Manage Cloud Volumes ONTAP

Cloud Manager

NetApp
June 15, 2020

Table of Contents

Manage Cloud Volumes ONTAP 1
Deploy Cloud Volumes ONTAP 1
Provision and manage storage 37
Replicating data between systems 58
Backup to Cloud 66
Monitor performance 82
Administer Cloud Volumes ONTAP 90

Manage Cloud Volumes ONTAP

Deploy Cloud Volumes ONTAP

Before you create Cloud Volumes ONTAP systems

Before you use Cloud Manager to create and manage Cloud Volumes ONTAP systems, your Cloud Manager administrator should have prepared networking and installed and set up Cloud Manager.

The following conditions should exist before you start deploying Cloud Volumes ONTAP:

- Networking requirements were met for Cloud Manager and Cloud Volumes ONTAP.
- Cloud Manager has permissions to perform operations in your chosen cloud provider.
- Cloud Manager was installed.

Cloud Manager should remain running at all times.

Related links

- Getting started in AWS
- Getting started in Azure
- Getting started in GCP
- Setting up Cloud Manager

Planning your Cloud Volumes ONTAP configuration

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

Choosing a license type

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

- Supported configurations for Cloud Volumes ONTAP 9.7 in AWS
- Supported configurations for Cloud Volumes ONTAP 9.7 in Azure

- Supported configurations for Cloud Volumes ONTAP 9.7 in GCP

Understanding storage limits

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

- Storage limits for Cloud Volumes ONTAP 9.7 in AWS
- Storage limits for Cloud Volumes ONTAP 9.7 in Azure
- Storage limits for Cloud Volumes ONTAP 9.7 in GCP

Choosing a write speed

Cloud Manager enables you to choose a write speed setting for single node Cloud Volumes ONTAP systems. 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.

Difference between normal write speed and high write speed

When you choose normal write speed, data is written directly to disk, thereby reducing the likelihood of data loss in the event of an unplanned system outage.

When you choose high write speed, data is buffered in memory before it is written to disk, which provides faster write performance. Due to this caching, there is the potential for data loss if an unplanned system outage occurs.

The amount of data that can be lost in the event of an unplanned system outage is the span of the last two consistency points. A consistency point is the act of writing buffered data to disk. A consistency point occurs when the write log is full or after 10 seconds (whichever comes first). However, AWS EBS volume performance can affect consistency point processing time.

When to use high write speed

High write speed is a good choice if fast write performance is required for your workload and you can withstand the risk of data loss in the event of an unplanned system outage.

Recommendations when using high write speed

If you enable high write speed, you should ensure write protection at the application layer.

Choosing a volume usage profile

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

which profile to use.

NetApp storage efficiency features provide the following benefits:

Thin provisioning

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

Deduplication

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

Compression

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

AWS planning

Plan your deployment of Cloud Volumes ONTAP in AWS by sizing your system and reviewing the network information that you need to enter.

- Sizing your system in AWS
- AWS network information worksheet

Sizing your system in AWS

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 an instance type, disk type, and disk size:

Instance type

- Match your workload requirements to the maximum throughput and IOPS for each EC2 instance type.
- If several users write to the system at the same time, choose an instance type that has enough CPUs to manage the requests.
- If you have an application that is mostly reads, then choose a system with enough RAM.
  - AWS Documentation: Amazon EC2 Instance Types
  - AWS Documentation: Amazon EBS–Optimized Instances

EBS disk type

General Purpose SSDs are the most common disk type for Cloud Volumes ONTAP. To view the use cases for EBS disks, refer to AWS Documentation: EBS Volume Types.

EBS disk size

You need to choose an initial disk size when you launch a Cloud Volumes ONTAP system. After that, you can let Cloud Manager manage a system's capacity for you, but if you want to build aggregates yourself, be aware of the following:

- All disks in an aggregate must be the same size.
- The performance of EBS disks is tied to disk size. The size determines the baseline IOPS and maximum burst duration for SSD disks and the baseline and burst throughput for HDD disks.
- Ultimately, you should choose the disk size that gives you the *sustained performance* that you need.
- Even if you do choose larger disks (for example, six 4 TB disks), you might not get all of the IOPS because the EC2 instance can reach its bandwidth limit.

  For more details about EBS disk performance, refer to AWS Documentation: EBS Volume Types.

Watch the following video for more details about sizing your Cloud Volumes ONTAP system in AWS:

AWS network information worksheet

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

Network information for Cloud Volumes ONTAP

AWS information	Your value
Region	
VPC	
Subnet	
Security group (if using your own)	

Network information for an HA pair in multiple AZs

AWS information	Your value
Region	
VPC	
Security group (if using your own)	
Node 1 availability zone	
Node 1 subnet	
Node 2 availability zone	
Node 2 subnet	
Mediator availability zone	
Mediator subnet	
Key pair for the mediator	
Floating IP address for cluster management port	
Floating IP address for data on node 1	
Floating IP address for data on node 2	
Route tables for floating IP addresses	

Azure planning

Plan your deployment of Cloud Volumes ONTAP in Azure by sizing your system and reviewing the network information that you need to enter.

- Sizing your system in Azure
- Azure network information worksheet

Sizing your system in Azure

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

Virtual machine type

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

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

Azure disk type

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

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

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

  For additional details about the use cases for these disks, see Microsoft Azure Documentation: Introduction to Microsoft Azure Storage.

Azure disk size

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

All disks in an aggregate must be the same size.

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

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

Azure network information worksheet

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

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

GCP planning

Plan your deployment of Cloud Volumes ONTAP in Google Cloud Platform by sizing your system and reviewing the network information that you need to enter.

- Sizing your system in GCP
- GCP network information worksheet

Sizing your system in GCP

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 machine type, disk type, and disk size:

Machine type

Look at the supported machine types in the Cloud Volumes ONTAP Release Notes and then review details from Google about each supported machine type. Match your workload requirements to the number of vCPUs and memory for the machine type. Note that each CPU core increases networking performance.

Refer to the following for more details:

- Google Cloud documentation: N1 standard machine types
- Google Cloud documentation: Performance

GCP disk type

When you create volumes for Cloud Volumes ONTAP, you need to choose the underlying cloud storage that Cloud Volumes ONTAP uses for a disk. The disk type can be either *Zonal SSD persistent disks* or *Zonal standard persistent disks*.

SSD persistent disks are best for workloads that require high rates of random IOPS, while Standard persistent disks are economical and can handle sequential read/write operations. For more details, see Google Cloud documentation: Zonal Persistent disks (Standard and SSD).

GCP disk size

You need to choose an initial disk size when you deploy a Cloud Volumes ONTAP system. After that you can let Cloud Manager manage a system's capacity for you, but if you want to build aggregates yourself, be aware of the following:

- All disks in an aggregate must be the same size.
- Determine the space that you need, while taking performance into consideration.
- The performance of persistent disks scales automatically with disk size and the number of vCPUs available to the system.

  Refer to the following for more details:

  - Google Cloud documentation: Zonal Persistent disks (Standard and SSD)
  - Google Cloud documentation: Optimizing Persistent Disk and Local SSD Performance

GCP network information worksheet

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

GCP information	Your value
Region	
Zone	
VPC network	
Subnet	
Firewall policy (if using your own)	

Finding your Cloud Manager system ID

To help you get started, your NetApp representative might ask you for your Cloud Manager system ID. The ID is typically used for licensing and troubleshooting purposes.

Steps

1. In the upper right of the Cloud Manager console, click the Settings icon.

2. Click **Support Dashboard**.

   Your system ID appears in the top right.

   Example

Enabling Flash Cache on Cloud Volumes ONTAP

Some Cloud Volumes ONTAP configurations in AWS and Azure include local NVMe storage, which Cloud Volumes ONTAP uses as *Flash Cache* for better performance.

What's Flash Cache?

Flash Cache speeds access to data through real-time intelligent caching of recently read user data and NetApp metadata. It is effective for random read-intensive workloads, including databases, email, and file services.

Limitations

- Compression must be disabled on all volumes to take advantage of the Flash Cache performance improvements.
- Cache rewarming after a reboot is not supported with Cloud Volumes ONTAP.

Enabling Flash Cache on Cloud Volumes ONTAP in AWS

Flash Cache is supported with Cloud Volumes ONTAP Premium and BYOL in AWS.

Steps

1. Select one of the following EC2 instance types with a new or existing Cloud Volumes ONTAP

Premium or BYOL system:

- c5d.4xlarge
- c5d.9xlarge
- c5d.18xlarge
- m5d.8xlarge
- m5d.12xlarge
- r5d.2xlarge

2. Disable compression on all volumes to take advantage of the Flash Cache performance improvements.

   Choose no storage efficiency when creating a volume from Cloud Manager, or create a volume and then disable data compression by using the CLI.

Enabling Flash Cache on Cloud Volumes ONTAP in Azure

Flash Cache is supported with Cloud Volumes ONTAP BYOL on single node systems.

Steps

1. Select the Standard_L8s_v2 VM type with a single node Cloud Volumes ONTAP BYOL system in Azure.
2. Disable compression on all volumes to take advantage of the Flash Cache performance improvements.

   Choose no storage efficiency when creating a volume from Cloud Manager, or create a volume and then disable data compression by using the CLI.

Launching Cloud Volumes ONTAP in AWS

You can launch Cloud Volumes ONTAP in a single-system configuration or as an HA pair in AWS.

Launching a single-node Cloud Volumes ONTAP system in AWS

If you want to launch Cloud Volumes ONTAP in AWS, you need to create a new working environment in Cloud Manager.

Before you begin

- You should have prepared by choosing a configuration and by obtaining AWS networking information from your administrator. For details, see Planning your Cloud Volumes ONTAP configuration.
- If you want to launch a BYOL system, you must have the 20-digit serial number (license key).

- If you want to use CIFS, you must have set up DNS and Active Directory. For details, see Networking requirements for Cloud Volumes ONTAP in AWS.
- You should be prepared to leave Cloud Manager running at all times.

About this task

Immediately after you create the working environment, Cloud Manager launches a test instance in the specified VPC to verify connectivity. If successful, Cloud Manager immediately terminates the instance and then starts deploying the Cloud Volumes ONTAP system. If Cloud Manager cannot verify connectivity, creation of the working environment fails. The test instance is either a t2.nano (for default VPC tenancy) or m3.medium (for dedicated VPC tenancy).

Steps

1. On the Working Environments page, click **Create Cloud Volumes ONTAP** and follow the prompts.
2. **Define Your Working Environment**: Select **Amazon Web Services** and **Cloud Volumes ONTAP**.
3. **Details and Credentials**: Optionally change the AWS credentials and subscription, enter a working environment name, add tags if needed, and then enter a password.

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

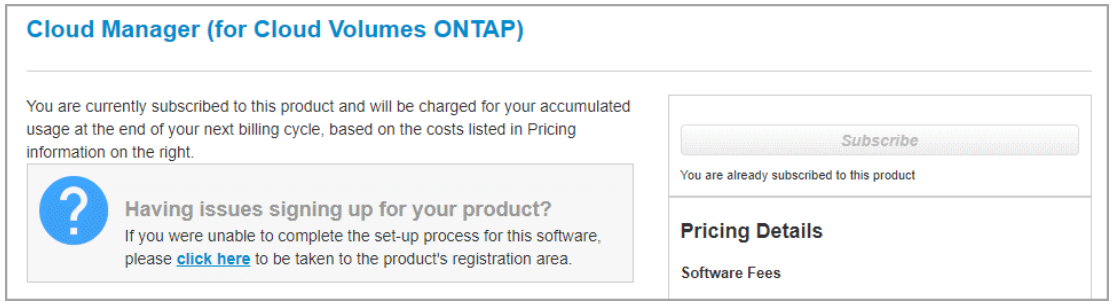
Field	Description
Working Environment Name	Cloud Manager uses the working environment name to name both the Cloud Volumes ONTAP system and the Amazon EC2 instance. It also uses the name as the prefix for the predefined security group, if you select that option.
Add tags	AWS tags are metadata for your AWS resources. Cloud Manager adds the tags to the Cloud Volumes ONTAP instance and each AWS resource associated with the instance. You can add up to four tags from the user interface when creating a working environment, and then you can add more after its created. Note that the API does not limit you to four tags when creating a working environment. For information about tags, refer to AWS Documentation: Tagging your Amazon EC2 Resources.
User name and password	These are the credentials for the Cloud Volumes ONTAP cluster admin account. You can use these credentials to connect to Cloud Volumes ONTAP through OnCommand System Manager or its CLI.

Field	Description
Edit Credentials	Choose the AWS credentials and marketplace subscription to use with this Cloud Volumes ONTAP system. Click **Add Subscription** to associate the selected credentials with a subscription. To create a pay-as-you-go Cloud Volumes ONTAP system, you need to select AWS credentials that are associated with a subscription to Cloud Volumes ONTAP from the AWS Marketplace. You'll be charged from this subscription for every Cloud Volumes ONTAP 9.6 and later PAYGO system that you create and each add-on feature that you enable. Learn how to add additional AWS credentials to Cloud Manager.

The following video shows how to associate a pay-as-you-go Marketplace subscription to your AWS credentials:

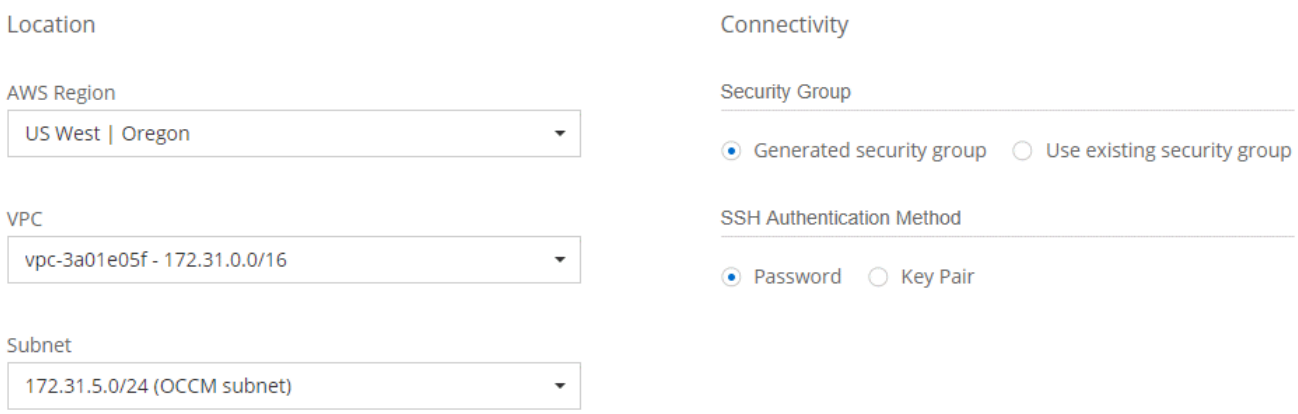
▶ https://docs.netapp.com/us-en/occm/media/video_subscribing_aws.mp4 *(video)*

If multiple IAM users work in the same AWS account, then each user needs to subscribe. After the first user subscribes, the AWS Marketplace informs subsequent users that they're already subscribed, as shown in the image below. While a subscription is in place for the AWS *account*, each IAM user needs to associate themselves with that subscription. If you see the message shown below, click the **click here** link to go to Cloud Central and complete the process.



4. **Services**: Keep the services enabled or disable the individual services that you don't want to use with Cloud Volumes ONTAP.
   - Learn more about Cloud Compliance.
   - Learn more about Backup to Cloud.
   - Learn more about Monitoring.
5. **Location & Connectivity**: Enter the network information that you recorded in the AWS worksheet.

   The following image shows the page filled out:



6. **Data Encryption**: Choose no data encryption or AWS-managed encryption.

   For AWS-managed encryption, you can choose a different Customer Master Key (CMK) from your account or another AWS account.

   > You can't change the AWS data encryption method after you create a Cloud Volumes ONTAP system.

   Learn how to set up the AWS KMS for Cloud Volumes ONTAP.

   Learn more about supported encryption technologies.

7. **License and Support Site Account**: Specify whether you want to use pay-as-you-go or BYOL, and then specify a NetApp Support Site account.

   To understand how licenses work, see Licensing.

   A NetApp Support Site Account is optional for pay-as-you-go, but required for BYOL systems. Learn how to add NetApp Support Site accounts.

8. **Preconfigured Packages**: Select one of the packages to quickly launch Cloud Volumes ONTAP, or click **Create my own configuration**.

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

9. **IAM Role**: You should keep the default option to let Cloud Manager create the role for you.

   If you prefer to use your own policy, it must meet policy requirements for Cloud Volumes ONTAP nodes.

10. **Licensing**: Change the Cloud Volumes ONTAP version as needed, select a license, an instance type, and the instance tenancy.

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

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

11. **Underlying Storage Resources**: Choose settings for the initial aggregate: a disk type, a size for each disk, and whether data tiering should be enabled.

    Note the following:

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

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

    - 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 how data tiering works.

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

    Learn more about write speed.

    Learn more about WORM storage.

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

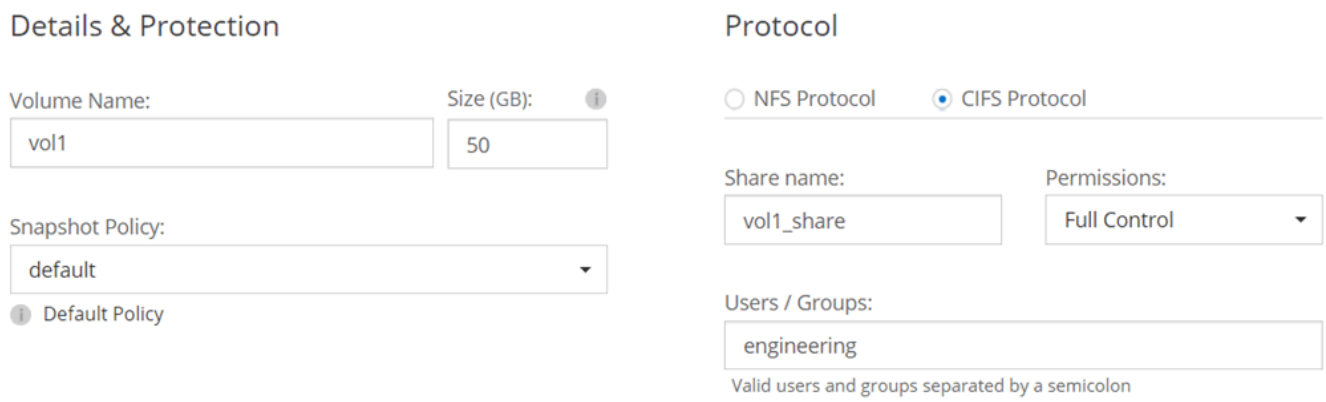
    You might skip this step if you want to create a volume for iSCSI. Cloud Manager sets up volumes for NFS and CIFS only.

    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.

Field	Description
Access control (for NFS only)	An export policy defines the clients in the subnet that can access the volume. By default, Cloud Manager enters a value that provides access to all instances in the subnet.
Permissions and Users / Groups (for CIFS only)	These fields enable you to control the level of access to a share for users and groups (also called access control lists or ACLs). You can specify local or domain Windows users or groups, or UNIX users or groups. If you specify a domain Windows user name, you must include the user's domain using the format domain\username.
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.

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



14. **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.

Field	Description
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. If you configure AWS Managed Microsoft AD as the AD server for Cloud Volumes ONTAP, you should enter **OU=Computers,OU=corp** in this field.
DNS Domain	The DNS domain for the Cloud Volumes ONTAP storage virtual machine (SVM). In most cases, the domain is the same as the AD domain.
NTP Server	Select **Use Active Directory Domain** to configure an NTP server using the Active Directory DNS. If you need to configure an NTP server using a different address, then you should use the API. See the Cloud Manager API Developer Guide for details.

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

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

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

Result

Cloud Manager launches the Cloud Volumes ONTAP instance. You can track the progress in the timeline.

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

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

After you finish

- If you provisioned a CIFS share, give users or groups permissions to the files and folders and verify that those users can access the share and create a file.

- If you want to apply quotas to volumes, use System Manager or the CLI.

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

Launching a Cloud Volumes ONTAP HA pair in AWS

If you want to launch a Cloud Volumes ONTAP HA pair in AWS, you need to create an HA working environment in Cloud Manager.

Before you begin

- You should have prepared by choosing a configuration and by obtaining AWS networking information from your administrator. For details, see Planning your Cloud Volumes ONTAP configuration.
- If you purchased BYOL licenses, you must have a 20-digit serial number (license key) for each node.
- If you want to use CIFS, you must have set up DNS and Active Directory. For details, see Networking requirements for Cloud Volumes ONTAP in AWS.
- You should be prepared to leave Cloud Manager running at all times.

About this task

Immediately after you create the working environment, Cloud Manager launches a test instance in the specified VPC to verify connectivity. If successful, Cloud Manager immediately terminates the instance and then starts deploying the Cloud Volumes ONTAP system. If Cloud Manager cannot verify connectivity, creation of the working environment fails. The test instance is either a t2.nano (for default VPC tenancy) or m3.medium (for dedicated VPC tenancy).

Steps

1. On the Working Environments page, click **Create Cloud Volumes ONTAP** and follow the prompts.
2. **Define Your Working Environment**: Select **Amazon Web Services** and **Cloud Volumes ONTAP HA**.
3. **Details and Credentials**: Optionally change the AWS credentials and subscription, enter a working environment name, add tags if needed, and then enter a password.

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

Field	Description
Working Environment Name	Cloud Manager uses the working environment name to name both the Cloud Volumes ONTAP system and the Amazon EC2 instance. It also uses the name as the prefix for the predefined security group, if you select that option.

Field	Description
Add tags	AWS tags are metadata for your AWS resources. Cloud Manager adds the tags to the Cloud Volumes ONTAP instance and each AWS resource associated with the instance. You can add up to four tags from the user interface when creating a working environment, and then you can add more after its created. Note that the API does not limit you to four tags when creating a working environment. For information about tags, refer to AWS Documentation: Tagging your Amazon EC2 Resources.
User name and password	These are the credentials for the Cloud Volumes ONTAP cluster admin account. You can use these credentials to connect to Cloud Volumes ONTAP through OnCommand System Manager or its CLI.
Edit Credentials	Choose the AWS credentials and marketplace subscription to use with this Cloud Volumes ONTAP system. Click **Add Subscription** to associate the selected credentials with a subscription. To create a pay-as-you-go Cloud Volumes ONTAP system, you need to select AWS credentials that are associated with a subscription to Cloud Volumes ONTAP from the AWS Marketplace. You'll be charged from this subscription for every Cloud Volumes ONTAP 9.6 and later PAYGO system that you create and each add-on feature that you enable. Learn how to add additional AWS credentials to Cloud Manager.

The following video shows how to associate a pay-as-you-go Marketplace subscription to your AWS credentials:

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

If multiple IAM users work in the same AWS account, then each user needs to subscribe. After the first user subscribes, the AWS Marketplace informs subsequent users that they're already subscribed, as shown in the image below. While a subscription is in place for the AWS *account*, each IAM user needs to associate themselves with that subscription. If you see the message shown below, click the **click here** link to go to Cloud Central and complete the process.

4. **Services**: Keep the services enabled or disable the individual services that you don't want to use

with this Cloud Volumes ONTAP system.

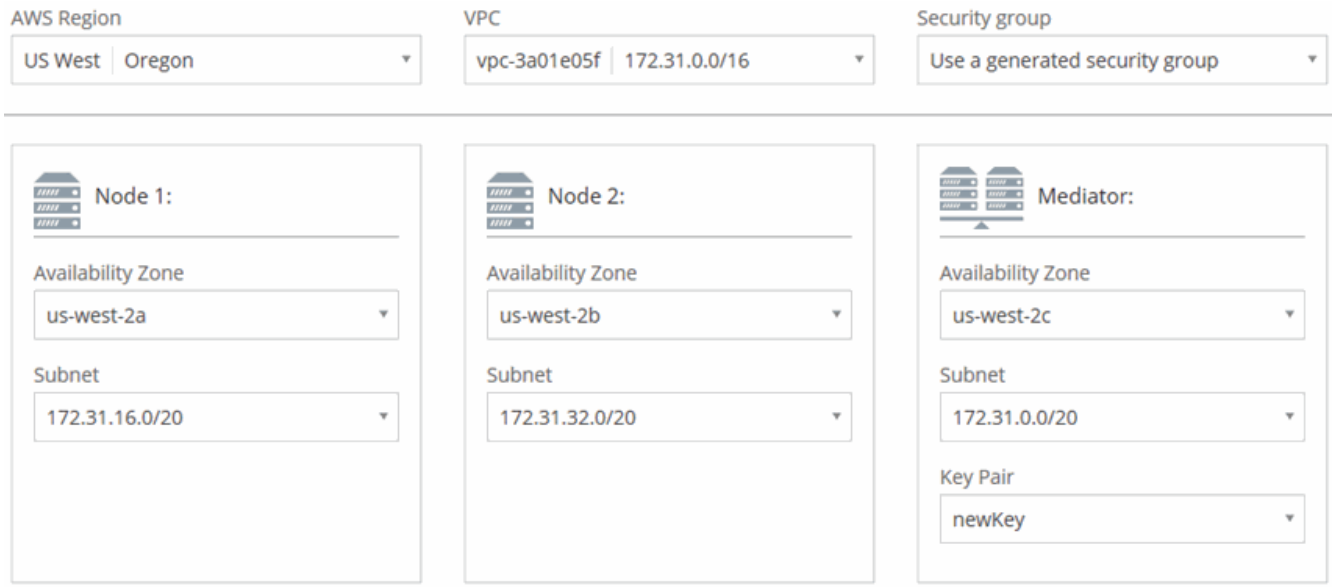
- Learn more about Backup to S3.
- Learn more about Cloud Compliance.
- Learn more about Monitoring.

5. **HA Deployment Models**: Choose an HA configuration.

