



# Concepts

## Cloud Manager 3.4

NetApp  
June 06, 2022

# Table of Contents

- Concepts ..... 1
  - Cloud Manager and ONTAP Cloud overview ..... 1
  - NetApp Cloud Central ..... 2
  - Storage ..... 3
  - Storage management ..... 6
  - High-availability pairs ..... 12
  - Security ..... 17
  - Licensing ..... 20
  - Performance ..... 21
  - Cloud Storage Automation ..... 21

# Concepts

## Cloud Manager and ONTAP Cloud overview

OnCommand Cloud Manager enables you to deploy ONTAP Cloud systems, which provide enterprise-class features for your cloud storage, and to easily replicate data across hybrid clouds built on NetApp.

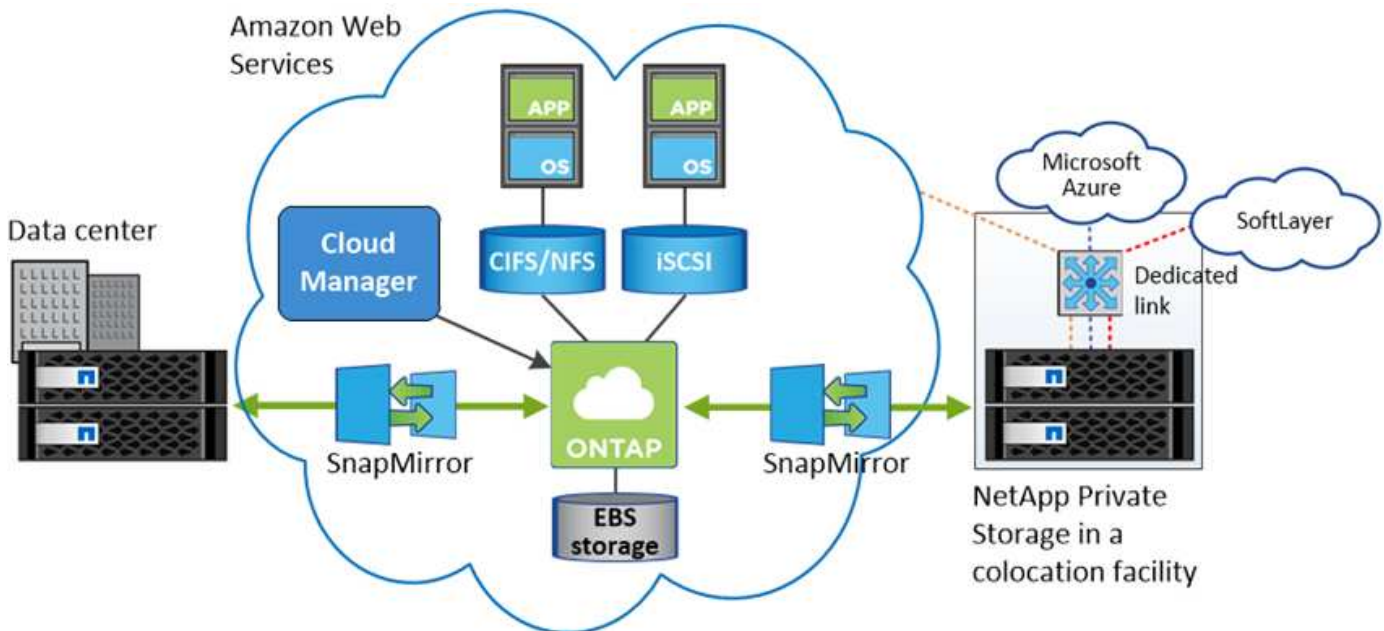
### Cloud Manager

Cloud Manager was built with simplicity in mind. It guides you through ONTAP Cloud setup in a few quick steps, eases data management by offering simplified storage provisioning and automated capacity management, enables drag-and-drop data replication across a hybrid cloud, and more.

Cloud Manager is required to deploy and manage ONTAP Cloud systems, but it can also discover and provision storage for on-premises ONTAP clusters. This provides a central point of control for your cloud and on-premises storage infrastructure.

Cloud Manager also offers insight into your AWS cloud storage. The Cloud Storage Automation feature analyzes your cloud storage to show you savings opportunities, data protection enhancements, and operations that can optimize the cloud storage associated with your AWS account.

You can run Cloud Manager in the cloud or in your network—it just needs a connection to the networks in which you want to deploy ONTAP Cloud systems. The following image shows Cloud Manager running in AWS and managing ONTAP Cloud systems in AWS and Azure. It also shows data replication across a hybrid cloud.



[Learn more about Cloud Manager](#)

### ONTAP Cloud

ONTAP Cloud is a software-only storage appliance that runs the ONTAP data management software in the cloud. You can use ONTAP Cloud for production workloads, disaster recovery, DevOps, file shares, and database management.

ONTAP Cloud extends enterprise storage to the cloud with the following key features:

- **Storage efficiencies**  
Leverage built-in data deduplication, data compression, thin provisioning, and cloning to minimize storage costs.
- **High availability**  
Ensure enterprise reliability and continuous operations in case of failures in your cloud environment (AWS only).
- **Data replication**  
ONTAP Cloud leverages SnapMirror, NetApp's industry-leading replication technology, to replicate on-premises data to the cloud so it's easy to have secondary copies available for multiple use cases.
- **Data tiering**  
Switch between high and low-performance storage pools on-demand without taking applications offline (AWS only).
- **Application consistency**  
Ensure consistency of NetApp Snapshot copies using the NetApp SnapManager tool suite.
- **Data security**  
Secure your data at rest with advanced data encryption (AWS only).



The licenses for these features are included with ONTAP Cloud.

[View supported ONTAP Cloud configurations](#)

[Learn more about ONTAP Cloud](#)

## NetApp Cloud Central

[NetApp Cloud Central](#) provides a centralized location to access and manage NetApp cloud data services. These services enable you to run critical applications in the cloud, create automated DR sites, back up your SaaS data, and effectively migrate and control data across multiple clouds.

Cloud Manager's integration with NetApp Cloud Central provides several benefits, including a simplified deployment experience, a single location to view and manage multiple Cloud Manager systems, and centralized user authentication.

With centralized user authentication, you can use the same set of credentials across Cloud Manager systems and between Cloud Manager and other data services, such as Cloud Sync. It's also easy to reset your password if you forgot it.

The following video provides an overview of NetApp Cloud Central:



Hi Kevin Hill, let's get started!



ONTAP Cloud

Loading...

[More Info](#)



Cloud Sync

Loading...

