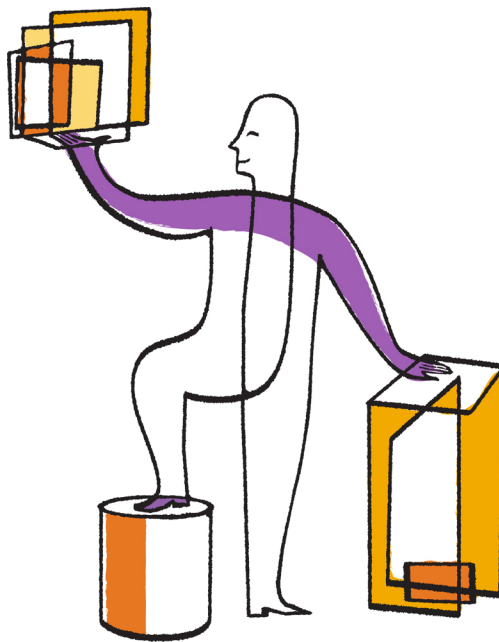




OnCommand® Cloud Manager 2.1

Storage Management Guide



NetApp, Inc.
495 East Java Drive
Sunnyvale, CA 94089
U.S.

Telephone: +1 (408) 822-6000
Fax: +1 (408) 822-4501
Support telephone: +1 (888) 463-8277
Web: www.netapp.com
Feedback: doccomments@netapp.com

Part number: 215-10495_A0
December 2015

Contents

Before you use this guide	5
Product overview	6
Cloud ONTAP for AWS overview	7
Cloud Manager REST APIs	8
Logging in to Cloud Manager	9
Overview of the Cloud Manager console	9
Changing your password	12
Creating Working Environment Admins	12
Launching and setting up Cloud ONTAP instances	14
Preparing to launch Cloud ONTAP instances	15
How Cloud ONTAP is configured by default	15
How Cloud ONTAP uses EBS storage	16
Cloud ONTAP configurations	18
Ways to encrypt Cloud ONTAP data	18
Considerations for choosing an underlying EBS disk type	19
Considerations for choosing EBS disk size	19
What volume usage profiles are	20
AWS network information worksheet	21
Launching Cloud ONTAP instances	21
Creating a Cloud ONTAP working environment	21
Registering Cloud ONTAP pay-as-you-go instances	25
Setting up Cloud ONTAP	26
Connecting to OnCommand System Manager	27
Connecting to the Cloud ONTAP CLI	28
Setting up Cloud ONTAP for iSCSI	29
Provisioning storage	29
How you can provision Cloud ONTAP storage in Cloud Manager	29
Provisioning volumes	30
Creating aggregates	32
Provisioning iSCSI LUNs	32
Managing Cloud ONTAP	34
Monitoring AWS storage and compute costs	34
Managing storage	35
Managing existing volumes	35
Managing existing aggregates	36
Modifying the CIFS server	37
Managing the state of Cloud ONTAP instances	37
Scheduling automatic shutdowns of Cloud ONTAP instances	38
Stopping a Cloud ONTAP instance	38
Deleting a Cloud ONTAP working environment	38
Updating Cloud ONTAP software	39

Preparing to update Cloud ONTAP software	40
Upgrading Cloud ONTAP to the latest version	41
Upgrading or downgrading Cloud ONTAP by using an HTTP or FTP server	42
Downgrading Cloud ONTAP by using a local image	43
Changing the configuration of Cloud ONTAP instances	43
How Cloud Manager enforces Cloud ONTAP BYOL subscriptions	44
Viewing Cloud ONTAP configuration details	44
Viewing Cloud ONTAP license information	44
Changing a Cloud ONTAP instance type	45
Changing between pay-as-you-go configurations	45
Moving to an alternate Cloud ONTAP subscription	45
Adding existing Cloud ONTAP instances to Cloud Manager	46
Managing Cloud ONTAP encryption	47
Understanding how Cloud ONTAP encryption works	47
Managing key managers and certificates for Cloud ONTAP	48
Finding the encryption key for an aggregate	48
Modifying the Storage Virtual Machine name	49
Changing the password for a Cloud ONTAP instance	49
Configuring Cloud ONTAP to send configuration backups to Cloud Manager	50
Discovering and managing Data ONTAP clusters	51
Discovering Data ONTAP clusters	51
Provisioning volumes for Data ONTAP clusters	51
Replicating data to and from the cloud	53
Considerations for choosing a replication policy	54
How SnapVault policies work	55
What happens when you replicate data to and from encrypted systems	56
Data replication requirements	56
Replicating data between systems	57
Managing data replication schedules and relationships	59
What to do after using Cloud Manager	61
Copyright information	62
Trademark information	63
How to send comments about documentation and receive update notifications	64
Index	65