   For an overview of the deployment models, see Cloud Volumes ONTAP HA for AWS.

6. **Region & VPC**: Enter the network information that you recorded in the AWS worksheet.

   The following image shows the page filled out for a multiple AZ configuration:



7. **Connectivity and SSH Authentication**: Choose connection methods for the HA pair and the mediator.
8. **Floating IPs**: If you chose multiple AZs, specify the floating IP addresses.

   The IP addresses must be outside of the CIDR block for all VPCs in the region. For additional details, see AWS networking requirements for Cloud Volumes ONTAP HA in multiple AZs.

9. **Route Tables**: If you chose multiple AZs, select the route tables that should include routes to the floating IP addresses.

   If you have more than one route table, it is very important to select the correct route tables. Otherwise, some clients might not have access to the Cloud Volumes ONTAP HA pair. For more information about route tables, refer to AWS Documentation: Route Tables.

10. **Data Encryption**: Choose no data encryption or AWS-managed encryption.

    For AWS-managed encryption, you can choose a different Customer Master Key (CMK) from your account or another AWS account.

You can't change the AWS data encryption method after you create a Cloud Volumes ONTAP system.

Learn how to set up the AWS KMS for Cloud Volumes ONTAP.

Learn more about supported encryption technologies.

11. **License and Support Site Account**: Specify whether you want to use pay-as-you-go or BYOL, and then specify a NetApp Support Site account.

    To understand how licenses work, see Licensing.

    A NetApp Support Site Account is optional for pay-as-you-go, but required for BYOL systems. Learn how to add NetApp Support Site accounts.

12. **Preconfigured Packages**: Select one of the packages to quickly launch 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.

13. **IAM Role**: You should keep the default option to let Cloud Manager create the roles for you.

    If you prefer to use your own policy, it must meet policy requirements for Cloud Volumes ONTAP nodes and the HA mediator.

14. **Licensing**: Change the Cloud Volumes ONTAP version as needed, select a license, an instance type, and the instance tenancy.

    If your needs change after you launch the instances, you can modify the license or instance type later.

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

15. **Underlying Storage Resources**: Choose settings for the initial aggregate: a disk type, a size for each disk, and whether data tiering should be enabled.

    Note the following:

    - The disk type is for the initial volume. You can choose a different disk type for subsequent volumes.

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

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

- 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 how data tiering works.

16. **WORM**: Activate write once, read many (WORM) storage, if desired.

    Learn more about WORM storage.

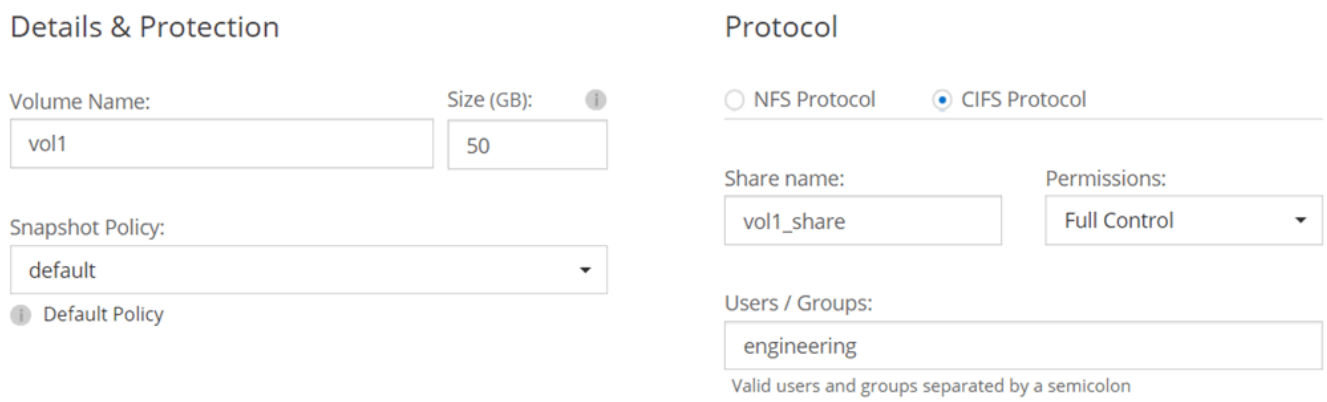
17. **Create Volume**: Enter details for the new volume or click **Skip**.

    You might skip this step if you want to create a volume for iSCSI. Cloud Manager sets up volumes for NFS and CIFS only.

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

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

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



18. **CIFS Setup**: If you selected 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.
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. If you configure AWS Managed Microsoft AD as the AD server for Cloud Volumes ONTAP, you should enter **OU=Computers,OU=corp** in this field.
DNS Domain	The DNS domain for the Cloud Volumes ONTAP storage virtual machine (SVM). In most cases, the domain is the same as the AD domain.
NTP Server	Select **Use Active Directory Domain** to configure an NTP server using the Active Directory DNS. If you need to configure an NTP server using a different address, then you should use the API. See the Cloud Manager API Developer Guide for details.

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

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

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

Result

Cloud Manager launches the Cloud Volumes ONTAP HA pair. You can track the progress in the timeline.

If you experience any issues launching the HA pair, review the failure message. You can also select the working environment and click Re-create environment.

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

After you finish

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

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

Launching Cloud Volumes ONTAP in Azure

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

Before you begin

- Make sure that your Azure account has the required permissions, especially if you upgraded from a previous release and are deploying an HA system for the first time.

  The latest permissions are in the NetApp Cloud Central policy for Azure.

- You should have chose a configuration and obtained Azure networking information from your administrator. For details, see Planning your Cloud Volumes ONTAP configuration.
- To deploy a BYOL system, you need the 20-digit serial number (license key) for each node.
- You should be prepared to leave Cloud Manager running at all times.

About this task

When Cloud Manager creates a Cloud Volumes ONTAP system in Azure, it creates several Azure

objects, such as a resource group, network interfaces, and storage accounts. You can review a summary of the resources at the end of the wizard.

Steps

1. On the Working Environments page, click **Create Cloud Volumes ONTAP** and follow the prompts.
2. **Define Your Working Environment**: Select **Microsoft Azure** and then choose a single node or HA pair.
3. **Details and Credentials**: Optionally change the Azure credentials and subscription, specify a cluster name and resource group name, add tags if needed, and then specify credentials.

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

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

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

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

4. **Services**: Keep the services enabled or disable the individual services that you don't want to use with Cloud Volumes ONTAP.
   - Learn more about Cloud Compliance.
   - Learn more about Backup to Cloud.
5. **Location & Connectivity**: Select a location and security group and select the checkbox to confirm network connectivity between Cloud Manager and the target location.
6. **License and Support Site Account**: Specify whether you want to use pay-as-you-go or BYOL, and then specify a NetApp Support Site account.

   To understand how licenses work, see Licensing.

   A NetApp Support Site Account is optional for pay-as-you-go, but required for BYOL systems. Learn how to add NetApp Support Site accounts.
7. **Preconfigured Packages**: Shelect 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.
8. **Licensing**: Change the Cloud Volumes ONTAP version as needed, select a license, and select a virtual machine type.

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

   > If a newer Release Candidate, General Availability, or patch release is available for the selected version, then Cloud Manager updates the system to that version when creating the working environment. For example, the update occurs if you select Cloud Volumes ONTAP 9.6 RC1 and 9.6 GA is available. The update does not occur from one release to another—for example, from 9.6 to 9.7.
9. **Subscribe from the Azure Marketplace**: Follow the steps if Cloud Manager could not enable programmatic deployments of Cloud Volumes ONTAP.
10. **Underlying Storage Resources**: Choose settings for the initial aggregate: a disk type, a size for each disk, and whether data tiering to Blob storage should be enabled.

    Note the following:
    - The disk type is for the initial volume. You can choose a different disk type for subsequent volumes.

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

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

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

  Learn more about data tiering.

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

    Choosing a write speed is supported with single node systems only.

    Learn more about write speed.

    Learn more about WORM storage.

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

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

    Learn more about WORM storage.

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

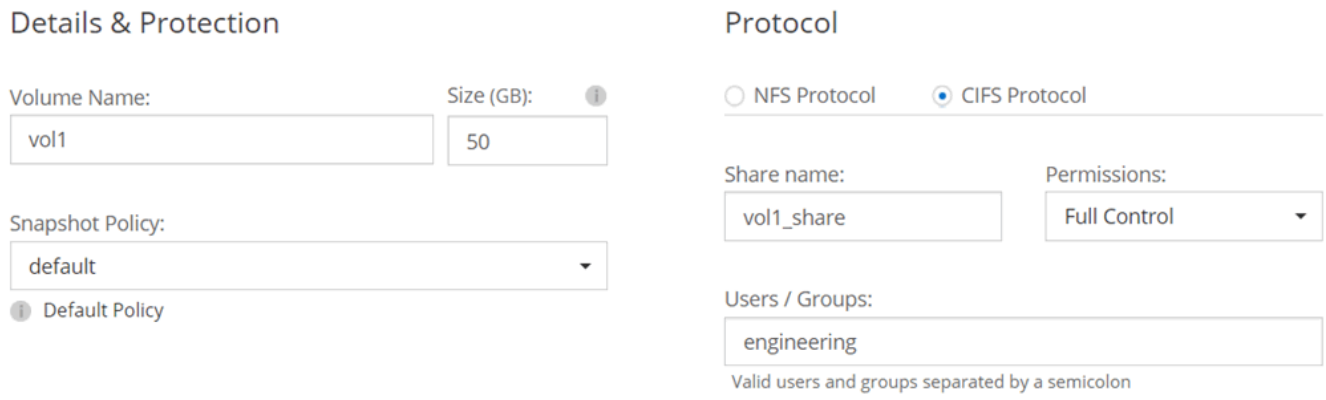
    You should skip this step if you want to use iSCSI. Cloud Manager enables you to create volumes for NFS and CIFS only.

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

Field	Description
Size	The maximum size that you can enter largely depends on whether you enable thin provisioning, which enables you to create a volume that is bigger than the physical storage currently available to it.
Access control (for NFS only)	An export policy defines the clients in the subnet that can access the volume. By default, Cloud Manager enters a value that provides access to all instances in the subnet.

Field	Description
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.
Advanced options (for NFS only)	Select an NFS version for the volume: either NFSv3 or NFSv4.

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



14. **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. See the Cloud Manager API Developer Guide for details.

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

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

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

Result

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

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

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

After you finish

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

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

Launching Cloud Volumes ONTAP in GCP

You can launch a single node Cloud Volumes ONTAP system in GCP by creating a working environment.

Before you begin

- You should have chose a configuration and obtained GCP networking information from your administrator. For details, see Planning your Cloud Volumes ONTAP configuration.
- To deploy a BYOL system, you need the 20-digit serial number (license key) for each node.
- You should be prepared to leave Cloud Manager running at all times.

Steps

1. On the Working Environments page, click **Create Cloud Volumes ONTAP** and follow the prompts.
2. **Define Your Working Environment**: Click **Continue**.
3. **Details & Credentials**: Select a project, specify a cluster name, optionally add labels, and then specify credentials.

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

Field	Description
Working Environment Name	Cloud Manager uses the working environment name to name both the Cloud Volumes ONTAP system and the GCP VM instance. It also uses the name as the prefix for the predefined security group, if you select that option.
Add Labels	Labels are metadata for your GCP resources. Cloud Manager adds the labels to the Cloud Volumes ONTAP system and GCP resources associated with the system. You can add up to four labels from the user interface when creating a working environment, and then you can add more after its created. Note that the API does not limit you to four labels when creating a working environment. For information about labels, refer to Google Cloud Documentation: Labeling Resources.
User name and password	These are the credentials for the Cloud Volumes ONTAP cluster admin account. You can use these credentials to connect to Cloud Volumes ONTAP through System Manager or its CLI.

Field	Description
Edit Project	Select the project where you want Cloud Volumes ONTAP to reside. The default project is the project where Cloud Manager resides. If you don't see any additional projects in the drop-down list, then you haven't yet associated the Cloud Manager service account with other projects. Go to the Google Cloud console, open the IAM service, and select the project. Add the service account with the Cloud Manager role to that project. You'll need to repeat this step for each project. This is the service account that you set up for Cloud Manager, as described in step 2b on this page. Click **Add Subscription** to associate the selected credentials with a subscription. To create a pay-as-you-go Cloud Volumes ONTAP system, you need to select a GCP project that's associated with a subscription to Cloud Volumes ONTAP from the GCP Marketplace.

The following video shows how to associate a pay-as-you-go Marketplace subscription to your GCP project:

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

4. **Location & Connectivity**: Select a location, choose a firewall policy, and select the checkbox to confirm network connectivity to Google Cloud storage for data tiering.

   If you want to tier cold data to a Google Cloud Storage bucket, the subnet in which Cloud Volumes ONTAP resides must be configured for Private Google Access. For instructions, refer to Google Cloud Documentation: Configuring Private Google Access.

5. **License & Support Site Account**: Specify whether you want to use pay-as-you-go or BYOL, and then specify a NetApp Support Site account.

   To understand how licenses work, see Licensing.

   A NetApp Support Site Account is optional for pay-as-you-go, but required for BYOL systems. Learn how to add NetApp Support Site accounts.

6. **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.

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

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

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

8. **Underlying Storage Resources**: Choose settings for the initial aggregate: a disk type and the size for each disk.

   The disk type is for the initial volume. You can choose a different disk type for subsequent volumes.

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

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

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

   Learn more about write speed.

   Learn more about WORM storage.

10. **Data Tiering in Google Cloud Platform**: Choose whether to enable data tiering on the initial aggregate, choose a storage class for the tiered data, and then either select a service account that has the predefined Storage Admin role (required for Cloud Volumes ONTAP 9.7), or select a GCP account (required for Cloud Volumes ONTAP 9.6).

    Note the following:

    - Cloud Manager sets the service account on the Cloud Volumes ONTAP instance. This service account provides permissions for data tiering to a Google Cloud Storage bucket. Be sure to add the Cloud Manager service account as a user of the tiering service account, otherwise, you can't select it from Cloud Manager.
    - For help with adding a GCP account, see Setting up and adding GCP accounts for data tiering with 9.6.
    - 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, but you'll need to turn off the system and add a service account from the GCP console.

  Learn more about data tiering.

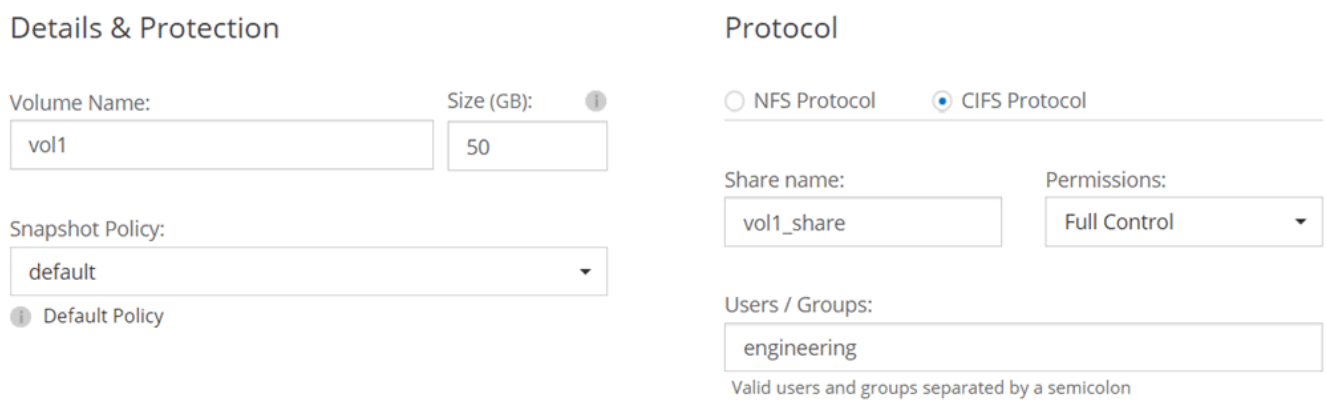
11. **Create Volume**: Enter details for the new volume or click **Skip**.

    You should skip this step if you want to use iSCSI. Cloud Manager enables you to create volumes for NFS and CIFS only.

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

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

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



12. **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.
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.
DNS Domain	The DNS domain for the Cloud Volumes ONTAP storage virtual machine (SVM). In most cases, the domain is the same as the AD domain.
NTP Server	Select **Use Active Directory Domain** to configure an NTP server using the Active Directory DNS. If you need to configure an NTP server using a different address, then you should use the API. See the Cloud Manager API Developer Guide for details.

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

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

14. **Review & Approve**: Review and confirm your selections.

a. Review details about the configuration.

b. Click **More information** to review details about support and the GCP resources that Cloud Manager will purchase.

c. Select the **I understand...** check boxes.

d. Click **Go**.

Result

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

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

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

After you finish

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

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

Registering pay-as-you-go systems

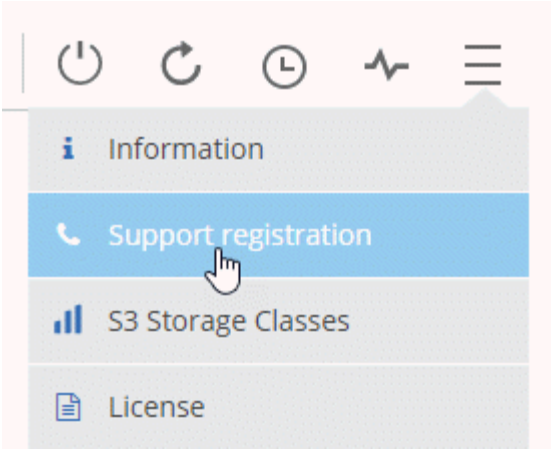
Support from NetApp is included with Cloud Volumes ONTAP Explore, Standard, and Premium systems, but you must first activate support by registering the systems with NetApp.

Steps

1. If you have not yet added your NetApp Support Site account to Cloud Manager, go to **Account Settings** and add it now.

   Learn how to add NetApp Support Site accounts.

2. On the Working Environments page, double-click the name of the system that you want to register.
3. Click the menu icon and then click **Support registration**:



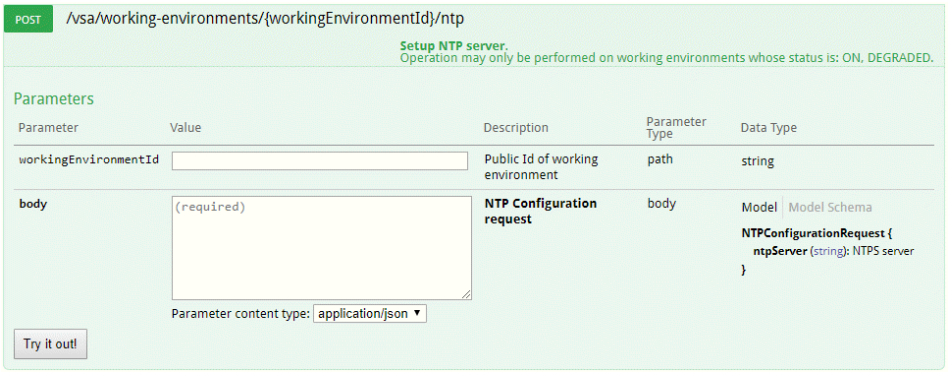
4. Select a NetApp Support Site account and click **Register**.

Result

Cloud Manager registers the system with NetApp.

Setting up Cloud Volumes ONTAP

After you deploy Cloud Volumes ONTAP, you can set it up by synchronizing the system time using NTP and by performing a few optional tasks from either System Manager or the CLI.

Task	Description
Synchronize the system time using NTP	Specifying an NTP server synchronizes the time between the systems in your network, which can help prevent issues due to time differences. Specify an NTP server using the Cloud Manager API or from the user interface when you set up a CIFS server. • Modifying the CIFS server • Cloud Manager API Developer Guide For example, here's the API for a single-node system in AWS: 
Optional: Configure AutoSupport	AutoSupport proactively monitors the health of your system and automatically sends messages to NetApp technical support by default. If the Account Admin added a proxy server to Cloud Manager before you launched your instance, Cloud Volumes ONTAP is configured to use that proxy server for AutoSupport messages. You should test AutoSupport to ensure that it can send messages. For instructions, see the System Manager Help or the ONTAP 9 System Administration Reference.
Optional: Configure Cloud Manager as the AutoSupport proxy	If your environment requires a proxy server to send AutoSupport messages, you can configure Cloud Manager to act as the proxy. No configuration for Cloud Manager is required, other than internet access. You simply need to go to the CLI for Cloud Volumes ONTAP and run the following command: `system node autosupport modify -proxy-url <cloud-manager-ip-address>`

Task	Description
Optional: Configure EMS	The Event Management System (EMS) collects and displays information about events that occur on Cloud Volumes ONTAP systems. To receive event notifications, you can set event destinations (email addresses, SNMP trap hosts, or syslog servers) and event routes for a particular event severity. You can configure EMS using the CLI. For instructions, see the ONTAP 9 EMS Configuration Express Guide.
Optional: Create an SVM management network interface (LIF) for HA systems in multiple AWS Availability Zones	A storage virtual machine (SVM) management network interface (LIF) is required if you want to use SnapCenter or SnapDrive for Windows with an HA pair. The SVM management LIF must use a *floating* IP address when using an HA pair across multiple AWS Availability Zones. Cloud Manager prompts you to specify the floating IP address when you launch the HA pair. If you did not specify the IP address, you can create the SVM Management LIF yourself from System Manager or the CLI. The following example shows how to create the LIF from the CLI: `network interface create -vserver svm_cloud -lif svm_mgmt -role data -data-protocol none -home-node cloud-01 -home -port e0a -address 10.0.2.126 -netmask 255.255.255.0 -status -admin up -firewall-policy mgmt`
Optional: Change the backup location of configuration files	Cloud Volumes ONTAP automatically creates configuration backup files that contain information about the configurable options that it needs to operate properly. By default, Cloud Volumes ONTAP backs up the files to the Cloud Manager host every eight hours. If you want to send the backups to an alternate location, you can change the location to an FTP or HTTP server in your data center or in AWS. For example, you might already have a backup location for your FAS storage systems. You can change the backup location using the CLI. See the ONTAP 9 System Administration Reference.

Provision and manage storage

Provisioning storage

You can provision additional storage for your Cloud Volumes ONTAP systems from Cloud Manager by managing volumes and aggregates.

All disks and aggregates must be created and deleted directly from Cloud Manager. You should not perform these actions from another management tool. Doing so can impact system stability, hamper the ability to add disks in the future, and potentially generate redundant cloud provider fees.

Creating FlexVol volumes

If you need more storage after you launch a Cloud Volumes ONTAP system, you can create new FlexVol volumes for NFS or CIFS from Cloud Manager.

Before you begin

If you want to use CIFS in AWS, you must have set up DNS and Active Directory. For details, see Networking requirements for Cloud Volumes ONTAP for AWS.

Steps

1. On the Working Environments page, double-click the name of the Cloud Volumes ONTAP system on which you want to provision FlexVol volumes.
2. Create a new volume on any aggregate or on a specific aggregate:

Action	Steps
Create a new volume and let Cloud Manager choose the containing aggregate	Click **Add New Volume**.
Create a new volume on a specific aggregate	a. Click the menu icon, and then click **Advanced** > **Advanced allocation**. b. Click the menu for an aggregate. c. Click **Create volume**.

3. Enter details for the new volume, and then click **Continue**.

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

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

4. If you chose the CIFS protocol and the CIFS server has not been set up, specify details for the server in the Create a CIFS Server dialog box, and then click **Save and continue**:

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.
CIFS server NetBIOS name	A CIFS server name that is unique in the AD domain.

Field	Description
Organizational Unit	The organizational unit within the AD domain to associate with the CIFS server. The default is CN=Computers. • To configure AWS Managed Microsoft AD as the AD server for Cloud Volumes ONTAP, you should enter **OU=Computers,OU=corp** in this field. • To configure Azure AD Domain Services as the AD server for Cloud Volumes ONTAP, you should enter **OU=AADDC Computers** or **OU=AADDC Users** in this field. Azure Documentation: Create an Organizational Unit (OU) in an Azure AD Domain Services managed domain
DNS Domain	The DNS domain for the Cloud Volumes ONTAP storage virtual machine (SVM). In most cases, the domain is the same as the AD domain.
NTP Server	Select **Use Active Directory Domain** to configure an NTP server using the Active Directory DNS. If you need to configure an NTP server using a different address, then you should use the API. See the Cloud Manager API Developer Guide for details.

5. On the Usage Profile, Disk Type, and Tiering Policy page, choose whether you want to enable storage efficiency features, choose a disk type, and edit the tiering policy, if needed.

   For help, refer to the following:

   - Understanding volume usage profiles
   - Sizing your system in AWS
   - Sizing your system in Azure
   - Data tiering overview

6. Click **Go**.

Result

Cloud Volumes ONTAP provisions the volume.

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

Creating FlexVol volumes on the second node in an HA configuration

By default, Cloud Manager creates volumes on the first node in an HA configuration. If you need an active-active configuration, in which both nodes serve data to clients, you must create aggregates and volumes on the second node.

Steps

1. On the Working Environments page, double-click the name of the Cloud Volumes ONTAP working environment on which you want to manage aggregates.
2. Click the menu icon and then click **Advanced** > **Advanced allocation**.
3. Click **Add Aggregate** and then create the aggregate.
4. For Home Node, choose the second node in the HA pair.
5. After Cloud Manager creates the aggregate, select it and then click **Create volume**.
6. Enter details for the new volume, and then click **Create**.

After you finish

You can create additional volumes on this aggregate if required.

For HA pairs deployed in multiple AWS Availability Zones, you must mount the volume to clients by using the floating IP address of the node on which the volume resides.

Creating aggregates

You can create aggregates yourself or let Cloud Manager do it for you when it creates volumes. The benefit of creating aggregates yourself is that you can choose the underlying disk size, which enables you to size your aggregate for the capacity or the performance that you need.