[More Info](#)



Cloud Control

[Go to Cloud Control](#)

[More Info](#)



Azure NFSaaS

[Register for Preview](#)

[More Info](#)



NFS Hybrid For AWS

[Register for Preview](#)

[More Info](#)

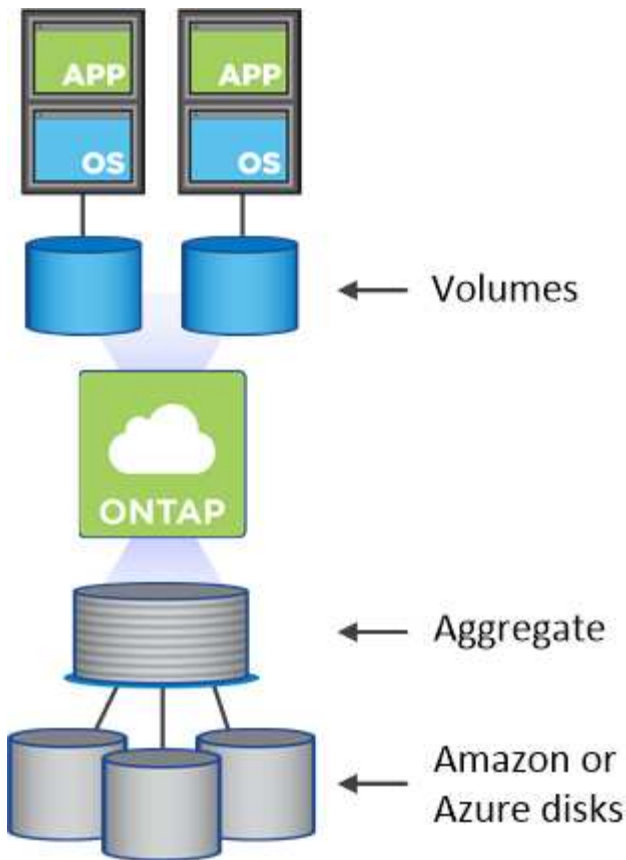
API

## Storage

Understanding how ONTAP Cloud uses cloud storage can help you understand your storage costs.

### How ONTAP Cloud uses cloud storage

ONTAP Cloud uses AWS and Azure volumes as back-end storage. It sees these volumes as disks and groups them into one or more aggregates. Aggregates provide storage to one or more ONTAP Cloud volumes.



In AWS, an aggregate can contain up to 6 disks, with a maximum disk size of 16 TB. The underlying disk type can be a single EBS storage type or a tiered storage configuration that includes an EBS performance tier and an S3 capacity tier.

In Azure, an aggregate can contain up to 12 disks, with a maximum disk size of 4 TB. The underlying Azure managed disk type can be either Standard Storage (HDD) or Premium Storage (SSD).

You choose the disk type and the default disk size when you deploy an ONTAP Cloud system. For more details, refer to the following:

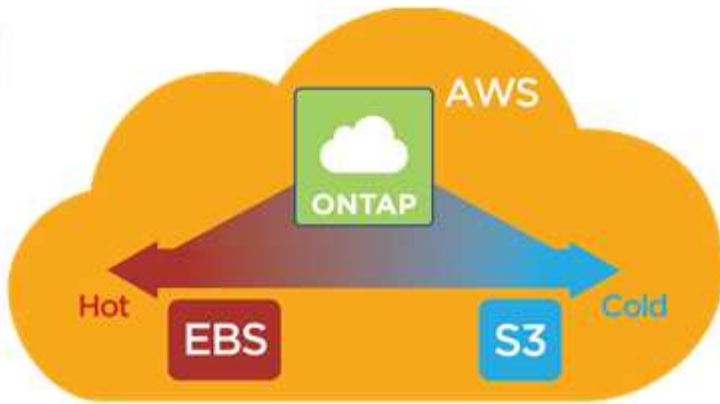
- [Choosing an AWS disk type](#)
- [Choosing an Azure disk type](#)
- [Choosing a disk size](#)



The total amount of storage purchased from AWS or Azure is the *raw capacity*. The *usable capacity* is less because approximately 12 to 14 percent is overhead that is reserved for ONTAP Cloud use. For example, if Cloud Manager creates a 500 GB aggregate, the usable capacity is 442.94 GB.

## Data tiering in AWS

With ONTAP Cloud for AWS, you can reduce storage costs by using EBS as a performance tier for "hot" data and AWS S3 as a capacity tier for "cold" data.



Tiering data is a good choice if your data changes frequently or if you use ONTAP Cloud for disaster recovery or long-term retention:

- After an aggregate has reached 50% capacity, ONTAP Cloud tiers Snapshot copies of read-write volumes to cost-effective S3 storage, freeing up the EBS performance tier for "hot" data.
- When you replicate a volume for disaster recovery or long-term retention, data for the destination volume resides in the S3 capacity tier. If you activate the destination volume, the data gradually moves to the EBS performance tier as it is read.

Note the following about the EBS and S3 tiers:

- An ONTAP Cloud system's capacity limit is spread across EBS and S3 storage.
- The EBS tier can be General Purpose SSDs or Throughput Optimized HDDs.
- An ONTAP Cloud working environment uses a single S3 bucket for tiered data. This includes an HA working environment.
- Cloud Manager creates the S3 bucket and names it *fabric-pool-cluster unique identifier*.



You do not need to install a feature license to enable data tiering.

### Setting up a tiered storage configuration

You simply need to create a VPC Endpoint to S3 and then enable S3 tiering when creating a volume. For details, see [Tiering data in AWS](#).

The screenshot shows four storage options in a row: General Purpose SSD (GP2), Throughput Optimized HDD (ST1), Provisioned IOPS SSD (IO1), and Cold HDD (SC1). Below these, a red box highlights the 'S3 Tying' section, which includes a checked checkbox labeled 'Use S3 as a capacity tier for cold data.'

# Storage management

Cloud Manager provides simplified and advanced management of ONTAP Cloud storage.

## Storage provisioning

Cloud Manager makes storage provisioning for ONTAP Cloud easy by purchasing disks and managing aggregates for you. You simply need to create volumes. You can use an advanced allocation option to provision aggregates yourself, if desired.

### Simplified provisioning

Aggregates provide cloud storage to ONTAP Cloud volumes. Cloud Manager creates aggregates for you when you launch an instance, and when you provision additional volumes.

When you create a volume, Cloud Manager does one of three things:

- It places the volume on an existing aggregate that has sufficient free space.
- It places the volume on an existing aggregate by purchasing more disks for that aggregate.
- It purchases disks for a new aggregate and places the volume on that aggregate.

Cloud Manager determines where to place a new volume by looking at several factors: an aggregate's maximum size, whether thin provisioning is enabled, and free space thresholds for aggregates.



The Cloud Manager Admin can modify free space thresholds from the **Settings** page.

### Disk size selection for aggregates in AWS

When Cloud Manager creates new aggregates for ONTAP Cloud systems in AWS, it gradually increases the disk size in an aggregate, as the number of aggregates in the system increases. Cloud Manager does this to ensure that you can utilize the system's maximum capacity before it reaches the maximum number of data disks allowed by AWS.

For example, Cloud Manager might choose the following disk sizes for aggregates in an ONTAP Cloud Premium or BYOL system:

Aggregate number	Disk size	Max aggregate capacity
1	500 MB	3 TB
4	1 TB	6 TB
6	2 TB	12 TB

You can choose the disk size yourself by using the advanced allocation option.

### Advanced allocation

Rather than let Cloud Manager manage aggregates for you, you can do it yourself. From the **Advanced allocation** page, you can create new aggregates that include a specific number of disks, add disks to an existing aggregate, and create volumes in specific aggregates.



## Capacity management

The Cloud Manager Admin can choose whether Cloud Manager notifies you of storage capacity decisions or whether Cloud Manager automatically manages capacity requirements for you. It might help for you to understand how these modes work.

### Automatic capacity management

If the Cloud Manager Admin set the Capacity Management Mode to automatic, Cloud Manager automatically purchases new disks for ONTAP Cloud instances when more capacity is needed, deletes unused collections of disks (aggregates), and moves volumes between aggregates, as needed.

The following examples illustrate how this mode works:

- If an aggregate with 5 or fewer EBS disks reaches the capacity threshold, Cloud Manager automatically purchases new disks for that aggregate so volumes can continue to grow.
- If an aggregate with 12 Azure disks reaches the capacity threshold, Cloud Manager automatically moves a volume from that aggregate to an aggregate with available capacity or to a new aggregate.

