Get started in NetApp Console

Cloud Volumes ONTAP

NetApp
January 13, 2026

Table of Contents

Get started in NetApp Console

Quick start for Cloud Volumes ONTAP in Azure

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

1 Create a Console agent

If you don't have a Console agent yet, you need to create one. Learn how to create a Console agent in Azure

Note that if you want to deploy Cloud Volumes ONTAP in a subnet where no internet access is available, then you need to manually install the Console agent and access the NetApp Console that's running on that Console agent. Learn how to manually install the Console agent in a location without internet access

2 Plan your configuration

The Console 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. For information, refer to Plan your Cloud Volumes ONTAP configuration in Azure.

3 Set up your networking

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

b. Enable outbound internet access from the target VPC for NetApp AutoSupport.

   This step isn't required if you're deploying Cloud Volumes ONTAP in a location where no internet access is available.

Learn more about networking requirements.

4 Launch Cloud Volumes ONTAP

Click **Add System**, 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

- Creating a Console agent from the Console
- Creating a Console agent from the Azure Marketplace
- Installing the Console agent software on a Linux host
- What the Console does with permissions

Plan 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.

Choose a Cloud Volumes ONTAP license

Several licensing options are available for Cloud Volumes ONTAP. Each option enables you to choose a consumption model that meets your needs.

- Learn about licensing options for Cloud Volumes ONTAP
- Learn how to set up licensing

Choose a supported region

Cloud Volumes ONTAP is supported in most Microsoft Azure regions. View the full list of supported regions.

Choose a supported VM type

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

Supported configurations for Cloud Volumes ONTAP in Azure

Understand 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

Size 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 with single node systems

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

Single node systems can use these types of Azure Managed Disks:

- *Premium SSD Managed Disks* provide high performance for I/O-intensive workloads at a higher cost.
- *Premium SSD v2 Managed Disks* provide higher performance with lower latency at a lower cost, compared to Premium SSD Managed Disks.
- *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, refer to Microsoft Azure Documentation: What disk types are available in Azure?.

Azure disk type with HA pairs

HA systems use Premium SSD Shared Managed Disks which both provide high performance for I/O-intensive workloads at a higher cost. HA deployments created before the 9.12.1 release use Premium page blobs.

Azure disk size

When you launch Cloud Volumes ONTAP instances, you must choose the default disk size for aggregates. The NetApp Console 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

View default system disks

In addition to the storage for user data, the Console also purchases cloud storage for Cloud Volumes ONTAP system data (boot data, root data, core data, and NVRAM). For planning purposes, it might help for you to review these details before you deploy Cloud Volumes ONTAP.

View the default disks for Cloud Volumes ONTAP system data in Azure.

The Console agent also requires a system disk. View details about the Console agent's default configuration.

Collect networking information

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)	

Choose a write speed

The Console 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.

Choose 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 the Console, 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.

Set up Azure networking for Cloud Volumes ONTAP

The NetApp Console handles the set up of networking components for Cloud Volumes ONTAP, such as IP addresses, netmasks, and routes. You need to make sure that outbound internet access is available, that enough private IP addresses are available, that the right connections are in place, and more.

Requirements for Cloud Volumes ONTAP

The following networking requirements must be met in Azure.

Outbound internet access

Cloud Volumes ONTAP systems require outbound internet access for accessing external endpoints for various functions. Cloud Volumes ONTAP can't operate properly if these endpoints are blocked in environments with strict security requirements.

The Console agent also contacts several endpoints for day-to-day operations. For information about endpoints, refer to View endpoints contacted from the Console agent and Prepare networking for using the Console.

Cloud Volumes ONTAP endpoints

Cloud Volumes ONTAP uses these endpoints to communicate with various services.

Endpoints	Applicable for	Purpose	Deployment modes	Impact if unavailable
https://netapp-cloud-account.auth0.com	Authentication	Used for authentication in the Console.	Standard and restricted modes.	User authentication fails and the following services remain unavailable: • Cloud Volumes ONTAP services • ONTAP services • Protocols and proxy services
https://vault.azure.net	Key Vault	Used to retrieve client secret keys from the Azure Key Vault when using customer-managed keys (CMK).	Standard, restricted, and private modes.	Cloud Volumes ONTAP services are unavailable.
https://api.bluexp.netapp.com/tenancy	Tenancy	Used to retrieve the Cloud Volumes ONTAP resources from the Console to authorize resources and users.	Standard and restricted modes.	Cloud Volumes ONTAP resources and the users are not authorized.
https://mysupport.netapp.com/aods/asupmessage https://mysupport.netapp.com/asupprod/post/1.0/postAsup	AutoSupport	Used to send AutoSupport telemetry data to NetApp support.	Standard and restricted modes.	AutoSupport information remains undelivered.
https://management.azure.com https://login.microsoftonline.com https://bluexpinfraprod.eastus2.data.azurecr.io https://core.windows.net	Public regions	Communication with Azure services.	Standard, restricted, and private modes.	Cloud Volumes ONTAP cannot communicate with Azure service to perform specific operations for the Console in Azure.

Endpoints	Applicable for	Purpose	Deployment modes	Impact if unavailable
https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn	China Region	Communication with Azure services.	Standard, restricted, and private modes.	Cloud Volumes ONTAP cannot communicate with Azure service to perform specific operations for the Console in Azure.
https://management.microsoftazure.de https://login.microsoftonline.de https://blob.core.cloudapi.de https://core.cloudapi.de	Germany Region	Communication with Azure services.	Standard, restricted, and private modes.	Cloud Volumes ONTAP cannot communicate with Azure service to perform specific operations for the Console in Azure.
https://management.usgovcloudapi.net https://login.microsoftonline.us https://blob.core.usgovcloudapi.net https://core.usgovcloudapi.net	Government regions	Communication with Azure services.	Standard, restricted, and private modes.	Cloud Volumes ONTAP cannot communicate with Azure service to perform specific operations for the Console in Azure.
https://management.azure.microsoft.scloud https://login.microsoftonline.microsoft.scloud https://blob.core.microsoft.scloud https://core.microsoft.scloud	Government DoD regions	Communication with Azure services.	Standard, restricted, and private modes.	Cloud Volumes ONTAP cannot communicate with Azure service to perform specific operations for the Console in Azure.

Network proxy configuration of NetApp Console agent

You can use the proxy servers configuration of the NetApp Console agent to enable outbound internet access from Cloud Volumes ONTAP. The Console supports two types of proxies:

- **Explicit proxy**: The outbound traffic from Cloud Volumes ONTAP uses the HTTP address of the proxy server specified during the proxy configuration of the Console agent. The administrator might also have configured user credentials and root CA certificates for additional authentication. If a root CA certificate is available for the explicit proxy, make sure to obtain and upload the same certificate to your Cloud Volumes ONTAP system using the ONTAP CLI: security certificate install command.
- **Transparent proxy**: The network is configured to automatically route outbound traffic from Cloud Volumes ONTAP through the proxy for the Console agent. When setting up a transparent proxy, the administrator needs to provide only a root CA certificate for connectivity from Cloud Volumes ONTAP, not the HTTP address of the proxy server. Make sure that you obtain and upload the same root CA certificate to your Cloud Volumes ONTAP system using the ONTAP CLI: security certificate install command.

For information about configuring proxy servers, refer to the Configure the Console agent to use a proxy server.

IP addresses

The Console automatically allocates the required number of private IP addresses to Cloud Volumes ONTAP in Azure. You need to make sure that your networking has enough private IP addresses available.

The number of LIFs allocated for Cloud Volumes ONTAP depends on whether you deploy a single node system or an HA pair. A LIF is an IP address associated with a physical port. An SVM management LIF is required for management tools like SnapCenter.

> An iSCSI LIF provides client access over the iSCSI protocol and is used by the system for other important networking workflows. These LIFs are required and should not be deleted.

IP addresses for a single node system

The Console allocates 5 or 6 IP addresses to a single node system:

- Cluster management IP
- Node management IP
- Intercluster IP for SnapMirror
- NFS/CIFS IP
- iSCSI IP

> The iSCSI IP provides client access over the iSCSI protocol. It is also used by the system for other important networking workflows. This LIF is required and should not be deleted.

- SVM management (optional - not configured by default)

IP addresses for HA pairs

The Console allocates IP addresses to 4 NICs (per node) during deployment.

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

NIC0

- Node management IP
- Intercluster IP
- iSCSI IP

> The iSCSI IP provides client access over the iSCSI protocol. It is also used by the system for other important networking workflows. This LIF is required and should not be deleted.

NIC1

- Cluster network IP

NIC2

- Cluster Interconnect IP (HA IC)

NIC3

- Pageblob NIC IP (disk access)

NIC3 is only applicable to HA deployments that use page blob storage.

The above IP addresses do not migrate on failover events.

Additionally, 4 frontend IPs (FIPs) are configured to migrate on failover events. These frontend IPs live in the load balancer.

- Cluster management IP
- NodeA data IP (NFS/CIFS)
- NodeB data IP (NFS/CIFS)
- SVM management IP

Secure connections to Azure services

By default, the Console enables an Azure Private Link for connections between Cloud Volumes ONTAP and Azure page blob storage accounts.

In most cases, there's nothing that you need to do—the Console manages the Azure Private Link for you. But if you use Azure Private DNS, then you'll need to edit a configuration file. You should also be aware of a requirement for the location of the Console agent in Azure.

You can also disable the Private Link connection, if required by your business needs. If you disable the link, the Console configures Cloud Volumes ONTAP to use a service endpoint instead.

Learn more about using Azure Private Links or service endpoints with Cloud Volumes ONTAP.

Connections to other ONTAP systems

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, your corporate network.

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

Port for the HA interconnect

A Cloud Volumes ONTAP HA pair includes an HA interconnect, which allows each node to continually check whether its partner is functioning and to mirror log data for the other's nonvolatile memory. The HA interconnect uses TCP port 10006 for communication.

