聚合”选项卡。
4. 对于所需的聚合，单击 ••• 管理操作的图标。



5. 通过可用选项管理您的聚合 ••• 菜单。

要将磁盘添加到聚合，聚合中的所有磁盘必须具有相同的大小。

对于 AWS，您可以增加支持 Amazon EBS 弹性卷的聚合的容量。

1. 根据 ••• 菜单上，单击*增加容量*。
2. 输入您想要添加的额外容量，然后单击*增加*。

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%。例如，如果您有 1.77 TiB 聚合，则 10% 就是 181 GiB。这低于 256 GiB，因此聚合的大小必须增加 256 GiB 的最小值。

在控制台代理上管理Cloud Volumes ONTAP聚合容量

每个控制台代理都有设置来确定如何管理Cloud Volumes ONTAP的聚合容量。

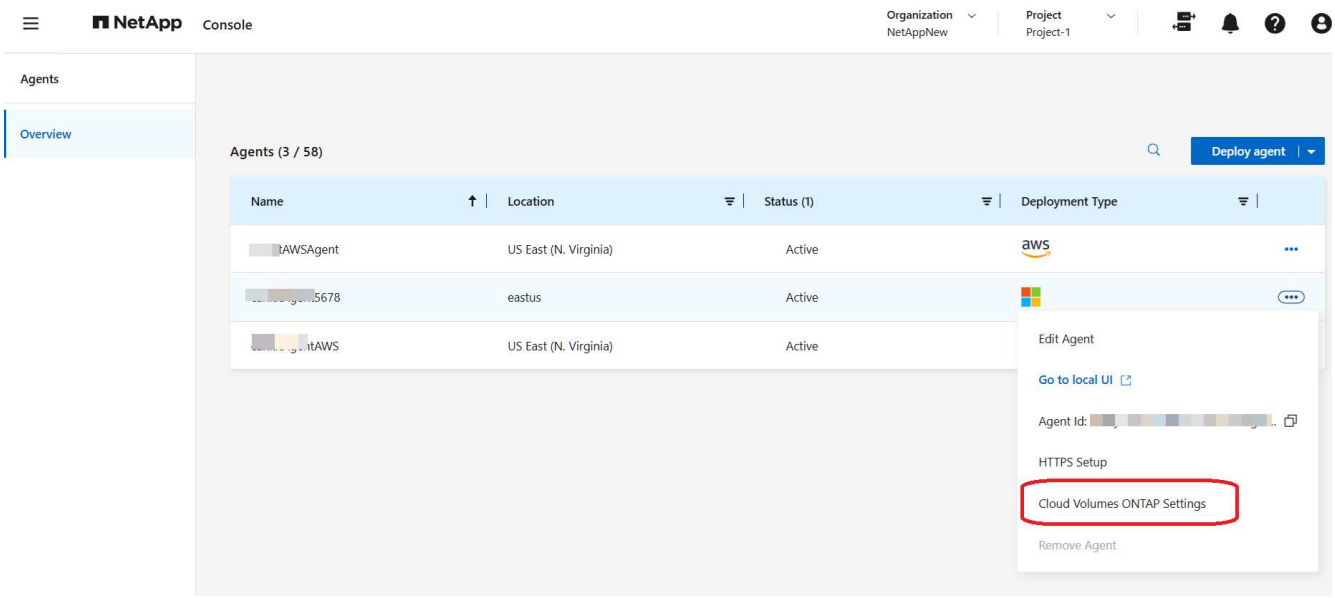
这些设置会影响控制台代理管理的所有Cloud Volumes ONTAP系统。如果您有另一个控制台代理，则可以进行不同的配置。

所需权限

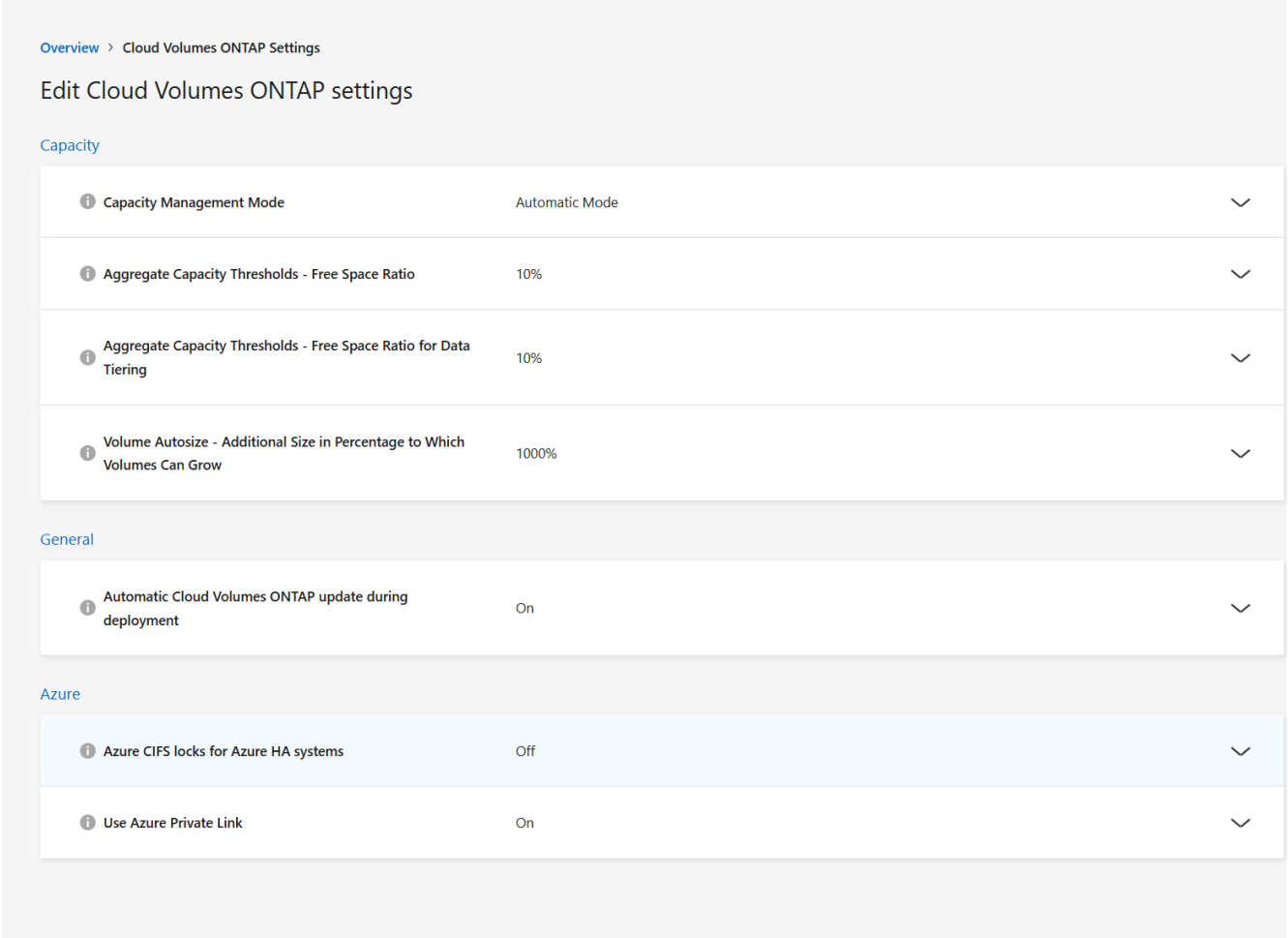
您需要NetApp Console的组织或帐户管理员权限才能修改Cloud Volumes ONTAP设置。

步骤

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



4. 在“容量”下，修改以下任意设置：



容量管理模式

选择控制台是否应通知您存储容量决策，或者是否应自动为您管理容量需求。

"了解容量管理模式的工作原理" 。

总容量阈值 - 可用空间比率

该比率是容量管理决策中的一个关键参数，无论您处于自动还是手动容量管理模式，了解其影响都至关重要。建议根据您的特定存储需求和预期增长来设置此阈值，以保持资源利用率和成本之间的平衡。

在手动模式下，如果聚合上的可用空间比率低于指定的阈值，则会触发通知，提醒您应采取措施解决低可用空间比率问题。监控这些通知并手动管理总容量以避免服务中断并确保最佳性能非常重要。

可用空间比率计算如下：（聚合容量 - 聚合上的总使用容量）/聚合容量

参考"自动容量管理"现在了解容量在Cloud Volumes ONTAP中自动管理。

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）上需要多少可用空间。

该比率对于灾难恢复场景很重要。当从容量层读取数据时， Cloud Volumes ONTAP会将数据移动到性能层以提供更好的性能。如果没有足够的空间，那么Cloud Volumes ONTAP就无法移动数据。

5. 单击“保存”。

在 Azure 中管理磁盘性能

在 Azure 中管理Cloud Volumes ONTAP的 Premium SSD v2 磁盘性能

您可以通过配置 Premium SSD v2 磁盘的 IOPS 和吞吐量参数来优化 Azure 中的Cloud Volumes ONTAP性能。此功能仅在Cloud Volumes ONTAP已部署 Azure Premium SSD v2 磁盘类型时可用，在初始部署期间不可用。通过提升性能，您可以充分利用 Azure Premium SSD v2 磁盘的灵活性和高性能功能。

Premium SSD v2 磁盘支持需要快速、可靠性能、低延迟、高 IOPS 和高吞吐量的工作负载。通过调整 IOPS 和吞吐量设置，您可以定制部署中聚合的性能。有关 Premium SSD v2 磁盘的更多信息，请参阅 "部署高级 SSD v2 磁盘"。

使用 API 实现修改 Premium SSD v2 磁盘设置的自动化过程。有关运行Cloud Volumes ONTAP API 调用的信息，请参阅 "您的第一次 API 调用"。

关于此任务

- 此功能适用于 Azure 单一可用性区域中的Cloud Volumes ONTAP部署。
- 更改磁盘设置会统一改变 RAID 组或聚合的性能。为了确保整个集群性能的一致性，集群中所有磁盘的性能都调整到同一水平。
- 这些变更仅影响单个聚合体，不会影响组内的其他聚合体。
- 在NetApp Console中部署Cloud Volumes ONTAP或进行容量优化时自动配置的高级 SSD v2 磁盘，或通过 API 添加的高级 SSD v2 磁盘，均可进行修改。
- 不支持磁盘调整大小（更改磁盘容量）。

开始之前

在配置 Premium SSD v2 磁盘的 IOPS 和吞吐量参数之前，请注意以下几点：

- 请确保您仅选择了高级 SSD v2 数据磁盘。 Premium SSD v1 磁盘或根磁盘和启动磁盘不符合此更改条件。
- 使用Cloud Volumes ONTAP在部署期间建立的预配置基线设置作为相应磁盘大小的最小 IOPS 和吞吐量值。这些基准设置与 Premium SSD v1 的性能特点相符。
- 将 IOPS 和吞吐量值设置为等于或高于磁盘大小的最低基准值。例如，对于 1TB 的磁盘大小，将最小 IOPS 值设置为 5,000，将最小吞吐量值设置为 200 MBps。您可以设置高于这些最小值的值，但不能低于这些最小值。
- 在支持的 Premium SSD v2 范围内配置值：IOPS 在 3000 到 80000 之间，吞吐量在 125 到 1200 MBps 之间。
- 请确保您的 Premium SSD v2 磁盘大小在 Azure Cloud Volumes ONTAP支持的 500GB 到 32TB 范围内。请注意，这些大小限制与 Azure 为高级 SSD v2 磁盘提供的最小值和最大值不同。

步骤

- 使用以下 API 调用来更改 IOPS 和吞吐量的属性值：

  在 24 小时内，您最多可以调用此 API 四次。

```
PUT /azure/vsa/aggregates/{workingEnvironmentId}/{aggregateName}
```

在请求主体中包含以下参数：

```
{
  "aggregateName": "aggr_name",
  "iops": "modified_iops_value",
  "throughput": "modified_throughput_value",
  "workingEnvironmentId": "we_id"
}
```

完成后

API 返回响应表明操作成功后，请在 Azure 门户中检查Cloud Volumes ONTAP系统的磁盘详细信息，以验证修改后的参数。

相关信息

- "准备使用 API"
- "Cloud Volumes ONTAP工作流程"
- "获取所需的标识符"
- "使用 REST API 访问Cloud Volumes ONTAP"
- "在可用性集中将 Premium SSD v2 与虚拟机一起使用"

在 **Azure Cloud Volumes ONTAP**中更改高级 **SSD** 磁盘的性能层级

您可以使用 Azure 门户升级 Azure Cloud Volumes ONTAP中高级 SSD 托管磁盘的性能层级。这是一个手动过程，涉及将每个高级 SSD 磁盘的磁盘层级更改为更高性能的层级。更改NVRAM磁盘的性能层级可以通过提供更高的 IOPS 和吞吐量能力来帮助缓解性能瓶颈并提高Cloud Volumes ONTAP系统的效率。

请务必与NetApp支持团队合作，确定您环境中遇到的瓶颈是由于NVRAM磁盘引起的，升级该层级可以解决该问题。

关于此任务

- 默认情况下，Azure 中的Cloud Volumes ONTAP在 P20 层部署高级 SSD 磁盘作为NVRAM 。P20 层级提供均衡的性能，适合大多数工作负载。但是，如果您的工作负载需要更高的性能，您可以将NVRAM磁盘升级到更高的级别，例如 P30。

  目前，您只能通过 Azure 门户将NVRAM磁盘从 P20 层升级到 P30 层。

- 您无需更改磁盘大小。容量仍然是 512 GB。此操作只会改变磁盘的性能等级。

开始之前

- 仔细评估是否有必要进行此项更改，因为将NVRAM磁盘升级到更高性能级别会产生额外的成本。
- 您的Cloud Volumes ONTAP版本必须为 9.11.1 或更高版本。对于较低版本，您可以升级到 9.11.1 或更高版本，或者向NetApp支持部门提出功能策略变更请求 (FPVR)。

步骤

此场景假设有两个节点 `node01` 和 `node02` 在Cloud Volumes ONTAP高可用性 (HA) 部署中。使用 Azure 门户升级层级。

1. 运行此命令以生成 `node1` 活动节点。手动故障转移 `node02`。

   ```
   storage failover takeover -ofnode <Node02>
   ```

2. Sign inAzure 门户。
3. 接管完成后，请转到虚拟机实例。 `node02`然后点击“停止”按钮将其关闭。
4. 导航至资源组 `node02` 从磁盘列表中选择NVRAM磁盘以更改层级。
5. 选择*尺寸+性能*。
6. 在“性能等级”下拉菜单中，选择 `P30 - 5000 IOPS, 200MB/s`。
7. 选择*调整大小*。
8. 打开 `node02` 实例。
9. 检查 Azure 串行控制台，直到看到以下消息： `waiting for giveback`。
10. 运行此命令即可回馈 `node02`：

    ```
    storage failover giveback -ofnode <Node02>
    ```

11. 重复这些步骤 `node01` 制作 `node02` 接管 `node01``这样您就可以升级NVRAM磁盘层。 `node01`。

完成后

当您启动两个节点后，请在 Azure 门户中检查Cloud Volumes ONTAP系统的磁盘详细信息，以验证修改后的参数。

相关信息

- Azure 文档： "无需停机即可更改性能等级"
- 支持团队知识库： "如何在 Azure CVO 中升级NVRAM磁盘的性能层"
- "升级Cloud Volumes ONTAP软件版本"

存储虚拟机管理

管理**Cloud Volumes ONTAP** 的存储虚拟机

存储虚拟机是在ONTAP内运行的虚拟机，可为您的客户端提供存储和数据服务。您可能知道这是一个_SVM_或_vserver_。 Cloud Volumes ONTAP默认配置一个存储虚拟机，但某些配置支持额外的存储虚拟机。

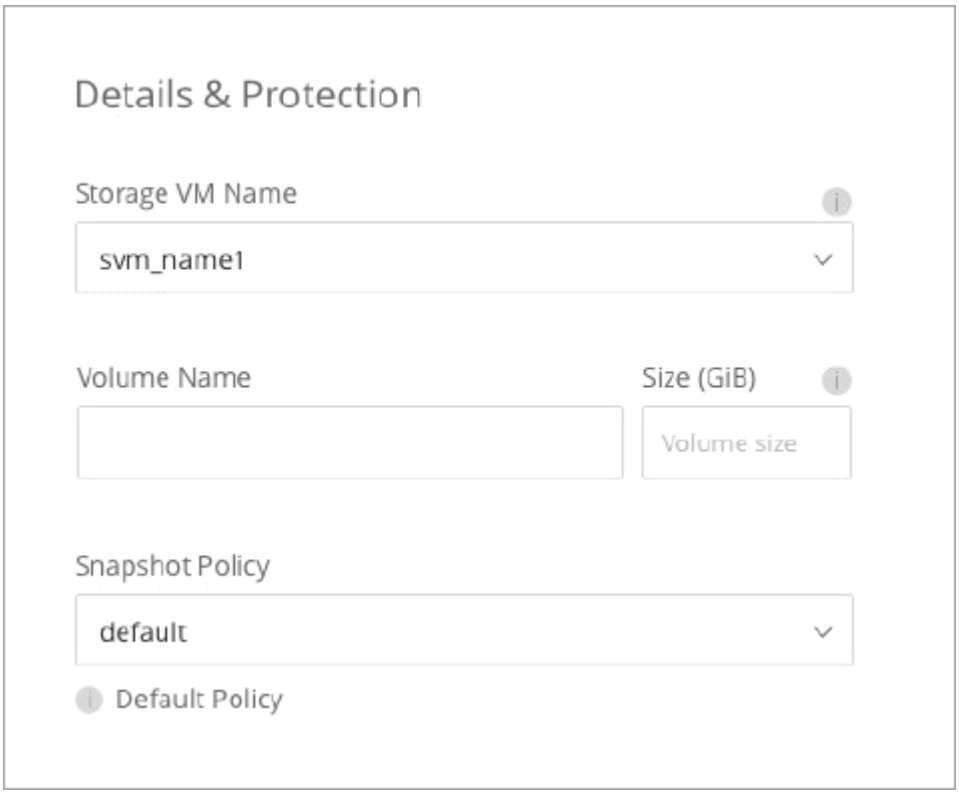
支持的存储虚拟机数量

特定配置支持多个存储虚拟机。前往 "Cloud Volumes ONTAP发行说明"验证您的Cloud Volumes ONTAP版本支持的存储虚拟机数量。

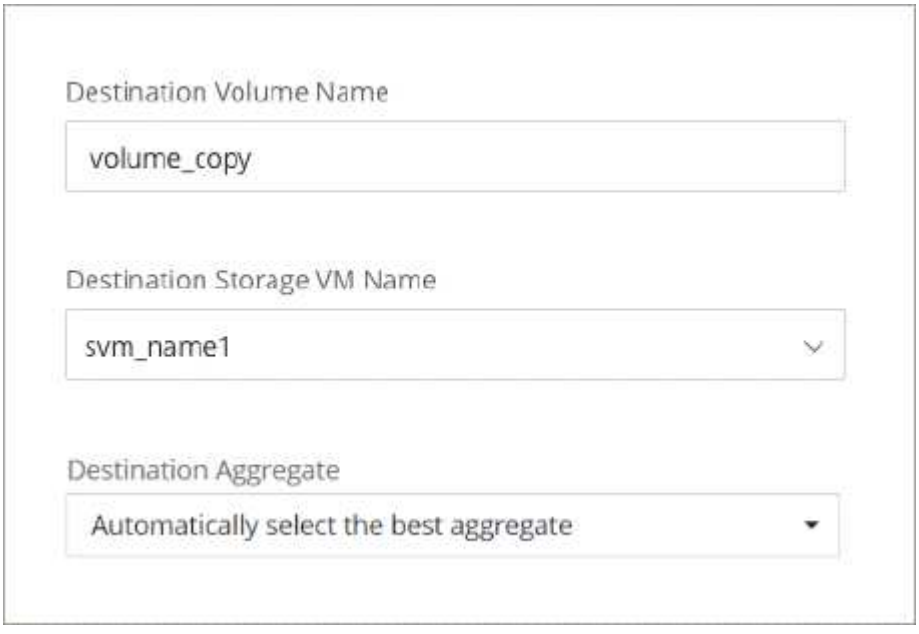
使用多个存储虚拟机

NetApp Console支持您从ONTAP系统管理器或ONTAP CLI 创建的任何其他存储虚拟机。

例如，下图显示了如何在创建卷时选择存储虚拟机。



下图显示了将卷复制到另一个系统时如何选择存储虚拟机。



修改默认存储虚拟机的名称

控制台会自动命名其为Cloud Volumes ONTAP创建的单个存储虚拟机。如果您有严格的命名标准，则可以

从ONTAP系统管理器、 ONTAP CLI 或 API 修改存储虚拟机的名称。例如，您可能希望该名称与ONTAP集群的存储虚拟机的命名方式相匹配。

管理 AWS 中Cloud Volumes ONTAP的数据服务存储虚拟机

存储虚拟机是在ONTAP内运行的虚拟机，可为您的客户端提供存储和数据服务。您可能知道这是一个_SVM_或_vserver_。 Cloud Volumes ONTAP默认配置一个存储虚拟机，但某些配置支持额外的存储虚拟机。

要创建额外的数据服务存储虚拟机，您需要在 AWS 中分配 IP 地址，然后根据您的Cloud Volumes ONTAP配置运行ONTAP命令。

支持的存储虚拟机数量

从 9.7 版本开始，特定的Cloud Volumes ONTAP配置支持多个存储虚拟机。前往 "Cloud Volumes ONTAP发行说明"验证您的Cloud Volumes ONTAP版本支持的存储虚拟机数量。

所有其他Cloud Volumes ONTAP配置都支持一个数据服务存储虚拟机和一个用于灾难恢复的目标存储虚拟机。如果源存储虚拟机发生中断，您可以激活目标存储虚拟机进行数据访问。

验证配置的限制

每个 EC2 实例支持每个网络接口的最大私有 IPv4 地址数量。在 AWS 中为新的存储虚拟机分配 IP 地址之前，您需要验证限制。

步骤

1. 去 "Cloud Volumes ONTAP发行说明中的存储限制部分"。
2. 确定您的实例类型每个接口的最大 IP 地址数。
3. 记下这个号码，因为在下一节中分配 AWS 中的 IP 地址时需要它。

在 **AWS** 中分配 **IP** 地址

在为新的存储虚拟机创建 LIF 之前，必须将私有 IPv4 地址分配给 AWS 中的端口 e0a。

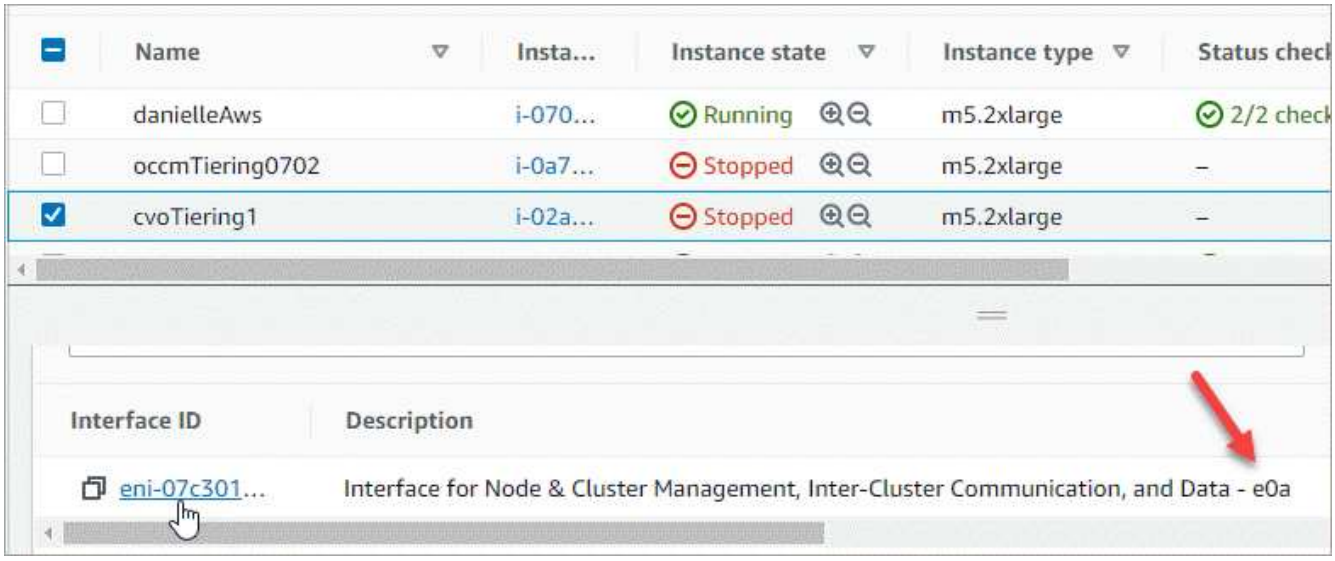
请注意，存储虚拟机的可选管理 LIF 需要单节点系统上的专用 IP 地址和单个 AZ 中的 HA 对。此管理 LIF 提供与 SnapCenter 等管理工具的连接。

步骤

1. 登录AWS并开启EC2服务。
2. 选择Cloud Volumes ONTAP实例并单击 网络。

   如果您要在 HA 对上创建存储虚拟机，请选择节点 1。

3. 向下滚动到*网络接口*并单击端口 e0a 的*接口 ID*。



4. 选择网络接口并单击*操作>管理 IP 地址*。
5. 展开 e0a 的 IP 地址列表。
6. 验证 IP 地址：
   a. 计算已分配的 IP 地址数量，以确认端口是否有空间容纳额外的 IP。

      您应该已经在本页的上一节中确定了每个接口支持的最大 IP 地址数量。

   b. 可选：转到Cloud Volumes ONTAP的ONTAP CLI 并运行 **network interface show** 以确认每个 IP 地址都在使用中。

      如果 IP 地址未被使用，那么您可以将其与新的存储 VM 一起使用。

7. 返回 AWS 控制台，单击“分配新 IP 地址”以根据新存储 VM 所需的数量分配其他 IP 地址。
   - 单节点系统：需要一个未使用的辅助专用 IP。

     如果您想在存储虚拟机上创建管理 LIF，则需要可选的辅助私有 IP。

   - 单个 AZ 中的 HA 对：节点 1 上需要一个未使用的辅助私有 IP。

     如果您想在存储虚拟机上创建管理 LIF，则需要可选的辅助私有 IP。

   - 多个可用区中的 HA 对：每个节点都需要一个未使用的辅助私有 IP。
8. 如果您要在单个 AZ 中的 HA 对上分配 IP 地址，请启用*允许重新分配辅助私有 IPv4 地址*。
9. 单击“保存”。
10. 如果您在多个可用区中有一个 HA 对，则需要对节点 2 重复这些步骤。

在单节点系统上创建存储虚拟机

这些步骤在单节点系统上创建新的存储虚拟机。创建 NAS LIF 需要一个私有 IP 地址，如果要创建管理 LIF，则需要另一个可选私有 IP 地址。

步骤

1. 创建存储虚拟机和到存储虚拟机的路由。

```
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 上未使用的辅助私有 IP。

3. 可选：创建存储虚拟机管理 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 上另一个未使用的辅助私有 IP。

4. 将一个或多个聚合分配给存储虚拟机。

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

此步骤是必需的，因为新的存储虚拟机需要访问至少一个聚合，然后您才能在存储虚拟机上创建卷。

在单个可用区内的 **HA** 对上创建存储虚拟机

这些步骤在单个 AZ 中的 HA 对上创建一个新的存储虚拟机。创建 NAS LIF 需要一个私有 IP 地址，如果要创建管理 LIF，则需要另一个可选的私有 IP 地址。

这两个 LIF 都分配在节点 1 上。如果发生故障，私有 IP 地址可以在节点之间移动。

步骤

1. 创建存储虚拟机和到存储虚拟机的路由。

```
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 上未使用的辅助私有 IP。在接管的情况下，该 IP 地址可以重新定位到 cvo-node2 的 e0a，因为服务策略 default-data-files 表明 IP 可以迁移到合作伙伴节点。

3. 可选：在节点 1 上创建存储虚拟机管理 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 上另一个未使用的辅助私有 IP。

4. 将一个或多个聚合分配给存储虚拟机。

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

此步骤是必需的，因为新的存储虚拟机需要访问至少一个聚合，然后您才能在存储虚拟机上创建卷。

5. 如果您运行的是Cloud Volumes ONTAP 9.11.1 或更高版本，请修改存储虚拟机的网络服务策略。

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
```

在多个可用区的 **HA** 对上创建存储虚拟机

这些步骤在多个 AZ 中的 HA 对上创建一个新的存储虚拟机。

对于 NAS LIF 来说，浮动 IP 地址是必需的，而对于管理 LIF 来说，浮动 IP 地址是可选的。这些浮动 IP 地址不需要您在 AWS 中分配私有 IP。相反，浮动 IP 会在 AWS 路由表中自动配置为指向同一 VPC 中特定节点的 ENI。

为了使浮动 IP 与ONTAP一起工作，必须在每个节点上的每个存储虚拟机上配置一个私有 IP 地址。这反映在以下步骤中，其中在节点 1 和节点 2 上创建 iSCSI LIF。

步骤

1. 创建存储虚拟机和到存储虚拟机的路由。

```
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
```

   - 浮动 IP 地址必须位于您部署 HA 配置的 AWS 区域中的所有 VPC 的 CIDR 块之外。 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 可以迁移到伙伴节点。

3. 可选：在节点 1 上创建存储虚拟机管理 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 nodei1Mask -lif
ip_node1_iscsi_2 -home-node cvo-node1
```

   - 此 iSCSI LIF 需要支持存储虚拟机中浮动 IP 的 LIF 迁移。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) 上未使用的辅助私有 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
```

   - 此 iSCSI LIF 需要支持存储虚拟机中浮动 IP 的 LIF 迁移。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) 上未使用的辅助私有 IP 地址。

6. 将一个或多个聚合分配给存储虚拟机。

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

此步骤是必需的，因为新的存储虚拟机需要访问至少一个聚合，然后您才能在存储虚拟机上创建卷。

7. 如果您运行的是Cloud Volumes ONTAP 9.11.1 或更高版本，请修改存储虚拟机的网络服务策略。

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
```

管理 **Azure** 中**Cloud Volumes ONTAP**的数据服务存储虚拟机

存储虚拟机是在ONTAP内运行的虚拟机，可为您的客户端提供存储和数据服务。您可能知道这是一个_SVM_或_vserver_。 Cloud Volumes ONTAP默认配置一个存储虚拟机，但您可以在 Azure 中运行Cloud Volumes ONTAP时创建其他存储虚拟机。

要在 Azure 中创建和管理其他数据服务存储虚拟机，您应该使用 API。这是因为 API 自动化了创建存储虚拟机和配置所需网络接口的过程。创建存储虚拟机时， NetApp Console会配置所需的 LIF 服务，以及存储虚拟机出站 SMB/CIFS 通信所需的 iSCSI LIF。

有关运行Cloud Volumes ONTAP API 调用的信息，请参阅 "您的第一次 API 调用"。

支持的存储虚拟机数量

从Cloud Volumes ONTAP 9.9.0 开始，根据您的许可证，支持具有特定配置的多个存储虚拟机。请参阅 "Cloud Volumes ONTAP发行说明"验证您的Cloud Volumes ONTAP版本支持的存储虚拟机数量。

9.9.0 之前的所有Cloud Volumes ONTAP版本都支持一个数据服务存储虚拟机和一个用于灾难恢复的目标存储虚拟机。如果源存储虚拟机发生中断，您可以激活目标存储虚拟机进行数据访问。

创建存储虚拟机

根据您的配置和许可证类型，您可以使用 NetApp Console 的 API 在单节点系统或高可用性 (HA) 配置中创建多个存储虚拟机。

关于此任务

当您使用 API 创建存储虚拟机并配置所需的网络接口时，控制台还会修改 `default-data-files`通过从 NAS 数据 LIF 中删除以下服务并将其添加到用于出站管理连接的 iSCSI 数据 LIF，可以在数据存储虚拟机上实施策略：

- `data-fpolicy-client`
- `management-ad-client`
- `management-dns-client`
- `management-ldap-client`
- `management-nis-client`

开始之前

控制台代理需要特定权限才能为Cloud Volumes ONTAP创建存储虚拟机。所需权限包含在 "NetApp提供的政策"。

单节点系统

使用以下 API 调用在单节点系统上创建存储 VM。

```
POST /azure/vsa/working-environments/{workingEnvironmentId}/svm
```

在请求主体中包含以下参数：

```
{ "svmName": "myNewSvm1"
   "svmPassword": "optional, the API takes the cluster password if not
provided"
   "mgmtLif": "optional, to create an additional management LIF, if you
want to use the storage VM for management purposes"}
```

HA 对

使用以下 API 调用在 HA 对上创建存储虚拟机：

```
POST /azure/ha/working-environments/{workingEnvironmentId}/svm
```

在请求主体中包含以下参数：

```
{ "svmName": "NewSvmName"
   "svmPassword": "optional value, the API takes the cluster password if
not provided"
   "mgmtLif": "optional value, to create an additional management LIF, if
you want to use the storage VM for management purposes"}
```

管理单节点系统和 HA 对上的 Storage VM

使用 API，您可以重命名和删除单节点和 HA 配置中的存储虚拟机。

开始之前

控制台代理需要特定权限来管理Cloud Volumes ONTAP 的存储虚拟机。所需权限包含在 "NetApp提供的政策"。

重命名存储虚拟机

要重命名存储虚拟机，您应该提供现有存储虚拟机和新存储虚拟机的名称作为参数。

步骤

- 使用以下 API 调用来重命名单节点系统上的存储 VM：

  ```
  PUT /azure/vsa/working-environments/{workingEnvironmentId}/svm
  ```

  在请求主体中包含以下参数：

  ```
  {
    "svmNewName": "NewSvmName",
    "svmName": "OldSvmName"
  }
  ```

- 使用以下 API 调用重命名 HA 对上的存储虚拟机：

```
PUT /azure/ha/working-environments/{workingEnvironmentId}/svm
```

在请求主体中包含以下参数：

```
{
  "svmNewName": "NewSvmName",
  "svmName": "OldSvmName"
}
```

删除存储虚拟机

在单节点或 HA 配置中，如果存储虚拟机没有任何活动卷，则可以将其删除。

步骤

- 使用以下 API 调用来删除单节点系统上的存储 VM：

  ```
  DELETE /azure/vsa/working-environments/{workingEnvironmentId}/svm/{svmName}
  ```

- 使用以下 API 调用删除 HA 对上的存储虚拟机：

  ```
  DELETE /azure/ha/working-environments/{workingEnvironmentId}/svm/{svmName}
  ```

相关信息

- "准备使用 API"
- "Cloud Volumes ONTAP工作流程"
- "获取所需的标识符"
- "使用NetApp Console的 REST API"

在 Google Cloud 中管理Cloud Volumes ONTAP的数据服务存储虚拟机

存储虚拟机是在ONTAP内运行的虚拟机，可为您的客户端提供存储和数据服务。您可能知道这是一个_SVM_或_vserver_。 Cloud Volumes ONTAP默认配置一个存储虚拟机，但某些配置支持额外的存储虚拟机。

要在 Google Cloud 中创建和管理其他数据服务存储虚拟机，您应该使用 API。这是因为 API 自动化了创建存储虚拟机和配置所需网络接口的过程。创建存储虚拟机时， NetApp Console会配置所需的 LIF 服务，以及存储虚拟机出站 SMB/CIFS 通信所需的 iSCSI LIF。

有关运行Cloud Volumes ONTAP API 调用的信息，请参阅 "您的第一次 API 调用"。

支持的存储虚拟机数量

从Cloud Volumes ONTAP 9.11.1 开始，根据您的许可证，支持具有特定配置的多个存储虚拟机。请参阅 "Cloud Volumes ONTAP发行说明"验证您的Cloud Volumes ONTAP版本支持的存储虚拟机数量。

9.11.1 之前的所有Cloud Volumes ONTAP版本都支持一个数据服务存储虚拟机和一个用于灾难恢复的目标存储

虚拟机。如果源存储虚拟机发生中断，您可以激活目标存储虚拟机进行数据访问。

创建存储虚拟机

根据您的配置和许可证类型，您可以使用 API 在单节点系统上或在高可用性 (HA) 配置中创建多个存储 VM。

关于此任务

当您使用 API 创建存储虚拟机并配置所需的网络接口时，控制台还会修改 `default-data-files`通过从 NAS 数据 LIF 中删除以下服务并将其添加到用于出站管理连接的 iSCSI 数据 LIF，可以在数据存储虚拟机上实施策略：

- `data-fpolicy-client`
- `management-ad-client`
- `management-dns-client`
- `management-ldap-client`
- `management-nis-client`

开始之前

控制台代理需要特定权限才能为Cloud Volumes ONTAP HA 对创建存储虚拟机。所需的权限包含在……"NetApp提供的政策" 。

单节点系统

使用以下 API 调用在单节点系统上创建存储 VM。

```
POST /gcp/vsa/working-environments/{workingEnvironmentId}/svm
```

在请求主体中包含以下参数：

```
{ "svmName": "NewSvmName"
   "svmPassword": "optional value, the API takes the cluster password if
not provided"
   "mgmtLif": "optional value, to create an additional management LIF, if
you want to use the storage VM for management purposes"}
```

HA 对

使用以下 API 调用在 HA 对上创建存储虚拟机：

```
POST /gcp/ha/working-environments/{workingEnvironmentId}/svm/
```

在请求主体中包含以下参数：

```
{ "svmName": "NewSvmName"
   "svmPassword": "optional value, the API takes the cluster password if
not provided"
}
```

管理存储虚拟机

使用 API，您可以重命名和删除单节点和 HA 配置中的存储虚拟机。

开始之前

控制台代理需要特定权限来管理Cloud Volumes ONTAP HA 对的存储虚拟机。所需的权限包含在…… "NetApp 提供的政策" 。

重命名存储虚拟机

要重命名存储虚拟机，您应该提供现有存储虚拟机和新存储虚拟机的名称作为参数。

步骤

- 使用以下 API 调用来重命名单节点系统上的存储 VM：

  `PUT /gcp/vsa/working-environments/{workingEnvironmentId}/svm`

  在请求主体中包含以下参数：

  ```
  {
    "svmNewName": "NewSvmName",
    "svmName": "OldSvmName"
  }
  ```

- 使用以下 API 调用重命名 HA 对上的存储虚拟机：

  `PUT /gcp/ha/working-environments/{workingEnvironmentId}/svm`

  在请求主体中包含以下参数：

  ```
  {
    "svmNewName": "NewSvmName",
    "svmName": "OldSvmName"
  }
  ```

删除存储虚拟机

在单节点或 HA 配置中，如果存储虚拟机没有任何活动卷，则可以将其删除。

步骤

- 使用以下 API 调用来删除单节点系统上的存储 VM：

```
DELETE /gcp/vsa/working-environments/{workingEnvironmentId}/svm/{svmName}
```

- 使用以下 API 调用删除 HA 对上的存储虚拟机：

```
DELETE /gcp/ha/working-environments/{workingEnvironmentId}/svm/{svmName}
```