Note that free space is now available on the original aggregate. Existing volumes or new volumes can use that space. The space cannot be returned to AWS or Azure in this scenario.

- If an aggregate contains no volumes for more than 12 hours, Cloud Manager deletes it.

### Manual capacity management

If the Cloud Manager Admin set the Capacity Management Mode to manual, Cloud Manager displays Action Required messages when capacity decisions must be made. The same examples described in the automatic mode apply to the manual mode, but it is up to you to accept the actions.

## Storage isolation using tenants

Cloud Manager enables you to provision and manage storage in isolated groups called tenants. You need to decide how to organize Cloud Manager users and their working environments across tenants.

### Working environments

Cloud Manager represents storage systems as *working environments*. A working environment is any of the following:


- A single ONTAP Cloud system or an HA pair
- An on-premises ONTAP cluster in your network
- An ONTAP cluster in a NetApp Private Storage configuration

The following image shows an ONTAP Cloud working environment:

Volumes

Search [Add New Volume]

2 Volumes | 0.59 TB Allocated | <0.01 TB Used (0 TB in S3)


vol1
■ ONLINE

---


GP2 Tier	150 GB Allocated Capacity	252 KB EBS Used Capacity
-------------	------------------------------	-----------------------------


**Tenants**


A *tenant* isolates working environments in groups. You create one or more working environments within a tenant. The following image shows three tenants defined in Cloud Manager:

**Engineering**

---


  
1 Regions


  
1 WE


  
1 GB

**Finance**

---


  
1 Regions


  
3 WE


  
2 TB

**IT**

---

  
1 Regions

  
1 WE

  
942 GB

**User management of tenants and working environments**

The tenants and working environments that Cloud Manager users can manage depend on user role and assignments. The three distinct user roles are as follows:

**Cloud Manager Admin**

Administers the product and can access all tenants and working environments.

**Tenant Admin**

Administers a single tenant. Can create and manage all working environments and users in the tenant.

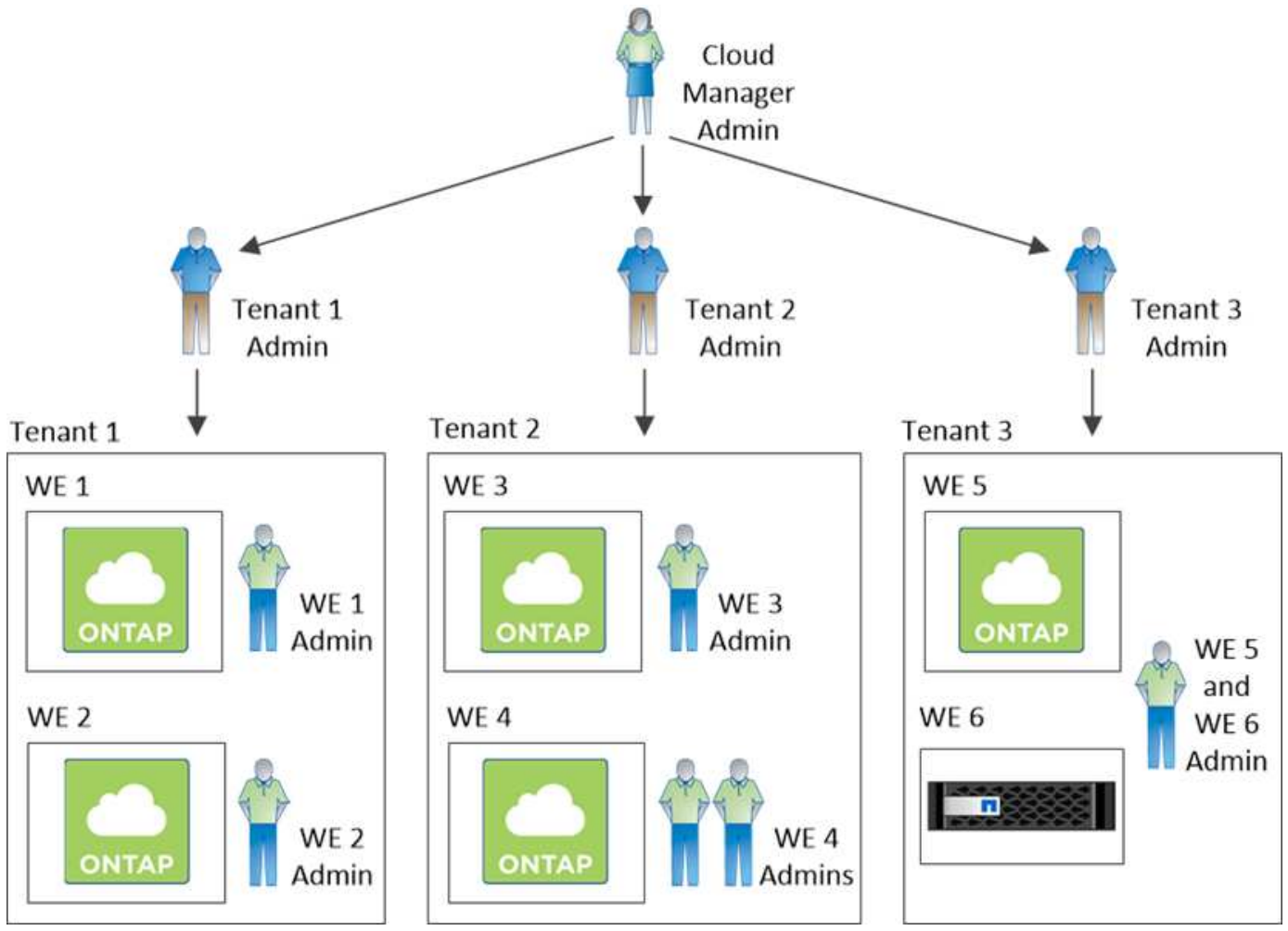
**Working Environment Admin**

Can create and manage one or more working environments in a tenant.

**Example of how you can create tenants and users**

If your organization has departments that operate independently, it is best to have a tenant for each department.

For example, you might create three tenants for three separate departments. You would then create a Tenant Admin for each tenant. Within each tenant would be one or more Working Environment Admins who manage working environments. The following image depicts this scenario:



### Why you should link a tenant to your NetApp Support Site account

Cloud Manager prompts you to enter NetApp Support Site credentials for a tenant because it uses the credentials to manage licenses for ONTAP Cloud BYOL systems, to register pay-as-you-go instances for support, and to upgrade ONTAP Cloud software.

#### License management for BYOL systems

Linking a tenant to your NetApp Support Site account is required if you plan to launch BYOL instances in a tenant. Cloud Manager uses your account to obtain license files from NetApp and installs them on ONTAP Cloud BYOL systems. The NetApp Support Site account must be authorized to access the serial numbers of the ONTAP Cloud BYOL systems in the tenant.

#### Support registration for pay-as-you-go instances

While entering an account is not required to launch pay-as-you-go instances, it is highly recommended because Cloud Manager automatically registers new pay-as-you-go instances for support.

## Software upgrades

Entering a NetApp Support Site account also enables ONTAP Cloud software upgrades directly from Cloud Manager for both pay-as-you-go and BYOL instances.