By default, communication between the HA interconnect LIFs is open and there are no security group rules for this port. But if you create a firewall between the HA interconnect LIFs, then you need to ensure that TCP traffic is open for port 10006 so that the HA pair can operate properly.

Only one HA pair in an Azure resource group

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.

The Console experiences connection issues if you try to deploy a second Cloud Volumes ONTAP HA pair in an

Azure resource group.

Security group rules

The Console creates Azure security groups that include the inbound and outbound rules for Cloud Volumes ONTAP to operate successfully. View security group rules for the Console agent.

The Azure security groups for Cloud Volumes ONTAP require the appropriate ports to be open for internal communication between the nodes. Learn about ONTAP internal ports.

We do not recommend modifying the predefined security groups or using custom security groups. However, if you must, note that the deployment process requires the Cloud Volumes ONTAP system to have full access within its own subnet. After the deployment is complete, if you decide to modify the network security group, ensure to keep the cluster ports and HA network ports open. This ensures seamless communication within the Cloud Volumes ONTAP cluster (any-to-any communication between the nodes).

Inbound rules for single node systems

When you add a Cloud Volumes ONTAP system and choose a predefined security group, you can choose to allow traffic within one of the following:

- **Selected VNet only**: The source for inbound traffic is the subnet range of the VNet for the Cloud Volumes ONTAP system and the subnet range of the VNet where the Console agent resides. This is the recommended option.
- **All VNets**: The source for inbound traffic is the 0.0.0.0/0 IP range.
- **Disabled**: This option restricts the public network access to your storage account, and disables data tiering for Cloud Volumes ONTAP systems. This is a recommended option if your private IP addresses should not be exposed even within the same VNet due to security regulations and policies.

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 ONTAP 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

Priority and name	Port and protocol	Source and destination	Description
1007 inbound_443	443 TCP	Any to Any	Connectivity with the Console agent and HTTPS access to the ONTAP 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
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

Priority and name	Port and protocol	Source and destination	Description
65500 DenyAllInBound	Any port Any protocol	Any to Any	Block all other inbound traffic

Inbound rules for HA systems

When you add a Cloud Volumes ONTAP system and choose a predefined security group, you can choose to allow traffic within one of the following:

- **Selected VNet only**: The source for inbound traffic is the subnet range of the VNet for the Cloud Volumes ONTAP system and the subnet range of the VNet where the Console agent resides. This is the recommended option.
- **All VNets**: The source for inbound traffic is the 0.0.0.0/0 IP range.

> 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.

- **Disabled**: This option restricts the public network access to your storage account, and disables data tiering for Cloud Volumes ONTAP systems. This is a recommended option if your private IP addresses should not be exposed even within the same VNet due to security regulations and policies.

Priority and name	Port and protocol	Source and destination	Description
100 inbound_443	443 Any protocol	Any to Any	Connectivity with the Console agent and HTTPS access to the ONTAP System Manager web console using the IP address of the cluster management LIF
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 AllowAzureLoad BalancerInBound	Any port Any protocol	AzureLoadBalancer to Any	Data traffic from the Azure Standard Load Balancer

Priority and name	Port and protocol	Source and destination	Description
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)

Service	Port	Protocol	Source	Destination	Purpose
AutoSupport	HTTPS	443	Node management LIF	mysupport.netapp.com	AutoSupport (HTTPS is the default)
	HTTP	80	Node management LIF	mysupport.netapp.com	AutoSupport (only if the transport protocol is changed from HTTPS to HTTP)
	TCP	3128	Node management LIF	Console agent	Sending AutoSupport messages through a proxy server on the Console agent, if an outbound internet connection isn't available
Configuration backups	HTTP	80	Node management LIF	http://<console-agent-IP-address>/occm/offboxconfig	Send configuration backups to the Console agent. ONTAP documentation.
DHCP	68	UDP	Node management LIF	DHCP	DHCP client for first-time setup
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

Requirements for the Console agent

If you haven't created a Console agent yet, you should review networking requirements for the Console agent as well.

- View networking requirements for the Console agent
- Security group rules in Azure

Related topics

- Verify AutoSupport setup for Cloud Volumes ONTAP
- Learn about ONTAP internal ports.

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 the NetApp Console, use the API to create a Cloud Volumes ONTAP system that uses the key.

How data is encrypted

The Console uses a disk encryption set, which enables management of encryption keys with managed disks not page blobs. Any new data disks also use the same disk encryption set. Lower versions will use Microsoft-managed key, instead of the customer-managed key.

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

Cloud Volumes ONTAP configuration	System disks used for key encryption	Data disks used for key encryption
Single node	• Boot • Core • NVRAM	• Root • Data

Cloud Volumes ONTAP configuration	System disks used for key encryption	Data disks used for key encryption
Azure HA single availability zone with page blobs	• Boot • Core • NVRAM	None
Azure HA single availability zone with shared managed disks	• Boot • Core • NVRAM	• Root • Data
Azure HA multiple availability zones with shared managed disks	• Boot • Core • NVRAM	• Root • Data

All Azure storage accounts for Cloud Volumes ONTAP are encrypted using a customer-managed key. If you want to encrypt your storage accounts during their creation, you must create and provide the ID of the resource in the Cloud Volumes ONTAP creation request. This applies for all type of deployments. If you do not provide it, the storage accounts still will be encrypted, but the Console first creates the storage accounts with Microsoft-managed key encryption and then updates the storage accounts to use the customer-managed key.

Key rotation in Cloud Volumes ONTAP

When you configure your encryption keys, you must use the Azure portal to set up and enable automatic key rotation. Creating and enabling a new version of encryption keys ensures that Cloud Volumes ONTAP can automatically detect and use the latest key version for encryption, ensuring your data remains secure without the need for manual intervention.

For information about configuring your keys and setting up key rotation, refer to the following Microsoft Azure documentation topics:

- Configure cryptographic key auto-rotation in Azure Key Vault
- Azure PowerShell - Enable customer-managed keys

After configuring the keys, ensure that you have selected *Enable auto rotation*, so that Cloud Volumes ONTAP can use the new keys when the previous keys expire. If you don't enable this option on the Azure portal, Cloud Volumes ONTAP can't automatically detect the new keys, which might cause issues with storage provisioning.

Create a user-assigned managed identity

You have the option to create a resource called a user-assigned managed identity. Doing so allows you to encrypt your storage accounts when you create a Cloud Volumes ONTAP system. We recommend creating this resource prior to creating a key vault and generating a key.

The resource has the following ID: `userassignedidentity`.

Steps

1. In Azure, go to Azure services and select **Managed Identities**.
2. Click **Create**.
3. Provide the following details:
   - **Subscription**: Choose a subscription. We recommend choosing the same subscription as the subscription of the Console agent.
   - **Resource group**: Use an existing resource group or create a new one.
   - **Region**: Optionally, select the same region as the Console agent.
   - **Name**: Enter a name for the resource.
4. Optionally, add tags.
5. Click **Create**.

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.

If you created a user-assigned managed identity, while creating the key vault, you should also create an access policy for the key vault.

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 systems, HA pairs in multiple zones, and HA single AZ deployments)

       Usage of Azure customer-managed encryption keys is contingent upon having Azure Disk encryption enabled for the key vault.

   - The following option should be enabled if you created a user-assigned managed identity:
     - **Vault access policy**
2. If you selected Vault access policy, click Create to create an access policy for the key vault. If not, skip to step 3.
   a. Select the following permissions:
      - get
      - list
      - decrypt
      - encrypt
      - unwrap key

- wrap key
- verify
- sign

b. Select the user-assigned managed identity (resource) as the principal.

c. Review and create the access policy.

3. 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 system 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 API.