相关信息

- "准备使用 API"
- "Cloud Volumes ONTAP工作流程"
- "获取所需的标识符"
- "使用NetApp Console的 REST API"

为Cloud Volumes ONTAP设置存储虚拟机灾难恢复

NetApp Console不提供存储虚拟机 (SVM) 灾难恢复的设置或编排支持。要执行这些任务，请使用ONTAP System Manager 或ONTAP 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。无法在 HA 对和单节点系统之间设置 SnapMirror SVM 复制。

有关ONTAP 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》"

安全和数据加密

使用NetApp加密解决方案加密Cloud Volumes ONTAP上的卷

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，可实现符合 FIPS 140-2 标准的卷静态数据加密。"了解有关这些加密解决方案的更多信息" 。

NVE 和 NAE 均由外部密钥管理器支持。

如果def::aws[] endif::aws[] 如果def::azure[] endif::azure[] 如果def::gcp[] endif::gcp[] 如果def::aws[] endif::aws[] 如果def::azure[] endif::azure[] 如果def::gcp[] endif::gcp[]

使用 AWS Key Management Service 管理Cloud Volumes ONTAP加密密钥

您可以使用"AWS 的密钥管理服务 (KMS)"在 AWS 部署的应用程序中保护您的ONTAP加密密钥。

可以使用 CLI 或ONTAP REST API 启用 AWS KMS 的密钥管理。

使用 KMS 时，请注意默认情况下使用数据 SVM 的 LIF 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，并且
- 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。

配置

AWS

1. 您必须创建一个"授予"用于管理加密的 IAM 角色将使用的 AWS KMS 密钥。 IAM 角色必须包含允许以下操作的策略：
   - `DescribeKey`
   - `Encrypt`
   - `Decrypt`要创建赠款，请参阅"AWS 文档"。
2. "向适当的 IAM 角色添加策略。"政策应该支持 `DescribeKey`， `Encrypt` ， 和 `Decrypt`运营。

Cloud Volumes ONTAP

1. 切换到您的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，输入密钥。
5. 确认 AWS KMS 配置正确：
   `security key-manager external aws show -vserver svm_name`

使用 **Azure Key Vault** 管理**Cloud Volumes ONTAP**加密密钥

您可以使用 Azure Key Vault (AKV) 来保护 Azure 部署的应用程序中ONTAP加密密钥。请参阅"Microsoft 文档"。

AKV 仅可用于保护数据 SVM 的NetApp卷加密 (NVE) 密钥。欲了解更多信息，请参阅"ONTAP 文档" 。

可以使用 CLI 或ONTAP REST API 启用 AKV 密钥管理。

使用 AKV 时，请注意默认情况下使用数据 SVM LIF 与云密钥管理端点通信。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（NetApp卷加密许可证会自动安装在每个在NetApp支持中注册的Cloud Volumes ONTAP系统上）
- 您必须拥有多租户加密密钥管理 (MT_EK_MGMT) 许可证
- 您必须是集群或 SVM 管理员
- 有效的 Azure 订阅

限制

- AKV 只能在数据 SVM 上配置
- NAE 不能与 AKV 一起使用。 NAE 需要外部支持的 KMIP 服务器。
- Cloud Volumes ONTAP节点每 15 分钟轮询一次 AKV，以确认可访问性和密钥可用性。此轮询周期是不可配置的，并且在轮询尝试连续四次失败后（总共 1 小时），卷将处于脱机状态。

配置过程

概述的步骤捕获了如何向 Azure 注册您的Cloud Volumes ONTAP配置以及如何创建 Azure Key Vault 和密钥。如果您已经完成这些步骤，请确保您具有正确的配置设置，特别是在创建 Azure Key Vault，然后继续Cloud Volumes ONTAP配置。

- Azure 应用程序注册
- 创建 Azure 客户端机密
- 创建 Azure Key Vault
- 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. 您必须首先在 Azure 订阅中注册您希望Cloud Volumes ONTAP用于访问 Azure Key Vault 的应用程序。在 Azure 门户中，选择应用注册。
2. 选择新注册。
3. 为您的应用程序提供一个名称并选择支持的应用程序类型。默认的单个租户足以满足 Azure Key Vault 的使用。选择注册。
4. 在 Azure 概览窗口中，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。在稍后的注册过程中将需要它们。

创建 **Azure** 客户端机密

1. 在 Azure Key Vault 应用注册的 Azure 门户中，选择“证书和机密”窗格。
2. 选择新客户端密钥。为您的客户端密钥输入一个有意义的名称。 NetApp建议的有效期为 24 个月；但是，您的特定云治理策略可能需要不同的设置。
3. 单击添加以创建客户端密钥。复制值列中列出的秘密字符串，并将其存储在安全的位置，以便稍后使

用Cloud Volumes ONTAP配置。离开该页面后，秘密值将不再显示。

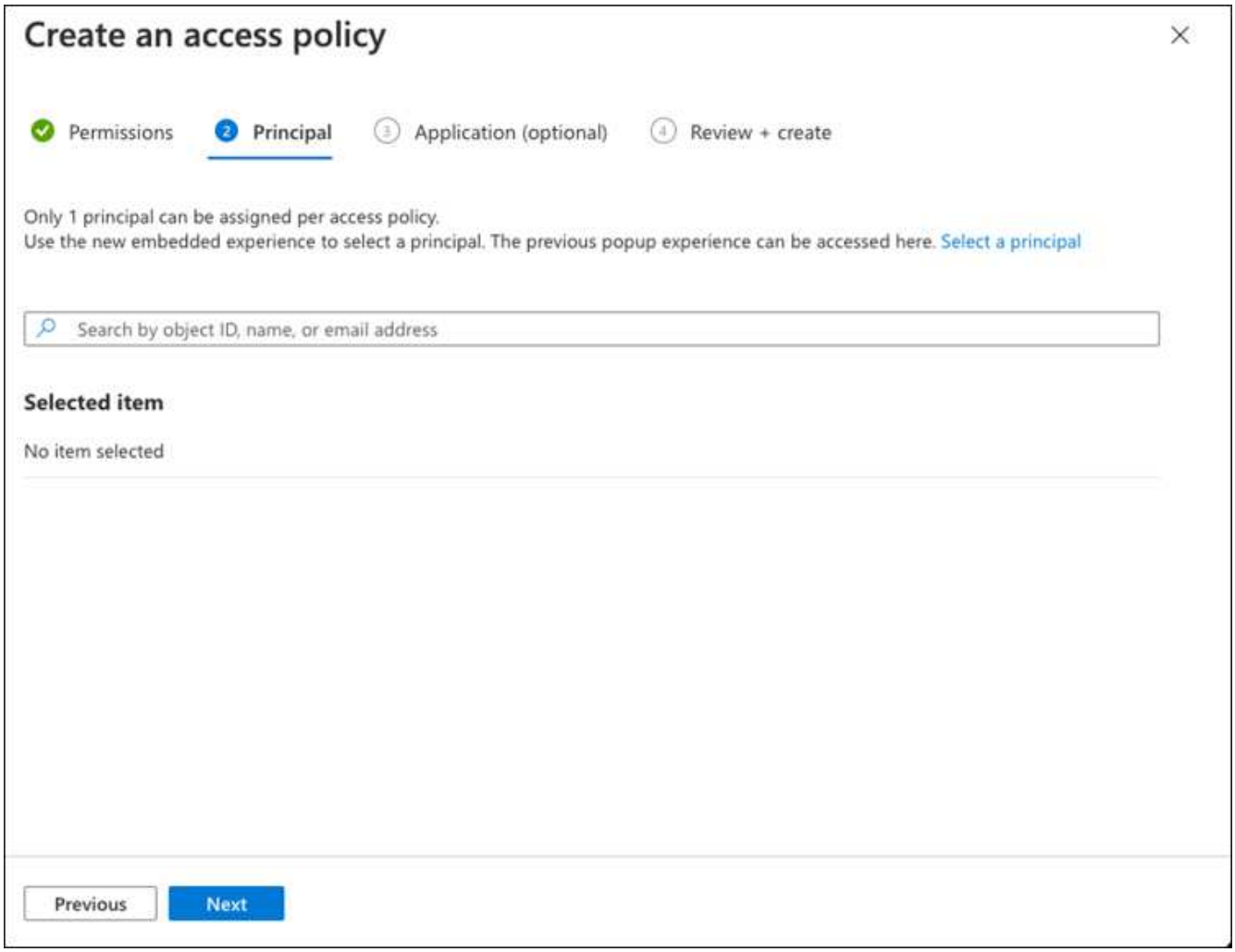
创建 **Azure Key Vault**

1. 如果您有现有的 Azure Key Vault，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 **Key Vaults** 部分。
3. 单击“+创建”并输入所需信息，包括资源组、区域和定价层。此外，输入保留已删除保管库的天数，并在密钥保管库上选择启用清除保护。
4. 选择下一步来选择访问策略。
5. 选择以下选项：
   a. 在访问配置下，选择**Vault** 访问策略。
   b. 在资源访问下，选择**Azure** 磁盘加密进行卷加密。
6. 选择“+创建”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、秘密、证书），然后在菜单列表顶部选择全选以选择所有可用的权限。您应该：
   - 关键权限：已选择 20 个
   - 秘密权限：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

9. 单击下一步，选择您在 Azure 中创建的主体注册应用程序Azure 应用程序注册。选择下一步。

   每个策略只能分配一个主体。



10. 单击下一步两次，直到到达审核并创建。然后，单击创建。
11. 选择下一步进入网络选项。
12. 选择适当的网络访问方法或选择所有网络和查看 + 创建来创建密钥保管库。 （网络访问方法可能由治理策略或您的企业云安全团队规定。）
13. 记录密钥保管库 URI：在您创建的密钥保管库中，导航到概览菜单并从右侧列复制**Vault URI**。您需要它来完成后面的步骤。

创建加密密钥

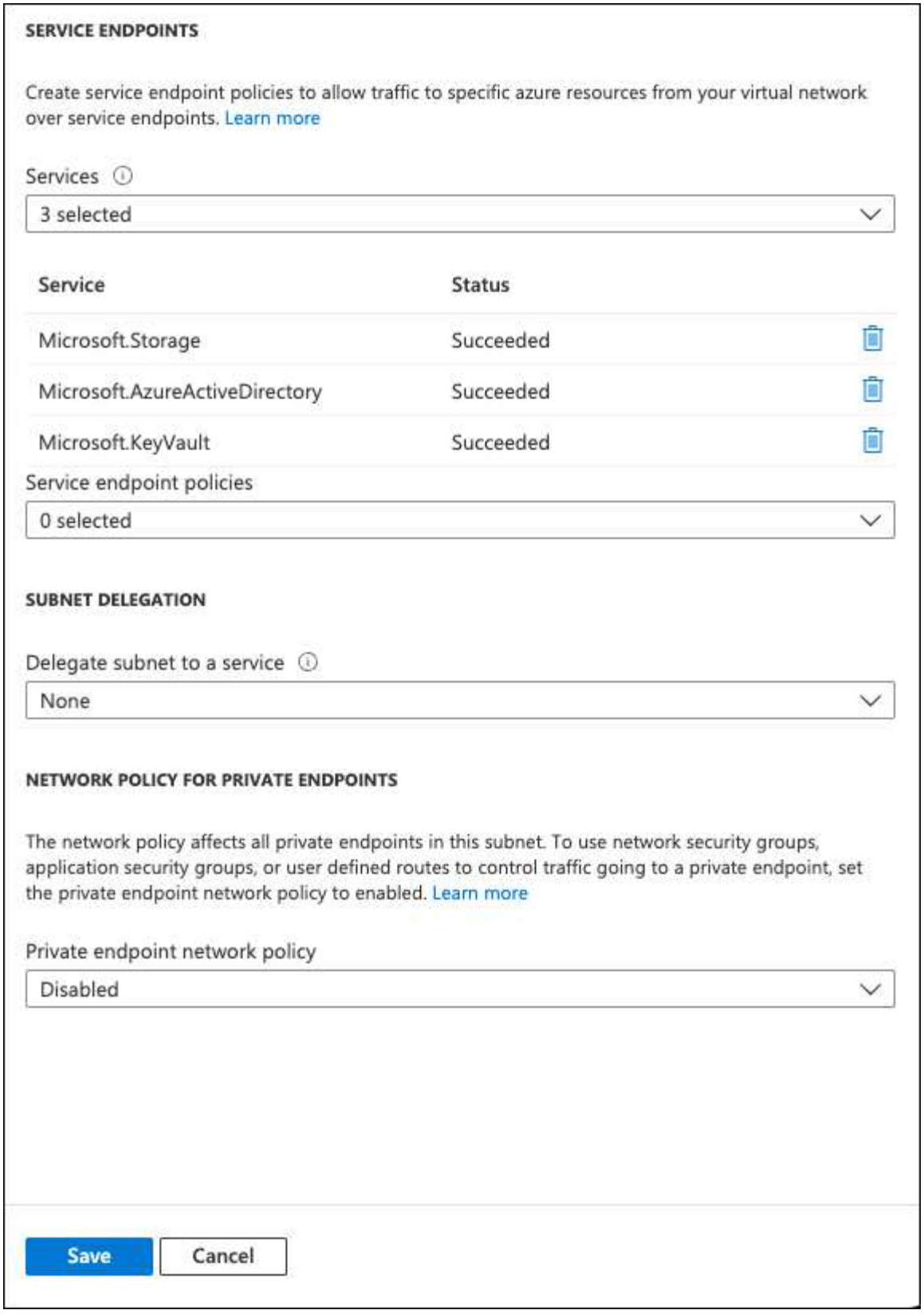
1. 在您为Cloud Volumes ONTAP创建的 Key Vault 菜单中，导航到 **Keys** 选项。
2. 选择生成/导入来创建新密钥。
3. 将默认选项设置为生成。
4. 提供以下信息：
   - 加密密钥名称

- 密钥类型：RSA
- RSA密钥大小：2048
- 已启用：是

5. 选择创建来创建加密密钥。
6. 返回**Keys**菜单并选择您刚刚创建的密钥。
7. 选择当前版本下的密钥ID，查看密钥属性。
8. 找到密钥标识符字段。复制 URI，直到但不包括十六进制字符串。

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

1. 仅当您为 HA Cloud Volumes ONTAP系统配置 Azure Key Vault 时才需要此过程。
2. 在 Azure 门户中导航到虚拟网络。
3. 选择部署Cloud Volumes ONTAP系统的虚拟网络，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：
   - **Microsoft.AzureActiveDirectory**
   - **Microsoft.KeyVault**
   - **Microsoft.Storage**（可选）



6. 选择保存来捕获您的设置。

Cloud Volumes ONTAP配置

1. 使用您首选的 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 条目存在并且包含 Azure DNS 条目，则无需执行任何操作。如果没有，请为数据 SVM 添加指向 Azure DNS、私有 DNS 或本地服务器的 DNS 服务器条目。这应该与集群管理员 SVM 的条目匹配：
      `vserver services name-service dns create -vserver SVM_name -domains domain -name-servers IP_address`

   b. 验证已为数据 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 Key Vault：
   `security key-manager external azure enable -vserver SVM_name -client-id Azure_client_ID -tenant-id Azure_tenant_ID -name key_vault_URI -key-id full_key_URI`

   这 `_full_key_URI`价值必须利用 `<https:// <key vault host name>/keys/<key label>`格式。

5. 成功启用 Azure Key Vault 后，输入 `client secret value`当出现提示时。

6. 检查密钥管理器的状态：
   `security key-manager external azure check`输出将如下所示：

```
::*> 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 无法通过所有必需的连接和权限访问 Azure Key Vault 服务。确保您的 Azure 网络策略和路由不会阻止您的私有 vNet 到达 Azure Key Vault 公共终结点。如果确实如此，请考虑使用 Azure Private 端点从 vNet 内部访问 Key Vault。您可能还需要在 SVM 上添加静态主机条目来解析端点的私有 IP 地址。

这 `kms_wrapped_key_status`将会报告 `UNKNOWN`在初始配置时。其状态将变为 `OK`第一卷加密后。

7. 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。

8. 确认卷已正确创建并加密。如果是的话， `-is-encrypted`参数将显示为 `true。
   ```
   vol show -vserver SVM_name -fields is-encrypted
   ```
9. 可选：如果要更新 Azure Key Vault 身份验证证书上的凭据，请使用以下命令：
   ```
   security key-manager external azure update-credentials -vserver v1
   -authentication-method certificate
   ```

相关链接

- "设置Cloud Volumes ONTAP以在 Azure 中使用客户管理的密钥"
- "Microsoft Azure 文档：关于 Azure Key Vault"
- "ONTAP命令参考指南"

使用 Google Cloud KMS 管理Cloud Volumes ONTAP加密密钥

您可以使用"Google Cloud Platform 的密钥管理服务（Cloud KMS）"在 Google Cloud Platform 部署的应用程序中保护您的Cloud Volumes ONTAP加密密钥。

可以使用ONTAP CLI 或ONTAP REST API 启用 Cloud KMS 的密钥管理。

使用 Cloud KMS 时，请注意默认情况下使用数据 SVM 的 LIF 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

- 您的系统应该运行Cloud Volumes ONTAP 9.10.1 或更高版本
- 您必须使用数据 SVM。 Cloud KMS 只能在数据 SVM 上配置。
- 您必须是集群或 SVM 管理员
- 应在 SVM 上安装卷加密 (VE) 许可证
- 从Cloud Volumes ONTAP 9.12.1 GA 开始，还应安装多租户加密密钥管理 (MTEKM) 许可证
- 需要有效的 Google Cloud Platform 订阅

配置

Google Cloud

1. 在您的 Google Cloud 环境中，"创建对称 GCP 密钥环和密钥" 。
2. 为 Cloud KMS 密钥和Cloud Volumes ONTAP服务帐户分配自定义角色。
   a. 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.cryptoKeyVersio
ns.list,cloudkms.cryptoKeyVersions.useToDecrypt,cloudkms.cryptoKeyVer
sions.useToEncrypt,cloudkms.cryptoKeys.get,cloudkms.keyRings.get,clou
dkms.locations.get,cloudkms.locations.list,resourcemanager.projects.g
et
    --stage=GA
```

b. 分配您创建的自定义角色：
`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`

> 如果您使用的是Cloud Volumes ONTAP 9.13.0 或更高版本，则无需创建自定义角色。您可以分配预定义的[cloudkms.cryptoKeyEncrypterDecrypter^] 角色。

3. 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. 使用您首选的 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 CMEK 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，请输入您的 GCP 帐户中的服务帐户 JSON 密钥。
6. 确认启用流程成功：
`security key-manager external gcp check -vserver svm_name`
7. 可选：创建卷来测试加密 `vol create volume_name -aggregate aggregate -vserver vserver_name -size 10G`

故障排除

如果需要进行故障排除，您可以在上面的最后两个步骤中跟踪原始 REST API 日志：

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

为Cloud Volumes ONTAP启用NetApp勒索软件防护解决方案

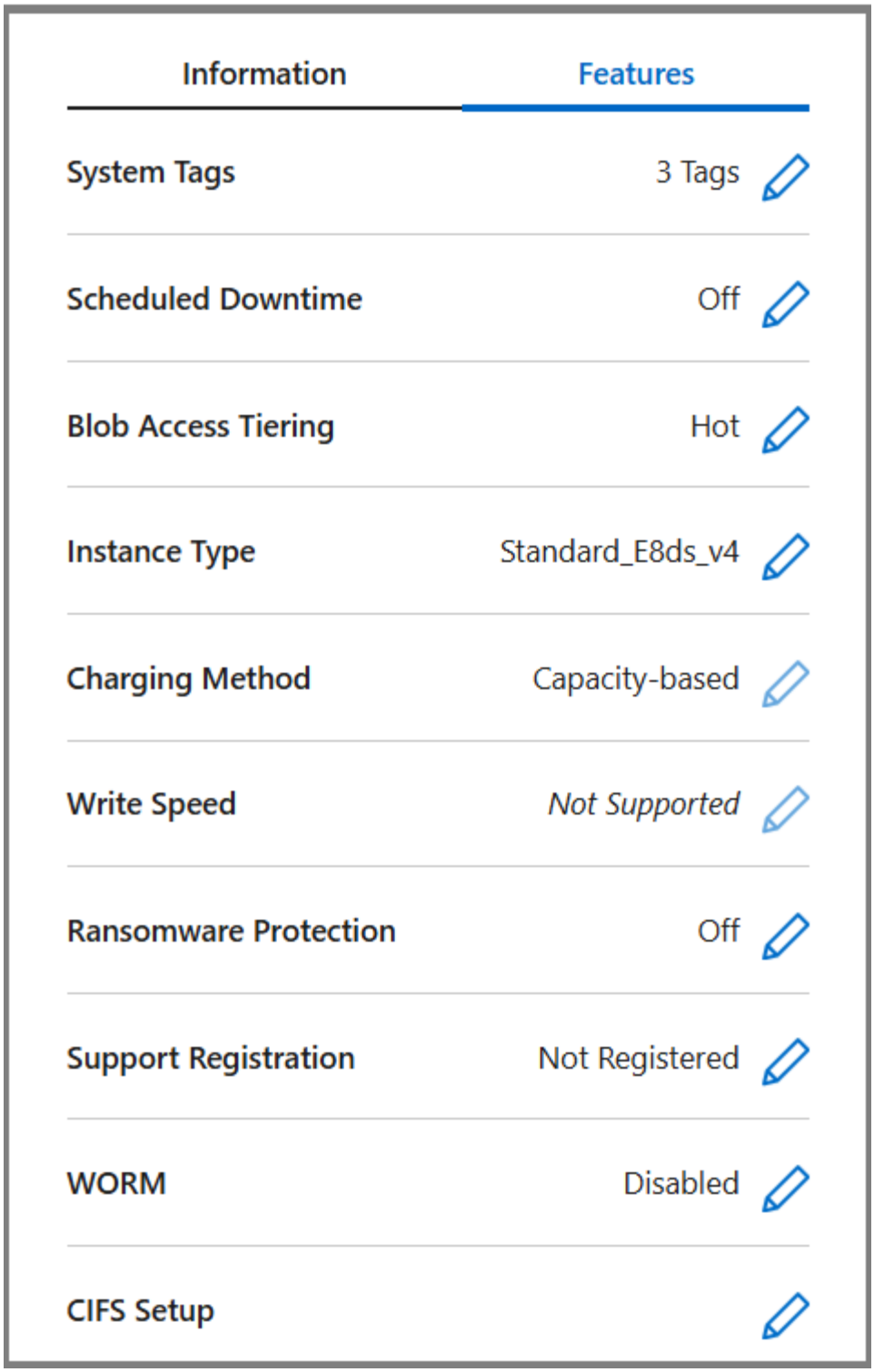
勒索软件攻击会浪费企业的时间、资源和声誉。 NetApp Console使您能够实施两种NetApp勒索软件解决方案：针对常见勒索软件文件扩展名的防护和自主勒索软件防护(ARP)。这些解决方案为可见性、检测和补救提供了有效的工具。

防御常见勒索软件文件扩展名

控制台上的勒索软件防护设置允许您利用ONTAP FPolicy 功能来防御常见的勒索软件文件扩展类型。

步骤

1. 在 **Systems** 页面上，双击您配置为使用勒索软件保护的Cloud Volumes ONTAP系统的名称。
2. 在“概述”选项卡上，单击“功能”面板，然后单击“勒索软件防护”旁边的铅笔图标。



3. 实施NetApp勒索软件解决方案：

   a. 如果您的卷未启用快照策略，请单击“激活快照策略”。

      NetApp Snapshot 技术提供了业界最佳的勒索软件补救解决方案。成功恢复的关键是从未受感染的备份中恢复。快照副本是只读的，可防止勒索软件破坏。他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的图像的粒度。

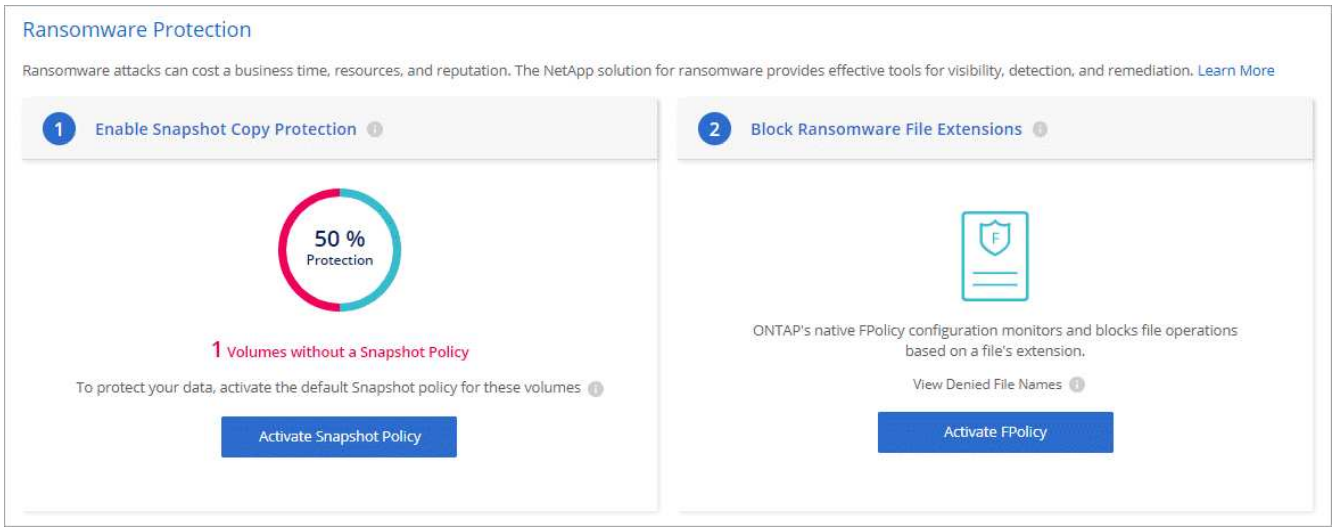
   b. 单击“激活 **FPolicy**”以启用 ONTAP 的 FPolicy 解决方案，该解决方案可以根据文件的扩展名阻止文件操作。

此预防解决方案通过阻止常见的勒索软件文件类型来提高对勒索软件攻击的防护。

默认 FPolicy 范围会阻止具有以下扩展名的文件：

micro、加密、锁定、加密、crypt、crinf、r5a、XRNT、XTBL、R16M01D05、pzdc、好、哈哈！、OMG！、RDM、RRK、encryptedRS、crjoker、EnCiPhErEd、LeChiffre

当您在Cloud Volumes ONTAP上激活 FPolicy 时，将创建此范围。该列表基于常见的勒索软件文件类型。您可以使用Cloud Volumes ONTAP CLI 中的 *vserver fpolicy policy scope* 命令自定义被阻止的文件扩展名。



自主勒索软件防护

Cloud Volumes ONTAP支持自主勒索软件防护 (ARP) 功能，该功能对工作负载进行分析，以主动检测并警告可能表明勒索软件攻击的异常活动。

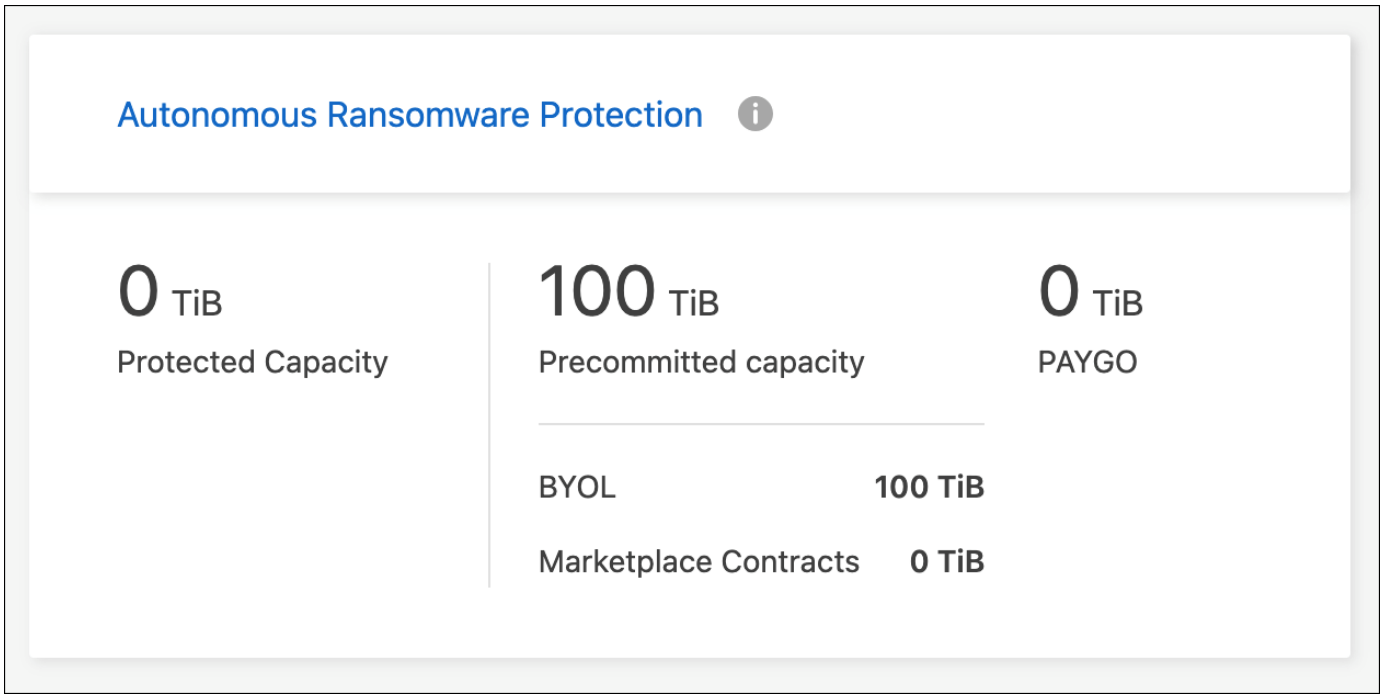
与通过以下方式提供的文件扩展名保护分开 "勒索软件防护设置"，ARP 功能使用工作负载分析根据检测到的“异常活动”向用户发出潜在攻击警报。勒索软件防护设置和 ARP 功能可以结合使用，以实现全面的勒索软件防护。

ARP 功能可与自带许可证 (BYOL) 一起使用，并且无需额外付费即可在市场订阅您的许可证。

启用 ARP 的卷具有指定状态“学习模式”或“活动”。

卷的 ARP 配置是通过ONTAP系统管理器和ONTAP CLI 执行的。

有关如何使用ONTAP System Manager 和ONTAP CLI 启用 ARP 的更多信息，请参阅 "ONTAP文档：启用自主勒索软件防护"。



在Cloud Volumes ONTAP上创建 WORM 文件的防篡改 Snapshot 副本

您可以在Cloud Volumes ONTAP系统上创建一次写入、多次读取 (WORM) 文件的防篡改 Snapshot 副本，并在特定保留期内以未修改的形式保留快照。此功能由SnapLock技术提供支持，并提供了额外的数据保护和合规性层。

开始之前

确保用于创建 Snapshot 副本的卷是SnapLock卷。有关在卷上启用SnapLock保护的信息，请参阅 "ONTAP文档：配置SnapLock"。

步骤

1. 从SnapLock卷创建 Snapshot 副本。有关使用 CLI 或系统管理器创建 Snapshot 副本的信息，请参阅 "ONTAP文档：管理本地 Snapshot 副本概述"。

   Snapshot 副本继承了卷的 WORM 属性，使其具有防篡改功能。底层的SnapLock技术可确保快照在指定的保留期结束之前受到保护，不会被编辑和删除。

2. 如果需要编辑这些快照，您可以修改保留期。欲了解更多信息，请参阅 "ONTAP文档：设置保留时间"。

即使 Snapshot 副本在特定保留期内受到保护，集群管理员也可以删除源卷，因为Cloud Volumes ONTAP中的 WORM 存储在“可信存储管理员”模型下运行。此外，受信任的云管理员可以通过操作云存储资源来删除WORM数据。

相关链接

- 有关 WORM 的更多信息，请参阅"了解Cloud Volumes ONTAP上的 WORM 存储"。
- 有关SnapLock卷的充电信息，请参阅"Cloud Volumes ONTAP中的许可和计费"。

系统管理

升级Cloud Volumes ONTAP

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

升级概述

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

仅从控制台升级

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

控制台提供了两种升级Cloud Volumes ONTAP 的方法：

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

支持的升级路径

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

支持的 **AWS** 升级路径

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

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

Azure 支持的升级路径

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

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

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

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

支持的 **Google Cloud** 升级路径

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

当前版本	可直接升级到的版本
9.0	9.1
8.3	9.0

请注意以下事项：

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

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

补丁版本

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

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

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

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

以下是几个例子：

- 9.13.0 → 9.13.1 P15
- 9.12.1 → 9.13.1 P2

恢复或降级

不支持将Cloud Volumes ONTAP恢复或降级到以前的版本。

支持注册

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

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

HA 调解器的升级

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

使用 c4、m4 和 r4 EC2 实例类型在 AWS 中进行升级

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

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

更改实例类型

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

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

如果您无法更改实例类型，请按照[启用增强联网]。

启用增强联网

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

准备升级

在执行升级之前，您必须验证系统已准备就绪并进行任何必要的配置更改。

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

规划停机时间

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

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

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

验证自动交还是否仍然启用

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

"ONTAP文档：用于配置自动交还的命令"

暂停SnapMirror传输

如果Cloud Volumes ONTAP系统具有活动的SnapMirror关系，最好在更新Cloud Volumes ONTAP软件之前暂停传输。暂停传输可防止SnapMirror故障。您必须暂停从目标系统的传输。

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

关于此任务

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

步骤

1. 从目标系统登录到系统管理器。

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

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

2. 单击*保护>关系*。
3. 选择关系并单击*操作>静默*。

验证聚合是否在线

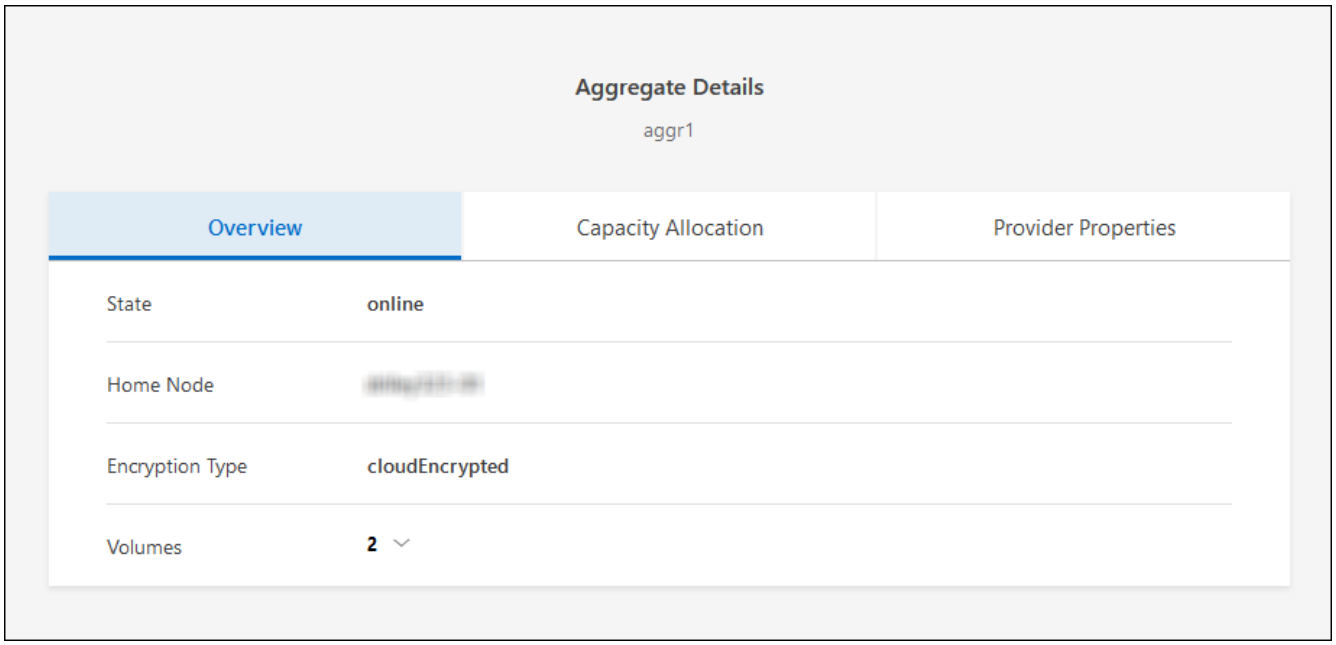
在更新软件之前， Cloud Volumes ONTAP的聚合必须处于在线状态。在大多数配置中，聚合应该处于在线状态，但如果没有，则应将其置于在线状态。

