# 开始使用 **Microsoft Azure**

## Cloud Volumes ONTAP

NetApp
February 17, 2026

This PDF was generated from https://docs.netapp.com/zh-cn/storage-management-cloud-volumes-ontap/concept-azure-mktplace-direct.html on February 17, 2026. Always check docs.netapp.com for the latest.

# 目录


开始使用 Microsoft Azure . . . 1
- 了解 Azure 中的Cloud Volumes ONTAP部署选项 . . . 1
- 开始使用NetApp Console . . . 2
  - Azure 中的Cloud Volumes ONTAP快速入门 . . . 2
  - 在 Azure 中规划Cloud Volumes ONTAP配置 . . . 3
  - 为Cloud Volumes ONTAP设置 Azure 网络 . . . 5
  - 设置Cloud Volumes ONTAP以在 Azure 中使用客户管理的密钥 . . . 14
  - 在 Azure 中设置Cloud Volumes ONTAP许可 . . . 19
  - 在 Azure 中为Cloud Volumes ONTAP启用高可用性模式 . . . 25
  - 在 Azure 中为Cloud Volumes ONTAP启用 VMOrchestratorZonalMultiFD . . . 27
  - 在 Azure 中启动Cloud Volumes ONTAP . . . 27
  - 验证 Azure 平台映像 . . . 38
- 从 Azure 市场部署Cloud Volumes ONTAP . . . 48
  - 解决部署问题 . . . 50
  - 在控制台中发现已部署的系统 . . . 50

# 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 |
| 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 | |
| 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：<br>• Cloud Volumes ONTAP服务<br>• ONTAP 服务<br>• 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<br>• 核<br>• NVRAM | • 根<br>• 数据 |
| 具有页 Blob 的 Azure HA 单可用性区域 | • 引导<br>• 核<br>• NVRAM | 无 |
| 具有共享托管磁盘的 Azure HA 单可用性区域 | • 引导<br>• 核<br>• NVRAM | • 根<br>• 数据 |
| 具有共享托管磁盘的 Azure HA 多个可用性区域 | • 引导<br>• 核<br>• NVRAM | • 根<br>• 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

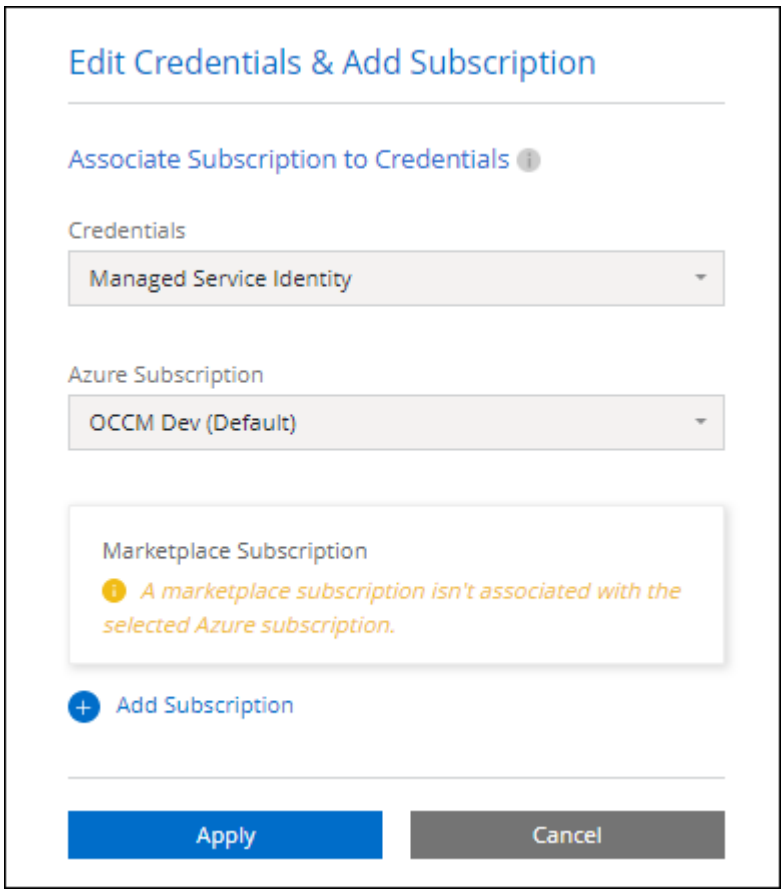
选择免费增值服务，免费使用Cloud Volumes ONTAP，最高可提供 500 GiB 的配置容量。"了解有关免费增值服务的更多信息" 。