## NetApp Support Site account requirements

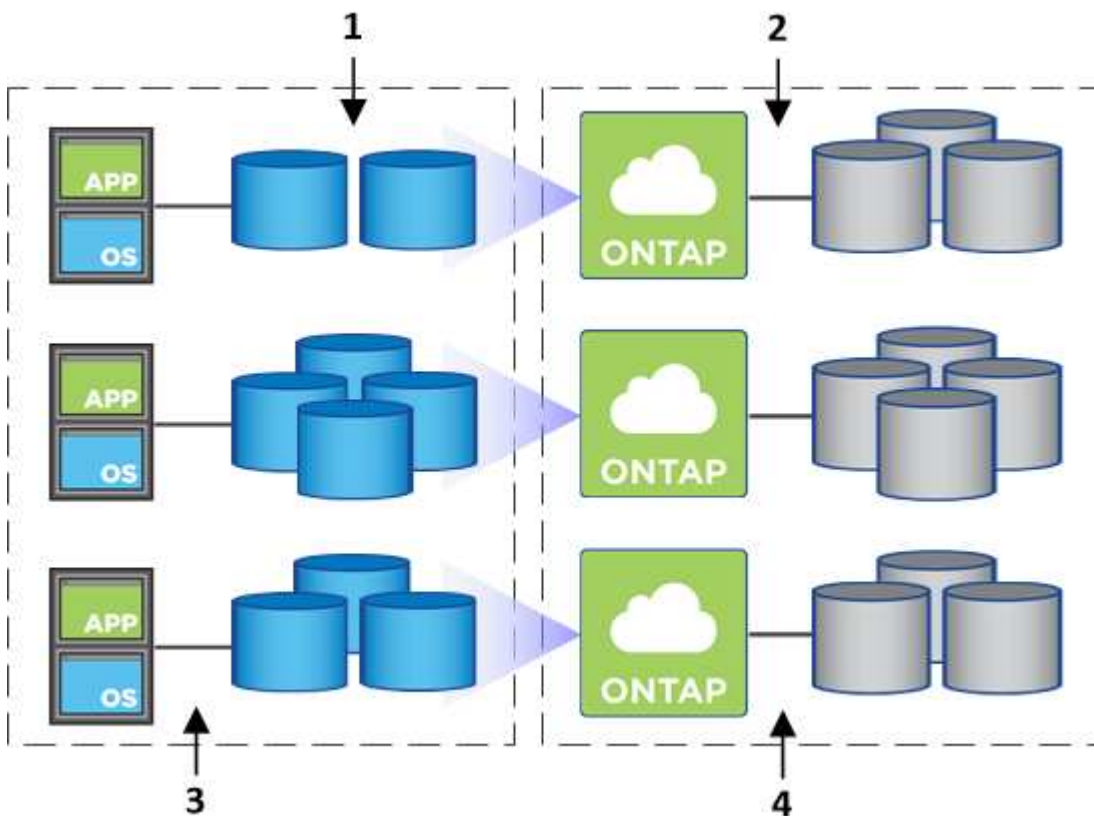
Each NetApp Support Site account that you link to a tenant must be a NetApp customer-level account (not a guest or temp account). For the AWS GovCloud (US) region, the NetApp Support Site account must be a secure account. If you do not have an account, you can create one from the [NetApp Support Site](#).

## Simplified storage management using the Volume View

Cloud Manager provides a separate management view called the *Volume View*, which further simplifies storage management in AWS.

The Volume View enables you to simply specify the NFS volumes that you need in AWS and then Cloud Manager handles the rest: it deploys ONTAP Cloud systems as needed and it makes capacity allocation decisions as volumes grow. This view gives you the benefits of enterprise-class storage in the cloud with very little storage management.

The following image shows how you interact with Cloud Manager in the Volume View:

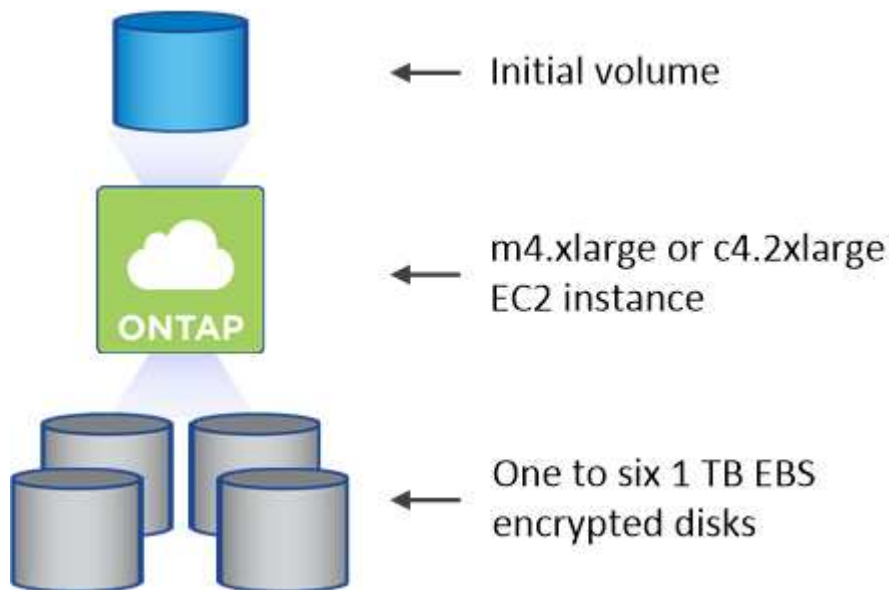


1. You create NFS volumes.
2. Cloud Manager launches ONTAP Cloud instances in AWS for new volumes or it creates volumes on existing instances. It also purchases physical EBS storage for the volumes.
3. You make the volumes available to your hosts and applications.
4. Cloud Manager makes capacity allocation decisions as your volumes grow.

This means that you simply need to interact with volumes (the image on the left), while Cloud Manager interacts with the storage system and its underlying storage (the image on the right).

### Allocation of cloud resources for the initial volume

When you create your first volume, Cloud Manager launches an ONTAP Cloud instance or an ONTAP Cloud HA pair in AWS and purchases Amazon EBS storage for the volume:



The size of the initial volume determines the EC2 instance type and the number of EBS disks.



Cloud Manager launches an ONTAP Cloud Explore or Standard instance, depending on the initial volume size. As the volumes grow, Cloud Manager might prompt you to make an AWS instance change which means it needs to upgrade the instance's license to Standard or Premium. Upgrading increases the EBS raw capacity limit, which allows your volumes to grow.



Cloud Manager does not launch ONTAP Cloud BYOL instances in the Volume View. You should use Cloud Manager in the Storage System View if you purchased an ONTAP Cloud license.

### Allocation of cloud resources for additional volumes

When you create additional volumes, Cloud Manager creates the volumes on existing ONTAP Cloud instances or on new ONTAP Cloud instances. Cloud Manager can create a volume on an existing instance if the instance's AWS location and disk type match the requested volume, and if there is enough space.

### NetApp storage efficiency features and storage costs

Cloud Manager automatically enables NetApp storage efficiency features on all volumes. These efficiencies can reduce the total amount of storage that you need. You might see a difference between your allocated capacity and the purchased AWS capacity, which can result in storage cost savings.

### Capacity allocation decisions that Cloud Manager automatically handles

- Cloud Manager purchases additional EBS disks as capacity thresholds are exceeded. This happens as your volumes grow.

- Cloud Manager deletes unused sets of EBS disks if the disks contain no volumes for 12 hours.
- Cloud Manager moves volumes between sets of disks to avoid capacity issues.

