开始使用 **Microsoft Azure**

Cloud Volumes ONTAP

NetApp
May 12, 2022

目录

开始使用 Microsoft Azure

在 Azure 中快速启动 Cloud Volumes ONTAP

只需几步即可开始使用适用于 Azure 的 Cloud Volumes ONTAP 。

如果您没有 "连接器" 但是，客户管理员需要创建一个。 "了解如何在 Azure 中创建 Connector"。

在创建首个 Cloud Volumes ONTAP 工作环境时，如果尚未部署 Connector ，则 Cloud Manager 会提示您部署一个。

Cloud Manager 可提供符合您的工作负载要求的预配置软件包，您也可以创建自己的配置。如果您选择自己的配置、则应了解可用的选项。 "了解更多信息。"。

跨度 **class="image><img src="https://raw.githubusercontent.com/NetAppDocs/common/main/media/number-3.png" Alt-Three ">** 设置您的网络连接

1. 确保您的 vNet 和子网支持连接器和 Cloud Volumes ONTAP 之间的连接。
2. 从目标 vNet 启用出站 Internet 访问，以便 Connector 和 Cloud Volumes ONTAP 可以联系多个端点。

   此步骤非常重要，因为没有出站 Internet 访问， Connector 无法管理 Cloud Volumes ONTAP 。如果需要限制出站连接，请参阅的端点列表 "连接器和 Cloud Volumes ONTAP"。

"详细了解网络要求"。

单击 * 添加工作环境 * ，选择要部署的系统类型，然后完成向导中的步骤。 "阅读分步说明"。

相关链接

- "使用 Cloud Manager 创建连接器"
- "从 Azure Marketplace 创建 Connector"
- "在 Linux 主机上安装 Connector 软件"
- "Cloud Manager 对权限的作用"

在 Azure 中规划 Cloud Volumes ONTAP 配置

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

查看支持的区域

大多数 Microsoft Azure 地区均支持 Cloud Volumes ONTAP 。 "查看支持的区域的完整列表"。

选择许可证

Cloud Volumes ONTAP 提供了多种许可选项。每个选项都允许您选择一种满足您需求的消费模式。 "了解

Cloud Volumes ONTAP 的许可选项"。

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。

"支持 Azure 中 Cloud Volumes ONTAP 的配置"

了解存储限制

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

"Azure 中 Cloud Volumes ONTAP 的存储限制"

在 Azure 中估算系统规模

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

虚拟机类型

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

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

Azure 磁盘类型

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

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

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

  有关这些磁盘的使用情形的其他详细信息，请参见 "Microsoft Azure 文档： Azure 中提供了哪些磁盘类型？"。

Azure 磁盘大小

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

聚合中的所有磁盘大小必须相同。

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

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

标准存储的磁盘大小之间没有性能差异。应根据需要的容量选择磁盘大小。

有关按磁盘大小显示的 IOPS 和吞吐量，请参见 Azure：

- "Microsoft Azure： 受管磁盘定价"
- "Microsoft Azure： 页面 Blob 定价"

选择支持 **Flash Cache** 的配置

Azure 中的 Cloud Volumes ONTAP 配置包括本地 NVMe 存储， Cloud Volumes ONTAP 使用此存储作为 *Flash Cache* 来提高性能。 "了解有关 Flash Cache 的更多信息"。

查看默认系统磁盘

除了用户数据存储之外， Cloud Manager 还为 Cloud Volumes ONTAP 系统数据（启动数据，根数据，核心数据和 NVRAM ）购买云存储。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"。

此连接器还需要一个系统磁盘。 "查看有关连接器默认配置的详细信息"。

Azure 网络信息工作表

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

Azure 信息	您的价值
Region	
虚拟网络（ VNet ）	
Subnet	
网络安全组（如果使用您自己的组）	

选择写入速度

您可以使用 Cloud Manager 为 Cloud Volumes ONTAP 选择写入速度设置。在选择写入速度之前、您应该了解正常和高设置之间的差异、以及使用高速写入速度时的风险和建议。 "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、可以减少您所需的存储总量。在 Cloud Manager 中创建卷时，您可以选择启用这些功能的配置文件或禁用这些功能的配置文件。您应该了解有关这些功能的更多信息、以帮助您确定要使用的配置文件。

NetApp 存储效率功能具有以下优势：

精简配置

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

重复数据删除

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

压缩

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

Azure 中的 Cloud Volumes ONTAP 的网络要求

设置 Azure 网络，以便 Cloud Volumes ONTAP 系统可以正常运行。其中包括连接器和 Cloud Volumes ONTAP 的网络连接。

Cloud Volumes ONTAP 的要求

在 Azure 中必须满足以下网络连接要求。

出站 Internet 访问

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

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

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

"了解如何验证 AutoSupport"。

IP 地址

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

- 单个节点： 5 个 IP 地址
- HA 对： 16 个 IP 地址

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

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

安全连接到 **Azure** 服务

Cloud Manager 可设置一个 vNet 服务端点和一个 Azure 专用链路端点，以便 Cloud Volumes ONTAP 可以私有连接到 Azure 服务。