Steps

1. On the Working Environments page, double-click the name of the Cloud Volumes ONTAP instance on which you want to manage aggregates.
2. Click the menu icon, and then click **Advanced** > **Advanced allocation**.
3. Click **Add Aggregate** and then specify details for the aggregate.

   For help with disk type and disk size, see Planning your configuration.
4. Click **Go**, and then click **Approve and Purchase**.

Provisioning iSCSI LUNs

Create iSCSI LUNs by using a Cloud Manager API or by going to System Manager.

If you want to use the Cloud Manager APIs, view an example here.

If you want to use System Manager, follow the steps below.

Before you begin

- The Host Utilities must be installed and set up on the hosts that will connect to the LUN.
- You must have recorded the iSCSI initiator name from the host. You need to supply this name when you create an igroup for the LUN.
- Before you create volumes in System Manager, you must ensure that you have an aggregate with sufficient space. You need to create aggregates in Cloud Manager. For details, see Creating aggregates.

About this task

These steps describe how to use System Manager for version 9.3 and later.

Steps

1. Log in to System Manager.
2. Click **Storage** > **LUNs**.
3. Click **Create** and follow the prompts to create the LUN.
4. Connect to the LUN from your hosts.

   For instructions, see the Host Utilities documentation for your operating system.

Using FlexCache volumes to accelerate data access

A FlexCache volume is a storage volume that caches NFS read data from an origin (or source) volume. Subsequent reads to the cached data result in faster access to that data.

You can use FlexCache volumes to speed up access to data or to offload traffic from heavily accessed volumes. FlexCache volumes help improve performance, especially when clients need to access the same data repeatedly, because the data can be served directly without having to access the origin volume. FlexCache volumes work well for system workloads that are read-intensive.

Cloud Manager does not provide management of FlexCache volumes at this time, but you can use the ONTAP CLI or ONTAP System Manager to create and manage FlexCache volumes:

- FlexCache Volumes for Faster Data Access Power Guide
- Creating FlexCache volumes in System Manager

Starting with the 3.7.2 release, Cloud Manager generates a FlexCache license for all new Cloud Volumes ONTAP systems. The license includes a 500 GB usage limit.

To generate the license, Cloud Manager needs to access https://ipa-signer.cloudmanager.netapp.com. Make sure that this URL is accessible from your firewall.

Managing existing storage

Cloud Manager enables you to manage volumes, aggregates, and CIFS servers. It also prompts you to move volumes to avoid capacity issues.

Managing existing volumes

You can manage existing volumes as your storage needs change. You can view, edit, clone, restore, and delete volumes.

Steps

1. On the Working Environments page, double-click the Cloud Volumes ONTAP working environment on which you want to manage volumes.
2. Manage your volumes:

Task	Action
View information about a volume	Select a volume, and then click **Info**.

Task	Action
Edit a volume (read-write volumes only)	a. Select a volume, and then click **Edit**. b. Modify the volume's Snapshot policy, NFS protocol version, NFS access control list, or share permissions, and then click **Update**.  If you need custom Snapshot policies, you can create them by using System Manager.
Clone a volume	a. Select a volume, and then click **Clone**. b. Modify the clone name as needed, and then click **Clone**. This process creates a FlexClone volume. A FlexClone volume is a writable, point-in-time copy that is space-efficient because it uses a small amount of space for metadata, and then only consumes additional space as data is changed or added. To learn more about FlexClone volumes, see the ONTAP 9 Logical Storage Management Guide.
Restore data from a Snapshot copy to a new volume	a. Select a volume, and then click **Restore from Snapshot copy**. b. Select a Snapshot copy, enter a name for the new volume, and then click **Restore**.
Create a Snapshot copy on demand	a. Select a volume, and then click **Create a Snapshot copy**. b. Change the name, if needed, and then click **Create**.
Get the NFS mount command	a. Select a volume, and then click **Mount Command**. b. Click **Copy**.
Change the underlying disk type	a. Select a volume, and then click **Change Disk Type & Tiering Policy**. b. Select the disk type, and then click **Change**.  Cloud Manager moves the volume to an existing aggregate that uses the selected disk type or it creates a new aggregate for the volume.

Task	Action
Change the tiering policy	a. Select a volume, and then click **Change Disk Type & Tiering Policy**. b. Click **Edit Policy**. c. Select a different policy and click **Change**.  Cloud Manager moves the volume to an existing aggregate that uses the selected disk type with tiering, or it creates a new aggregate for the volume.
Delete a volume	a. Select a volume, and then click **Delete**. b. Click **Delete** again to confirm.

Managing existing aggregates

Manage aggregates yourself by adding disks, viewing information about the aggregates, and by deleting them.

Before you begin

If you want to delete an aggregate, you must have first deleted the volumes in the aggregate.

About this task

If an aggregate is running out of space, you can move volumes to another aggregate by using OnCommand System Manager.

Steps

1. On the Working Environments page, double-click the Cloud Volumes ONTAP working environment on which you want to manage aggregates.
2. Click the menu icon and then click **Advanced** > **Advanced allocation**.
3. Manage your aggregates:

Task	Action
View information about an aggregate	Select an aggregate and click **Info**.
Create a volume on a specific aggregate	Select an aggregate and click **Create volume**.

Task	Action
Add disks to an aggregate	a. Select an aggregate and click **Add AWS disks** or **Add Azure disks**. b. Select the number of disks that you want to add and click **Add**.  All disks in an aggregate must be the same size.
Delete an aggregate	a. Select an aggregate that does not contain any volumes and click **Delete**. b. Click **Delete** again to confirm.

Modifying the CIFS server

If you change your DNS servers or Active Directory domain, you need to modify the CIFS server in Cloud Volumes ONTAP so that it can continue to serve storage to clients.

Steps

1. From the working environment, click the menu icon and then click **Advanced** > **CIFS setup**.
2. Specify settings for the CIFS server:

Task	Action
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.
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. If you configure AWS Managed Microsoft AD as the AD server for Cloud Volumes ONTAP, you should enter **OU=Computers,OU=corp** in this field.

Task	Action
DNS Domain	The DNS domain for the Cloud Volumes ONTAP storage virtual machine (SVM). In most cases, the domain is the same as the AD domain.
NTP Server	Select **Use Active Directory Domain** to configure an NTP server using the Active Directory DNS. If you need to configure an NTP server using a different address, then you should use the API. See the Cloud Manager API Developer Guide for details.

3. Click **Save**.

Result

Cloud Volumes ONTAP updates the CIFS server with the changes.

Moving a volume

Move volumes for capacity utilization, improved performance, and to satisfy service-level agreements.

You can move a volume in System Manager by selecting a volume and the destination aggregate, starting the volume move operation, and optionally monitoring the volume move job. When using System Manager, a volume move operation finishes automatically.

Steps

1. Use System Manager or the CLI to move the volumes to the aggregate.

   In most situations, you can use System Manager to move volumes.

   For instructions, see the ONTAP 9 Volume Move Express Guide.

Moving a volume when Cloud Manager displays an Action Required message

Cloud Manager might display an Action Required message that says moving a volume is necessary to avoid capacity issues, but that it cannot provide recommendations to correct the issue. If this happens, you need to identify how to correct the issue and then move one or more volumes.

Steps

1. Identify how to correct the issue.
2. Based on your analysis, move volumes to avoid capacity issues:
   - Move volumes to another system.
   - Move volumes to another aggregate on the same system.

Identifying how to correct capacity issues

If Cloud Manager cannot provide recommendations for moving a volume to avoid capacity issues, you

must identify the volumes that you need to move and whether you should move them to another aggregate on the same system or to another system.

Steps

1. View the advanced information in the Action Required message to identify the aggregate that has reached its capacity limit.

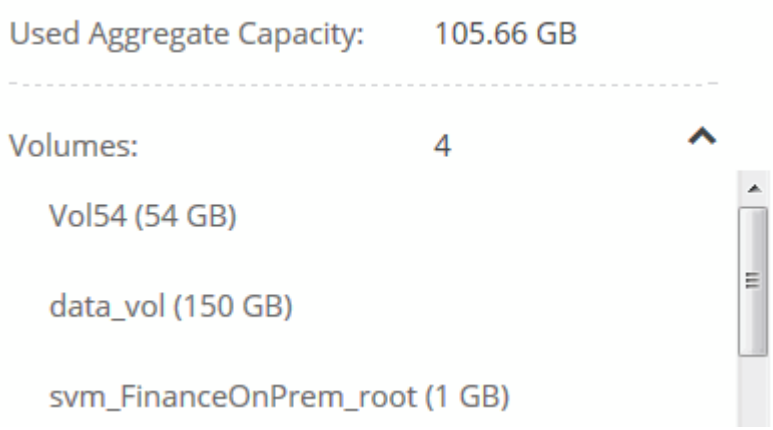
   For example, the advanced information should say something similar to the following: Aggregate aggr1 has reached its capacity limit.

2. Identify one or more volumes to move out of the aggregate:

   a. In the working environment, click the menu icon, and then click **Advanced** > **Advanced allocation**.

   b. Select the aggregate, and then click **Info**.

   c. Expand the list of volumes.



   d. Review the size of each volume and choose one or more volumes to move out of the aggregate.

      You should choose volumes that are large enough to free space in the aggregate so that you avoid additional capacity issues in the future.

3. If the system has not reached the disk limit, you should move the volumes to an existing aggregate or a new aggregate on the same system.

   For details, see Moving volumes to another aggregate to avoid capacity issues.

4. If the system has reached the disk limit, do any of the following:

   a. Delete any unused volumes.

   b. Rearrange volumes to free space on an aggregate.

      For details, see Moving volumes to another aggregate to avoid capacity issues.

   c. Move two or more volumes to another system that has space.

For details, see Moving volumes to another system to avoid capacity issues.

Moving volumes to another system to avoid capacity issues

You can move one or more volumes to another Cloud Volumes ONTAP system to avoid capacity issues. You might need to do this if the system reached its disk limit.

About this task

You can follow the steps in this task to correct the following Action Required message:

```
Moving a volume is necessary to avoid capacity issues; however, Cloud Manager cannot
perform this action for you because the system has reached the disk limit.
```

Steps

1. Identify a Cloud Volumes ONTAP system that has available capacity, or deploy a new system.
2. Drag and drop the source working environment on the target working environment to perform a one-time data replication of the volume.

   For details, see Replicating data between systems.

3. Go to the Replication Status page, and then break the SnapMirror relationship to convert the replicated volume from a data protection volume to a read/write volume.

   For details, see Managing data replication schedules and relationships.

4. Configure the volume for data access.

   For information about configuring a destination volume for data access, see the ONTAP 9 Volume Disaster Recovery Express Guide.

5. Delete the original volume.

   For details, see Managing existing volumes.

Moving volumes to another aggregate to avoid capacity issues

You can move one or more volumes to another aggregate to avoid capacity issues.

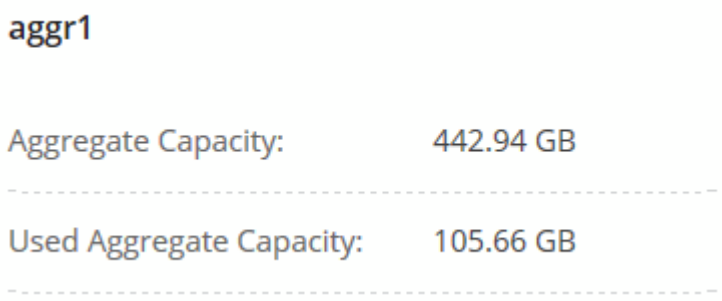
About this task

You can follow the steps in this task to correct the following Action Required message:

```
Moving two or more volumes is necessary to avoid capacity issues; however, Cloud Manager
cannot perform this action for you.
```

Steps

1. Verify whether an existing aggregate has available capacity for the volumes that you need to move:
   a. In the working environment, click the menu icon, and then click **Advanced** > **Advanced allocation**.
   b. Select each aggregate, click **Info**, and then view the available capacity (aggregate capacity minus used aggregate capacity).



2. If needed, add disks to an existing aggregate:
   a. Select the aggregate, and then click **Add disks**.
   b. Select the number of disks to add, and then click **Add**.
3. If no aggregates have available capacity, create a new aggregate.

   For details, see Creating aggregates.
4. Use System Manager or the CLI to move the volumes to the aggregate.
5. In most situations, you can use System Manager to move volumes.

   For instructions, see the ONTAP 9 Volume Move Express Guide.

Reasons why a volume move might perform slowly

Moving a volume might take longer than you expect if any of the following conditions are true for Cloud Volumes ONTAP:

- The volume is a clone.
- The volume is a parent of a clone.
- The source or destination aggregate has a single Throughput Optimized HDD (st1) disk.
- The Cloud Volumes ONTAP system is in AWS and one aggregate uses an older naming scheme for objects. Both aggregates have to use the same name format.

  An older naming scheme is used if data tiering was enabled on an aggregate in the 9.4 release or earlier.
- The encryption settings don't match on the source and destination aggregates, or a rekey is in

progress.

- The *-tiering-policy* option was specified on the volume move to change the tiering policy.
- The *-generate-destination-key* option was specified on the volume move.

Tiering inactive data to low-cost object storage

You can reduce storage costs by combining an SSD or HDD performance tier for hot data with an object storage capacity tier for inactive data. For a high-level overview, see Data tiering overview.

To set up data tiering, you simply need to do the following:

Choose a supported configuration

Most configurations are supported. If you have a Cloud Volumes ONTAP Standard, Premium, or BYOL system running the most recent version, then you should be good to go. Learn more.

Ensure connectivity between Cloud Volumes ONTAP and object storage

- For AWS, you'll need a VPC Endpoint to S3. Learn more.
- For Azure, you won't need to do anything as long as Cloud Manager has the required permissions. Learn more.
- For GCP, you need to configure the subnet for Private Google Access and set up a service account. Learn more.

Choose a tiering policy when creating, modifying, or replicating a volume

Cloud Manager prompts you to choose a tiering policy when you create, modify, or replicate a volume.

- Tiering data on read-write volumes
- Tiering data on data protection volumes

What's not required for data tiering

- You don't need to install a feature license to enable data tiering.
- You don't need to create the capacity tier (an S3 bucket, Azure Blob container, or GCP bucket). Cloud Manager does that for you.

Configurations that support data tiering

You can enable data tiering when using specific configurations and features:

- Data tiering is supported with Cloud Volumes ONTAP Standard, Premium, and BYOL, starting with the following versions:
  - Version 9.2 in AWS
  - Version 9.4 in Azure with single node systems
  - Version 9.6 in Azure with HA pairs
  - Version 9.6 in GCP

  Data tiering is not supported in Azure with the DS3_v2 virtual machine type.
- In AWS, the performance tier can be General Purpose SSDs, Provisioned IOPS SSDs, or Throughput Optimized HDDs.
- In Azure, the performance tier can be Premium SSD managed disks, Standard SSD managed disks, or Standard HDD managed disks.
- In GCP, the performance tier can be either SSDs or HDDs (standard disks).
- Data tiering is supported with encryption technologies.
- Thin provisioning must be enabled on volumes.

Requirements to tier cold data to AWS S3

Ensure that Cloud Volumes ONTAP has a connection to S3. The best way to provide that connection is by creating a VPC Endpoint to the S3 service. For instructions, see AWS Documentation: Creating a Gateway Endpoint.

When you create the VPC Endpoint, be sure to select the region, VPC, and route table that corresponds to the Cloud Volumes ONTAP instance. You must also modify the security group to add an outbound HTTPS rule that enables traffic to the S3 endpoint. Otherwise, Cloud Volumes ONTAP cannot connect to the S3 service.

If you experience any issues, see AWS Support Knowledge Center: Why can't I connect to an S3 bucket using a gateway VPC endpoint?.

Requirements to tier cold data to Azure Blob storage

You don't need to set up a connection between the performance tier and the capacity tier as long as Cloud Manager has the required permissions. Cloud Manager enables a VNet service endpoint for you if the Cloud Manager policy has these permissions:

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

The permissions are included in the latest Cloud Manager policy.

Requirements to tier cold data to a Google Cloud Storage bucket

- The subnet in which Cloud Volumes ONTAP resides must be configured for Private Google Access. For instructions, refer to Google Cloud Documentation: Configuring Private Google Access.
- Cloud Volumes ONTAP 9.7: You need to create a service account that has the predefined Storage Admin role. You'll need to select this service account when you create a Cloud Volumes ONTAP working environment. For more details, see step 3 in Getting started with Cloud Volumes ONTAP in Google Cloud Platform.

  If you don't enable data tiering and select a service account when you create the Cloud Volumes ONTAP 9.7 system, then you'll need to turn off the system and add the service account to Cloud Volumes ONTAP from the GCP console.

- Cloud Volumes ONTAP 9.6: You need to add a Google Cloud Platform account to Cloud Manager by entering storage access keys for a service account. The keys enable Cloud Manager to set up a Cloud Storage bucket for data tiering. For instructions, see Setting up and adding GCP accounts for data tiering with 9.6.

Tiering data from read-write volumes

Cloud Volumes ONTAP can tier inactive data on read-write volumes to cost-effective object storage, freeing up the performance tier for hot data.

Steps

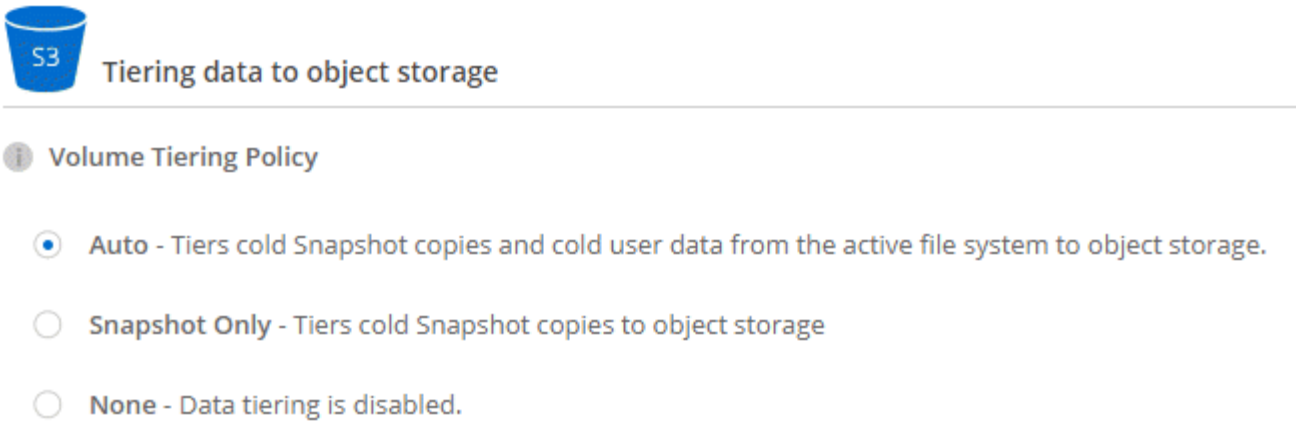
1. In the working environment, create a new volume or change the tier of an existing volume:

Task	Action
Create a new volume	Click **Add New Volume**.
Modify an existing volume	Select the volume and click **Change Disk Type & Tiering Policy**.

2. Select the Snapshot Only policy or the Auto policy.

   For a description of these policies, see Data tiering overview.

   Example



Cloud Manager creates a new aggregate for the volume if a data tiering-enabled aggregate does not already exist.

If you prefer to create aggregates yourself, you can enable data tiering on aggregates when you create them.

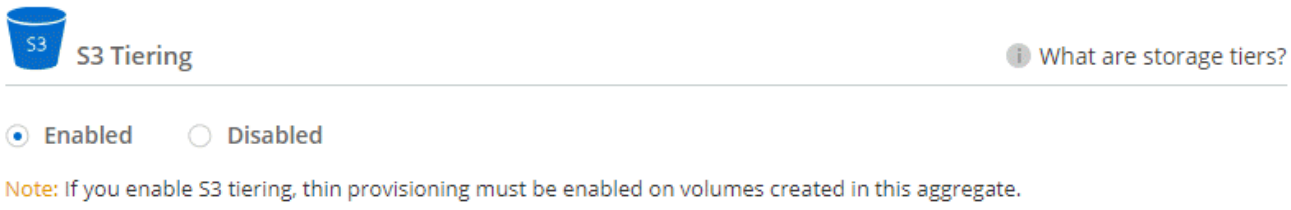
Tiering data from data protection volumes

Cloud Volumes ONTAP can tier data from a data protection volume to a capacity tier. If you activate the destination volume, the data gradually moves to the performance tier as it is read.

Steps

1. On the Working Environments page, select the working environment that contains the source volume, and then drag it to the working environment to which you want to replicate the volume.
2. Follow the prompts until you reach the tiering page and enable data tiering to object storage.

   Example



   For help with replicating data, see Replicating data to and from the cloud.

Changing the storage class for tiered data

After you deploy Cloud Volumes ONTAP, you can reduce your storage costs by changing the storage class for inactive data that hasn't been accessed for 30 days. The access costs are higher if you do access the data, so you must take that into consideration before you change the storage class.

The storage class for tiered data is system wide—it's not per volume.

For information about supported storage classes, see Data tiering overview.

Steps

1. From the working environment, click the menu icon and then click **Storage Classes** or **Blob Storage Tiering**.
2. Choose a storage class and then click **Save**.

Using ONTAP as persistent storage for Kubernetes

Cloud Manager can automate the deployment of NetApp Trident on Kubernetes clusters so you can use ONTAP as persistent storage for containers. This works with Cloud Volumes ONTAP and on-prem ONTAP clusters.

Before you complete these steps, you need to create a Cloud Volumes ONTAP system or discover an on-premises ONTAP cluster from Cloud Manager.

Verify network connectivity

a. A network connection must be available between Cloud Manager and the Kubernetes clusters, and from the Kubernetes clusters to ONTAP systems.

b. Cloud Manager needs an outbound internet connection to access the following endpoints when installing Trident:

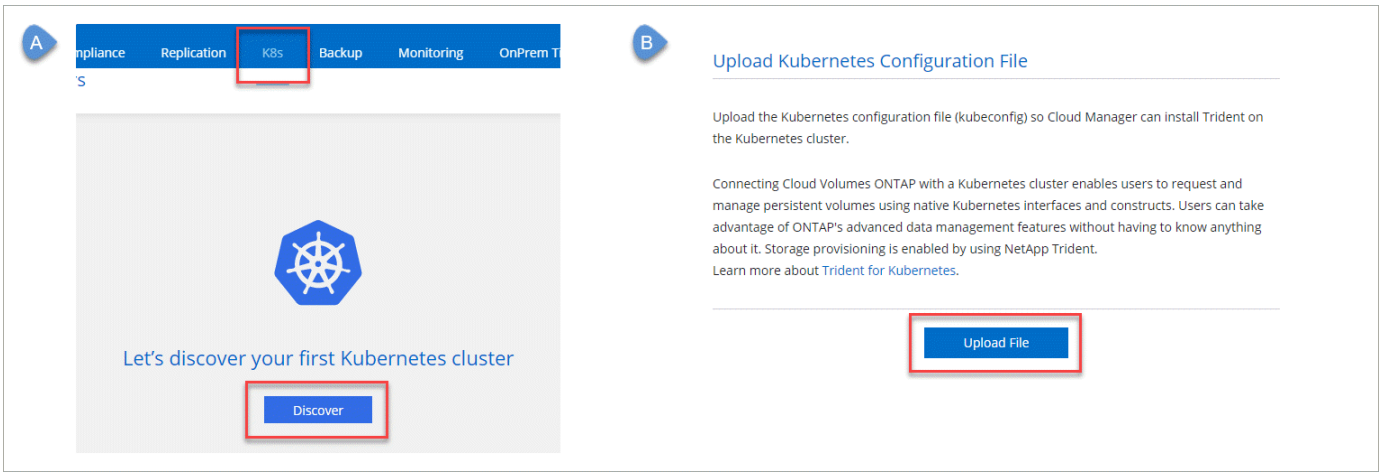
   https://packages.cloud.google.com/yum
   https://github.com/NetApp/trident/releases/download/

   Cloud Manager installs Trident on a Kubernetes cluster when you connect a working environment to the cluster.

Upload Kubernetes configuration files to Cloud Manager

For each Kubernetes cluster, the Account Admin needs to upload a configuration file (kubeconfig) that is in YAML format. After you upload the file, Cloud Manager verifies connectivity to the cluster and saves an encrypted copy of the kubeconfig file.

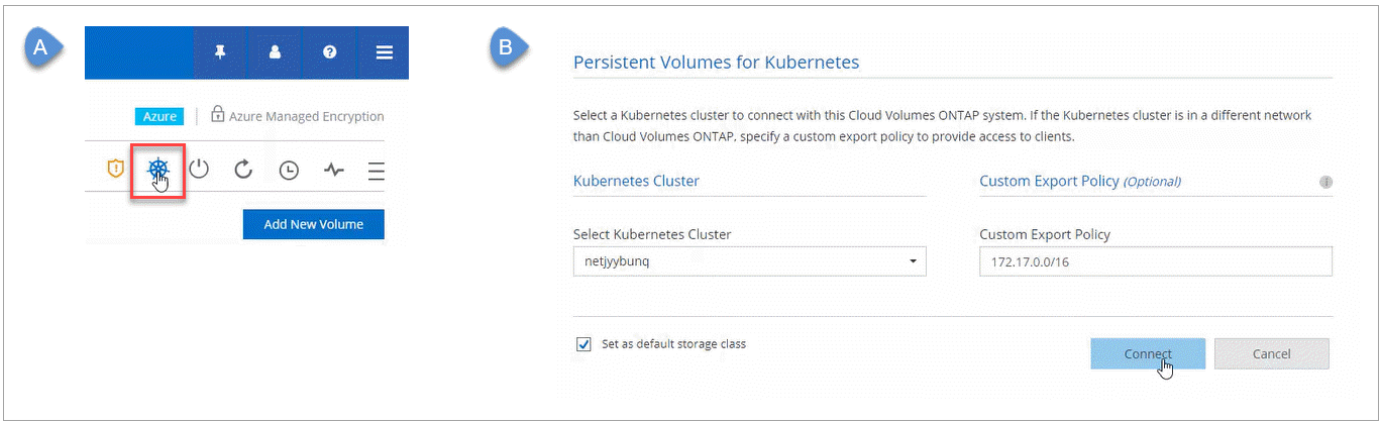
Click **K8s** > **Discover** > **Upload File** and select the kubeconfig file.



