Get started in Azure

Cloud Manager

NetApp
October 11, 2021

Table of Contents

Get started in Azure

Getting started with Cloud Volumes ONTAP for Azure

Get started with Cloud Volumes ONTAP for Azure in a few steps.

Create a Connector

If you don't have a Connector yet, an Account Admin needs to create one. Learn how to create a Connector in Azure.

When you create your first Cloud Volumes ONTAP working environment, Cloud Manager prompts you to deploy a Connector if you don't have one yet.

Plan your configuration

Cloud Manager offers preconfigured packages that match your workload requirements, or you can create your own configuration. If you choose your own configuration, you should understand the options available to you. Learn more.

Set up your networking

a. Ensure that your VNet and subnets will support connectivity between the Connector and Cloud Volumes ONTAP.

b. Enable outbound internet access from the target VNet so the Connector and Cloud Volumes ONTAP can contact several endpoints.

   This step is important because the Connector can't manage Cloud Volumes ONTAP without outbound internet access. If you need to limit outbound connectivity, refer to the list of endpoints for the Connector and Cloud Volumes ONTAP.

Learn more about networking requirements.

Launch Cloud Volumes ONTAP using Cloud Manager

Click **Add Working Environment**, select the type of system that you would like to deploy, and complete the steps in the wizard. Read step-by-step instructions.

Related links

- Evaluating
- Creating a Connector from Cloud Manager
- Creating a Connector from the Azure Marketplace
- Installing the Connector software on a Linux host

- What Cloud Manager does with Azure permissions

Planning your Cloud Volumes ONTAP configuration in Azure

When you deploy Cloud Volumes ONTAP in Azure, you can choose a preconfigured system that matches your workload requirements, or you can create your own configuration. If you choose your own configuration, you should understand the options available to you.

Choosing a license type

Cloud Volumes ONTAP is available in two pricing options: pay-as-you-go and Bring Your Own License (BYOL). For pay-as-you-go, you can choose from three licenses: Explore, Standard, or Premium. Each license provides different capacity and compute options.

Supported configurations for Cloud Volumes ONTAP in Azure

Supported VM types

Cloud Volumes ONTAP supports several VM types, depending on the license type that you choose.

Supported configurations for Cloud Volumes ONTAP in Azure

Understanding storage limits

The raw capacity limit for a Cloud Volumes ONTAP system is tied to the license. Additional limits impact the size of aggregates and volumes. You should be aware of these limits as you plan your configuration.

Storage limits for Cloud Volumes ONTAP in Azure

Sizing your system in Azure

Sizing your Cloud Volumes ONTAP system can help you meet requirements for performance and capacity. You should be aware of a few key points when choosing a VM type, disk type, and disk size:

Virtual machine type

Look at the supported virtual machine types in the Cloud Volumes ONTAP Release Notes and then review details about each supported VM type. Be aware that each VM type supports a specific number of data disks.

- Azure documentation: General purpose virtual machine sizes
- Azure documentation: Memory optimized virtual machine sizes

Azure disk type

When you create volumes for Cloud Volumes ONTAP, you need to choose the underlying cloud storage that Cloud Volumes ONTAP uses as a disk.

HA systems use Premium page blobs. Meanwhile, single node systems can use two types of Azure Managed Disks:

- *Premium SSD Managed Disks* provide high performance for I/O-intensive workloads at a higher cost.
- *Standard SSD Managed Disks* provide consistent performance for workloads that require low IOPS.
- *Standard HDD Managed Disks* are a good choice if you don't need high IOPS and want to reduce your costs.

  For additional details about the use cases for these disks, see Microsoft Azure Documentation: What disk types are available in Azure?.

Azure disk size

When you launch Cloud Volumes ONTAP instances, you must choose the default disk size for aggregates. Cloud Manager uses this disk size for the initial aggregate, and for any additional aggregates that it creates when you use the simple provisioning option. You can create aggregates that use a disk size different from the default by using the advanced allocation option.

All disks in an aggregate must be the same size.

When choosing a disk size, you should take several factors into consideration. The disk size impacts how much you pay for storage, the size of volumes that you can create in an aggregate, the total capacity available to Cloud Volumes ONTAP, and storage performance.

The performance of Azure Premium Storage is tied to the disk size. Larger disks provide higher IOPS and throughput. For example, choosing 1 TiB disks can provide better performance than 500 GiB disks, at a higher cost.

There are no performance differences between disk sizes for Standard Storage. You should choose disk size based on the capacity that you need.

Refer to Azure for IOPS and throughput by disk size:

- Microsoft Azure: Managed Disks pricing
- Microsoft Azure: Page Blobs pricing

Choosing a configuration that supports Flash Cache

A Cloud Volumes ONTAP configuration in Azure includes local NVMe storage, which Cloud Volumes ONTAP uses as *Flash Cache* for better performance. Learn more about Flash Cache.

Azure network information worksheet

When you deploy Cloud Volumes ONTAP in Azure, you need to specify details about your virtual network. You can use a worksheet to collect the information from your administrator.