Required permissions

If you want to use a customer-managed key with a single node Cloud Volumes ONTAP system, ensure that the Console agent 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",
"Microsoft.ManagedIdentity/userAssignedIdentities/assign/action"
```

View the latest list of permissions

Steps

1. Obtain the list of key vaults in your Azure subscription by using the following 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 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 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"
      }
      ```

      Include the `"userAssignedIdentity": " userAssignedIdentityId"` field if you created this resource to be used for storage account encryption.

      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"
      }
      ```

      Include the `"userAssignedIdentity": " userAssignedIdentityId"` field if you created this resource to be used for storage account encryption.

      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.

Set up licensing for Cloud Volumes ONTAP in Azure

After you decide which licensing option you want to use with Cloud Volumes ONTAP, a few steps are required before you can choose that licensing option when creating a new system.

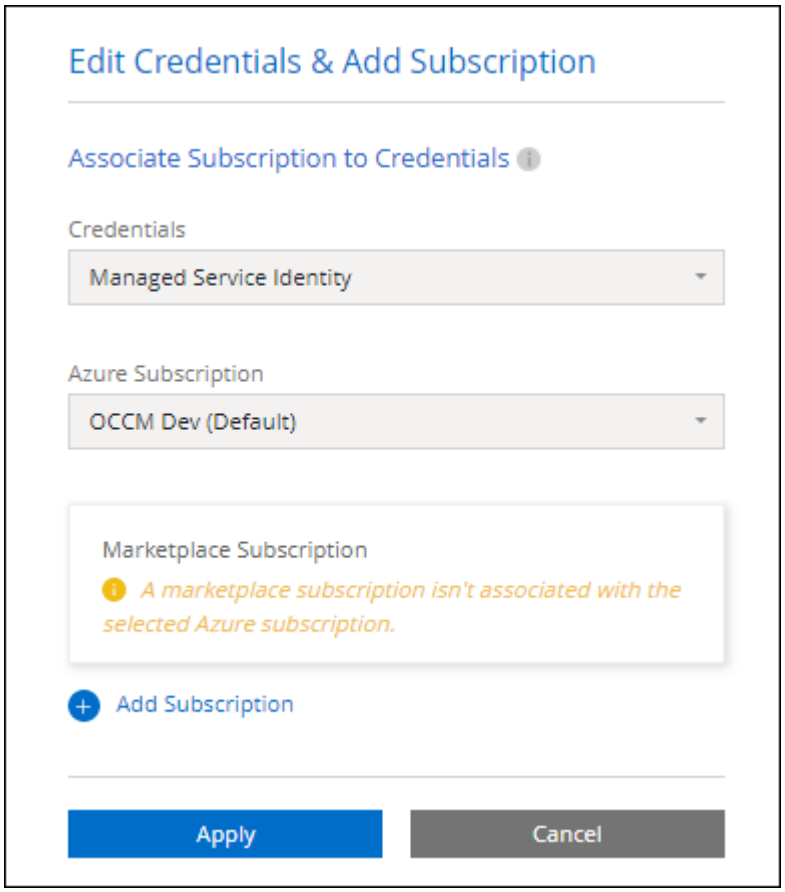
Freemium

Select the Freemium offering to use Cloud Volumes ONTAP free of charge with up to 500 GiB of provisioned capacity. Learn more about the Freemium offering.

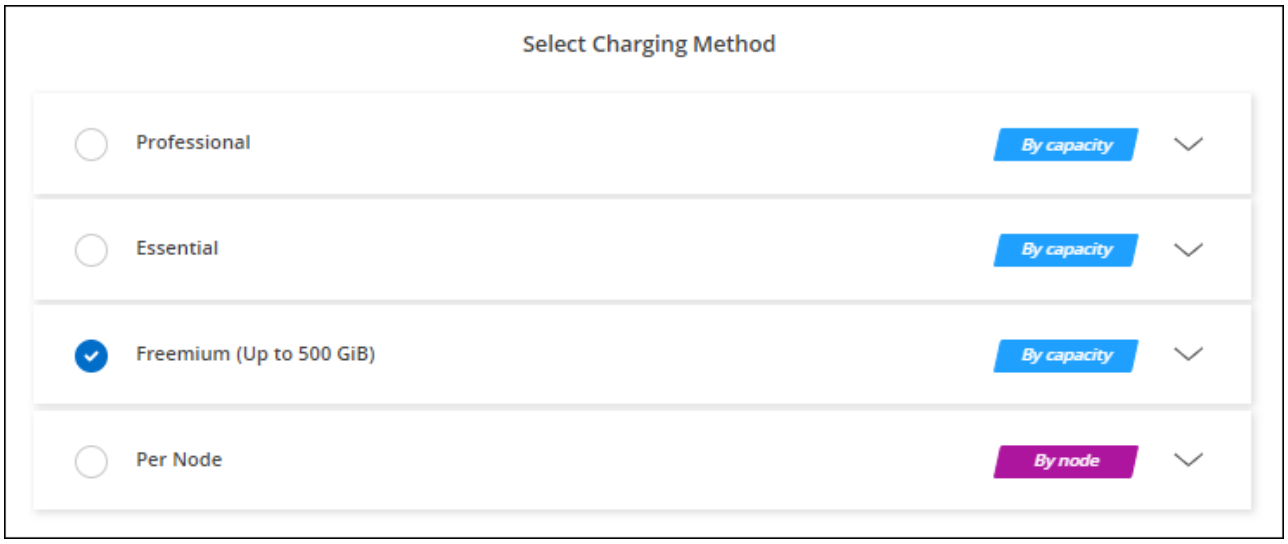
Steps

1. From the left navigation menu of the NetApp Console, select **Storage > Management**.
2. On the **Systems** page, click **Add System** and follow the steps.
   a. On the **Details and Credentials** page, click **Edit Credentials > Add Subscription** and then follow the prompts to subscribe to the pay-as-you-go offering in the Azure Marketplace.

      You won't be charged through the marketplace subscription unless you exceed 500 GiB of provisioned capacity, at which time the system is automatically converted to the Essentials package.



   b. After you return to the Console, select **Freemium** when you reach the charging methods page.



View step-by-step instructions to launch Cloud Volumes ONTAP in Azure.

Capacity-based license

Capacity-based licensing enables you to pay for Cloud Volumes ONTAP per TiB of capacity. Capacity-based licensing is available in the form of a *package*: the Essentials package or the Professional package.

The Essentials and Professional packages are available with the following consumption models or purchase options:

- A license (bring your own license (BYOL)) purchased from NetApp
- An hourly, pay-as-you-go (PAYGO) subscription from the Azure Marketplace
- An annual contract

Learn more about capacity-based licensing.

The following sections describe how to get started with each of these consumption models.

BYOL

Pay upfront by purchasing a license (BYOL) from NetApp to deploy Cloud Volumes ONTAP systems in any cloud provider.

NetApp has restricted the purchase, extension, and renewal of BYOL licensing. For more information, refer to Restricted availability of BYOL licensing for Cloud Volumes ONTAP.

Steps

1. Contact NetApp Sales to obtain a license
2. Add your NetApp Support Site account to the Console

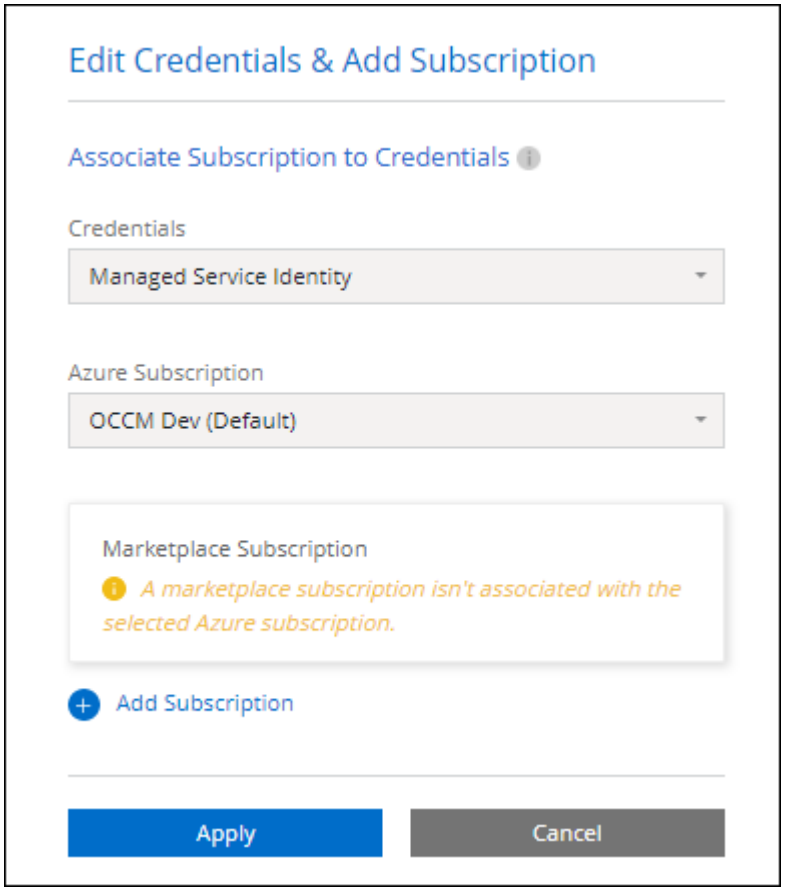
   The Console automatically queries NetApp's licensing service to obtain details about the licenses associated with your NetApp Support Site account. If there are no errors, the Console automatically adds the licenses to the Console.

   Your license must be available from the Console before you can use it with Cloud Volumes ONTAP. If

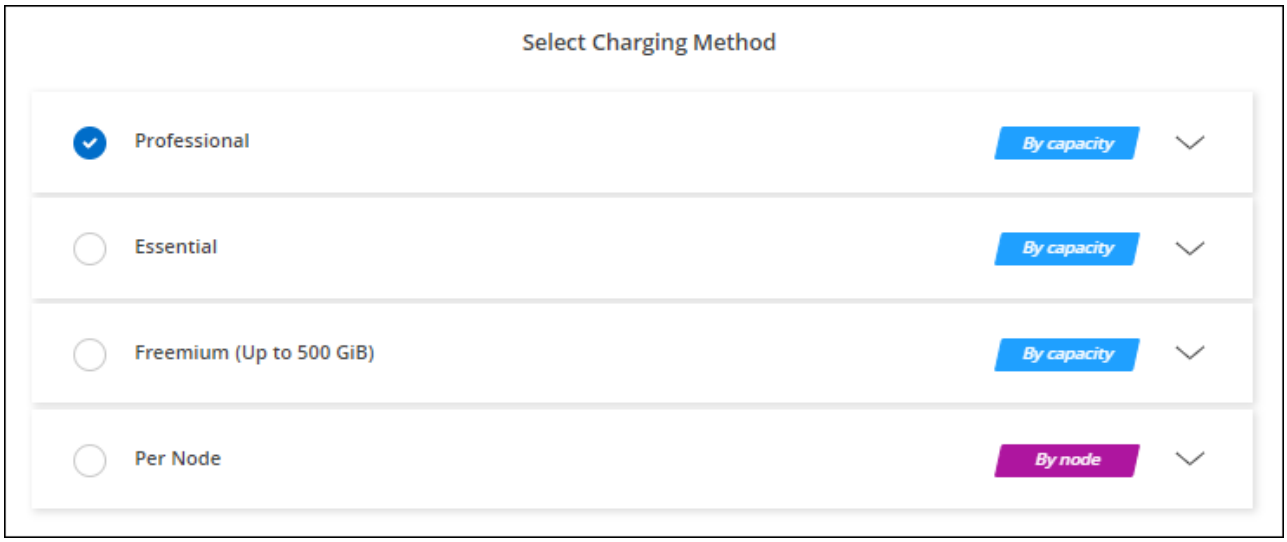
needed, you can manually add the license to the Console.

3. On the **Systems** page, click **Add System** and follow the steps.
   a. On the **Details and Credentials** page, click **Edit Credentials > Add Subscription** and then follow the prompts to subscribe to the pay-as-you-go offering in the Azure Marketplace.

      The license that you purchased from NetApp is always charged first, but you'll be charged from the hourly rate in the marketplace if you exceed your licensed capacity or if the term of your license expires.



   b. After you return to the Console, select a capacity-based package when you reach the charging methods page.



View step-by-step instructions to launch Cloud Volumes ONTAP in Azure.

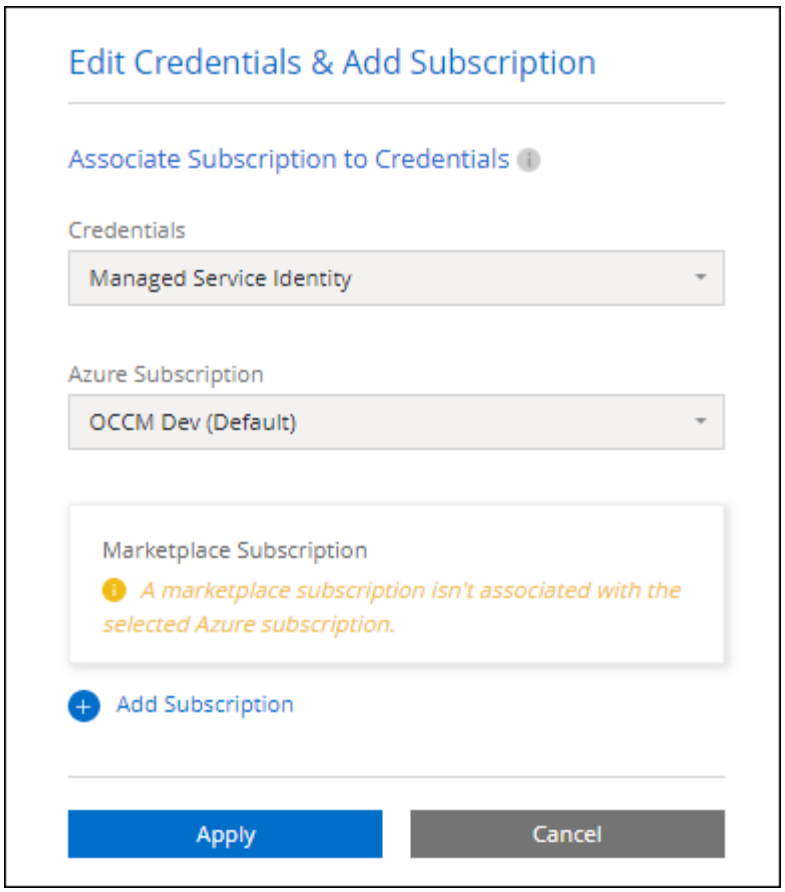
PAYGO subscription

Pay hourly by subscribing to the offer from your cloud provider's marketplace.

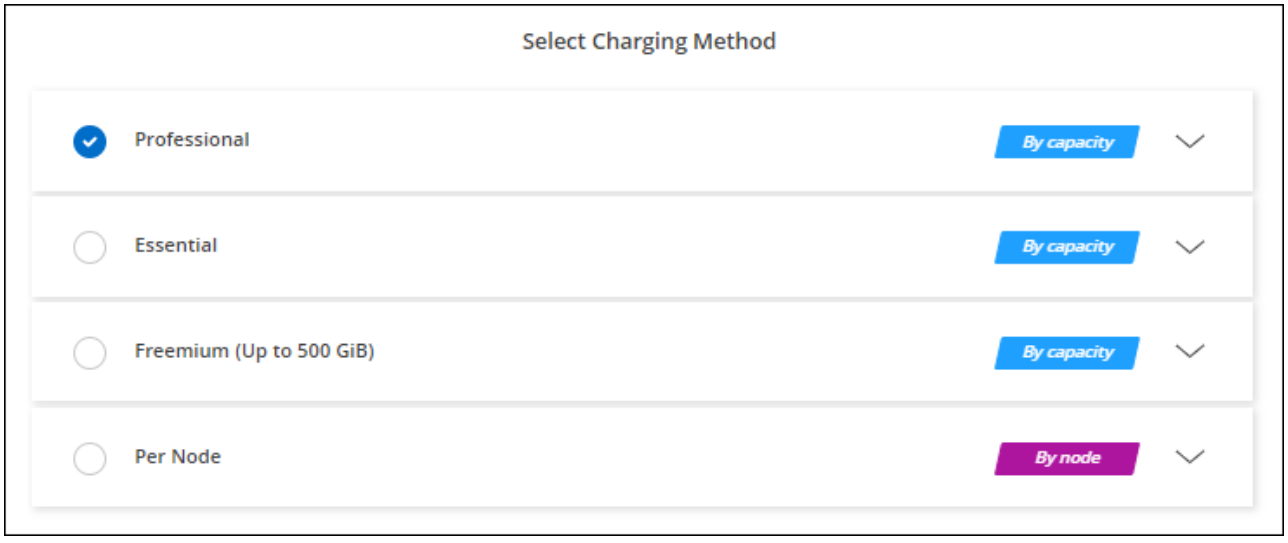