步骤

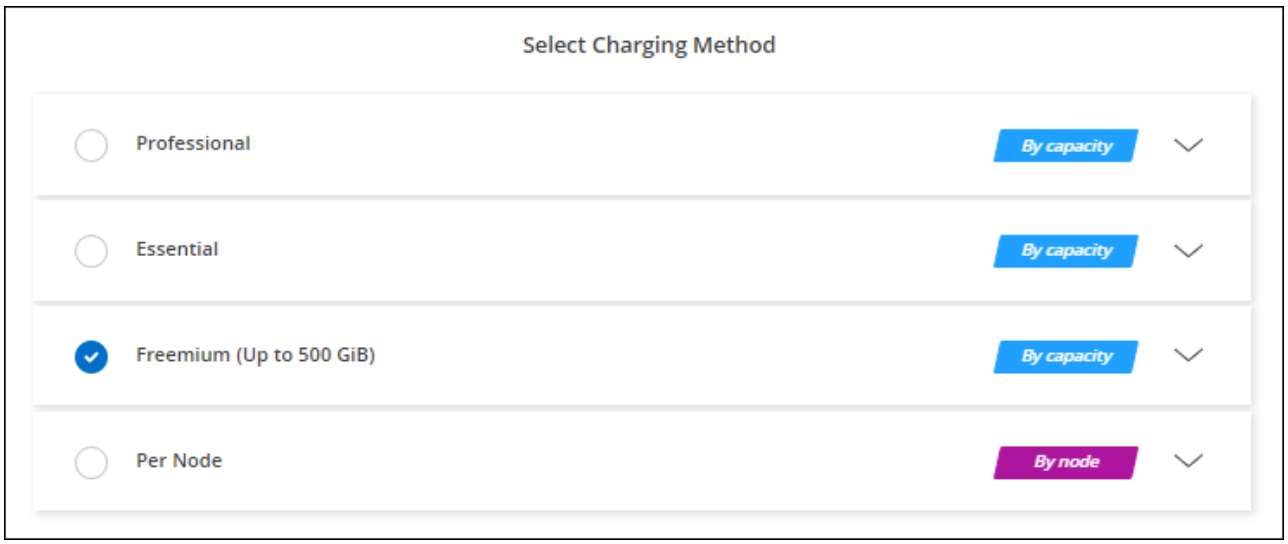
1. 从NetApp Console的左侧导航菜单中，选择“存储”>“管理”。
2. 在*系统*页面上，单击*添加系统*并按照步骤操作。

    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。

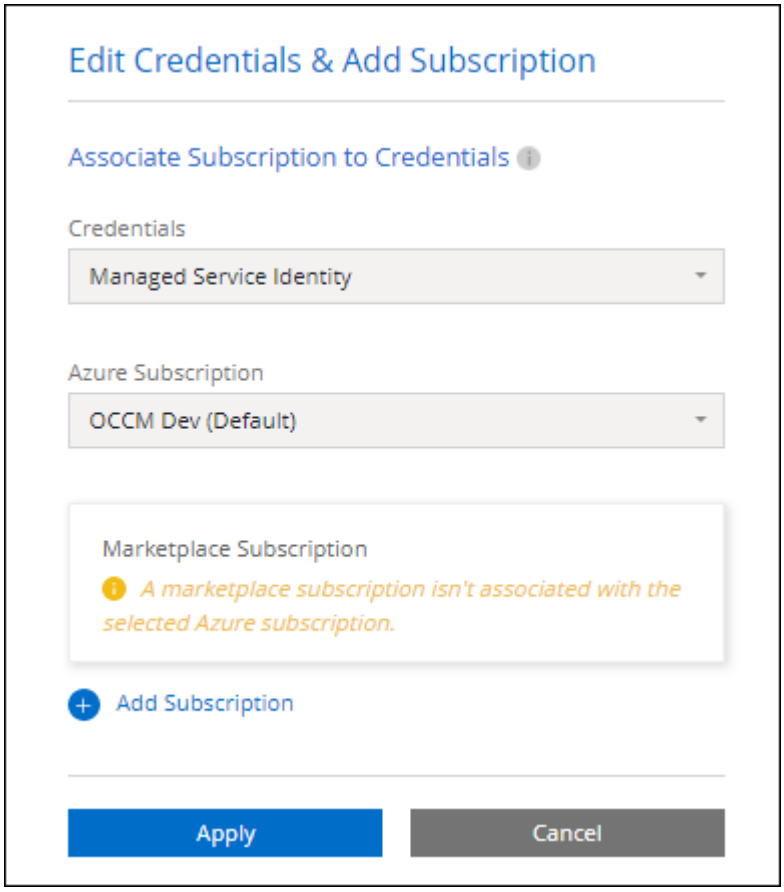
   您必须先从控制台获取许可证，然后才能将其与Cloud Volumes ONTAP一起使用。如果需要的话，你可以"