3 Connect your working environments to Kubernetes clusters

From the working environment, click the Kubernetes icon and follow the prompts. You can connect different clusters to different ONTAP systems and multiple clusters to the same ONTAP system.

You have the option to set the NetApp storage class as the default storage class for the Kubernetes cluster. When a user creates a persistent volume, the Kubernetes cluster can use connected ONTAP systems as the backend storage by default.



4 Start provisioning Persistent Volumes

Request and manage Persistent Volumes using native Kubernetes interfaces and constructs. Cloud Manager creates four Kubernetes storage classes that you can use when provisioning Persistent Volumes:

- **netapp-file**: for binding Persistent Volumes to single-node ONTAP systems
- **netapp-file-san**: for binding iSCSI Persistent Volumes to single-node ONTAP systems
- **netapp-file-redundant**: for binding Persistent Volumes to ONTAP HA pairs
- **netapp-file-redundant-san**: for binding iSCSI Persistent Volumes to ONTAP HA pairs

Cloud Manager configures Trident to use the following provisioning options by default:

- Thin volumes
- The default Snapshot policy
- Accessible Snapshot directory

Learn more about provisioning your first volume with Trident for Kubernetes

What are the trident_trident volumes?

Cloud Manager creates a volume on the first ONTAP system that you connect to a Kubernetes cluster. The name of the volume is appended with "_trident_trident." ONTAP uses this volume to connect to the Kubernetes cluster. You should not delete these volumes.

What happens when you disconnect or remove a Kubernetes cluster?

Cloud Manager enables you to disconnect individual ONTAP systems from a Kubernetes cluster. When you disconnect a system, you can no longer use that ONTAP system as persistent storage for containers. Existing Persistent Volumes are not deleted.

After you disconnect all systems from a Kubernetes cluster, you can also remove the entire Kubernetes configuration from Cloud Manager. Cloud Manager does not uninstall Trident when you remove the cluster and it does not delete any Persistent Volumes.

Both of these actions are available through APIs only. We plan to add the actions to the interface in a future release.
Click here for details about the APIs.

Encrypting volumes with NetApp encryption solutions

Cloud Volumes ONTAP supports both NetApp Volume Encryption (NVE) and NetApp Aggregate Encryption (NAE) with an external key manager. NVE and NAE are software-based solutions that enable (FIPS) 140-2–compliant data-at-rest encryption of volumes. Learn more about these encryption solutions.

Starting with Cloud Volumes ONTAP 9.7, new aggregates will have NAE enabled by default after you set up an external key manager. New volumes that aren't part of an NAE aggregate will have NVE enabled by default (for example, if you have existing aggregates that were created before setting up an external key manager).

Cloud Volumes ONTAP doesn't support onboard key management.

What you'll need

Your Cloud Volumes ONTAP system should be registered with NetApp support. Starting with Cloud Manager 3.7.1, a NetApp Volume Encryption license is automatically installed on each Cloud Volumes ONTAP system that is registered with NetApp Support.

- Adding NetApp Support Site accounts to Cloud Manager
- Registering pay-as-you-go systems

Cloud Manager doesn't install the NVE license on systems that reside in the China region.

Steps

1. Review the list of supported key managers in the NetApp Interoperability Matrix Tool.

   Search for the **Key Managers** solution.

2. Connect to the Cloud Volumes ONTAP CLI.
3. Install SSL certificates and connect to the external key management servers.

   ONTAP 9 NetApp Encryption Power Guide: Configuring external key management

Replicating data between systems

You can replicate data between working environments by choosing a one-time data replication for data transfer, or a recurring schedule for disaster recovery or long-term retention. For example, you can set up data replication from an on-prem ONTAP system to Cloud Volumes ONTAP for disaster recovery.

Cloud Manager simplifies data replication between volumes on separate systems using SnapMirror and SnapVault technologies. You simply need to identify the source volume and the destination volume, and then choose a replication policy and schedule. Cloud Manager purchases the required disks, configures relationships, applies the replication policy, and then initiates the baseline transfer between volumes.

The baseline transfer includes a full copy of the source data. Subsequent transfers contain differential copies of the source data.

Data replication requirements

Before you can replicate data, you should confirm that specific requirements are met for both Cloud Volumes ONTAP systems and ONTAP clusters.

Version requirements

You should verify that the source and destination volumes are running compatible ONTAP versions before replicating data. For details, see the Data Protection Power Guide.

Requirements specific to Cloud Volumes ONTAP

- The instance's security group must include the required inbound and outbound rules: specifically, rules for ICMP and ports 11104 and 11105.

  These rules are included in the predefined security group.

- To replicate data between two Cloud Volumes ONTAP systems in different subnets, the subnets must be routed together (this is the default setting).
- To replicate data between a Cloud Volumes ONTAP system in AWS and a system in Azure, you must have a VPN connection between the AWS VPC and the Azure VNet.

Requirements specific to ONTAP clusters

- An active SnapMirror license must be installed.
- If the cluster is on your premises, you should have a connection from your corporate network to AWS or Azure, which is typically a VPN connection.
- ONTAP clusters must meet additional subnet, port, firewall, and cluster requirements.

  For details, see the Cluster and SVM Peering Express Guide for your version of ONTAP.

Setting up data replication between systems

You can replicate data between Cloud Volumes ONTAP systems and ONTAP clusters by choosing a one-time data replication, which can help you move data to and from the cloud, or a recurring schedule, which can help with disaster recovery or long-term retention.

About this task

Cloud Manager supports simple, fanout, and cascade data protection configurations:

- In a simple configuration, replication occurs from volume A to volume B.
- In a fanout configuration, replication occurs from volume A to multiple destinations.
- In a cascade configuration, replication occurs from volume A to volume B and from volume B to volume C.

You can configure fanout and cascade configurations in Cloud Manager by setting up multiple data replications between systems. For example, by replicating a volume from system A to system B and then by replicating the same volume from system B to system C.

Steps

1. On the Working Environments page, select the working environment that contains the source

volume, and then drag it to the working environment to which you want to replicate the volume:

2. If the Source and Destination Peering Setup pages appear, select all of the intercluster LIFs for the cluster peer relationship.

   The intercluster network should be configured so that cluster peers have *pair-wise full-mesh connectivity*, which means that each pair of clusters in a cluster peer relationship has connectivity among all of their intercluster LIFs.

   These pages appear if an ONTAP cluster that has multiple LIFs is the source or destination.

3. On the Source Volume Selection page, select the volume that you want to replicate.
4. On the Destination Volume Name and Tiering page, specify the destination volume name, choose an underlying disk type, change any of the advanced options, and then click **Continue**.

   If the destination is an ONTAP cluster, you must also specify the destination SVM and aggregate.

5. On the Max Transfer Rate page, specify the maximum rate (in megabytes per second) at which data can be transferred.
6. On the Replication Policy page, choose one of the default policies or click **Additional Policies**, and then select one of the advanced policies.

   For help, see Choosing a replication policy.

   If you choose a custom backup (SnapVault) policy, the labels associated with the policy must match the labels of the Snapshot copies on the source volume. For more information, see How backup policies work.

7. On the Schedule page, choose a one-time copy or a recurring schedule.

   Several default schedules are available. If you want a different schedule, you must create a new schedule on the *destination* cluster using System Manager.

8. On the Review page, review your selections, and then click **Go**.

Result

Cloud Manager starts the data replication process. You can view details about the replication in the Replication Status page.

Managing data replication schedules and relationships

After you set up data replication between two systems, you can manage the data replication schedule and relationship from Cloud Manager.

Steps

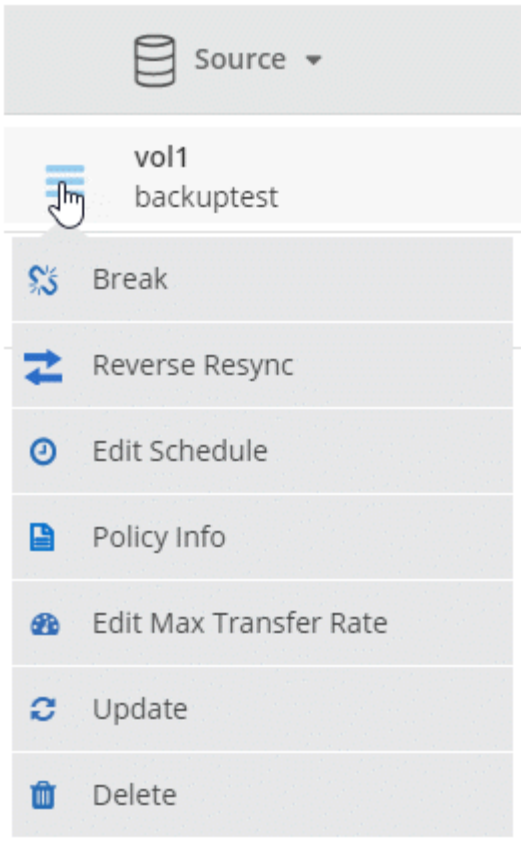
1. On the Working Environments page, view the replication status for all working environments in the workspace or for a specific working environment:

Option	Action
All working environments in the workspace	At the top of Cloud Manager, click **Replication Status**.
A specific working environment	Open the working environment and click **Replications**.

2. Review the status of the data replication relationships to verify that they are healthy.

If the Status of a relationship is idle and the Mirror State is uninitialized, you must initialize the relationship from the destination system for the data replication to occur according to the defined schedule. You can initialize the relationship by using System Manager or the command-line interface (CLI). These states can appear when the destination system fails and then comes back online.

3. Select the menu icon next to the source volume, and then choose one of the available actions.



The following table describes the available actions:

Action	Description
Break	Breaks the relationship between the source and destination volumes, and activates the destination volume for data access. This option is typically used when the source volume cannot serve data due to events such as data corruption, accidental deletion, or an offline state. For information about configuring a destination volume for data access and reactivating a source volume, see the ONTAP 9 Volume Disaster Recovery Express Guide.

Action	Description
Resync	Reestablishes a broken relationship between volumes and resumes data replication according to the defined schedule. When you resynchronize the volumes, the contents on the destination volume are overwritten by the contents on the source volume. To perform a reverse resync, which resynchronizes the data from the destination volume to the source volume, see the ONTAP 9 Volume Disaster Recovery Express Guide.
Reverse Resync	Reverses the roles of the source and destination volumes. Contents from the original source volume are overwritten by contents of the destination volume. This is helpful when you want to reactivate a source volume that went offline. Any data written to the original source volume between the last data replication and the time that the source volume was disabled is not preserved.
Edit Schedule	Enables you to choose a different schedule for data replication.
Policy Info	Shows you the protection policy assigned to the data replication relationship.
Edit Max Transfer Rate	Enables you to edit the maximum rate (in kilobytes per second) at which data can be transferred.
Update	Starts an incremental transfer to update the destination volume.
Delete	Deletes the data protection relationship between the source and destination volumes, which means that data replication no longer occurs between the volumes. This action does not activate the destination volume for data access. This action also deletes the cluster peer relationship and the storage virtual machine (SVM) peer relationship, if there are no other data protection relationships between the systems.

Result

After you select an action, Cloud Manager updates the relationship or schedule.

Choosing a replication policy

You might need help choosing a replication policy when you set up data replication in Cloud Manager. A replication policy defines how the storage system replicates data from a source volume to a destination volume.

What replication policies do

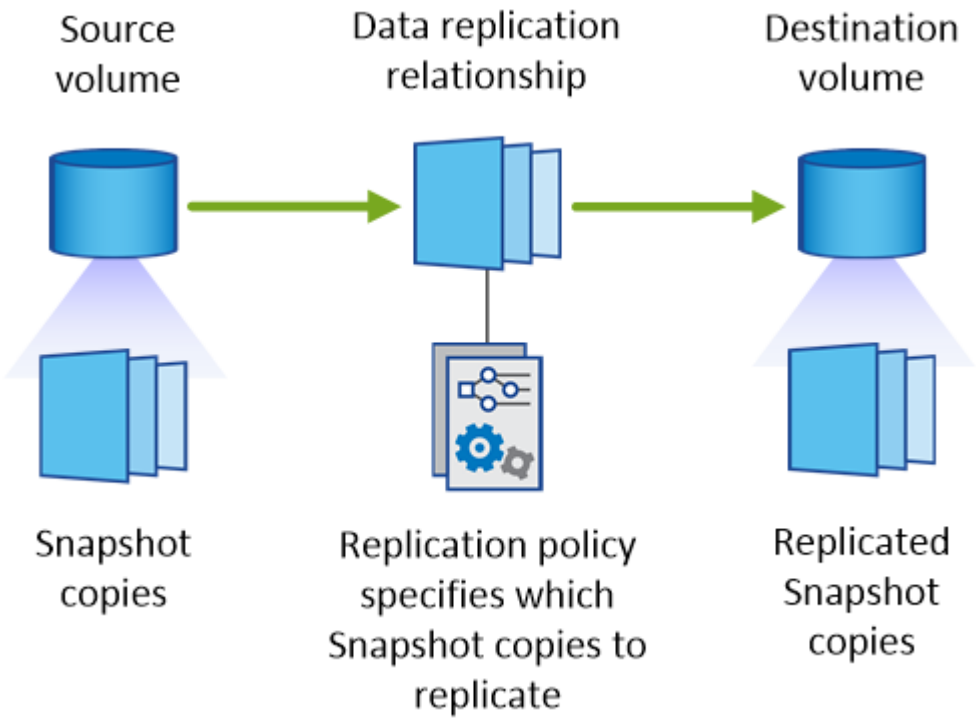
The ONTAP operating system automatically creates backups called Snapshot copies. A Snapshot copy is

a read-only image of a volume that captures the state of the file system at a point in time.

When you replicate data between systems, you replicate Snapshot copies from a source volume to a destination volume. A replication policy specifies which Snapshot copies to replicate from the source volume to the destination volume.

Replication policies are also referred to as *protection* policies because they are powered by SnapMirror and SnapVault technologies, which provide disaster recovery protection and disk-to-disk backup and recovery.

The following image shows the relationship between Snapshot copies and replication policies:



Types of replication policies

There are three types of replication policies:

- A *Mirror* policy replicates newly created Snapshot copies to a destination volume.

  You can use these Snapshot copies to protect the source volume in preparation for disaster recovery or for one-time data replication. You can activate the destination volume for data access at any time.

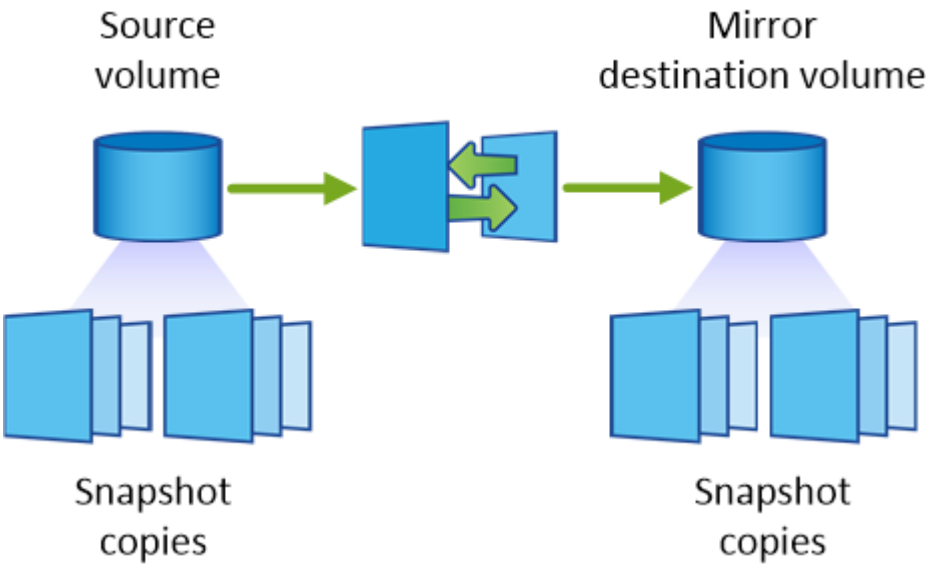
- A *Backup* policy replicates specific Snapshot copies to a destination volume and typically retains them for a longer period of time than you would on the source volume.

  You can restore data from these Snapshot copies when data is corrupted or lost, and retain them for standards compliance and other governance-related purposes.

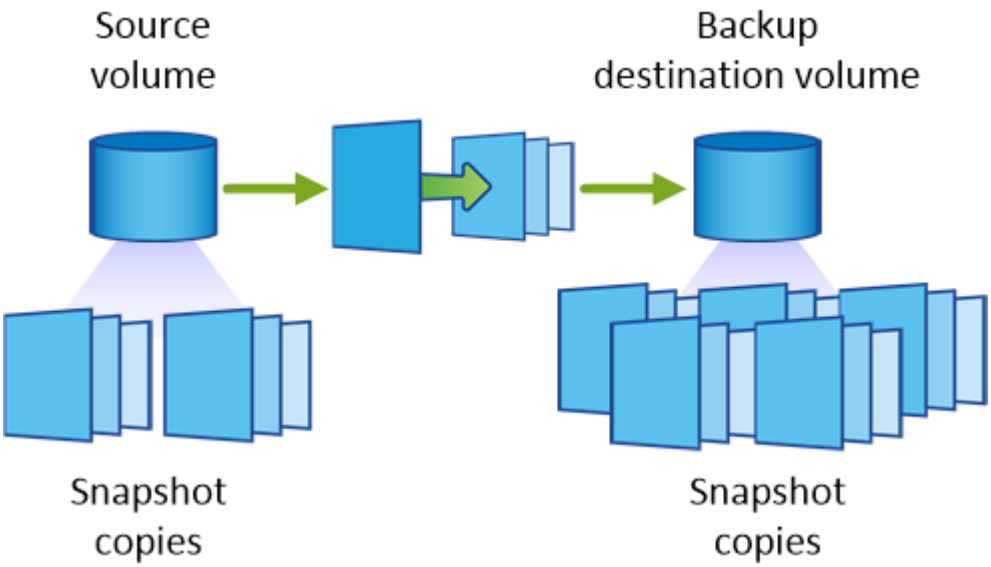
- A *Mirror and Backup* policy provides both disaster recovery and long-term retention.

  Each system includes a default Mirror and Backup policy, which works well for many situations. If you find that you need custom policies, you can create your own using System Manager.

The following images show the difference between the Mirror and Backup policies. A Mirror policy mirrors the Snapshot copies available on the source volume.



A Backup policy typically retains Snapshot copies longer than they are retained on the source volume:



How Backup policies work

Unlike Mirror policies, Backup (SnapVault) policies replicate specific Snapshot copies to a destination volume. It is important to understand how Backup policies work if you want to use your own policies instead of the default policies.

Understanding the relationship between Snapshot copy labels and Backup policies

A Snapshot policy defines how the system creates Snapshot copies of volumes. The policy specifies when to create the Snapshot copies, how many copies to retain, and how to label them. For example, a system might create one Snapshot copy every day at 12:10 a.m., retain the two most recent copies, and label them "daily".

A Backup policy includes rules that specify which labeled Snapshot copies to replicate to a destination volume and how many copies to retain. The labels defined in a Backup policy must match one or more labels defined in a Snapshot policy. Otherwise, the system cannot replicate any Snapshot copies.

For example, a Backup policy that includes the labels "daily" and "weekly" results in replication of Snapshot copies that include only those labels. No other Snapshot copies are replicated, as shown in the following image:

Default policies and custom policies

The default Snapshot policy creates hourly, daily, and weekly Snapshot copies, retaining six hourly, two daily, and two weekly Snapshot copies.

You can easily use a default Backup policy with the default Snapshot policy. The default Backup policies replicate daily and weekly Snapshot copies, retaining seven daily and 52 weekly Snapshot copies.

If you create custom policies, the labels defined by those policies must match. You can create custom policies using System Manager.

Backup to Cloud

Learn about Backup to Cloud

Backup to Cloud is an add-on service for Cloud Volumes ONTAP that delivers backup and restore capabilities for protection, and long-term archive of your cloud data. Backups are stored in an object store in your cloud account, independent of volume Snapshot copies used for near-term recovery or cloning.

Backup to Cloud is powered by the Cloud Backup Service.

You must use Cloud Manager for all backup and restore operations. Any actions taken directly from ONTAP or from your cloud provider results in an unsupported configuration.

Features

- Back up independent copies of your data volumes to low-cost object storage in the cloud.

  Backup data is secured with AES-256 bit encryption at-rest and TLS 1.2 HTTPS connections in-flight.

- Restore data from a specific point in time.
- Restore the data to the source Cloud Volumes ONTAP system or to a different system.

Supported object storage providers

Backup to Cloud is supported with the following types of working environments:

- Cloud Volumes ONTAP in AWS
- Cloud Volumes ONTAP in Azure

Cost

You'll need to pay your cloud provider for object storage costs and NetApp for backup licensing costs. The licensing costs are based on used capacity (before storage efficiencies).

- AWS: A 30-day free trial is available. Go to the Cloud Manager Marketplace offering for pricing details.
- Azure: A 30-day free trial is available. Go to the Cloud Manager Marketplace offering for pricing details.

How Backup to Cloud works

When you enable Backup to Cloud, the service performs a full backup of your data. After the initial backup, all additional backups are incremental, which means that only changed blocks and new blocks are backed up.

Where backups reside

Backup copies are stored in an S3 bucket or Azure Blob container that Cloud Manager creates in your cloud account. The object store is created in the same region where the Cloud Volumes ONTAP system is located. There's one object store per Cloud Volumes ONTAP system.

Cloud Manager names the object store as follows: netapp-backup-*clusteruuid*

Be sure not to delete this object store.

Notes:

- In AWS, Cloud Manager enables the Amazon S3 Block Public Access feature on the S3 bucket.
- In Azure, Cloud Manager creates a new resource group with a storage account for the Blob container.

Supported S3 storage classes

In Amazon S3, backups start in the *Standard* storage class and transition to the *Standard-Infrequent Access* storage class after 30 days.

Supported Azure Blob access tiers

In Azure, each backup is associated with the *cold* access tier.

Backup settings are system wide

When you enable Backup to Cloud, *all* supported volumes on the system are backed up to the cloud.

The schedule and number of backups to retain are defined at the system level. The backup settings affect all volumes on the system.

The schedule is daily, *or* weekly, *or* monthly

You can choose daily, or weekly, or monthly backups of all volumes. A combination of these backup frequency options isn't supported.

Backups are taken at midnight

- Daily backups start just after midnight each day.
- Weekly backups start just after midnight on Sunday mornings.
- Monthly backups start just after midnight on the first of each month.

At this time, you can't schedule backup operations at a user specified time.

Backup copies are associated with your Cloud Central account

Backup copies are associated with the Cloud Central account in which Cloud Manager resides.

If you have multiple Cloud Manager systems in the same Cloud Central account, each Cloud Manager system will display the same list of backups. That includes the backups associated with Cloud Volumes ONTAP instances from other Cloud Manager systems.

Supported volumes

Backup to Cloud supports read-write volumes only.

FlexGroup volumes and data protection volumes aren't supported.

Limitations

- Volumes that you create outside of Cloud Manager aren't automatically backed up.

  For example, if you create a volume from the ONTAP CLI, ONTAP API, or System Manager, then the volume won't be automatically backed up.

If you want to back up these volumes, you would need to disable Backup to Cloud and then enable it again.

- Backup to Cloud can maintain up to 1,019 total backups of a volume.
- In Azure, if you enable Backup to Cloud when Cloud Volumes ONTAP is deployed, Cloud Manager creates the resource group for you and you cannot change it. If you want to pick your own resource group when enabling Backup to Cloud, **disable** Backup to Cloud when deploying Cloud Volumes ONTAP and then enable Backup to Cloud and choose the resource group from the Backup to Cloud Settings page.
- WORM storage is not supported on a Cloud Volumes ONTAP system when Backup to Cloud is enabled.

Get started

Backing up data to Amazon S3

Complete a few steps to get started backing up data from Cloud Volumes ONTAP to Amazon S3.

Quick start

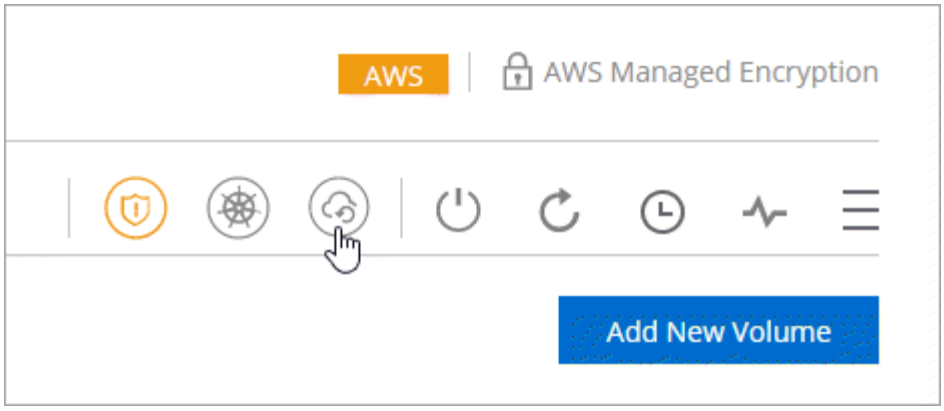
Get started quickly by following these steps or scroll down to the remaining sections for full details.