In some cases, this requires purchasing additional EBS disks. It also frees space on the original set of disks for new and existing volumes.

## High-availability pairs

An ONTAP Cloud high availability (HA) configuration provides nondisruptive operations and fault tolerance. HA pairs are supported in AWS only.

### Overview

ONTAP Cloud HA configurations include the following components:

- Two ONTAP Cloud systems (nodes) whose data is synchronously mirrored between each other.
- A mediator instance that provides a communication channel between the nodes to assist in storage takeover and giveback processes.



The mediator instance runs the Linux operating system on a t2.micro instance and uses one EBS magnetic disk that is approximately 8 GB.

### Storage takeover and giveback

If a node goes down, the other node can serve data for its partner to provide continued data service. Clients can access the same data from the partner node because the data was synchronously mirrored to the partner.

After the node reboots, the partner must resync data before it can return the storage. The time that it takes to resync data depends on how much data was changed while the node was down.

### RPO and RTO

An ONTAP Cloud HA configuration maintains high availability of your data as follows:

- The recovery point objective (RPO) is 0 seconds.  
Your data is transactionally consistent with no data loss.
- The recovery time objective (RTO) is 60 seconds.  
In the event of an outage, data should be available in 60 seconds or less.

### HA deployment models

You can ensure the high availability of your data by deploying an ONTAP Cloud HA configuration across multiple Availability Zones (AZs) or in a single AZ. You should review more details about each configuration to choose which best fits your needs.

## ONTAP Cloud HA in multiple Availability Zones

Deploying an ONTAP Cloud HA configuration in multiple Availability Zones (AZs) ensures high availability of your data if a failure occurs with an AZ or an instance that runs an ONTAP Cloud node. You should understand how NAS IP addresses impact data access and storage failover.

## NFS and CIFS data access for clients within the VPC

When an ONTAP Cloud HA configuration is spread across multiple Availability Zones, three floating IP addresses are required for NAS data access from within the VPC. The floating IP addresses, which must be outside of the CIDR blocks for all VPCs in the region, can migrate between nodes when failures occur.

These floating IP addresses are not natively accessible to clients that are outside of the VPC.

You should review requirements for floating IP addresses and route tables before you deploy an HA configuration across multiple Availability Zones. You must specify the floating IP addresses when you deploy the configuration.

For details, see [Networking requirements for ONTAP Cloud HA in multiple AZs](#).

## NFS and CIFS data access for clients outside the VPC

When deployed in multiple AZs, ONTAP Cloud HA includes a separate set of IP addresses for NAS clients that are outside of the VPC. These IP addresses are static—they cannot migrate between nodes.

## iSCSI data access

Cross-VPC data communication is not an issue since iSCSI does not use floating IP addresses.

## Storage takeover and giveback for iSCSI

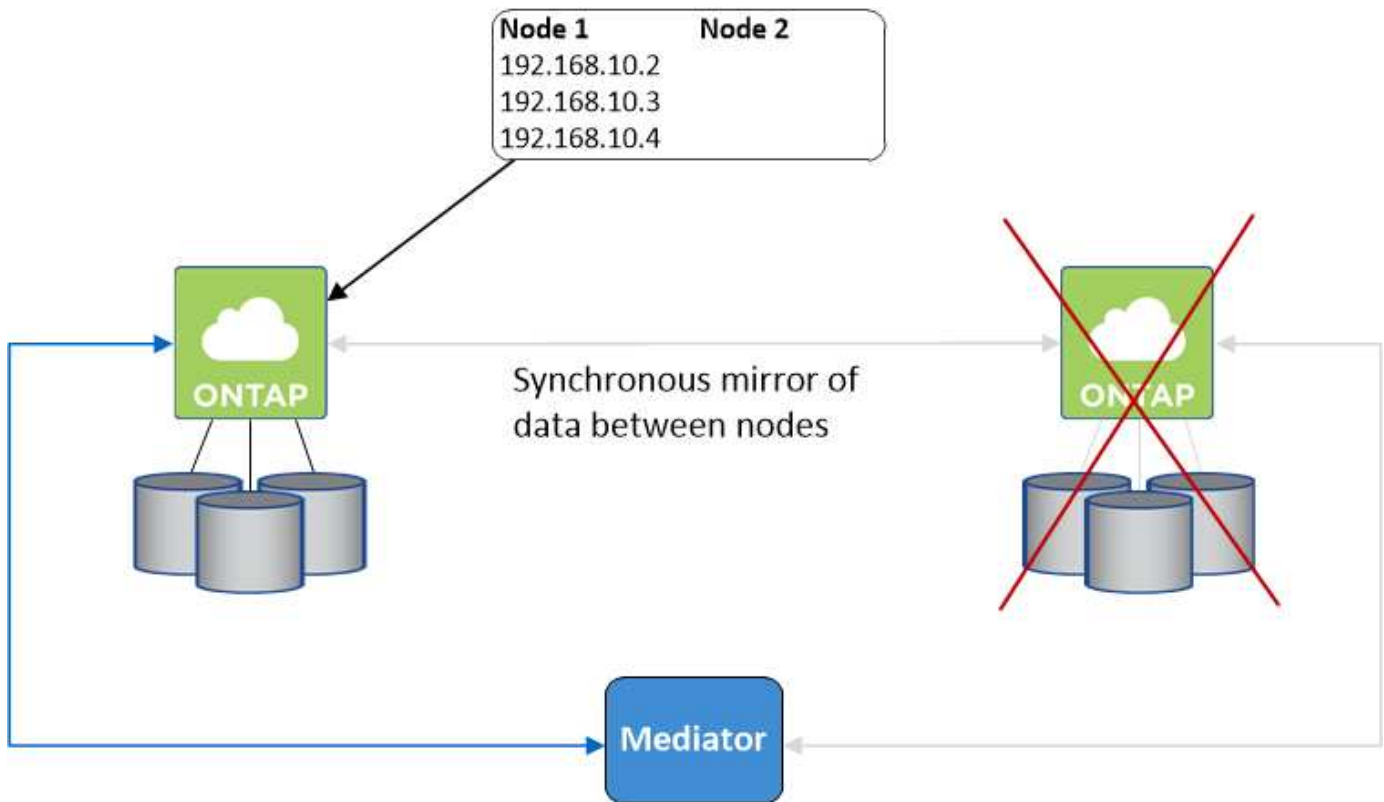
For iSCSI, ONTAP Cloud uses multipath I/O (MPIO) and Asymmetric Logical Unit Access (ALUA) to manage path failover between the active-optimized and non-optimized paths.



For information about which specific host configurations support ALUA, see the [NetApp Interoperability Matrix Tool](#) and the Host Utilities Installation and Setup Guide for your host operating system.

## Storage takeover and giveback for NAS

When takeover occurs in a NAS configuration using floating IPs, the node's floating IP address that clients use to access data moves to the other node. The following image depicts storage takeover in a NAS configuration using floating IPs. If node 2 goes down, the floating IP address for node 2 moves to node 1.



NAS data IPs used for external VPC access cannot migrate between nodes if failures occur. If a node goes offline, you must manually remount volumes to clients outside the VPC by using the IP address on the other node.

After the failed node comes back online, remount clients to volumes using the original IP address. This step is needed to avoid transferring unnecessary data between two HA nodes, which can cause significant performance and stability impact.

You can easily identify the correct IP address from Cloud Manager by selecting the volume and clicking **Mount Command**.