Azure information	Your value
Region	
Virtual network (VNet)	
Subnet	
Network security group (if using your own)	

Choosing a write speed

Cloud Manager enables you to choose a write speed setting for Cloud Volumes ONTAP. Before you choose a write speed, you should understand the differences between the normal and high settings and risks and recommendations when using high write speed. Learn more about write speed.

Choosing a volume usage profile

ONTAP includes several storage efficiency features that can reduce the total amount of storage that you need. When you create a volume in Cloud Manager, you can choose a profile that enables these features or a profile that disables them. You should learn more about these features to help you decide which profile to use.

NetApp storage efficiency features provide the following benefits:

Thin provisioning

Presents more logical storage to hosts or users than you actually have in your physical storage pool. Instead of preallocating storage space, storage space is allocated dynamically to each volume as data is written.

Deduplication

Improves efficiency by locating identical blocks of data and replacing them with references to a single shared block. This technique reduces storage capacity requirements by eliminating redundant blocks of data that reside in the same volume.

Compression

Reduces the physical capacity required to store data by compressing data within a volume on primary, secondary, and archive storage.

Networking requirements for Cloud Volumes ONTAP in Azure

Set up your Azure networking so Cloud Volumes ONTAP systems can operate properly. This includes networking for the Connector and Cloud Volumes ONTAP.

Requirements for Cloud Volumes ONTAP

The following networking requirements must be met in Azure.

Outbound internet access for Cloud Volumes ONTAP

Cloud Volumes ONTAP requires outbound internet access to send messages to NetApp AutoSupport, which proactively monitors the health of your storage.

Routing and firewall policies must allow HTTP/HTTPS traffic to the following endpoints so Cloud Volumes ONTAP can send AutoSupport messages:

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

Learn how to configure AutoSupport.

Security groups

You do not need to create security groups because Cloud Manager does that for you. If you need to use your own, refer to the security group rules listed below.

Number of IP addresses

Cloud Manager allocates the following number of IP addresses to Cloud Volumes ONTAP in Azure:

- Single node: 5 IP addresses
- HA pair: 16 IP addresses

Note that Cloud Manager creates an SVM management LIF on HA pairs, but not on single node systems in Azure.

A LIF is an IP address associated with a physical port. An SVM management LIF is required for management tools like SnapCenter.

Connection from Cloud Volumes ONTAP to Azure Blob storage for data tiering

If you want to tier cold data to Azure Blob storage, you don't need to set up a connection between the performance tier and the capacity tier as long as Cloud Manager has the required permissions. Cloud Manager enables a VNet service endpoint for you if the Cloud Manager policy has these permissions:

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

These permissions are included in the latest Cloud Manager policy.

For details about setting up data tiering, see Tiering cold data to low-cost object storage.

Connections to ONTAP systems in other networks

To replicate data between a Cloud Volumes ONTAP system in Azure and ONTAP systems in other networks, you must have a VPN connection between the Azure VNet and the other network—for example, an AWS VPC or your corporate network.

For instructions, refer to Microsoft Azure Documentation: Create a Site-to-Site connection in the Azure portal.

Requirements for the Connector

Set up your networking so that the Connector can manage resources and processes within your public cloud environment. The most important step is ensuring outbound internet access to various endpoints.

If your network uses a proxy server for all communication to the internet, you can specify the proxy server from the Settings page. Refer to Configuring the Connector to use a proxy server.

Connections to target networks

A Connector requires a network connection to the VPCs and VNets in which you want to deploy Cloud Volumes ONTAP.

For example, if you install a Connector in your corporate network, then you must set up a VPN connection to

the VPC or VNet in which you launch Cloud Volumes ONTAP.

Outbound internet access

The Connector requires outbound internet access to manage resources and processes within your public cloud environment. A Connector contacts the following endpoints when managing resources in Azure:

Endpoints	Purpose
https://management.azure.com https://login.microsoftonline.com	Enables Cloud Manager to deploy and manage Cloud Volumes ONTAP in most Azure regions.
https://management.microsoftazure.de https://login.microsoftonline.de	Enables Cloud Manager to deploy and manage Cloud Volumes ONTAP in the Azure Germany regions.
https://management.usgovcloudapi.net https://login.microsoftonline.com	Enables Cloud Manager to deploy and manage Cloud Volumes ONTAP in the Azure US Gov regions.
https://api.services.cloud.netapp.com:443	API requests to NetApp Cloud Central.
https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com	Provides access to software images, manifests, and templates.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://sts.amazonaws.com https://cloud-support-netapp-com-accelerated.s3.amazonaws.com	Enables the Connector to access and download manifests, templates, and Cloud Volumes ONTAP upgrade images.
https://cloudmanagerinfraprod.azurecr.io *.blob.core.windows.net	Access to software images of container components for an infrastructure that's running Docker and provides a solution for service integrations with Cloud Manager.
https://kinesis.us-east-1.amazonaws.com	Enables NetApp to stream data from audit records.
https://cloudmanager.cloud.netapp.com	Communication with the Cloud Manager service, which includes Cloud Central accounts.
https://netapp-cloud-account.auth0.com	Communication with NetApp Cloud Central for centralized user authentication.
support.netapp.com:443 https://mysupport.netapp.com	Communication with NetApp AutoSupport. Note that the Connector communicates with support.netapp.com:443, which redirects to https://mysupport.netapp.com.
https://support.netapp.com/svcgw https://support.netapp.com/ServiceGW/entitlement https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com	Communication with NetApp for system licensing and support registration.