Verify support for your configuration

- You're running Cloud Volumes ONTAP 9.6 or later in AWS.
- You have subscribed to the new Cloud Manager Marketplace offering.
- The IAM role that provides Cloud Manager with permissions includes S3 permissions from the latest Cloud Manager policy.

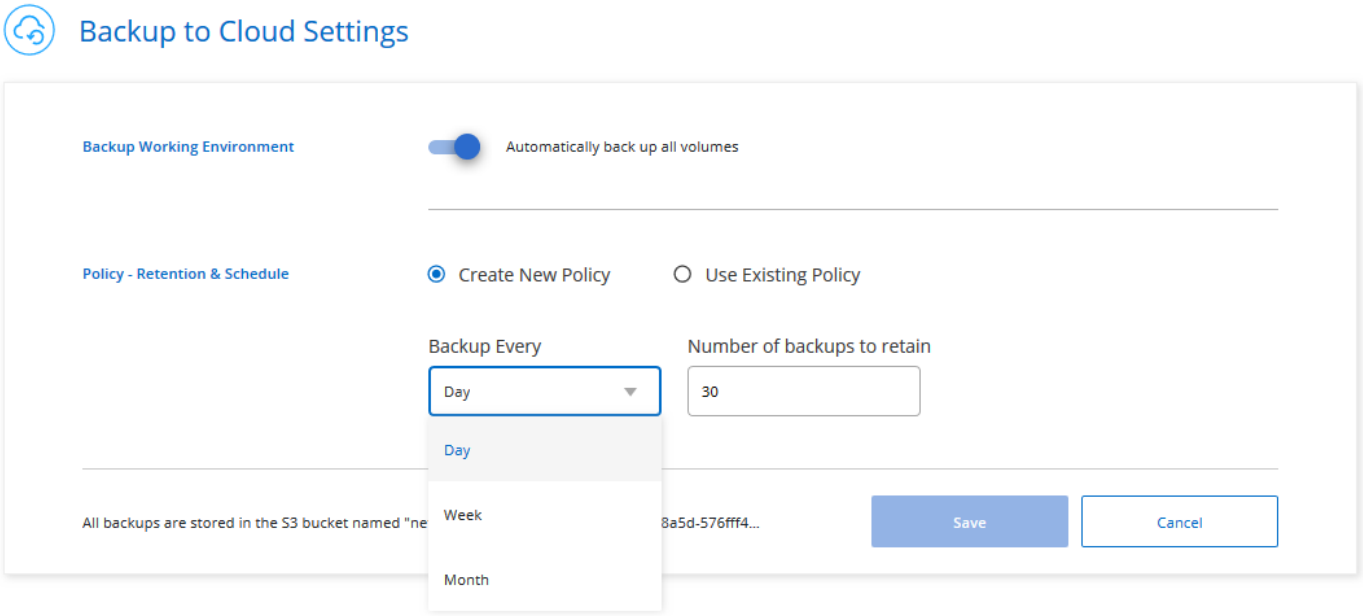
Enable Backup to Cloud on your new or existing system

- New systems: Backup to Cloud is enabled by default in the working environment wizard. Be sure to keep the option enabled.
- Existing systems: Open the working environment, click the backup settings icon and enable backups.



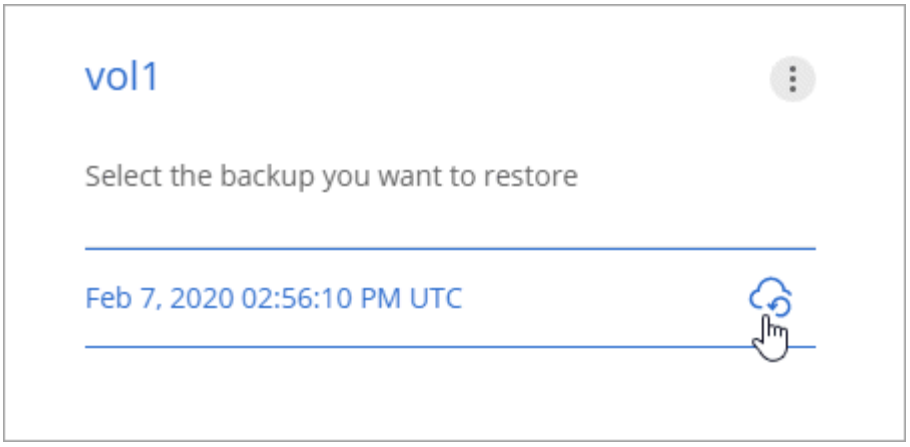
If needed, modify the backup policy

The default policy backs up volumes every day and retains the most recent 30 backup copies of each volume. Change to weekly or monthly backups, or select one of the system-defined policies that provide more options. You can also change the number of backup copies to retain.



Restore your data, as needed

At the top of Cloud Manager, click **Backup**, select a volume, select a backup, and then restore data from the backup to a new volume.



Requirements

Read the following requirements to make sure that you have a supported configuration before you start backing up volumes to S3.

Supported ONTAP versions

Cloud Volumes ONTAP 9.6 and later.

Supported AWS regions

Backup to Cloud is supported in all AWS regions where Cloud Volumes ONTAP is supported.

AWS subscription requirement

Starting with the 3.7.3 release, a new Cloud Manager subscription is available in the AWS Marketplace. This subscription enables deployments of Cloud Volumes ONTAP 9.6 and later (PAYGO) and Backup to Cloud. You need to subscribe to this new Cloud Manager subscription before you enable Backup to Cloud. Billing for Backup to Cloud is done through this subscription.

AWS permissions required

The IAM role that provides Cloud Manager with permissions must include S3 permissions from the latest Cloud Manager policy.

Here are the specific permissions from the policy:

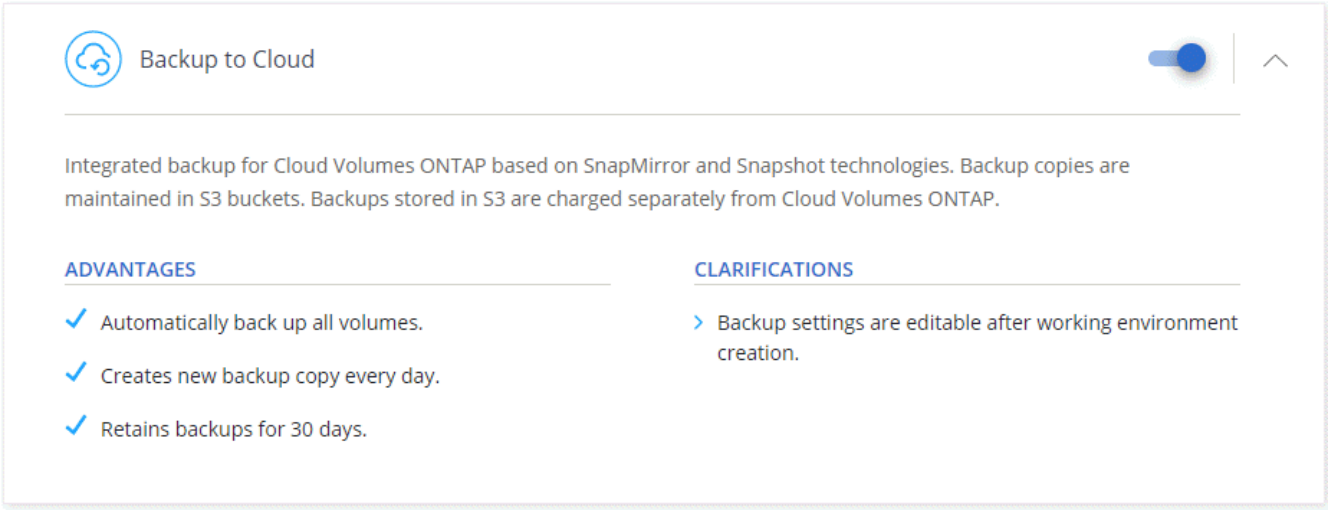
```
{
            "Sid": "backupPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:ListAllMyBuckets",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "s3:PutBucketPublicAccessBlock"
            ],
            "Resource": [
                "arn:aws:s3:::netapp-backup-*"
            ]
        },
```

Enabling Backup to Cloud on a new system

Backup to Cloud is enabled by default in the working environment wizard. Be sure to keep the option enabled.

Steps

1. Click **Create Cloud Volumes ONTAP**.
2. Select Amazon Web Services as the cloud provider and then choose a single node or HA system.
3. Fill out the Details & Credentials page.
4. On the Services page, leave the service enabled and click **Continue**.



5. Complete the pages in the wizard to deploy the system.

Result

Backup to Cloud is enabled on the system and backs up volumes every day and retains the most recent 30 backup copies.

What's next?

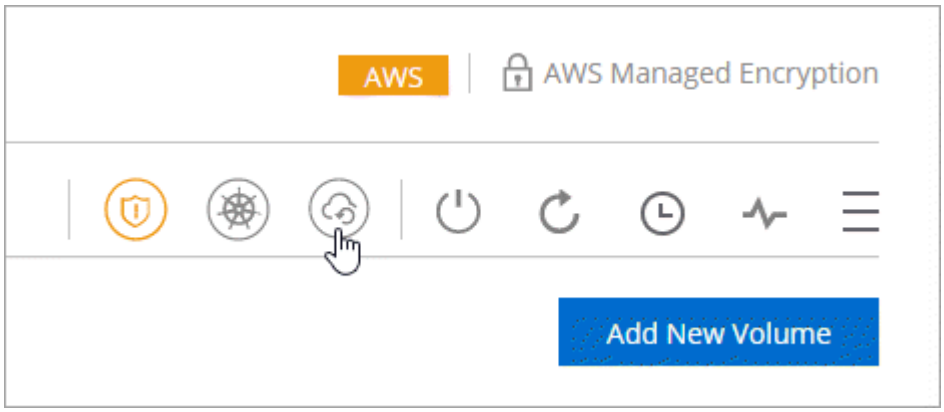
You can manage backups by changing the backup schedule, restoring volumes, and more.

Enabling Backup to Cloud on an existing system

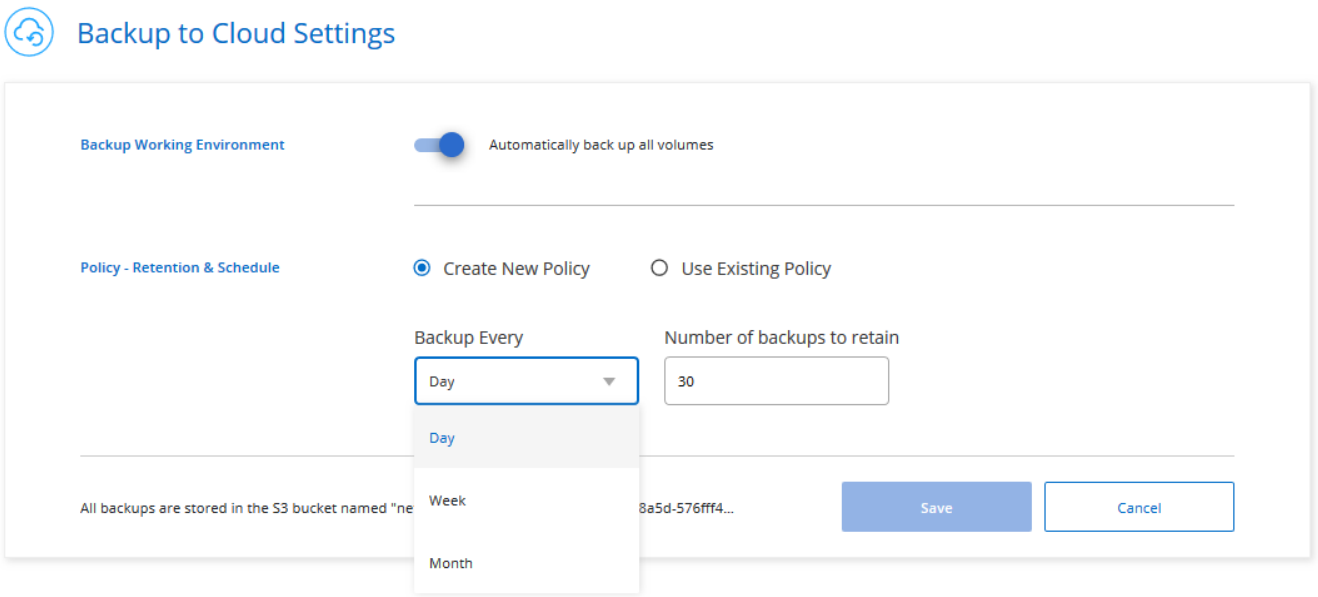
Enable Backup to Cloud at any time directly from the working environment.

Steps

1. Open the working environment.
2. Click the backup settings icon.



3. Select **Automatically back up all volumes**.
4. Choose your backup schedule and retention value and then click **Save**.



Result

Backup to Cloud starts taking the initial backups of each volume.

What's next?

You can manage backups by changing the backup schedule, restoring volumes, and more.

Backing up data to Azure Blob storage

Complete a few steps to get started backing up data from Cloud Volumes ONTAP to Azure Blob storage.

Quick start

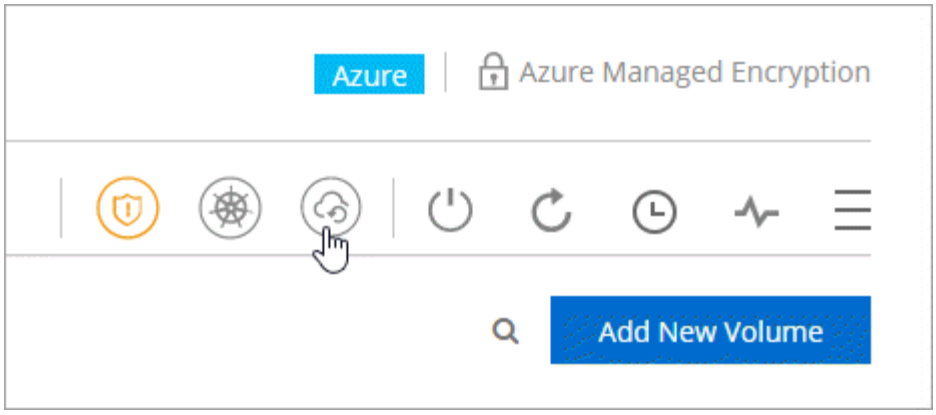
Get started quickly by following these steps or scroll down to the remaining sections for full details.

1 Verify support for your configuration

You're running Cloud Volumes ONTAP 9.7 or later in Azure.

2 Enable Backup to Cloud on your new or existing system

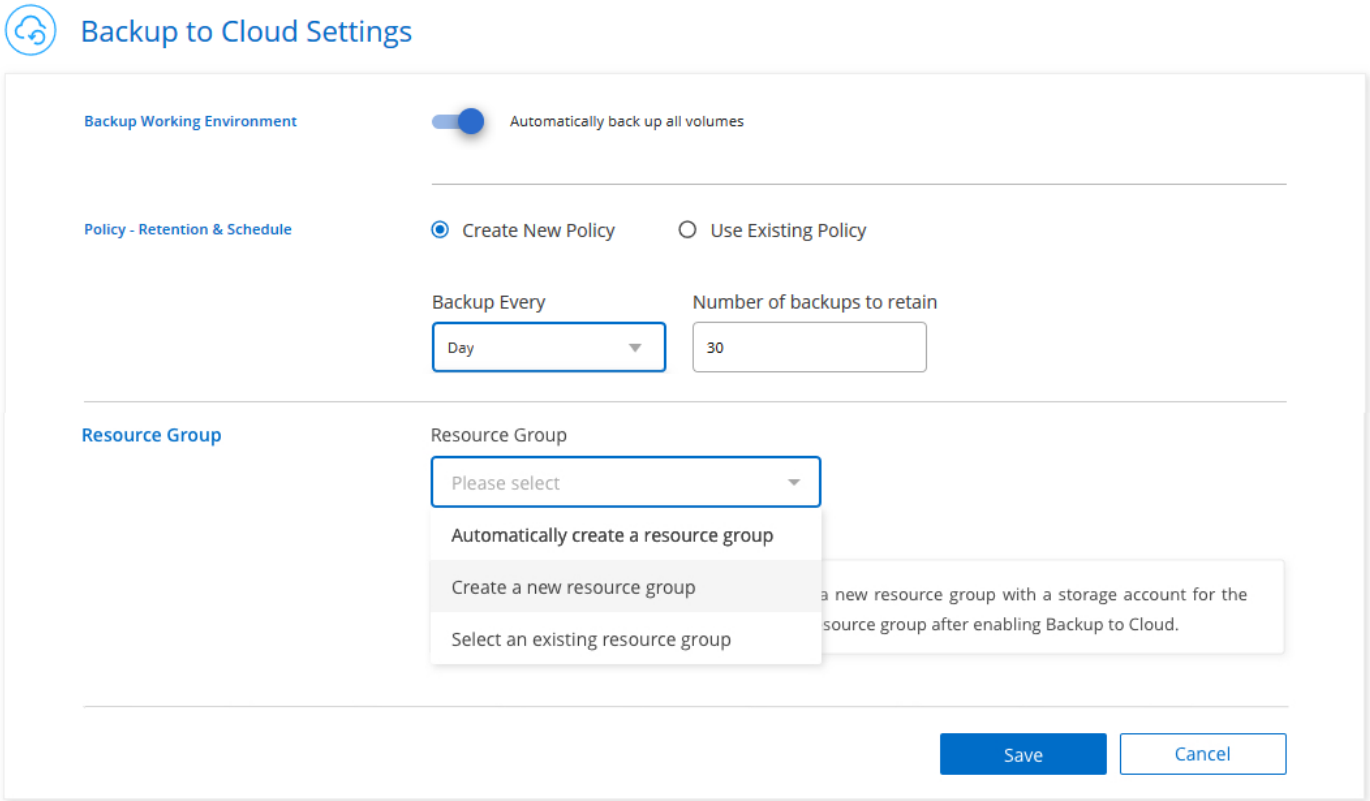
- New systems: Backup to Cloud is enabled by default in the working environment wizard. Be sure to keep the option enabled.
- Existing systems: Open the working environment, click the backup settings icon and enable backups.



3 If needed, modify the backup policy

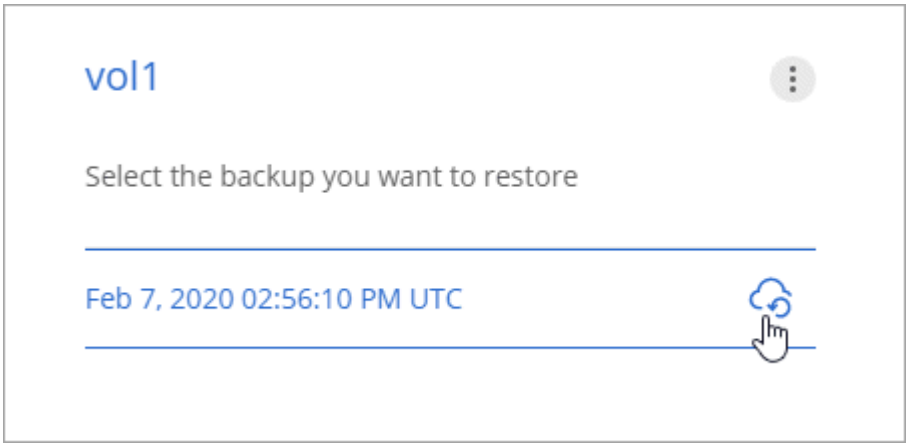
The default policy backs up volumes every day and retains the most recent 30 backup copies of each volume. Change to weekly or monthly backups, or select one of the system-defined policies that provide more options.

On existing systems, you can pick your own resource group when enabling Backup to Cloud for the first time. If you enable Backup to Cloud when Cloud Volumes ONTAP is deployed, Cloud Manager creates the resource group for you and you cannot change it.



Restore your data, as needed

At the top of Cloud Manager, click **Backup**, select a volume, select a backup, and then restore data from the backup to a new volume.



Requirements

Read the following requirements to make sure that you have a supported configuration before you start backing up volumes to Azure Blob storage.

Supported ONTAP versions

Cloud Volumes ONTAP 9.7 and later.

Supported Azure regions

Backup to Cloud is supported in all Azure regions where Cloud Volumes ONTAP is supported.

Azure Marketplace subscription

A subscription through the Azure Marketplace is required before you enable Backup to Cloud. You can subscribe from the Details & Credentials page of the working environment wizard.

Enabling Backup to Cloud on a new system

Backup to Cloud is enabled by default in the working environment wizard. Be sure to keep the option enabled.

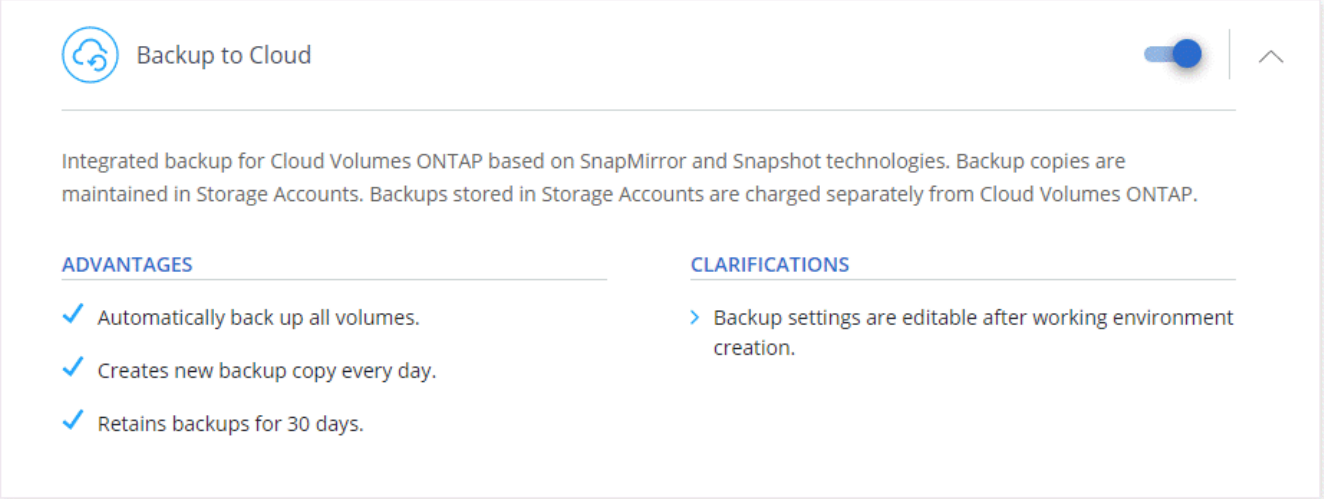
If you want to pick the name of the resource group, **disable** Backup to Cloud when deploying Cloud Volumes ONTAP. Follow the steps for enabling backup to cloud on an existing system to enable Backup to Cloud and choose the resource group.

Steps

1. Click **Create Cloud Volumes ONTAP**.
2. Select Microsoft Azure as the cloud provider and then choose a single node or HA system.
3. Fill out the Details & Credentials page and be sure that an Azure Marketplace subscription is in

place.

4. On the Services page, leave the service enabled and click **Continue**.



5. Complete the pages in the wizard to deploy the system.

Result

Backup to Cloud is enabled on the system and backs up volumes every day and retains the most recent 30 backup copies.

What's next?

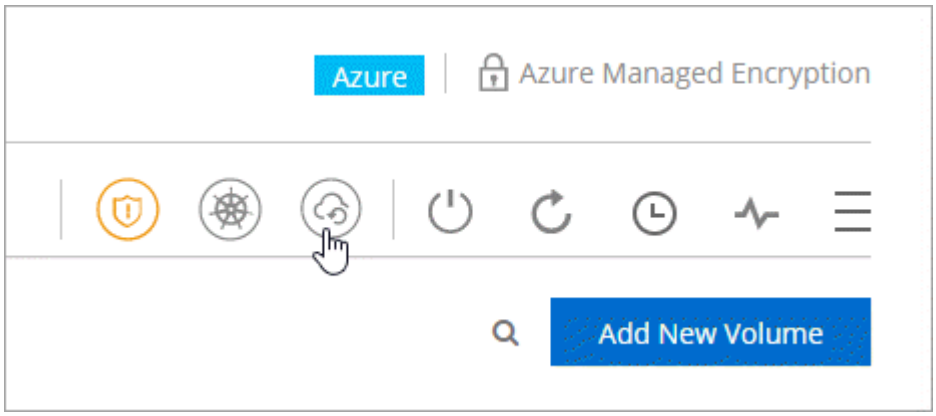
You can manage backups by changing the backup schedule, restoring volumes, and more.

Enabling Backup to Cloud on an existing system

Enable Backup to Cloud at any time directly from the working environment.