手动将许可证添加到控制台"。

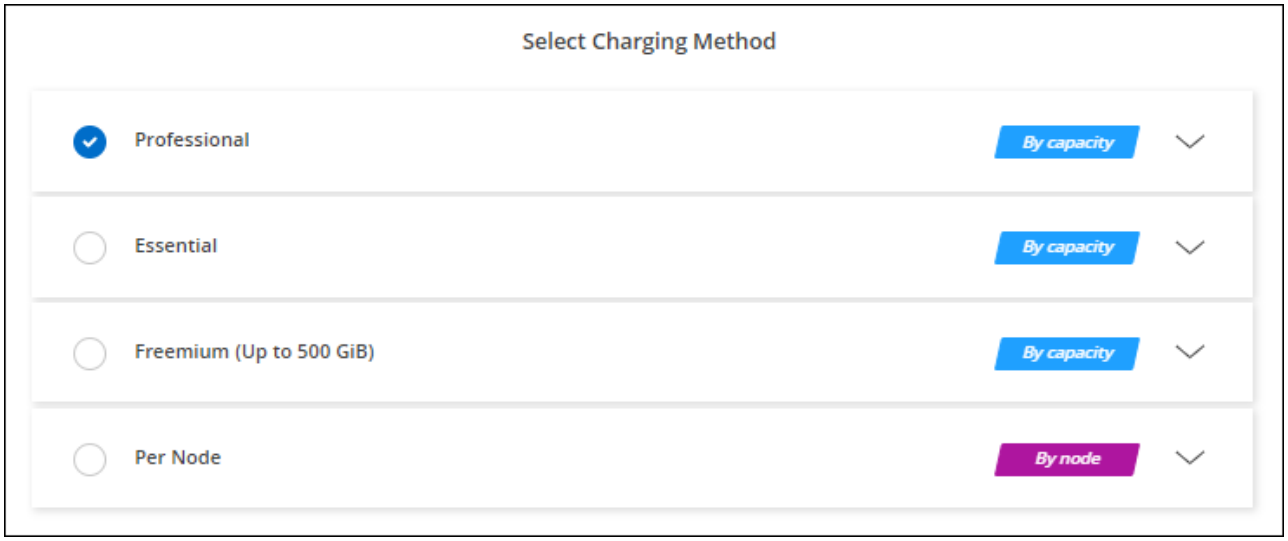
3. 在*系统*页面上，单击*添加系统*并按照步骤操作。

   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" 。

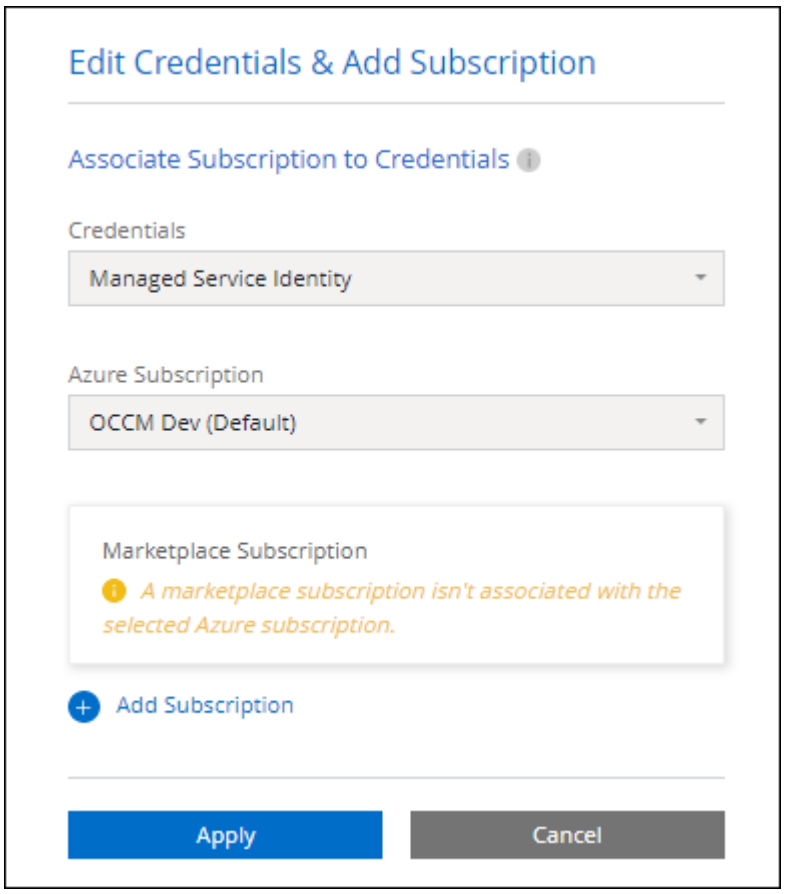