Endpoints	Purpose
https://client.infra.support.netapp.com.s3.us-west-1.amazonaws.com https://cloud-support-netapp-com-accelerated.s3.us-west-1.amazonaws.com https://trigger.asup.netapp.com.s3.us-west-1.amazonaws.com	Enables NetApp to collect information needed to troubleshoot support issues.
https://ipa-signer.cloudmanager.netapp.com	Enables Cloud Manager to generate licenses (for example, a FlexCache license for Cloud Volumes ONTAP)
*.blob.core.windows.net	Required for HA pairs when using a proxy.
Various third-party locations, for example: • https://repo1.maven.org/maven2 • https://oss.sonatype.org/content/repositories • https://repo.typesafe.com Third-party locations are subject to change.	During upgrades, Cloud Manager downloads the latest packages for third-party dependencies.

While you should perform almost all tasks from the SaaS user interface, a local user interface is still available on the Connector. The machine running the web browser must have connections to the following endpoints:

Endpoints	Purpose
The Connector host	You must enter the host's IP address from a web browser to load the Cloud Manager console. Depending on your connectivity to your cloud provider, you can use the private IP or a public IP assigned to the host: • A private IP works if you have a VPN and direct connect access to your virtual network • A public IP works in any networking scenario In any case, you should secure network access by ensuring that security group rules allow access from only authorized IPs or subnets.
https://auth0.com https://cdn.auth0.com https://netapp-cloud-account.auth0.com https://services.cloud.netapp.com	Your web browser connects to these endpoints for centralized user authentication through NetApp Cloud Central.
https://widget.intercom.io	For in-product chat that enables you to talk to NetApp cloud experts.

Security group rules for Cloud Volumes ONTAP

Cloud Manager creates Azure security groups that include the inbound and outbound rules that Cloud Volumes ONTAP needs to operate successfully. You might want to refer to the ports for testing purposes or if you prefer your to use own security groups.

The security group for Cloud Volumes ONTAP requires both inbound and outbound rules.

Inbound rules for single node systems

The rules listed below allow traffic, unless the description notes that it blocks specific inbound traffic.

Priority and name	Port and protocol	Source and destination	Description
1000 inbound_ssh	22 TCP	Any to Any	SSH access to the IP address of the cluster management LIF or a node management LIF
1001 inbound_http	80 TCP	Any to Any	HTTP access to the System Manager web console using the IP address of the cluster management LIF
1002 inbound_111_tcp	111 TCP	Any to Any	Remote procedure call for NFS
1003 inbound_111_udp	111 UDP	Any to Any	Remote procedure call for NFS
1004 inbound_139	139 TCP	Any to Any	NetBIOS service session for CIFS
1005 inbound_161-162 _tcp	161-162 TCP	Any to Any	Simple network management protocol
1006 inbound_161-162 _udp	161-162 UDP	Any to Any	Simple network management protocol
1007 inbound_443	443 TCP	Any to Any	HTTPS access to the System Manager web console using the IP address of the cluster management LIF
1008 inbound_445	445 TCP	Any to Any	Microsoft SMB/CIFS over TCP with NetBIOS framing
1009 inbound_635_tcp	635 TCP	Any to Any	NFS mount
1010 inbound_635_udp	635 UDP	Any to Any	NFS mount
1011 inbound_749	749 TCP	Any to Any	Kerberos
1012 inbound_2049_tcp	2049 TCP	Any to Any	NFS server daemon
1013 inbound_2049_udp	2049 UDP	Any to Any	NFS server daemon

Priority and name	Port and protocol	Source and destination	Description
1014 inbound_3260	3260 TCP	Any to Any	iSCSI access through the iSCSI data LIF
1015 inbound_4045-4046_tcp	4045-4046 TCP	Any to Any	NFS lock daemon and network status monitor
1016 inbound_4045-4046_udp	4045-4046 UDP	Any to Any	NFS lock daemon and network status monitor
1017 inbound_10000	10000 TCP	Any to Any	Backup using NDMP
1018 inbound_11104-11105	11104-11105 TCP	Any to Any	SnapMirror data transfer
3000 inbound_deny_all_tcp	Any port TCP	Any to Any	Block all other TCP inbound traffic
3001 inbound_deny_all_udp	Any port UDP	Any to Any	Block all other UDP inbound traffic
65000 AllowVnetInBound	Any port Any protocol	VirtualNetwork to VirtualNetwork	Inbound traffic from within the VNet
65001 AllowAzureLoadBalancerInBound	Any port Any protocol	AzureLoadBalancer to Any	Data traffic from the Azure Standard Load Balancer
65500 DenyAllInBound	Any port Any protocol	Any to Any	Block all other inbound traffic

Inbound rules for HA systems

The rules listed below allow traffic, unless the description notes that it blocks specific inbound traffic.