关于此任务

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

步骤

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



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

验证所有 **LIF** 是否位于主端口

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

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

升级Cloud Volumes ONTAP

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

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

从控制台通知升级

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

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

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

开始之前

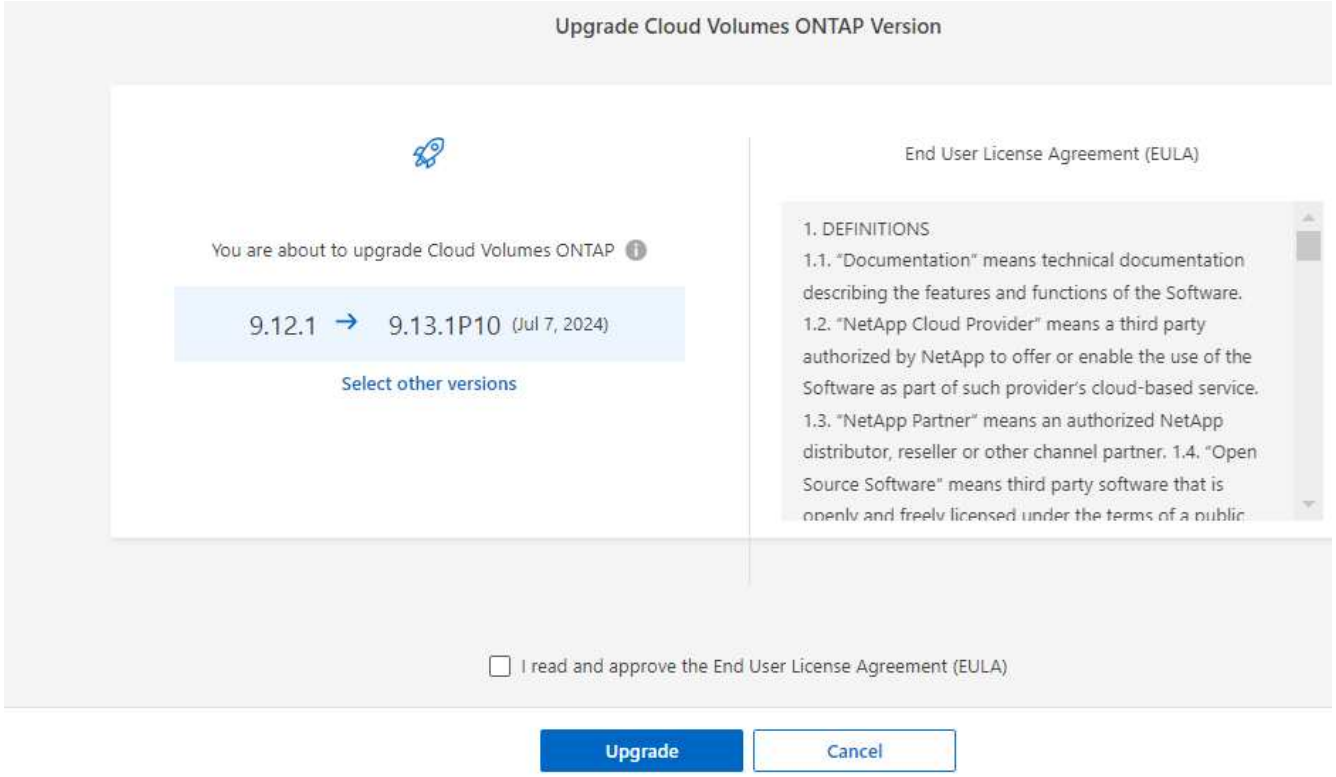
Cloud Volumes ONTAP系统上不得进行卷或聚合创建等操作。

步骤

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

   如果有新版本可用，概览选项卡中会出现通知：

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

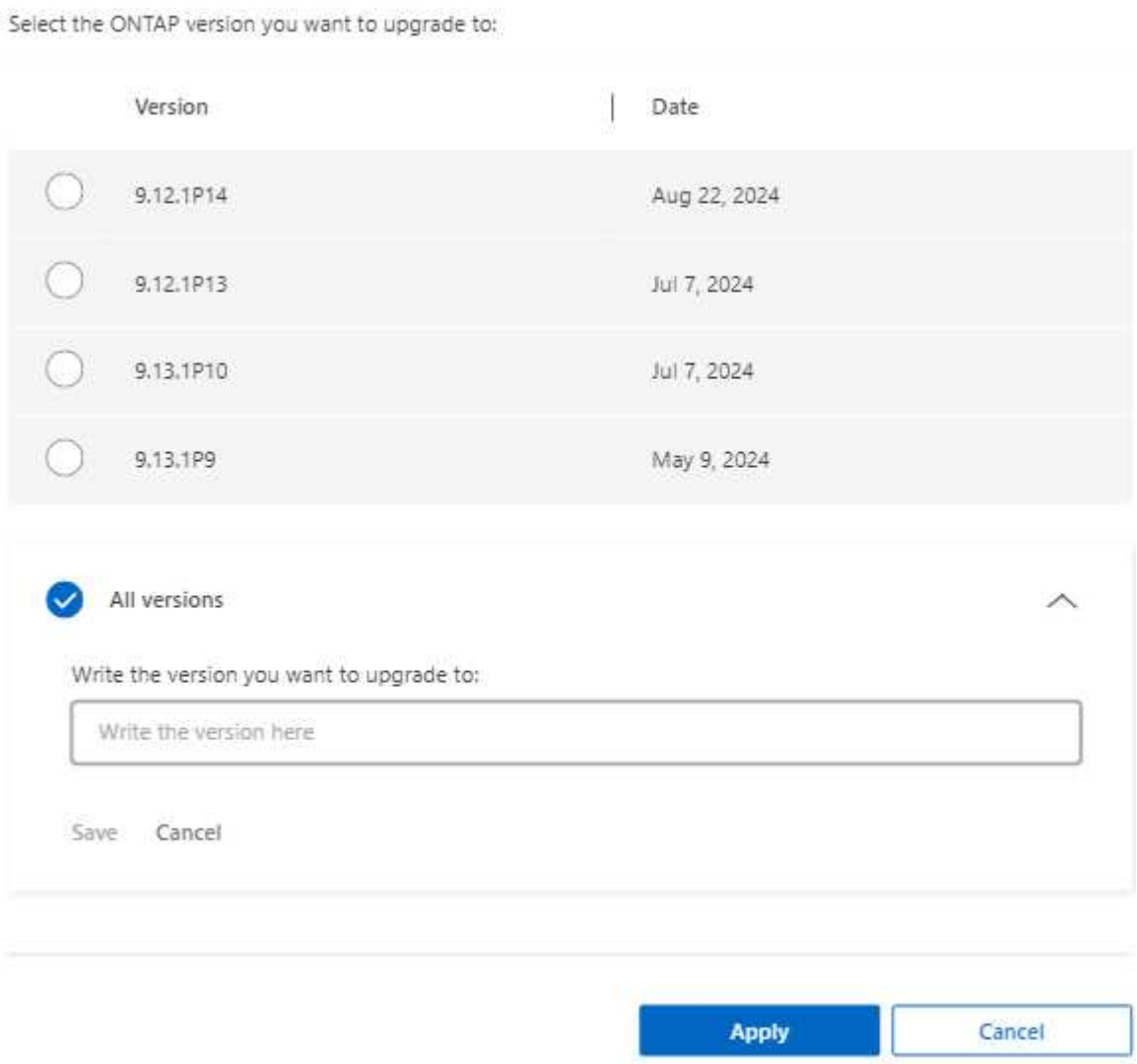


   如果要升级到其他版本，请单击“选择其他版本”。您会看到列出的最新Cloud Volumes ONTAP版本，这些版本也与您系统上安装的版本兼容。例如，您的系统上安装的版本是9.12.1P3，并且有以下兼容版本可用：

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

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

5. 单击“保存”，然后单击“应用”



。

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

结果

控制台开始软件升级。软件更新完成后，您可以在系统上执行操作。

完成后

如果您暂停了SnapMirror传输，请使用系统管理器恢复传输。

通过 **URL** 上的可用图像进行升级

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

开始之前

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

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

  转至NetApp知识库查看分步说明：

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

步骤

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

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

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

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

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

   有两条路径可用。正确的路径取决于您的控制台代理版本。

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

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

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

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

7. 单击“继续”进行确认。

结果

控制台开始软件更新。软件更新完成后，您就可以在系统上执行操作。

完成后

如果您暂停了SnapMirror传输，请使用系统管理器恢复传输。

修复使用 **Google Cloud NAT** 网关时下载失败的问题

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

步骤

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

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

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

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

"了解有关 /occm/config API 调用的更多信息" 。

注册Cloud Volumes ONTAP即用即付系统

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

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

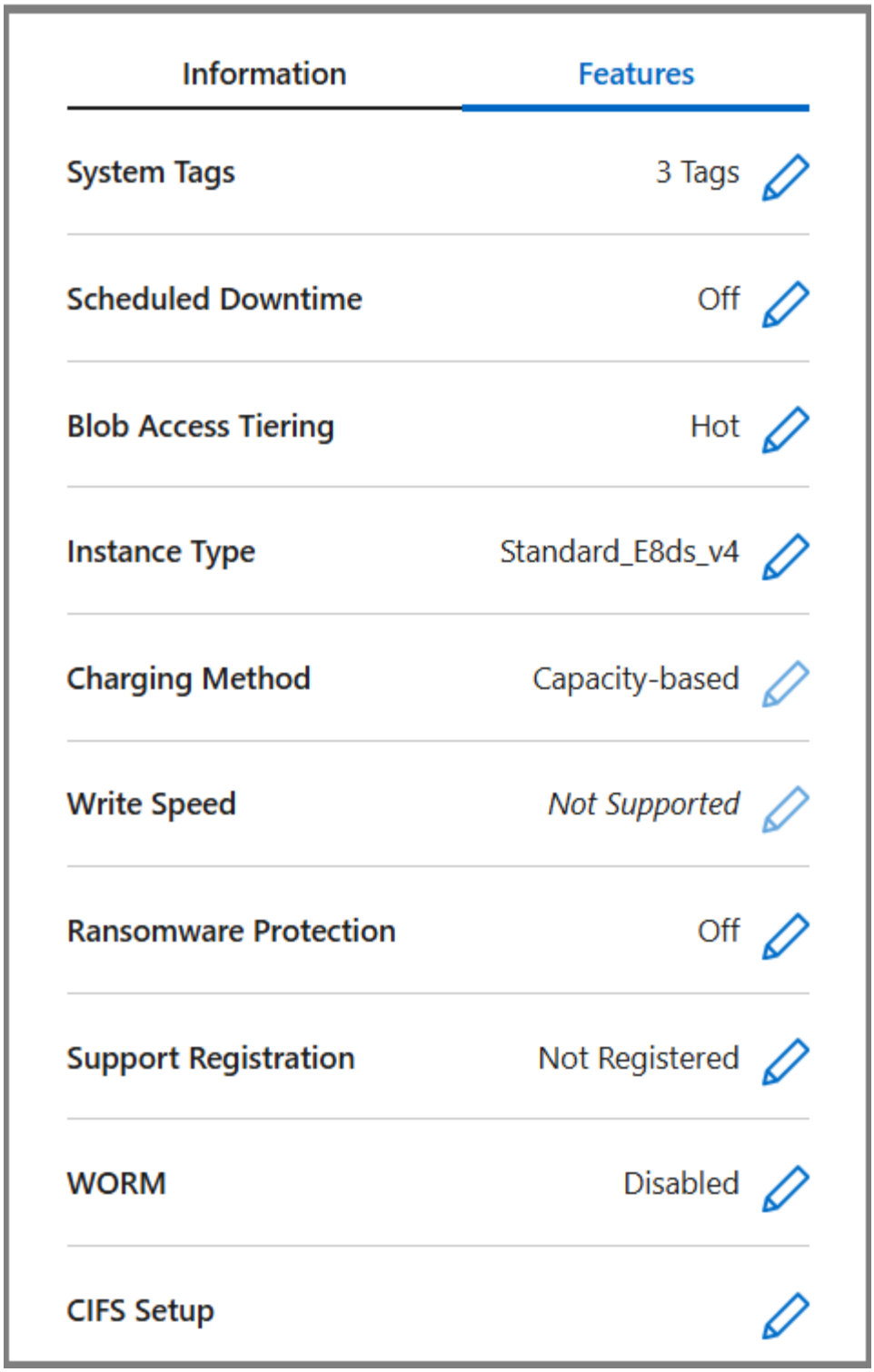
未注册支持的系统仍会在有新版本可用时收到NetApp Console中显示的软件更新通知。但您需要先注册系统才能升级软件。

步骤

1. 如果您尚未将NetApp支持站点帐户添加到控制台，请转到 帐户设置 并立即添加。

   "了解如何添加NetApp支持站点帐户" 。

2. 在“系统”页面上，双击要注册的系统的名称。
3. 在“概述”选项卡上，单击“功能”面板，然后单击“支持注册”旁边的铅笔图标。



4. 选择NetApp支持站点帐户并单击“注册”。

结果

该系统已在NetApp注册。

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

在基于节点的许可证的可用性终止 (EOA) 之后，您应该使用NetApp Console中的许可证转

换工具过渡到基于容量的许可证。

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

有关 EOA 和 EOS 的信息，请参阅"基于节点的许可证的可用性终止"。

关于此任务

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

开始之前

- 您应该拥有一个具有客户访问权限或管理员访问权限的 NSS 帐户。
- 您的 NSS 帐户应使用您用于访问控制台的用户凭据进行注册。
- Cloud Volumes ONTAP系统应链接到具有客户访问权限或管理员访问权限的 NSS 帐户。
- 您应该拥有有效的基于容量的许可证，可以是 BYOL 许可证或市场订阅。
- 您的帐户中应该有基于容量的许可证。此许可证可以是市场订阅，也可以是控制台中 **Licenses and subscriptions** 下提供的 BYOL/私人优惠包。
- 在选择目的地套餐之前，请了解以下标准：
  - 如果账户具有基于容量的 BYOL 许可证，则所选目标包应与账户的 BYOL 基于容量的许可证保持一致：
    - 什么时候 `Professional`被选为目标包，该帐户应具有带有专业包的 BYOL 许可证：
    - 什么时候 `Essentials`被选为目标包，该帐户应具有 Essentials 包的 BYOL 许可证。
  - 如果目标包与帐户的 BYOL 许可证可用性不一致，则意味着基于容量的许可证可能不包含所选包。在这种情况下，我们将通过您的市场订阅向您收费。
  - 如果没有基于容量的 BYOL 许可证而只有市场订阅，则应确保所选包包含在基于容量的市场订阅中。
  - 如果您现有的基于容量的许可证中没有足够的容量，并且您有市场订阅来对额外的容量使用收费，那么

您将通过市场订阅为额外的容量付费。

- 如果您现有的基于容量的许可证中没有足够的容量，并且您没有市场订阅来收取额外容量使用的费用，则无法进行转换。您应该添加市场订阅来收取额外容量或将可用容量扩展到当前许可证。
- 如果目标包与帐户的 BYOL 许可证可用性不一致，并且您现有的基于容量的许可证中没有足够的容量，那么您将通过市场订阅付费。

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

步骤

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

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

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

完成后

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

不同超标量中的定价

有关定价的详细信息，请访问 "NetApp Console网站"。

有关特定超标量中的私人优惠的信息，请写信至：

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

启动和停止**Cloud Volumes ONTAP**系统

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

安排**Cloud Volumes ONTAP**自动关闭

您可能希望在特定时间间隔内关闭Cloud Volumes ONTAP以降低计算成本。您无需手动执行此操作，而是可以将控制台配置为在特定时间自动关闭然后重新启动系统。

关于此任务

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

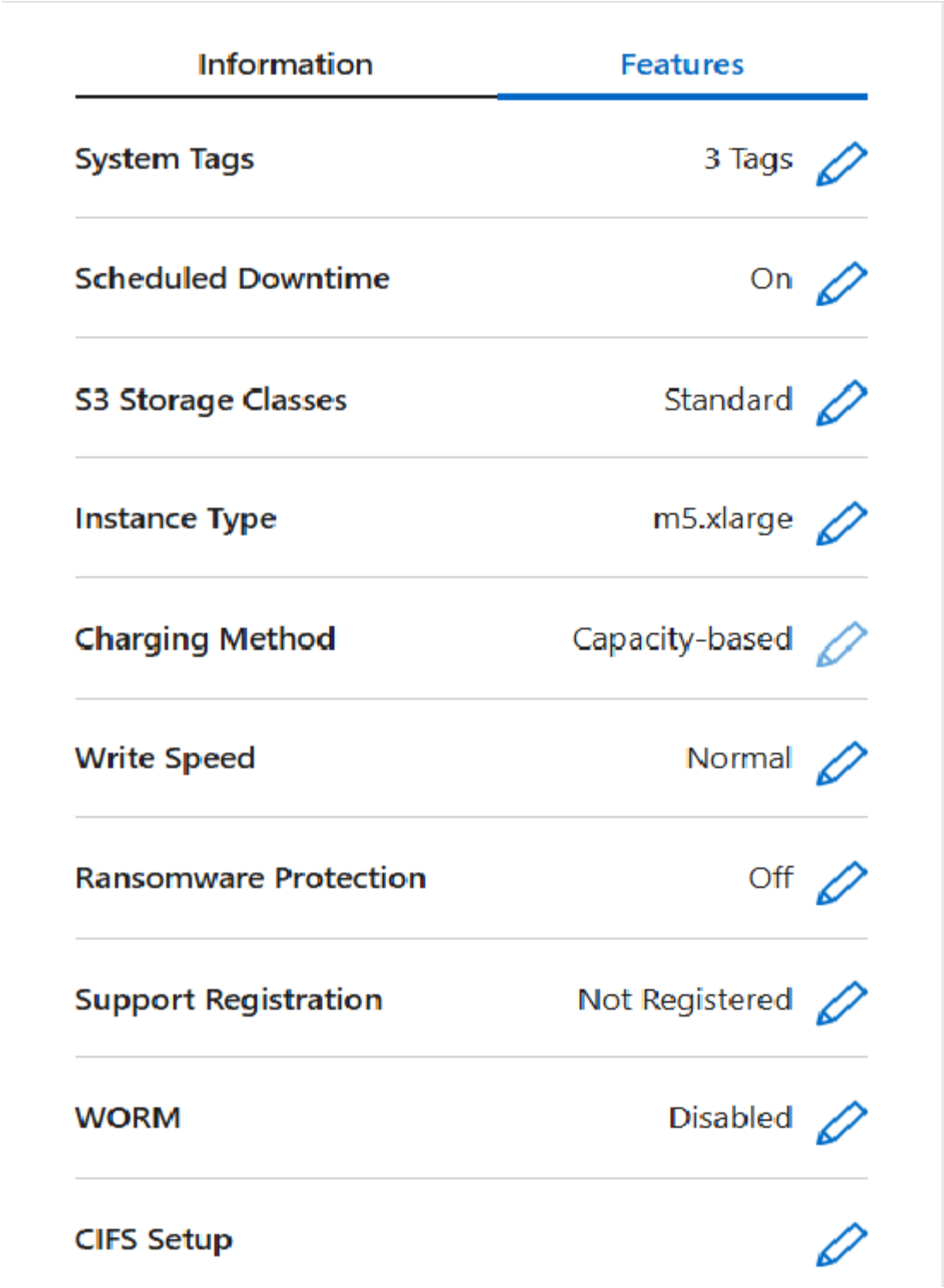
  传输完成后，系统将关闭。

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

  如下一节所述，只有在执行手动关机时才会自动创建快照。

步骤

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



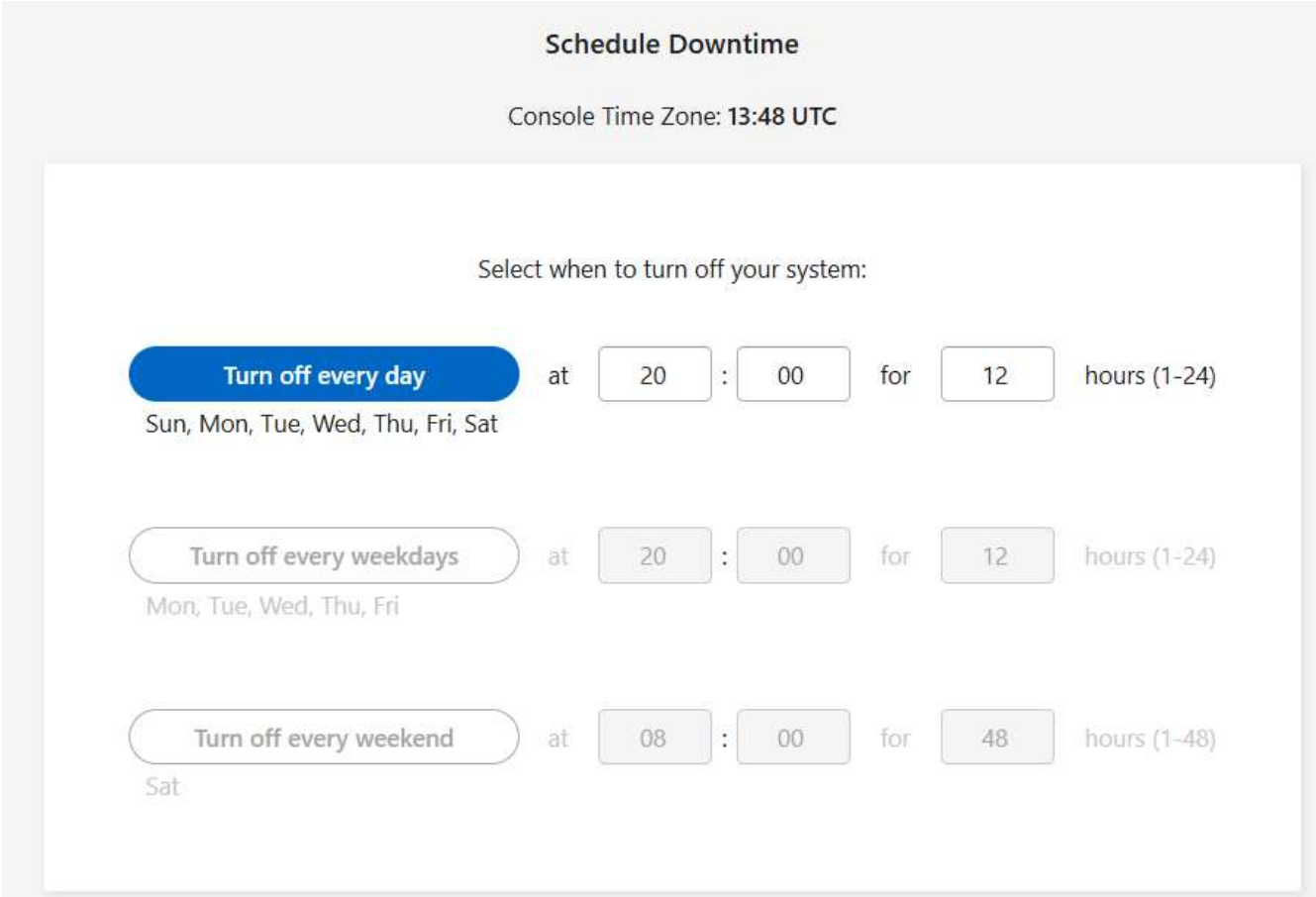
3. 指定关机计划：

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

   b. 指定您想要关闭系统的时间以及关闭系统的时间长度。

      例子

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



4. 单击“保存”。

结果

时间表已保存。功能面板下相应的计划停机时间行项目显示“开启”。

停止Cloud Volumes ONTAP

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

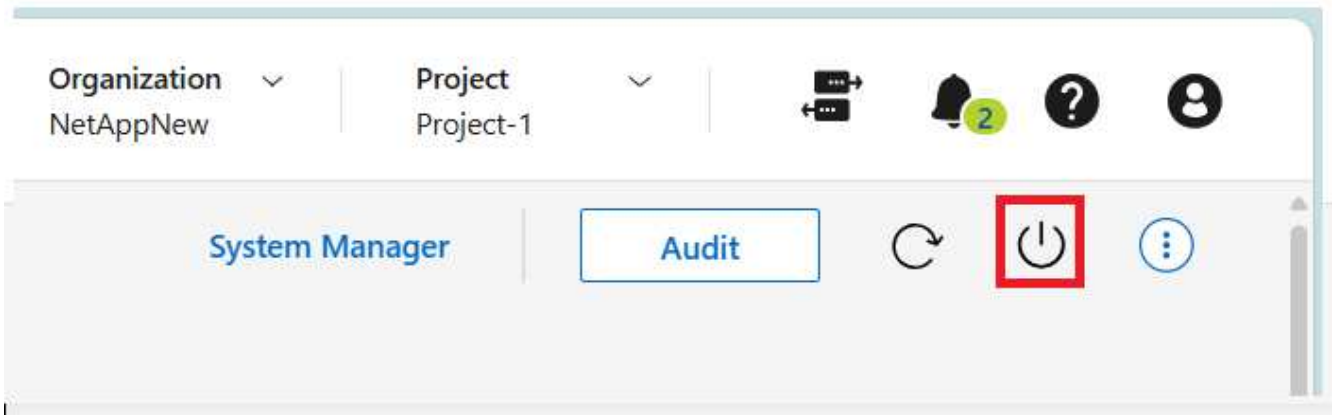
> 为了降低成本，控制台会定期删除根和启动磁盘的旧快照。根磁盘和启动磁盘仅保留最近的两个快照。

关于此任务

当您停止 HA 对时，控制台将关闭两个节点。

步骤

1. 在系统中，单击“关闭”图标。



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

   停止系统可能需要几分钟的时间。您可以稍后从*系统*页面重新启动系统。

   重启时会自动创建快照。

使用 NTP 服务器同步 Cloud Volumes ONTAP 系统时间

为 Cloud Volumes ONTAP 群集配置网络时间协议 (NTP) 服务器可确保群集时间与网络和外部服务器中的其他系统准确时间同步。将群集时间与外部 NTP 服务器同步有助于保持整个基础架构的一致性。NetApp 默认为新的 Cloud Volumes ONTAP 部署配置 NTP 服务器。但是，如果没有为现有的 Cloud Volumes ONTAP 群集进行配置，则必须配置 NTP 服务器，以便在网络内外进行准确的时间同步。

您可以使用以下命令指定 NTP 服务器：

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

如果您不配置 NTP 服务器，可能会遇到服务中断和时间同步不准确的情况。

相关链接

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

修改系统写入速度

您可以在NetApp Console中为Cloud Volumes ONTAP选择正常或高写入速度。默认写入速

度正常。如果您的工作负载需要快速写入性能，您可以更改为高写入速度。

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

在更改写入速度之前，您应该"了解正常设置和高设置之间的差异"。

关于此任务

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

步骤

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

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

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

4. 单击“保存”，查看确认消息，然后单击“批准”。

更改Cloud Volumes ONTAP集群管理员密码

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

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

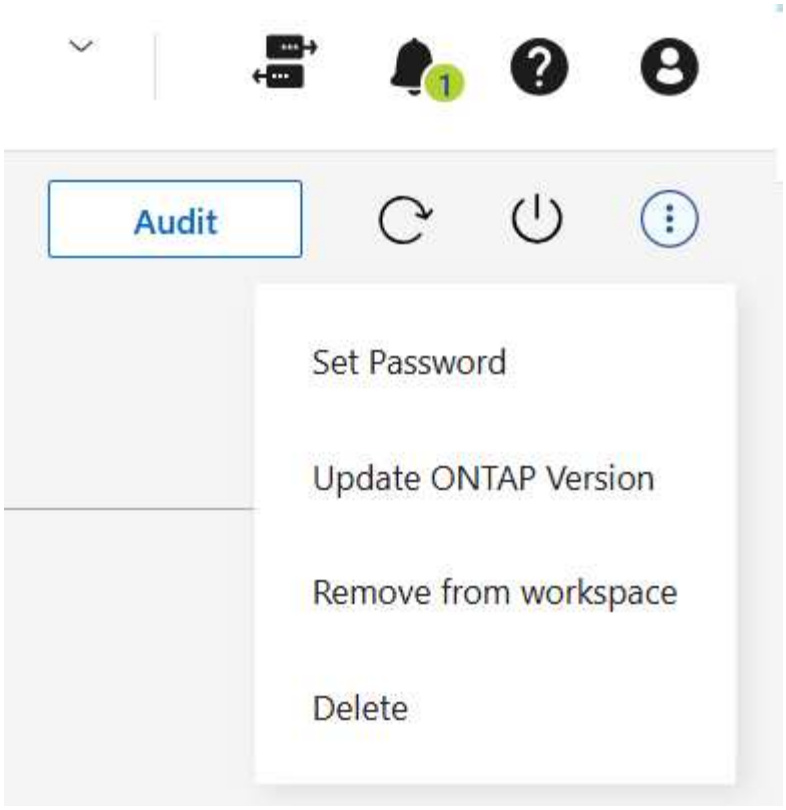
关于此任务

密码必须遵守一些规则。新密码：

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

步骤

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



添加、移除或删除系统

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

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

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

您无法发现、查看或管理在其他帐户或组织中注册的系统。

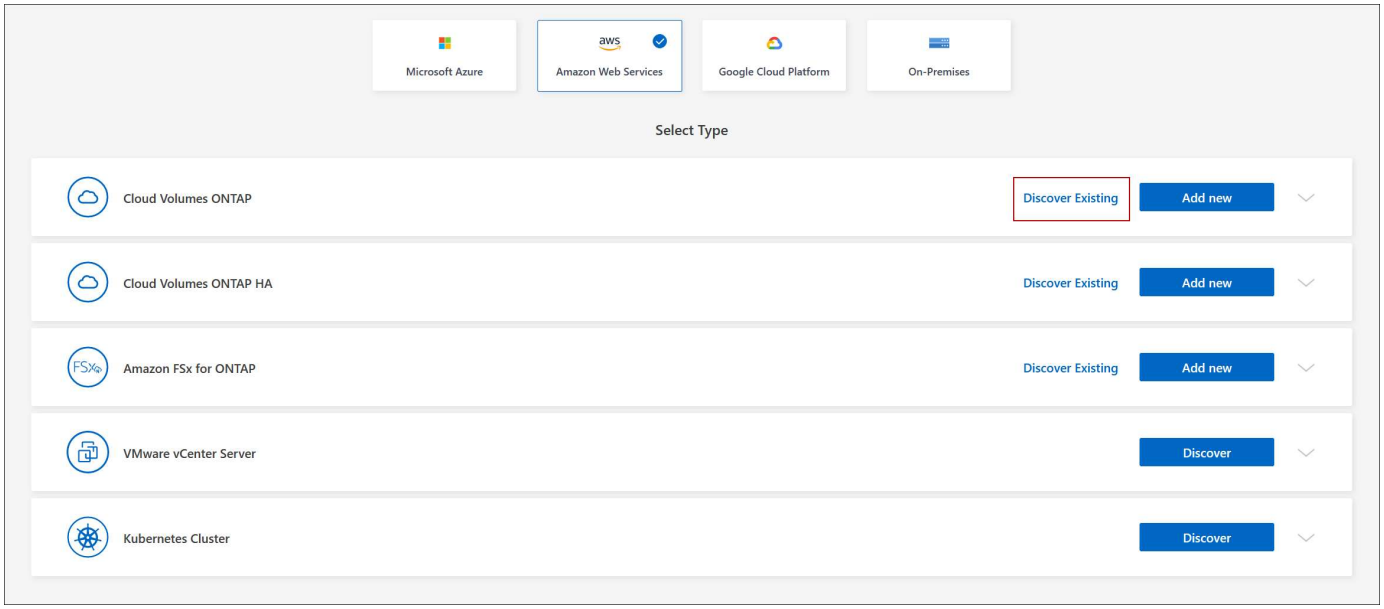
开始之前

您必须知道Cloud Volumes ONTAP管理员用户帐户的密码。

步骤

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

+



1. 在“区域”页面上，选择一个区域。您可以看到在所选区域中运行的系统。

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

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

结果

控制台将Cloud Volumes ONTAP系统添加到 系统 页面。

从**NetApp Console**中删除**Cloud Volumes ONTAP**系统

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

关于此任务

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

步骤

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

结果

控制台删除系统。用户可以随时从*系统*页面重新发现已删除的系统。

从**NetApp Console**删除**Cloud Volumes ONTAP**系统

您应该始终从NetApp Console中删除Cloud Volumes ONTAP系统，而不是从云提供商的应用程序中删除。例如，如果您终止了云提供商许可的Cloud Volumes ONTAP实例，则您不能将该许可证密钥用于另一个实例。您必须从控制台中删除Cloud Volumes ONTAP系统才

能释放许可证。

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

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

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

步骤

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

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

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

   "了解有关数据分类实例的更多信息" 。

3. 删除Cloud Volumes ONTAP系统。

   a. 在“系统”页面上，双击要删除的Cloud Volumes ONTAP系统的名称。

   b. 在控制台的右上角，单击 ••• 图标，然后选择*删除*。

   c. 输入要删除的系统的名称，然后单击“删除”。删除系统最多可能需要五分钟。

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

AWS 管理

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

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

关于此任务

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

  "ONTAP 9 文档：用于配置自动交还的命令"

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

  对于单节点系统，I/O 被中断。

对于 HA 对来说，这种变化是无中断的。 HA 对继续提供数据。

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

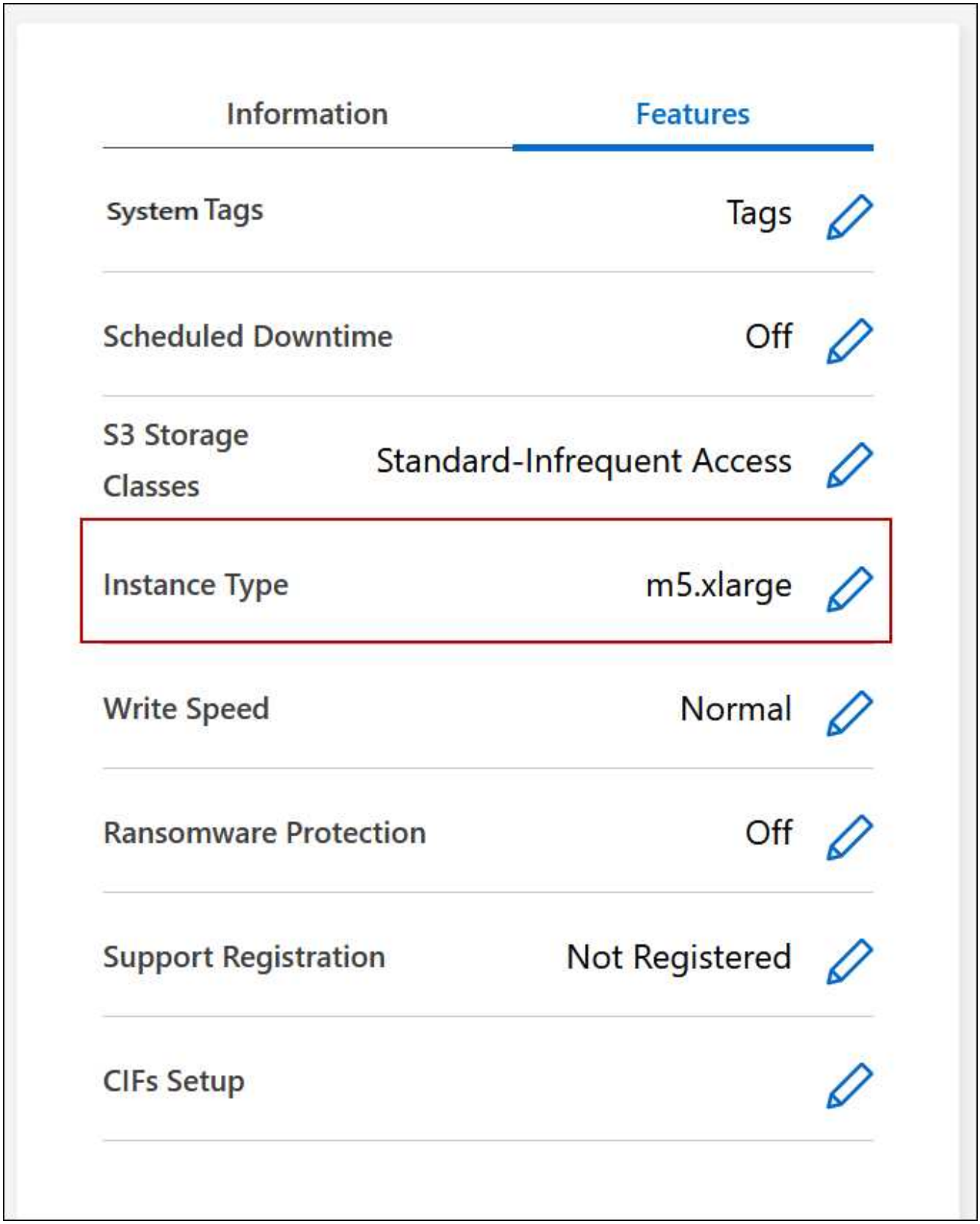
参考

有关 AWS 支持的实例类型列表，请参阅"支持的 EC2 实例"。

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

步骤

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



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

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

结果

Cloud Volumes ONTAP使用新配置重新启动。

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

您可以修改 AWS 路由表，其中包含部署在多个 AWS 可用区 (AZ) 中的 HA 对的浮动 IP 地址的路由。如果新的 NFS 或 CIFS 客户端需要访问 AWS 中的 HA 对，您可以这样做。

步骤

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

结果

NetApp Console发送 AWS 请求来修改路由表。

Azure 管理

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

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

关于此任务

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

  "ONTAP 9 文档：用于配置自动交还的命令"

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

  对于单节点系统，I/O 被中断。

  对于 HA 对来说，这种变化是无中断的。 HA 对继续提供数据。

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

步骤

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

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

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

结果

Cloud Volumes ONTAP使用新配置重新启动。

覆盖 **Azure** 中**Cloud Volumes ONTAP HA** 对的 **CIFS** 锁

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

关于此任务

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

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

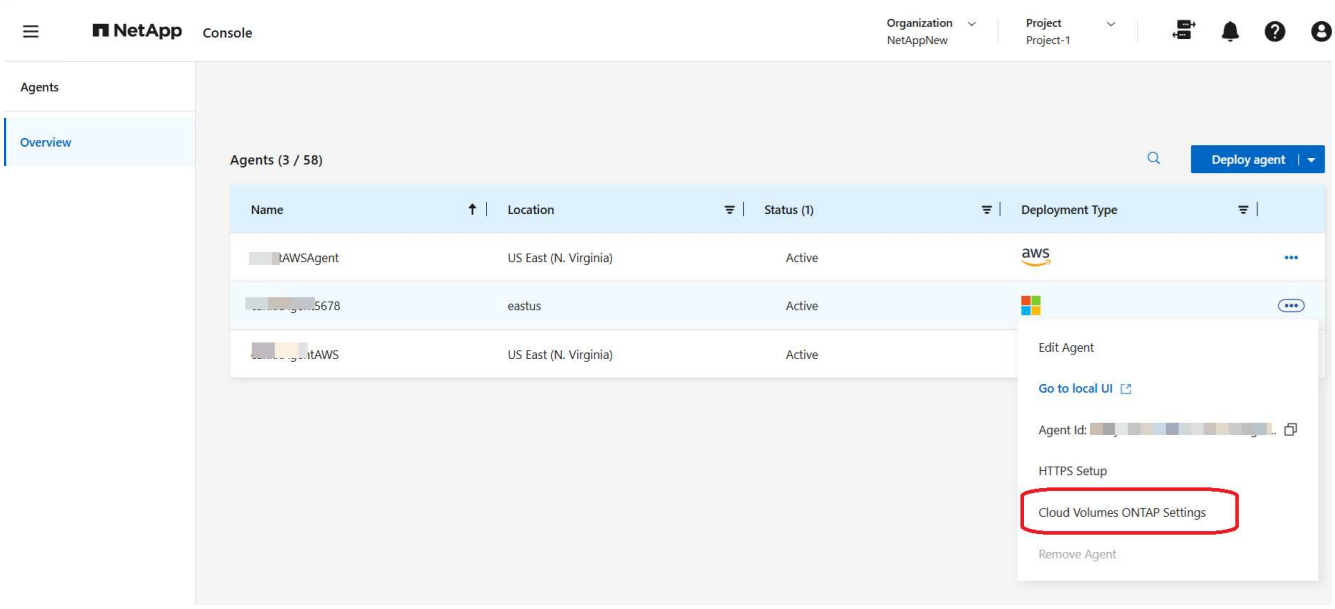
此过程可能会对 CIFS 客户端造成破坏。 CIFS 客户端未提交的数据可能会丢失。