**PAYGO** 订阅

通过订阅云提供商市场提供的服务按小时付费。

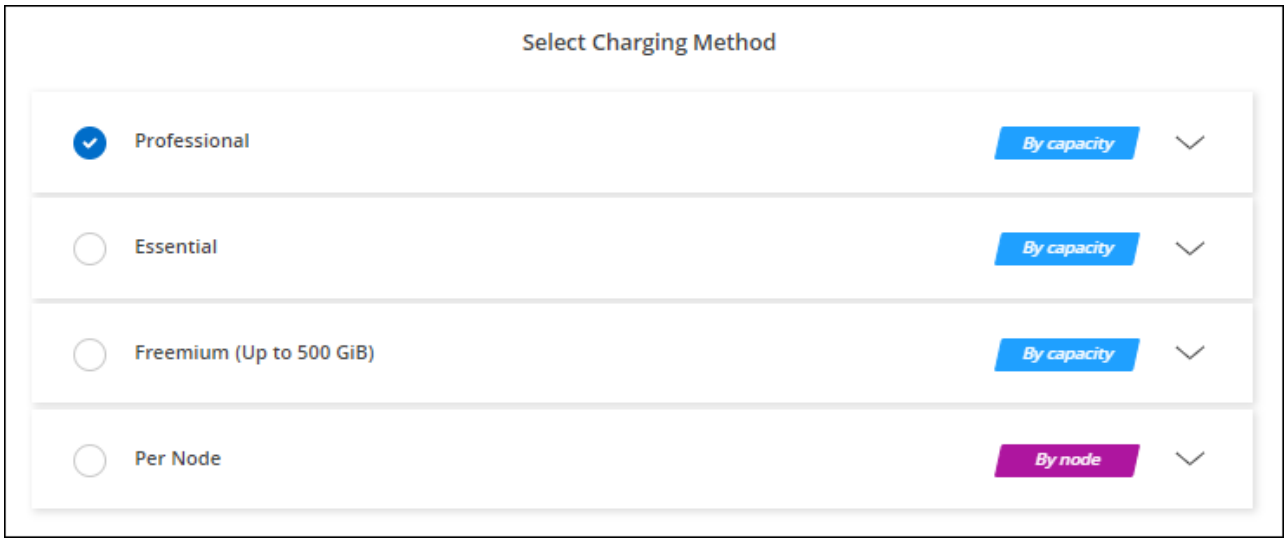
当您创建Cloud Volumes ONTAP系统时，控制台会提示您订阅 Azure 市场中提供的协议。然后将该订阅与系统关联以进行收费。您可以将同一订阅用于其他系统。