HA systems have less inbound rules than single node systems because inbound data traffic goes through the Azure Standard Load Balancer. Because of this, traffic from the Load Balancer should be open, as shown in the "AllowAzureLoadBalancerInBound" rule.

Priority and name	Port and protocol	Source and destination	Description
100 inbound_443	443 Any protocol	Any to Any	HTTPS access to the System Manager web console using the IP address of the cluster management LIF

Priority and name	Port and protocol	Source and destination	Description
101 inbound_111_tcp	111 Any protocol	Any to Any	Remote procedure call for NFS
102 inbound_2049_tcp	2049 Any protocol	Any to Any	NFS server daemon
111 inbound_ssh	22 Any protocol	Any to Any	SSH access to the IP address of the cluster management LIF or a node management LIF
121 inbound_53	53 Any protocol	Any to Any	DNS and CIFS
65000 AllowVnetInBound	Any port Any protocol	VirtualNetwork to VirtualNetwork	Inbound traffic from within the VNet
65001 AllowAzureLoadBalancerInBound	Any port Any protocol	AzureLoadBalancer to Any	Data traffic from the Azure Standard Load Balancer
65500 DenyAllInBound	Any port Any protocol	Any to Any	Block all other inbound traffic

Outbound rules

The predefined security group for Cloud Volumes ONTAP opens all outbound traffic. If that is acceptable, follow the basic outbound rules. If you need more rigid rules, use the advanced outbound rules.

Basic outbound rules

The predefined security group for Cloud Volumes ONTAP includes the following outbound rules.

Port	Protocol	Purpose
All	All TCP	All outbound traffic
All	All UDP	All outbound traffic

Advanced outbound rules

If you need rigid rules for outbound traffic, you can use the following information to open only those ports that are required for outbound communication by Cloud Volumes ONTAP.

The source is the interface (IP address) on the Cloud Volumes ONTAP system.

Service	Port	Protocol	Source	Destination	Purpose
Active Directory	88	TCP	Node management LIF	Active Directory forest	Kerberos V authentication
	137	UDP	Node management LIF	Active Directory forest	NetBIOS name service
	138	UDP	Node management LIF	Active Directory forest	NetBIOS datagram service
	139	TCP	Node management LIF	Active Directory forest	NetBIOS service session
	389	TCP & UDP	Node management LIF	Active Directory forest	LDAP
	445	TCP	Node management LIF	Active Directory forest	Microsoft SMB/CIFS over TCP with NetBIOS framing
	464	TCP	Node management LIF	Active Directory forest	Kerberos V change & set password (SET_CHANGE)
	464	UDP	Node management LIF	Active Directory forest	Kerberos key administration
	749	TCP	Node management LIF	Active Directory forest	Kerberos V change & set Password (RPCSEC_GSS)
	88	TCP	Data LIF (NFS, CIFS, iSCSI)	Active Directory forest	Kerberos V authentication
	137	UDP	Data LIF (NFS, CIFS)	Active Directory forest	NetBIOS name service
	138	UDP	Data LIF (NFS, CIFS)	Active Directory forest	NetBIOS datagram service
	139	TCP	Data LIF (NFS, CIFS)	Active Directory forest	NetBIOS service session
	389	TCP & UDP	Data LIF (NFS, CIFS)	Active Directory forest	LDAP
	445	TCP	Data LIF (NFS, CIFS)	Active Directory forest	Microsoft SMB/CIFS over TCP with NetBIOS framing
	464	TCP	Data LIF (NFS, CIFS)	Active Directory forest	Kerberos V change & set password (SET_CHANGE)
	464	UDP	Data LIF (NFS, CIFS)	Active Directory forest	Kerberos key administration
	749	TCP	Data LIF (NFS, CIFS)	Active Directory forest	Kerberos V change & set password (RPCSEC_GSS)
DHCP	68	UDP	Node management LIF	DHCP	DHCP client for first-time setup

Service	Port	Protocol	Source	Destination	Purpose
DHCPS	67	UDP	Node management LIF	DHCP	DHCP server
DNS	53	UDP	Node management LIF and data LIF (NFS, CIFS)	DNS	DNS
NDMP	18600–18699	TCP	Node management LIF	Destination servers	NDMP copy
SMTP	25	TCP	Node management LIF	Mail server	SMTP alerts, can be used for AutoSupport
SNMP	161	TCP	Node management LIF	Monitor server	Monitoring by SNMP traps
	161	UDP	Node management LIF	Monitor server	Monitoring by SNMP traps
	162	TCP	Node management LIF	Monitor server	Monitoring by SNMP traps
	162	UDP	Node management LIF	Monitor server	Monitoring by SNMP traps
SnapMirror	11104	TCP	Intercluster LIF	ONTAP intercluster LIFs	Management of intercluster communication sessions for SnapMirror
	11105	TCP	Intercluster LIF	ONTAP intercluster LIFs	SnapMirror data transfer
Syslog	514	UDP	Node management LIF	Syslog server	Syslog forward messages

Security group rules for the Connector

The security group for the Connector requires both inbound and outbound rules.