Before you use this guide

The *OnCommand Cloud Manager Storage Management Guide* describes how you can use Cloud Manager to manage storage across a hybrid cloud configuration that includes Cloud ONTAP, NetApp Private Storage for Cloud solutions, and on-premises Data ONTAP clusters. Before you can use Cloud Manager to manage storage, your Cloud Manager administrator should have prepared, installed, and set up Cloud Manager as described in the *OnCommand Cloud Manager Installation and Setup Guide*.

Note: This guide describes how to perform tasks using the Cloud Manager user interface. If you need help using the Cloud Manager APIs, see the [OnCommand Cloud Manager 2.1 API Getting Started Guide](#).

This guide assumes the following conditions exist:

- AWS networking requirements were met for Cloud Manager and Cloud ONTAP.
- IAM users have been granted the appropriate AWS permissions.
- Each Cloud ONTAP product that users will launch was subscribed to from the AWS Marketplace.
- Cloud Manager was installed.
- If users want to enable Cloud ONTAP encryption, a key management infrastructure was set up and Cloud Manager encryption settings were defined.
- If necessary, Cloud Manager was configured to use a proxy server.
- Tenants were defined.
- At least one Tenant Admin user was created.

Related information

[OnCommand Cloud Manager 2.1 Installation and Setup Guide](#)

Product overview

OnCommand Cloud Manager provides an enterprise-level standard for setting up and managing hybrid cloud storage environments built on clustered Data ONTAP. You can use Cloud Manager to launch and manage Cloud ONTAP instances in Amazon Web Services (AWS) and to replicate data across your hybrid cloud.

Management of Cloud ONTAP for AWS

Cloud Manager enables you to manage Cloud ONTAP systems as follows:

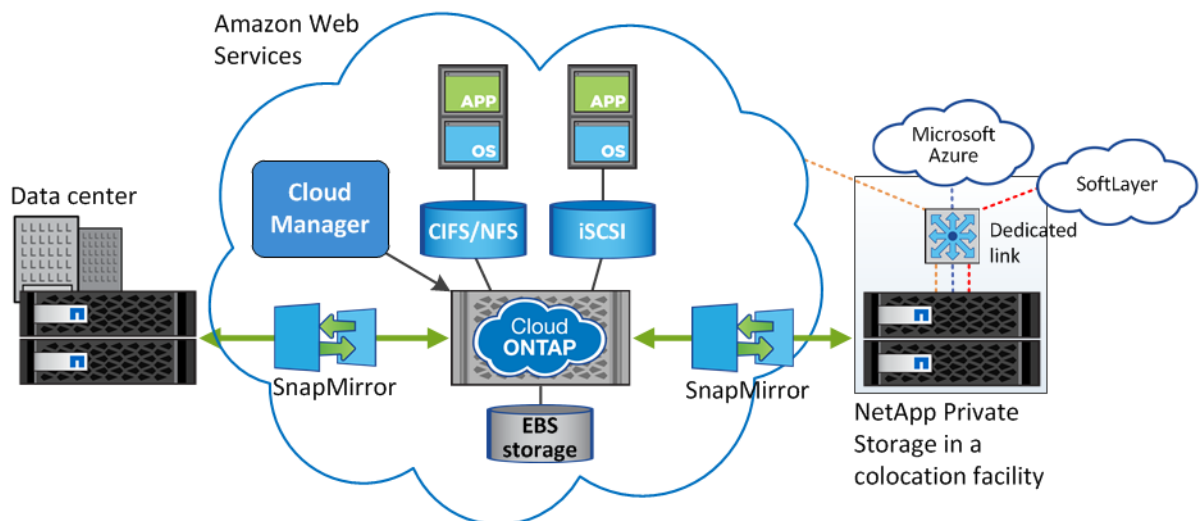
- Deploy Cloud ONTAP systems in approximately 25 minutes
- Set up Cloud ONTAP for data-at-rest encryption
- Provision NFS and CIFS storage using a simplified provisioning wizard
- Replicate data to and from the cloud
- Upgrade Cloud ONTAP systems to the latest version using an automated process
- Monitor AWS storage and compute charges associated with Cloud ONTAP systems