服务端点

通过 Cloud Manager ， vNet 服务端点可以创建从 Cloud Volumes ONTAP 到 Azure Blob 存储的安全连接，以便进行数据分层。不支持从 Cloud Volumes ONTAP 到 Azure 服务的其他服务端点。

如果 Cloud Manager 策略具有以下权限，则 Cloud Manager 将为您启用 vNet 服务端点：

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

这些权限包含在最新版本中 "Cloud Manager 策略"。

有关设置数据分层的详细信息，请参见 "将冷数据分层到低成本对象存储"。

私有端点

默认情况下， Cloud Manager 会在 Cloud Volumes ONTAP 及其关联存储帐户之间启用 Azure 专用链路连接。专用链路可确保 Azure 中端点之间的连接安全，并可提供性能优势。在大多数情况下，您无需执行任何操作— Cloud Manager 为您管理 Azure 专用链路。但是，如果您使用 Azure 私有 DNS ，则需要编辑配置文件。如果需要，您还可以禁用专用链路连接。

"了解有关将 Azure 专用链路与 Cloud Volumes ONTAP 结合使用的更多信息"。

连接到其他 **ONTAP** 系统

要在Azure中的Cloud Volumes ONTAP 系统与其他网络中的ONTAP 系统之间复制数据、您必须在Azure vNet与其他网络(例如您的企业网络)之间建立VPN连接。

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

用于 **HA** 互连的端口

Cloud Volumes ONTAP HA 对包括一个 HA 互连，通过该互连，每个节点可以持续检查其配对节点是否正常运行，并镜像另一节点的非易失性内存的日志数据。HA 互连使用 TCP 端口 10006 进行通信。

默认情况下， HA 互连 LIF 之间的通信处于打开状态，并且此端口没有安全组规则。但是，如果在 HA 互连 LIF 之间创建防火墙，则需要确保端口 10006 的 TCP 流量处于打开状态，以便 HA 对可以正常运行。

一个 **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 _dedicated 资源组。一个资源组仅支持一个 HA 对。

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

安全组

您无需创建安全组，因为 Cloud Manager 可以为您创建安全组。如果您需要使用自己的，请参阅下面列出的安全组规则。

安全组规则

Cloud Manager 可创建包含 Cloud Volumes ONTAP 成功运行所需入站和出站规则的 Azure 安全组。您可能希望参考这些端口进行测试或使用自己的安全组。

Cloud Volumes ONTAP 的安全组需要入站和出站规则。

单节点系统的入站规则

除非问题描述注意到它会阻止特定入站流量，否则以下规则允许流量。

优先级和名称	端口和协议	源和目标	**Description**
1000 个 inbound_ssh	22 TCP	任意到任意	SSH 访问集群管理 LIF 或节点管理 LIF 的 IP 地址
1001inbound_http	80/TCP	任意到任意	使用集群管理 LIF 的 IP 地址对系统管理器 Web 控制台进行 HTTP 访问
1002inbound_111_tcp	111 TCP	任意到任意	远程过程调用 NFS
1003 入站 _111_UDP	111 UDP	任意到任意	远程过程调用 NFS
1004 inbound_139	139 TCP	任意到任意	用于 CIFS 的 NetBIOS 服务会话
1005 inbound_161-162_TCP	161-162 TCP	任意到任意	简单网络管理协议
1006 inbound_161-162_UDP	161-162 UDP	任意到任意	简单网络管理协议
1007 inbound_443	443/TCP	任意到任意	使用集群管理 LIF 的 IP 地址对 System Manager Web 控制台进行 HTTPS 访问
1008 inbound_445	445 TCP	任意到任意	Microsoft SMB/CIFS over TCP （通过 TCP ）和 NetBIOS 成帧
1009 inbound_635_tcp	635 TCP	任意到任意	NFS 挂载
1010 inbound_635_udp	635 UDP	任意到任意	NFS 挂载
1011 inbound_749	749 TCP	任意到任意	Kerberos
1012 inbound_2049_tcp	2049 TCP	任意到任意	NFS 服务器守护进程
1013 inbound_2049_udp	2049 UDP	任意到任意	NFS 服务器守护进程
1014 inbound_3260	3260 TCP	任意到任意	通过 iSCSI 数据 LIF 进行 iSCSI 访问

优先级和名称	端口和协议	源和目标	Description
1015 Inbound_4045-4046_tcp	4045-4046 TCP	任意到任意	NFS 锁定守护进程和网络状态监控器
1016 inbound_4045-4046_udp	4045-4046 UDP	任意到任意	NFS 锁定守护进程和网络状态监控器
1017 inbound_10000	10000 TCP	任意到任意	使用 NDMP 备份
1018 inbound_11104-11105	11104-11105 TCP	任意到任意	SnapMirror 数据传输
3000 个 inbound_deny_all_tcp	任何端口 TCP	任意到任意	阻止所有其他 TCP 入站流量
3001 inbound_deny_all_udp	任何端口 UDP	任意到任意	阻止所有其他 UDP 入站流量
65000 个 AllowVnetInBound	任何端口任何协议	VirtualNetwork 到 VirtualNetwork	vNet 中的入站流量
65001 AllowAzureLoadBalancerInBound	任何端口任何协议	AzureLoadBalancer 到任何	来自 Azure 标准负载平衡器的数据流量
65500 DenyAllInBound	任何端口任何协议	任意到任意	阻止所有其他入站流量