Inbound rules

Port	Protocol	Purpose
22	SSH	Provides SSH access to the Connector host
80	HTTP	Provides HTTP access from client web browsers to the local user interface
443	HTTPS	Provides HTTPS access from client web browsers to the local user interface

Outbound rules

The predefined security group for the Connector opens all outbound traffic. If that is acceptable, follow the basic outbound rules. If you need more rigid rules, use the advanced outbound rules.

Basic outbound rules

The predefined security group for the Connector includes the following outbound rules.

Port	Protocol	Purpose
All	All TCP	All outbound traffic
All	All UDP	All outbound traffic

Advanced outbound rules

If you need rigid rules for outbound traffic, you can use the following information to open only those ports that are required for outbound communication by the Connector.

The source IP address is the Connector host.

Service	Port	Protocol	Destination	Purpose
Active Directory	88	TCP	Active Directory forest	Kerberos V authentication
	139	TCP	Active Directory forest	NetBIOS service session
	389	TCP	Active Directory forest	LDAP
	445	TCP	Active Directory forest	Microsoft SMB/CIFS over TCP with NetBIOS framing
	464	TCP	Active Directory forest	Kerberos V change & set password (SET_CHANGE)
	749	TCP	Active Directory forest	Active Directory Kerberos V change & set password (RPCSEC_GSS)
	137	UDP	Active Directory forest	NetBIOS name service
	138	UDP	Active Directory forest	NetBIOS datagram service
	464	UDP	Active Directory forest	Kerberos key administration
API calls and AutoSupport	443	HTTPS	Outbound internet and ONTAP cluster management LIF	API calls to AWS and ONTAP, and sending AutoSupport messages to NetApp
DNS	53	UDP	DNS	Used for DNS resolve by Cloud Manager

Set up Cloud Volumes ONTAP to use a customer-managed key in Azure

Data is automatically encrypted on Cloud Volumes ONTAP in Azure using Azure Storage Service Encryption with a Microsoft-managed key. But you can use your own encryption

key instead by following the steps on this page.

Data encryption overview

Cloud Volumes ONTAP data is automatically encrypted in Azure using Azure Storage Service Encryption. The default implementation uses a Microsoft-managed key. No setup is required.

If you want to use a customer-managed key with Cloud Volumes ONTAP, then you need to complete the following steps:

1. From Azure, create a key vault and then generate a key in that vault
2. From Cloud Manager, use the API to create a Cloud Volumes ONTAP working environment that uses the key

Key rotation

If you create a new version of your key, Cloud Volumes ONTAP automatically uses the latest key version.

How data is encrypted

After you create a Cloud Volumes ONTAP working environment that is configured to use a customer-managed key, Cloud Volumes ONTAP data is encrypted as follows.

HA pairs

- All Azure storage accounts for Cloud Volumes ONTAP are encrypted using a customer-managed key.
- Any new storage accounts (for example, when you add disks or aggregates) also use the same key.

Single node

- All Azure storage accounts for Cloud Volumes ONTAP are encrypted using a customer-managed key.
- For root, boot, and data disks, Cloud Manager uses a disk encryption set, which enables management of encryption keys with managed disks.
- Any new data disks also use the same disk encryption set.
- NVRAM and the core disk are encrypted using a Microsoft-managed key, instead of the customer-managed key.

Create a key vault and generate a key

The key vault must reside in the same Azure subscription and region in which you plan to create the Cloud Volumes ONTAP system.

Steps

1. Create a key vault in your Azure subscription.

   Note the following requirements for the key vault:

   - The key vault must reside in the same region as the Cloud Volumes ONTAP system.
   - The following options should be enabled:
     - **Soft-delete** (this option is enabled by default, but must *not* be disabled)
     - **Purge protection**

- **Azure Disk Encryption for volume encryption** (for single node Cloud Volumes ONTAP systems only)

2. Generate a key in the key vault.

   Note the following requirements for the key:

   - The key type must be **RSA**.
   - The recommended RSA key size is **2048**, but other sizes are supported.

Create a working environment that uses the encryption key

After you create the key vault and generate an encryption key, you can create a new Cloud Volumes ONTAP system that is configured to use the key. These steps are supported by using the Cloud Manager API.

Required permissions

If you want to use a customer-managed key with a single node Cloud Volumes ONTAP system, ensure that the Cloud Manager Connector has the following permissions:

```
"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"
```

You can find the latest list of permissions on the Cloud Manager policies page.

These permissions aren't required for HA pairs.

Steps

1. Obtain the list of key vaults in your Azure subscription by using the following Cloud Manager API call.

   For an HA pair: `GET /azure/ha/metadata/vaults`

   For single node: `GET /azure/vsa/metadata/vaults`

   Make note of the **name** and **resourceGroup**. You'll need to specify those values in the next step.

   Learn more about this API call.

2. Obtain the list of keys within the vault by using the following Cloud Manager API call.

   For an HA pair: `GET /azure/ha/metadata/keys-vault`

   For single node: `GET /azure/vsa/metadata/keys-vault`

   Make note of the **keyName**. You'll need to specify that value (along with the vault name) in the next step.