开始之前

您需要先创建控制台代理，然后才能更改控制台设置。 "了解详情" 。

步骤

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



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

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

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

概述

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

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

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

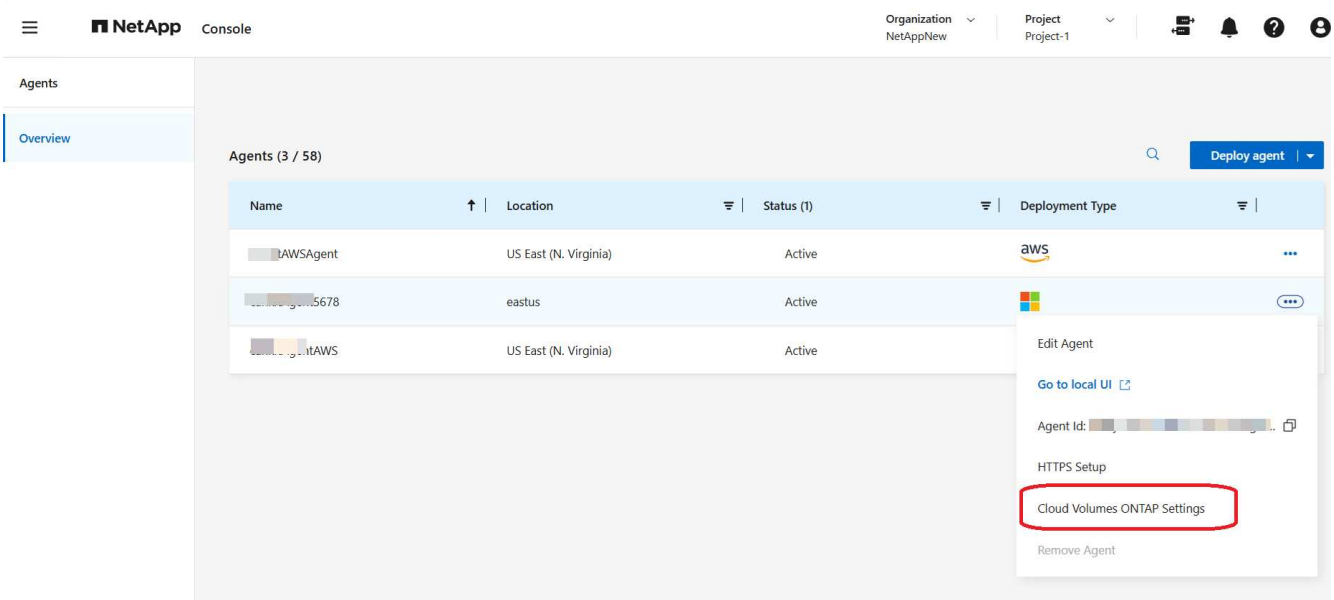
禁用 Azure Private Links 并改用服务终结点

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

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

步骤

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



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

完成后

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

"了解如何在控制台代理上启用直接 API 流量"

使用 **Azure Private Links**

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

自定义 **DNS** 的要求

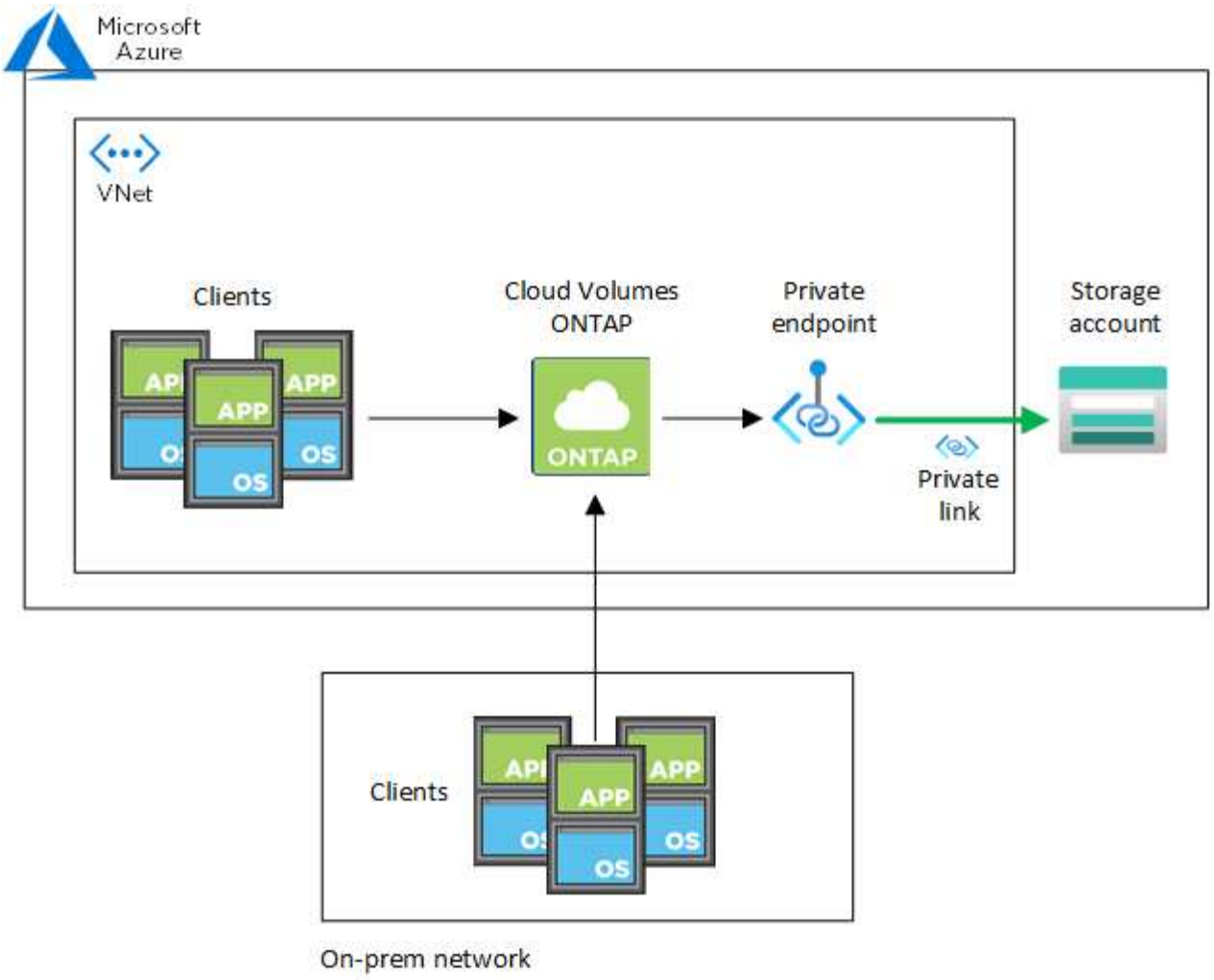
或者，如果您使用自定义 DNS，则需要从自定义 DNS 服务器创建到 Azure 私有 DNS 区域的条件转发器。要了解更多信息，请参阅"Azure 关于使用 DNS 转发器的文档"。

专用链接连接的工作原理

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

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

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



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

提供有关 **Azure** 专用 **DNS** 的详细信息

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

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

步骤

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

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

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

4. 保存文件并注销控制台代理。

   不需要重新启动。

启用故障回滚

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

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

如果启用回滚，控制台将停止该操作并回滚作为该操作的一部分创建的所有资源。

您可以通过 API 或更新 app.conf 文件来启用回滚。

通过 **API** 启用回滚

步骤

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

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

通过更新 **app.conf** 启用回滚

步骤

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

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

. 保存文件并注销控制台代理。

不需要重新启动。

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

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

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

步骤

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

   要完成移动，请参阅"Microsoft Azure 文档中的“将资源移动到新的资源组或订阅”"。
3. 在*系统*页面上，发现系统。
4. 在系统信息中查找新的资源组。

结果

系统及其资源（虚拟机、磁盘、存储帐户、网络接口、快照）位于新的资源组中。

在 **Azure** 中隔离**SnapMirror**流量

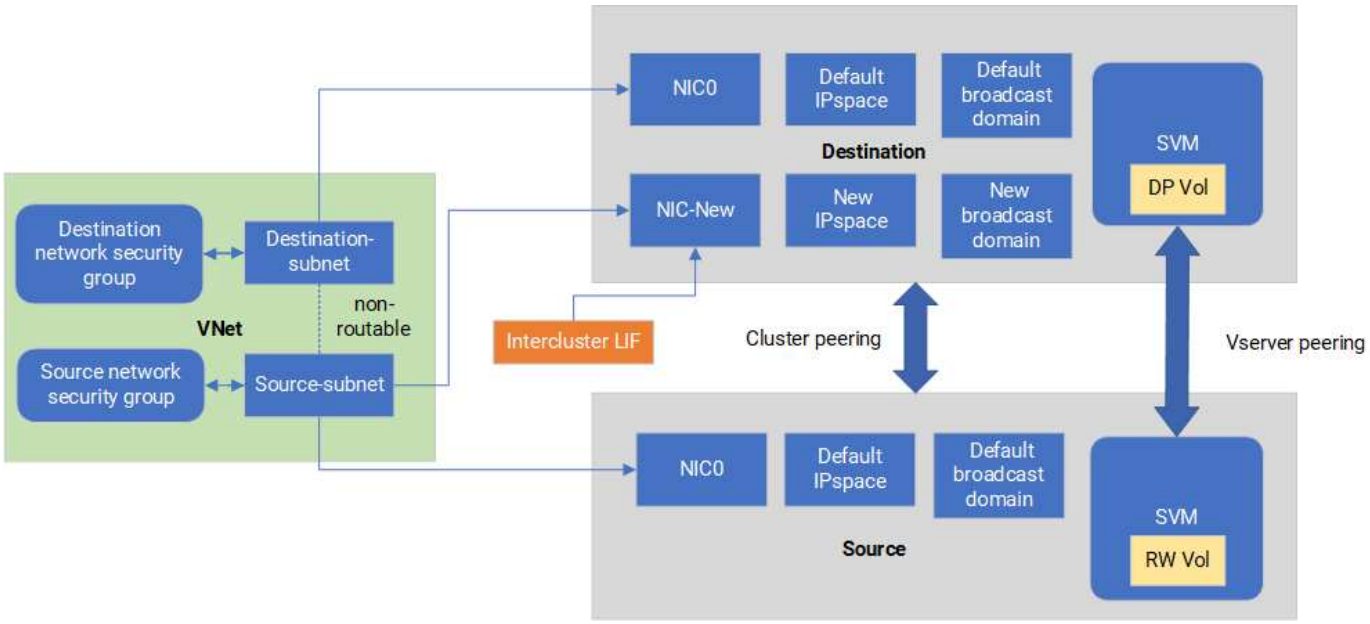
使用 Azure 中的Cloud Volumes ONTAP ，您可以将SnapMirror复制流量与数据和管理流量分离。为了将SnapMirror复制流量与数据流量隔离，您需要添加一个新的网络接口卡 (NIC)、一个相关的集群间 LIF 和一个不可路由的子网。

关于 **Azure** 中的**SnapMirror**流量隔离

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

图 **1**

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



开始之前

回顾以下注意事项：

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

步骤 1：创建额外的 NIC 并连接到目标 VM

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

步骤

1. 在ONTAP CLI 中，停止节点。

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

2. 在 Azure 门户中，检查 VM（节点）状态是否已停止。

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

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

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

b. 解除分配节点。

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

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

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

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

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

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

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

6. 启动虚拟机（节点）。

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

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

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

对于 HA 对部署，请对合作伙伴节点重复这些步骤。

步骤 2：为新 NIC 创建新的 IP 空间、广播域和集群间 LIF

集群间 LIF 的单独 IP 空间为集群间复制的网络功能提供了逻辑分离。

使用ONTAP CLI 执行以下步骤。

步骤

1. 创建新的 IP 空间（new_ipspace）。

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

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

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

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

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

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

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

5. 验证新的集群间 LIF 的创建。

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

对于 HA 对部署，请对合作伙伴节点重复这些步骤。

步骤 3：验证源系统和目标系统之间的集群对等连接

本节提供有关如何验证源系统和目标系统之间的对等关系的说明。

使用ONTAP CLI 执行以下步骤。

步骤

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

此目标 IP 地址是源上的集群间 LIF IP 地址。

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

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

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

对于 HA 对部署，请对合作伙伴节点重复这些步骤。

步骤 4：在源系统和目标系统之间创建 SVM 对等连接

本节提供有关如何在源系统和目标系统之间创建 SVM 对等的说明。

使用ONTAP CLI 执行以下步骤。

步骤

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

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

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

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

4. 输入并确认密码。
5. 检查集群是否对等。

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

成功的对等连接在可用性字段中显示 可用。

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

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

7. 接受 SVM 对等连接。

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

8. 检查 SVM 是否已对等。

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

同行国家显示*peered* 和对等应用程序显示*snapmirror*.

步骤 5：在源系统和目标系统之间创建SnapMirror复制关系

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

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

使用ONTAP CLI 执行以下步骤。

步骤

1. 在目标 SVM 上创建数据保护卷。

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

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

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

3. 在目标上初始化SnapMirror复制关系。

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

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

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

关系状态是 `Snapmirrored`关系的健康是 `true`。

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

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

或者，您可以挂载源卷和目标卷，将文件写入源卷，并验证卷是否复制到目标卷。

Google Cloud 管理

更改Cloud Volumes ONTAP的 Google Cloud 机器类型

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

关于此任务

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

  "ONTAP 9 文档：用于配置自动交还的命令"

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

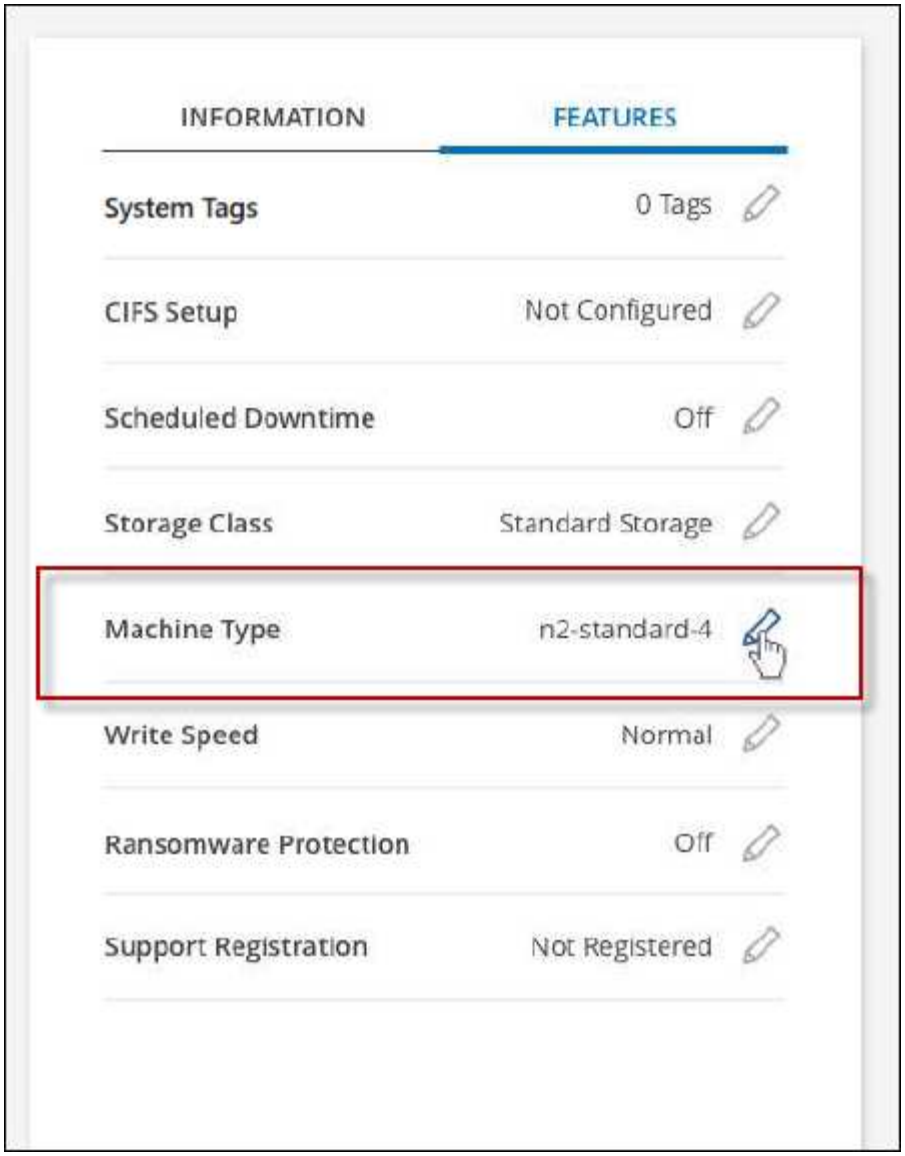
  对于单节点系统，I/O 被中断。

  对于 HA 对来说，这种变化是无中断的。 HA 对继续提供数据。

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

步骤

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



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

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

结果

Cloud Volumes ONTAP使用新配置重新启动。

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

从 2026 年 2 月 9 日起，Google Cloud 中的新 Cloud Volumes ONTAP 部署可以使用 Google Cloud Infrastructure Manager。Google 即将弃用 Google Cloud Deployment Manager，转而使用 Infrastructure Manager。因此，您需要手动运行过渡工具，将现有 Cloud Volumes ONTAP 部署从 Deployment Manager 转换为 Infrastructure Manager。这是一个一次性流程，之后您的系统将自动开始使用 Infrastructure Manager。

关于此任务

转换工具在 "NetApp 支持站点" 中可用，并创建以下工件：

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

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

开始之前

- 确保您的 Cloud Volumes ONTAP 系统为 9.16.1 或更高版本。
- 请确保未从 Google Cloud Console 手动编辑任何 Cloud Volumes ONTAP 资源或其属性。
- 请确保已启用 Google Cloud API。请参阅 "启用 Google Cloud API"。请确保与其他 API 一起启用 Google Cloud Quotas API。
- 验证 NetApp Console 代理的服务帐户是否具有所需的所有权限。请参阅 "控制台代理的 Google Cloud 权限"。

  对于专用模式部署，请确保以下附加先决条件：

  - 确保拥有最新的 Console 代理版本。从 NetApp 支持站点下载产品安装程序，然后在主机上手动安装代理，以便代理可以使用 Infrastructure Manager API。
  - 如果在专用模式下运行工具，请确保已与其他 API 一起启用 Cloud Build API "启用 Google Cloud API"。
  - 确保已完成网络配置并为专用模式部署创建工作者池。请参阅 "适用于专用模式部署的 Infrastructure Manager 配置"。

- 转换工具使用以下域。在网络中的端口 443 上启用它们：

域	端口	协议	方向	目的
cloudresourcemanager.googleapis.com	443	TCP	EGRESS	项目验证
deploymentmanager.googleapis.com	443	TCP	EGRESS	部署发现

域	端口	协议	方向	目的
config.googleapis.com	443	TCP	EGRESS	基础架构管理器 API
storage.googleapis.com	443	TCP	EGRESS	GCS 存储桶操作
iam.googleapis.com	443	TCP	EGRESS	服务帐户验证
compute.googleapis.com	443	TCP	EGRESS	Google Cloud 和 Terraform Import 和 Plan 使用的计算 API 调用
cloudbuild.googleapis.com	443	TCP	EGRESS	仅专用模式需要构建操作
openidconnect.googleapis.com	443	TCP	EGRESS	身份验证
oauth2.googleapis.com	443	TCP	EGRESS	OAuth2 令牌交换
registry.terraform.io	443	TCP	EGRESS	Terraform 提供程序注册表
releases.hashicorp.com	443	TCP	EGRESS	Terraform 二进制文件下载
apt.releases.hashicorp.com	443	TCP	EGRESS	HashiCorp APT 存储库
us-central1-docker.pkg.dev	443	TCP	EGRESS	GCP Artifact Registry
metadata.google.internal	80	HTTP	内部	VM 元数据和身份验证令牌
pypi.org	443	TCP	EGRESS	Python 软件包索引
files.pythonhosted.org	443	TCP	EGRESS	Python 软件包下载
checkpoint-api.hashicorp.com	443	TCP	EGRESS	Terraform 版本检查
download.docker.com	443	TCP	EGRESS	Docker APT 仓库
security.ubuntu.com	80/443	TCP	EGRESS	Ubuntu 安全更新
*.gce.archive.ubuntu.com	80	TCP	EGRESS	Ubuntu 软件包镜像

准备运行工具的环境

在运行工具之前运行这些步骤。

步骤

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

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

包括专用模式部署的其他权限

如果在私有模式下运行此工具，请将 `cloudbuild.workerpools.get`权限也添加到 YAML 文件。

   b. 使用 YAML 文件中定义的权限在 Google Cloud 中创建自定义角色。
`gcloud iam roles create dmtoim_convert_tool_role --project=PROJECT_ID \
--file=YAML_FILE_PATH`有关详细信息，请参阅 "创建和管理自定义角色"。
   c. 将自定义角色附加到将用于创建 VM 的服务帐户。
   d. 将 `roles/iam.serviceAccountUser`角色添加到此服务帐户。请参阅 "服务账户概述"。

2. 使用以下配置创建虚拟机。在此虚拟机上运行工具。
   - 机器类型：Google Compute Engine 机器类型 e2-medium
   - 操作系统：根据您的要求，选择以下任一图像：
     - Ubuntu 25.10 AMD64 精简版（镜像：ubuntu-minimal-2510-amd64）
     - SUSE Linux Enterprise Server 15 SP7 x86_64
   - 网络：允许 HTTP 和 HTTPS 的防火墙
   - 磁盘大小：20GB
   - 安全：服务帐户：您创建的服务帐户
   - 安全性：访问范围 - 为每个 API 设置访问权限：
     - 云平台：已启用
     - Compute Engine：只读
     - 存储：只读（默认）
     - Google Cloud Logging（以前称为 Stackdriver Logging）API：仅写入（默认）
     - Stackdriver Monitoring（现已成为 Google Cloud Operations 的一部分）API：仅写入（默认）
     - 服务管理：只读（默认）
     - 服务控制：已启用（默认）
     - Google Cloud Trace（以前称为 Stackdriver Trace）：仅写入（默认）
3. 使用 SSH 连接到新创建的虚拟机： `gcloud compute ssh dmtoim-convert-executor-vm --zone <region where VM is deployed>`
4. 使用您的 NSS 凭据从 "NetApp 支持站点"下载转换工具： `wget <download link from NetApp Support site>`
5. 提取下载的 TAR 文件： `unzip <downloaded file name>`

Ubuntu

1. 下载并安装以下必备软件包：
   - Docker：28.2.2 build 28.2.2-0ubuntu1 或更高版本
   - Terraform：1.14.1 或更高版本
   - Python：3.13.7、python3-pip、python3 venv

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

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

SUSE Linux Enterprise Server

1. 设置 Python： `sudo update-alternatives --install /usr/bin/python3 python3 /usr/bin/python3.11 2`
2. 安装 pip3 以安装软件包： `python3.11 -m ensurepip --upgrade`
3. 安装 Terraform：

   ```
   wget
   https://releases.hashicorp.com/terraform/1.7.4/terraform_1.7.4_linux
   _amd64.zip
   unzip terraform_1.7.4_linux_amd64.zip
   sudo mv terraform /usr/local/bin/
   rm terraform_1.7.4_linux_amd64.zip
   ```

4. 安装 Google Cloud SDK (gcloud)

   ```
   curl https://sdk.cloud.google.com | bash
   exec -l $SHELL
   ```

运行转换工具

这些步骤适用于运行转换工具的 Ubuntu 和 SUSE Linux Enterprise Server。

步骤

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

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

2. 安装转换工具：

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

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

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

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

在私有模式部署中运行工具

指定 `--worker-pool` 参数以在私有模式部署中运行工具。有关工作池配置，请参阅 "适用于专用模式部署的 Infrastructure Manager 配置"。

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

完成后

该工具显示所有 Cloud Volumes ONTAP 系统和 SVM 详细信息的列表。当它完成运行时，您可以看到所有已转

换系统的状态。每个转换后的系统都以 *<system-name-imdeploy>* 格式显示在 Google Console 的 Infrastructure Manager 下，表明 Console 现在使用 Infrastructure Manager API 来管理该 Cloud Volumes ONTAP 系统。

> 转换后，请勿在 Google Cloud Console 中删除 Deployment Manager 的部署对象。此部署对象包含回滚转换的系统可能需要的信息。

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

回滚转换

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

步骤

1. 在同一个 为运行工具而创建的虚拟机 上，运行此命令：

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

2. 等待回滚完成。

相关链接

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

使用系统管理器管理Cloud Volumes ONTAP

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

功能

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

- 高级存储管理：管理一致性组、共享、qtree、配额和存储虚拟机。
- 成交量变动： "将卷移动到不同的聚合。"
- 网络管理：管理 IP 空间、网络接口、端口集和以太网端口。
- 管理FlexGroup卷：您只能通过系统管理器创建和管理FlexGroup卷。BlueXP控制台不支持FlexGroup卷创建。
- 事件和作业：查看事件日志、系统警报、作业和审计日志。

- 高级数据保护：保护存储虚拟机、LUN 和一致性组。
- 主机管理：设置 SAN 启动器组和 NFS 客户端。
- ONTAP S3 对象存储管理：Cloud Volumes ONTAP 中的 ONTAP S3 存储管理功能仅在 System Manager 中可用，在 Console 中不可用。

支持的配置

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

限制

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

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

配置访问系统管理器的身份验证

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

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

所需权限

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

步骤

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

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

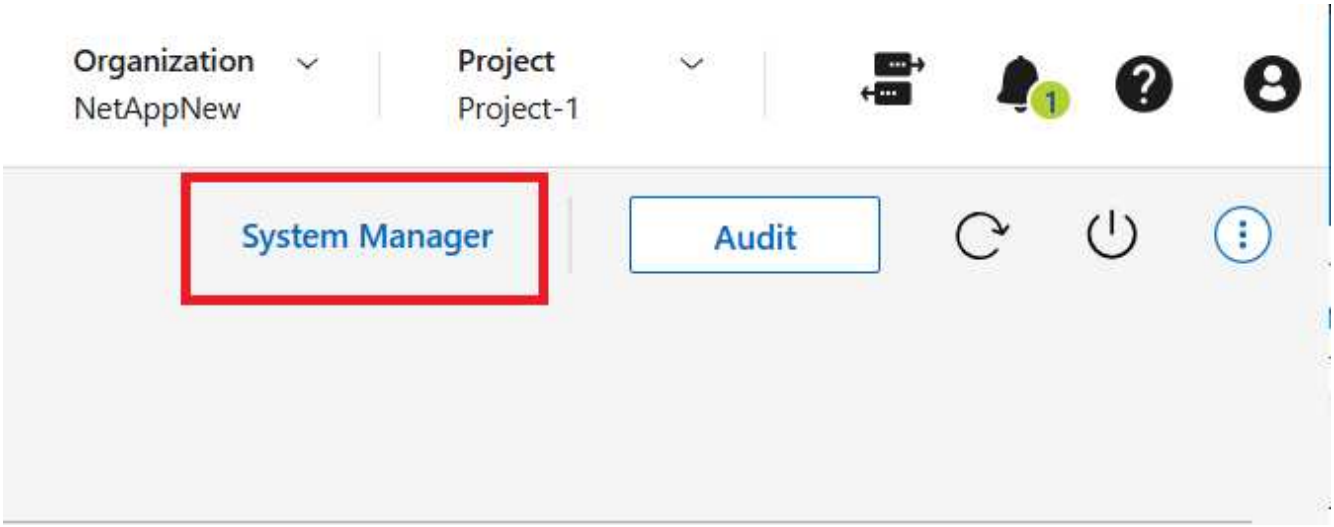
4. 单击“保存”。

开始使用系统管理器

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

步骤

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



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

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

有关使用系统管理器的帮助

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

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

从 CLI 管理Cloud Volumes ONTAP

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

开始之前

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

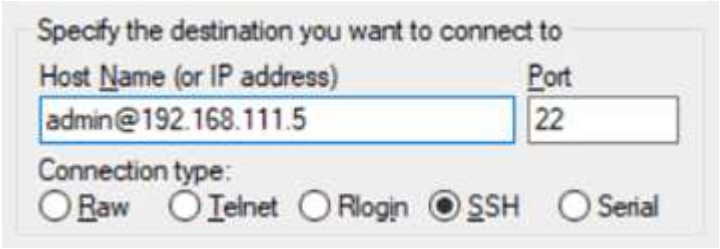
当部署在多个 AZ 中时， Cloud Volumes ONTAP HA 配置使用浮动 IP 地址作为集群管理接口，这意味着外部路由不可用。您必须从属于同一路由域的主机进行连接。

步骤

1. 在NetApp Console中，确定集群管理接口的 IP 地址：
   a. 从左侧导航菜单中，选择“存储”>“管理”。
   b. 在*系统*页面上，选择Cloud Volumes ONTAP系统。
   c. 复制右侧窗格中显示的集群管理 IP 地址。
2. 使用 SSH 使用管理员帐户连接到集群管理接口 IP 地址。

   例子

   下图显示了使用 PuTTY 的示例：



3. 在登录提示符下，输入管理员帐户的密码。

   例子

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

系统健康和事件

验证**Cloud Volumes ONTAP** 的**AutoSupport**设置

AutoSupport主动监控系统的健康状况并向NetApp技术支持发送消息。默认情况下，每个节点上都启用AutoSupport ，以使用 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具有出站互联网连接。有关详细信息，请参阅您的云提供商的网络要求。

AutoSupport要求

Cloud Volumes ONTAP节点需要NetApp AutoSupport的出站互联网访问权限，它可以主动监控系统的健康状况并向NetApp技术支持发送消息。

路由和防火墙策略必须允许 HTTPS 流量到达以下端点，以便Cloud Volumes ONTAP可以发送AutoSupport消息：

- \ https://mysupport.netapp.com/aods/asupmessage
- \ https://mysupport.netapp.com/asupprod/post/1.0/postAsup

如果没有可用的出站互联网连接来发送AutoSupport消息， NetApp Console会自动配置您的Cloud Volumes ONTAP系统以使用控制台代理作为代理服务器。唯一的要求是确保控制台代理的安全组允许通过端口 3128 进行入站连接。部署控制台代理后，您需要打开此端口。

如果您为Cloud Volumes ONTAP定义了严格的出站规则，那么您还需要确保Cloud Volumes ONTAP安全组允许通过端口 3128 进行出站连接。

如果您使用 HA 对，则 HA 中介不需要出站互联网访问。

验证出站互联网访问可用后，您可以测试AutoSupport以确保它可以发送消息。有关说明，请参阅 "ONTAP文档：设置AutoSupport"。

排除AutoSupport配置故障

如果出站连接不可用，并且控制台无法配置您的Cloud Volumes ONTAP系统以使用控制台代理作为代理服务器，您将收到来自控制台的通知，提示您的系统无法发送AutoSupport消息。请按照以下步骤解决此问题。

步骤

1. 使用 SSH 安全地连接到Cloud Volumes ONTAP系统，以使用ONTAP CLI。

   "了解如何通过 SSH 连接到Cloud Volumes ONTAP" 。

2. 查看AutoSupport子系统的详细状态：

   ```
   autosupport check show-details
   ```

   回复内容如下：

```
    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 类别的状态是 `OK` 这意味着AutoSupport已正确配置，可以发送消息。

3. 否则，请验证每个Cloud Volumes ONTAP节点的代理 URL：

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

4. 如果代理 URL 参数为空，请配置Cloud Volumes ONTAP以使用控制台代理作为代理：

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

5. 再次确认AutoSupport状态：

   ```
   autosupport check show-details
   ```

6. 如果状态仍然为失败，请验证Cloud Volumes ONTAP和控制台代理之间是否通过端口建立连接。 `3128`。

7. 如果验证后状态仍然失败，请通过 SSH 连接到控制台代理。

   "了解有关控制台代理连接到 Linux VM 的更多信息"

8. 前往 `/opt/application/netapp/cloudmanager/docker_occm/data/`。
9. 打开代理配置文件 `squid.conf`。这是文件的结构：

```
http_port 3128
acl netapp_support dst support.netapp.com
http_access allow netapp_support
request_header_max_size 21 KB
reply_header_max_size 21 KB
http_access deny all
httpd_suppress_version_string on
```

10. 如果您的文件中没有Cloud Volumes ONTAP系统的 CIDR 块条目，请添加新条目并允许访问：

    ```
    acl cvonet src <cidr>

    http_access allow cvonet
    ```

    以下是一个例子：