HA 系统的入站规则

除非问题描述注意到它会阻止特定入站流量，否则以下规则允许流量。

与单节点系统相比， HA 系统的入站规则更少，因为入站数据流量通过 Azure 标准负载平衡器。因此，来自负载平衡器的流量应处于打开状态，如 "AllowAzureLoadBalancerInBound" 规则中所示。

优先级和名称	端口和协议	源和目标	Description
100 inbound_443	443 任何协议	任意到任意	使用集群管理 LIF 的 IP 地址对 System Manager Web 控制台进行 HTTPS 访问
101 inbound_111_tcp	111 任何协议	任意到任意	远程过程调用 NFS
102 inbound_2049_tcp	2049 任何协议	任意到任意	NFS 服务器守护进程
111 inbound_ssh	22 任何协议	任意到任意	SSH 访问集群管理 LIF 或节点管理 LIF 的 IP 地址
121 inbound_53	53 任何协议	任意到任意	DNS 和 CIFS
65000 个 AllowVnetInBound	任何端口任何协议	VirtualNetwork 到 VirtualNetwork	vNet 中的入站流量
65001 AllowAzureLoadBalancerInBound	任何端口任何协议	AzureLoadBalancer 到任何	来自 Azure 标准负载平衡器的数据流量
65500 DenyAllInBound	任何端口任何协议	任意到任意	阻止所有其他入站流量

出站规则

为 Cloud Volumes ONTAP 预定义的安全组将打开所有出站流量。如果可以接受，请遵循基本出站规则。如果您需要更严格的规则、请使用高级出站规则。

基本外向规则

为 Cloud Volumes ONTAP 预定义的安全组包括以下出站规则。

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

高级出站规则

如果您需要严格的出站流量规则、则可以使用以下信息仅打开 Cloud Volumes ONTAP 出站通信所需的端口。

源是 Cloud Volumes ONTAP 系统上的接口（ IP 地址）。

服务	Port	协议	源	目标	目的
Active Directory	88	TCP	节点管理 LIF	Active Directory 目录林	Kerberos V 身份验证
	137.	UDP	节点管理 LIF	Active Directory 目录林	NetBIOS 名称服务
	138.	UDP	节点管理 LIF	Active Directory 目录林	NetBIOS 数据报服务
	139.	TCP	节点管理 LIF	Active Directory 目录林	NetBIOS 服务会话
	389.	TCP 和 UDP	节点管理 LIF	Active Directory 目录林	LDAP
	445	TCP	节点管理 LIF	Active Directory 目录林	Microsoft SMB/CIFS over TCP （通过 TCP ）和 NetBIOS 成帧
	464.	TCP	节点管理 LIF	Active Directory 目录林	Kerberos V 更改和设置密码（ set_change ）
	464.	UDP	节点管理 LIF	Active Directory 目录林	Kerberos 密钥管理
	749	TCP	节点管理 LIF	Active Directory 目录林	Kerberos V 更改和设置密码（ RPCSEC_GSS ）
	88	TCP	数据 LIF （ NFS ， CIFS ， iSCSI ）	Active Directory 目录林	Kerberos V 身份验证
	137.	UDP	数据 LIF （ NFS 、 CIFS ）	Active Directory 目录林	NetBIOS 名称服务
	138.	UDP	数据 LIF （ NFS 、 CIFS ）	Active Directory 目录林	NetBIOS 数据报服务
	139.	TCP	数据 LIF （ NFS 、 CIFS ）	Active Directory 目录林	NetBIOS 服务会话
	389.	TCP 和 UDP	数据 LIF （ NFS 、 CIFS ）	Active Directory 目录林	LDAP
	445	TCP	数据 LIF （ NFS 、 CIFS ）	Active Directory 目录林	Microsoft SMB/CIFS over TCP （通过 TCP ）和 NetBIOS 成帧
	464.	TCP	数据 LIF （ NFS 、 CIFS ）	Active Directory 目录林	Kerberos V 更改和设置密码（ set_change ）
	464.	UDP	数据 LIF （ NFS 、 CIFS ）	Active Directory 目录林	Kerberos 密钥管理
	749	TCP	数据 LIF （ NFS 、 CIFS ）	Active Directory 目录林	Kerberos V 更改和设置密码（ RPCSEC_GSS ）
AutoSupport	HTTPS	443.	节点管理 LIF	support.netapp.com	AutoSupport （默认设置为 HTTPS ）
	HTTP	80	节点管理 LIF	support.netapp.com	AutoSupport （仅当传输协议从 HTTPS 更改为 HTTP 时）