   Learn more about this API call.

3. Create a Cloud Volumes ONTAP system by using the following Cloud Manager API call.
   a. For an HA pair:

      `POST /azure/ha/working-environments`

      The request body must include the following fields:

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

      Learn more about this API call.

   b. For a single node system:

      `POST /azure/vsa/working-environments`

      The request body must include the following fields:

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

      Learn more about this API call.

Result

You have a new Cloud Volumes ONTAP system that is configured to use your customer-managed key for data encryption.

Launching Cloud Volumes ONTAP in Azure

You can launch a single node system or an HA pair in Azure by creating a Cloud Volumes ONTAP working environment in Cloud Manager.

What you'll need

You need the following to create a working environment.

- A Connector that's up and running.
  - You should have a Connector that is associated with your workspace.
  - You should be prepared to leave the Connector running at all times.
- An understanding of the configuration that you want to use.

  You should have chose a configuration and obtained Azure networking information from your administrator. For details, see Planning your Cloud Volumes ONTAP configuration.

- An understanding of what's required in the Add Working Environment wizard for the licensing method that you want to use.

Licensing option	Requirement	How to meet the requirement
PAYGO free trial	A Marketplace subscription is required.	You'll have the option to subscribe to your cloud provider's marketplace from the **Details & Credentials** page.
Freemium	A Marketplace subscription or NetApp Support Site (NSS) account is required.	You'll have the option to subscribe to your cloud provider's marketplace from the **Details & Credentials** page You can enter your NSS account on the **Charging Methods and NSS Account** page.
Capacity-based BYOL	A Marketplace subscription or NetApp Support Site (NSS) account is required. A Marketplace subscription is recommended for capacity-based charging in the event that your account doesn't have a valid capacity-based license, or in the event that your provisioned capacity exceeds the licensed capacity.	You'll have the option to subscribe to your cloud provider's marketplace from the **Details & Credentials** page You can enter your NSS account on the **Charging Methods and NSS Account** page.
Node-based BYOL	The 20-digit serial number (license key) is required.	You'll enter the serial number on the **Charging Methods and NSS Account** page.

About this task

When Cloud Manager creates a Cloud Volumes ONTAP system in Azure, it creates several Azure objects, such as a resource group, network interfaces, and storage accounts. You can review a summary of the resources at the end of the wizard.

Potential for Data Loss

The best practice is to use a new, dedicated resource group for each Cloud Volumes ONTAP system.

Deploying Cloud Volumes ONTAP in an existing, shared resource group is not recommended due to the risk of data loss. While Cloud Manager can remove Cloud Volumes ONTAP resources from a shared resource group in case of deployment failure or deletion, an Azure user might accidentally delete Cloud Volumes ONTAP resources from a shared resource group.

Steps

1. On the Canvas page, click **Add Working Environment** and follow the prompts.
2. **Choose a Location**: Select **Microsoft Azure** and **Cloud Volumes ONTAP Single Node** or **Cloud Volumes ONTAP High Availability**.
3. If you're prompted, create a Connector.
4. **Details and Credentials**: Optionally change the Azure credentials and subscription, specify a cluster name, add tags if needed, and then specify credentials.

The following table describes fields for which you might need guidance:

Field	Description
Working Environment Name	Cloud Manager uses the working environment name to name both the Cloud Volumes ONTAP system and the Azure virtual machine. It also uses the name as the prefix for the predefined security group, if you select that option.
Resource Group Tags	Tags are metadata for your Azure resources. When you enter tags in this field, Cloud Manager adds them to the resource group associated with the Cloud Volumes ONTAP system. You can add up to four tags from the user interface when creating a working environment, and then you can add more after its created. Note that the API does not limit you to four tags when creating a working environment. For information about tags, refer to Microsoft Azure Documentation: Using tags to organize your Azure resources.
User name and password	These are the credentials for the Cloud Volumes ONTAP cluster admin account. You can use these credentials to connect to Cloud Volumes ONTAP through System Manager or its CLI.
Edit Credentials	You can choose different Azure credentials and a different Azure subscription to use with this Cloud Volumes ONTAP system. You need to associate an Azure Marketplace subscription with the selected Azure subscription in order to deploy a pay-as-you-go Cloud Volumes ONTAP system. Learn how to add credentials.

The following video shows how to associate a Marketplace subscription to an Azure subscription:

► https://docs.netapp.com/us-en/occm//media/video_subscribing_azure.mp4 *(video)*

5. **Services**: Keep the services enabled or disable the individual services that you don't want to use with Cloud Volumes ONTAP.
   - Learn more about Cloud Data Sense.
   - Learn more about Cloud Backup.
   - Learn more about the Monitoring service.
6. **Location & Connectivity**: Select a location, a resource group, a security group, and then select the checkbox to confirm network connectivity between the Connector and the target location.

   The following table describes fields for which you might need guidance:

Field	Description
Location	For single node systems, you can choose the Availability Zone in which you'd like to deploy Cloud Volumes ONTAP. If you don't select an AZ, Cloud Manager will select one for you.