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。

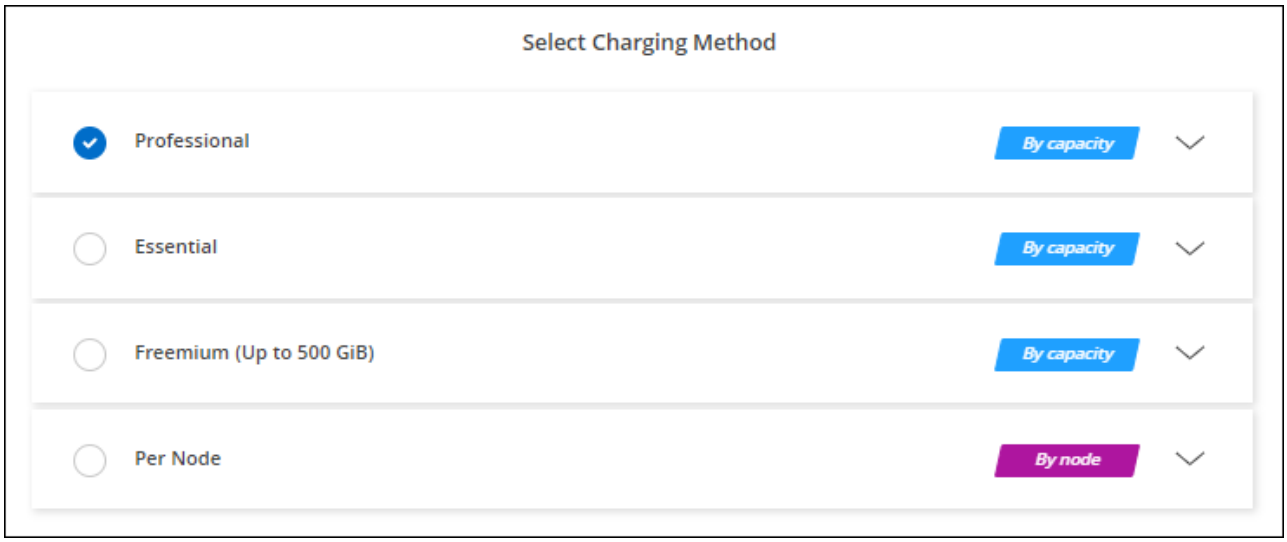
步骤

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。



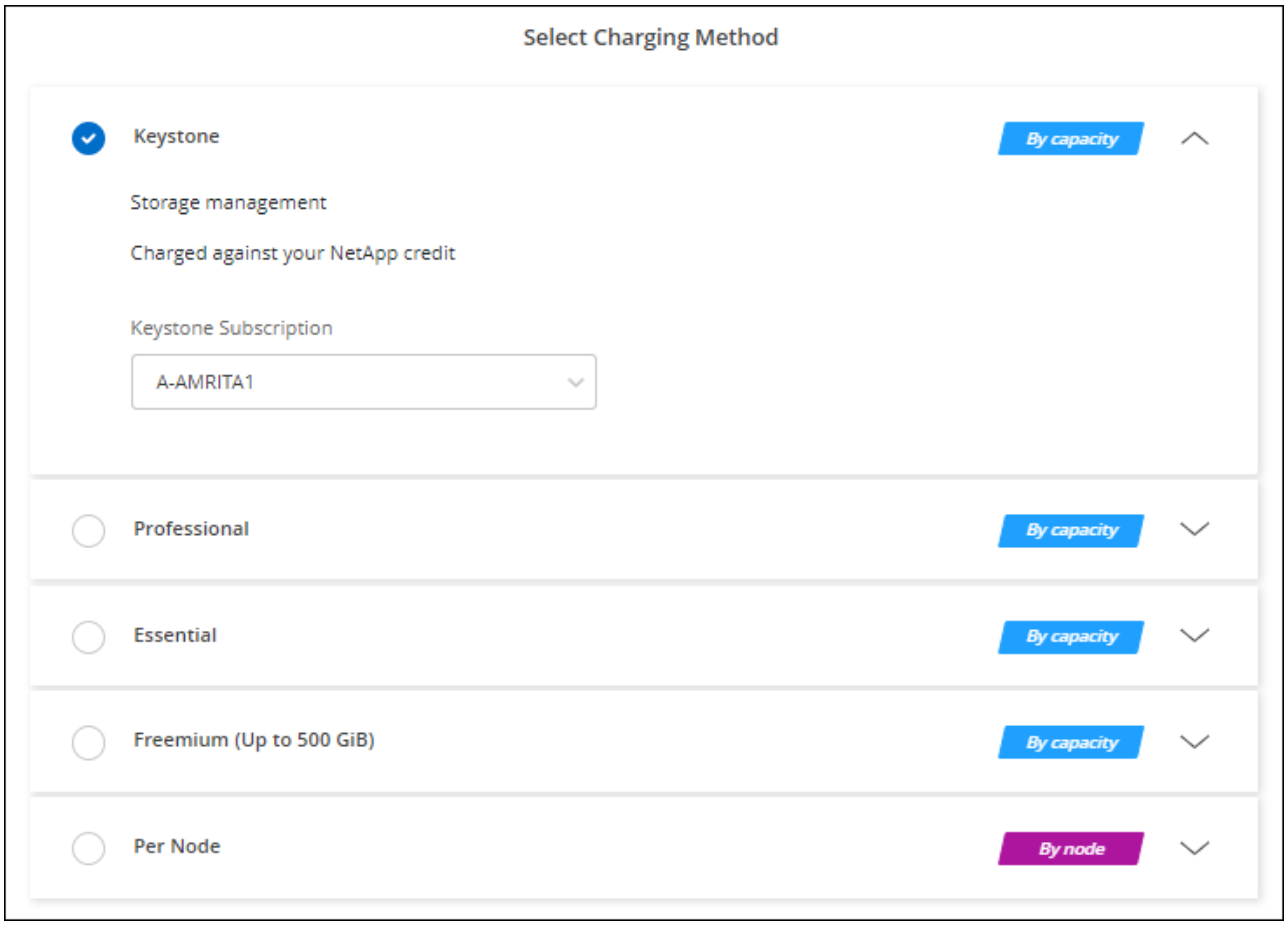

"查看在 Azure 中启动Cloud Volumes ONTAP 的分步说明" 。

**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。<br><br>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：<br><br>• 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。