```
http_port 3128
acl netapp_support dst support.netapp.com
acl cvonet src <cidr>
http_access allow netapp_support
http_access allow cvonet
request_header_max_size 21 KB
reply_header_max_size 21 KB
http_access deny all
httpd_suppress_version_string on
```

11. 编辑配置文件后，重启代理容器。 `sudo`。然后，根据您使用的是 Docker 还是 Podman，运行以下命令：

    对于 Docker，请运行 `docker restart squid`。

    如果您使用的是 Podman，请运行 `podman restart squid`。

12. 返回ONTAP CLI 并验证Cloud Volumes ONTAP是否可以发送AutoSupport消息：

    ```
    autosupport check show-details
    ```

相关链接

- "AWS 中Cloud Volumes ONTAP的网络要求"

- "Azure 中Cloud Volumes ONTAP的网络要求"
- "Google Cloud 中Cloud Volumes ONTAP的网络要求"

为Cloud Volumes ONTAP系统配置 EMS

事件管理系统 (EMS) 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的地（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，请参阅 "ONTAP文档：EMS 配置概述"。

概念

许可

Cloud Volumes ONTAP许可

Cloud Volumes ONTAP有多种许可选项。每个选项都可以让您选择符合您需求的消费模式。

许可概述

新客户可以使用以下许可选项。

基于容量的许可
: 按配置容量支付NetApp帐户中的多个Cloud Volumes ONTAP系统的费用。包括购买附加云数据服务的能力。有关基于容量的许可证的消费模式或购买选项的更多信息，请参阅："了解有关基于容量的许可证的更多信息" 。

Keystone订阅
: 一种按需付费的订阅式服务，为高可用性 (HA) 对提供无缝的混合云体验。

以下部分提供了有关每个选项的更多详细信息。

> 对于未经许可而使用许可的功能，我们将不提供支持。

基于容量的许可

基于容量的许可包使您能够按 TiB 容量支付Cloud Volumes ONTAP费用。该许可证与您的NetApp帐户相关联，只要许可证提供足够的容量，您就可以根据许可证为多个系统收费。

例如，您可以购买单个 20 TiB 许可证，部署四个Cloud Volumes ONTAP系统，然后为每个系统分配一个 5 TiB 卷，总共 20 TiB。该容量可供该帐户中部署的每个Cloud Volumes ONTAP系统上的卷使用。

基于容量的许可以_包_的形式提供。部署Cloud Volumes ONTAP系统时，您可以根据业务需求从多个许可包中进行选择。

> 虽然NetApp Console中管理的产品和服务的实际使用情况和计量始终以 GiB 和 TiB 计算，但 GB/GiB 和 TB/TiB 这两个术语可互换使用。这反映在云市场列表、价格报价、列表描述和其他支持文档中。

套餐

以下基于容量的软件包可用于Cloud Volumes ONTAP。有关基于容量的许可证包的更多信息，请参阅"了解有关基于容量的许可证的更多信息"。

有关以下基于容量的包所支持的 VM 类型的列表，请参阅：

- "Azure 中支持的配置"

- "Google Cloud 中支持的配置"

免费增值

免费提供NetApp提供的所有Cloud Volumes ONTAP功能（仍需支付云提供商费用）。免费增值套餐具有以下特点：

- 不需要许可证或合同。
- 不包括来自NetApp的支持。
- 每个Cloud Volumes ONTAP系统的配置容量限制为 500 GiB。
- 对于任何云提供商，每个NetApp帐户最多可以使用 10 个Cloud Volumes ONTAP系统和免费增值服务。
- 如果Cloud Volumes ONTAP系统的配置容量超过 500 GiB，则控制台会将该系统转换为 Essentials 包。

  一旦系统转换为 Essentials 包，"最低收费"适用于它。

  已转换为 Essentials 包的Cloud Volumes ONTAP系统无法切换回 Freemium，即使配置容量减少到 500 GiB 以下。其他预置容量少于 500 GiB 的系统仍保留在免费增值版上（只要它们是使用免费增值产品部署的）。

必需品

您可以通过多种不同的配置按容量付费：

- 选择您的Cloud Volumes ONTAP配置：
  - 单节点或 HA 系统
  - 用于灾难恢复 (DR) 的文件和块存储或辅助数据
- 额外付费即可添加任何 NetApp 云数据服务

专业的

按容量支付任何类型的Cloud Volumes ONTAP配置的费用，并提供无限备份。

- 为任何Cloud Volumes ONTAP配置提供许可

  单节点或 HA，以相同的费率对主卷和辅助卷进行容量计费

- 包括使用NetApp Backup and Recovery进行无限卷备份，但仅适用于使用专业版软件包的Cloud Volumes ONTAP系统。

  备份和恢复需要按使用量付费 (PAYGO) 订阅，但使用此服务不会产生任何费用。有关设置备份和恢复许可的更多信息，请参阅 "设置备份和恢复许可"。

- 额外付费即可添加任何 NetApp 云数据服务

基于容量的许可证的可用性

Cloud Volumes ONTAP系统的 PAYGO 和 BYOL 许可证的可用性要求控制台代理启动并运行。

"了解控制台代理" 。

已限制 BYOL 许可证的购买、延期和续订。有关更多信息，请参阅 "Cloud Volumes ONTAPP的 BYOL 许可可用性受限" 。

如何开始

了解如何开始使用基于容量的许可：

- "在 AWS 中设置Cloud Volumes ONTAP许可"
- "在 Azure 中设置Cloud Volumes ONTAP许可"
- "在 Google Cloud 中设置Cloud Volumes ONTAP许可"

Keystone订阅

一种按需付费的订阅式服务，为那些喜欢 OpEx 消费模式而非前期资本支出或租赁的用户提供无缝的混合云体验。

收费基于Keystone订阅中一个或多个Cloud Volumes ONTAP HA 对的承诺容量大小。

每个卷的预配置容量都会定期汇总并与您的Keystone订阅中的承诺容量进行比较，任何超额部分都会作为Keystone订阅中的突发容量收费。

"了解有关NetApp Keystone 的更多信息" 。

支持的配置

HA 对支持 Keystone 订阅。此时单节点系统不支持此许可选项。

容量限制

在基于容量的许可模型中，每个Cloud Volumes ONTAP系统都支持分层到对象存储，并且总分层容量可以扩展到云提供商的存储桶限制。虽然许可证没有施加容量限制，但遵循 "FabricPool最佳实践"确保在配置和管理分层时实现最佳性能、可靠性和成本效率。

有关每个云提供商的容量限制的信息，请参阅其文档：

- "AWS 文档"
- "托管磁盘的 Azure 文档"和 "Azure Blob 存储文档"
- "Google Cloud 文档"

如何开始

了解如何开始使用Keystone订阅：

- "在 AWS 中设置Cloud Volumes ONTAP许可"
- "在 Azure 中设置Cloud Volumes ONTAP许可"
- "在 Google Cloud 中设置Cloud Volumes ONTAP许可"

基于节点的许可

基于节点的许可是上一代许可模式，使您能够按节点许可Cloud Volumes ONTAP 。此许可模式不适用于新客户。按节点充电已被上述按容量充电方法所取代。

NetApp已计划终止基于节点的许可的可用性 (EOA) 和支持 (EOS)。在 EOA 和 EOS 之后，基于节点的许可证将需要转换为基于容量的许可证。

有关信息，请参阅 "客户公报：CPC-00589"。

基于节点的许可证的可用性终止

从 2024 年 11 月 11 日起，基于节点的许可证的有限可用性已终止。基于节点的许可支持将于 2024 年 12 月 31 日结束。

如果您拥有有效的基于节点的合同，并且该合同的有效期超出了 EOA 日期，那么您可以继续使用该许可证，直到合同到期。一旦合同到期，就需要过渡到基于容量的许可模式。如果您没有Cloud Volumes ONTAP节点的长期合同，则务必在 EOS 日期之前规划转换。

从下表中了解有关每种许可证类型以及 EOA 对其影响的更多信息：

许可证类型	**EOA** 之后的影响
通过自带许可证 (BYOL) 购买的有效基于节点的许可证	许可证有效期至到期日。现有未使用的基于节点的许可证可用于部署新的Cloud Volumes ONTAP系统。
通过 BYOL 购买的基于节点的许可证已过期	您无权使用此许可证部署新的Cloud Volumes ONTAP系统。现有系统可能会继续运行，但在 EOS 日期之后，您将不会收到任何系统支持或更新。
具有 PAYGO 订阅的有效基于节点的许可证	自 EOS 日期起将停止获得NetApp支持，直到您过渡到基于容量的许可证。

除外事项

NetApp认识到某些情况需要特殊考虑，基于节点的许可的 EOA 和 EOS 不适用于以下情况：

- 美国公共部门客户
- 私有模式下的部署
- AWS 中国区Cloud Volumes ONTAP部署

对于这些特殊情况， NetApp将提供支持，以满足符合合同义务和运营需求的独特许可要求。

即使在这些情况下，新的基于节点的许可证和许可证续订自批准之日起最长有效期为一年。

许可证转换

控制台可以通过许可证转换工具将基于节点的许可证无缝转换为基于容量的许可证。有关基于节点的许可的 EOA 的信息，请参阅"基于节点的许可证的可用性终止"。

在转换之前，最好熟悉两种许可模式之间的区别。基于节点的许可包括每个ONTAP实例的固定容量，这可能会限制灵活性。另一方面，基于容量的许可允许跨多个实例共享存储池，从而提供增强的灵活性，优化资源利用率，并降低重新分配工作负载时可能产生的经济损失。基于容量的充电可以无缝适应不断变化的存储需求。

要了解如何执行此转换，请参阅"将Cloud Volumes ONTAP基于节点的许可证转换为基于容量的许可证"。

不支持将系统从基于容量的许可转换为基于节点的许可。

了解有关Cloud Volumes ONTAP基于容量的许可证的更多信息

您应该熟悉基于容量的许可证的收费方式和容量使用情况。

消费模式或许可购买选项

我们提供基于容量的许可套餐，并有以下几种消费模式或购买选项：

- **BYOL**：自带许可证（BYOL）。从NetApp购买的许可证，可用于在任何云提供商中部署Cloud Volumes ONTAP 。

  已限制 BYOL 许可证的购买、延期和续订。有关更多信息，请参阅 "Cloud Volumes ONTAP 的 BYOL 许可可用性受限" 。

- **PAYGO**：即用即付 (PAYGO) 订阅是从云提供商市场按小时订阅的。
- 年度：来自云提供商市场的年度合同。

请注意以下事项：

- 如果您从NetApp购买了 BYOL 许可证，则还需要从云提供商的云市场订阅 PAYGO 产品。NetApp已限制 BYOL 许可。当您的 BYOL 许可证到期时，您需要将其替换为云市场订阅。

  您的许可证始终会被首先收费，但在以下情况下，我们将按照市场上的小时费率向您收费：

  - 如果您超出许可容量
  - 如果您的许可证期限已到期
- 如果您与市场签订了年度合同，则您部署的所有Cloud Volumes ONTAP系统都将根据该合同收费。您不能将年度市场合同与 BYOL 混合搭配。
- 中国地区仅支持具有 BYOL 的单节点系统。中国地区的部署不受 BYOL 许可限制。

更改许可证包

部署后，您可以更改使用基于容量的许可的Cloud Volumes ONTAP系统的软件包。例如，如果您使用 Essentials 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 包。

"了解如何更改充电方式" 。

有关将基于节点的许可证转换为基于容量的许可证的信息，请参阅

支持的存储类型和套餐如何收费

Cloud Volumes ONTAP的计费基于多种因素，例如套餐和卷类型。Cloud Volumes ONTAP 9.7 及更高版本提供基于容量的许可包。

有关定价的详细信息，请访问 "NetApp Console网站"。

Storage VM

- 额外的数据服务存储虚拟机 (SVM) 无需额外的许可费用，但每个数据服务 SVM 至少需支付 4 TiB 的容量费用。
- 灾难恢复 SVM 根据预置容量收费。

HA 对

对于 HA 对，您只需为节点上配置的容量付费。您无需为同步镜像到合作伙伴节点的数据付费。

FlexClone和FlexCache卷

- 您无需为FlexClone卷使用的容量付费。
- 源和目标FlexCache卷被视为主数据，并根据配置的空间收费。

读/写卷

如果您创建或使用可写（读/写）卷，则该卷将被视为主卷，并按每个存储虚拟机 (SVM) 的最低费用收取已配置容量的费用。例如FlexVol读/写卷、 SnapLock审计卷和 CIFS/NFS 审计卷。所有用户创建的数据量均按您的订阅和套餐类型收费。 ONTAP内部自动创建且无法存储数据的卷（例如 SVM 根卷）不收费。

基本套装

使用 Essentials 套餐时，您需要根据部署类型（HA 或单节点）和卷类型（主卷或辅助卷）付费。价格从高到低的顺序如下：*Essentials Primary HA*、*Essentials Primary Single Node*、*Essentials Secondary HA* 和 *Essentials Secondary Single Node*。或者，当您购买市场合同或接受私人优惠时，任何部署或卷类型的容量费用都是相同的。

许可完全基于Cloud Volumes ONTAP系统内创建的卷类型：

- 基本单节点：仅使用一个ONTAP节点在Cloud Volumes ONTAP系统上创建的读/写卷。
- Essentials HA：使用两个ONTAP节点读取/写入卷，这两个节点可以相互故障转移，以实现无中断数据访问。
- 基本辅助单节点：仅使用一个ONTAP节点在Cloud Volumes ONTAP系统上创建的数据保护 (DP) 类型卷（通常是只读的SnapMirror或SnapVault目标卷）。

  如果只读/DP 卷成为主卷，则控制台会将其视为主数据，并且收费成本将根据卷处于读/写模式的时间来计算。当卷再次变为只读/DP 时，它会再次将该卷视为辅助数据，并使用控制台中最匹配的许可证进行相应的收费。

- 基本辅助 HA：在Cloud Volumes ONTAP系统上使用两个可以相互故障转移以实现无中断数据访问的ONTAP节点创建的数据保护 (DP) 类型卷（通常是只读的SnapMirror或SnapVault目标卷）。

容量限制

在基于容量的许可模型中，每个Cloud Volumes ONTAP系统都支持分层到对象存储，并且总分层容量可以扩展到云提供商的存储桶限制。虽然许可证没有施加容量限制，但遵循 "FabricPool最佳实践"确保在配置和管理分层时实现最佳性能、可靠性和成本效率。

有关每个云提供商的容量限制的信息，请参阅其文档：

- "AWS 文档"
- "托管磁盘的 Azure 文档"和 "Azure Blob 存储文档"
- "Google Cloud 文档"

最大系统数量

通过基于容量的许可，Cloud Volumes ONTAP 系统的最大数量限制为每个 NetApp Console 组织 24 个。_系统_是 Cloud Volumes ONTAP HA 对、Cloud Volumes ONTAP 单节点系统或您创建的任何其他存储 VM。默认存储 VM 不计入限制。此限制适用于所有许可模式。

例如，假设您有三个系统：

- 具有一个存储虚拟机的单节点Cloud Volumes ONTAP系统（这是部署Cloud Volumes ONTAP时创建的默认存储虚拟机）

  该系统算作一个系统。

- 具有两个存储虚拟机（默认存储虚拟机，加上您创建的一个额外的存储虚拟机）的单节点Cloud Volumes ONTAP系统

  此系统计为两个系统：一个用于单节点系统，一个用于附加存储 VM。

- 具有三个存储虚拟机（默认存储虚拟机，以及您创建的两个额外的存储虚拟机）的Cloud Volumes ONTAP HA 对

  该系统计为三个系统：一个用于 HA 对，两个用于附加存储虚拟机。

总共有六个系统。这样一来，您的组织中就可以再容纳 14 个系统。

如果您需要部署超过 24 台系统，请联系您的客户代表或销售团队。

"了解 AWS、Azure 和 Google Cloud 的存储限制" 。

最低收费

对于每个具有至少一个主（读写）卷的提供数据的存储虚拟机，最低收费为 4 TiB。如果主卷的总和小于 4 TiB，则控制台将对该存储虚拟机应用 4 TiB 的最低费用。

如果您尚未配置任何卷，则不适用最低费用。

对于 Essentials 包，4 TiB 最低容量费用不适用于仅包含辅助（数据保护）卷的存储虚拟机。例如，如果您有一个包含 1 TiB 二级数据的存储虚拟机，那么您只需为该 1 TiB 数据付费。对于专业套餐类型，无论卷类型如何，最低容量收费均为 4 TiB。

计费偏好和超额费用

您可以在控制台的“**Licenses and subscriptions**”部分选择您的收费方式。当您的使用量超过许可证套餐或年度订阅中规定的容量时，就会产生超额费用。

- * NetApp优先授权*：在此模式下，您的使用量首先会根据您的许可证包（自带许可证）的容量进行计费。如果您超出许可容量，超出部分将根据您的年度市场订阅或市场按需小时费率（PAYGO）收取费用。如果您的 BYOL 许可证到期，您必须通过云市场过渡到基于容量的许可模式。更多信息请参阅 "将Cloud Volumes ONTAP基于节点的许可证转换为基于容量的许可证"。
- 仅限市场订阅用户：在此模式下，您的使用费用将首先计入您的年度市场订阅费用。任何额外使用均按市场按需小时费率（PAYGO）收费。任何未使用的许可证容量在计费时均不予考虑。

有关账单偏好设置的更多信息，请参阅 "了解许可证和订阅的计费方式"。

Essentials许可证超额费用如何收取

如果您从NetApp购买 Essentials 许可证（自带许可证），并且超出了特定 Essentials 软件包的许可容量，则控制台会将超出部分的费用计入价格更高的 Essentials 许可证（如果您有可用容量的许可证）。游戏主机首先会使用您已付费的可用容量，然后再向市场收费。如果您的 BYOL 许可证没有可用容量，超出容量的部分将按市场按需小时费率 (PAYGO) 收费，并添加到您的月账单中。

同样，如果您签订了年度市场合同或包含多个 Essentials 套餐的私人优惠，并且您的使用量超过了特定套餐的部署和容量类型的承诺容量，则控制台会根据可用容量，向价格更高的 Essentials 套餐收取超额费用。当该容量耗尽后，剩余的超额容量将按市场按需（PAYGO）小时费率计费，并添加到您的月账单中。

有关 Essentials 许可证收费的信息，请参阅"基本套装"。

这是一个例子。假设您拥有 Essentials 包的以下许可证：

- 具有 500 TiB 承诺容量的 500 TiB *Essentials Secondary HA* 许可证
- 500 TiB _Essentials 单节点_许可证，仅具有 100 TiB 的承诺容量

另外 50 TiB 在具有辅助卷的 HA 对上进行配置。控制台不会向 PAYGO 收取这 50 TiB 的费用，而是向 *Essentials Single Node* 许可证收取 50 TiB 的超额费用。该许可证的价格高于_Essentials Secondary HA_，但它利用您已购买的许可证，并且不会增加您的每月账单费用。

在“管理”> “Licenses and subscriptions”中，您可以看到针对“Essentials 单节点”许可证收取了 50 TiB 的费用。

这是另一个例子。假设您拥有 Essentials 包的以下许可证：

- 具有 500 TiB 承诺容量的 500 TiB *Essentials Secondary HA* 许可证
- 500 TiB _Essentials 单节点_许可证，仅具有 100 TiB 的承诺容量

另外 100 TiB 在具有主卷的 HA 对上进行配置。您购买的许可证没有_Essentials Primary HA_承诺容量。*Essentials Primary HA* 许可证的价格高于 *Essentials Primary Single Node* 和 *Essentials Secondary HA* 许可证。

在此示例中，控制台按照市场价格对额外的 100 TiB 收取超额费用。超额费用将出现在您的每月账单上。

存储

Cloud Volumes ONTAP支持的客户端协议

Cloud Volumes ONTAP支持 iSCSI、NFS、SMB、NVMe-TCP 和 S3 客户端协议。

iSCSI

iSCSI 是一种可以在标准以太网网络上运行的块协议。大多数客户端操作系统都提供通过标准以太网端口运行的软件启动器。

NFS

NFS是UNIX和LINUX系统的传统文件访问协议。客户端可以使用 NFSv3、NFSv4 和 NFSv4.1 协议访问ONTAP卷中的文件。您可以使用 UNIX 样式权限、NTFS 样式权限或两者的混合来控制文件访问。

客户端可以使用 NFS 和 SMB 协议访问相同的文件。

SMB

SMB是Windows系统的传统文件访问协议。客户端可以使用 SMB 2.0、SMB 2.1、SMB 3.0 和 SMB 3.1.1 协议访问ONTAP卷中的文件。与 NFS 一样，支持混合的权限样式。

S3

Cloud Volumes ONTAP支持 S3 作为横向扩展存储的选项。 S3 协议支持使您能够配置 S3 客户端对存储虚拟机 (SVM) 中存储桶所含对象的访问。

"ONTAP文档：了解 S3 多协议的工作原理" 。"ONTAP文档：了解如何在ONTAP中配置和管理 S3 对象存储服务" 。

NVMe-TCP

从ONTAP版本 9.12.1 开始，所有云提供商均支持 NVMe-TCP。 Cloud Volumes ONTAP在部署期间支持 NVMe-TCP 作为存储虚拟机 (SVM) 的块协议，并自动安装所需的 NVMe 许可证。

NetApp Console不提供任何针对 NVMe-TCP 的管理功能。

有关通过ONTAP配置 NVMe 的更多信息，请参阅 "ONTAP文档：为 NVMe 配置存储虚拟机"。

用于Cloud Volumes ONTAP集群的磁盘和聚合

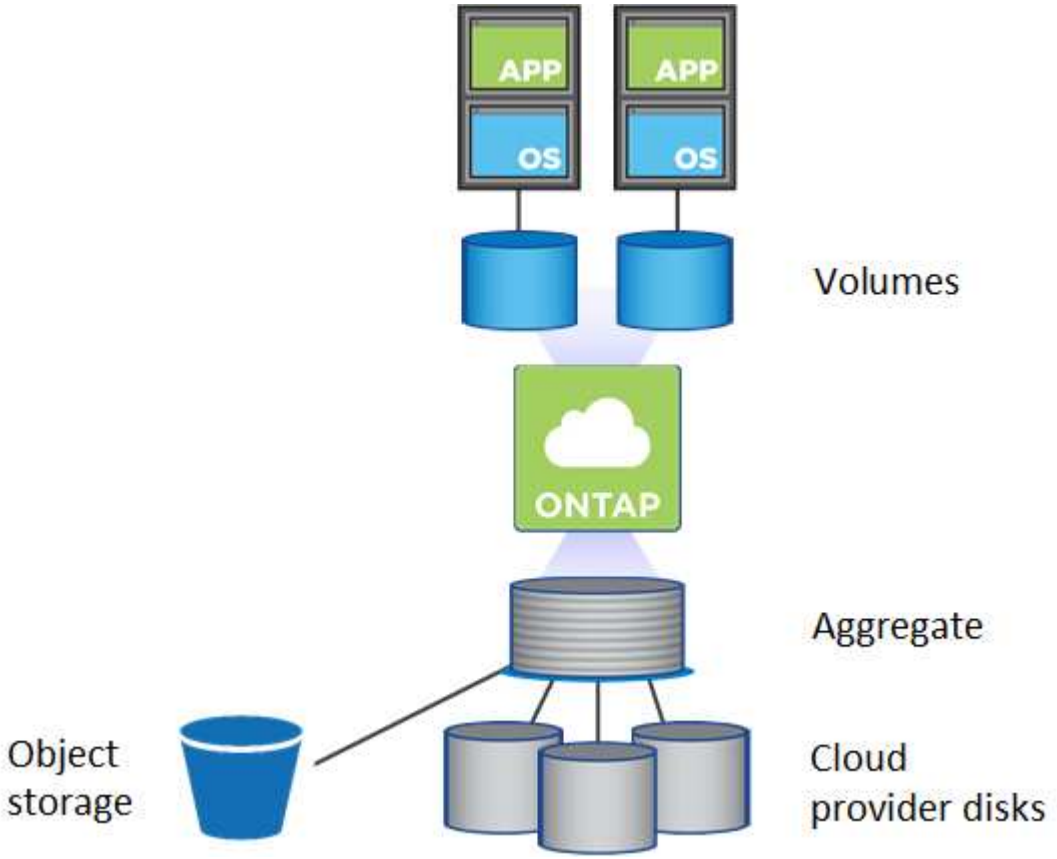
了解Cloud Volumes ONTAP如何使用云存储可以帮助您了解存储成本。

> 您必须从NetApp Console创建和删除所有磁盘和聚合。您不应从其他管理工具执行这些操作。这样做会影响系统稳定性，妨碍将来添加磁盘的能力，并可能产生冗余的云提供商费用。

概述

Cloud Volumes ONTAP使用云提供商存储作为磁盘并将它们分组为一个或多个聚合。聚合为一个或多个卷提供

存储。



支持多种类型的云盘。创建卷时选择磁盘类型，部署Cloud Volumes ONTAP时选择默认磁盘大小。

从云提供商处购买的存储总量是_原始容量_。 _可用容量_较少，因为大约 12% 到 14% 是为Cloud Volumes ONTAP使用保留的开销。例如，如果控制台创建 500 GiB 聚合，则可用容量为 442.94 GiB。

AWS 存储

在 AWS 中， Cloud Volumes ONTAP使用 EBS 存储来存储用户数据，并在某些 EC2 实例类型上使用本地 NVMe 存储作为闪存缓存。

EBS 存储

在 AWS 中，一个聚合最多可以包含 6 个大小相同的磁盘。但是，如果您的配置支持 Amazon EBS 弹性卷功能，则聚合最多可以包含 8 个磁盘。"了解有关弹性卷支持的更多信息" 。

最大磁盘大小为 16 TiB。

底层 EBS 磁盘类型可以是通用 SSD（gp3 或 gp2）、预配置 IOPS SSD（io1）或吞吐量优化 HDD（st1）。您可以将 EBS 磁盘与 Amazon Simple Storage Service (Amazon S3) 配对以"低成本对象存储"。

使用吞吐量优化 HDD (st1) 时，不建议将数据分层到对象存储。

本地 **NVMe** 存储

一些 EC2 实例类型包括本地 NVMe 存储， Cloud Volumes ONTAP将其用作"Flash Cache"。

相关链接

- "AWS 文档：EBS 卷类型"
- "了解如何为 AWS 中的系统选择磁盘类型和磁盘大小"
- "查看 AWS 中Cloud Volumes ONTAP的存储限制"
- "查看 AWS 中Cloud Volumes ONTAP支持的配置"

Azure 存储

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

单节点系统

单节点系统可以使用以下类型的 Azure 托管磁盘：

- 高级 *SSD* 托管磁盘 以更高的成本为 I/O 密集型工作负载提供高性能。
- 与高级 SSD 托管磁盘相比，高级 *SSD v2* 托管磁盘 为单节点和 HA 对提供了更高的性能和更低的延迟，并且成本更低。
- _标准 SSD 托管磁盘_为需要低 IOPS 的工作负载提供一致的性能。
- 如果您不需要高 IOPS 并且想要降低成本，那么“标准 HDD 托管磁盘”是一个不错的选择。

  每种托管磁盘类型的最大磁盘大小为 32 TiB。

  您可以将托管磁盘与 Azure Blob 存储配对，以"低成本对象存储"。

HA 对

HA 对使用两种类型的磁盘，它们以更高的成本为 I/O 密集型工作负载提供高性能：

- *Premium page blob*，最大磁盘大小为 8 TiB
- 托管磁盘，最大磁盘大小为 32 TiB

相关链接

- "了解如何为 Azure 中的系统选择磁盘类型和磁盘大小"
- "在 Azure 中启动Cloud Volumes ONTAP HA 对"
- "Microsoft Azure 文档：Azure 托管磁盘类型"
- "Microsoft Azure 文档：Azure 页 Blob 概述"
- "查看 Azure 中Cloud Volumes ONTAP的存储限制"

Google 云端存储

在 Google Cloud 中，聚合最多可以包含 6 个大小相同的磁盘。最大磁盘大小为 64 TiB。

磁盘类型可以是_区域 SSD 持久磁盘_、区域平衡持久磁盘_或_区域标准持久磁盘。您可以将永久性磁盘与 Google 存储桶配对，以"低成本对象存储"。

相关链接

- "Google Cloud 文档：存储选项"
- "查看 Google Cloud 中Cloud Volumes ONTAP 的存储限制"

RAID 类型

每个Cloud Volumes ONTAP聚合的 RAID 类型是 RAID0（条带化）。 Cloud Volumes ONTAP依赖云提供商来实现磁盘的可用性和耐用性。不支持其他 RAID 类型。

热备件

RAID0 不支持使用热备件实现冗余。

创建连接到Cloud Volumes ONTAP实例的未使用磁盘（热备用）是不必要的开支，并且可能会阻止根据需要配置额外的空间。因此，不建议这么做。

了解**Cloud Volumes ONTAP**对 **AWS Elastic Volumes** 的支持

通过Cloud Volumes ONTAP聚合支持 Amazon EBS Elastic Volumes 功能可提供更好的性能和额外的容量，同时使NetApp Console能够根据需要自动增加底层磁盘容量。

受益

- 动态磁盘增长

  当Cloud Volumes ONTAP正在运行且磁盘仍处于连接状态时，控制台可以动态增加磁盘的大小。

- 更好的性能

  启用弹性卷的聚合最多可以拥有八个磁盘，这些磁盘在两个 RAID 组中平均利用。此配置可提供更高的吞吐量和稳定的性能。

- 较大的骨料

  支持八个磁盘，最大聚合容量为 128 TiB。对于未启用弹性卷功能的聚合，这些限制高于六个磁盘限制和 96 TiB 限制。

  请注意，系统总容量限制保持不变。

"AWS 文档：了解有关 AWS 弹性卷的更多信息"

支持的配置

特定Cloud Volumes ONTAP版本和特定 EBS 磁盘类型支持 Amazon EBS Elastic Volumes 功能。

Cloud Volumes ONTAP版本

从 9.11.0 或更高版本创建的 *new* Cloud Volumes ONTAP系统支持弹性卷功能。 9.11.0 之前部署的现有Cloud Volumes ONTAP系统不支持该功能。

例如，如果您创建了Cloud Volumes ONTAP 9.9.0 系统，然后将该系统升级到版本 9.11.0，则不支持弹性卷功能。它必须是使用 9.11.0 或更高版本部署的新系统。

EBS 磁盘类型

使用通用 SSD（gp3）或预配置 IOPS SSD（io1）时，弹性卷功能会在聚合级别自动启用。使用任何其他磁盘类型的聚合不支持弹性卷功能。

所需的 AWS 权限

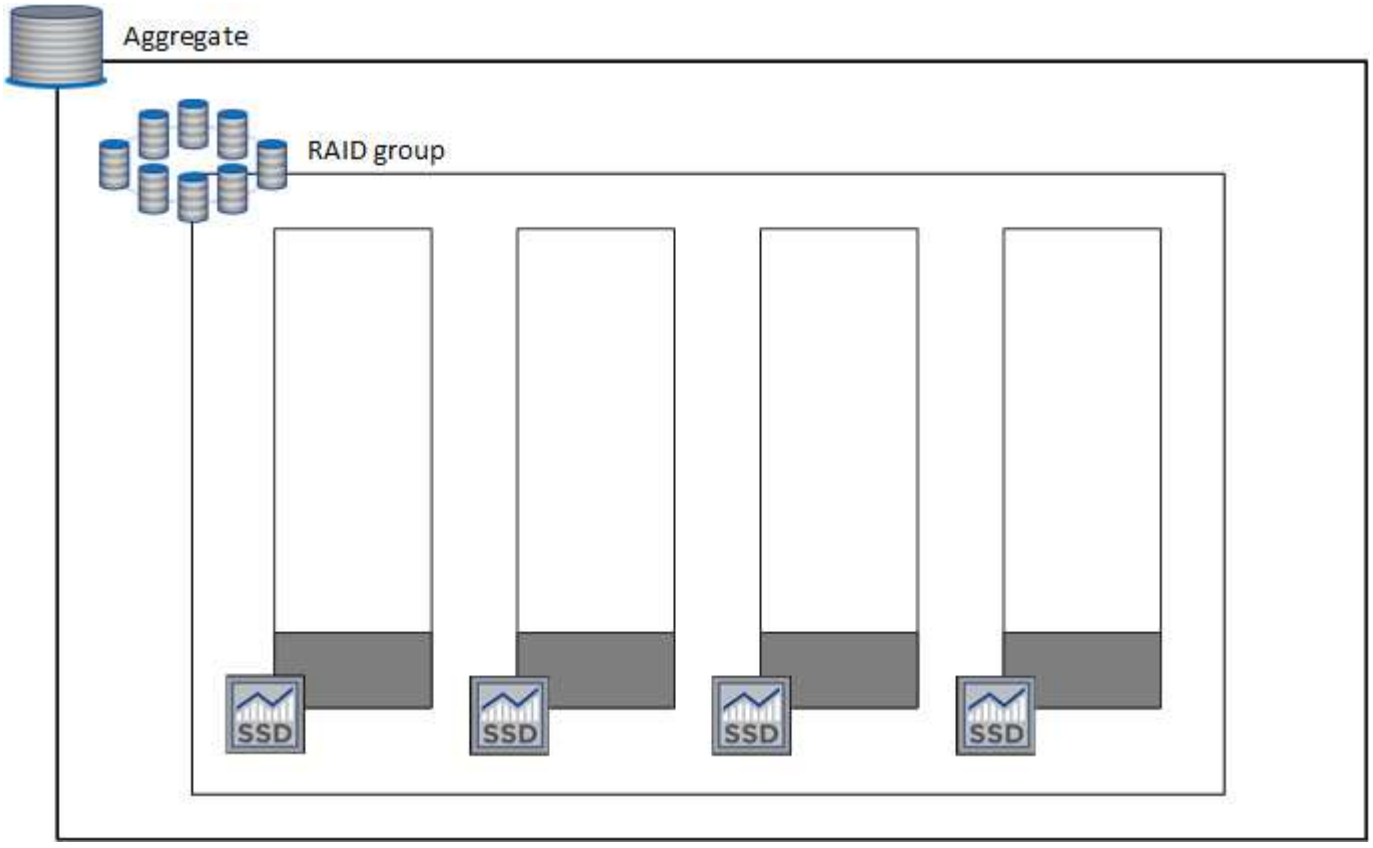
从 3.9.19 版本开始，控制台代理需要以下权限才能在Cloud Volumes ONTAP聚合上启用和管理弹性卷功能：

- ec2：描述卷修改
- ec2：修改卷

这些权限包含在 "NetApp提供的政策"

弹性卷支持如何运作

启用了弹性卷功能的聚合由一个或两个 RAID 组组成。每个 RAID 组有四个相同的磁盘，容量相同。下面是一个 10 TiB 聚合的示例，该聚合包含四个磁盘，每个磁盘大小为 2.5 TiB：



当控制台创建聚合时，它从一个 RAID 组开始。如果需要额外的容量，它会通过将 RAID 组中所有磁盘的容量增

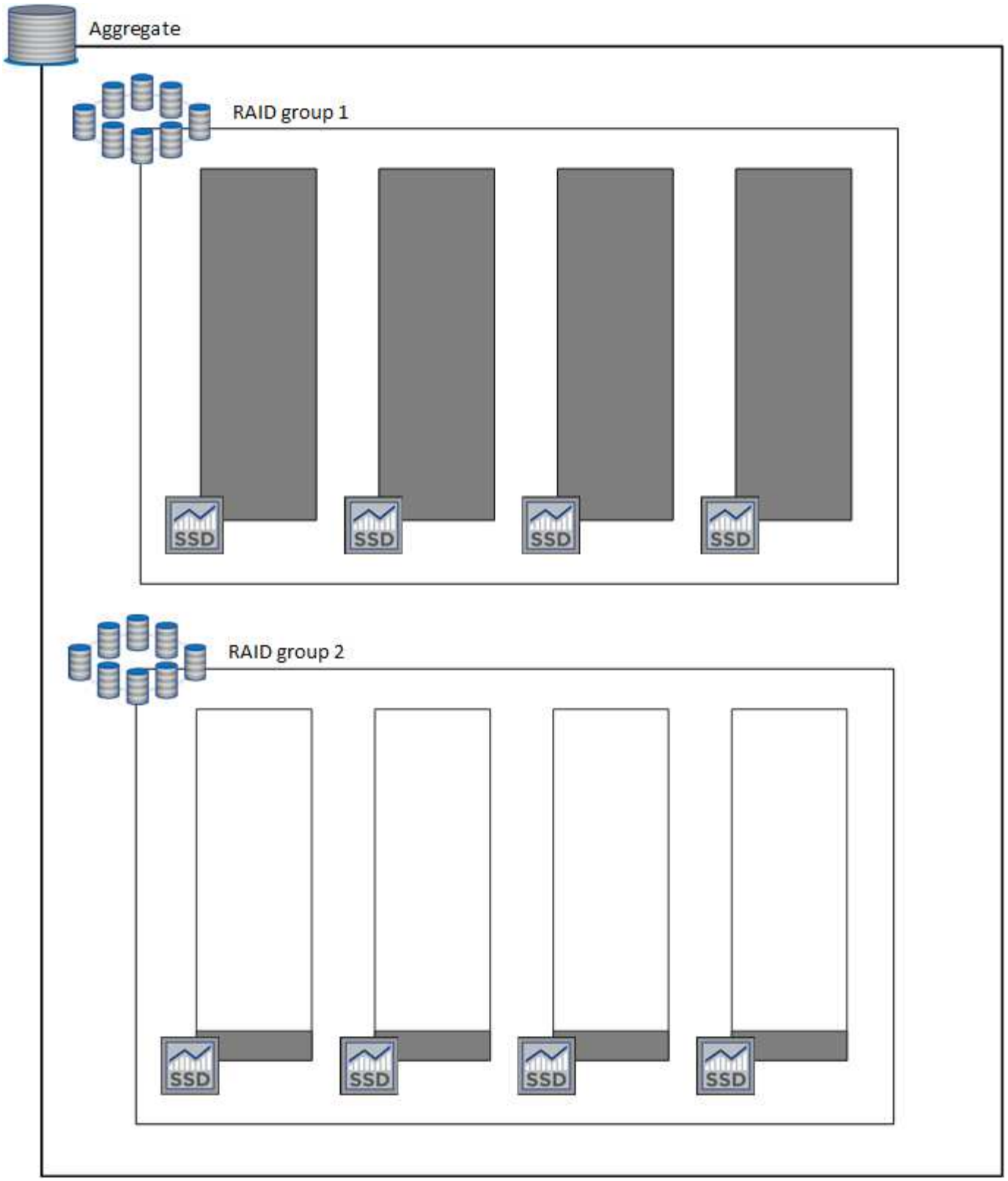
加相同的量来增加聚合。容量增加至少为 256 GiB 或聚合大小的 10%。

例如，如果您有一个 1 TiB 聚合，则每个磁盘为 250 GiB。聚合容量的 10% 为 100 GiB。这低于 256 GiB，因此聚合的大小增加了 256 GiB 的最小值（或每个磁盘 64 GiB）。

当Cloud Volumes ONTAP系统正在运行且磁盘仍处于连接状态时，控制台会增加磁盘的大小。该变化不会造成破坏。

如果聚合达到 64 TiB（或每个磁盘 16 TiB），控制台将创建第二个 RAID 组以提供额外的容量。第二个 RAID 组的工作方式与第一个 RAID 组相同：它有四个容量完全相同的磁盘，并且可以增长到 64 TiB。这意味着聚合的最大容量可以为 128 TiB。

以下是具有两个 RAID 组的聚合的示例。第一个 RAID 组已达到容量限制，而第二个 RAID 组中的磁盘有足够的可用空间。



创建卷时会发生什么

如果您创建使用 gp3 或 io1 磁盘的卷，控制台将按如下方式在聚合上创建该卷：

- 如果存在启用了弹性卷的现有 gp3 或 io1 聚合，则控制台会在该聚合上创建卷。
- 如果有多个启用了弹性卷的 gp3 或 io1 聚合，则控制台会在需要最少资源的聚合上创建卷。

- 如果系统仅具有未启用弹性卷的 gp3 或 io1 聚合，则会在该聚合上创建卷。

  虽然这种情况不太可能发生，但在两种情况下是有可能的：

  - 从 API 创建聚合时，您明确禁用了弹性卷功能。
  - 您从用户界面创建了一个新的Cloud Volumes ONTAP系统，在这种情况下，初始聚合上的弹性卷功能被禁用。审查[限制]请参阅下文以了解更多信息。

- 如果现有聚合都没有足够的容量，控制台将创建启用弹性卷的聚合，然后在该新聚合上创建卷。

  聚合的大小基于请求的卷大小加上额外的 10% 容量。

容量管理模式

控制台代理的容量管理模式与弹性卷的工作方式类似于与其他类型的聚合的工作方式：

- 启用自动模式（这是默认设置）时，如果需要额外的容量，控制台会自动增加聚合的大小。
- 如果将容量管理模式更改为手动，控制台将要求您批准购买额外容量。

"了解有关容量管理模式的更多信息" 。

限制

增加聚合体的大小最多可能需要 6 个小时。在此期间，控制台无法为该聚合请求任何额外容量。

如何使用弹性卷

您可以使用弹性卷执行以下任务：

- 使用 gp3 或 io1 磁盘时，创建一个在初始聚合上启用弹性卷的新系统

  "了解如何创建Cloud Volumes ONTAP系统"

- 在启用了弹性卷的聚合上创建新卷

  如果您创建使用 gp3 或 io1 磁盘的卷，控制台会自动在启用了弹性卷的聚合上创建该卷。有关详细信息，请参阅[创建卷时会发生什么]。

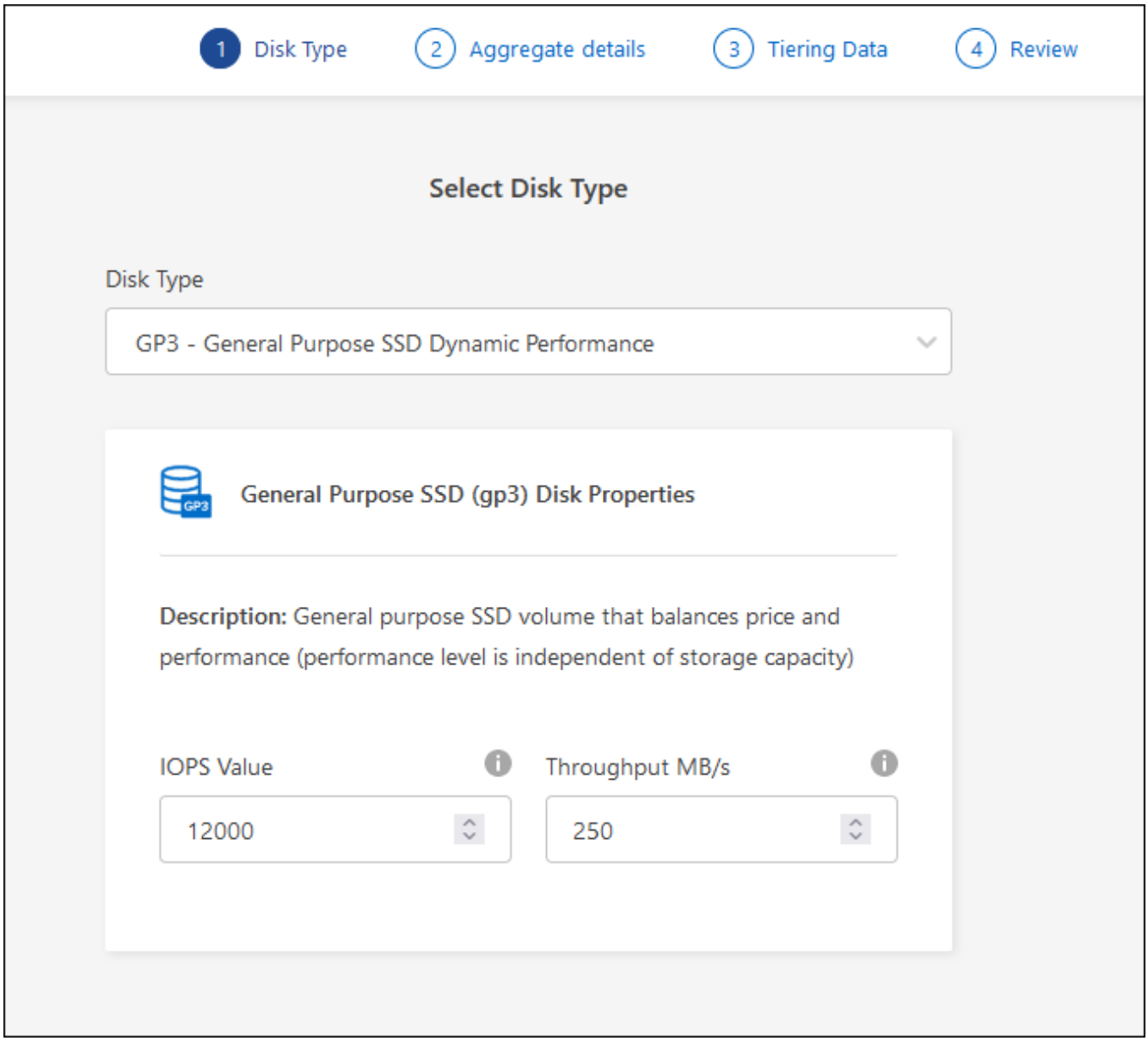
  "了解如何创建卷" 。

- 创建已启用弹性卷的新聚合

  只要Cloud Volumes ONTAP系统是从 9.11.0 或更高版本创建的，弹性卷就会在使用 gp3 或 io1 磁盘的新聚合上自动启用。

  创建聚合时，控制台会提示您输入聚合的容量大小。这与选择磁盘大小和磁盘数量的其他配置不同。

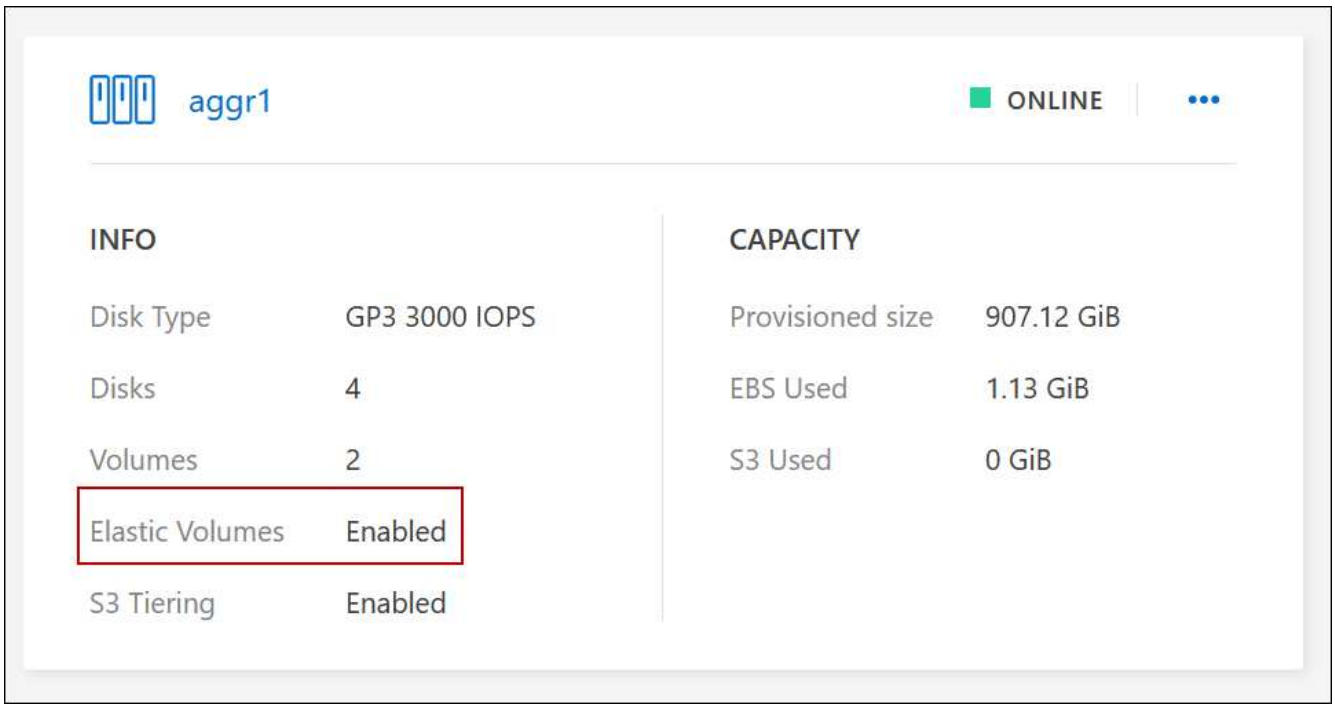
  以下屏幕截图显示了由 gp3 磁盘组成的新聚合的示例。



"了解如何创建聚合"。

- 识别已启用弹性卷的聚合

  当您转到“高级分配”页面时，您可以确定聚合上是否启用了弹性卷功能。在以下示例中，aggr1 启用了弹性卷。



- 向聚合添加容量

  虽然控制台会根据需要自动向聚合添加容量，但您也可以手动增加容量。

  "了解如何提高总容量"。

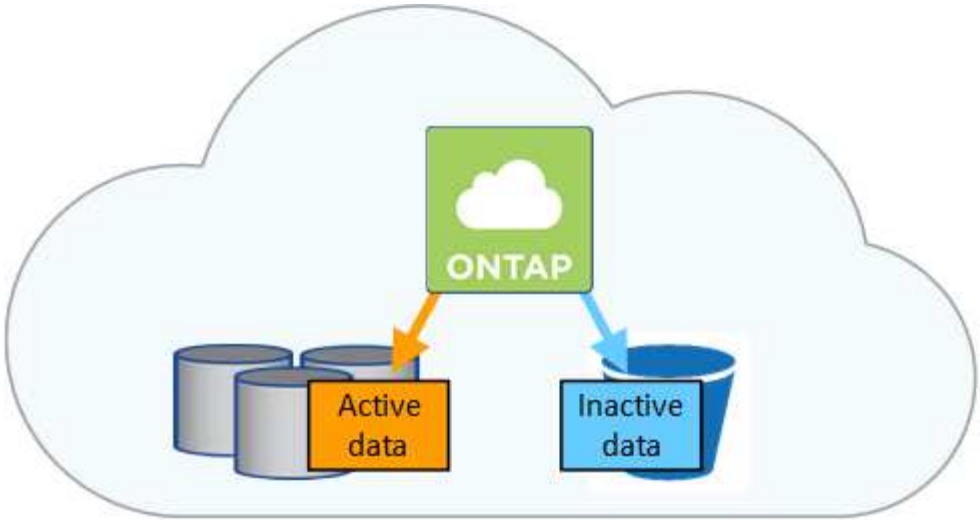
- 将数据复制到已启用弹性卷的聚合

  如果目标Cloud Volumes ONTAP系统支持弹性卷，则目标卷将放置在启用了弹性卷的聚合上（只要您选择 gp3 或 io1 磁盘）。

  "了解如何设置数据复制"

了解 AWS、Azure 或 Google Cloud 中的Cloud Volumes ONTAP数据分层

通过将非活动数据自动分层到低成本的对象存储来降低存储成本。活动数据保留在高性能 SSD 或 HDD 中，而非活动数据则分层到低成本对象存储中。这使您能够回收主存储上的空间并缩小辅助存储。



数据分层由FabricPool技术提供支持。 Cloud Volumes ONTAP为所有Cloud Volumes ONTAP集群提供数据分层，无需额外的许可证。当您启用数据分层时，分层到对象存储的数据会产生费用。有关对象存储成本的详细信息，请参阅云提供商的文档。

AWS 中的数据分层

在 AWS 中启用数据分层时，Cloud Volumes ONTAP 将 EBS 用作热数据的性能层，将 Amazon Simple Storage Service (Amazon S3) 用作非活动数据的容量层。

性能层

性能层可以是通用 SSD（gp3 或 gp2）或预配置 IOPS SSD（io1）。

使用吞吐量优化 HDD (st1) 时，不建议将数据分层到对象存储。

容量层

Cloud Volumes ONTAP系统将非活动数据分层到单个 S3 存储桶。

NetApp Console为每个系统创建一个 S3 存储桶，并将其命名为 fabric-pool-*cluster unique identifier*。不会为每个卷创建不同的 S3 存储桶。

当控制台创建 S3 存储桶时，它使用以下默认设置：

- 存储类别：标准
- 默认加密：已禁用
- 阻止公共访问：阻止所有公共访问
- 对象所有权：已启用 ACL
- 存储桶版本控制：已禁用
- 对象锁定：已禁用

存储类别

AWS 中分层数据的默认存储类别是“标准”。标准非常适合跨多个可用区域存储的频繁访问的数据。

如果您不打算访问非活动数据，则可以通过将存储类别更改为以下之一来降低存储成本：智能分层、单区不频繁访问、标准不频繁访问_或_*S3 Glacier* 即时检索。当您更改存储类别时，非活动数据将从标准存储类别

开始，如果 30 天后未访问该数据，则将转换到您选择的存储类别。

如果访问数据，访问成本会更高，因此在更改存储类之前请考虑这一点。 "Amazon S3 文档：了解有关 Amazon S3 存储类的更多信息" 。

您可以在创建系统时选择一个存储类，之后可以随时更改它。有关更改存储类别的说明，请参阅"将非活动数据分层到低成本对象存储"。

数据分层的存储类别是系统范围的 - 而不是每个卷的。

Azure 中的数据分层

当您在 Azure 中启用数据分层时， Cloud Volumes ONTAP会使用 Azure 托管磁盘作为热数据的性能层，并使用 Azure Blob 存储作为非活动数据的容量层。

性能层

性能层可以是 SSD 或 HDD。

容量层

Cloud Volumes ONTAP系统将非活动数据分层到单个 Blob 容器。

控制台为每个Cloud Volumes ONTAP系统创建一个带有容器的新存储帐户。存储帐户的名称是随机的。不会为每个卷创建不同的容器。

控制台使用以下设置创建存储帐户：

- 访问层：热
- 性能：标准
- 冗余：根据 Cloud Volume ONTAP部署
  - 单一可用区：本地冗余存储（LRS）
  - 多可用区域：区域冗余存储（ZRS）
- 帐户：StorageV2（通用 v2）
- 要求 REST API 操作进行安全传输：已启用
- 存储帐户密钥访问：已启用
- 最低 TLS 版本：版本 1.2
- 基础设施加密：已禁用

存储访问层

Azure 中分层数据的默认存储访问层是_热_层。热层非常适合容量层中频繁访问的数据。

如果您不打算访问容量层中的非活动数据，则可以选择_cool_存储层，其中非活动数据至少保留 30 天。您还可以选择冷层，其中非活动数据至少存储 90 天。根据您的存储要求和成本考虑，您可以选择最适合您需求的层。当您将存储层更改为_cool_或_cold_时，非活动容量层数据将直接移动到冷存储层。与热层相比，冷层提供的存储成本较低，但访问成本较高，因此在更改存储层之前请考虑到这一点。参考 "Microsoft Azure 文档：了解有关 Azure Blob 存储访问层的更多信息"。

您可以在添加Cloud Volumes ONTAP系统时选择一个存储层，之后可以随时更改它。有关更改存储层的详细

信息，请参阅"将非活动数据分层到低成本对象存储"。

数据分层的存储访问层是系统范围的，而不是每个卷的。

Google Cloud 中的数据分层

当您在 Google Cloud 中启用数据分层时， Cloud Volumes ONTAP会使用持久磁盘作为热数据的性能层，并使用 Google Cloud Storage 存储桶作为非活动数据的容量层。

性能层

性能层可以是 SSD 持久磁盘、平衡持久磁盘或标准持久磁盘。

容量层

Cloud Volumes ONTAP系统将非活动数据分层到单个 Google Cloud Storage 存储桶。

控制台为每个系统创建一个存储桶并将其命名为 fabric-pool-*cluster unique identifier*。不会为每个卷创建不同的存储桶。

当控制台创建存储桶时，它使用以下默认设置：

- 位置类型：区域
- 存储类别：标准
- 公共访问：受对象 ACL 约束
- 访问控制：细粒度
- 保护：无
- 数据加密：Google 管理的密钥

存储类别

分层数据的默认存储类是“标准存储”类。如果数据不经常访问，您可以通过更改为_Nearline Storage_或_Coldline Storage_来降低存储成本。当您更改存储类别时，后续非活动数据将直接移动到您选择的类别。

> 当您更改存储类别时，任何现有的非活动数据都将保持默认存储类别。要更改现有非活动数据的存储类别，您必须手动执行指定。

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请考虑到这一点。要了解更多信息，请参阅"Google Cloud 文档：存储类别"。

您可以在创建系统时选择一个存储层，之后可以随时更改它。有关更改存储类别的详细信息，请参阅"将非活动数据分层到低成本对象存储"。

数据分层的存储类别是系统范围的 - 而不是每个卷的。

数据分层和容量限制

如果启用数据分层，系统的容量限制将保持不变。该限制分布在性能层和容量层。

卷分层策略

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

一些分层策略具有相关的最小冷却期，该冷却期规定了卷中的用户数据必须保持不活动的时间，以便数据被视为“冷”并移动到容量层。当数据写入聚合时，冷却期开始。

您可以更改最短冷却期和 50% 的默认聚合阈值（更多内容见下文）。 "了解如何更改冷却时间"和"学习如何改变阈值"。

控制台允许您在创建或修改卷时从以下卷分层策略中进行选择：

仅快照

当聚合达到 50% 容量后， Cloud Volumes ONTAP会将与活动文件系统不关联的 Snapshot 副本的冷用户数据分层到容量层。冷却期约为2天。

如果读取，容量层上的冷数据块会变热并被移动到性能层。

全部

所有数据（不包括元数据）都会立即标记为冷数据，并尽快分层到对象存储。无需等待 48 小时让卷中的新块变冷。请注意，在设置“全部”策略之前位于卷中的块需要 48 小时才能冷却。

如果读取，云层上的冷数据块将保持冷状态并且不会写回性能层。此策略从ONTAP 9.6 开始可用。

自动

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

从Cloud Volumes ONTAP 9.4 开始支持此策略。

如果通过随机读取，容量层中的冷数据块会变热并移动到性能层。如果通过顺序读取（例如与索引和防病毒扫描相关的读取），冷数据块将保持冷状态并且不会移动到性能层。

无

将卷的数据保留在性能层中，防止其移动到容量层。

复制

复制卷时，您可以选择是否将数据分层到对象存储。如果这样做，控制台会将*备份*策略应用于数据保护卷。从Cloud Volumes ONTAP 9.6 开始，*全部*分层策略取代了备份策略。删除复制关系时，目标卷将保留复制期间生效的分层策略。

关闭**Cloud Volumes ONTAP**会影响冷却期

数据块通过冷却扫描进行冷却。在此过程中，未使用的块的温度将移动（冷却）到下一个较低的值。默认冷却时间取决于卷分层策略：

- 自动：31天
- 仅限快照：2 天

必须运行Cloud Volumes ONTAP才能使冷却扫描正常工作。如果关闭Cloud Volumes ONTAP ，冷却也会停止。因此，您可以体验更长的冷却时间。

当Cloud Volumes ONTAP关闭时，每个块的温度都会保留，直到您重新启动系统。例如，如果关闭系统时某个块的温度为 5，则重新打开系统时温度仍为 5。

设置数据分层

有关说明和受支持配置的列表，请参阅"将非活动数据分层到低成本对象存储"。

Cloud Volumes ONTAP存储管理

NetApp Console提供了对Cloud Volumes ONTAP存储的简化和高级管理。

您必须直接从控制台创建和删除所有磁盘和聚合。您不应从其他管理工具执行这些操作。这样做会影响系统稳定性，妨碍将来添加磁盘的能力，并可能产生冗余的云提供商费用。

存储配置

控制台通过为您购买磁盘和管理聚合，使Cloud Volumes ONTAP 的存储配置变得简单。您只需要创建卷。如果您愿意，您可以使用高级分配选项自行配置聚合。

简化配置

聚合为卷提供云存储。当您启动实例以及配置其他卷时，控制台会为您创建聚合。

创建卷时，控制台会执行以下三件事之一：

- 它将卷放置在具有足够可用空间的现有聚合上。
- 它通过为聚合购买更多磁盘将卷放置在现有聚合上。

+ 如果 AWS 中的聚合支持弹性卷，它还会增加 RAID 组中磁盘的大小。"了解有关弹性卷支持的更多信息" 。

- 它为新聚合购买磁盘并将卷放置在该聚合上。

控制台通过查看几个因素来确定新卷的放置位置：聚合的最大大小、是否启用精简配置以及聚合的可用空间阈值。

AWS 中聚合的磁盘大小选择

当控制台在 AWS 中为Cloud Volumes ONTAP创建新聚合时，它会随着聚合数量的增加逐渐增加磁盘大小，以在达到 AWS 数据磁盘限制之前最大化系统容量。

例如，控制台可能会选择以下磁盘大小：

总数	磁盘大小	最大总容量
1	500 GiB	3 TiB
4	1 TiB	6 TiB
6	2 TiB	12 TiB

此行为不适用于支持 Amazon EBS 弹性卷功能的聚合。启用了弹性卷的聚合由一个或两个 RAID 组组成。每个 RAID 组有四个相同的磁盘，容量相同。"了解有关弹性卷支持的更多信息" 。

您可以使用高级分配选项自行选择磁盘大小。

高级分配

您还可以管理聚合。"从“高级分配”页面" ，您可以创建包含特定数量磁盘的新聚合、将磁盘添加到现有聚合以及在特定聚合中创建卷。

容量管理

组织或帐户管理员可以配置控制台来通知您存储容量决策或是否自动为您管理容量需求。

此行为由控制台代理上的_容量管理模式_决定。容量管理模式会影响该控制台代理管理的所有Cloud Volumes ONTAP系统。如果您有另一个控制台代理，则可以进行不同的配置。

自动容量管理

容量管理模式默认设置为自动。在此模式下，控制台每 15 分钟检查一次可用空间比率，以确定可用空间比率是否低于指定的阈值。如果需要更多容量，它会启动购买新磁盘、删除未使用的磁盘集合（聚合）、根据需要在聚合之间移动卷，并尝试防止磁盘故障。

以下示例说明了此模式的工作原理：

- 如果聚合达到容量阈值并且有空间容纳更多磁盘，则控制台会自动为该聚合购买新磁盘，以便卷可以继续增长。

对于支持弹性卷的 AWS 中的聚合，它还会增加 RAID 组中磁盘的大小。"了解有关弹性卷支持的更多信息" 。

+ * 如果聚合达到容量阈值并且无法支持任何额外的磁盘，则控制台会自动将卷从该聚合移动到具有可用容量的聚合或新的聚合。

+ 如果控制台为卷创建新的聚合，它会选择适合该卷大小的磁盘大小。

+ 请注意，原始聚合上现在有可用空间。现有卷或新卷可以使用该空间。在这种情况下，空间无法返回给云提供商。

- 如果聚合中超过 12 小时没有卷，控制台就会将其删除。

使用自动容量管理来管理 **LUN**

控制台的自动容量管理不适用于 LUN。当它创建 LUN 时，它会禁用自动增长功能。

手动容量管理

如果组织或帐户管理员将*容量管理模式*设置为手动，控制台会通知您采取适当的容量决策措施。自动模式中描述的相同示例也适用于手动模式，但是否接受操作取决于您。

了解更多

"了解如何修改容量管理模式" 。

写入速度

NetApp Console使您能够为大多数Cloud Volumes ONTAP配置选择正常或高写入速度。在选择写入速度之前，您应该了解正常设置和高设置之间的差异以及使用高写入速度时的风险和建议。

正常写入速度

当您选择正常写入速度时，数据将直接写入磁盘。当数据直接写入磁盘时，可以降低发生意外系统中断或涉及意外系统中断的级联故障（仅限 HA 对）时数据丢失的可能性。

正常写入速度是默认选项。

高写入速度

当您选择高写入速度时，数据会在写入磁盘之前缓冲在内存中，从而提供更快的写入性能。由于这种缓存，如果发生意外的系统中断，则可能会丢失数据。

发生意外系统中断时可能丢失的数据量是最后两个一致点的跨度。一致点是将缓冲数据写入磁盘的行为。当写入日志已满或 10 秒后（以先到者为准）就会出现一致点。但是，云提供商提供的存储性能可能会影响一致点处理时间。

何时使用高写入速度

如果您的工作负载需要快速写入性能，并且您可以承受意外系统中断或涉及意外系统中断的级联故障（仅限 HA 对）时数据丢失的风险，那么高写入速度是一个不错的选择。

使用高写入速度时的建议

如果启用高写入速度，则应确保应用程序层的写保护，或者确保应用程序能够容忍数据丢失（如果发生）。

AWS 中的 HA 对具有高写入速度

如果您计划在 AWS 中的 HA 对上启用高写入速度，则应该了解多可用区 (AZ) 部署和单可用区部署之间的保护级别差异。跨多个可用区部署 HA 对可提供更高的弹性，并有助于降低数据丢失的可能性。

"了解有关 AWS 中的 HA 对的更多信息" 。

支持高写入速度的配置

并非所有Cloud Volumes ONTAP配置都支持高写入速度。这些配置默认使用正常的写入速度。

AWS

如果使用单节点系统，则 Cloud Volumes ONTAP 支持所有实例类型的高写入速度。

从 9.8 版本开始， Cloud Volumes ONTAP在使用几乎所有受支持的 EC2 实例类型（m5.xlarge 和 r5.xlarge 除外）时都支持具有 HA 对的高写入速度。

"了解有关Cloud Volumes ONTAP支持的 Amazon EC2 实例的更多信息" 。

Azure

如果使用单节点系统，则 Cloud Volumes ONTAP 支持所有虚拟机类型的高写入速度。

如果您使用 HA 对，从 9.8 版本开始， Cloud Volumes ONTAP支持多种 VM 类型的高写入速度。前往 "Cloud Volumes ONTAP发行说明"查看支持高写入速度的虚拟机类型。

Google Cloud

如果使用单节点系统，则 Cloud Volumes ONTAP 支持所有机器类型的高写入速度。

如果您使用 HA 对，从 9.13.0 版本开始， Cloud Volumes ONTAP支持多种 VM 类型的高写入速度。前往 "Cloud Volumes ONTAP发行说明"查看支持高写入速度的虚拟机类型。

"详细了解Cloud Volumes ONTAP支持的 Google Cloud 机器类型" 。

如何选择写入速度

您可以在添加新的Cloud Volumes ONTAP系统时选择写入速度，并且可以"更改现有系统的写入速度"。

如果发生数据丢失会发生什么

如果由于写入速度过快而导致数据丢失，事件管理系统 (EMS) 会报告以下两个事件：

- Cloud Volumes ONTAP 9.12.1 或更高版本