Field	Description
Resource Group	Create a new resource group for Cloud Volumes ONTAP or use an existing resource group. The best practice is to use a new, dedicated resource group for Cloud Volumes ONTAP. While it is possible to deploy Cloud Volumes ONTAP in an existing, shared resource group, it's not recommended due to the risk of data loss. See the warning above for more details. You must use a dedicated resource group for each Cloud Volumes ONTAP HA pair that you deploy in Azure. Only one HA pair is supported in a resource group. Cloud Manager experiences connection issues if you try to deploy a second Cloud Volumes ONTAP HA pair in an Azure resource group. If the Azure account that you're using has the required permissions, Cloud Manager removes Cloud Volumes ONTAP resources from a resource group, in case of deployment failure or deletion.
Security group	If you choose an existing security group, then it must meet Cloud Volumes ONTAP requirements. View the default security group.

7. **Charging Methods and NSS Account**: Specify which charging option would you like to use with this system, and then specify a NetApp Support Site account.
   - Learn about these charging methods.
   - Learn what's required in the wizard for the licensing method that you want to use.
8. **Preconfigured Packages**: Select one of the packages to quickly deploy a Cloud Volumes ONTAP system, or click **Create my own configuration**.

   If you choose one of the packages, you only need to specify a volume and then review and approve the configuration.

9. **Licensing**: Change the Cloud Volumes ONTAP version as needed, select a license, and select a virtual machine type.

   If your needs change after you launch the system, you can modify the license or virtual machine type later.

   If a newer Release Candidate, General Availability, or patch release is available for the selected version, then Cloud Manager updates the system to that version when creating the working environment. For example, the update occurs if you select Cloud Volumes ONTAP 9.6 RC1 and 9.6 GA is available. The update does not occur from one release to another—for example, from 9.6 to 9.7.

10. **Subscribe from the Azure Marketplace**: Follow the steps if Cloud Manager could not enable programmatic deployments of Cloud Volumes ONTAP.
11. **Underlying Storage Resources**: Choose settings for the initial aggregate: a disk type, a size for each disk, and whether data tiering to Blob storage should be enabled.

    Note the following:

- The disk type is for the initial volume. You can choose a different disk type for subsequent volumes.
- The disk size is for all disks in the initial aggregate and for any additional aggregates that Cloud Manager creates when you use the simple provisioning option. You can create aggregates that use a different disk size by using the advanced allocation option.

  For help choosing a disk type and size, see Sizing your system in Azure.

- You can choose a specific volume tiering policy when you create or edit a volume.
- If you disable data tiering, you can enable it on subsequent aggregates.

  Learn more about data tiering.

12. **Write Speed & WORM** (single node systems only): Choose **Normal** or **High** write speed, and activate write once, read many (WORM) storage, if desired.

    Learn more about write speed.

    WORM can't be enabled if Cloud Backup was enabled or if data tiering was enabled.

    Learn more about WORM storage.

13. **Secure Communication to Storage & WORM** (HA only): Choose whether to enable an HTTPS connection to Azure storage accounts, and activate write once, read many (WORM) storage, if desired.

    The HTTPS connection is from a Cloud Volumes ONTAP 9.7 HA pair to Azure storage accounts. Note that enabling this option can impact write performance. You can't change the setting after you create the working environment.

    Learn more about WORM storage.

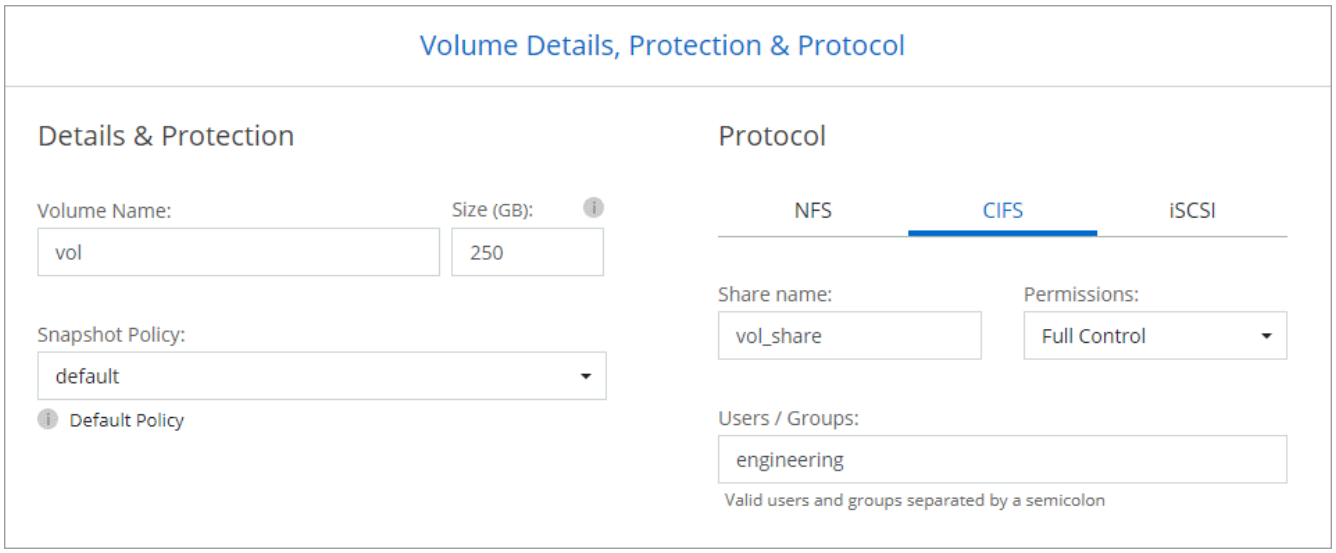
14. **Create Volume**: Enter details for the new volume or click **Skip**.