服务	Port	协议	源	目标	目的
DHCP	68	UDP	节点管理 LIF	DHCP	首次设置 DHCP 客户端
DHCP	67	UDP	节点管理 LIF	DHCP	DHCP 服务器
DNS	53.	UDP	节点管理 LIF 和数据 LIF （ NFS 、 CIFS ）	DNS	DNS
NDMP	18600 – 18699	TCP	节点管理 LIF	目标服务器	NDMP 副本
SMTP	25.	TCP	节点管理 LIF	邮件服务器	SMTP 警报、可用于 AutoSupport
SNMP	161.	TCP	节点管理 LIF	监控服务器	通过 SNMP 陷阱进行监控
	161.	UDP	节点管理 LIF	监控服务器	通过 SNMP 陷阱进行监控
	162.	TCP	节点管理 LIF	监控服务器	通过 SNMP 陷阱进行监控
	162.	UDP	节点管理 LIF	监控服务器	通过 SNMP 陷阱进行监控
SnapMirror	11104.	TCP	集群间 LIF	ONTAP 集群间 LIF	管理 SnapMirror 的集群间通信会话
	11105.	TCP	集群间 LIF	ONTAP 集群间 LIF	SnapMirror 数据传输
系统日志	514.	UDP	节点管理 LIF	系统日志服务器	系统日志转发消息

连接器的要求

设置您的网络，以便 Connector 能够管理公有云环境中的资源和流程。最重要的步骤是确保对各种端点的出站 Internet 访问。

如果您的网络使用代理服务器与 Internet 进行所有通信，则可以从设置页面指定代理服务器。请参见 "将 Connector 配置为使用代理服务器"。

连接到目标网络

连接器要求与要部署 Cloud Volumes ONTAP 的 VPC 和 VN 集建立网络连接。

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

出站 **Internet** 访问

连接器需要通过出站 Internet 访问来管理公有云环境中的资源和流程。

端点	目的
https://support.netapp.com	获取许可信息并向 NetApp 支持部门发送 AutoSupport 消息。
https://*.cloudmanager.cloud.netapp.com	在 Cloud Manager 中提供 SaaS 功能和服务。
https://cloudmanagerinfraprod.azurecr.io https://*.blob.core.windows.net	升级 Connector 及其 Docker 组件。

安全组规则

Connector 的安全组需要入站和出站规则。

入站规则

Port	协议	目的
22.	SSH	提供对 Connector 主机的 SSH 访问
80	HTTP	提供从客户端 Web 浏览器到本地用户界面的 HTTP 访问
443.	HTTPS	提供从客户端 Web 浏览器到本地用户界面的 HTTPS 访问

出站规则

连接器的预定义安全组将打开所有出站流量。如果可以接受，请遵循基本出站规则。如果您需要更严格的规则、请使用高级出站规则。

基本外向规则

Connector 的预定义安全组包括以下出站规则。

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

高级出站规则

如果您需要对出站流量设置严格的规则，则可以使用以下信息仅打开 Connector 进行出站通信所需的端口。

源 IP 地址是 Connector 主机。

服务	Port	协议	目标	目的
API 调用和 AutoSupport	443.	HTTPS	出站 Internet 和 ONTAP 集群管理 LIF	API调用Azure 和ONTAP 、云数据感知、勒索软件服务以及向NetApp发送AutoSupport 消息
DNS	53.	UDP	DNS	用于云管理器进行 DNS 解析

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

数据会使用在 Azure 中的 Cloud Volumes ONTAP 上自动加密 "Azure 存储服务加密" 使用 Microsoft 管理的密钥。但是，您可以按照此页面上的步骤使用自己的加密密钥。

数据加密概述

Cloud Volumes ONTAP 数据在 Azure 中使用自动加密 "Azure 存储服务加密"。默认实施使用 Microsoft 管理的密钥。无需设置。

如果要在 Cloud Volumes ONTAP 中使用客户管理的密钥，则需要完成以下步骤：

1. 从 Azure 创建密钥存储，然后在该存储中生成密钥
2. 在 Cloud Manager 中，使用 API 创建使用密钥的 Cloud Volumes ONTAP 工作环境

密钥轮换

如果创建新版本的密钥， Cloud Volumes ONTAP 将自动使用最新版本的密钥。

如何对数据进行加密

创建配置为使用客户管理的密钥的 Cloud Volumes ONTAP 工作环境后， Cloud Volumes ONTAP 数据将按如下所示进行加密。

HA 对

- 适用于 Cloud Volumes ONTAP 的所有 Azure 存储帐户均使用客户管理的密钥进行加密。
- 任何新存储帐户（例如，添加磁盘或聚合时）也会使用相同的密钥。

单个节点

- 适用于 Cloud Volumes ONTAP 的所有 Azure 存储帐户均使用客户管理的密钥进行加密。
- 对于根磁盘，启动磁盘和数据磁盘， Cloud Manager 使用 "磁盘加密集"，用于管理具有受管磁盘的加密密钥。
- 任何新数据磁盘也会使用相同的磁盘加密集。
- NVRAM 和核心磁盘会使用 Microsoft 管理的密钥进行加密，而不是使用客户管理的密钥进行加密。

创建密钥存储并生成密钥

密钥存储必须位于您计划创建 Cloud Volumes ONTAP 系统的同一 Azure 订阅和区域中。

步骤

1. "在 Azure 订阅中创建密钥存储"。

   请注意密钥存储的以下要求：

   - 密钥存储必须与 Cloud Volumes ONTAP 系统位于同一区域。
   - 应启用以下选项：
     - * 软删除 *（默认情况下，此选项处于启用状态，但必须禁用 *not* ）
     - * 清除保护 *
     - * 用于卷加密的 Azure 磁盘加密 *（仅适用于单节点 Cloud Volumes ONTAP 系统）
2. "在密钥存储中生成密钥"。