## ONTAP Cloud HA in a single Availability Zone

Deploying an ONTAP Cloud HA configuration in a single Availability Zone (AZ) can ensure high availability of your data if an instance that runs an ONTAP Cloud node fails. All data is natively accessible from outside of the VPC.



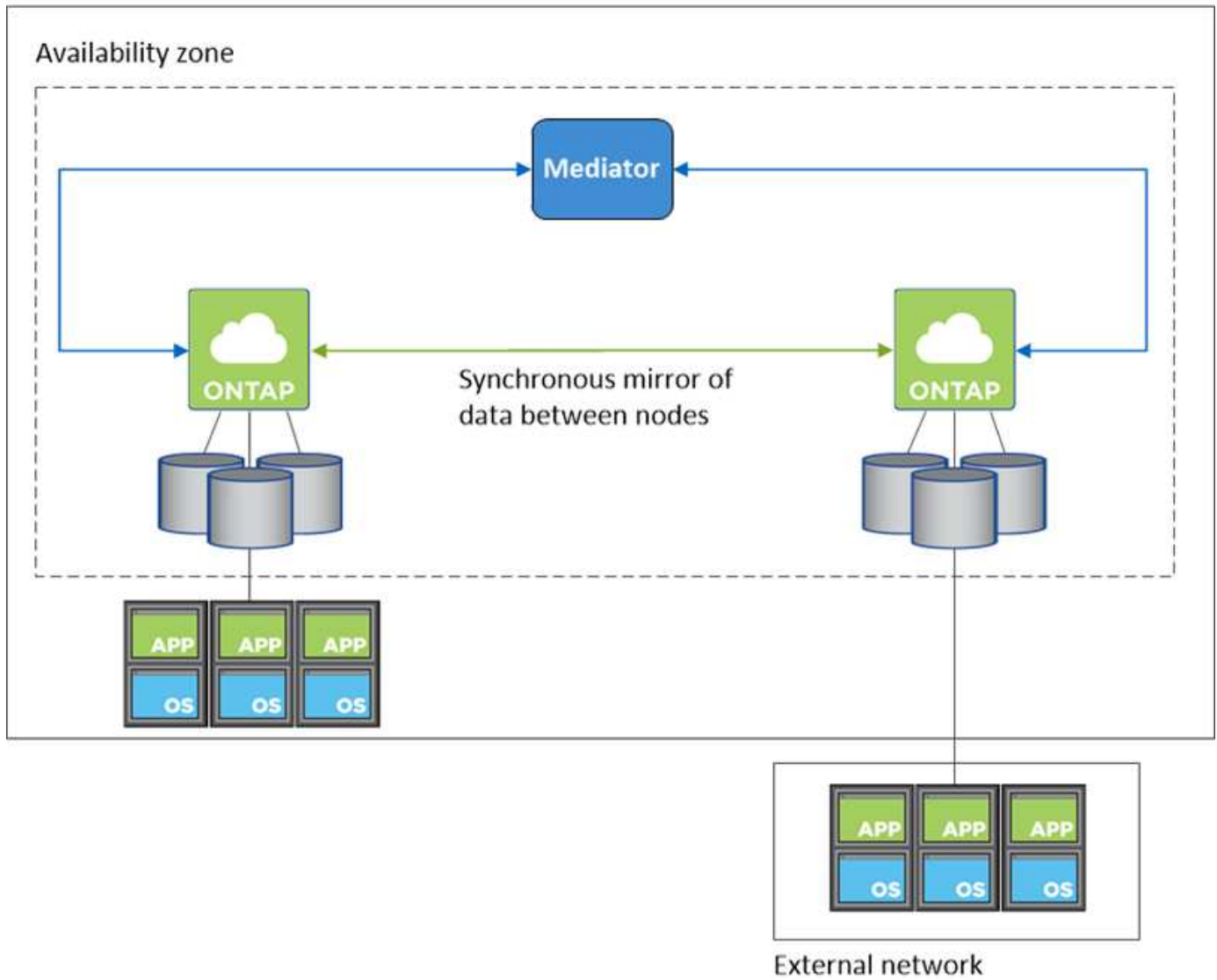
This HA configuration is not supported in the Volume View.

### Data access

Because this configuration is in a single AZ, it does not require floating IP addresses. You can use the same IP address for data access from within the VPC and from outside the VPC.

The following image shows an HA configuration in a single AZ. Data is accessible from within the VPC and from outside the VPC.





### Storage takeover and giveback

For iSCSI, ONTAP Cloud uses multipath I/O (MPIO) and Asymmetric Logical Unit Access (ALUA) to manage path failover between the active-optimized and non-optimized paths.



For information about which specific host configurations support ALUA, see the [NetApp Interoperability Matrix Tool](#) and the Host Utilities Installation and Setup Guide for your host operating system.

For NAS configurations, the data IP addresses can migrate between HA nodes if failures occur. This ensures client access to storage.

### How storage works in an ONTAP Cloud HA pair

Unlike an ONTAP cluster, storage in an ONTAP Cloud HA pair is not shared between nodes. Instead, data is synchronously mirrored between the nodes so that the data is available in the event of failure.

## Storage allocation

When you create a new volume and additional disks are required, Cloud Manager allocates the same number of disks to both nodes, creates a mirrored aggregate, and then creates the new volume. For example, if two disks are required for the volume, Cloud Manager allocates two disks per node for a total of four disks.

## Storage configurations

You can use an ONTAP Cloud HA pair as an active-active configuration, in which both nodes serve data to clients, or as an active-passive configuration, in which the passive node responds to data requests only if it has taken over storage for the active node.



You can set up an active-active configuration only when using Cloud Manager in the Storage System View.

## Performance expectations for an ONTAP Cloud HA configuration

An ONTAP Cloud HA configuration synchronously replicates data between nodes, which consumes network bandwidth. As a result, you can expect the following performance in comparison to a single-node ONTAP Cloud configuration:

- For HA configurations that serve data from only one node, read performance is comparable to the read performance of a single-node configuration, whereas write performance is lower.
- For HA configurations that serve data from both nodes, read performance is higher than the read performance of a single-node configuration, and write performance is the same or higher.

For more details about ONTAP Cloud performance, see [Performance](#).

## Client access to storage

Clients should access NFS and CIFS volumes by using the data IP address of the node on which the volume resides. If NAS clients access a volume by using the IP address of the partner node, traffic goes between both nodes, which reduces performance.

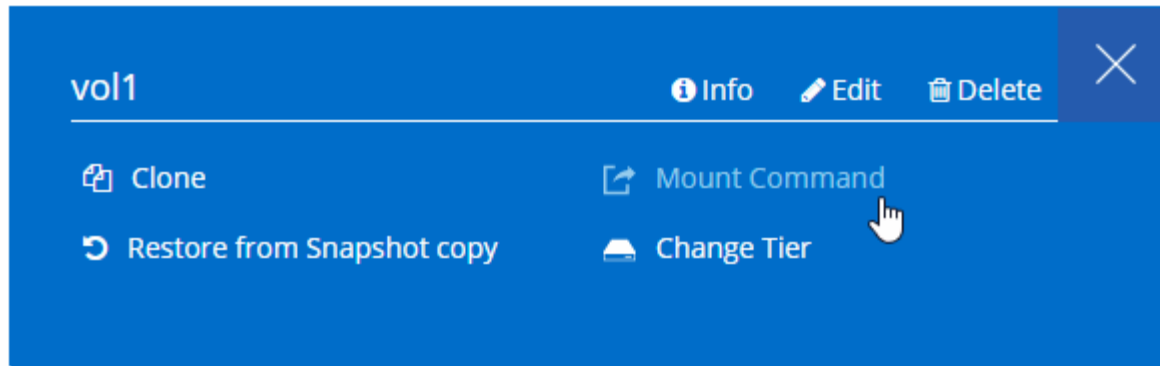


If you move a volume between nodes in an HA pair, you should remount the volume by using the IP address of the other node. Otherwise, you can experience reduced performance. If clients support NFSv4 referrals or folder redirection for CIFS, you can enable those features on the ONTAP Cloud systems to avoid remounting the volume. For details, see ONTAP documentation.