Data replication across your hybrid cloud

Cloud Manager can discover Data ONTAP clusters in your on-premises environment, and clusters that belong to a NetApp Private Storage for Cloud configuration in AWS, Microsoft Azure, and SoftLayer. Discovering these clusters enables you to easily replicate data across your hybrid cloud environment: between on-premises Data ONTAP clusters, Cloud ONTAP systems, and NetApp Private Storage for Cloud configurations.

Where to deploy Cloud Manager

Cloud Manager can run in AWS or in your network. The following image shows Cloud Manager running in AWS and managing a Cloud ONTAP system and data replication to and from Data ONTAP clusters:



Cloud ONTAP for AWS overview

Cloud ONTAP for Amazon Web Services (AWS) is a software-only storage appliance that runs the clustered Data ONTAP storage operating system in the cloud. Building your cloud environment on Cloud ONTAP provides enterprise-class features for your cloud storage and gives you a universal storage platform that enables you to easily replicate data between your data center and the cloud.

What Cloud ONTAP provides

Cloud ONTAP manages Amazon Elastic Block Store (EBS) volumes with the NetApp clustered Data ONTAP storage operating system, which provides enterprise-class features:

- Multiprotocol support (NFS, CIFS, and iSCSI)
- Data protection (NetApp Snapshot copies, SnapMirror technology, and SnapVault technology)
- Storage efficiency (thin provisioning, data deduplication, and data compression)
- Data-at-rest encryption using encryption keys that are stored on key managers under your control

Note: The licenses for these features are included with Cloud ONTAP.

How you deploy Cloud ONTAP

You must use OnCommand Cloud Manager to launch Cloud ONTAP as an Elastic Cloud Compute (EC2) instance in AWS. Cloud Manager uses your AWS access key and secret key to launch the EC2 instance and to purchase the EBS volumes that Cloud ONTAP uses as back-end storage.

Cloud ONTAP products

Cloud ONTAP is available in a pay-as-you-go AMI and a Bring Your Own License (BYOL) AMI. The pay-as-you-go AMI is available in three configurations: Explore, Standard, and Premium.

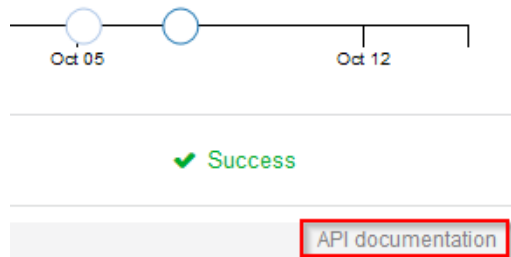
	Cloud ONTAP Explore	Cloud ONTAP Standard	Cloud ONTAP Premium	Cloud ONTAP BYOL
Cloud ONTAP encryption ¹	Not supported	Supported	Supported	Supported
EC2 instance types ²	• m3.xlarge • m4.xlarge	• m3.2xlarge • m4.2xlarge • r3.xlarge	r3.2xlarge	• m3.xlarge • m3.2xlarge • m4.xlarge • m4.2xlarge • r3.xlarge • r3.2xlarge
EBS storage type	General Purpose (SSD) or Magnetic	General Purpose (SSD) or Magnetic	General Purpose (SSD) or Magnetic	General Purpose (SSD) or Magnetic
EBS raw capacity limit	2 TB	10 TB	368 TB for SSD disks 46 TB for Magnetic disks	368 TB for SSD disks 46 TB for Magnetic disks
Term	Hourly or annual	Hourly or annual	Hourly or annual	6 or 12 months

1. Cloud ONTAP encryption is not supported with M3 instances and with m4.xlarge instances.
2. M4 instances are supported starting with Cloud ONTAP 8.3.2.