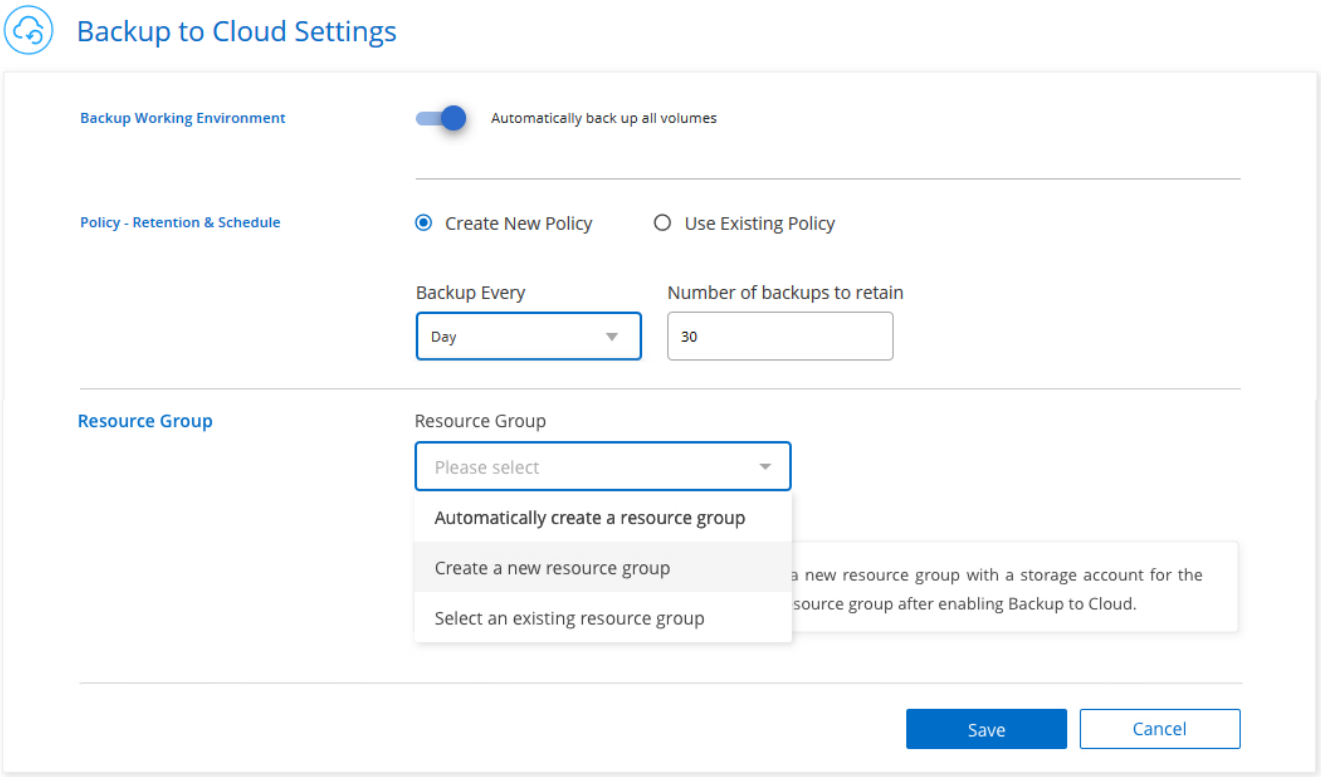
Steps

1. Open the working environment.
2. Click the backup settings icon.



3. Select **Automatically back up all volumes**.

4. Choose your backup schedule and retention value.



5. Choose how the resource group is created and click **Save**.
   - **Automatically create a resource group** - Cloud Manager creates a resource group
   - **Create a new resource group** - You create the resource group
   - **Select an existing resource group** - You select an existing resource group

Result

Backup to Cloud starts taking the initial backups of each volume.

What's next?

You can manage backups by changing the backup schedule, restoring volumes, and more.

Managing backups for Cloud Volumes ONTAP

Manage backups for Cloud Volumes ONTAP by changing the backup schedule, restoring volumes, and more.

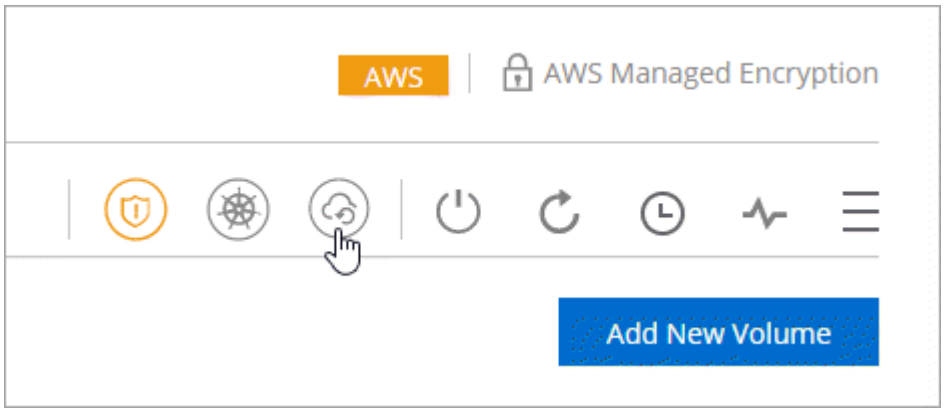
Changing the schedule and backup retention

The default policy backs up volumes every day and retains the most recent 30 backup copies of each volume. You can change to weekly or monthly backups and you can change the number of backup copies to retain. You can also select one of the system-defined policies that provide more options, such as *NetappRecommended2* that provides 30 daily, 13 weekly, and 12 monthly backups.

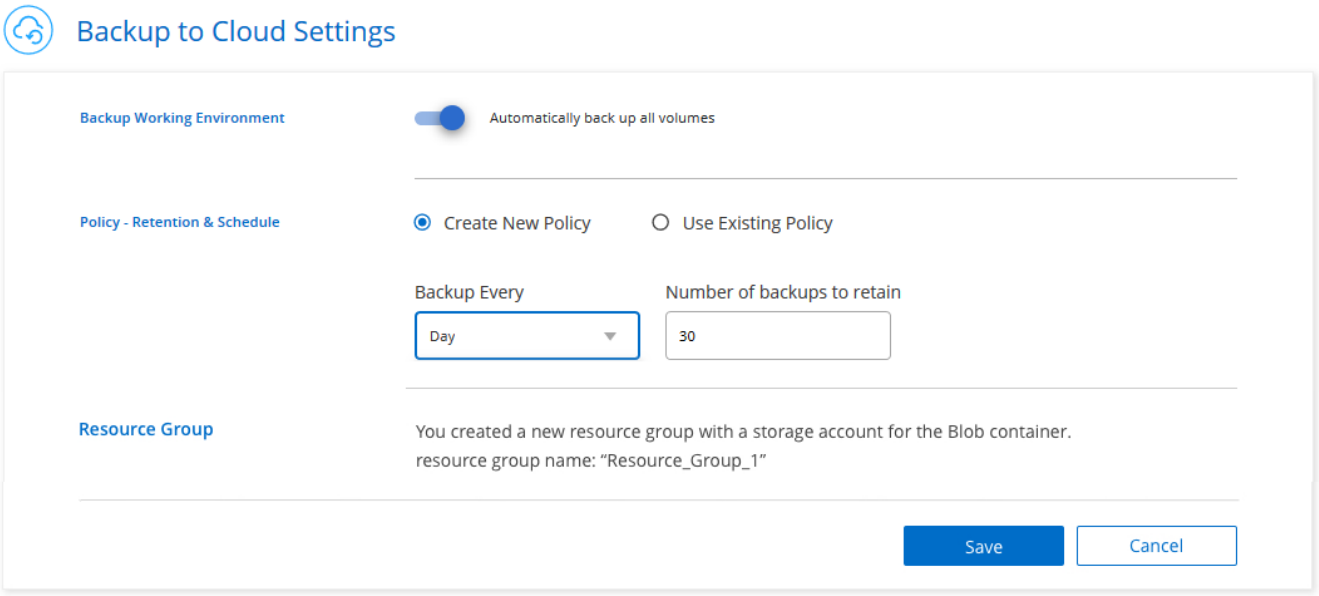
Changing the backup policy affects all future backups. It doesn't affect any previous backups that were created.

Steps

1. Open the working environment.
2. Click the backup settings icon.



3. Change the schedule and backup retention and then click **Save**.

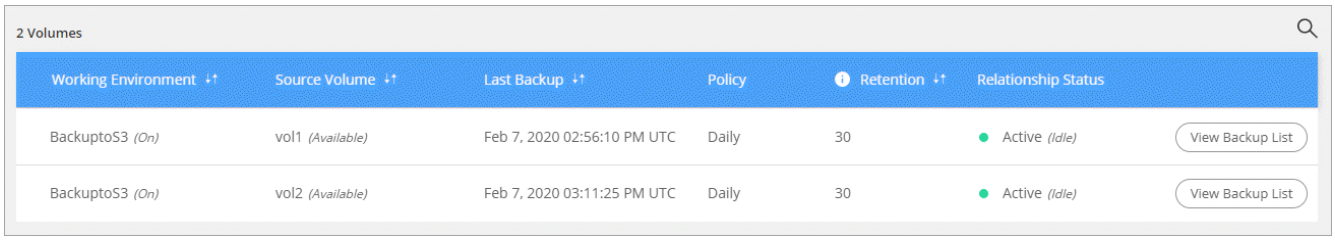


Restoring a volume

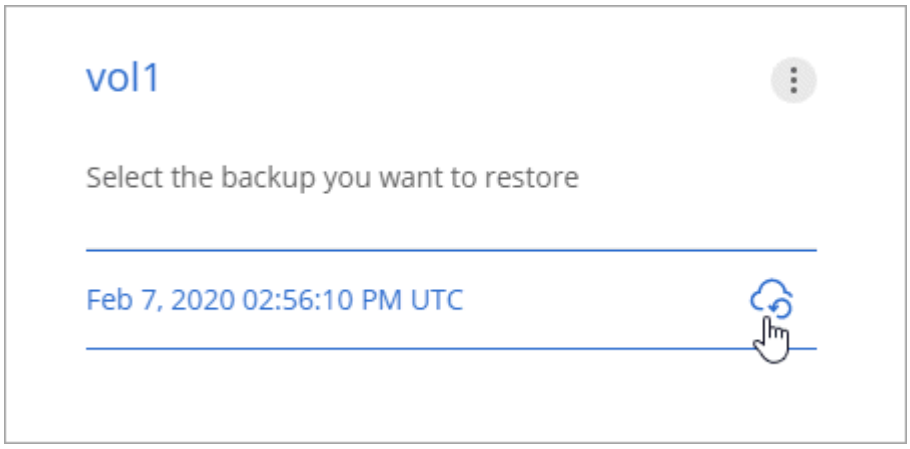
When you restore data from a backup, Cloud Manager performs a full volume restore to a *new* volume. You can restore the data to the same working environment or to a different working environment that's located in the same AWS account as the source working environment.

Steps

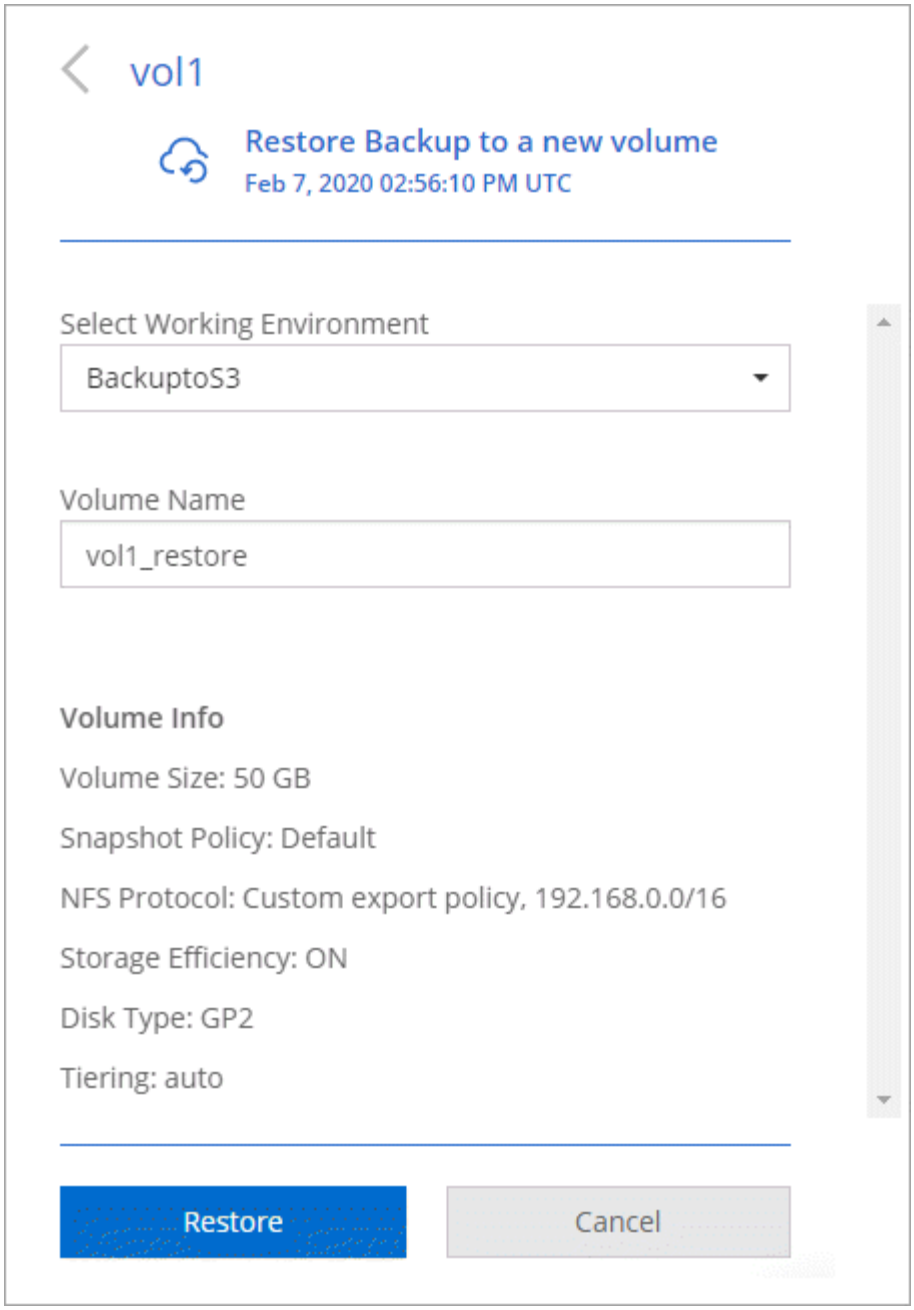
1. At the top of Cloud Manager, click **Backup**.
2. Select the volume that you want to restore.



3. Find the backup that you want to restore from and click the restore icon.



4. Select the working environment to which you want to restore the volume.
5. Enter a name for the volume.
6. Click **Restore**.



Deleting backups

Backup to Cloud enables you to delete *all* backups of a specific volume. You can't delete *individual* backups.

You might do this if you deleted a volume or if you deleted a Cloud Volumes ONTAP system. Backup to Cloud doesn't automatically delete backups when you delete a volume or when you delete a system.

Steps

1. At the top of Cloud Manager, click **Backup**.
2. Click **View Backup List** for a volume.
3. Click the menu and select **Delete All Backups**.

Result

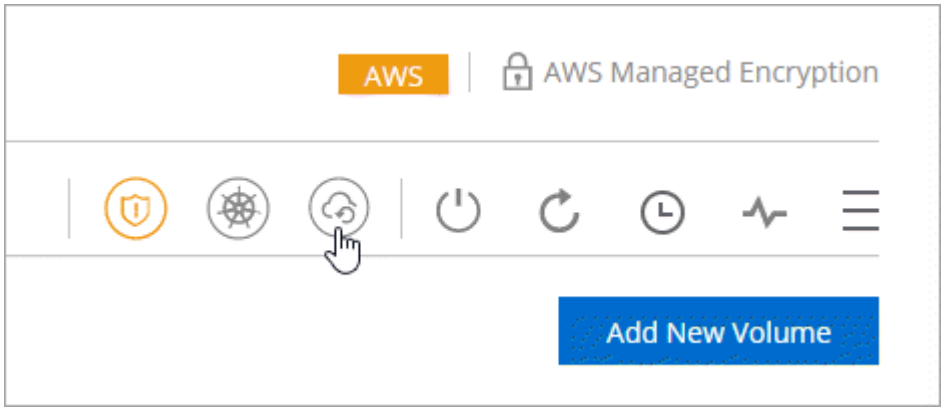
Cloud Manager deletes all backups for the selected volume.

Disabling Backup to Cloud

Disabling Backup to Cloud disables backups of each volume on the system. Any existing backups will not be deleted.

Steps

1. Open the working environment.
2. Click the backup settings icon.



3. Disable **Automatically back up all volumes** and then click **Save**.

Monitor performance

Learn about the Monitoring service

By leveraging the NetApp Cloud Insights service, Cloud Manager gives you insights into the health and performance of your Cloud Volumes ONTAP instances and helps you troubleshoot and optimize the performance of your cloud storage environment.

Features

- Automatically monitor all volumes
- View volume performance data in terms of IOPS, throughput, and latency
- Identify performance issues to minimize impact on your users and apps

Supported cloud providers

The Monitoring service is supported with Cloud Volumes ONTAP for AWS.

Cost

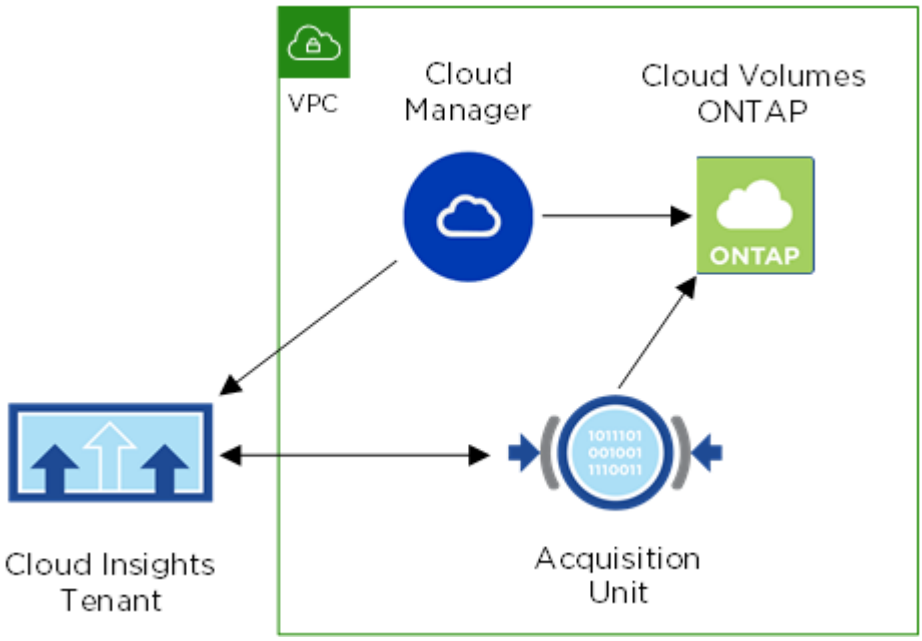
Monitoring is currently available as a Preview. Activation is free, but Cloud Manager launches a virtual machine in your VPC to facilitate monitoring. This VM results in charges from your cloud provider.

How Cloud Insights works with Cloud Manager

At a high-level, Cloud Insights integration with Cloud Manager works like this:

1. You enable the Monitoring service on Cloud Volumes ONTAP.
2. Cloud Manager configures your environment. It does the following:
    1. Creates a Cloud Insights tenant (also called *environment*) and associates all users in your Cloud Central account to the tenant.
    2. Enables a 30-day free trial of Cloud Insights.
    3. Deploys a virtual machine in your VPC called an Acquisition Unit, which facilitates monitoring of volumes (this is the VM mentioned in the Cost section above).
    4. Connects the Acquisition Unit to Cloud Volumes ONTAP and to the Cloud Insights tenant.
3. In Cloud Manager, you click Monitoring and use the performance data to troubleshoot and optimize performance.

The following image shows the relationship between these components:



The Acquisition Unit

When you enable Monitoring, Cloud Manager deploys an Acquisition Unit in the same subnet as Cloud Manager.

An *Acquisition Unit* collects performance data from Cloud Volumes ONTAP and sends it to the Cloud

Insights tenant. Cloud Manager then queries that data and presents it to you.

Note the following about the Acquisition Unit instance:

- The Acquisition Unit runs on a t3.xlarge instance with a 100 GB GP2 volume.
- The instance is named *AcquisitionUnit* with a generated hash (UUID) concatenated to it. For example: *AcquisitionUnit-FAN7FqeH*
- Only one Acquisition Unit is deployed per Cloud Manager system.
- The instance must be running to access performance information in the Monitoring tab.

Cloud Insights tenant

Cloud Manager sets up a *tenant* for you when you enable Monitoring. A Cloud Insights tenant enables you to access the performance data that the Acquisition Unit collects. The tenant is a secure data partition within the NetApp Cloud Insights service.

Cloud Insights web interface

The Monitoring tab in Cloud Manager provides basic performance data for your volumes. You can go to the Cloud Insights web interface from your browser to perform more in-depth monitoring and to configure alerts for your Cloud Volumes ONTAP systems.

Free trial and subscription

Cloud Manager enables a 30-day free trial of Cloud Insights to provide performance data within Cloud Manager and for you to explore the features that Cloud Insights Standard Edition has to offer.

You need to subscribe by the end of the free trial or your Cloud Insights tenant will eventually be deleted. You can subscribe to either the Basic, Standard, or Premium edition to continue using the Monitoring feature within Cloud Manager.

Learn how to subscribe to Cloud Insights.

Monitoring Cloud Volumes ONTAP in AWS

Complete a few steps to get started monitoring Cloud Volumes ONTAP performance.

Quick start

Get started quickly by following these steps or scroll down to the remaining sections for full details.

Verify support for your configuration

You need a new installation of Cloud Manager 3.8.4 or later in AWS, Cloud Volumes ONTAP in AWS, and

you must be a new Cloud Insights customer.

 **Enable Monitoring on your new or existing system**

- New working environments: Be sure to keep Monitoring enabled when you create the working environment (it's enabled by default).
- Existing working environments: Select a working environment and click **Start Monitoring**.

 **View performance data**

Click **Monitoring** and view performance data for your volumes.

 **Subscribe to Cloud Insights**

Subscribe before your 30-day free trial ends to continue seeing performance data within Cloud Manager and Cloud Insights. Learn how to subscribe.

Requirements

Read the following requirements to make sure that you have a supported configuration.

Supported Cloud Manager versions

You need a new installation of Cloud Manager 3.8.4 or later. A new installation is needed because a new infrastructure is required to enable the Monitoring service. This infrastructure is available starting with new installations of Cloud Manager 3.8.4.

Supported Cloud Volumes ONTAP versions

Any version of Cloud Volumes ONTAP in AWS.

Cloud Insights requirement

You must be a new Cloud Insights customer. Monitoring isn't supported if you already have a Cloud Insights tenant.

Email address for Cloud Central

The email address for your Cloud Central user account should be your business email address. Free email domains like gmail and hotmail aren't supported when creating a Cloud Insights tenant.

Networking for the Acquisition Unit

The Acquisition Unit uses 2-way/mutual authentication to connect to the Cloud Insights server. The client certificate must be passed to the Cloud Insights server to be authenticated. To accomplish this, the proxy must be set up to forward the http request to the Cloud Insights server without decrypting the data.

The Acquisition Unit uses the following two endpoints to communicate with Cloud Insights. If you have a firewall between the Acquisition Unit server and Cloud Insights, you need these endpoints when configuring firewall rules:

```
https://aulogin.<Cloud Insights Domain>
https://<your-tenant-ID>.<Cloud Insights Domain>
```

For example:

```
https://aulogin.c01.cloudinsights.netapp.com
https://cg0c586a-ee05-45rb-a5ac-333b5ae7718d7.c01.cloudinsights.netapp.com
```

Contact us through the in-product chat if you need help identifying your Cloud Insights domain and tenant ID.

Networking for Cloud Manager

Similar to the Acquisition Unit, Cloud Manager must have outbound connectivity to the Cloud Insights tenant. But the endpoint that Cloud Manager contacts is slightly different. It contacts the tenant host URL using the shortened tenant ID:

```
https://<your-short-tenant-ID>.<Cloud Insights Domain>
```

For example:

```
https://abcd12345.c01.cloudinsights.netapp.com
```

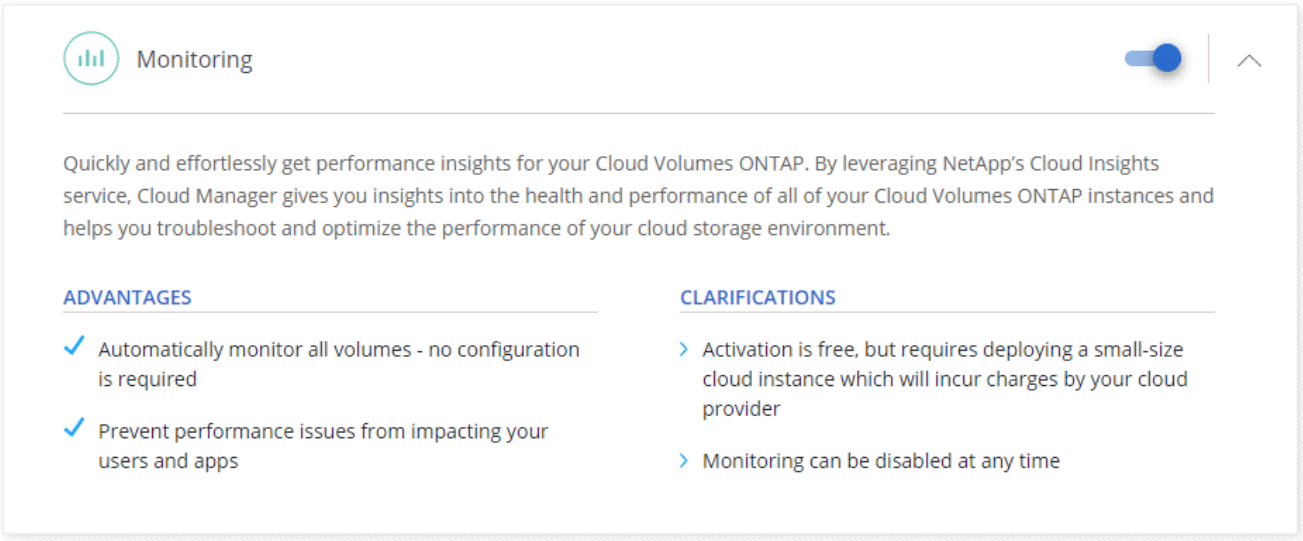
Again, you can contact us through the in-product chat if you need help identifying the tenant host URL.