You can easily identify the correct IP address from Cloud Manager. The following image shows the Storage System View:

# Volumes

2 Volumes | 0.22 TB Allocated | < 0.01 TB Used (0 TB in S3)



The following image shows the Volume View:

Volume Name	Capacity	Used Capacity	Disk Type	Exported as	Location	Status	
vol1	500 GB	188 KB	SSD	172.31.11.229:vol1	us-east-1, 172...	Online	
vol2	1,000 GB	188 KB	SSD	Mount	Manage Access	Clone	Delete

## Security

ONTAP Cloud supports data encryption and provides protection against viruses.

### Data encryption in Azure

[Azure Storage Service Encryption](#) for data at rest is enabled by default for ONTAP Cloud data in Azure.



Customer-managed keys are not supported with ONTAP Cloud.

### Data encryption in AWS

You can choose whether to encrypt data on ONTAP Cloud systems in AWS when you create a new working environment. If data encryption is needed, you can choose between AWS-managed encryption and ONTAP Cloud encryption.

#### Encryption using the AWS KMS

The AWS Key Management Service (KMS) is a managed service that gives you control of encryption keys without having to administer a key management infrastructure. If you choose AWS-managed encryption, Cloud Manager requests data keys using a customer master key (CMK).

If you want to use this encryption option, then you must ensure that the AWS KMS is set up appropriately. For details, see [Setting up the AWS KMS](#).

For more information about the AWS KMS, refer to the following:

- [AWS Documentation: EBS Encryption](#)
- [AWS Documentation: What is AWS Key Management Service?](#)

## **ONTAP Cloud encryption**

You can protect your data from unauthorized access by using data-at-rest encryption provided by ONTAP Cloud. This optional feature encrypts and decrypts data using encryption keys that are stored on one or more key managers that are under your control.

Communication with key managers is always secure. ONTAP Cloud connects to key managers using a TLS connection and communicates using the Key Management Interoperability Protocol (KMIP).

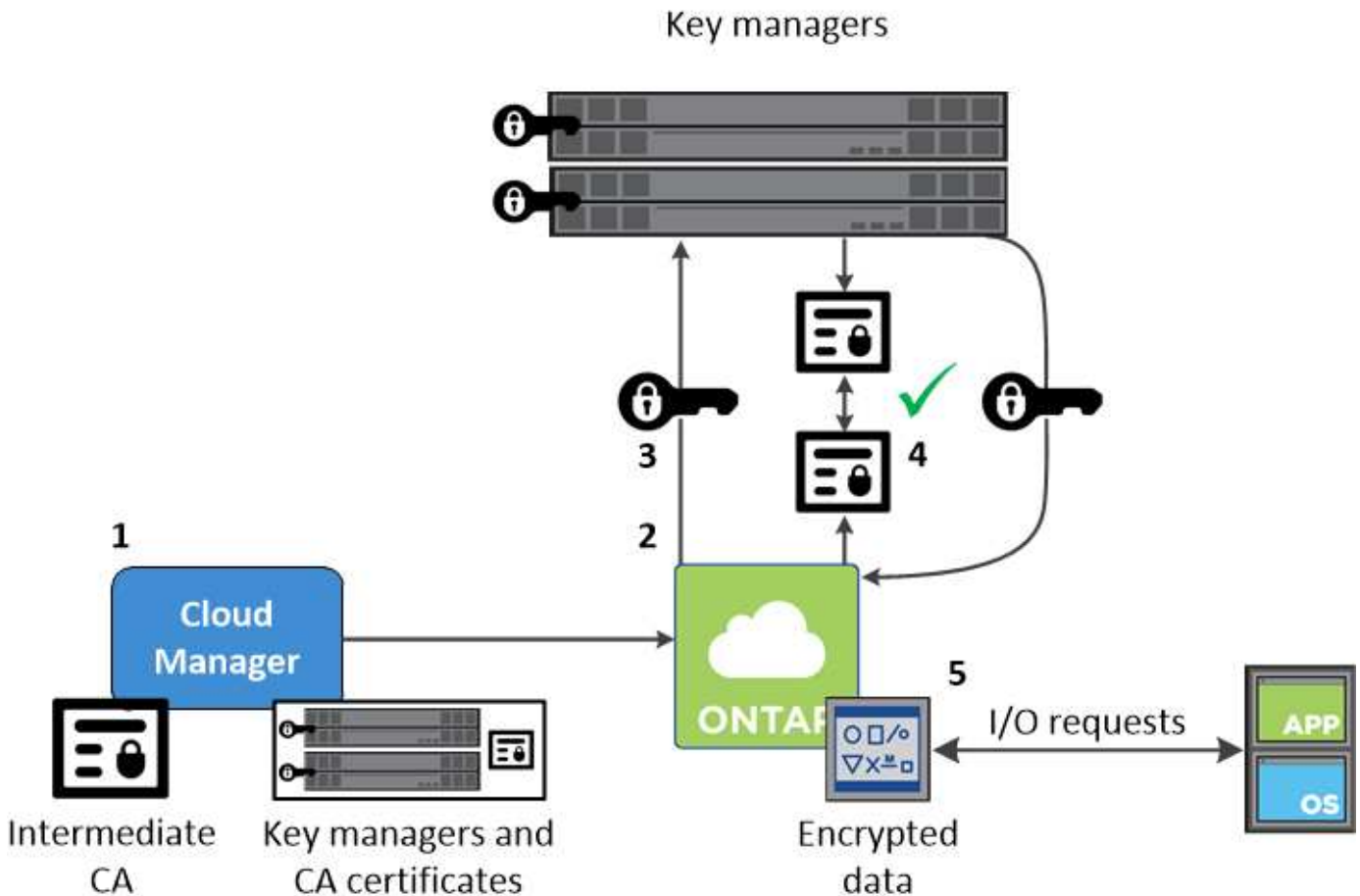
ONTAP Cloud uses the XTS-AES algorithm, a mode of the Advanced Encryption Standard (AES), to protect data-at-rest. Before data is written to disk, it is encrypted using XTS-AES. When data is read from disk, the encrypted data is decrypted using XTS-AES before being sent to the requester.

If you use the NetApp Storage Encryption feature with a physical FAS system and enable encryption on an ONTAP Cloud system, any data that you replicate between those systems is decrypted before it is replicated and then re-encrypted after it is replicated.

You must set up and configure a key management infrastructure to use ONTAP Cloud encryption. For details, see [Setting up ONTAP Cloud encryption](#).

### **How ONTAP Cloud encryption works with SafeNet key managers**

Understanding how ONTAP Cloud encryption works with SafeNet key managers can help you set up and use the feature. The following graphic shows the steps and components involved in the encryption process when using SafeNet key managers:



1. The Cloud Manager Admin sets up Cloud Manager as follows:
  - a. Generates a certificate signing request (CSR), uses it to obtain a signed certificate from a certificate authority (CA), and then installs the signed certificate in Cloud Manager.
  - b. Adds details about key managers and key manager CA certificates in Cloud Manager.
2. Users launch ONTAP Cloud instances with encryption enabled (it cannot be enabled afterward).