```
 NOTICE nv.data.loss.possible: An unexpected shutdown occurred while in
high write speed mode, which possibly caused a loss of data.
* Cloud Volumes ONTAP 9.11.0 至 9.11.1
```

```
DEBUG nv.check.failed: NVRAM check failed with error "NVRAM disabled due
to dirty shutdown with High Write Speed mode"
```

```
 ERROR wafl.root.content.changed: Contents of the root volume '' might
have changed. Verify that all recent configuration changes are still in
effect..
* Cloud Volumes ONTAP 9.8 至 9.10.1
```

```
DEBUG nv.check.failed: NVRAM check failed with error "NVRAM disabled due
to dirty shutdown"
```

```
ERROR wafl.root.content.changed: Contents of the root volume '' might
have changed. Verify that all recent configuration changes are still in
effect.
```

当这种情况发生时， Cloud Volumes ONTAP应该能够启动并继续提供数据，而无需用户干预。

如果发生数据丢失，如何停止数据访问

如果您担心数据丢失，希望应用程序在数据丢失时停止运行，并在正确解决数据丢失问题后恢复数据访问，则可以使用 CLI 中的 NVFAIL 选项来实现该目标。

启用 **NVFAIL** 选项

```
vol modify -volume <vol-name> -nvfail on
```

检查 **NVFAIL** 设置

```
vol show -volume <vol-name> -fields nvfail
```

禁用 **NVFAIL** 选项

```
vol modify -volume <vol-name> -nvfail off
```

当发生数据丢失时，启用 NVFAIL 的 NFS 或 iSCSI 卷应停止提供数据（这对无状态协议 CIFS 没有影响）。有关详细信息，请参阅 "NVFAIL 如何影响对 NFS 卷或 LUN 的访问"。

检查 **NVFAIL** 状态

```
vol show -fields in-nvfailed-state
```

正确解决数据丢失问题后，您可以清除 NVFAIL 状态，然后卷将可供数据访问。

清除 **NVFAIL** 状态