Enabling monitoring on a new system

The Monitoring service is enabled by default in the working environment wizard. Be sure to keep the option enabled.

Steps

1. Click **Create Cloud Volumes ONTAP**.
2. Select Amazon Web Services as the cloud provider and then choose a single node or HA system.
3. Fill out the Details & Credentials page.
4. On the Services page, leave the service enabled and click **Continue**.

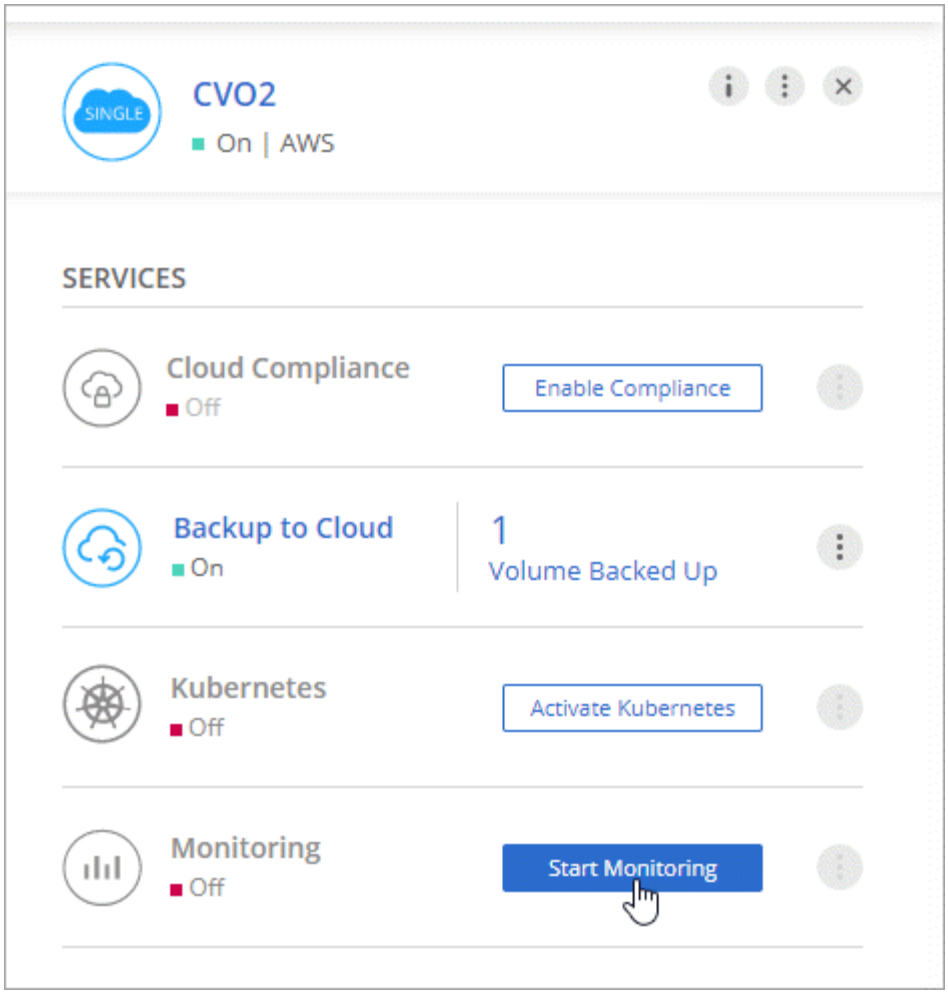


Enabling monitoring on an existing system

Enable monitoring at any time from the working environment.

Steps

1. At the top of Cloud Manager, click **Working Environments**.
2. Select a working environment.
3. In the pane on the right, click **Start Monitoring**.



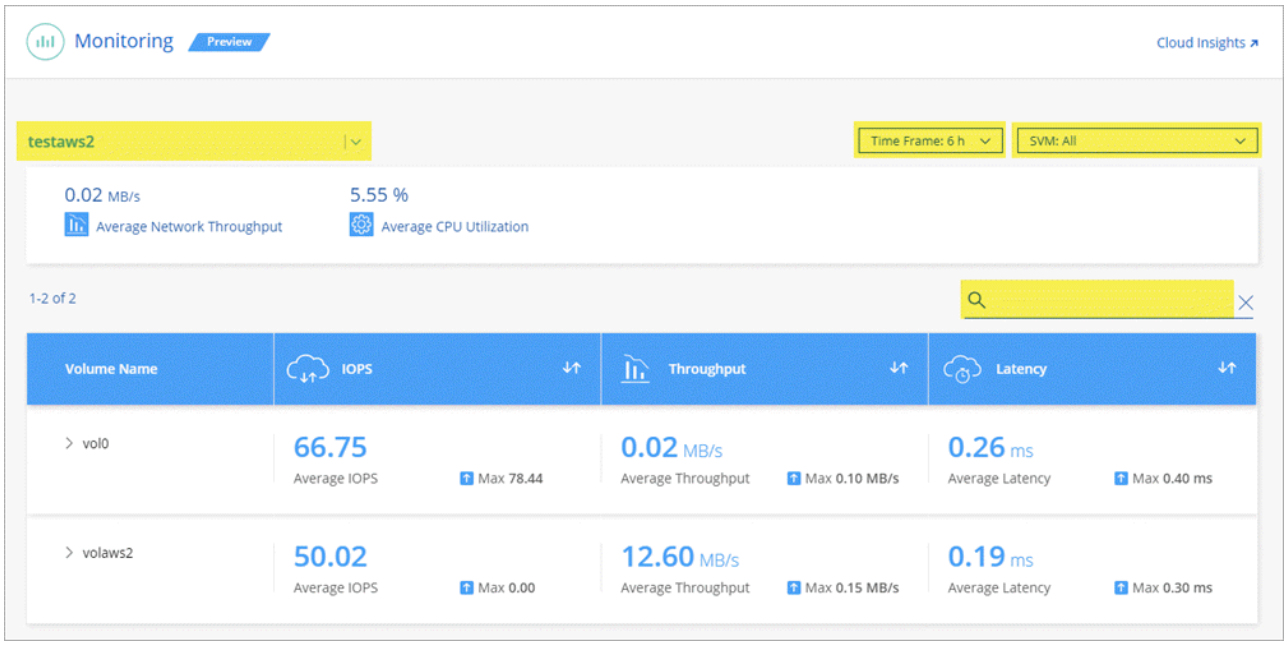
Monitoring your volumes

Monitor performance by viewing IOPS, throughput, and latency for each of your volumes.

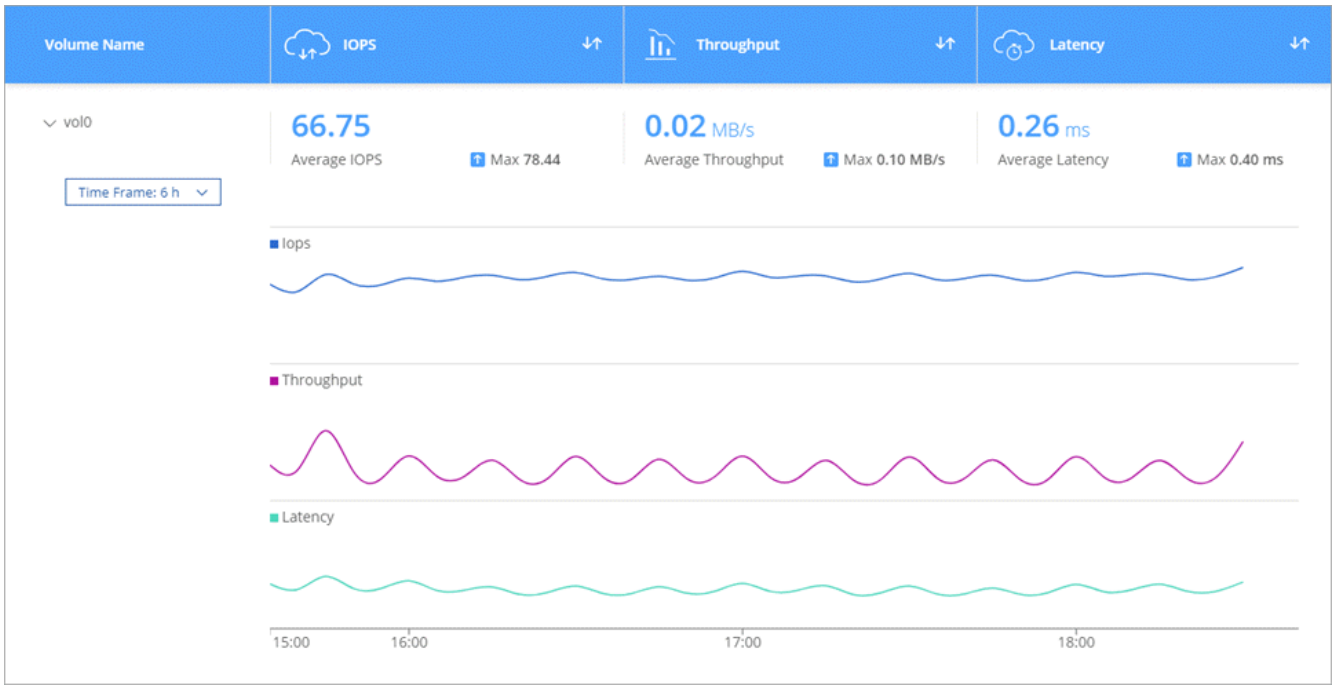
Steps

1. At the top of Cloud Manager, click **Monitoring**.
2. Filter the contents of the dashboard to get the information that you need.
    - Select a specific working environment.
    - Select a different timeframe.
    - Select a specific SVM.
    - Search for a specific volume.

    The following image highlights each of these options:



3. Click a volume in the table to expand the row and view a timeline for IOPS, throughput, and latency.



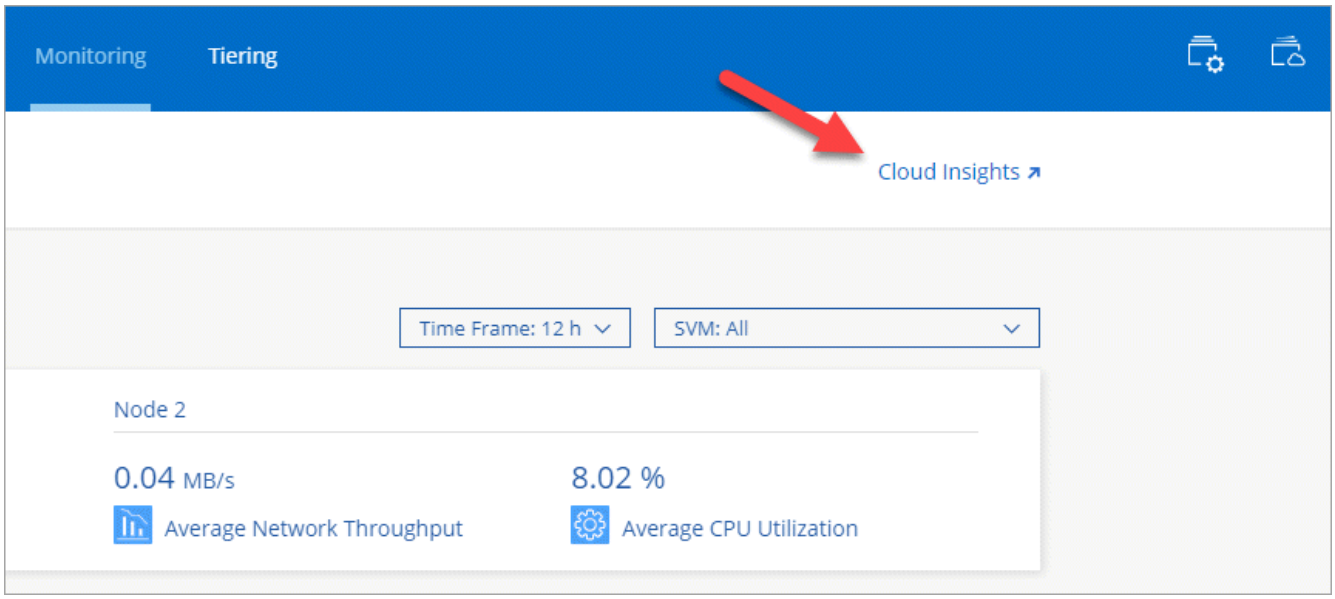
4. Use the data to identify performance issues to minimize impact on your users and apps.

Getting more information from Cloud Insights

The Monitoring tab in Cloud Manager provides basic performance data for your volumes. You can go to the Cloud Insights web interface from your browser to perform more in-depth monitoring and to configure alerts for your Cloud Volumes ONTAP systems.

Steps

1. At the top of Cloud Manager, click **Monitoring**.
2. Click the **Cloud Insights** link.



Result

Cloud Insights open in a new browser tab. If you need help, refer to the Cloud Insights documentation.

Disabling monitoring

If you no longer want to monitor Cloud Volumes ONTAP, you can disable the service at any time.

> If you disable monitoring from each of your working environments, you'll need to delete the EC2 instance yourself. The instance is named *AcquisitionUnit* with a generated hash (UUID) concatenated to it. For example: *AcquisitionUnit-FAN7FqeH*

Steps

1. At the top of Cloud Manager, click **Working Environments**.
2. Select a working environment.
3. In the pane on the right, click the icon and select **Deactivate Scan**.

Administer Cloud Volumes ONTAP

Connecting to Cloud Volumes ONTAP

If you need to perform advanced management of Cloud Volumes ONTAP, you can do so using OnCommand System Manager or the command line interface.

Connecting to OnCommand System Manager

You might need to perform some Cloud Volumes ONTAP tasks from OnCommand System Manager, which is a browser-based management tool that runs on the Cloud Volumes ONTAP system. For example, you need to use System Manager if you want to create LUNs.

Before you begin

The computer from which you are accessing Cloud Manager must have a network connection to Cloud Volumes ONTAP. For example, you might need to log in to Cloud Manager from a jump host in AWS or Azure.

When deployed in multiple AWS Availability Zones, Cloud Volumes ONTAP HA configurations use a floating IP address for the cluster management interface, which means external routing is not available. You must connect from a host that is part of the same routing domain.

Steps

1. From the Working Environments page, double-click the Cloud Volumes ONTAP system that you want to manage with System Manager.
2. Click the menu icon, and then click **Advanced** > **System Manager**.
3. Click **Launch**.

   System Manager loads in a new browser tab.

4. At the login screen, enter **admin** in the User Name field, enter the password that you specified when you created the working environment, and then click **Sign In**.

Result

The System Manager console loads. You can now use it to manage Cloud Volumes ONTAP.

Connecting to the Cloud Volumes ONTAP CLI

The Cloud Volumes ONTAP CLI enables you to execute all administrative commands and is a good choice for advanced tasks or if you are more comfortable using the CLI. You can connect to the CLI using Secure Shell (SSH).

Before you begin

The host from which you use SSH to connect to Cloud Volumes ONTAP must have a network connection to Cloud Volumes ONTAP. For example, you might need to use SSH from a jump host in AWS or Azure.

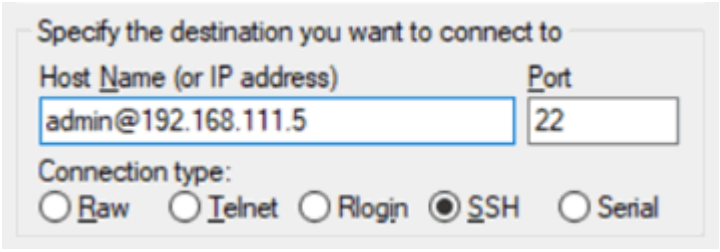
When deployed in multiple AZs, Cloud Volumes ONTAP HA configurations use a floating IP address for the cluster management interface, which means external routing is not available. You must connect from a host that is part of the same routing domain.

Steps

1. In Cloud Manager, identify the IP address of the cluster management interface:
   a. On the Working Environments page, select the Cloud Volumes ONTAP system.
   b. Copy the cluster management IP address that appears in the right pane.
2. Use SSH to connect to the cluster management interface IP address using the admin account.

   Example

   The following image shows an example using PuTTY:



3. At the login prompt, enter the password for the admin account.

   Example

```
Password: ********
COT2::>
```

Updating Cloud Volumes ONTAP software

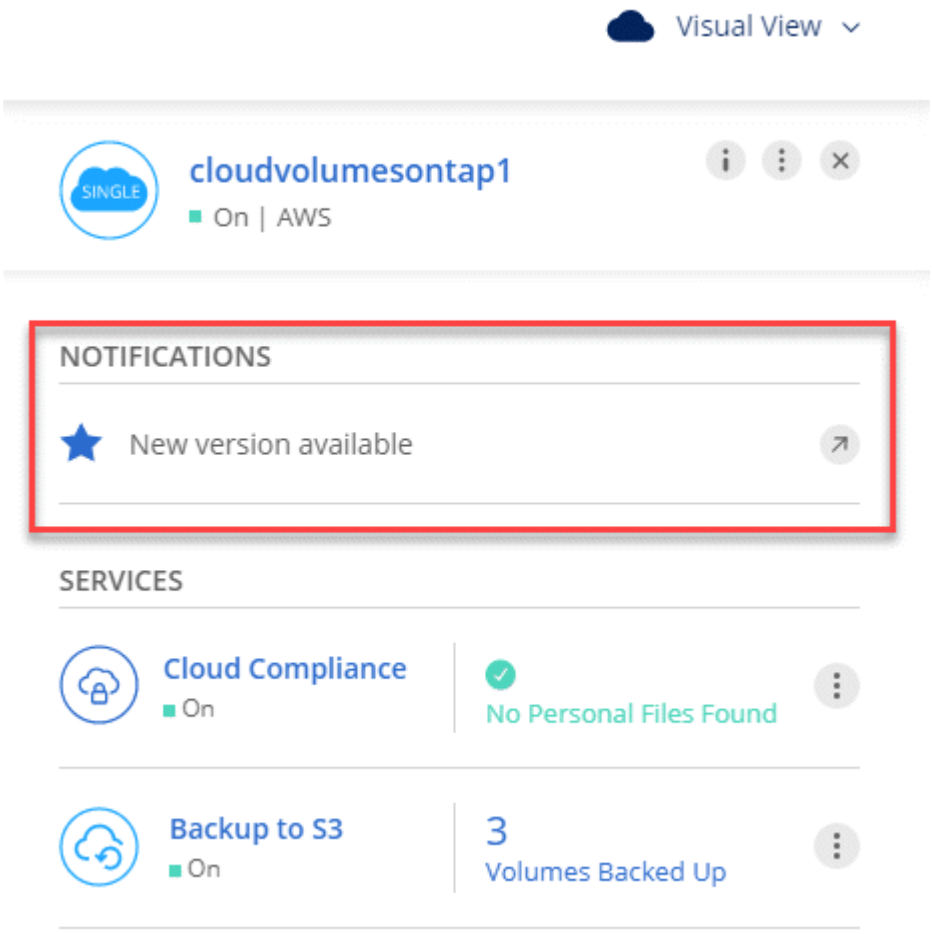
Cloud Manager includes several options that you can use to upgrade to the current Cloud Volumes ONTAP release or to downgrade Cloud Volumes ONTAP to an earlier release. You should prepare Cloud Volumes ONTAP systems before you upgrade or downgrade the software.

Software updates must be completed by Cloud Manager

Upgrades of Cloud Volumes ONTAP must be completed from Cloud Manager. You should not upgrade Cloud Volumes ONTAP by using System Manager or the CLI. Doing so can impact system stability.

Ways to update Cloud Volumes ONTAP

Cloud Manager displays a notification in Cloud Volumes ONTAP working environments when a new version of Cloud Volumes ONTAP is available:



You can start the upgrade process from this notification, which automates the process by obtaining the software image from an S3 bucket, installing the image, and then restarting the system. For details, see Upgrading Cloud Volumes ONTAP from Cloud Manager notifications.

For HA systems in AWS, Cloud Manager might upgrade the HA mediator as part of the upgrade process.

Advanced options for software updates

Cloud Manager also provides the following advanced options for updating Cloud Volumes ONTAP software:

- Software updates using an image on an external URL

  This option is helpful if Cloud Manager cannot access the S3 bucket to upgrade the software, if you were provided with a patch, or if you want to downgrade the software to a specific version.

For details, see Upgrading or downgrading Cloud Volumes ONTAP by using an HTTP or FTP server.

- Software updates using the alternate image on the system

  You can use this option to downgrade to the previous version by making the alternate software image the default image. This option is not available for HA pairs.

  For details, see Downgrading Cloud Volumes ONTAP by using a local image.

Preparing to update Cloud Volumes ONTAP software

Before performing an upgrade or downgrade, you must verify that your systems are ready and make any required configuration changes.

- Planning for downtime
- Reviewing version requirements
- Verifying that automatic giveback is still enabled
- Suspending SnapMirror transfers
- Verifying that aggregates are online

Planning for downtime

When you upgrade a single-node system, the upgrade process takes the system offline for up to 25 minutes, during which I/O is interrupted.

Upgrading an HA pair is nondisruptive and I/O is uninterrupted. During this nondisruptive upgrade process, each node is upgraded in tandem to continue serving I/O to clients.

Reviewing version requirements

The version of ONTAP that you can upgrade or downgrade to varies based on the version of ONTAP currently running on your system.

To understand version requirements, refer to ONTAP 9 Documentation: Cluster update requirements.

Verifying that automatic giveback is still enabled

Automatic giveback must be enabled on a Cloud Volumes ONTAP HA pair (this is the default setting). If it isn't, then the operation will fail.

ONTAP 9 Documentation: Commands for configuring automatic giveback

Suspending SnapMirror transfers

If a Cloud Volumes ONTAP system has active SnapMirror relationships, it is best to suspend transfers before you update the Cloud Volumes ONTAP software. Suspending the transfers prevents SnapMirror

failures. You must suspend the transfers from the destination system.

About this task

These steps describe how to use System Manager for version 9.3 and later.

Steps

1. Log in to System Manager from the destination system.
2. Click **Protection** > **Relationships**.
3. Select the relationship and click **Operations** > **Quiesce**.

Verifying that aggregates are online

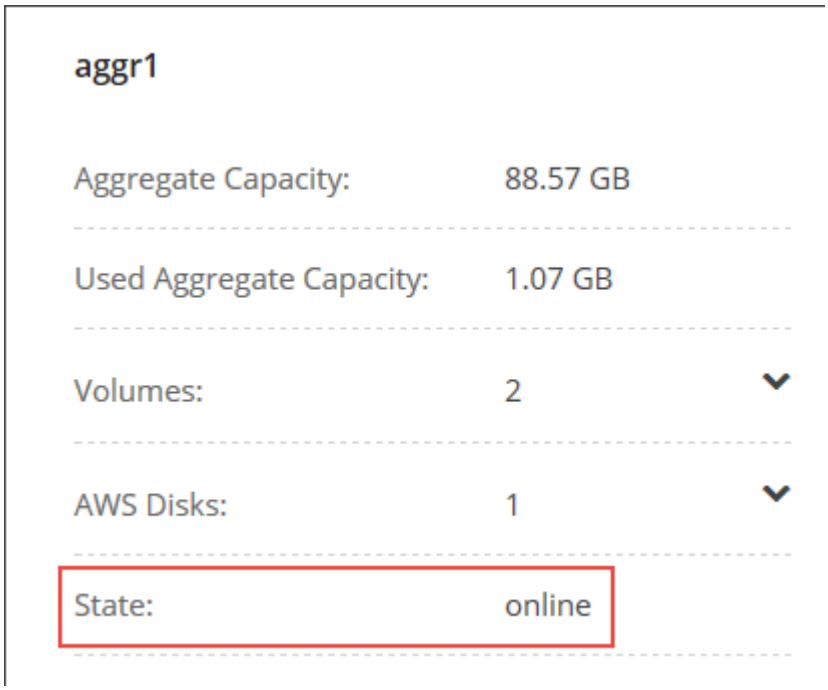
Aggregates for Cloud Volumes ONTAP must be online before you update the software. Aggregates should be online in most configurations, but if they are not, then you should bring them online.

About this task

These steps describe how to use System Manager for version 9.3 and later.

Steps

1. In the working environment, click the menu icon, and then click **Advanced** > **Advanced allocation**.
2. Select an aggregate, click **Info**, and then verify that the state is online.



3. If the aggregate is offline, use System Manager to bring the aggregate online:
   a. Log in to System Manager.
   b. Click **Storage** > **Aggregates & Disks** > **Aggregates**.

c. Select the aggregate, and then click **More Actions** > **Status** > **Online**.

Upgrading Cloud Volumes ONTAP from Cloud Manager notifications

Cloud Manager notifies you when a new version of Cloud Volumes ONTAP is available. Click the notification to start the upgrade process.