Cloud Manager sets up ONTAP Cloud by installing the key manager CA certificate, generating and installing a client certificate, configuring the KMIP client, and linking the system to one or more key managers.



All data on the system is encrypted, except for the root aggregate, which does not contain user data.

3. For each aggregate, ONTAP Cloud generates and sends an encryption key to key managers.
4. Each time ONTAP Cloud boots, it authenticates with key managers to obtain encryption keys, which are then stored in cache and never displayed in cleartext.



ONTAP Cloud communicates with key managers when it boots and when new aggregates are created. It does not communicate with key managers at any other time.

5. Before data is written to disk, it is encrypted using XTS-AES.

When data is read from disk, the encrypted data is decrypted using XTS-AES before being sent.

## ONTAP virus scanning

You can use integrated antivirus functionality on ONTAP systems to protect data from being compromised by viruses or other malicious code.

ONTAP virus scanning, called *Vscan*, combines best-in-class third-party antivirus software with ONTAP features that give you the flexibility you need to control which files get scanned and when.

For information about the vendors, software, and versions supported by Vscan, see the [NetApp Interoperability Matrix](#).

For information about how to configure and manage the antivirus functionality on ONTAP systems, see the [ONTAP 9 Antivirus Configuration Guide](#).

## Licensing

Each ONTAP Cloud BYOL system must have a license installed with an active subscription. If an active license is not installed, the ONTAP Cloud system shuts itself down after 30 days. Cloud Manager simplifies the process by managing licenses for you and by notifying you before they expire.

### License management for a new system

A tenant must be linked to a NetApp Support Site account so Cloud Manager can obtain licenses for ONTAP Cloud BYOL systems. If the credentials are not present, Cloud Manager prompts you to enter them when you create a new ONTAP Cloud BYOL working environment.

### Why you should link a tenant to your NetApp Support Site account

Each time you launch an ONTAP Cloud BYOL system, Cloud Manager automatically downloads the license from NetApp and installs it on the ONTAP Cloud system.

If Cloud Manager cannot access the license file over the secure Internet connection, you can obtain the file yourself and then manually upload the file to Cloud Manager.

### License expiration

Cloud Manager warns you 30 days before a license is due to expire and again when the license expires. The following image shows a 30-day expiration warning:



You can select the working environment to review the message.

If you do not renew the license in time, the ONTAP Cloud system shuts itself down. If you restart it, it shuts itself down again.



ONTAP Cloud can also notify you through email, an SNMP trap host, or syslog server using EMS (Event Management System) event notifications. For instructions, see the [ONTAP 9 EMS Configuration Express Guide](#).

### License renewal

When you renew a BYOL subscription by contacting a NetApp representative, Cloud Manager automatically obtains the new license from NetApp and installs it on the ONTAP Cloud system.

If Cloud Manager cannot access the license file over the secure internet connection, you can obtain the file yourself and then manually upload the file to Cloud Manager. For instructions, see [Installing license files on ONTAP Cloud BYOL systems](#).

## Performance

You can review performance results to help you decide which workloads are appropriate for ONTAP Cloud.

For ONTAP Cloud for AWS, refer to [NetApp Technical Report 4383: Performance Characterization of ONTAP Cloud in Amazon Web Services with Application Workloads](#).

For ONTAP Cloud for Microsoft Azure, refer to [NetApp Technical Report 4671: Performance Characterization of ONTAP Cloud in Azure with Application Workloads](#).

## Cloud Storage Automation

The Cloud Storage Automation Report analyzes your cloud storage to show you savings opportunities, data protection enhancements, and operations that can optimize the storage associated with your AWS account. This is a beta feature.

### Sample report

The following image shows a sample report:

### Savings Opportunities

**\$309,411**  
Total Savings (Annual)

\$ 44,366  
Overallocation (Estimated Amount)

---

\$ 201,371  
Unattached EBS Volumes

---

\$ 63,674  
Unassociated EBS Snapshots

### Protection

EBS Volumes:

**588** With EBS Snapshots

**796** Without EBS Snapshots

1 month  
Average RPO

---

32  
Average Number of EBS Snapshots

Average RPO and Average Number of EBS Snapshots are calculated only for EBS volumes with EBS Snapshots.

### Operations

**21,221**  
Exceptions Detected

3  
Volumes running out of space View List

---

796  
EBS Volumes without EBS Snapshots

---

44  
Unattached EBS Volumes View List

---

20,378  
Unassociated EBS Snapshots View List

In some cases, the report enables you to take immediate action. For example, when you view the list of unattached EBS volumes or unassociated EBS snapshots, you can delete them right from Cloud Manager:

← Unattached EBS Volumes

Delete all selected

44 EBS Volumes 4 selected

<input type="checkbox"/>	EBS Volume ID	Type	Allocated Capacity	Tags	Creation Time	Deleting Status
<input checked="" type="checkbox"/>	vol-0f569b8cbb8f3728c	gp2	16 TB	None	Nov 20, 2017 07:30:27 pm	
<input checked="" type="checkbox"/>	vol-044641bbcf5c0595	gp2	9.77 TB	None	Oct 27, 2017 09:16:26 am	
<input checked="" type="checkbox"/>	vol-0ba66d87777af9a39	gp2	9.77 TB	8 Tags	Oct 28, 2017 04:12:54 pm	
<input checked="" type="checkbox"/>	vol-0d4b3a3a4b77e91a8	gp2	9.77 TB	None	Nov 6, 2017 06:34:48 pm	
<input type="checkbox"/>	vol-00acf6e082030125	gp2	7.81 TB	None	Dec 1, 2017 02:36:25 am	
<input type="checkbox"/>	vol-0276f5ac55a477e67	gp2	7.81 TB	None	Oct 11, 2017 07:25:22 pm	
<input type="checkbox"/>	vol-0343fd60e5e62b29c	gp2	7.81 TB	None	Jul 21, 2017 07:32:42 pm	
<input type="checkbox"/>	vol-03f34df0e7c5c125e	gp2	7.81 TB	4 Tags	Aug 24, 2017 04:22:02 pm	
<input type="checkbox"/>	vol-0476b62ea98a6743b	gp2	7.81 TB	None	Oct 10, 2017 05:54:46 pm	
<input type="checkbox"/>	vol-06d0f6c2164f21090	gp2	7.81 TB	None	Nov 16, 2017 06:56:51 pm	
<input type="checkbox"/>	vol-086e06fb6540c3386	gp2	7.81 TB	None	Oct 11, 2017 07:28:24 pm	

## What happens when you enable the report

Cloud Manager collects information about the EC2 instances, EBS volumes, and EBS snapshots associated



with your AWS account, in the region where Cloud Manager resides. AWS resources used for ONTAP Cloud systems are excluded. There is no performance impact on AWS resources.

When Cloud Manager collects the information, it identifies improvement opportunities by using EBS snapshots to calculate used capacity and daily usage growth predictions.

The report runs once a week, but you can initiate an immediate data collection at any time.

## **Required permissions**

The AWS permissions required for Cloud Storage Automation are included in the Cloud Manager IAM policy. If you set up permissions correctly, then there is nothing further to do. See [Granting AWS permissions](#) for details.

## Copyright Information

Copyright © 2022 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system-without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

## Trademark Information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.