<br>• 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*。

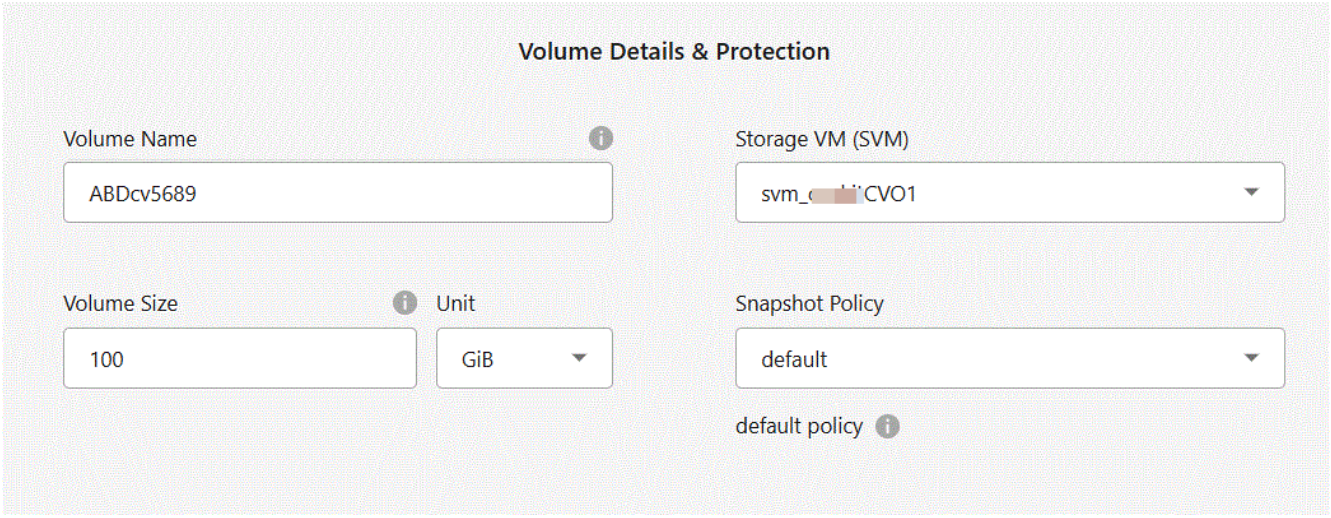
    "了解支持的客户端协议和版本" 。

    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。<br><br>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。<br><br>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：<br><br>• 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。<br>• 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*。