请注意此密钥的以下要求：

- 密钥类型必须为 * RSA * 。
- 建议的 RSA 密钥大小为 * 2048 * ，但支持其他大小。

创建一个使用加密密钥的工作环境

创建密钥存储并生成加密密钥后，您可以创建一个配置为使用此密钥的新 Cloud Volumes ONTAP 系统。使用 Cloud Manager API 可支持这些步骤。

如果要在单节点 Cloud Volumes ONTAP 系统中使用客户管理的密钥，请确保 Cloud Manager Connector 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"
```

您可以在上找到最新的权限列表 "Cloud Manager 策略页面"。

HA 对不需要这些权限。

步骤

1. 使用以下 Cloud Manager API 调用获取 Azure 订阅中的密钥存储列表。

   对于 HA 对： `get /azure/ha/metadata/vaults`

   对于单个节点： `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 Cloud Manager API 调用获取存储中的密钥列表。

   对于 HA 对： `get /azure/ha/metadata/keys-vault`

   对于单个节点： `get /azure/vsa/metadata/keys-vault`

   记下 * 密钥名称 * 。您需要在下一步中指定该值（以及存储名称）。

   "了解有关此 API 调用的更多信息"。

3. 使用以下 Cloud Manager API 调用创建 Cloud Volumes ONTAP 系统。

   a. 对于 HA 对：

发布 `/azure/ha/cluster-environments`

请求正文必须包含以下字段：

```
"azureEncryptionParameters": {
       "key": "keyName",
       "vaultName": "vaultName"
}
```

"了解有关此 API 调用的更多信息"。

b. 对于单节点系统：

发布 `/azure/vsa/cluster-environments`

请求正文必须包含以下字段：