When you create a Cloud Volumes ONTAP system, the Console prompts you to subscribe to the agreement that's available in the Azure Marketplace. That subscription is then associated with the system for charging. You can use that same subscription for additional systems.

Steps

1. From the left navigation menu, select **Storage > Management**.
2. On the **Systems** page, click **Add System** and follow the steps.
   a. On the **Details and Credentials** page, click **Edit Credentials > Add Subscription** and then follow the prompts to subscribe to the pay-as-you-go offering in the Azure Marketplace.



b. After you return to the Console, select a capacity-based package when you reach the charging methods page.



View step-by-step instructions to launch Cloud Volumes ONTAP in Azure.

You can manage the Azure Marketplace subscriptions associated with your Azure accounts from the Settings > Credentials page. Learn how to manage your Azure accounts and subscriptions

Annual contract

Pay for Cloud Volumes ONTAP annually by purchasing an annual contract.

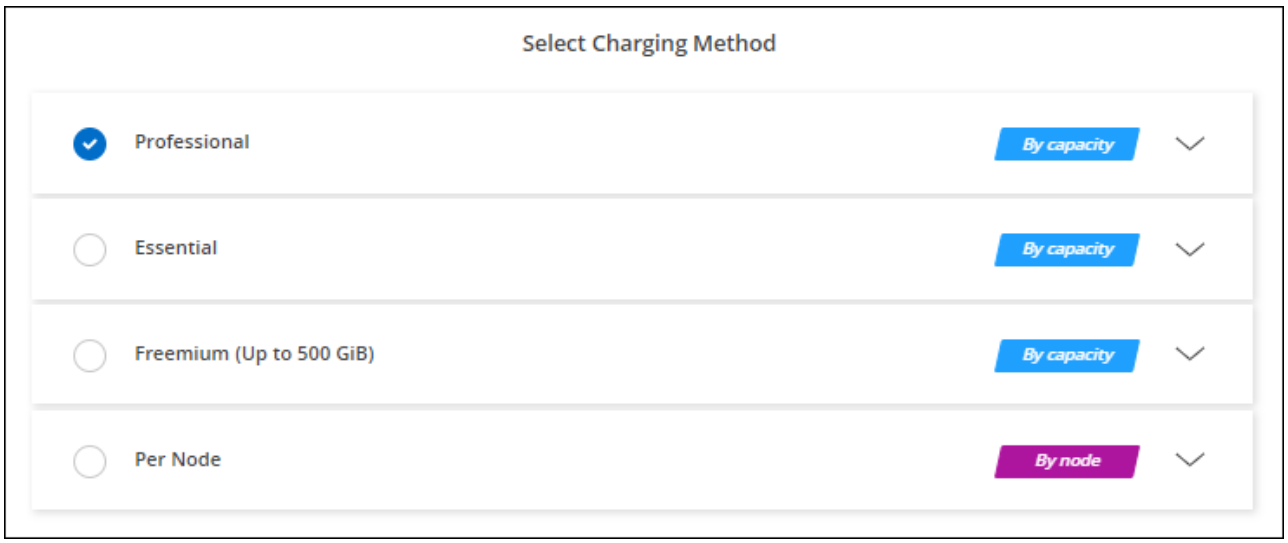
Steps

1. Contact your NetApp sales representative to purchase an annual contract.

   The contract is available as a *private* offer in the Azure Marketplace.

   After NetApp shares the private offer with you, you can select the annual plan when you subscribe from the Azure Marketplace during system creation.

2. On the **Systems** page, click **Add System** and follow the steps.
   a. On the **Details and Credentials** page, click **Edit Credentials > Add Subscription > Continue**.
   b. In the Azure portal, select the annual plan that was shared with your Azure account and then click **Subscribe**.
   c. After you return to the Console, select a capacity-based package when you reach the charging methods page.



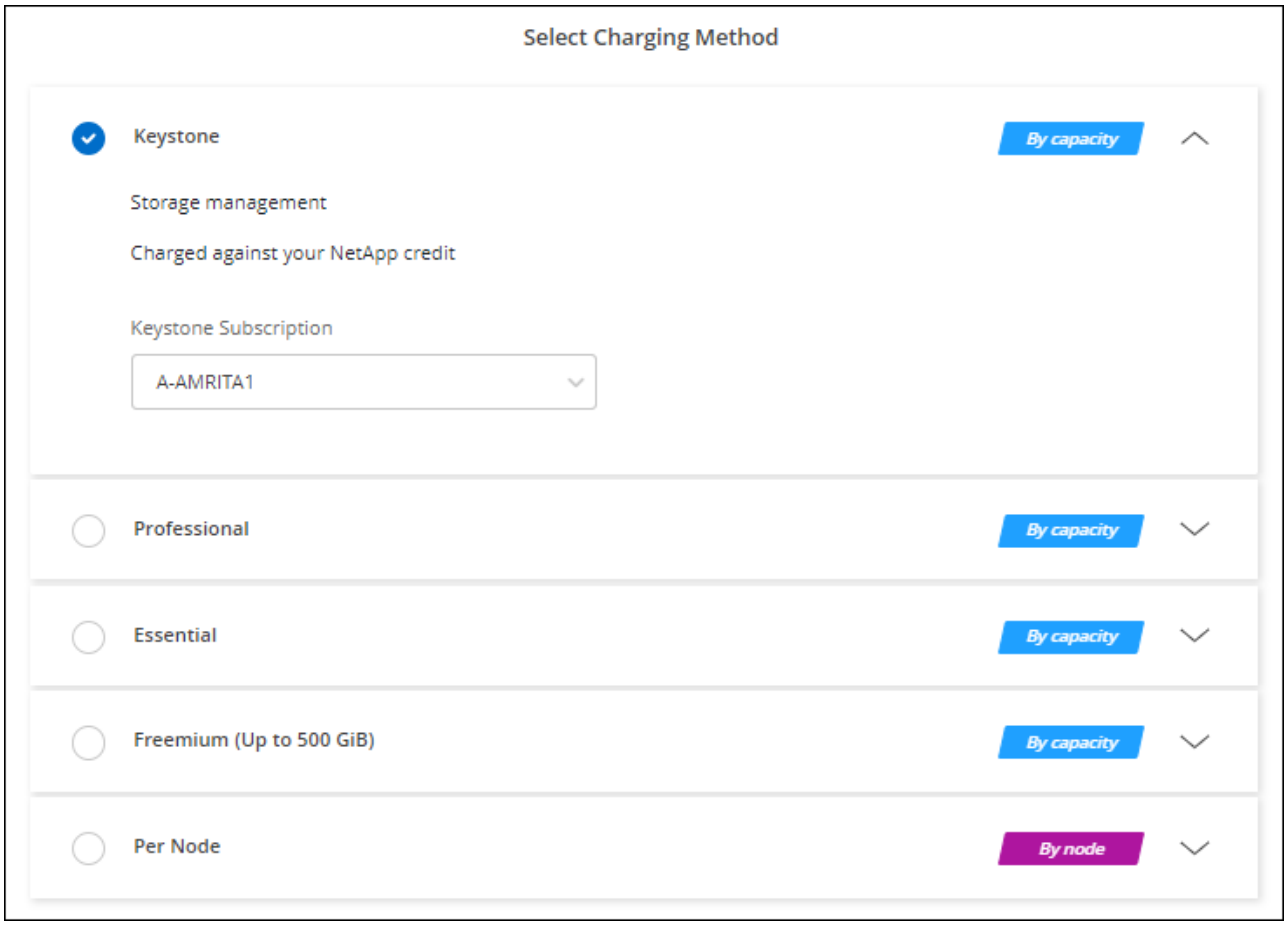
View step-by-step instructions to launch Cloud Volumes ONTAP in Azure.

Keystone Subscription

A Keystone Subscription is a pay-as-you-grow subscription-based service. Learn more about NetApp Keystone Subscriptions.

Steps

1. If you don’t have a subscription yet, contact NetApp
2. Contact NetApp to authorize your user account in the Console with one or more Keystone Subscriptions.
3. After NetApp authorizes your account, link your subscriptions for use with Cloud Volumes ONTAP.
4. On the **Systems** page, click **Add System** and follow the steps.
   a. Select the Keystone Subscription charging method when prompted to choose a charging method.



View step-by-step instructions to launch Cloud Volumes ONTAP in Azure.

Node-based license

A node-based license is the previous generation license for Cloud Volumes ONTAP. A node-based license could be procured from NetApp (BYOL) and is available for license renewals, only in specific cases. For information, refer to:

- End of availability for node-based licenses
- End of availability of node-based licenses
- Convert a node-based license to a capacity-based license

Enable high-availability mode for Cloud Volumes ONTAP in Azure

Microsoft Azure's high-availability (HA) mode should be enabled to reduce unplanned failover times and to enable NFSv4 support for Cloud Volumes ONTAP. In this mode, your Cloud Volumes ONTAP HA nodes can achieve a low (60 seconds) recovery time objective (RTO) during unplanned failovers on CIFS and NFSv4 clients.

Beginning with Cloud Volumes ONTAP 9.10.1, we reduced the unplanned failover time for Cloud Volumes ONTAP HA pairs running in Microsoft Azure and added support for NFSv4. To make these enhancements available to Cloud Volumes ONTAP, you need to enable the high-availability feature on your Azure

subscription.

NetApp Console prompts you with these details when the feature needs to be enabled on an Azure subscription.

Note the following:

- There are no problems with the high availability of your Cloud Volumes ONTAP HA pair. This Azure feature works in concert with ONTAP to reduce the client observed application outage time for NFS protocols that result from unplanned failover events.
- Enabling this feature is non-disruptive to Cloud Volumes ONTAP HA pairs.
- Enabling this feature on your Azure subscription doesn't cause issues to other VMs.
- Cloud Volumes ONTAP uses an internal Azure Load Balancer during failovers of cluster and SVM management LIFs on CIFS and NFS clients.
- When the HA mode is enabled, the Console scans the system every 12 hours to update the internal Azure Load Balancer rules.

An Azure user who has "Owner" privileges can enable the feature from the Azure CLI.

Steps

1. Access the Azure Cloud Shell from the Azure Portal
2. Register the high-availability mode feature:

```
az account set -s AZURE_SUBSCRIPTION_NAME_OR_ID
az feature register --name EnableHighAvailabilityMode --namespace
Microsoft.Network
az provider register -n Microsoft.Network
```

3. Optionally verify that the feature is now registered:

```
az feature show --name EnableHighAvailabilityMode --namespace
Microsoft.Network
```

   The Azure CLI should return a result similar to the following:

```
{
  "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"
}
```

Enable VMOrchestratorZonalMultiFD for Cloud Volumes ONTAP in Azure

For deploying VM instances in locally-redundant storage (LRS) single availability zones (AZ), you should activate the Microsoft `Microsoft.Compute/VMOrchestratorZonalMultiFD` feature for your subscriptions. In a high-availability (HA) mode, this feature facilitates deploying nodes in separate fault domains in the same availability zone.

Unless you activate this feature, zonal deployment doesn't occur, and the previous LRS non-zonal deployment becomes effective.

For information about VM deployment in single availability zone, refer to High-availability pairs in Azure.

Perform these steps as a user with "Owner" privileges:

Steps

1. Access Azure Cloud Shell from the Azure portal. For information, refer to the Microsoft Azure documentation: Get started with Azure Cloud Shell.
2. Register for the `Microsoft.Compute/VMOrchestratorZonalMultiFD` feature by running this command:

```
az account set -s <Azure_subscription_name_or_ID>
az feature register --name VMOrchestratorZonalMultiFD --namespace Microsoft.Compute
```

3. Verify the registration status and output sample:

```
az feature show -n VMOrchestratorZonalMultiFD --namespace Microsoft.Compute
{
"id": "/subscriptions/
<ID>/providers/Microsoft.Features/providers/Microsoft.Compute/features/VMOrchestratorZonalMultiF
D",
"name": "Microsoft.Compute/VMOrchestratorZonalMultiFD",
"properties": {
"state": "Registered"
},
"type": "Microsoft.Features/providers/features"
}
```

Launch Cloud Volumes ONTAP in Azure

You can launch a single node system or an HA pair in Azure by creating a Cloud Volumes ONTAP system in NetApp Console.

Before you begin

You need the following before you begin.

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

  You should have a configuration planned, and the necessary Azure networking details from your administrator. For more information, refer to Planning your Cloud Volumes ONTAP configuration.

- An understanding of what's required to set up licensing for Cloud Volumes ONTAP.

  Learn how to set up licensing.

About this task

When the Console 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 the Console 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.

Launch a single-node Cloud Volumes ONTAP system in Azure

If you want to launch a single-node Cloud Volumes ONTAP system in Azure, you need to create an single node system in the Console.

Steps

1. From the left navigation menu, select **Storage > Management**.
2. On the **Systems** page, click **Add System** and follow the prompts.
3. **Choose a Location**: Select **Microsoft Azure** and **Cloud Volumes ONTAP Single Node**.
4. If you're prompted, create a Console agent.
5. **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
System Name	The Console uses the system 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.

Field	Description
Resource Group Tags	Tags are metadata for your Azure resources. When you enter tags in this field, the Console 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 system, and then you can add more after it's created. Note that the API does not limit you to four tags when creating a system. For information about tags, refer to the Microsoft Azure Documentation: Using tags to organize your Azure resources.
User name and password	These are the credentials for the Cloud Volumes ONTAP cluster administrator account. You can use these credentials to connect to Cloud Volumes ONTAP through ONTAP System Manager or the ONTAP CLI. Keep the default *admin* user name or change it to a custom user name.
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.

6. **Services**: Enable or disable the individual services that you want to or don't want to use with Cloud Volumes ONTAP.
   - Learn more about NetApp Data Classification
   - Learn more about NetApp Backup and Recovery

   If you would like to utilize WORM and data tiering, you must disable Backup and Recovery and deploy a Cloud Volumes ONTAP system with version 9.8 or above.

7. **Location**: Select a region, availability zone, VNet, and subnet, and then select the checkbox to confirm network connectivity between the Console agent and the target location.

   For China regions, single node deployments are supported only in Cloud Volumes ONTAP 9.12.1 GA and 9.13.0 GA. You can upgrade these versions to later patches and releases of Cloud Volumes ONTAP as supported in Azure. If you want to deploy later Cloud Volumes ONTAP versions in China regions, contact NetApp Support. Only licenses purchased directly from NetApp are supported in China regions, marketplace subscriptions are not available.

8. **Connectivity**: Choose a new or existing resource group and then choose whether to use the predefined security group or to use your own.

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

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. If the Azure account that you're using has the required permissions, the Console removes Cloud Volumes ONTAP resources from a resource group, in case of deployment failure or deletion.
Generated security group	If you let the Console generate the security group for you, you need to choose how you'll allow traffic: • If you choose **Selected VNet only**, the source for inbound traffic is the subnet range of the selected VNet and the subnet range of the VNet where the Console agent resides. This is the recommended option. • If you choose **All VNets**, the source for inbound traffic is the 0.0.0.0/0 IP range.
Use existing	If you choose an existing security group, then it must meet Cloud Volumes ONTAP requirements. View the default security group.

9. **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 licensing options for Cloud Volumes ONTAP.
   - Learn how to set up licensing.
10. **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.

11. **Licensing**: Change the Cloud Volumes ONTAP version if required, and select a virtual machine type.

    If a newer Release Candidate, General Availability, or patch release is available for the selected version, then BlueXP updates the system to that version when creating the working environment. For example, the update occurs if you select Cloud Volumes ONTAP 9.16.1 P3 and 9.16.1 P4 is available. The update does not occur from one release to another—for example, from 9.15 to 9.16.

12. **Subscribe from the Azure Marketplace**: You see this page if the Console could not enable programmatic deployments of Cloud Volumes ONTAP. Follow the steps listed on the screen. refer to Programmatic deployment of Marketplace products for more information.
13. **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:

- If the public access to your storage account is disabled within the VNet, you cannot enable data tiering in your Cloud Volumes ONTAP system. For information, refer to Security group rules.
- 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 the Console 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, refer to 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.

14. **Write Speed & WORM**:
    a. Choose **Normal** or **High** write speed, if desired.

       Learn more about write speed.

    b. Activate write once, read many (WORM) storage, if desired.

       This option is only available for certain VM types. To find out which VM types are supported, refer to Supported configurations by license for HA pairs.

       WORM can't be enabled if data tiering was enabled for Cloud Volumes ONTAP versions 9.7 and below. Reverting or downgrading to Cloud Volumes ONTAP 9.8 is blocked after enabling WORM and tiering.

       Learn more about WORM storage.

    c. If you activate WORM storage, select the retention period.
15. **Create Volume**: Enter details for the new volume or click **Skip**.

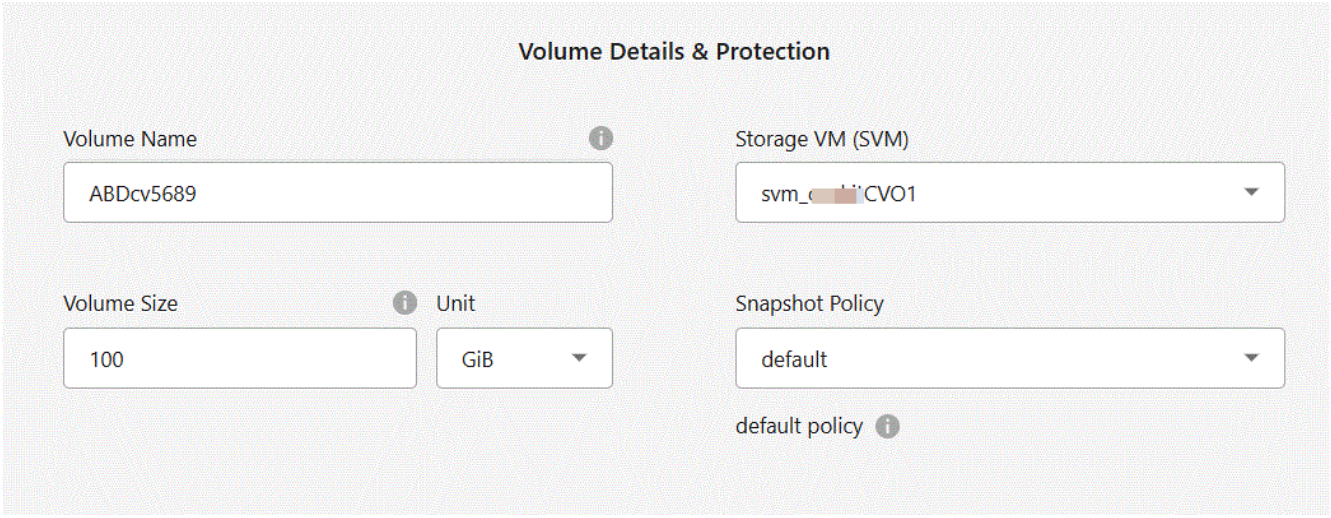
    Learn about supported client protocols and versions.

    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, the Console 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, the Console 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 first page of the volume creation wizard:



16. **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. Refer to the NetApp Console automation docs for details. Note that you can configure an NTP server only when creating a CIFS server. It's not configurable after you create the CIFS server.

17. **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, refer to Understanding volume usage profiles and Data tiering overview.

18. **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 the Console will purchase.
    c. Select the **I understand…** check boxes.
    d. Click **Go**.

Result

The Console deploys the Cloud Volumes ONTAP system. You can track the progress on the Audit page.

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

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

After the deployment process completes, do not modify the system-generated Cloud Volumes ONTAP configurations in the Azure portal, especially the system tags. Any changes made to these configurations may lead to unexpected behavior or data loss.

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 ONTAP System Manager or the ONTAP CLI.

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

Launch a Cloud Volumes ONTAP HA pair in Azure

If you want to launch a Cloud Volumes ONTAP HA pair in Azure, you need to create an HA system in the Console.

Steps

1. From the left navigation menu, select **Storage > Management**.
2. On the **Systems** page, click **Add System** and follow the prompts.
3. If you're prompted, create a Console agent.
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
System Name	The Console uses the system 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, the Console 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 system, and then you can add more after it's created. Note that the API does not limit you to four tags when creating a system. For information about tags, refer to the Microsoft Azure Documentation: Using tags to organize your Azure resources.
User name and password	These are the credentials for the Cloud Volumes ONTAP cluster administrator account. You can use these credentials to connect to Cloud Volumes ONTAP through ONTAP System Manager or the ONTAP CLI. Keep the default *admin* user name or change it to a custom user name.
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.

5. **Services**: Enable or disable the individual services based on whether you want to use them with Cloud Volumes ONTAP.
   - Learn more about NetApp Data Classification

◦ Learn more about NetApp Backup and Recovery

If you would like to utilize WORM and data tiering, you must disable Backup and Recovery and deploy a Cloud Volumes ONTAP system with version 9.8 or above.

6. **HA Deployment Models**:
   a. Select **Single Availability Zone** or **Multiple Availability Zone**.
      - For single availability zones, select an Azure region, availability zone, VNet, and subnet.

        Beginning with Cloud Volumes ONTAP 9.15.1, you can deploy virtual machine (VM) instances in HA mode in single availability zones (AZs) in Azure. You need to select a zone and a region that support this deployment. If the zone or the region does not support zonal deployment, then the previous non-zonal deployment mode for LRS is followed. For understanding the supported configurations for shared managed disks, refer to HA single availability zone configuration with shared managed disks.

      - For multiple availability zones, select a region, VNet, subnet, zone for node 1, and zone for node 2.
   b. Select the **I have verified network connectivity…** check box.
7. **Connectivity**: Choose a new or existing resource group and then choose whether to use the predefined security group or to use your own.

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

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. The Console 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, the Console removes Cloud Volumes ONTAP resources from a resource group, in case of deployment failure or deletion.
Generated security group	If you let the Console generate the security group for you, you need to choose how you'll allow traffic: • If you choose **Selected VNet only**, the source for inbound traffic is the subnet range of the selected VNet and the subnet range of the VNet where the Console agent resides. This is the recommended option. • If you choose **All VNets**, the source for inbound traffic is the 0.0.0.0/0 IP range.

Field	Description
Use existing	If you choose an existing security group, then it must meet Cloud Volumes ONTAP requirements. View the default security group.

8. **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 licensing options for Cloud Volumes ONTAP.
   - Learn how to set up licensing.
9. **Preconfigured Packages**: Select one of the packages to quickly deploy a Cloud Volumes ONTAP system, or click **Change configuration**.

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

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

    If a newer Release Candidate, General Availability, or patch release is available for the selected version, then the Console updates the system to that version when creating it. For example, the update occurs if you select Cloud Volumes ONTAP 9.13.1 and 9.13.1 P4 is available. The update does not occur from one release to another— for example, from 9.13 to 9.14.

11. **Subscribe from the Azure Marketplace**: Follow the steps if the Console could not enable programmatic deployments of Cloud Volumes ONTAP.
12. **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 size is for all disks in the initial aggregate and for any additional aggregates that the Console 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 size, refer to Size your system in Azure.

    - If the public access to your storage account is disabled within the VNet, you cannot enable data tiering in your Cloud Volumes ONTAP system. For information, refer to Security group rules.
    - 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.

    - Starting with Cloud Volumes ONTAP 9.15.0P1, Azure page blobs are no longer supported for new high-availability pair deployments. If you currently use Azure page blobs in existing high-availability pair deployments, you can migrate to newer VM instance types in the Edsv4-series VMs and Edsv5-series VMs.

      Learn more about supported configurations in Azure.

13. **Write Speed & WORM**:

a. Choose **Normal** or **High** write speed, if desired.

   Learn more about write speed.

b. Activate write once, read many (WORM) storage, if desired.

   This option is only available for certain VM types. To find out which VM types are supported, refer to Supported configurations by license for HA pairs.

   WORM can't be enabled if data tiering was enabled for Cloud Volumes ONTAP versions 9.7 and below. Reverting or downgrading to Cloud Volumes ONTAP 9.8 is blocked after enabling WORM and tiering.

   Learn more about WORM storage.

c. If you activate WORM storage, select the retention period.

14. **Secure Communication to Storage & WORM**: 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 page blob storage accounts. Note that enabling this option can impact write performance. You can't change the setting after you create the system.

    Learn more about WORM storage.

    WORM can't be enabled if data tiering was enabled.

    Learn more about WORM storage.

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

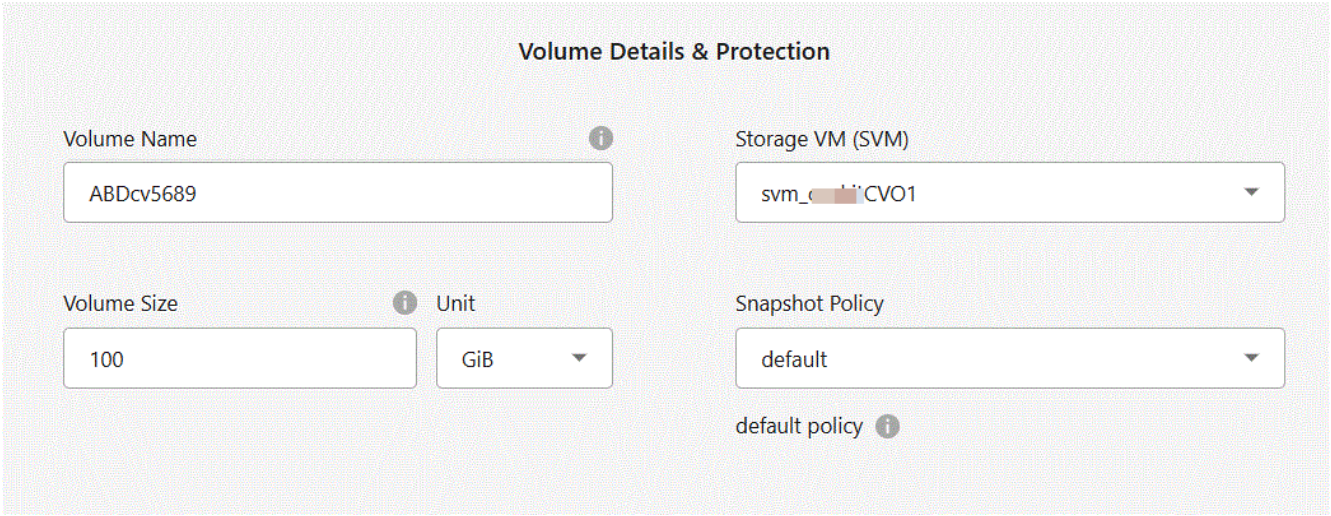
    Learn about supported client protocols and versions.

    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, the Console 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.
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.

Field	Description
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, the Console 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 first page of the volume creation wizard:



16. **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.
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.

Field	Description
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. Refer to the NetApp Console automation docs for details. Note that you can configure an NTP server only when creating a CIFS server. It's not configurable after you create the CIFS server.

17. **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, refer to Choose a volume usage profile, Data tiering overview, and KB: What Inline Storage Efficiency features are supported with CVO?

18. **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 the Console will purchase.
    c. Select the **I understand…** check boxes.
    d. Click **Go**.

Result

The Console deploys the Cloud Volumes ONTAP system. You can track the progress on the Audit page.

If you experience any issues deploying the Cloud Volumes ONTAP system, review the failure message. You can also select the system 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 ONTAP System Manager or the ONTAP CLI.

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

After the deployment process completes, do not modify the system-generated Cloud Volumes ONTAP configurations in the Azure portal, especially the system tags. Any changes made to these configurations may lead to unexpected behavior or data loss.

Related links

*Planning your Cloud Volumes ONTAP configuration in Azure
*Deploy Cloud Volumes ONTAP in Azure from the Azure Marketplace

Verify Azure platform image

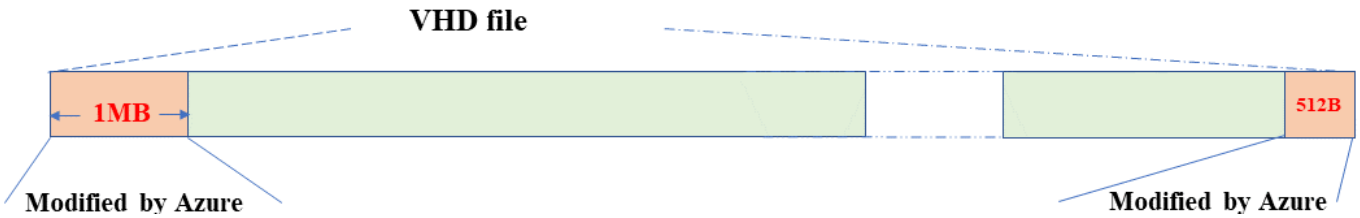
Azure marketplace image verification for Cloud Volumes ONTAP

Azure image verification complies with enhanced NetApp security requirements. Verifying an image file is a straightforward process. However, the Azure image signature verification requires specific considerations for the Azure VHD image file because it is altered in the Azure marketplace.

Azure image verification is supported on Cloud Volumes ONTAP 9.15.0 and later.

Azure's alteration of published VHD files

The 1 MB (1048576 bytes) at the beginning and 512 bytes at the end of the VHD file is modified by Azure. NetApp signs the remaining VHD file.



In the example, the VHD file is of 10GB. The portion that NetApp signed is marked in green (10 GB - 1 MB - 512 bytes).

Related links

- Page Fault Blog: How to sign and verify using OpenSSL
- Use Azure Marketplace image to create VM image for your Azure Stack Edge Pro GPU | Microsoft Learn
- Export/Copy a managed disk to a storage account using the Azure CLI | Microsoft Learn
- Azure Cloud Shell Quickstart - Bash | Microsoft Learn
- How to install the Azure CLI | Microsoft Learn
- az storage blob copy | Microsoft Learn
- Sign in with Azure CLI — Login and Authentication | Microsoft Learn

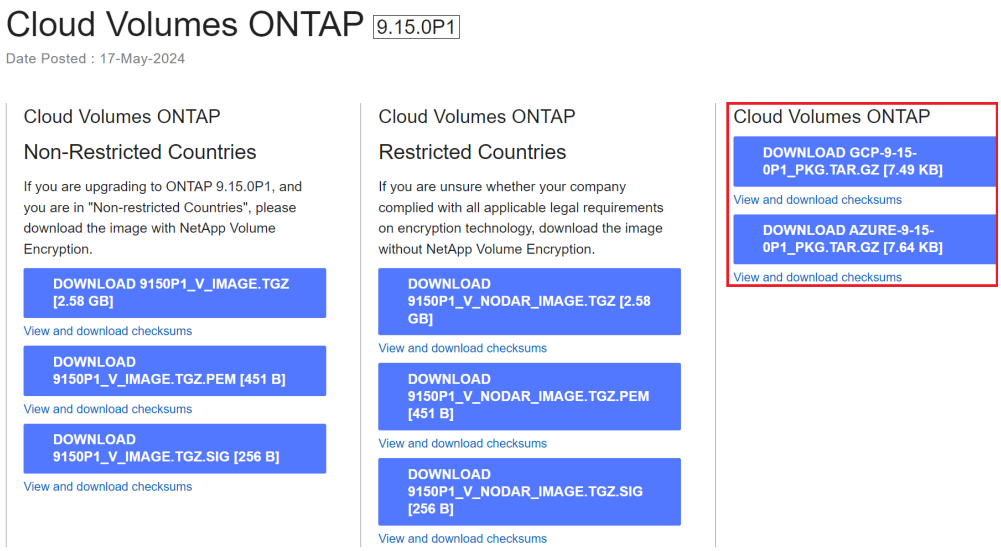
Download the Azure image file for Cloud Volumes ONTAP

You can download the Azure image file from the NetApp Support Site.

The *tar.gz* file contains the files required for image signature verification. Along with the *tar.gz* file, you should also download the *checksum* file for the image. The checksum file contains the `md5` and `sha256` checksums of the *tar.gz* file.

Steps

1. Go to the Cloud Volumes ONTAP product page on the NetApp Support Site and download the required software version from the **Downloads** section.
2. On the Cloud Volumes ONTAP download page, click the downloadable file for the Azure image and download the *tar.gz* file.



3. On Linux, run `md5sum AZURE-<version>_PKG.TAR.GZ`.

   On macOS, run `sha256sum AZURE-<version>_PKG.TAR.GZ`.

4. Verify that the `md5sum` and `sha256sum` values match those in the downloaded Azure image.
5. On Linux and macOS, extract the *tar.gz* file using the `tar -xzf` command.

   The extracted *tar.gz* file contains the digest (*.sig*) file, public key certificate (*.pem*) file, and chain certificate (*.pem*) file.

   Example output after extracting the tar.gz file:

```
$ 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
```

Export VHD images for Cloud Volumes ONTAP from the Azure marketplace

Once the VHD image is published to Azure cloud, it is no longer managed by NetApp. Instead, the published image is placed on the Azure marketplace. When the image is staged and published on the Azure marketplace, Azure modifies 1 MB at the beginning and 512 bytes at the end of the VHD. To verify the signature of the VHD file, you need to export the VHD image modified by Azure from the Azure marketplace.

Before you begin

Ensure that the Azure CLI is installed on your system, or the Azure Cloud Shell is available through the Azure portal. For more information about how to install the Azure CLI, refer to the Microsoft documentation: How to install the Azure CLI.

Steps

1. Map the Cloud Volumes ONTAP version on your system to the Azure marketplace image version using the contents of the *version_readme* file. The Cloud Volumes ONTAP version is represented by `buildname` and the Azure marketplace image version is represented by `version` in the version mappings.

   In the following example, the Cloud Volumes ONTAP version `9.15.0P1` is mapped to the Azure marketplace image version `9150.01000024.05090105`. This Azure marketplace image version is later used to set the image URN.

   ```
   [
    "buildname": "9.15.0P1",
       "publisher": "netapp",
        "version": "9150.01000024.05090105"

   ]
   ```

2. Identify the region where you want to create the VMs. The region name is used as the value for the `locName` variable when setting the URN of the marketplace image. To list the available regions, run this command:

   ```
   az account list-locations -o table
   ```

   In this table, the region name appears in the `Name` field.

   ```
   $ 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. Review the SKU names for the corresponding Cloud Volumes ONTAP versions and VM deployment types in the table below. The SKU name is used as the value for the `skuName` variable when setting the URN of the marketplace image.