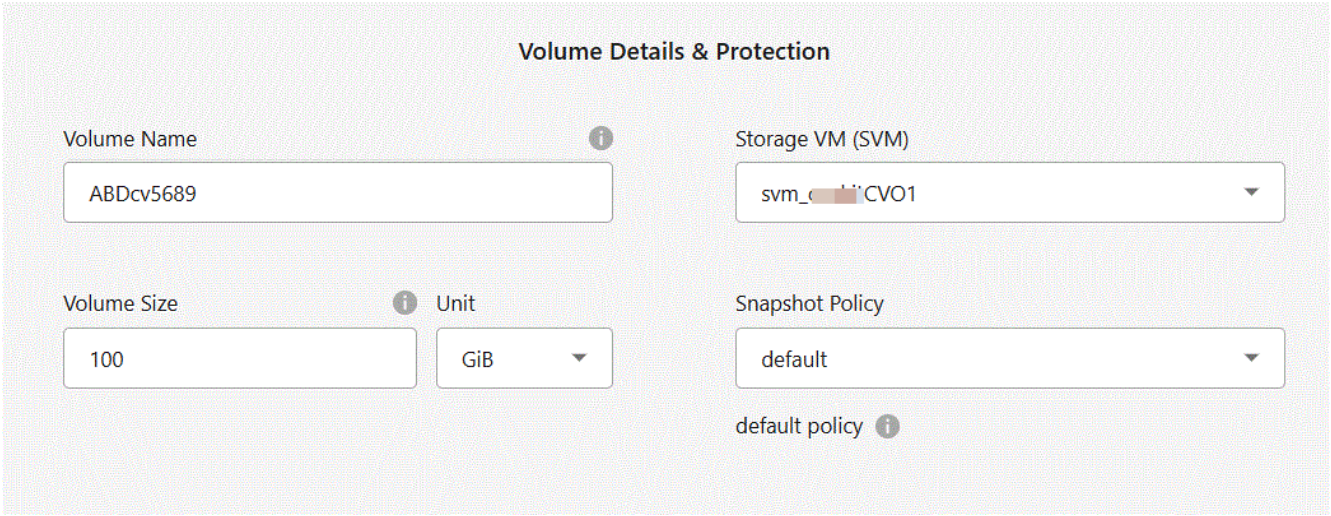
    "了解支持的客户端协议和版本" 。

    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

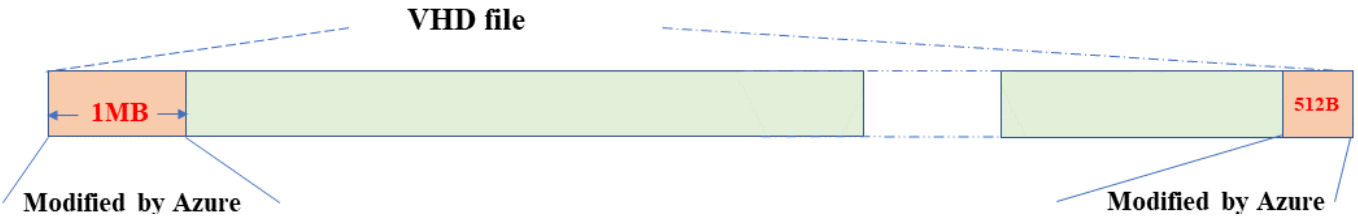
## 针对Cloud Volumes ONTAP 的Azure 市场映像验证

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"