Cloud Manager REST APIs

Cloud Manager includes REST APIs that enable software developers to automate the management of NetApp storage in the cloud. There is an API for every action that is available from the user interface.

Cloud Manager provides interactive API documentation using the Swagger interface. A link to the API documentation is available in the lower-right corner of the console:



If you need help getting started with the APIs, see the [OnCommand Cloud Manager 2.1 API Getting Started Guide](#).

Logging in to Cloud Manager

You can log in to Cloud Manager from any web browser that has a connection to the Cloud Manager host.

Steps

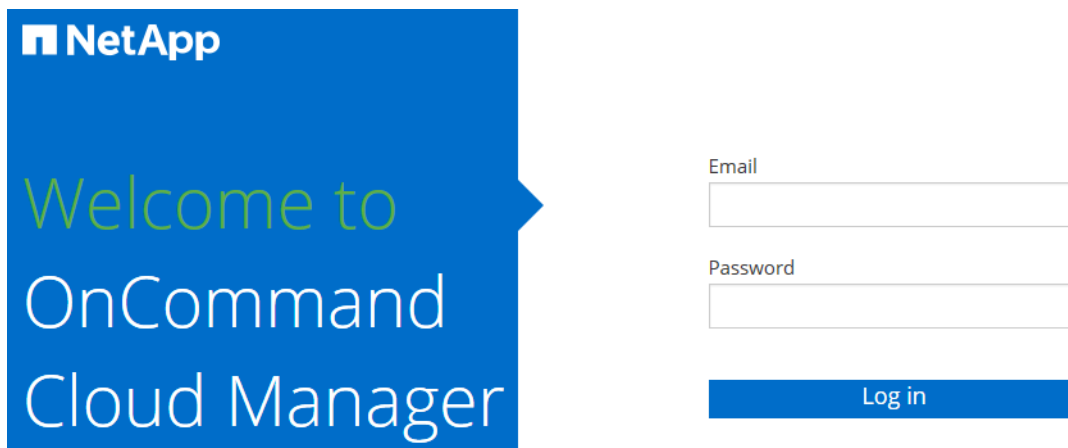
1. Open a web browser and enter the following URL:

`https://ipaddress:port`

ipaddress can be **localhost**, a private IP address, or a public IP address, depending on the configuration of the Cloud Manager host. For example, if Cloud Manager is installed in AWS and the instance does not have a public IP address, you must enter a private IP address from a host in AWS that has a connection to the Cloud Manager host.

port is required if you changed the default HTTP (80) or HTTPS (443) ports. For example, if the HTTPS port was changed to 8443, you would enter **`https://ipaddress:8443`**

After you enter the URL, the Cloud Manager log in screen appears:



The screenshot shows the login interface for NetApp OnCommand Cloud Manager. On the left, a blue banner displays the NetApp logo and the text "Welcome to OnCommand Cloud Manager". On the right, there is a login form with two input fields: "Email" and "Password". Below these fields is a blue button labeled "Log in".