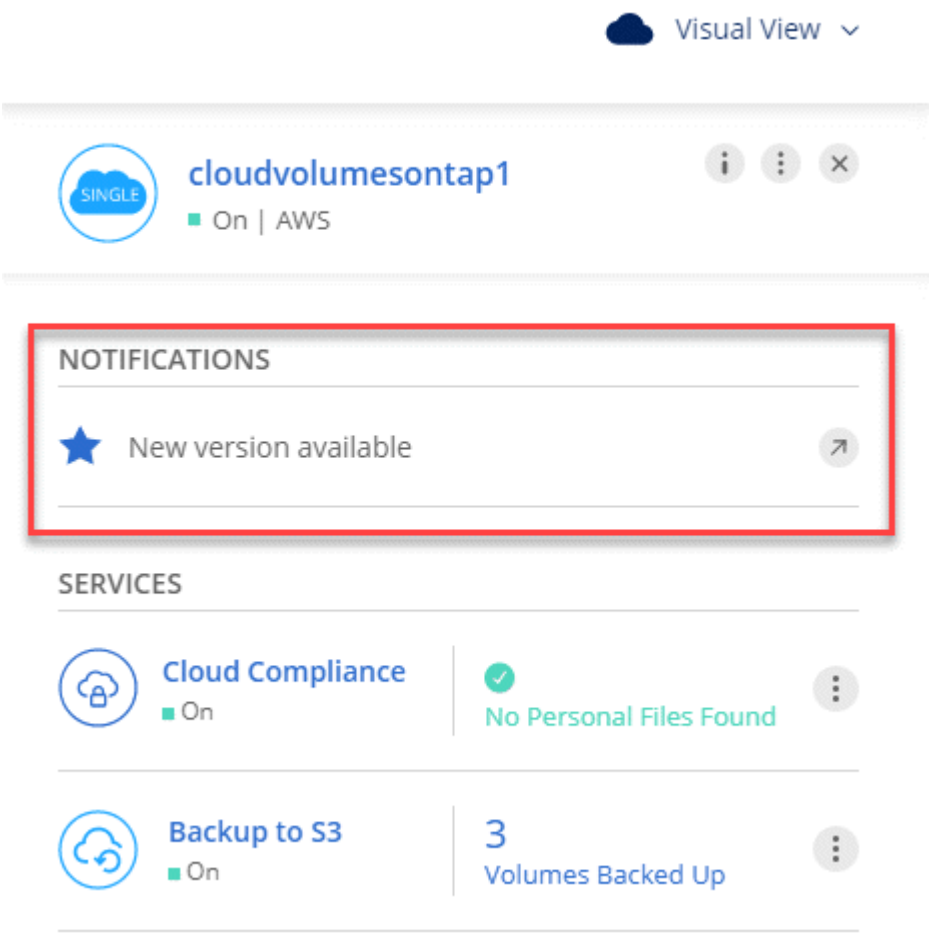
Before you begin

Cloud Manager operations such as volume or aggregate creation must not be in progress for the Cloud Volumes ONTAP system.

Steps

1. Click **Working Environments**.
2. Select a working environment.

   A notification appears in the right pane if a new version is available:



3. If a new version is available, click **Upgrade**.
4. In the Release Information page, click the link to read the Release Notes for the specified version, and then select the **I have read...** check box.

5. In the End User License Agreement (EULA) page, read the EULA, and then select **I read and approve the EULA**.
6. In the Review and Approve page, read the important notes, select **I understand...**, and then click **Go**.

Result

Cloud Manager starts the software upgrade. You can perform actions on the working environment once the software update is complete.

After you finish

If you suspended SnapMirror transfers, use System Manager to resume the transfers.

Upgrading or downgrading Cloud Volumes ONTAP by using an HTTP or FTP server

You can place the Cloud Volumes ONTAP software image on an HTTP or FTP server and then initiate the software update from Cloud Manager. You might use this option if Cloud Manager cannot access the S3 bucket to upgrade the software or if you want to downgrade the software.

Steps

1. Set up an HTTP server or FTP server that can host the Cloud Volumes ONTAP software image.
2. If you have a VPN connection to the virtual network, you can place the Cloud Volumes ONTAP software image on an HTTP server or FTP server in your own network. Otherwise, you must place the file on an HTTP server or FTP server in the cloud.
3. If you use your own security group for Cloud Volumes ONTAP, ensure that the outbound rules allow HTTP or FTP connections so Cloud Volumes ONTAP can access the software image.

The predefined Cloud Volumes ONTAP security group allows outbound HTTP and FTP connections by default.

4. Obtain the software image from the NetApp Support Site.
5. Copy the software image to the directory on the HTTP or FTP server from which the file will be served.
6. From the working environment in Cloud Manager, click the menu icon, and then click **Advanced** > **Update Cloud Volumes ONTAP**.
7. On the update software page, choose **Select an image available from a URL**, enter the URL, and then click **Change Image**.
8. Click **Proceed** to confirm.

Result

Cloud Manager starts the software update. You can perform actions on the working environment once the software update is complete.

After you finish

If you suspended SnapMirror transfers, use System Manager to resume the transfers.

Downgrading Cloud Volumes ONTAP by using a local image

Transitioning Cloud Volumes ONTAP to an earlier release in the same release family (for example, 9.5 to 9.4) is referred to as a downgrade. You can downgrade without assistance when downgrading new or test clusters, but you should contact technical support if you want to downgrade a production cluster.

Each Cloud Volumes ONTAP system can hold two software images: the current image that is running, and an alternate image that you can boot. Cloud Manager can change the alternate image to be the default image. You can use this option to downgrade to the previous version of Cloud Volumes ONTAP, if you are experiencing issues with the current image.

About this task

This downgrade process is available for single Cloud Volumes ONTAP systems only. It is not available for HA pairs.

Steps

1. From the working environment, click the menu icon, and then click **Advanced** > **Update Cloud Volumes ONTAP**.
2. On the update software page, select the alternate image, and then click **Change Image**.
3. Click **Proceed** to confirm.

Result

Cloud Manager starts the software update. You can perform actions on the working environment once the software update is complete.

After you finish

If you suspended SnapMirror transfers, use System Manager to resume the transfers.

Modifying Cloud Volumes ONTAP systems

You might need to change the configuration of Cloud Volumes ONTAP instances as your storage needs change. For example, you can change between pay-as-you-go configurations, change the instance or VM type, and move to an alternate subscription.

Installing license files on Cloud Volumes ONTAP BYOL systems

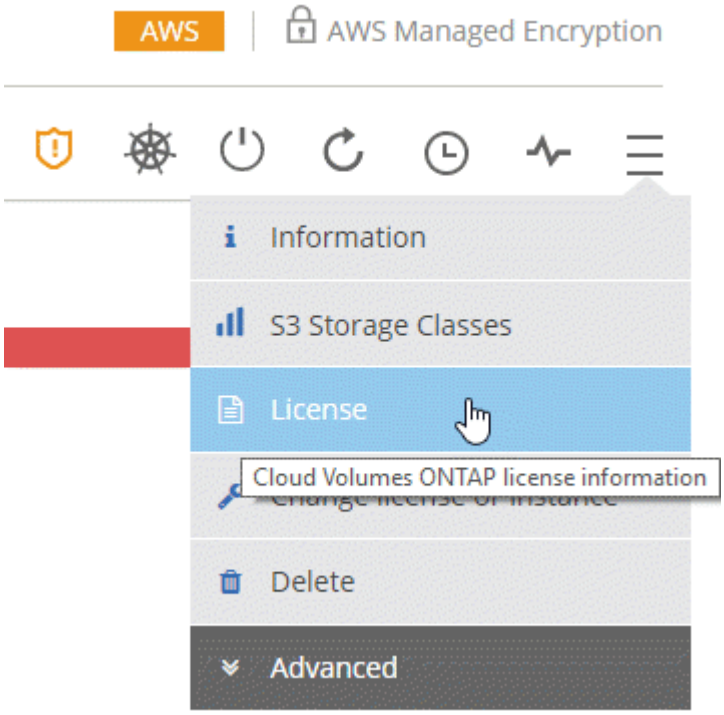
If Cloud Manager cannot obtain a BYOL license file from NetApp, you can obtain the file yourself and then manually upload the file to Cloud Manager so it can install the license on the Cloud Volumes ONTAP system.

Steps

1. Go to the NetApp License File Generator and log in using your NetApp Support Site credentials.
2. Enter your password, choose your product, enter the serial number, confirm that you have read and accepted the privacy policy, and then click **Submit**.

   Example

3. Choose whether you want to receive the serialnumber.NLF JSON file through email or direct download.
4. In Cloud Manager, open the Cloud Volumes ONTAP BYOL working environment.
5. Click the menu icon and then click **License**.



6. Click **Upload License File**.
7. Click **Upload** and then select the file.

Result

Cloud Manager installs the new license file on the Cloud Volumes ONTAP system.

Changing the instance or machine type for Cloud Volumes ONTAP

You can choose from several instance or machine types when you launch Cloud Volumes ONTAP in AWS, Azure, or GCP. You can change the instance or machine type at any time if you determine that it is undersized or oversized for your needs.

About this task

- Automatic giveback must be enabled on a Cloud Volumes ONTAP HA pair (this is the default setting). If it isn't, then the operation will fail.

  ONTAP 9 Documentation: Commands for configuring automatic giveback

- The operation restarts Cloud Volumes ONTAP.

  For single node systems, I/O is interrupted.

  For HA pairs, the change is nondisruptive. HA pairs continue to serve data.

- Changing the instance or machine type affects cloud provider service charges.

Steps

1. From the working environment, click the menu icon, and then click **Change license or instance** for AWS, **Change license or VM** for Azure, or **Change license or machine** for GCP.
2. If you are using a pay-as-you-go configuration, you can optionally choose a different license.
3. Select an instance or machine type, select the check box to confirm that you understand the implications of the change, and then click **OK**.

Result

Cloud Volumes ONTAP reboots with the new configuration.

Changing between pay-as-you-go configurations

After you launch pay-as-you-go Cloud Volumes ONTAP systems, you can change between the Explore, Standard, and Premium configurations at any time by modifying the license. Changing the license increases or decreases the raw capacity limit and enables you to choose from different AWS instance types or Azure virtual machine types.

In GCP, a single machine type is available for each pay-as-you-go configuration. You can't choose between different machine types.

About this task

Note the following about changing between pay-as-you-go licenses:

- The operation restarts Cloud Volumes ONTAP.

  For single node systems, I/O is interrupted.

  For HA pairs, the change is nondisruptive. HA pairs continue to serve data.

- Changing the instance or machine type affects cloud provider service charges.

Steps

1. From the working environment, click the menu icon, and then click **Change license or instance** for AWS, **Change license or VM** for Azure, or **Change license or machine** for GCP.
2. Select a license type and an instance type or machine type, select the check box to confirm that you understand the implications of the change, and then click **OK**.

Result

Cloud Volumes ONTAP reboots with the new license, instance type or machine type, or both.

Moving to an alternate Cloud Volumes ONTAP configuration

If you want to move between a pay-as-you-go subscription and a BYOL subscription or between a single Cloud Volumes ONTAP system and an HA pair, you can deploy a new system and then replicate data from the existing system to the new system.

Steps

1. Create a new Cloud Volumes ONTAP working environment.

   Launching Cloud Volumes ONTAP in AWS
   Launching Cloud Volumes ONTAP in Azure
   Launching Cloud Volumes ONTAP in GCP

2. Set up one-time data replication between the systems for each volume that you must replicate.
3. Terminate the Cloud Volumes ONTAP system that you no longer need by deleting the original working environment.

Changing write speed to normal or high

Cloud Manager enables you to choose a write speed setting for single node Cloud Volumes ONTAP systems. The default write speed is normal. You can change to high write speed if fast write performance is required for your workload. Before you change the write speed, you should understand the differences between the normal and high settings.

About this task

- Ensure that operations such as volume or aggregate creation are not in progress.
- Be aware that this change restarts Cloud Volumes ONTAP, which means I/O is interrupted.

Steps

1. From the working environment, click the menu icon, and then click **Advanced** > **Writing Speed**.
2. Select **Normal** or **High**.

   If you choose High, then you'll need to read the "I understand..." statement and confirm by checking the box.

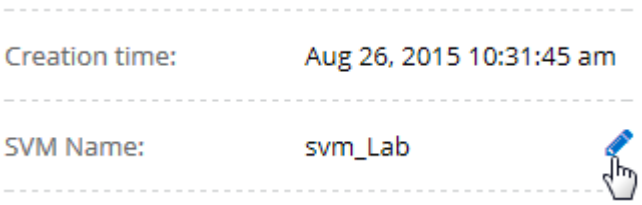
3. Click **Save**, review the confirmation message, and then click **Proceed**.

Modifying the storage virtual machine name

Cloud Manager automatically names the storage virtual machine (SVM) for Cloud Volumes ONTAP. You can modify the name of the SVM if you have strict naming standards. For example, you might want it to match how you name the SVMs for your ONTAP clusters.

Steps

1. From the working environment, click the menu icon, and then click **Information**.
2. Click the edit icon to the right of the SVM name.



3. In the Modify SVM Name dialog box, modify the SVM name, and then click **Save**.

Changing the password for Cloud Volumes ONTAP

Cloud Volumes ONTAP includes a cluster admin account. You can change the password for this account from Cloud Manager, if needed.

You should not change the password for the admin account through System Manager or the CLI. The password will not be reflected in Cloud Manager. As a result, Cloud Manager cannot monitor the instance properly.

Steps

1. From the working environment, click the menu icon, and then click **Advanced** > **Set password**.
2. Enter the new password twice and then click **Save**.

   The new password must be different than one of the last six passwords that you used.

Changing the network MTU for c4.4xlarge and c4.8xlarge instances

By default, Cloud Volumes ONTAP is configured to use 9,000 MTU (also called jumbo frames) when you choose the c4.4xlarge instance or the c4.8xlarge instance in AWS. You can change the network MTU to 1,500 bytes if that is more appropriate for your network configuration.

About this task

A network maximum transmission unit (MTU) of 9,000 bytes can provide the highest maximum network throughput possible for specific configurations.

9,000 MTU is a good choice if clients in the same VPC communicate with the Cloud Volumes ONTAP system and some or all of those clients also support 9,000 MTU. If traffic leaves the VPC, packet

fragmentation can occur, which degrades performance.

A network MTU of 1,500 bytes is a good choice if clients or systems outside of the VPC communicate with the Cloud Volumes ONTAP system.

Steps

1. From the working environment, click the menu icon and then click **Advanced** > **Network Utilization**.
2. Select **Standard** or **Jumbo Frames**.
3. Click **Change**.

Changing route tables associated with HA pairs in multiple AWS AZs

You can modify the AWS route tables that include routes to the floating IP addresses for an HA pair. You might do this if new NFS or CIFS clients need to access an HA pair in AWS.

Steps

1. From the working environment, click the menu icon and then click **Information**.
2. Click **Route Tables**.
3. Modify the list of selected route tables and then click **Save**.

Result

Cloud Manager sends an AWS request to modify the route tables.

Managing the state of Cloud Volumes ONTAP

You can stop and start Cloud Volumes ONTAP from Cloud Manager to manage your cloud compute costs.

Scheduling automatic shutdowns of Cloud Volumes ONTAP

You might want to shut down Cloud Volumes ONTAP during specific time intervals to lower your compute costs. Rather than do this manually, you can configure Cloud Manager to automatically shut down and then restart systems at specific times.

About this task

When you schedule an automatic shutdown of your Cloud Volumes ONTAP system, Cloud Manager postpones the shutdown if an active data transfer is in progress. Cloud Manager shuts down the system after the transfer is complete.

This task schedules automatic shutdowns of both nodes in an HA pair.

Steps

1. From the working environment, click the clock icon:

2. Specify the shutdown schedule:
   a. Choose whether you want to shut down the system every day, every weekday, every weekend, or any combination of the three options.
   b. Specify when you want to turn off the system and for how long you want it turned off.

      Example

      The following image shows a schedule that instructs Cloud Manager to shut down the system every Saturday at 12:00 a.m. for 48 hours. Cloud Manager restarts the system every Monday at 12:00 a.m.

3. Click **Save**.

Result

Cloud Manager saves the schedule. The clock icon changes to indicate that a schedule is set: 

Stopping Cloud Volumes ONTAP

Stopping Cloud Volumes ONTAP saves you from accruing compute costs and creates snapshots of the root and boot disks, which can be helpful for troubleshooting.

About this task

When you stop an HA pair, Cloud Manager shuts down both nodes.

Steps

1. From the working environment, click the **Turn off** icon.

2. Keep the option to create snapshots enabled because the snapshots can enable system recovery.
3. Click **Turn Off**.

It can take up to a few minutes to stop the system. You can restart systems at a later time from the working environment page.

Monitoring AWS resource costs

Cloud Manager enables you to view the resource costs associated with running Cloud Volumes ONTAP in AWS. You can also see how much money you saved by using NetApp features that can reduce storage costs.

About this task

Cloud Manager updates the costs when you refresh the page. You should refer to AWS for final cost details.

Step

1. Verify that Cloud Manager can obtain cost information from AWS:

   a. Ensure that the IAM policy that provides Cloud Manager with permissions includes the following actions:

   ```
   "ce:GetReservationUtilization",
   "ce:GetDimensionValues",
   "ce:GetCostAndUsage",
   "ce:GetTags"
   ```

   These actions are included in the latest Cloud Manager policy. New systems deployed from NetApp Cloud Central automatically include these permissions.

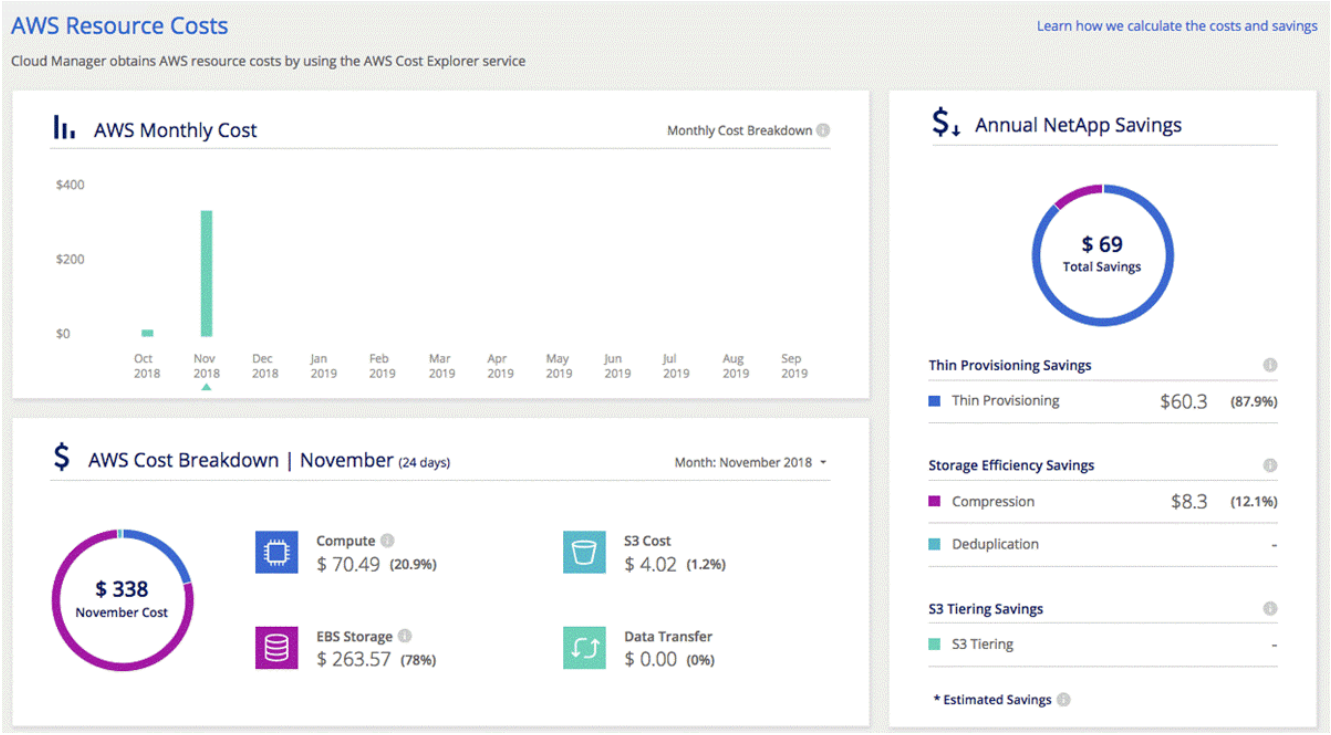
   b. Activate the **WorkingEnvironmentId** tag.

   To track your AWS costs, Cloud Manager assigns a cost allocation tag to Cloud Volumes ONTAP instances. After you create your first working environment, activate the **WorkingEnvironmentId** tag. User-defined tags don't appear on AWS billing reports until you activate them in the Billing and Cost Management console.

2. On the Working Environments page, select a Cloud Volumes ONTAP working environment and then click **Cost**.

   The Cost page displays costs for the current and previous months and shows your annual NetApp savings, if you enabled NetApp's cost-saving features on volumes.

   The following image shows a sample Cost page:

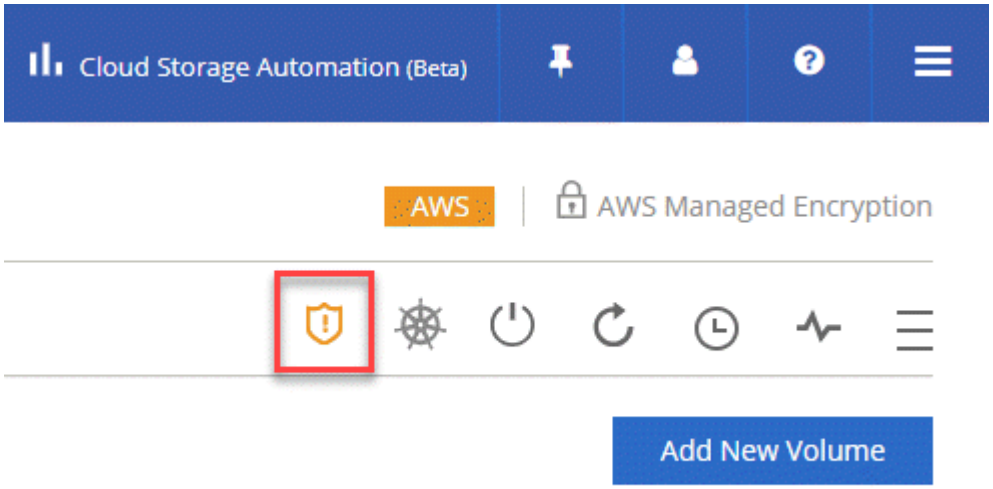


Improving protection against ransomware

Ransomware attacks can cost a business time, resources, and reputation. Cloud Manager enables you to implement the NetApp solution for ransomware, which provides effective tools for visibility, detection, and remediation.

Steps

1. From the working environment, click the **Ransomware** icon.



2. Implement the NetApp solution for ransomware:

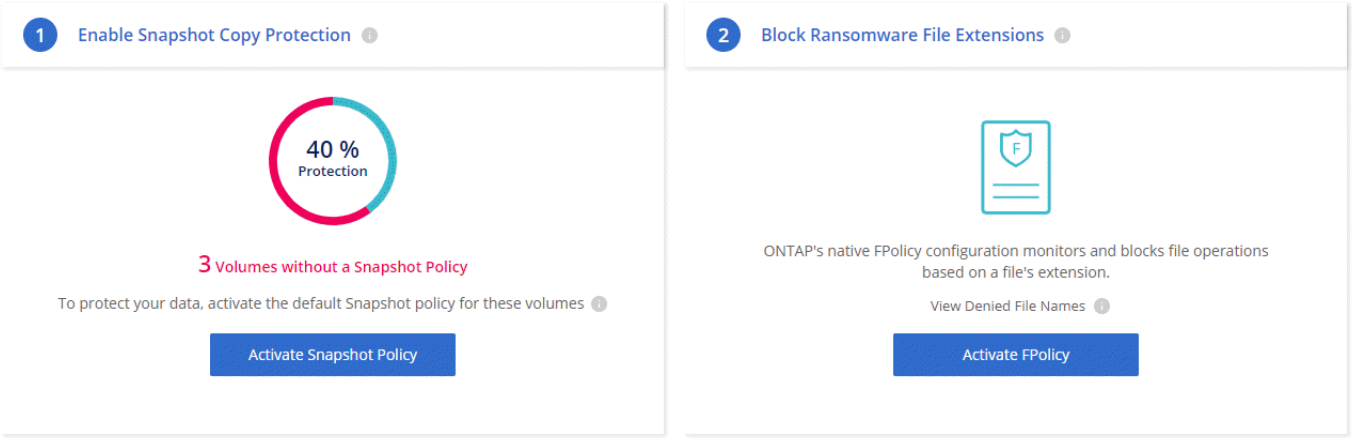
   a. Click **Activate Snapshot Policy**, if you have volumes that do not have a Snapshot policy

enabled.

NetApp Snapshot technology provides the industry's best solution for ransomware remediation. The key to a successful recovery is restoring from uninfected backups. Snapshot copies are read-only, which prevents ransomware corruption. They can also provide the granularity to create images of a single file copy or a complete disaster recovery solution.

b. Click **Activate FPolicy** to enable ONTAP's FPolicy solution, which can block file operations based on a file's extension.

This preventative solution improves protection from ransomware attacks by blocking common ransomware file types.



Adding existing Cloud Volumes ONTAP systems to Cloud Manager

You can discover and add existing Cloud Volumes ONTAP systems to Cloud Manager. You might do this if you deployed a new Cloud Manager system.

Before you begin

You must know the password for the Cloud Volumes ONTAP admin user account.

Steps

1. On the Working Environments page, click **Discover** and select **Cloud Volumes ONTAP**.
2. Select the cloud provider in which the system resides.
3. On the Region page, choose the region where the instances are running, and then select the instances.
4. On the Credentials page, enter the password for the Cloud Volumes ONTAP admin user, and then click **Go**.

Result

Cloud Manager adds the Cloud Volumes ONTAP instances to the workspace.

Deleting a Cloud Volumes ONTAP working environment

It is best to delete Cloud Volumes ONTAP systems from Cloud Manager, rather than from your cloud provider's console. For example, if you terminate a licensed Cloud Volumes ONTAP instance from AWS, then you can't use the license key for another instance. You must delete the working environment from Cloud Manager to release the license.

About this task

When you delete a working environment, Cloud Manager terminates instances, deletes disks, and snapshots.

Cloud Volumes ONTAP instances have termination protection enabled to help prevent accidental termination from AWS. However, if you do terminate a Cloud Volumes ONTAP instance from AWS, you must go to the AWS CloudFormation console and delete the instance's stack. The stack name is the name of the working environment.

Steps

1. From the working environment, click menu icon and then click **Delete**.
2. Type the name of the working environment and then click **Delete**.

   It can take up to 5 minutes to delete the working environment.