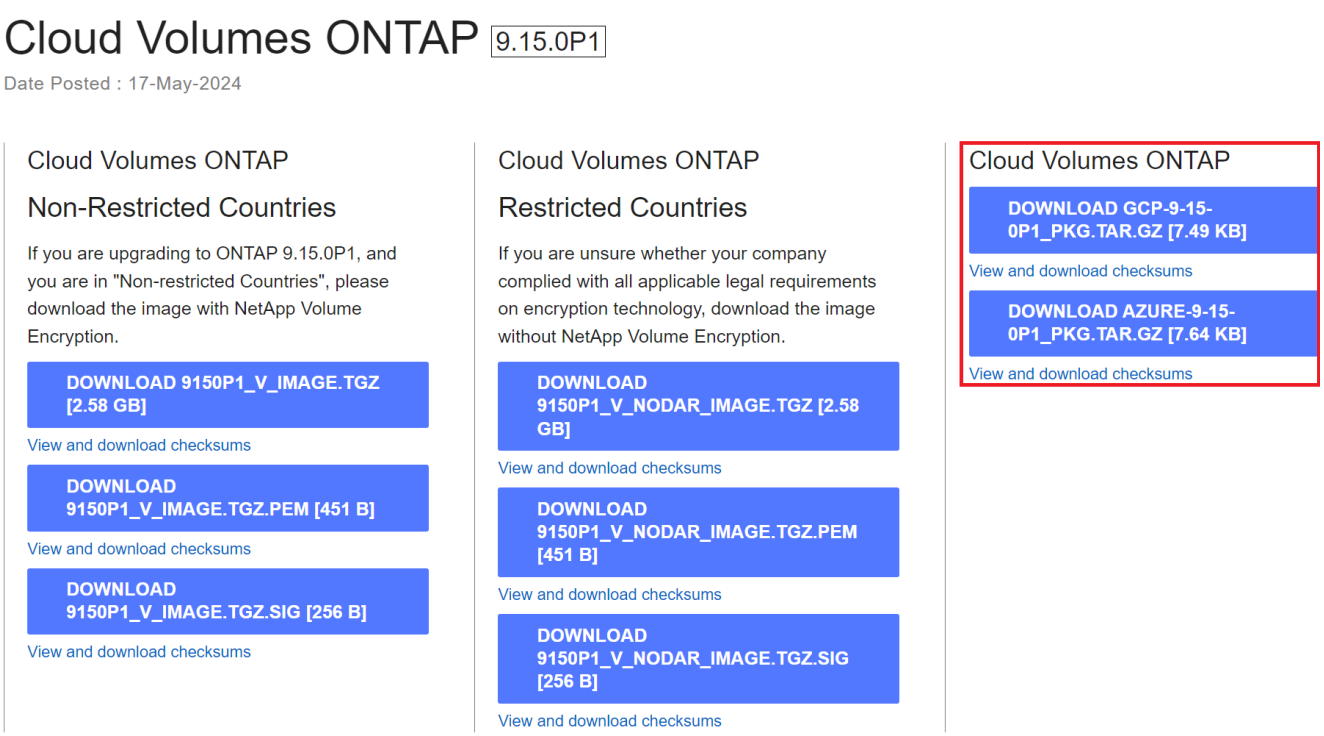
## 下载适用于Cloud Volumes ONTAP 的Azure 映像文件

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": "\"0xXXXXXXXXXXXXXXXXX\"",
  "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-xxxxxxxxxxxx",
      "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
```

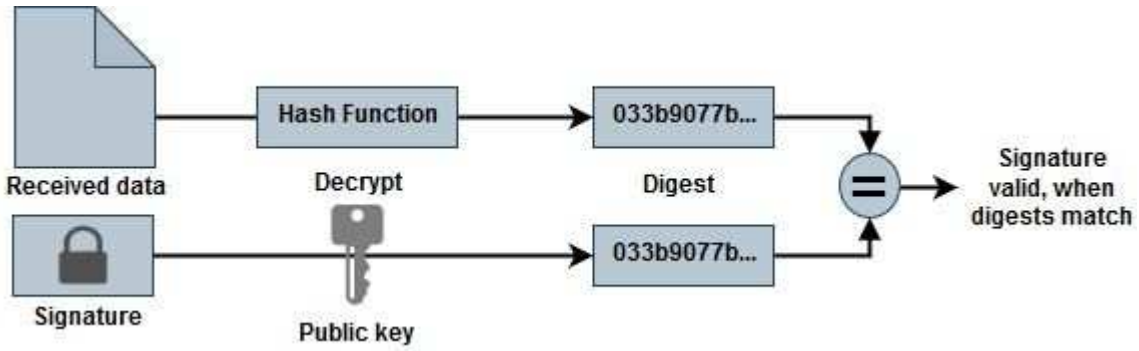
验证文件签名

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"

版权信息

版权所有 © 2026 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本文档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。 美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

商标信息

NetApp、NetApp 标识和 http://www.netapp.com/TM 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。