   For example, all single node deployments with Cloud Volumes ONTAP 9.15.0 should use `ontap_cloud_byol` as the SKU name.

Cloud Volumes ONTAP version	VM deployment through	SKU name
9.17.1 and later	The Azure marketplace	ontap_cloud_direct_gen2
9.17.1 and later	The NetApp Console	ontap_cloud_gen2
9.16.1	The Azure marketplace	ontap_cloud_direct
9.16.1	The Console	ontap_cloud
9.15.1	The Console	ontap_cloud
9.15.0	The Console, single node deployments	ontap_cloud_byol
9.15.0	The Console, high availability (HA) deployments	ontap_cloud_byol_ha

4. After mapping the ONTAP version and Azure marketplace image, export the VHD file from the Azure marketplace using the Azure Cloud Shell or Azure CLI.

Export VHD file using the Azure Cloud Shell on Linux

From the Azure Cloud Shell, export the marketplace image to the VHD file (for example, *9150.01000024.05090105.vhd*), and download it to your local Linux system. Perform these steps to get the VHD image from the Azure marketplace.

Steps

1. Set the URN and other parameters of the marketplace image. The URN format is `<publisher>:<offer>:<sku>:<version>`. Optionally, you can list NetApp marketplace images to confirm the correct image version.

```
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. Create a new managed disk from the marketplace image with the matching image version:

```
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. Export the VHD file from the managed disk to Azure Storage. Create a container with the appropriate access level. In this example, we've used a container named `vm-images` with `Container` access level. Get the storage account access key from the Azure portal: **Storage Accounts > *examplesaname* > Access Key > *key1* > *key* > Show > <*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. Download the generated image to your Linux system. Use the `wget` command to download the VHD file:

```
wget <URL of filename/Containers/vm-images/9150.01000024.05090105.vhd>
```

The URL follows a standard format. For automation, you can derive the URL string as shown below. Alternatively, you can use the Azure CLI `az` command to get the URL.
Example URL:
https://examplesaname.bluexpinfraprod.eastus2.data.azurecr.io/vm-images/9150.01000024.05090105.vhd

5. Clean up the managed disk

```
PS /home/user1> Revoke-AzDiskAccess -ResourceGroupName $diskRG -DiskName
$diskName
PS /home/user1> Remove-AzDisk -ResourceGroupName $diskRG -DiskName
$diskName
```

Export VHD file using the Azure CLI on Linux

Export the marketplace image to a VHD file using the Azure CLI from a local Linux system.

Steps

1. Log in to the Azure CLI and list marketplace images:

```
% az login --use-device-code
```

2. To sign in, use a web browser to open the page https://microsoft.com/devicelogin and enter the authentication code.

```
% 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. Create a new managed disk from the marketplace image with the matching image version.

```
% 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"
```

To automate the process, the SAS needs to be extracted from the standard output. Refer to the appropriate documents for guidance.

4. Export the VHD file from the managed disk.
   a. Create a container with the appropriate access level. In this example, a container named `vm-images` with `Container` access level is used.
   b. Get the storage account access key from the Azure portal: **Storage Accounts > *examplesaname* > Access Key > *key1* > *key* > Show > <*copy*>**

      You can also use the `az` command for this step.

```
% export storageAccountName="examplesaname"
% export containerName="vm-images"
% export storageAccountKey="xxxxxxxxxx"
% export destBlobName="9150.01000024.05090105.vhd"

% az storage blob copy start --source-uri $diskAccessSAS
--destination-container $containerName --account-name
$storageAccountName --account-key $storageAccountKey --destination
-blob $destBlobName

{
  "client_request_id": "xxxx-xxxx-xxxx-xxxx-xxxx",
  "copy_id": "xxxx-xxxx-xxxx-xxxx-xxxx",
  "copy_status": "pending",
  "date": "2022-11-02T22:02:38+00:00",
  "etag": "\"0xXXXXXXXXXXXXXXXX\"",
  "last_modified": "2022-11-02T22:02:39+00:00",
  "request_id": "xxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx",
  "version": "2020-06-12",
  "version_id": null
}
```

5. Check the status of the blob copy.

```
% az storage blob show --name $destBlobName --container-name
$containerName --account-name $storageAccountName

....
    "copy": {
      "completionTime": null,
      "destinationSnapshot": null,
      "id": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxx",
      "incrementalCopy": null,
      "progress": "10737418752/10737418752",
      "source": "https://md-
xxxxxx.bluexpinfraprod.eastus2.data.azurecr.io/xxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx",
      "status": "success",
      "statusDescription": null
    },
....
```

6. Download the generated image to your Linux server.

```
wget <URL of file examplesaname/Containers/vm-
images/9150.01000024.05090105.vhd>
```

The URL follows a standard format. For automation, you can derive the URL string as shown below. Alternatively, you can use the Azure CLI `az` command to get the URL.
Example URL:
https://examplesaname.bluexpinfraprod.eastus2.data.azurecr.io/vm-images/9150.01000024.05090105.vhd

7. Clean up the managed disk

```
az disk revoke-access --name $diskName --resource-group $diskRG
az disk delete --name $diskName --resource-group $diskRG --yes
```

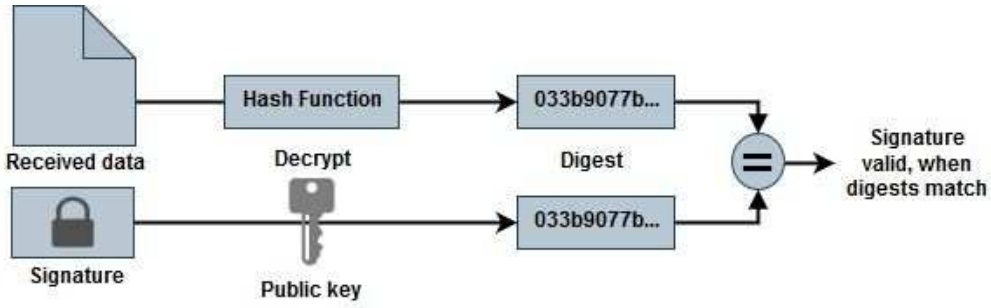
Verify file signature

Azure marketplace image signature verfication for Cloud Volumes ONTAP

The Azure image verification process generates a digest file from the VHD file by stripping 1 MB at the beginning and 512 bytes at the end, then applying a hash function. To match the signing procedure, *sha256* is used for hashing.

File signature verification workflow summary

The following is an overview of the file signature verification workflow process.



- Downloading the Azure image from the NetApp Support Site and extracting the digest (.sig) file, public key certificate (.pem) file, and chain certificate (.pem) file. Refer to Download the Azure image digest file for more information.
- Verification of the chain of trust.
- Extracting the public key (.pub) from the public key certificate (.pem).
- Decrypting the digest file by using the extracted public key.
- Comparing the result against a newly generated digest of a temporary file created from the image file after removing 1 MB at the beginning and 512 bytes at the end. This step is performed by using the OpenSSL command line tool. The OpenSSL CLI tool displays appropriate messaging on success or failure in matching the files.

```
openssl dgst -verify <public_key> -keyform <form> <hash_function>
-signature <digest_file> -binary <temporary_file>
```

Verify Azure marketplace image signature for Cloud Volumes ONTAP on Linux

Verification of an exported VHD file signature on Linux includes validating the chain of trust, editing the file, and verifying the signature.

Steps

1. Download the Azure image file from the NetApp Support Site and extract the digest (.sig) file, public key certificate (.pem) file, and chain certificate (.pem) file.

   Refer to Download the Azure image digest file for more information.

2. Verify the chain of trust.

```
% openssl verify -CAfile Certificate-Chain-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem: OK
```

3. Remove 1 MB (1,048,576 bytes) at the beginning and 512 bytes at the end of the VHD file. When using `tail`, the `-c +K` option generates bytes from the Kth byte of the file. Therefore, it passes 1048577 to `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. Use OpenSSL to extract the public key from the certificate and verify the stripped file (sign.tmp) with the signature file and the public key.

   The command prompt displays messages indicating success or failure based on the verification.

```
% 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. Clean up the workspace.

```
% rm ./9150.01000024.05090105.vhd ./sign.tmp
% rm *.sig *.pub *.pem
```

Verify Azure marketplace image signature for Cloud Volumes ONTAP on macOS

Verification of an exported VHD file signature on Linux includes validating the chain of trust, editing the file, and verifying the signature.

Steps

1. Download the Azure image file from the NetApp Support Site and extract the digest (.sig) file, public key certificate (.pem) file, and chain certificate (.pem) file.

   Refer to Download the Azure image digest file for more information.

2. Verify the chain of trust.

```
% openssl verify -CAfile Certificate-Chain-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem: OK
```

3. Remove 1MB (1,048,576 bytes) at the beginning and 512 bytes at the end of the VHD file. When using `tail`, the `-c +K` option generates bytes from the Kth byte of the file. Therefore, it passes 1048577 to `tail -c`. Note that on macOS, the tail command might take about ten minutes to complete.

```
% tail -c +1048577 ./9150.01000024.05090105.vhd > ./sign.tmp.tail
% head -c -512 ./sign.tmp.tail > sign.tmp
% rm ./sign.tmp.tail
```

4. Use OpenSSL to extract the public key from the certificate and verify the stripped file (sign.tmp) with the signature file and public key. The command prompt displays messages indicating success or failure based on the verification.

```
% 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. Clean up the workspace.

```
% rm ./9150.01000024.05090105.vhd ./sign.tmp
% rm *.sig *.pub *.pem
```

Copyright information

Trademark information