```
vol modify -volume <vol-name> -in-nvfailed-state false
```

Flash Cache

一些Cloud Volumes ONTAP配置包括本地 NVMe 存储， Cloud Volumes ONTAP将其用作_Flash Cache_ 以获得更好的性能。

什么是闪存?

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

支持的配置

特定的Cloud Volumes ONTAP配置支持 Flash Cache。查看支持的配置 "Cloud Volumes ONTAP发行说明"

限制

- 在 AWS 中为Cloud Volumes ONTAP 9.12.0 或更早版本配置 Flash Cache 时，必须在所有卷上禁用压缩才能利用 Flash Cache 性能改进。当您部署或升级到Cloud Volumes ONTAP 9.12.1 或更高版本时，您无需禁用压缩。

  从NetApp Console创建卷时跳过选择存储效率设置，或者创建卷然后 "使用 CLI 禁用数据压缩"。

- Cloud Volumes ONTAP不支持重新启动后缓存重新预热。

相关主题

- "AWS 中Cloud Volumes ONTAP支持的配置"
- "Azure 中Cloud Volumes ONTAP支持的配置"
- "Google Cloud 中 Cloud Volumes ONTAP 支持的配置"

了解**Cloud Volumes ONTAP**上的 **WORM** 存储

您可以在Cloud Volumes ONTAP系统上激活一次写入、多次读取 (WORM) 存储，以便在指定的保留期内以未修改的形式保留文件。云 WORM 存储由SnapLock技术提供支持，这意味着 WORM 文件在文件级别受到保护。

WORM 功能可与自带许可证 (BYOL) 一起使用，并且无需额外付费即可在市场订阅您的许可证。请联系您的NetApp销售代表，将 WORM 添加到您当前的许可证中。

WORM存储的工作原理

一旦文件被提交到 WORM 存储，即使保留期已过，也无法修改。防篡改时钟确定 WORM 文件的保留期何时结束。

保留期过后，您有责任删除不再需要的任何文件。

激活 **WORM** 存储

如何激活 WORM 存储取决于您使用的Cloud Volumes ONTAP版本。

版本 **9.10.1** 及更高版本

从Cloud Volumes ONTAP 9.10.1 开始，您可以选择在卷级别启用或禁用 WORM。

添加Cloud Volumes ONTAP系统时，系统会提示您启用或禁用 WORM 存储：

- 如果在添加系统时启用 WORM 存储，则从NetApp Console创建的每个卷都将启用 WORM。但是您可以使用ONTAP系统管理器或ONTAP CLI 来创建已禁用 WORM 的卷。
- 如果在添加系统时禁用 WORM 存储，则从控制台、 ONTAP系统管理器或ONTAP CLI 创建的每个卷都将被禁用 WORM。

版本 **9.10.0** 及更早版本

添加新系统时，您可以在Cloud Volumes ONTAP系统上激活 WORM 存储。您从控制台创建的每个卷都启用了 WORM。您无法禁用单个卷上的 WORM 存储。

将文件提交至 **WORM**

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

在Cloud Volumes ONTAP系统上激活 WORM 存储后，您必须使用ONTAP CLI 进行所有 WORM 存储的管理。有关说明，请参阅 "有关SnapLock的ONTAP文档"。

在**Cloud Volumes ONTAP**系统上启用 **WORM**

您可以在控制台上创建Cloud Volumes ONTAP系统时启用 WORM 存储。如果在创建系统时未启用 WORM，您也可以在系统上启用 WORM。启用后，您将无法禁用 WORM。

关于此任务

- ONTAP 9.10.1 及更高版本支持 WORM。
- ONTAP 9.11.1 及更高版本支持带有备份的 WORM。

步骤

1. 在“系统”页面上，双击要启用 WORM 的系统的名称。
2. 在“概述”选项卡上，单击“功能”面板，然后单击“**WORM**”旁边的铅笔图标。

   如果系统上已启用 WORM，则铅笔图标将被禁用。

3. 在*WORM*页面上，设置集群合规时钟的保留期限。

   欲了解更多信息，请参阅 "ONTAP文档：初始化合规时钟"。

4. 单击“设置”。

完成后

您可以在“功能”面板上验证 **WORM** 的状态。启用 WORM 后， SnapLock许可证会自动安装在集群上。您可以在ONTAP系统管理器上查看SnapLock许可证。

删除 **WORM** 文件

您可以使用特权删除功能删除保留期内的 WORM 文件。

有关说明，请参阅 "ONTAP 文档"。

WORM 和数据分层

创建新的Cloud Volumes ONTAP 9.8 系统或更高版本时，您可以同时启用数据分层和 WORM 存储。使用 WORM 存储启用数据分层允许您将数据分层到云中的对象存储。

您应该了解有关启用数据分层和 WORM 存储的以下内容：

- 分层到对象存储的数据不包含ONTAP WORM 功能。为了确保端到端 WORM 功能，您需要正确设置存储桶权限。
- 分层到对象存储的数据不具备 WORM 功能，这意味着从技术上讲，任何拥有存储桶和容器完全访问权限的人都可以删除由ONTAP分层的对象。

- 启用 WORM 和分层后，恢复或降级到Cloud Volumes ONTAP 9.8 的操作将被阻止。

限制

- Cloud Volumes ONTAP中的 WORM 存储在“可信存储管理员”模型下运行。虽然 WORM 文件受到保护以防止更改或修改，但即使这些卷包含未过期的 WORM 数据，集群管理员也可以删除这些卷。
- 除了可信存储管理员模型之外， Cloud Volumes ONTAP中的 WORM 存储也隐式地在“可信云管理员”模型下运行。云管理员可以通过直接从云提供商处删除或编辑云存储来在 WORM 数据到期之前将其删除。

相关链接

- "为 WORM 存储创建防篡改 Snapshot 副本"
- "Cloud Volumes ONTAP中的许可和计费"

高可用性对

了解 **AWS** 中的**Cloud Volumes ONTAP HA** 对

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

HA 组件

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

- 两个Cloud Volumes ONTAP节点，其数据彼此同步镜像。
- 中介实例在节点之间提供通信通道，以协助存储接管和交还过程。

调解器

以下是有关 AWS 中中介实例的一些关键细节：

实例类型
: t3-micro

磁盘
: 两个 8 GiB 和 4 GiB 的 st1 磁盘

操作系统
: Debian 11

> 对于Cloud Volumes ONTAP 9.10.0 及更早版本，调解器上安装了 Debian 10。

升级
: 升级Cloud Volumes ONTAP时， NetApp Console还会根据需要更新中介实例。

访问实例

当您从控制台创建Cloud Volumes ONTAP HA 对时，系统会提示您为中介实例提供密钥对。您可以使用该密钥对进行 SSH 访问 `admin`用户。

第三方代理

中介实例不支持第三方代理或 VM 扩展。

存储接管和交还

如果一个节点发生故障，另一个节点可以为其伙伴提供数据以提供持续的数据服务。客户端可以从伙伴节点访问相同的数据，因为数据已同步镜像到伙伴节点。

节点重启后，伙伴必须重新同步数据才能返回存储。重新同步数据所需的时间取决于节点关闭时更改的数据量。

默认情况下，存储接管、重新同步和恢复都是自动的。无需用户操作。

RPO 和 RTO

HA 配置通过以下方式维护数据的高可用性：

- 恢复点目标 (RPO) 为 0 秒。您的数据在事务上是一致的，没有数据丢失。
- 恢复时间目标 (RTO) 为 120 秒。如果发生中断，数据应在 120 秒或更短时间内可用。

HA部署模型

您可以通过跨多个可用区 (AZ) 或在单个可用区 (AZ) 中部署 HA 配置来确保数据的高可用性。您应该查看有关每种配置的更多详细信息，以选择最适合您需求的配置。

多个可用区域

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

NFS 和 CIFS 数据访问

当 HA 配置分布在多个可用区域时，_浮动 IP 地址_可启用 NAS 客户端访问。浮动 IP 地址必须位于区域内所有 VPC 的 CIDR 块之外，当发生故障时，浮动 IP 地址可以在节点之间迁移。 VPC 之外的客户端无法原生访问它们，除非你"设置 AWS 中转网关"。

如果您无法设置传输网关，则可以为 VPC 外部的 NAS 客户端提供私有 IP 地址。但是，这些 IP 地址是静态的——它们无法在节点之间进行故障转移。

在跨多个可用区域部署 HA 配置之前，您应该查看浮动 IP 地址和路由表的要求。部署配置时必须指定浮动 IP 地址。私有 IP 地址是自动创建的。

有关详细信息，请参阅"多个可用区中Cloud Volumes ONTAP HA 的 AWS 网络要求" 。

iSCSI 数据访问

由于 iSCSI 不使用浮动 IP 地址，因此跨 VPC 数据通信不是问题。

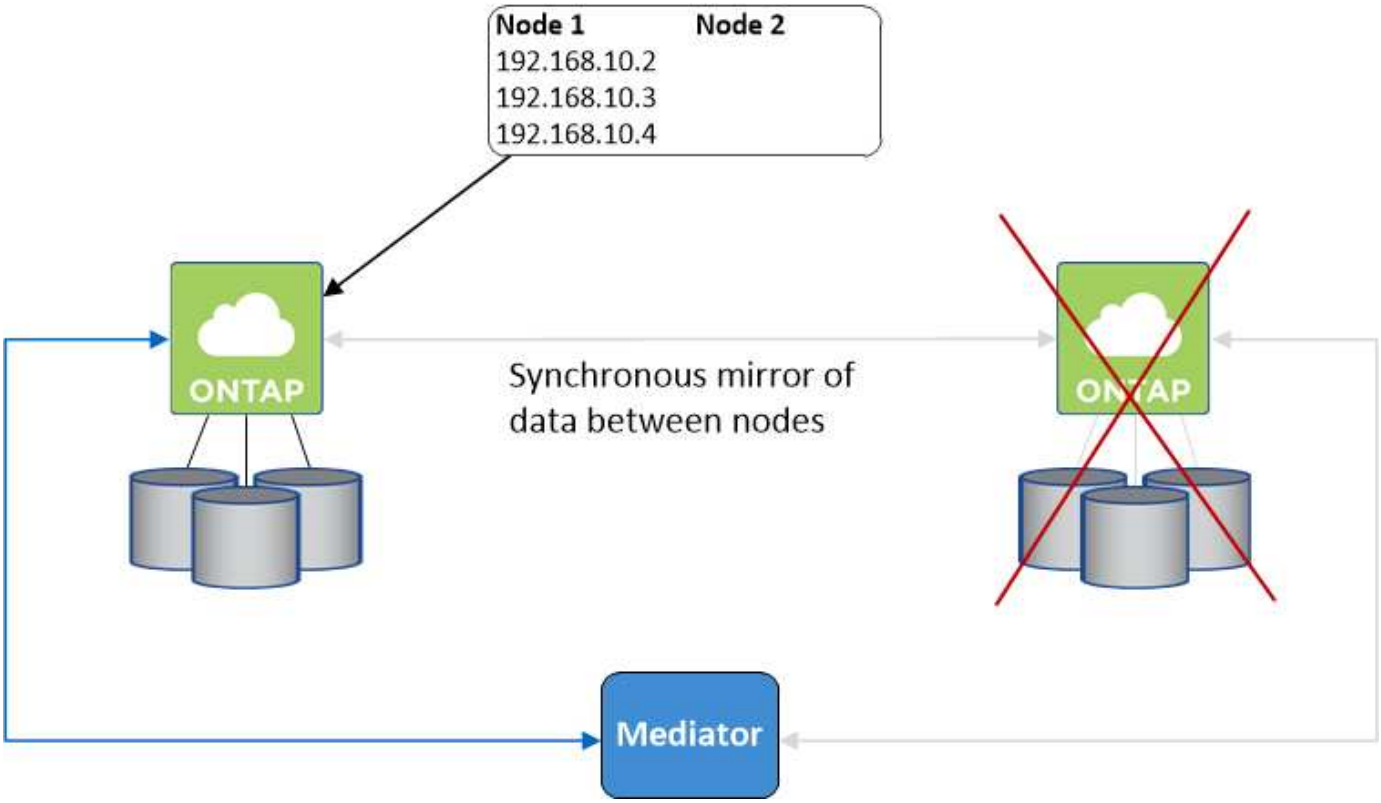
iSCSI 的接管和交还

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

有关哪些特定主机配置支持 ALUA 的信息，请参阅 "NetApp 互操作性表工具"以及 "SAN 主机和云客户端指南"适用于您的主机操作系统。

NAS 的接管和交还

当使用浮动 IP 的 NAS 配置中发生接管时，客户端用于访问数据的节点的浮动 IP 地址将移动到另一个节点。下图描述了使用浮动 IP 的 NAS 配置中的存储接管。如果节点 2 出现故障，则节点 2 的浮动 IP 地址将移动到节点 1。



用于外部 VPC 访问的 NAS 数据 IP 如果发生故障，则无法在节点之间迁移。如果某个节点离线，您必须使用另一个节点上的 IP 地址手动将卷重新挂载到 VPC 外部的客户端。

故障节点恢复在线后，使用原始 IP 地址将客户端重新挂载到卷。需要执行此步骤以避免在两个 HA 节点之间传输不必要的数据，这会对性能和稳定性造成严重影响。

您可以通过选择卷并单击“安装命令”从控制台找到正确的 IP 地址。

单个可用区域

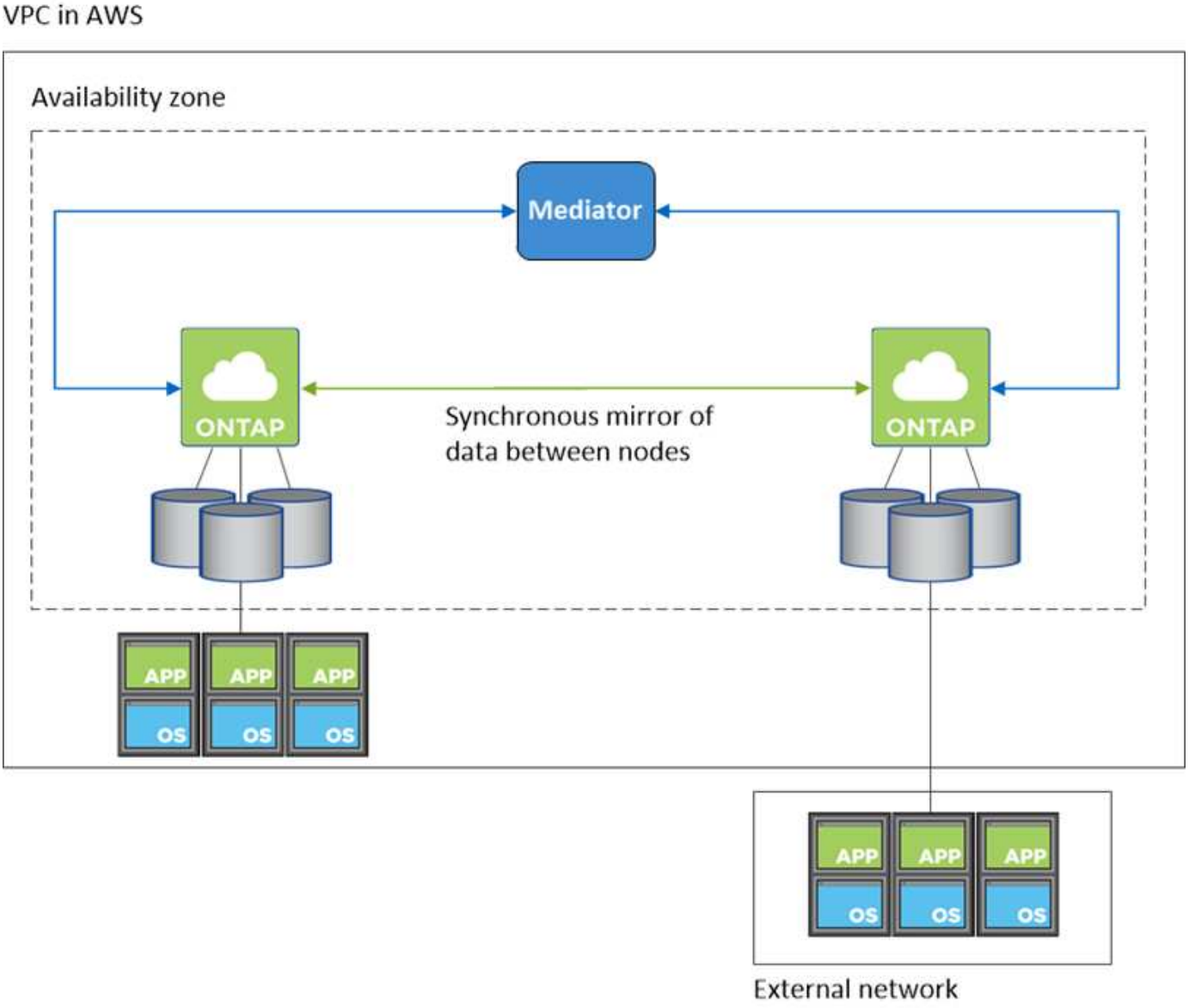
如果运行Cloud Volumes ONTAP节点的实例发生故障，在单个可用区 (AZ) 中部署 HA 配置可以确保数据的高可用性。所有数据都可以从 VPC 外部本地访问。

控制台创建一个 "AWS 文档：AWS 分散置放群组"并启动该放置组中的两个 HA 节点。放置组通过将实例分布在不同的底层硬件上来降低同时发生故障的风险。此功能从计算角度而不是从磁盘故障角度提高了冗余度。

数据访问

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

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



接管和交还

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

有关哪些特定主机配置支持 ALUA 的信息，请参阅 "NetApp 互操作性表工具"以及 "SAN 主机和云客户端指南"适用于您的主机操作系统。

对于 NAS 配置，如果发生故障，数据 IP 地址可以在 HA 节点之间迁移。这确保了客户端可以访问存储。

AWS 本地区域

AWS 本地区域是一种基础设施部署，其中存储、计算、数据库和其他精选 AWS 服务位于大城市和工业区附近。借助 AWS 本地区域，您可以让 AWS 服务更接近您，从而改善工作负载的延迟并在本地维护数据库。在Cloud Volumes ONTAP，

您可以在 AWS 本地区域中部署单个 AZ 或多个 AZ 配置。

在标准和私有模式下使用控制台时支持 AWS 本地区域。目前，AWS 本地区域不支持受限模式。

AWS 本地区域配置示例

AWS 中的Cloud Volumes ONTAP仅支持单个可用区域中的高可用性 (HA) 模式。不支持单节点部署。

Cloud Volumes ONTAP不支持 AWS 本地区域中的数据分层、云分层和不合格实例。

以下是示例配置：

- 单一可用区域：集群节点和中介器均位于同一本地区域中。
- 多可用区 在多可用区配置中，有三个实例、两个节点和一个中介器。三个实例中必须有一个实例位于单独的区域中。您可以选择如何设置。

  以下是三个示例配置：

  - 每个集群节点位于不同的本地区域，中介位于公共可用区域。
  - 一个集群节点位于本地区域中，调解器位于本地区域中，第二个集群节点位于可用区域中。
  - 每个集群节点和中介器位于单独的本地区域中。

支持的磁盘和实例类型

唯一支持的磁盘类型是 GP2。目前支持以下大小从 xlarge 到 4xlarge 的 EC2 实例类型系列：

- M5
- C5
- C5d
- R5
- R5d

Cloud Volumes ONTAP 仅支持这些配置。在 AWS Local Zone 配置中选择不受支持的磁盘类型或不合格的实例可能会导致部署失败。如果您的 Cloud Volumes ONTAP 系统位于 AWS Local Zone 中，则不支持将数据分层到 Amazon Simple Storage Service (Amazon S3)，因为在 Local Zone 之外访问 Amazon S3 存储桶涉及更高的延迟并影响 Cloud Volumes ONTAP 活动。

"AWS 文档：本地区域中的 EC2 实例类型" 。

HA 对中的存储工作原理

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

存储分配

当您创建新卷并且需要额外的磁盘时，控制台会为两个节点分配相同数量的磁盘，创建镜像聚合，然后创建新卷。例如，如果卷需要两个磁盘，则控制台会为每个节点分配两个磁盘，总共四个磁盘。

存储配置

您可以将 HA 对用作主动-主动配置，其中两个节点都向客户端提供数据，或者用作主动-被动配置，其中被动节点仅在接管主动节点的存储后才会响应数据请求。

仅当使用存储系统视图中的控制台时，您才可以设置主动-主动配置。

绩效预期

Cloud Volumes ONTAP HA 配置在节点之间同步复制数据，这会消耗网络带宽。因此，与单节点Cloud Volumes ONTAP配置相比，您可以获得以下性能：

- 对于仅从一个节点提供数据的 HA 配置，读取性能与单节点配置的读取性能相当，而写入性能较低。
- 对于从两个节点提供数据的 HA 配置，读取性能高于单节点配置的读取性能，写入性能相同或更高。

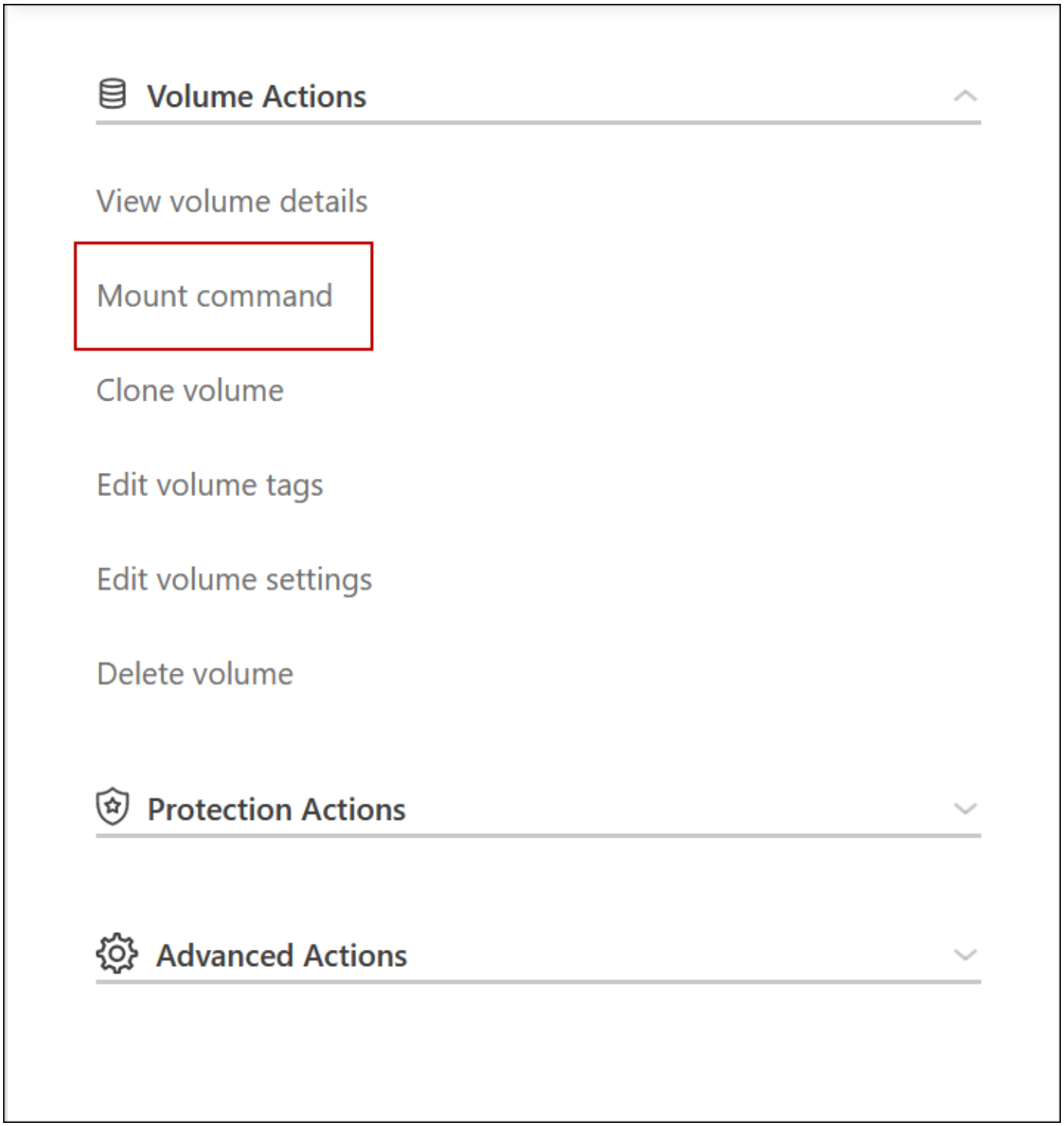
有关Cloud Volumes ONTAP性能的更多详细信息，请参阅"性能"。

客户端访问存储

客户端应使用卷所在节点的数据 IP 地址访问 NFS 和 CIFS 卷。如果 NAS 客户端使用伙伴节点的 IP 地址访问卷，则流量会在两个节点之间流动，从而降低性能。

如果在 HA 对中的节点之间移动卷，则应使用另一个节点的 IP 地址重新挂载该卷。否则，您可能会遇到性能下降的情况。如果客户端支持 NFSv4 引用或 CIFS 文件夹重定向，您可以在Cloud Volumes ONTAP系统上启用这些功能以避免重新挂载卷。有关详细信息，请参阅ONTAP文档。

您可以通过管理卷面板下的_Mount Command_选项轻松识别正确的IP地址。

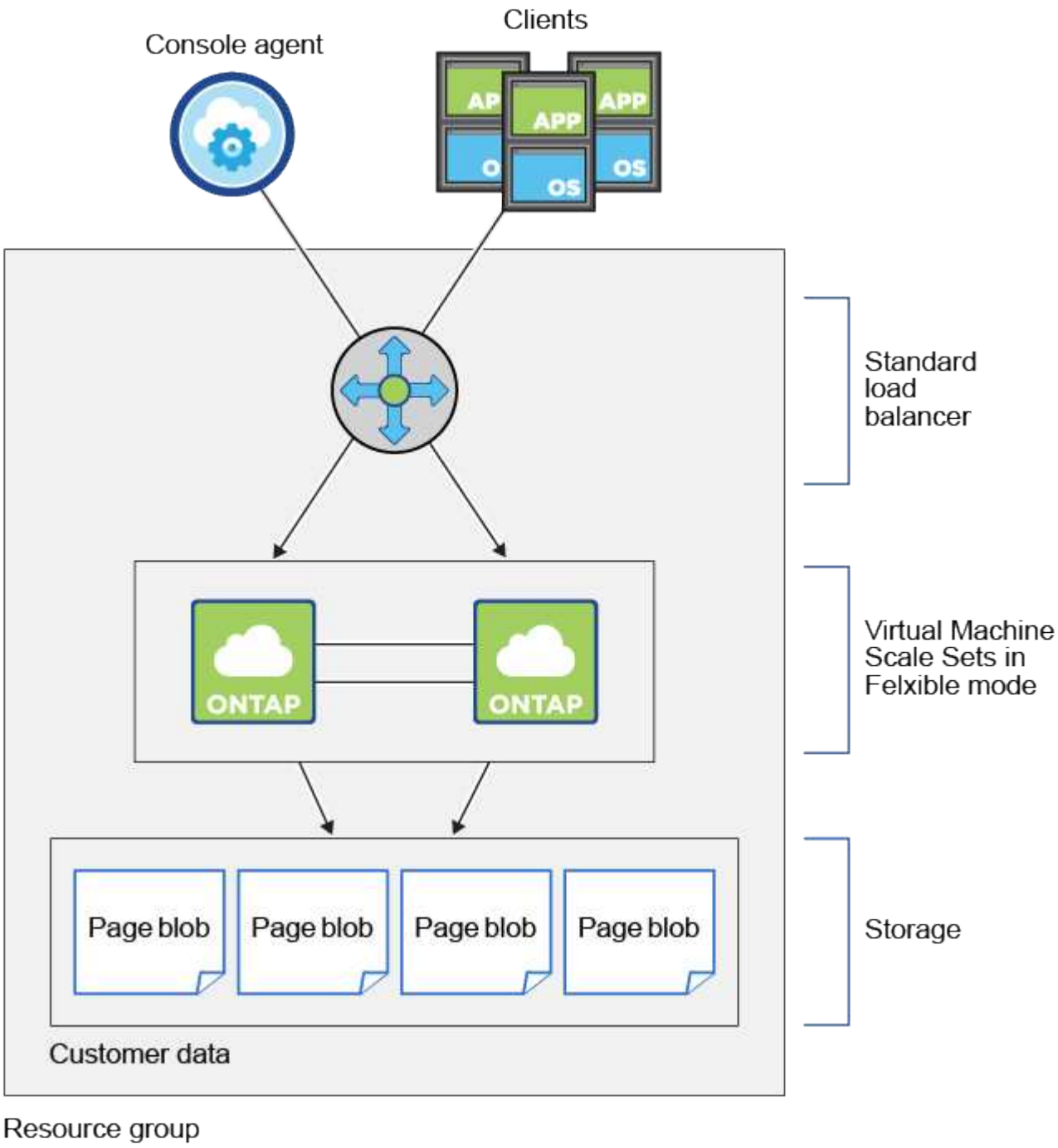


了解 **Azure** 中的**Cloud Volumes ONTAP HA** 对

Cloud Volumes ONTAP高可用性 (HA) 对可在您的云环境出现故障时提供企业可靠性和持续运行。在 Azure 中，存储在两个节点之间共享。

HA 组件

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



请注意有关NetApp Console为您部署的 Azure 组件的以下事项：

Azure 标准负载均衡器

负载均衡器管理传入Cloud Volumes ONTAP HA 对的流量。

单个可用区域中的虚拟机

从Cloud Volumes ONTAP 9.15.1 开始，您可以在单个可用区 (AZ) 中创建和管理异构虚拟机 (VM)。您可以在同一可用区内的不同故障域中部署高可用性 (HA) 节点，以确保最佳可用性。要了解有关实现此功能的灵活编

排模式的更多信息，请参阅 "Microsoft Azure 文档：虚拟机规模集"。

磁盘

客户数据驻留在高级存储页面 blob 上。每个节点都可以访问其他节点的存储。还需要额外的存储空间"引导、根和核心数据"。

存储帐户

- 托管磁盘需要一个存储帐户。
- 由于已达到每个存储帐户的磁盘容量限制，因此高级存储页面 Blob 需要一个或多个存储帐户。

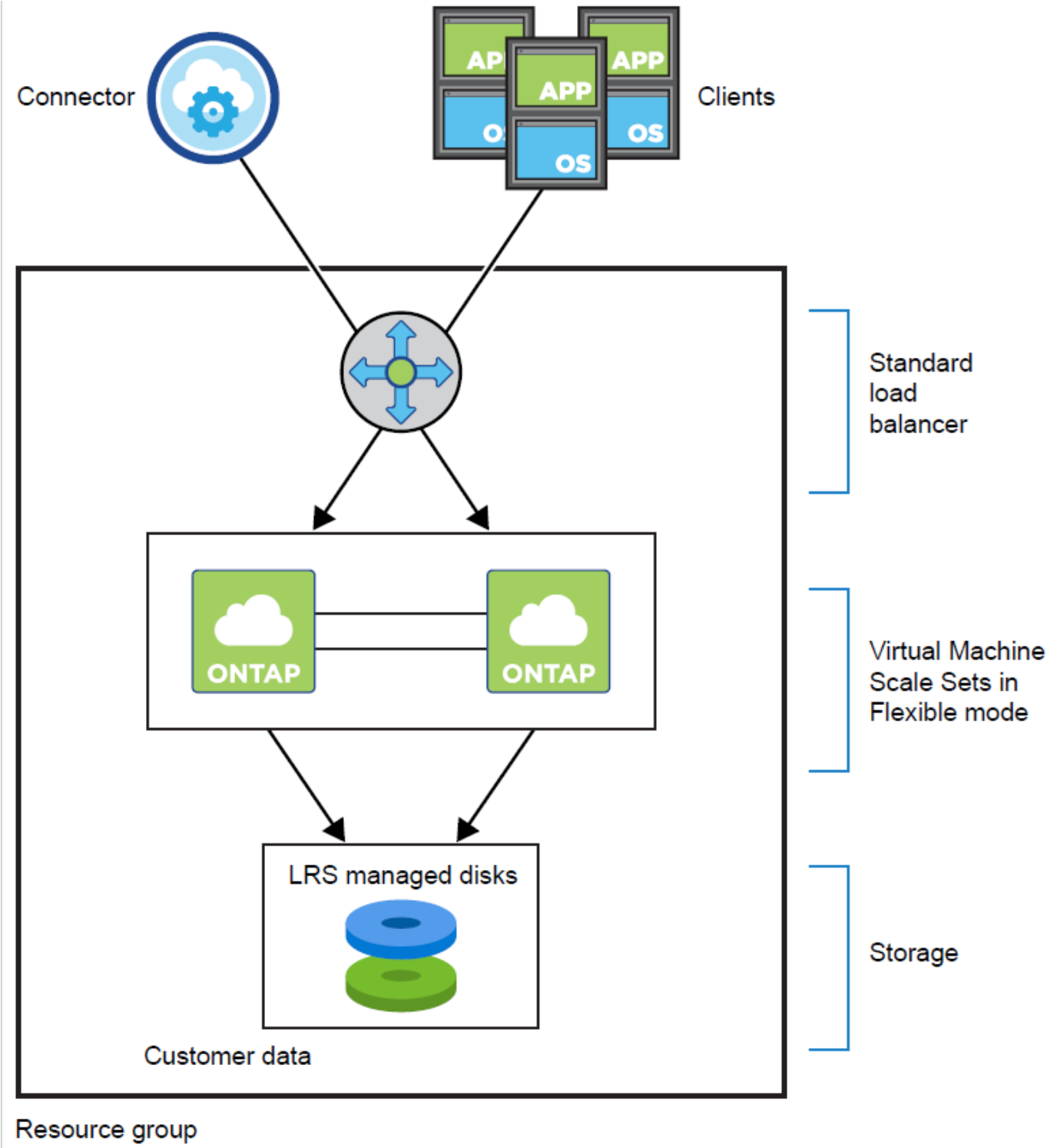
  "Microsoft Azure 文档：Azure 存储可扩展性和存储帐户的性能目标" 。

- 将数据分层到 Azure Blob 存储需要一个存储帐户。
- 从Cloud Volumes ONTAP 9.7 开始，控制台为 HA 对创建的存储帐户是通用 v2 存储帐户。
- 添加Cloud Volumes ONTAP系统时，您可以启用从Cloud Volumes ONTAP 9.7 HA 对到 Azure 存储帐户的 HTTPS 连接。请注意，启用此选项可能会影响写入性能。创建系统后，您无法更改设置。

从Cloud Volumes ONTAP 9.15.0P1 开始，Azure 页面 blob 不再支持新的高可用性对部署。如果您当前在现有的高可用性对部署中使用 Azure 页 Blob，则可以迁移到 Edsv4 系列 VM 和 Edsv5 系列 VM 中较新的 VM 实例类型。"详细了解 Azure 中支持的配置" 。

具有共享托管磁盘的 **HA** 单可用区域配置

在共享托管磁盘上运行的Cloud Volumes ONTAP HA 单可用区配置包括以下组件：



请注意有关控制台为您部署的 Azure 组件的以下事项：

Azure 标准负载均衡器

负载均衡器管理传入Cloud Volumes ONTAP HA 对的流量。

单个可用区域中的虚拟机

从Cloud Volumes ONTAP 9.15.1 开始，您可以在单个可用区 (AZ) 中创建和管理异构虚拟机 (VM)。您可以在同一可用区内的不同故障域中部署高可用性 (HA) 节点，以确保最佳可用性。要了解有关实现此功能的灵活编排模式的更多信息，请参阅 "Microsoft Azure 文档：虚拟机规模集"。

当满足以下条件时，区域部署将使用高级 SSD v2 托管磁盘：

- Cloud Volumes ONTAP的版本为 9.15.1 或更高版本。
- 所选区域和区域支持高级 SSD v2 托管磁盘。有关受支持区域的信息，请参阅 "Microsoft Azure 网站：按地区提供的产品"。
- 订阅已注册为 Microsoft"Microsoft.Compute/VMOrchestratorZonalMultiFD 功能" 。

> 如果您为符合上述条件的环境选择高级 SSD 管理磁盘，控制台将自动部署高级 SSD v2 管理磁盘。您无法切换到高级 SSD v1 管理磁盘。

磁盘

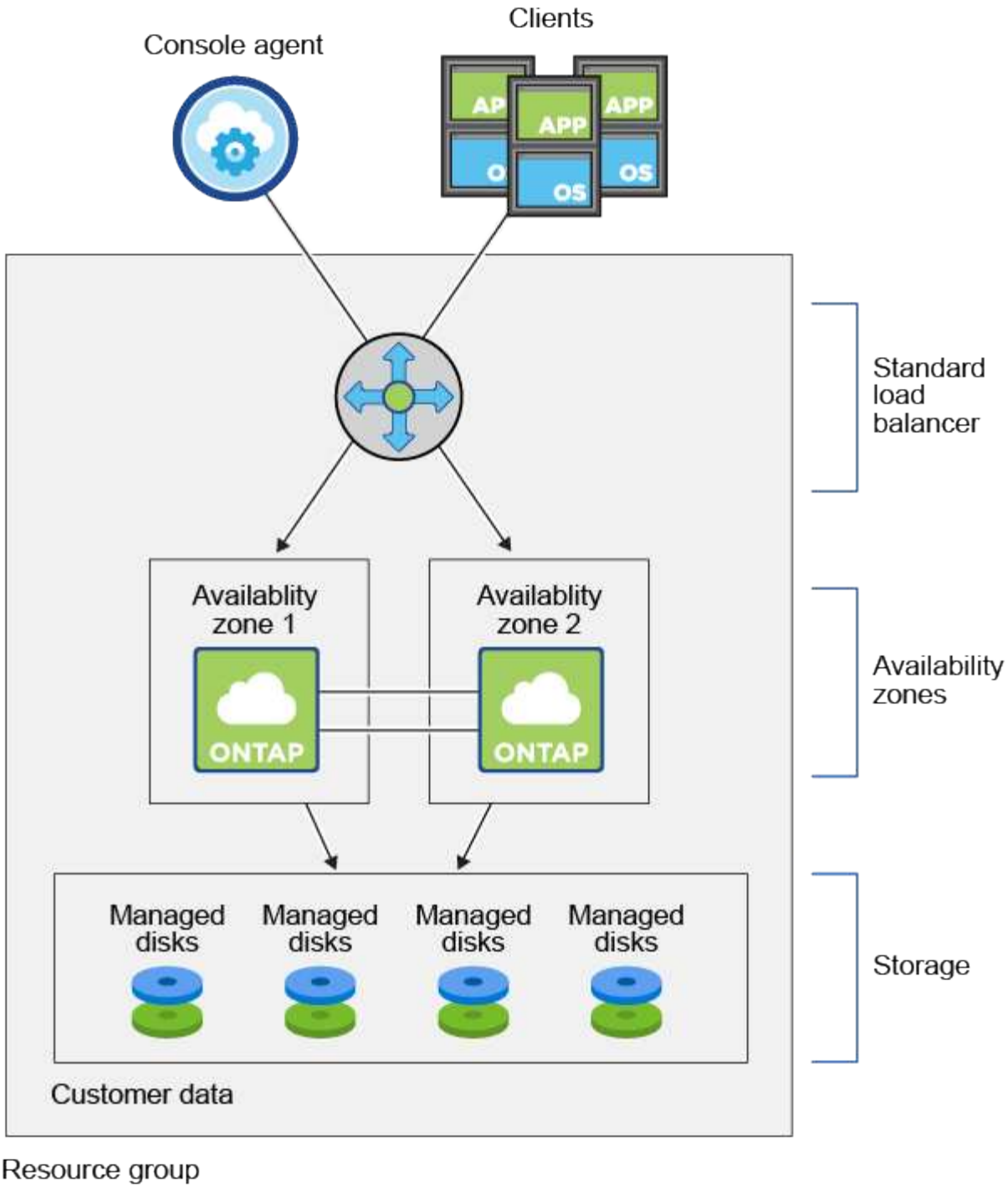
客户数据驻留在本地冗余存储 (LRS) 管理的磁盘上。每个节点都可以访问其他节点的存储。还需要额外的存储空间"启动、根、合作伙伴根、核心和NVRAM数据"。

存储帐户

存储帐户用于基于托管磁盘的部署，以处理诊断日志和分层到 Blob 存储。

HA 多可用区配置

Azure 中的Cloud Volumes ONTAP HA 多可用区域配置包括以下组件：



请注意有关控制台为您部署的 Azure 组件的以下事项：

Azure 标准负载均衡器

负载均衡器管理传入Cloud Volumes ONTAP HA 对的流量。

可用区域

HA 多可用区配置采用一种部署模型，其中两个Cloud Volumes ONTAP节点部署到不同的可用区，确保节点位于不同的故障域中以提供冗余和可用性。要了解灵活编排模式下的虚拟机规模集如何使用 Azure 中的可用性区域，请参阅 "Microsoft Azure 文档：创建使用可用性区域的虚拟机规模集"。

磁盘

客户数据驻留在区域冗余存储 (ZRS) 托管磁盘上。每个节点都可以访问其他节点的存储。还需要额外的存储空间"启动、根、合作伙伴根和核心数据"。

存储帐户

存储帐户用于基于托管磁盘的部署，以处理诊断日志和分层到 Blob 存储。

RPO 和 RTO

HA 配置可按照以下方式维护数据的高可用性：

- 恢复点目标 (RPO) 为 0 秒。您的数据在事务上是一致的，没有数据丢失。
- 恢复时间目标 (RTO) 为 120 秒。如果发生中断，数据应在 120 秒或更短时间内可用。

存储接管和交还

与物理ONTAP集群类似，Azure HA 对中的存储在节点之间共享。与合作伙伴存储的连接允许每个节点在发生_接管_时访问其他节点的存储。网络路径故障转移机制确保客户端和主机继续与幸存节点通信。当节点重新上线时，合作伙伴将归还存储。

对于 NAS 配置，如果发生故障，数据 IP 地址会在 HA 节点之间自动迁移。

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

> 有关哪些特定主机配置支持 ALUA 的信息，请参阅 "NetApp 互操作性表工具"以及 "SAN 主机和云客户端指南"适用于您的主机操作系统。

默认情况下，存储接管、重新同步和恢复都是自动的。无需用户操作。

存储配置

您可以将 HA 对用作主动-主动配置，其中两个节点都向客户端提供数据，或者用作主动-被动配置，其中被动节点仅在接管主动节点的存储后才会响应数据请求。

了解 Google Cloud 中的Cloud Volumes ONTAP HA 对

Cloud Volumes ONTAP高可用性 (HA) 配置提供无中断操作和容错功能。在 Google Cloud 中，数据在两个节点之间同步镜像。

HA 组件

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

- 两个Cloud Volumes ONTAP节点，其数据彼此同步镜像。
- 中介实例在节点之间提供通信通道，以协助存储接管和交还过程。
- 一个区域或三个区域（推荐）。

  如果您选择三个区域，则两个节点和中介器位于单独的 Google Cloud 区域。

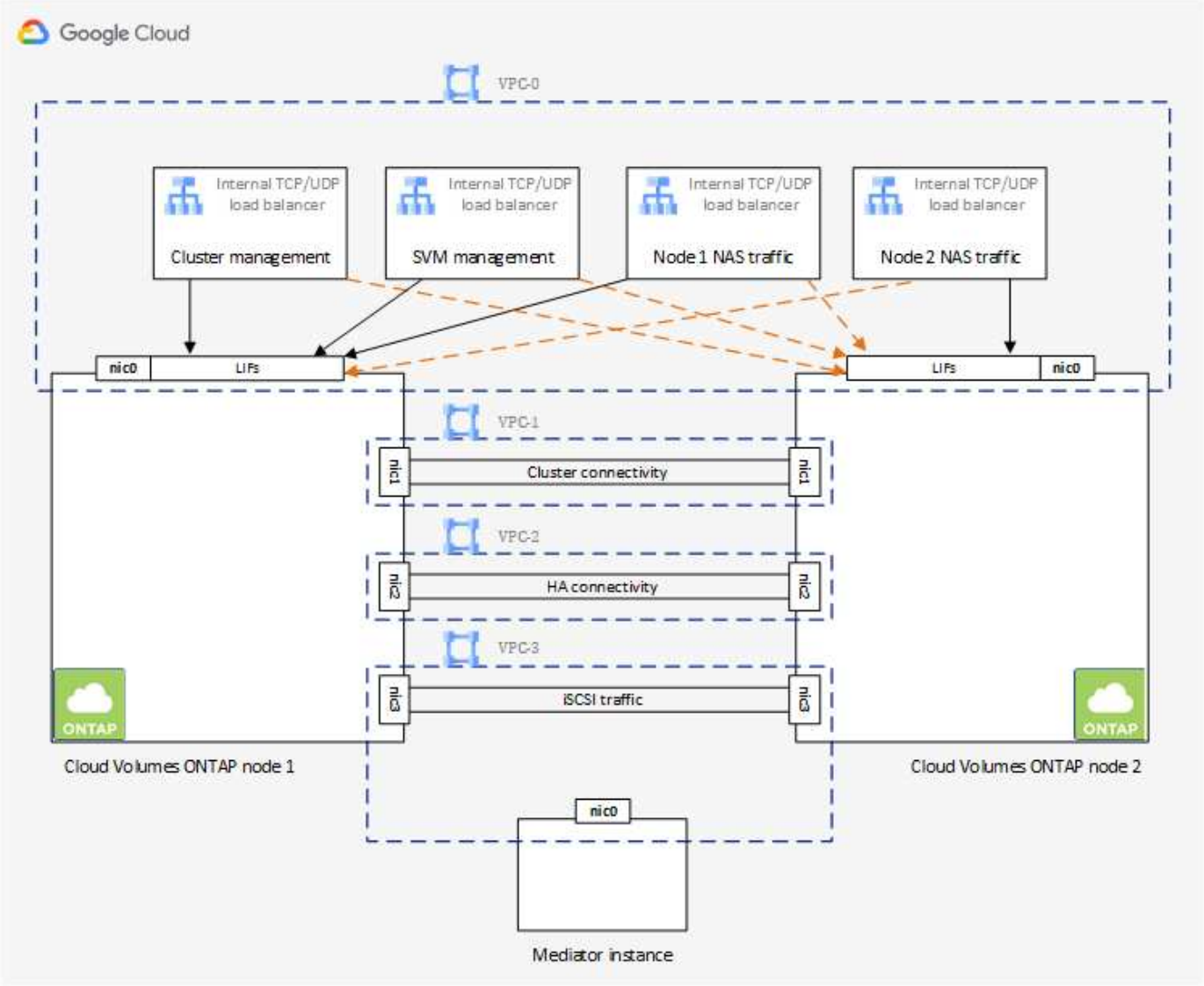
- 四个虚拟私有云（VPC）。

  该配置使用四个 VPC，因为 GCP 要求每个网络接口位于单独的 VPC 网络中。

- 四个 Google Cloud 内部负载均衡器（TCP/UDP），用于管理传入Cloud Volumes ONTAP HA 对的流量。

"了解网络要求"，包括有关负载均衡器、VPC、内部 IP 地址、子网等的更多详细信息。

以下概念图展示了Cloud Volumes ONTAP HA 对及其组件：



调解器

以下是有关 Google Cloud 中中介实例的一些关键细节：

实例类型

e2-micro（之前使用过 f1-micro 实例）

磁盘

两个标准永久性磁盘，每个磁盘 10 GiB

操作系统

Debian 11

对于Cloud Volumes ONTAP 9.10.0 及更早版本，调解器上安装了 Debian 10。

升级

升级Cloud Volumes ONTAP时， NetApp Console还会根据需要更新中介实例。

访问实例

对于 Debian，默认的云用户是 `admin`。当通过 Google Cloud Console 或 gcloud 命令行请求 SSH 访问时，Google Cloud 会为 `admin`用户创建并添加证书。您可以指定 `sudo`以获得 root 权限。

第三方代理

中介实例不支持第三方代理或 VM 扩展。

存储接管和交还

如果一个节点发生故障，另一个节点可以为其伙伴提供数据以提供持续的数据服务。客户端可以从伙伴节点访问相同的数据，因为数据已同步镜像到伙伴节点。

节点重启后，伙伴必须重新同步数据才能返回存储。重新同步数据所需的时间取决于节点关闭时更改的数据量。

默认情况下，存储接管、重新同步和恢复都是自动的。无需用户操作。

RPO 和 **RTO**

HA 配置可按照以下方式维护数据的高可用性：

- 恢复点目标 (RPO) 为 0 秒。

  您的数据在事务上是一致的，没有数据丢失。

- 恢复时间目标 (RTO) 为 120 秒。

  如果发生中断，数据应在 120 秒或更短时间内可用。

HA部署模型

您可以通过在多个区域或单个区域中部署 HA 配置来确保数据的高可用性。

多区域（推荐）

跨三个区域部署 HA 配置可确保当一个区域内发生故障时数据仍然可用。请注意，与使用单个区域相比，写入性能略低，但差别很小。

单区

在单个区域中部署时， Cloud Volumes ONTAP HA 配置使用分散放置策略。此策略可确保 HA 配置免受区域内单点故障的影响，而无需使用单独的区域来实现故障隔离。

这种部署模型确实降低了您的成本，因为区域之间没有数据流出费用。

HA 对中的存储工作原理

与ONTAP集群不同，GCP 中的Cloud Volumes ONTAP HA 对中的存储不会在节点之间共享。相反，数据在节点之间同步镜像，以便在发生故障时数据可用。

存储分配

当您创建新卷并且需要额外的磁盘时，控制台会为两个节点分配相同数量的磁盘，创建镜像聚合，然后创建新卷。例如，如果卷需要两个磁盘，则控制台会为每个节点分配两个磁盘，总共四个磁盘。

存储配置

您可以将 HA 对用作主动-主动配置，其中两个节点都向客户端提供数据，或者用作主动-被动配置，其中被动节点仅在接管主动节点的存储后才会响应数据请求。

HA 配置的性能预期

Cloud Volumes ONTAP HA 配置在节点之间同步复制数据，这会消耗网络带宽。因此，与单节点Cloud Volumes ONTAP配置相比，您可以获得以下性能：

- 对于仅从一个节点提供数据的 HA 配置，读取性能与单节点配置的读取性能相当，而写入性能较低。
- 对于从两个节点提供数据的 HA 配置，读取性能高于单节点配置的读取性能，写入性能相同或更高。

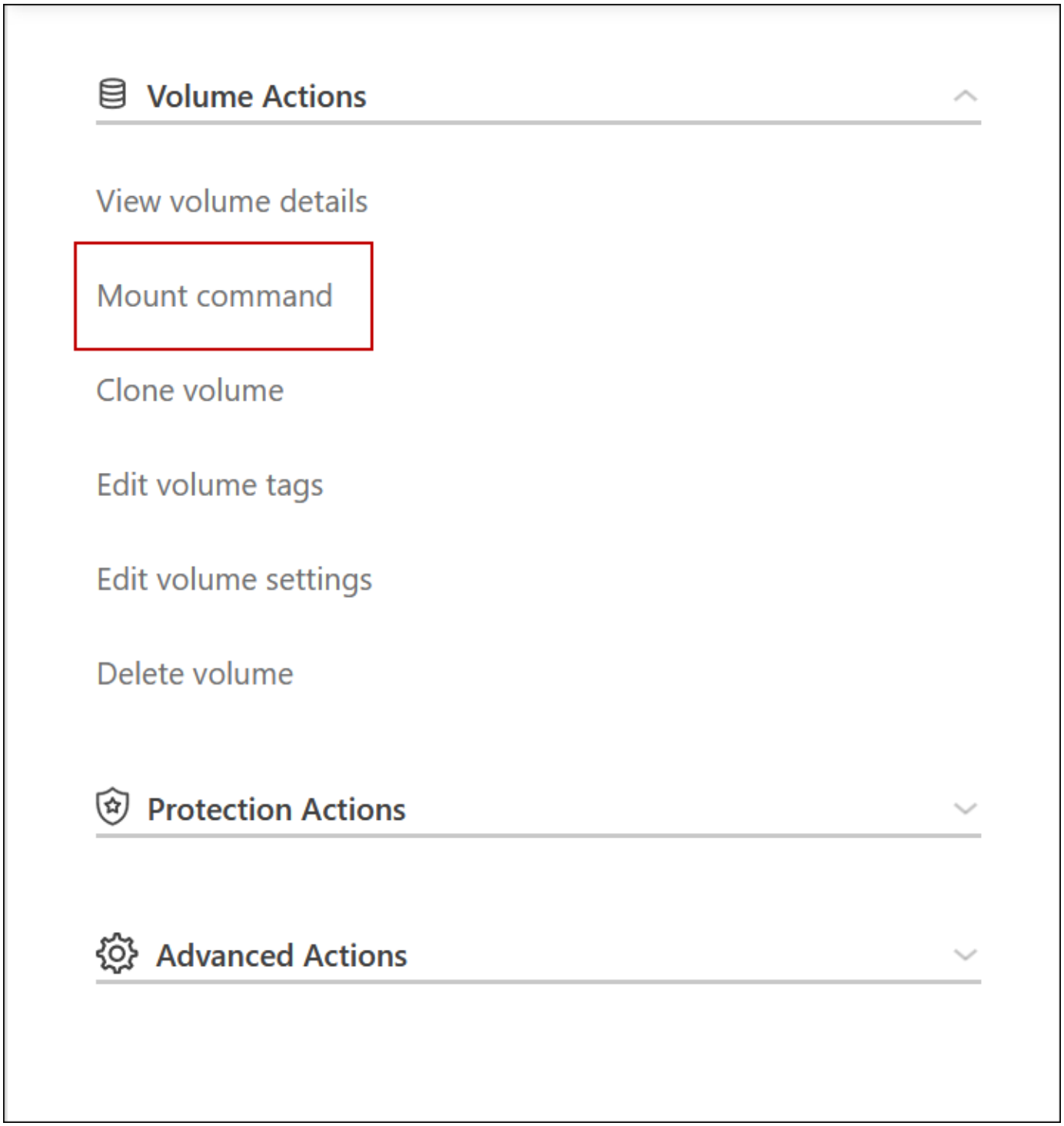
有关Cloud Volumes ONTAP性能的更多详细信息，请参阅"性能"。

客户端访问存储

客户端应使用卷所在节点的数据 IP 地址访问 NFS 和 CIFS 卷。如果 NAS 客户端使用伙伴节点的 IP 地址访问卷，则流量会在两个节点之间流动，从而降低性能。

如果在 HA 对中的节点之间移动卷，则应使用另一个节点的 IP 地址重新挂载该卷。否则，您可能会遇到性能下降的情况。如果客户端支持 NFSv4 引用或 CIFS 文件夹重定向，您可以在Cloud Volumes ONTAP系统上启用这些功能以避免重新挂载卷。有关详细信息，请参阅ONTAP文档。

您可以通过选择卷并单击“安装命令”从控制台找到正确的 IP 地址。



相关链接

- "了解网络要求"
- "了解如何开始使用 GCP"

当Cloud Volumes ONTAP HA 对中的节点处于离线状态时，操作不可用

当 HA 对中的一个节点不可用时，另一个节点将为其伙伴提供数据以提供持续的数据服务。这被称为_存储接管_。在存储恢复完成之前，有些操作无法执行。

当 HA 对中的某个节点不可用时， NetApp Console中的系统状态为“Degraded”。

存储接管后无法执行以下操作：

- 支持注册
- 许可证变更
- 实例或虚拟机类型更改
- 写入速度变化
- CIFS 设置
- 更改配置备份的位置
- 设置集群密码
- 管理磁盘和聚合（高级分配）

存储交还完成且系统状态恢复正常后，这些操作将再次可用。

了解Cloud Volumes ONTAP数据加密和勒索软件防护

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

静态数据加密

Cloud Volumes ONTAP支持以下加密技术：

- NetApp加密解决方案（NVE 和 NAE）
- AWS 密钥管理服务
- Azure 存储服务加密
- Google Cloud Platform 默认加密

您可以将NetApp加密解决方案与云提供商提供的本机加密结合使用，以在虚拟机管理程序级别加密数据。这样做可以提供双重加密，这对于非常敏感的数据来说可能是必要的。当访问加密数据时，它会被解密两次 - 一次在虚拟机管理程序级别（使用来自云提供商的密钥），然后再次使用NetApp加密解决方案（使用来自外部密钥管理器的密钥）。

NetApp加密解决方案（NVE 和 NAE）

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，可实现符合 (FIPS) 140-2 标准的卷静态数据加密。 NVE 和 NAE 都使用 AES 256 位加密。

- NVE 每次对一个卷的静态数据进行加密。每个数据卷都有自己独特的加密密钥。
- NAE 是 NVE 的扩展——它对每个卷的数据进行加密，并且卷在聚合体中共享一个密钥。 NAE 还允许对聚合中所有卷的公共块进行重复数据删除。

Cloud Volumes ONTAP通过 AWS、Azure 和 Google Cloud 提供的外部密钥管理服务 (EKM) 支持 NVE 和 NAE，包括第三方解决方案，例如 Fortanix。与ONTAP不同，对于Cloud Volumes ONTAP，加密密钥是在云提供商端生成的，而不是在ONTAP中生成的。Cloud Volumes ONTAP不支持 "板载密钥管理器"。

Cloud Volumes ONTAP使用ONTAP使用的标准密钥管理互操作性协议 (KMIP) 服务。有关支持服务的更多信息，请参阅 "互操作性表工具"。

如果您使用 NVE，则可以选择使用云提供商的密钥保管库来保护ONTAP加密密钥：

- AWS 密钥管理服务 (KMS)
- Azure 密钥保管库 (AKV)
- Google Cloud 密钥管理服务

设置外部密钥管理器后，新聚合默认启用NetApp聚合加密 (NAE)。不属于 NAE 聚合的新卷默认启用 NVE（例如，如果您有在设置外部密钥管理器之前创建的现有聚合）。

设置支持的密钥管理器是唯一需要的步骤。有关设置说明，请参阅"使用NetApp加密解决方案加密卷"。

AWS 密钥管理服务

在 AWS 中启动Cloud Volumes ONTAP系统时，您可以使用 "AWS 密钥管理服务 (KMS)"。 NetApp Console使用客户主密钥 (CMK) 请求数据密钥。

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