    Some of the fields in this page are self-explanatory. The following table describes fields for which you might need guidance:

Field	Description
Size	The maximum size that you can enter largely depends on whether you enable thin provisioning, which enables you to create a volume that is bigger than the physical storage currently available to it.
Access control (for NFS only)	An export policy defines the clients in the subnet that can access the volume. By default, Cloud Manager enters a value that provides access to all instances in the subnet.
Permissions and Users / Groups (for CIFS only)	These fields enable you to control the level of access to a share for users and groups (also called access control lists or ACLs). You can specify local or domain Windows users or groups, or UNIX users or groups. If you specify a domain Windows user name, you must include the user's domain using the format domain\username.

Field	Description
Snapshot Policy	A Snapshot copy policy specifies the frequency and number of automatically created NetApp Snapshot copies. A NetApp Snapshot copy is a point-in-time file system image that has no performance impact and requires minimal storage. You can choose the default policy or none. You might choose none for transient data: for example, tempdb for Microsoft SQL Server.
Advanced options (for NFS only)	Select an NFS version for the volume: either NFSv3 or NFSv4.
Initiator group and IQN (for iSCSI only)	iSCSI storage targets are called LUNs (logical units) and are presented to hosts as standard block devices. Initiator groups are tables of iSCSI host node names and control which initiators have access to which LUNs. iSCSI targets connect to the network through standard Ethernet network adapters (NICs), TCP offload engine (TOE) cards with software initiators, converged network adapters (CNAs) or dedicated host bust adapters (HBAs) and are identified by iSCSI qualified names (IQNs). When you create an iSCSI volume, Cloud Manager automatically creates a LUN for you. We've made it simple by creating just one LUN per volume, so there's no management involved. After you create the volume, use the IQN to connect to the LUN from your hosts.

The following image shows the Volume page filled out for the CIFS protocol:



15. **CIFS Setup**: If you chose the CIFS protocol, set up a CIFS server.

Field	Description
DNS Primary and Secondary IP Address	The IP addresses of the DNS servers that provide name resolution for the CIFS server. The listed DNS servers must contain the service location records (SRV) needed to locate the Active Directory LDAP servers and domain controllers for the domain that the CIFS server will join.

Field	Description
Active Directory Domain to join	The FQDN of the Active Directory (AD) domain that you want the CIFS server to join.
Credentials authorized to join the domain	The name and password of a Windows account with sufficient privileges to add computers to the specified Organizational Unit (OU) within the AD domain.
CIFS server NetBIOS name	A CIFS server name that is unique in the AD domain.
Organizational Unit	The organizational unit within the AD domain to associate with the CIFS server. The default is CN=Computers. To configure Azure AD Domain Services as the AD server for Cloud Volumes ONTAP, you should enter **OU=AADDC Computers** or **OU=AADDC Users** in this field. Azure Documentation: Create an Organizational Unit (OU) in an Azure AD Domain Services managed domain
DNS Domain	The DNS domain for the Cloud Volumes ONTAP storage virtual machine (SVM). In most cases, the domain is the same as the AD domain.
NTP Server	Select **Use Active Directory Domain** to configure an NTP server using the Active Directory DNS. If you need to configure an NTP server using a different address, then you should use the API. See the Cloud Manager automation docs for details.

16. **Usage Profile, Disk Type, and Tiering Policy**: Choose whether you want to enable storage efficiency features and change the volume tiering policy, if needed.

    For more information, see Understanding volume usage profiles and Data tiering overview.

17. **Review & Approve**: Review and confirm your selections.
    a. Review details about the configuration.
    b. Click **More information** to review details about support and the Azure resources that Cloud Manager will purchase.
    c. Select the **I understand…** check boxes.
    d. Click **Go**.

Result

Cloud Manager deploys the Cloud Volumes ONTAP system. You can track the progress in the timeline.

If you experience any issues deploying the Cloud Volumes ONTAP system, review the failure message. You can also select the working environment and click **Re-create environment**.

For additional help, go to NetApp Cloud Volumes ONTAP Support.

After you finish

- If you provisioned a CIFS share, give users or groups permissions to the files and folders and verify that those users can access the share and create a file.
- If you want to apply quotas to volumes, use System Manager or the CLI.

  Quotas enable you to restrict or track the disk space and number of files used by a user, group, or qtree.