```
"azureEncryptionParameters": {
       "key": "keyName",
       "vaultName": "vaultName"
}
```

+
"了解有关此 API 调用的更多信息"。

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 中启动 Cloud Volumes ONTAP

您可以通过在 Cloud Manager 中创建 Cloud Volumes ONTAP 工作环境在 Azure 中启动单节点系统或 HA 对。

要创建工作环境，您需要满足以下要求。

- 已启动且正在运行的连接器。
  - 您应具有 "与工作空间关联的连接器"。
  - "您应做好准备，使 Connector 始终保持运行"。
- 了解要使用的配置。

  您应已选择配置并从管理员处获取 Azure 网络信息。有关详细信息，请参见 "规划 Cloud Volumes ONTAP 配置"。
- 了解在添加工作环境向导中选择特定许可选项所需的条件。 "了解有关 Cloud Volumes ONTAP 许可的更多信息"。

许可选项	要求	如何满足要求
免费	需要提供 Marketplace 订阅或 NetApp 支持站点（ NSS ）帐户。	您可以从 * 详细信息和凭据 * 页面订阅云提供商的市场。您可以在 * 充电方法和 NSS 帐户 * 页面上输入 NSS 帐户。
专业或基本软件包	需要 Marketplace 订阅或基于容量的许可证（ BYOL ）。如果您的帐户没有有效的基于容量的许可证，或者您配置的容量超过许可容量，则建议使用 Marketplace 订阅进行基于容量的收费。	您可以从 * 详细信息和凭据 * 页面订阅云提供商的市场。如果要使用从 NetApp 购买的基于容量的许可证（ BYOL ），必须先将其添加到 * 数字电子钱包 * 中。 "了解如何添加基于容量的 BYOL 许可证"。
Keystone Flex 订阅	您的帐户必须获得授权，并且必须启用订阅才能在 Cloud Volumes ONTAP 中使用。	a. mailto： ng-keystone-success@netapp.com （联系 NetApp ）授权您的 Cloud Manager 用户帐户订阅一个或多个 Keystone Flex 订阅。 b. 在 NetApp 授权您的帐户后， "链接您的订阅以用于 Cloud Volumes ONTAP"。 c. 创建 Cloud Volumes ONTAP HA 对时，请选择 Keystone Flex 订阅收费方法。
按节点许可	需要订阅 Marketplace ，或者您需要自带许可证（ BYOL ）。具有现有订阅或现有许可证的客户可以使用此选项。它不适用于新客户。	如果要使用从 NetApp 购买的基于节点的许可证（ BYOL ），必须先将其添加到 * 数字电子钱包 * 中。 "了解如何添加基于节点的 BYOL 许可证"。您可以在 * 充电方法和 NSS 帐户 * 页面上输入 NSS 帐户。

当 Cloud Manager 在 Azure 中创建 Cloud Volumes ONTAP 系统时，它会创建多个 Azure 对象，例如资源组，网络接口和存储帐户。您可以在向导结束时查看资源摘要。

可能会丢失数据

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，建议不要在现有共享资源组中部署 Cloud Volumes ONTAP 。虽然 Cloud Manager 可以在部署失败或删除时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。

步骤

1. 【订阅】在 " 画布 " 页面上，单击 * 添加工作环境 * 并按照提示进行操作。
2. * 选择位置 * ：选择 * Microsoft Azure* 和 * Cloud Volumes ONTAP 单节点 * 或 * Cloud Volumes ONTAP 高可用性 * 。
3. 如果出现提示， "创建连接器"。
4. * 详细信息和凭据 * ：可选择更改 Azure 凭据和订阅，指定集群名称，根据需要添加标记，然后指定凭据。

   下表介绍了可能需要指导的字段：

字段	Description
工作环境名称	Cloud Manager 使用工作环境名称来命名 Cloud Volumes ONTAP 系统和 Azure 虚拟机。如果您选择了预定义安全组的前缀，则它还会使用该名称作为前缀。
资源组标记	标记是 Azure 资源的元数据。在此字段中输入标记后， Cloud Manager 会将其添加到与 Cloud Volumes ONTAP 系统关联的资源组中。在创建工作环境时，最多可以从用户界面添加四个标签，然后可以在创建工作环境后添加更多标签。请注意，在创建工作环境时， API 不会将您限制为四个标记。有关标记的信息，请参见 "Microsoft Azure 文档：使用标记组织 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 System Manager 或其命令行界面连接到 Cloud Volumes ONTAP 。保留默认的 *admin* 用户名或将其更改为自定义用户名。