如果您想使用此加密选项，则必须确保 AWS KMS 已正确设置。有关信息，请参阅"设置 AWS KMS"。

Azure 存储服务加密

使用以下方式在 Azure 中的Cloud Volumes ONTAP上自动加密数据 "Azure 存储服务加密"使用 Microsoft 管理的密钥。

如果您愿意，您可以使用自己的加密密钥。"了解如何设置Cloud Volumes ONTAP以在 Azure 中使用客户管理的密钥" 。

Google Cloud Platform 默认加密

"Google Cloud Platform 静态数据加密"对于Cloud Volumes ONTAP ，默认启用。无需设置。

虽然 Google Cloud Storage 始终会在将数据写入磁盘之前对其进行加密，但您可以使用控制台 API 创建使用_客户管理加密密钥_的Cloud Volumes ONTAP系统。这些是您使用云密钥管理服务在 GCP 中生成和管理的密钥。"了解更多" 。

ONTAP病毒扫描

您可以使用ONTAP系统上的集成防病毒功能来保护数据免受病毒或其他恶意代码的侵害。

ONTAP病毒扫描（称为“Vscan”）将一流的第三方防病毒软件与ONTAP功能相结合，让您可以灵活地控制扫描哪些文件以及何时扫描。

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

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

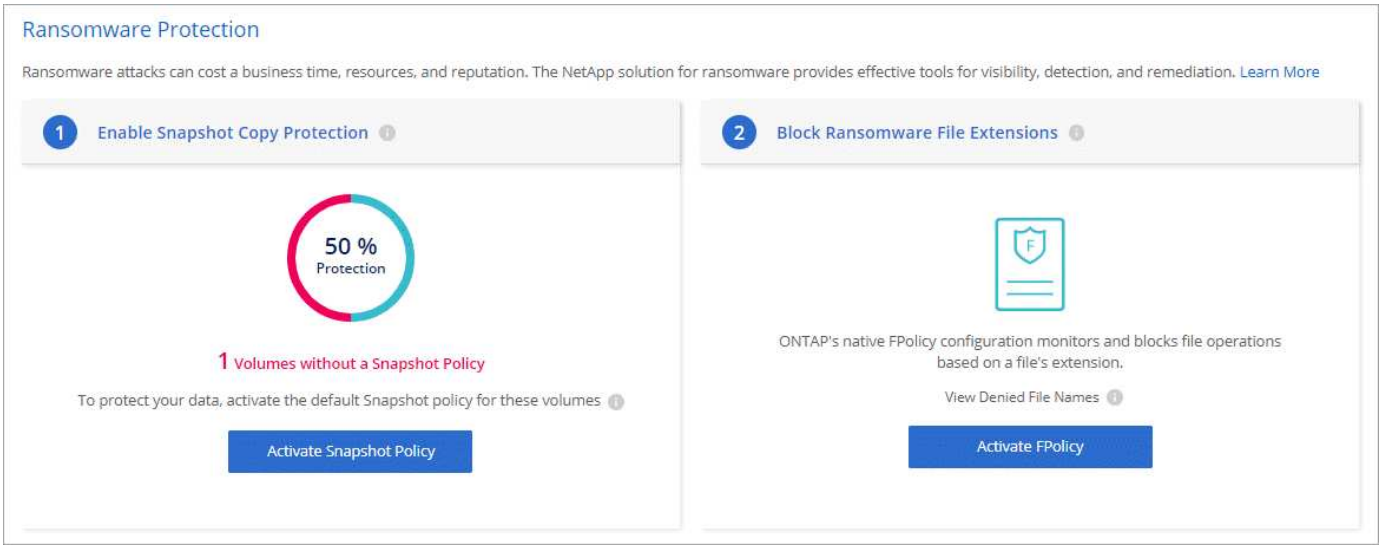
勒索软件防护

勒索软件攻击会浪费企业的时间、资源和声誉。控制台使您能够实施针对勒索软件的NetApp解决方案，该解决方案提供了有效的可见性、检测和补救工具。

- 控制台识别未受快照策略保护的卷，并允许您在这些卷上激活默认快照策略。

  快照副本是只读的，可防止勒索软件破坏。他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的图像的粒度。

- 通过启用 ONTAP 的 FPolicy 解决方案，控制台还允许您阻止常见的勒索软件文件扩展名。



"了解如何实施NetApp勒索软件解决方案" 。

了解Cloud Volumes ONTAP工作负载的性能监控

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

性能技术报告

- 适用于 AWS 的Cloud Volumes ONTAP

  "NetApp技术报告 4383：Amazon Web Services 中Cloud Volumes ONTAP与应用程序工作负载的性能特征"

- 适用于 Microsoft Azure 的Cloud Volumes ONTAP

  "NetApp技术报告 4671：Azure 中Cloud Volumes ONTAP与应用程序工作负载的性能特征"

- 适用于 Google Cloud 的Cloud Volumes ONTAP

  "NetApp技术报告 4816：适用于 Google Cloud 的Cloud Volumes ONTAP的性能特征"

CPU 性能

从您的云提供商的监控工具来看， Cloud Volumes ONTAP节点的利用率很高（超过 90%）。这是因为ONTAP保留了虚拟机中存在的所有 vCPU，以便在需要时可用。

欲了解更多信息，请参阅 "NetApp知识库文章，介绍如何使用 CLI 监控ONTAP CPU 利用率"

基于节点的 BYOL 许可证管理

每个具有基于节点的自带许可证 (BYOL) 的Cloud Volumes ONTAP系统都必须安装具有有效订阅的系统许可证。 NetApp Console通过为您管理许可证并在许可证到期前显示警告来简化该流程。

基于节点的许可证是Cloud Volumes ONTAP的上一代许可证。基于节点的许可证可以从NetApp (BYOL) 处购买，并且仅在特定情况下才可以续订许可证。

"了解有关Cloud Volumes ONTAP许可选项的更多信息" 。

"了解有关如何管理基于节点的许可证的更多信息" 。

BYOL 系统许可证

可从 NetApp 采购基于节点的许可证。您可以为单节点系统或 HA 对购买的许可证数量是无限的。

已限制 BYOL 许可证的购买、延期和续订。有关更多信息，请参阅 "Cloud Volumes ONTAPP的 BYOL 许可可用性受限" 。

基于节点的许可证最多可为单个节点或 HA 对提供 368 TiB 的容量。您可能已为Cloud Volumes ONTAP BYOL系统购买了多个许可证，以分配超过 368 TiB 的容量。例如，您可能有两个许可证，为Cloud Volumes ONTAP分配最多 736 TiB 的容量。或者，您可能有四个许可证，以获得最多 1.4 PiB 的容量。

请注意，磁盘限制可能会阻止您仅使用磁盘就达到容量限制。您可以通过以下方式超越磁盘限制"将非活动数据分层到对象存储"。有关磁盘限制的信息，请参阅 "Cloud Volumes ONTAP发行说明中的存储限制"。

新系统的许可证管理

当您创建基于节点的 BYOL 系统时，控制台会提示您输入许可证的序列号和NetApp支持站点帐户。控制台使用该帐户从NetApp下载许可证文件并将其安装在Cloud Volumes ONTAP系统上。

"了解如何将NetApp支持站点帐户添加到控制台" 。

如果控制台无法通过安全的互联网连接访问许可证文件，您可以"自行获取文件，然后手动将文件上传到控制台"。

许可证到期

控制台会在基于节点的许可证到期前 30 天显示警告，并在许可证到期时再次显示警告。下图显示了用户界面中出现的 30 天到期警告：

您可以选择系统来查看该消息。

如果您是组织或帐户管理员并且启用了该选项，则控制台会在通过电子邮件发送给您的Cloud Volumes ONTAP报告中包含许可证到期警告。通过电子邮件发送的报告包含每两周一次的许可证到期警告。

如果您不及时续订许可证， Cloud Volumes ONTAP系统将自动关闭。如果您重新启动它，它就会再次自动关闭。

执照续期

如果您通过联系NetApp代表续订基于节点的 BYOL 订阅，控制台将自动从NetApp获取新许可证并将其安装在Cloud Volumes ONTAP系统上。

如果控制台无法通过安全的互联网连接访问许可证文件，您可以"自行获取文件，然后手动将文件上传到控制台"。

许可证转移到新系统

当您删除现有系统然后使用相同的许可证创建新系统时，基于节点的 BYOL 许可证可以在Cloud Volumes ONTAP系统之间转移。

例如，您可能想要删除现有的许可系统，然后将许可证与不同 VPC/VNet 或云提供商中的新 BYOL 系统一起使用。请注意，只有_cloud-agnostic_序列号才适用于任何云提供商。与云无关的序列号以 *908xxxx* 前缀开头。

值得注意的是，您的 BYOL 许可证与您的公司和一组特定的NetApp支持站点凭证相关联。

了解如何将AutoSupport和Digital Advisor用于Cloud Volumes ONTAP

ONTAP的AutoSupport组件收集遥测数据并将其发送以供分析。 Active IQ Digital Advisor（也称为Digital Advisor）分析来自AutoSupport 的数据并提供主动护理和优化。利用人工智能，Digital Advisor可以识别潜在问题并在其影响您的业务之前帮助您解决它们。

Digital Advisor通过基于云的门户和移动应用程序提供可操作的预测分析和主动支持，使您能够优化全球混合云中的数据基础设施。所有拥有有效SupportEdge合同的NetApp客户均可获得来自Digital Advisor的数据驱动见解和建议（功能因产品和支持层级而异）。

您可以使用Digital Advisor执行以下一些操作：

- 计划升级。

  Digital Advisor可识别您环境中可以通过升级到较新版本的ONTAP来解决的问题，而升级顾问组件可帮助您规划成功的升级。

- 查看系统健康状况。

  您的Digital Advisor仪表板会报告任何健康问题并帮助您纠正这些问题。监控系统容量以确保永远不会耗尽存储空间。查看您的系统的支持案例。

- 管理绩效。

  Digital Advisor显示的系统性能比您在ONTAP System Manager 中看到的更长。识别影响您性能的配置和系统问题。最大限度提高效率。查看存储效率指标并确定在更少空间内存储更多数据的方法。

- 查看库存和配置。

  Digital Advisor显示完整的库存和软件和硬件配置信息。查看服务合同何时到期并进行续订以确保您继续获得支持。

相关链接

- "NetApp文档：Digital Advisor"
- "启动Digital Advisor"
- "SupportEdge服务"

Cloud Volumes ONTAP支持的默认配置

了解Cloud Volumes ONTAP 的默认配置方式可以帮助您设置和管理系统，特别是如果您熟悉ONTAP ，因为Cloud Volumes ONTAP的默认设置与ONTAP不同。

默认设置

- NetApp Console在部署Cloud Volumes ONTAP时会创建一个数据服务存储虚拟机。某些配置支持额外的存储虚拟机。"了解有关管理存储虚拟机的更多信息" 。

  从 3.9.5 版本开始，初始存储虚拟机上启用逻辑空间报告。当逻辑报告空间时， ONTAP会报告卷空间，以便存储效率功能节省的所有物理空间也被报告为已使用。有关内联存储效率功能的信息，请参阅知识库文章"KB：CVO 支持哪些内联存储效率功能？"

- 控制台会自动在Cloud Volumes ONTAP上安装以下ONTAP功能许可证：
  - CIFS
  - FlexCache
  - FlexClone
  - iSCSI
  - 多租户加密密钥管理 (MTEKM)，从Cloud Volumes ONTAP 9.12.1 GA 开始
  - NetApp卷加密（仅适用于自带许可证 (BYOL) 或注册的即用即付 (PAYGO) 系统）
  - NFS ifdef::aws[] endif::aws[] ifdef::azure[] endif::azure[]
  - SnapMirror
  - SnapRestore
  - SnapVault

- 默认创建了几个网络接口：
  - 集群管理 LIF
  - 集群间 LIF
- Azure 中 HA 系统上的 SVM 管理 LIF
- Google Cloud 中 HA 系统上的 SVM 管理 LIF
- AWS 单节点系统上的 SVM 管理 LIF
- 节点管理 LIF

+ 在 Google Cloud 中，此 LIF 与集群间 LIF 结合在一起。

- iSCSI 数据 LIF
- CIFS 和 NFS 数据 LIF

> 由于云提供商的要求， Cloud Volumes ONTAP默认禁用 LIF 故障转移。将 LIF 迁移到其他端口会破坏实例上 IP 地址和网络接口之间的外部映射，从而使 LIF 无法访问。

  - Cloud Volumes ONTAP使用 HTTP 将配置备份发送到控制台代理。

    可以从 http://ipaddress/occm/offboxconfig/ 访问备份，其中 *ipaddress* 是控制台代理主机的 IP 地址。

    您可以使用备份重新配置您的Cloud Volumes ONTAP系统。有关配置备份的更多信息，请参阅 "ONTAP 文档"。

  - 控制台设置的一些卷属性与其他管理工具（例如ONTAP系统管理器或ONTAP CLI）不同。

    下表列出了与默认值不同的卷属性设置：

属性	控制台配置的值
自动调整大小模式	生长
最大自动调整大小	1000% 组织或帐户管理员可以从“设置”页面修改此值。
安全模式	NTFS 用于 CIFS 卷 UNIX 用于 NFS 卷
空间保证风格	无
UNIX 权限（仅限 NFS）	777

+
有关这些属性的信息，请参阅"ONTAP卷创建手册页"。

用于系统数据的内部磁盘

除了用户数据的存储外，控制台还购买了系统数据的云存储。

AWS

- 每个节点有三个磁盘用于启动、根和核心数据：
  - 47 GiB io1 磁盘用于启动数据
  - 140 GiB gp3 磁盘用于根数据
  - 540 GiB gp2 磁盘用于核心数据
- 对于 HA 对：
  - 两个用于中介实例的 st1 EBS 卷，其中一个约 8 GiB，用作根磁盘，另一个约 4 GiB，用作数据磁盘
  - 每个节点中有一个 140 GiB gp3 磁盘，用于保存另一个节点的根数据副本

    在某些区域中，可用的EBS磁盘类型只能是gp2。
- 每个启动磁盘和根磁盘一个 EBS 快照

  重启时会自动创建快照。
- 当您使用密钥管理服务 (KMS) 在 AWS 中启用数据加密时， Cloud Volumes ONTAP的启动磁盘和根磁盘也会被加密。这包括 HA 对中中介实例的启动磁盘。磁盘使用您在添加Cloud Volumes ONTAP系统时选择的 CMK 进行加密。

在 AWS 中， NVRAM位于启动盘上。

Azure（单节点）

- 三个高级 SSD 磁盘：
  - 一个 10 GiB 磁盘用于启动数据
  - 一个 140 GiB 磁盘用于根数据
  - 一个 512 GiB 磁盘用于NVRAM

    如果您为Cloud Volumes ONTAP选择的虚拟机支持 Ultra SSD，则系统将使用 32 GiB Ultra SSD 作为NVRAM，而不是 Premium SSD。
- 一个 1024 GiB 标准 HDD 磁盘，用于保存核心
- 每个启动磁盘和根磁盘对应一个 Azure 快照
- 默认情况下，Azure 中的每个磁盘都是静态加密的。

  如果您为Cloud Volumes ONTAP选择的虚拟机支持 Premium SSD v2 托管磁盘作为数据磁盘，则系统将使用 32 GiB Premium SSD v2 托管磁盘作为NVRAM，并使用另一个磁盘作为根磁盘。

Azure（HA 对）

HA 与页 Blob 对

- 两个 10 GiB Premium SSD 磁盘用于启动卷（每个节点一个）
- 两个用于根卷的 140 GiB 高级存储页 Blob（每个节点一个）
- 两个 1024 GiB 标准 HDD 磁盘用于保存核心（每个节点一个）
- 两个 512 GiB 高级 SSD 磁盘用于NVRAM （每个节点一个）
- 每个启动磁盘和根磁盘对应一个 Azure 快照

  重启时会自动创建快照。

- 默认情况下，Azure 中的每个磁盘都是静态加密的。

HA 对与多个可用区域中的共享托管磁盘

- 两个 10 GiB Premium SSD 磁盘用于启动卷（每个节点一个）
- 两个 512 GiB 高级 SSD 磁盘用于根卷（每个节点一个）
- 两个 1024 GiB 标准 HDD 磁盘用于保存核心（每个节点一个）
- 两个 512 GiB 高级 SSD 磁盘用于NVRAM （每个节点一个）
- 每个启动磁盘和根磁盘对应一个 Azure 快照

  重启时会自动创建快照。

- 默认情况下，Azure 中的每个磁盘都是静态加密的。

单个可用区域中具有共享托管磁盘的 HA 对

- 两个 10 GiB Premium SSD 磁盘用于启动卷（每个节点一个）
- 两个 512 GiB 高级 SSD 共享托管磁盘，用于根卷（每个节点一个）
- 两个 1024 GiB 标准 HDD 磁盘用于保存核心（每个节点一个）
- 两个 512 GiB 高级 SSD 托管磁盘用于NVRAM （每个节点一个）

如果您的虚拟机支持高级 SSD v2 托管磁盘作为数据磁盘，它将使用 32 GiB 高级 SSD v2 托管磁盘作为NVRAM ，并使用 512 GiB 高级 SSD v2 共享托管磁盘作为根卷。

当满足以下条件时，您可以在单个可用区域中部署 HA 对并使用高级 SSD v2 托管磁盘：

- Cloud Volumes ONTAP的版本为 9.15.1 或更高版本。
- 所选区域和区域支持高级 SSD v2 托管磁盘。有关受支持区域的信息，请参阅 "Microsoft Azure 网站：按地区提供的产品"。
- 订阅已注册为 Microsoft"Microsoft.Compute/VMOrchestratorZonalMultiFD 功能" 。

Google Cloud（单节点）

- 一个 10 GiB SSD 永久磁盘，用于存储启动数据

- 一个 64 GiB SSD 持久磁盘，用于存储根数据
- 一个 500 GiB SSD 持久磁盘，用于NVRAM
- 一个 315 GiB 标准持久磁盘，用于保存核心
- 启动和根数据的快照

  重启时会自动创建快照。

- 默认情况下，启动磁盘和根磁盘是加密的。

Google Cloud（高可用性对）

- 两个 10 GiB SSD 持久磁盘用于启动数据
- 四个 64 GiB SSD 持久磁盘用于根数据
- 两个 500 GiB SSD 持久磁盘用于NVRAM
- 两个 315 GiB 标准持久磁盘，用于保存核心
- 一个 10 GiB 标准持久磁盘，用于存储中介数据
- 一个 10 GiB 标准永久磁盘，用于中介启动数据
- 启动和根数据的快照

  重启时会自动创建快照。

- 默认情况下，启动磁盘和根磁盘是加密的。

磁盘所在位置

存储布局：

- 启动数据驻留在连接到实例或虚拟机的磁盘上。

  此磁盘包含启动映像，但不适用于Cloud Volumes ONTAP。

- 包含系统配置和日志的根数据位于 aggr0 中。
- 存储虚拟机 (SVM) 根卷位于 aggr1 中。
- 数据卷也驻留在 aggr1 中。

知识和支持

注册以获得支持

需要进行支持注册才能获得针对NetApp Console及其存储解决方案和数据服务的技术支持。还需要支持注册才能启用Cloud Volumes ONTAP系统的关键工作流程。

注册支持并不能使NetApp获得云提供商文件服务的支持。有关云提供商文件服务、其基础设施或使用该服务的任何解决方案的技术支持，请参阅该产品文档中的“获取帮助”。

- "适用于ONTAP 的Amazon FSx"
- "Azure NetApp Files"
- "Google Cloud NetApp Volumes"

支持注册概述

激活支持权利的注册方式有两种：

- 注册您的NetApp Console帐户序列号（您的 20 位 960xxxxxxxx 序列号位于控制台中的“支持资源”页面上）。

  这可作为控制台内任何服务的单一支持订阅 ID。每个控制台帐户都必须注册。

- 在您的云提供商市场中注册与订阅相关的Cloud Volumes ONTAP序列号（这些是 20 位 909201xxxxxxxx 序列号）。

  这些序列号通常称为_PAYGO 序列号_，由NetApp Console在Cloud Volumes ONTAP部署时生成。

注册两种类型的序列号可以实现开立支持票和自动生成案例等功能。通过将NetApp支持站点 (NSS) 帐户添加到控制台即可完成注册，如下所述。

注册**NetApp Console**以获取**NetApp**支持

要注册支持并激活支持权利，您的NetApp Console帐户中的一名用户必须将NetApp支持站点帐户与其控制台登录名关联。如何注册NetApp支持取决于您是否已经拥有NetApp支持站点 (NSS) 帐户。

拥有 **NSS** 帐户的现有客户

如果您是拥有 NSS 帐户的NetApp客户，则只需通过控制台注册即可获得支持。

步骤

1. 选择“管理”>“凭证”。
2. 选择*用户凭证*。
3. 选择*添加 NSS 凭据*并按照NetApp支持站点 (NSS) 身份验证提示进行操作。
4. 要确认注册过程是否成功，请选择“帮助”图标，然后选择“支持”。

   *资源*页面应显示您的控制台帐户已注册以获得支持。

请注意，如果其他控制台用户尚未将NetApp支持站点帐户与其登录名关联，他们将看不到相同的支持注册状态。但是，这并不意味着您的帐户没有注册支持。只要组织中的一名用户遵循了这些步骤，您的帐户就已注册。

现有客户但没有 **NSS** 账户

如果您是现有的NetApp客户，拥有现有许可证和序列号但没有 NSS 帐户，则需要创建一个 NSS 帐户并将其与您的控制台登录关联。

步骤

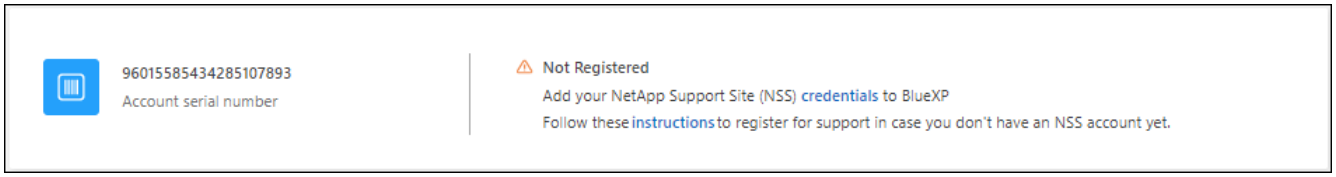
1. 通过完成以下操作创建NetApp支持站点帐户 "NetApp支持站点用户注册表"
   a. 请务必选择适当的用户级别，通常为* NetApp客户/最终用户*。
   b. 请务必复制上面用于序列号字段的控制台帐户序列号（960xxxx）。这将加快账户处理速度。
2. 完成以下步骤，将您的新 NSS 帐户与您的控制台登录名关联拥有 NSS 帐户的现有客户。

NetApp全新产品

如果您是NetApp新用户并且没有 NSS 帐户，请按照以下步骤操作。

步骤

1. 在控制台的右上角，选择“帮助”图标，然后选择“支持”。
2. 从支持注册页面找到您的帐户 ID 序列号。



3. 导航至 "NetApp 的支持注册网站"并选择*我不是注册的NetApp客户*。
4. 填写必填字段（带有红色星号的字段）。
5. 在*产品线*字段中，选择*云管理器*，然后选择适用的计费提供商。
6. 从上面的步骤 2 复制您的帐户序列号，完成安全检查，然后确认您已阅读 NetApp 的全球数据隐私政策。

   一封电子邮件会立即发送到提供的邮箱以完成此安全交易。如果几分钟内没有收到验证电子邮件，请务必检查您的垃圾邮件文件夹。

7. 从电子邮件中确认操作。

   确认向NetApp提交您的请求并建议您创建NetApp支持站点帐户。

8. 通过完成以下操作创建NetApp支持站点帐户 "NetApp支持站点用户注册表"
   a. 请务必选择适当的用户级别，通常为* NetApp客户/最终用户*。
   b. 请务必复制上面用于序列号字段的帐户序列号（960xxxx）。这将加快处理速度。

完成后

NetApp应该在此过程中与您联系。这是针对新用户的一次性入职培训。

拥有NetApp支持站点帐户后，请按照以下步骤将该帐户与您的控制台登录关联拥有 NSS 帐户的现有客户。

关联 NSS 凭据以获得Cloud Volumes ONTAP支持

需要将NetApp支持站点凭据与您的控制台帐户关联，才能为Cloud Volumes ONTAP启用以下关键工作流程：

- 注册即用即付Cloud Volumes ONTAP系统以获得支持

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

- 自带许可证 (BYOL) 时部署Cloud Volumes ONTAP

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

- 将Cloud Volumes ONTAP软件升级到最新版本

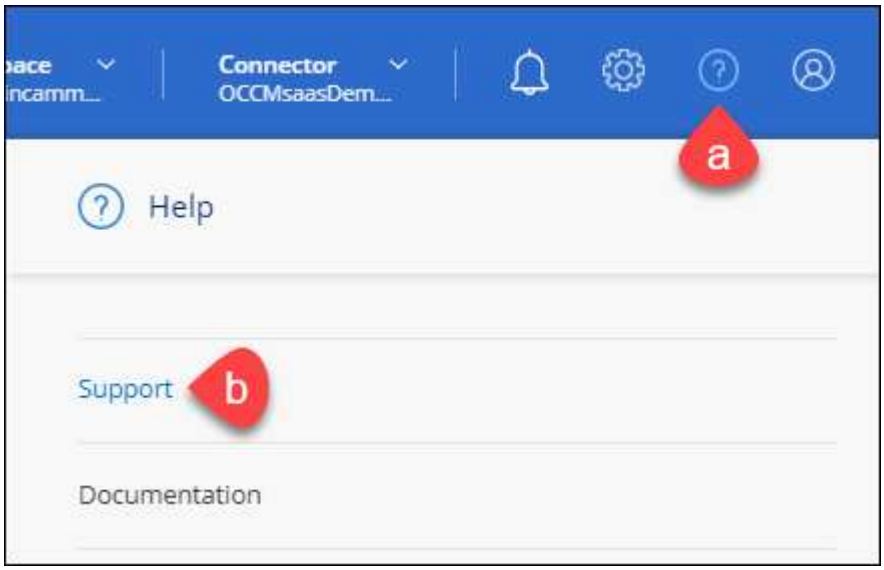
将 NSS 凭据与您的NetApp Console帐户关联与将 NSS 帐户与控制台用户登录关联不同。

这些 NSS 凭证与您的特定控制台帐户 ID 相关联。属于控制台组织的用户可以从*支持 > NSS 管理*访问这些凭据。

- 如果您有客户级帐户，则可以添加一个或多个 NSS 帐户。
- 如果您有合作伙伴或经销商帐户，则可以添加一个或多个 NSS 帐户，但不能与客户级帐户一起添加。

步骤

1. 在控制台的右上角，选择“帮助”图标，然后选择“支持”。



2. 选择*NSS 管理 > 添加 NSS 帐户*。
3. 当出现提示时，选择“继续”以重定向到 Microsoft 登录页面。

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

4. 在登录页面，提供您的NetApp支持站点注册的电子邮件地址和密码以执行身份验证过程。

   这些操作使控制台能够使用您的 NSS 帐户进行许可证下载、软件升级验证和未来支持注册等操作。

   请注意以下事项：

   - NSS 帐户必须是客户级帐户（不是访客或临时帐户）。您可以拥有多个客户级 NSS 帐户。
   - 如果该帐户是合作伙伴级别帐户，则只能有一个 NSS 帐户。如果您尝试添加客户级 NSS 帐户并且合作伙伴级帐户已存在，您将收到以下错误消息：

     “此帐户不允许使用 NSS 客户类型，因为已经存在不同类型的 NSS 用户。”

   如果您已有客户级 NSS 帐户并尝试添加合作伙伴级帐户，情况也是如此。

   - 成功登录后， NetApp将存储 NSS 用户名。

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

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

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

获取帮助

NetApp以多种方式为NetApp Console及其云服务提供支持。全天候提供广泛的免费自助支持选项，例如知识库 (KB) 文章和社区论坛。您的支持注册包含通过网络工单获取的远程技术支持。

获取云提供商文件服务的支持

有关云提供商文件服务、其基础设施或使用该服务的任何解决方案的技术支持，请参阅该产品的文档。

- "适用于ONTAP 的Amazon FSx"
- "Azure NetApp Files"
- "Google Cloud NetApp Volumes"

要获得特定于NetApp及其存储解决方案和数据服务的技术支持，请使用下面描述的支持选项。

使用自助选项

这些选项每周 7 天、每天 24 小时免费提供：

- 文档

  您当前正在查看的NetApp Console文档。

- "知识库"

搜索NetApp知识库以查找有助于解决问题的文章。

- "社区"

  加入NetApp Console社区，关注正在进行的讨论或创建新的讨论。

向NetApp支持创建案例

除了上述自助支持选项之外，您还可以在激活支持后与NetApp支持专家合作解决任何问题。

开始之前

- 要使用“创建案例”功能，您必须首先将您的NetApp支持站点凭据与您的控制台登录关联。 "了解如何管理与控制台登录相关的凭据" 。
- 如果您要为具有序列号的ONTAP系统打开案例，那么您的 NSS 帐户必须与该系统的序列号相关联。

步骤

1. 在NetApp Console中，选择“帮助”>“支持”。
2. 在“资源”页面上，选择“技术支持”下的可用选项之一：

   a. 如果您想通过电话与某人交谈，请选择“致电我们”。您将被引导至 netapp.com 上的一个页面，其中列出了您可以拨打的电话号码。

   b. 选择“创建案例”向NetApp支持专家开具一张票：

      - 服务：选择与问题相关的服务。例如，* NetApp Console* 特定于控制台内的工作流或功能的技术支持问题。
      - 系统：如果适用于存储，请选择* Cloud Volumes ONTAP* 或 **On-Prem**，然后选择相关的工作环境。

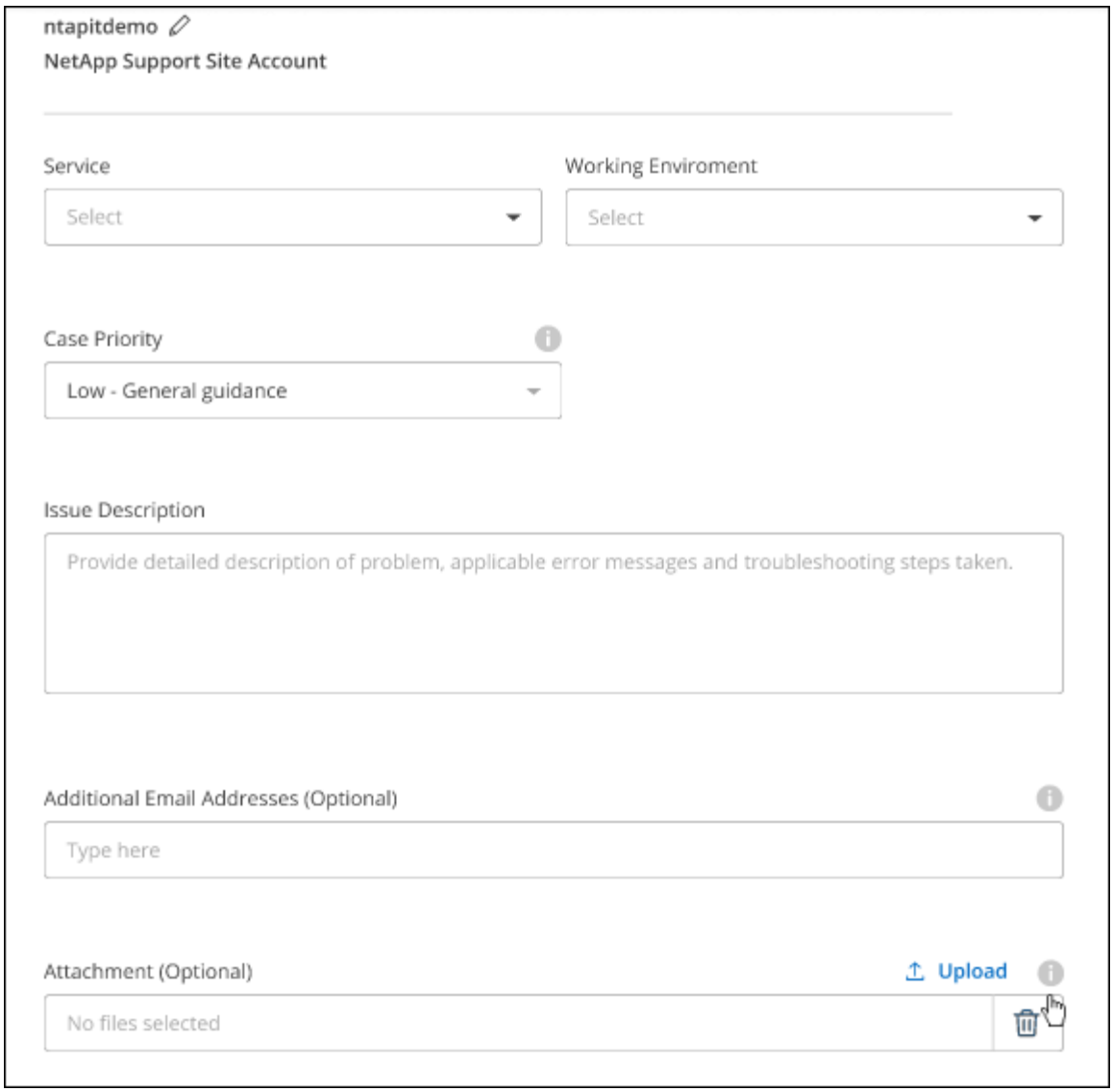
        系统列表位于控制台组织范围内，并且您在顶部横幅中选择了控制台代理。

      - 案例优先级：选择案例的优先级，可以是低、中、高或严重。

        要了解有关这些优先事项的更多详细信息，请将鼠标悬停在字段名称旁边的信息图标上。

      - 问题描述：提供问题的详细描述，包括任何适用的错误消息或您执行的故障排除步骤。
      - 其他电子邮件地址：如果您想让其他人知道此问题，请输入其他电子邮件地址。
      - 附件（可选）：一次最多上传五个附件。

        每个附件文件大小限制为 25 MB。支持以下文件扩展名：txt、log、pdf、jpg/jpeg、rtf、doc/docx、xls/xlsx 和 csv。



完成后

将会出现一个弹出窗口，其中显示您的支持案例编号。NetApp支持专家将审查您的案例并尽快回复您。

要查看支持案例的历史记录，您可以选择*设置>时间线*并查找名为“创建支持案例”的操作。最右边的按钮可让您展开操作以查看详细信息。

尝试创建案例时，您可能会遇到以下错误消息：

“您无权针对所选服务创建案例”

此错误可能意味着 NSS 帐户及其关联的记录公司与NetApp Console帐户序列号的记录公司不同（即。960xxxx）或工作环境序列号。您可以使用以下选项之一寻求帮助：

- 提交非技术案例 https://mysupport.netapp.com/site/help

管理您的支持案例

您可以直接从控制台查看和管理活动和已解决的支持案例。您可以管理与您的 NSS 帐户和公司相关的案例。

请注意以下事项：

- 页面顶部的案例管理仪表板提供两种视图：
  - 左侧视图显示了您提供的用户 NSS 帐户在过去 3 个月内打开的案件总数。
  - 右侧的视图根据您的用户 NSS 帐户显示了过去 3 个月内贵公司级别开设的案件总数。

  表中的结果反映了与您选择的视图相关的案例。
- 您可以添加或删除感兴趣的列，并且可以过滤优先级和状态等列的内容。其他列仅提供排序功能。

  请查看以下步骤以了解更多详细信息。
- 在每个案件级别，我们提供更新案件记录或关闭尚未关闭或待关闭状态的案件的功能。

步骤

1. 在NetApp Console中，选择“帮助”>“支持”。
2. 选择*案例管理*，如果出现提示，请将您的 NSS 帐户添加到控制台。

   案例管理*页面显示与您的控制台用户帐户关联的 **NSS** 帐户相关的未结案例。这与出现在 ***NSS** 管理 页面顶部的 NSS 帐户相同。
3. （可选）修改表中显示的信息：
   - 在“组织的案例”下，选择“查看”以查看与您的公司相关的所有案例。
   - 通过选择精确的日期范围或选择不同的时间范围来修改日期范围。
   - 过滤列的内容。
   - 通过选择然后选择您想要显示的列。
4. 通过选择管理现有案例并选择其中一个可用选项：
   - 查看案例：查看有关特定案例的完整详细信息。
   - 更新案例说明：提供有关您的问题的更多详细信息，或选择*上传文件*以附加最多五个文件。

     每个附件文件大小限制为 25 MB。支持以下文件扩展名：txt、log、pdf、jpg/jpeg、rtf、doc/docx、xls/xlsx 和 csv。
   - 结案：提供有关结案原因的详细信息，然后选择*结案*。

法律声明

法律声明提供对版权声明、商标、专利等的访问。

版权

"https://www.netapp.com/company/legal/copyright/"

商标

NETAPP、NETAPP 徽标和NetApp商标页面上列出的标志是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。

"https://www.netapp.com/company/legal/trademarks/"

专利

NetApp拥有的专利的最新列表可以在以下位置找到：

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

隐私政策

"https://www.netapp.com/company/legal/privacy-policy/"

开源

通知文件提供有关NetApp软件中使用的第三方版权和许可的信息。

- "NetApp Console通知"
- "Cloud Volumes ONTAP通知"
- "ONTAP通知"