【视频】编辑凭据	您可以选择不同的 Azure 凭据和不同的 Azure 订阅以用于此 Cloud Volumes ONTAP 系统。您需要将 Azure Marketplace 订阅与选定 Azure 订阅关联，才能部署按需购买的 Cloud Volumes ONTAP 系统。 "了解如何添加凭据"。

以下视频显示了如何将 Marketplace 订阅与 Azure 订阅关联：

► https://docs.netapp.com/zh-cn/cloud-manager-cloud-volumes-

ontap//media/video_subscribing_azure.mp4 *(video)*

5. * 服务 * ： 保持服务处于启用状态或禁用不想在 Cloud Volumes ONTAP 中使用的单个服务。
   - "了解有关 Cloud Data sense 的更多信息"。
   - "了解有关 Cloud Backup 的更多信息"。
   - "了解有关监控服务的更多信息"。
6. * 位置和连接 * ： 选择一个位置，一个资源组，一个安全组，然后选中此复选框以确认连接器与目标位置之间的网络连接。

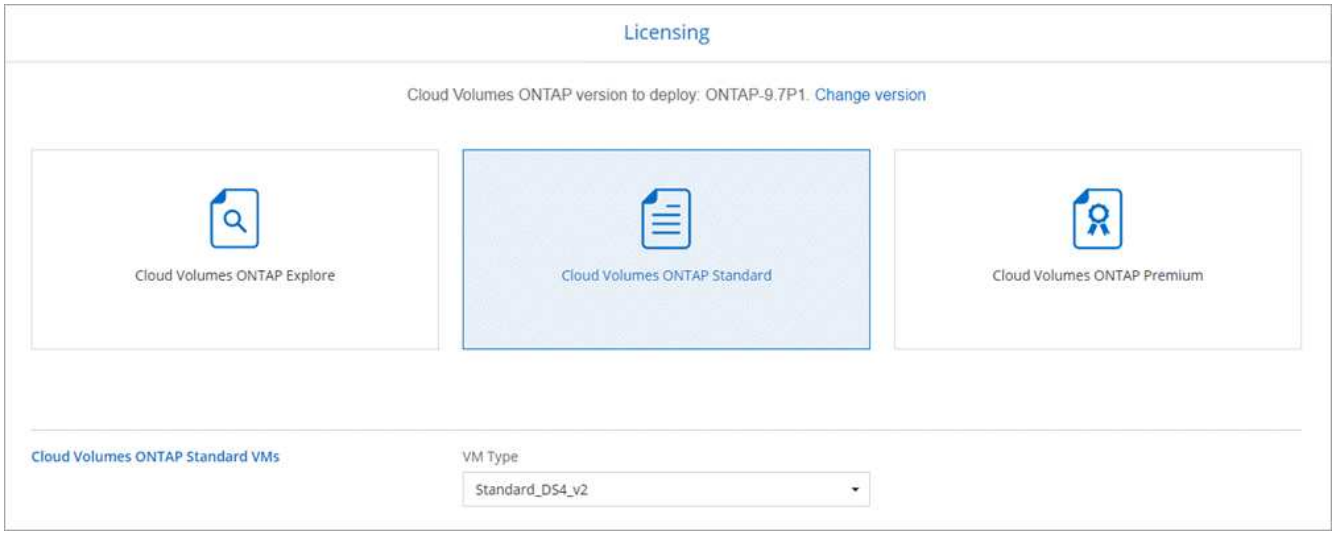
   下表介绍了可能需要指导的字段：

字段	Description
位置	对于单节点系统，您可以选择要在其中部署 Cloud Volumes ONTAP 的可用性区域。如果不选择 AZ ， Cloud Manager 将为您选择一个。
Resource Group	为 Cloud Volumes ONTAP 创建新资源组或使用现有资源组。最佳实践是为 Cloud Volumes ONTAP 使用新的专用资源组。虽然可以在现有共享资源组中部署 Cloud Volumes ONTAP ，但由于存在数据丢失的风险，建议不要这样做。有关详细信息，请参见上述警告。 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，则 Cloud Manager 会遇到连接问题。 如果您正在使用的 Azure 帐户具有 "所需权限"，在部署失败或删除时， Cloud Manager 会从资源组中删除 Cloud Volumes ONTAP 资源。
安全组	如果选择现有安全组，则该组必须满足 Cloud Volumes ONTAP 要求。 "查看默认安全组"。

7. * 充电方法和 NSS 帐户 * ： 指定要在此系统中使用的充电选项，然后指定 NetApp 支持站点帐户。
   - "了解这些充电方法"。
   - "在向导中了解要使用的许可方法的要求"。
8. * 预配置软件包 * ： 选择一个软件包以快速部署 Cloud Volumes ONTAP 系统，或者单击 * 创建自己的配置 * 。

   如果选择其中一个包、则只需指定卷、然后检查并批准配置。

9. * 许可 * ： 根据需要更改 Cloud Volumes ONTAP 版本，选择许可证并选择虚拟机类型。



如果在启动系统后需要更改、您可以稍后修改许可证或虚拟机类型。

> 如果选定版本有较新的候选版本、一般可用性或修补程序版本可用、则在创建工作环境时，Cloud Manager 会将系统更新为该版本。例如，如果您选择 Cloud Volumes ONTAP 9.6 RC1 和 9.6 GA 可用，则会发生此更新。更新不会从一个版本更新到另一个版本，例如从 9.6 到 9.7 。

10. * 订阅 Azure Marketplace * ：如果 Cloud Manager 无法启用 Cloud Volumes ONTAP 的编程部署，请按照以下步骤操作。
11. * 底层存储资源 * ：选择初始聚合的设置：磁盘类型，每个磁盘的大小以及是否应启用到 Blob 存储的数据分层。

    请注意以下事项：

    - 磁盘类型用于初始卷。您可以为后续卷选择不同的磁盘类型。
    - 磁盘大小适用于初始聚合中的所有磁盘以及使用 Simple Provisioning （简单配置）选项时 Cloud Manager 创建的任何其他聚合。您可以使用高级分配选项创建使用不同磁盘大小的聚合。

      有关选择磁盘类型和大小的帮助，请参见 "在 Azure 中估算系统规模"。
    - 您可以在创建或编辑卷时选择特定的卷分层策略。
    - 如果禁用数据分层，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。"。
12. * 写入速度和 WORM* （仅限单节点系统）：选择 * 正常 * 或 * 高 * 写入速度，并根据需要激活一次写入，多次读取（ WORM ）存储。

    "了解有关写入速度的更多信息。"。

    如果启用了 Cloud Backup 或启用了数据分层，则无法启用 WORM 。

    "了解有关 WORM 存储的更多信息。"。
13. * 安全通信到存储和 WORM* （仅限 HA ）：选择是否启用与 Azure 存储帐户的 HTTPS 连接，并根据需要

激活一次写入，多次读取（ WORM ）存储。

HTTPS 连接从 Cloud Volumes ONTAP 9.7 HA 对连接到 Azure 存储帐户。请注意，启用此选项可能会影响写入性能。创建工作环境后，您无法更改此设置。

"了解有关 WORM 存储的更多信息。"。

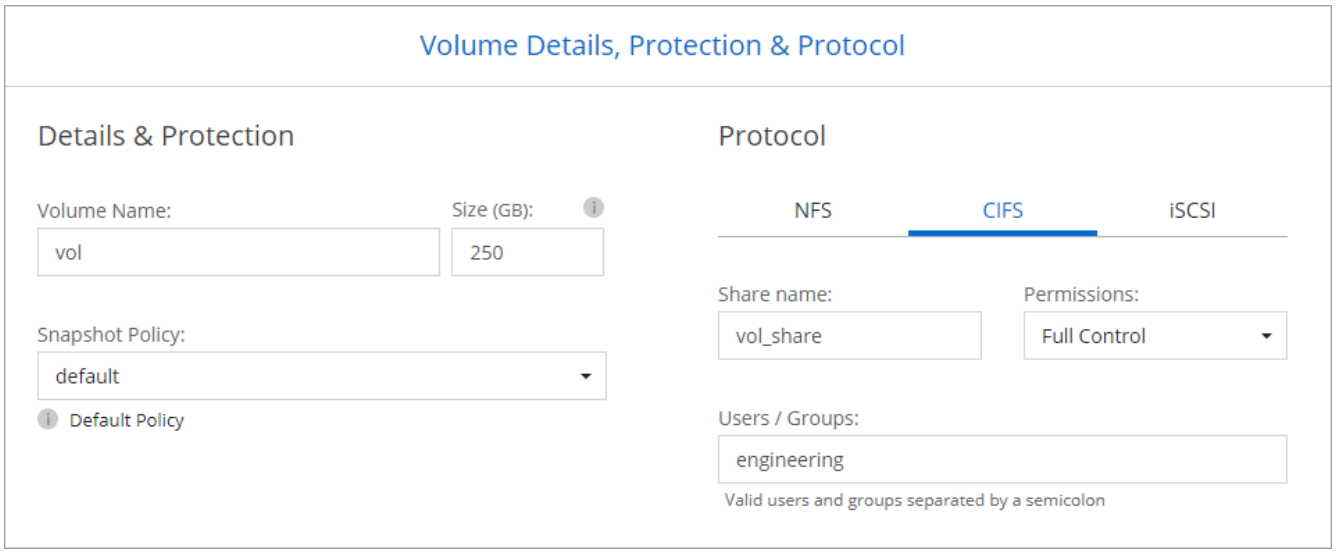
14. * 创建卷 * ：输入新卷的详细信息或单击 * 跳过 * 。

"了解支持的客户端协议和版本"。

本页中的某些字段是不言自明的。下表介绍了可能需要指导的字段：

字段	Description
Size	您可以输入的最大大小在很大程度上取决于您是否启用精简配置、这样您就可以创建一个大于当前可用物理存储的卷。
访问控制（仅适用于 NFS ）	导出策略定义子网中可以访问卷的客户端。默认情况下， Cloud Manager 会输入一个值、用于访问子网中的所有实例。
权限和用户 / 组（仅限 CIFS ）	这些字段使您能够控制用户和组对共享的访问级别（也称为访问控制列表或 ACL ）。您可以指定本地或域 Windows 用户或组、 UNIX 用户或组。如果指定域 Windows 用户名，则必须使用 domain\username 格式包含用户的域。
快照策略	Snapshot 副本策略指定自动创建的 NetApp Snapshot 副本的频率和数量。NetApp Snapshot 副本是一个时间点文件系统映像、对性能没有影响、并且只需要极少的存储。您可以选择默认策略或无。您可以为瞬态数据选择无：例如， Microsoft SQL Server 的 tempdb 。
高级选项（仅适用于 NFS ）	为卷选择 NFS 版本： NFSv3 或 NFSv4 。
启动程序组和 IQN （仅适用于 iSCSI ）	iSCSI 存储目标称为 LUN （逻辑单元），并作为标准块设备提供给主机。启动程序组是包含 iSCSI 主机节点名称的表，用于控制哪些启动程序可以访问哪些 LUN 。iSCSI 目标通过标准以太网网络适配器（ NIC ），带软件启动程序的 TCP 卸载引擎（ TOE ）卡，融合网络适配器（ CNA ）或专用主机总线适配器（ HBA ）连接到网络，并通过 iSCSI 限定名称（ IQN ）进行标识。创建 iSCSI 卷时， Cloud Manager 会自动为您创建 LUN 。我们通过为每个卷仅创建一个 LUN 来简化此过程，因此无需进行管理。创建卷后， "使用 IQN 从主机连接到 LUN"。

下图显示了已填写 CIFS 协议的卷页面：



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

字段	Description
DNS 主 IP 地址和次 IP 地址	为 CIFS 服务器提供名称解析的 DNS 服务器的 IP 地址。列出的 DNS 服务器必须包含为 CIFS 服务器将加入的域定位 Active Directory LDAP 服务器和域控制器所需的服务位置记录（服务位置记录）。
要加入的 Active Directory 域	您希望 CIFS 服务器加入的 Active Directory （ AD ）域的 FQDN 。
授权加入域的凭据	具有足够权限将计算机添加到 AD 域中指定组织单位 (OU) 的 Windows 帐户的名称和密码。
CIFS server NetBIOS name	在 AD 域中唯一的 CIFS 服务器名称。
组织单位	AD 域中要与 CIFS 服务器关联的组织单元。默认值为 cn = computers 。要将 Azure AD 域服务配置为 Cloud Volumes ONTAP 的 AD 服务器，应在此字段中输入 * OU=ADDC Computers * 或 * OU=ADDC Users* 。https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou["Azure 文档：在 Azure AD 域服务托管域中创建组织单位（ OU ）"^]
DNS 域	Cloud Volumes ONTAP Storage Virtual Machine （ SVM ）的 DNS 域。在大多数情况下，域与 AD 域相同。
NTP 服务器	选择 * 使用 Active Directory 域 * 以使用 Active Directory DNS 配置 NTP 服务器。如果需要使用其他地址配置 NTP 服务器，则应使用 API 。请参见 "Cloud Manager 自动化文档" 了解详细信息。请注意，只有在创建 CIFS 服务器时才能配置 NTP 服务器。在创建 CIFS 服务器后，它不可配置。

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，并根据需要更改卷分层策略。

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

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. 单击 * 更多信息 * 以查看有关支持和 Cloud Manager 将购买的 Azure 资源的详细信息。

c. 选中 * 我了解 …* 复选框。

d. 单击 * 执行 * 。

Cloud Manager 部署了 Cloud Volumes ONTAP 系统。您可以跟踪时间链中的进度。

如果您在部署 Cloud Volumes ONTAP 系统时遇到任何问题、请查看故障消息。您也可以选择工作环境并单击 * 重新创建环境 * 。

要获得更多帮助，请转至 "NetApp Cloud Volumes ONTAP 支持"。

完成后

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

  配额允许您限制或跟踪用户、组或 qtree 使用的磁盘空间和文件数量。