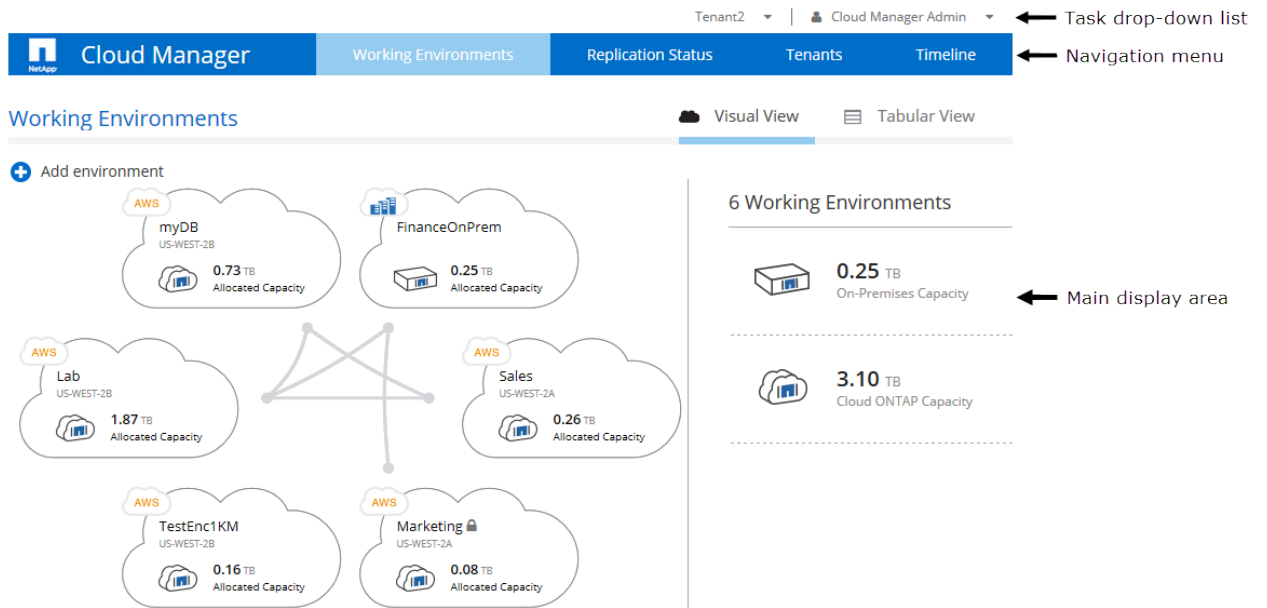
2. Enter your email address and password, and then click **Log in**.

Overview of the Cloud Manager console

The Cloud Manager console is a web-based interface that gives users the ability to provision and manage storage (working environments) in isolated groups called tenants.

Major components of the console

The console consists of a task drop-down list, a navigation menu, and a main display area:

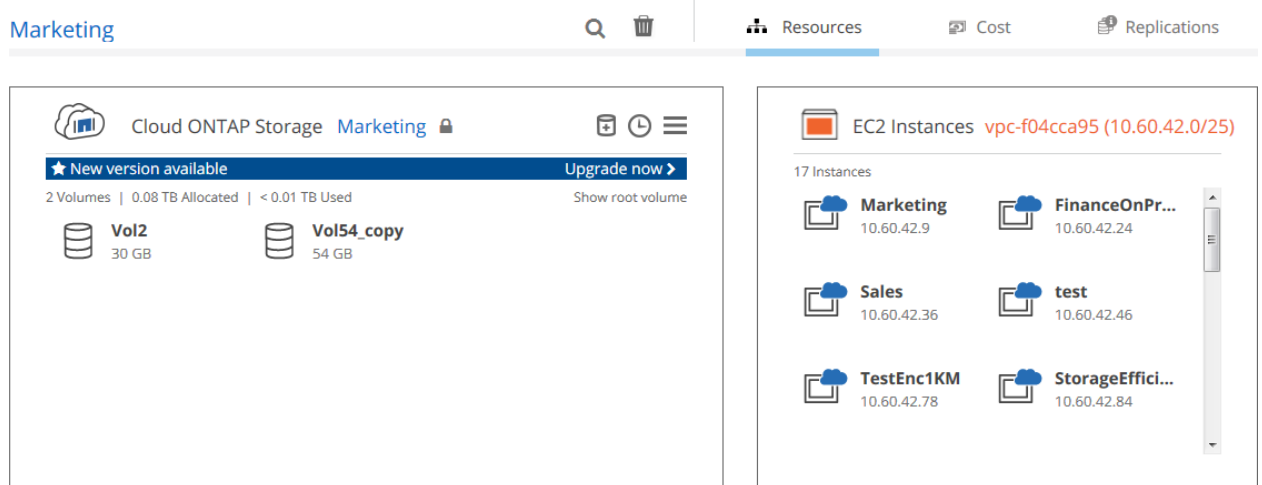


Working environments

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

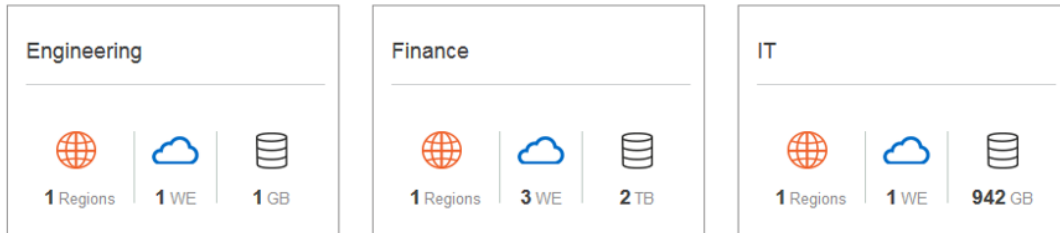
- A Cloud ONTAP system
- An on-premises Data ONTAP cluster in your network
- A Data ONTAP cluster in a NetApp Private Storage configuration

The following image shows a Cloud ONTAP working environment:



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:



How Cloud Manager users relate to tenants and working environments

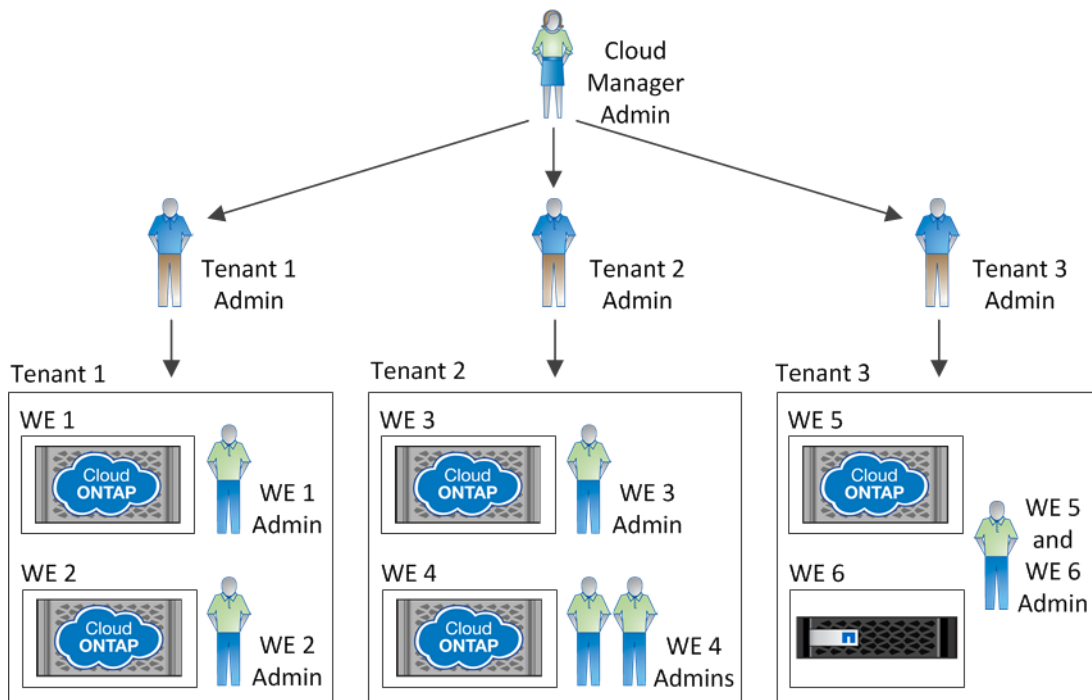
The tenants and working environments that you can manage depends on your user role and assignments.

The three distinct user roles are as follows:

- **Cloud Manager Admin:** Administers the product and has access to 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:** Administers one or more working environments in a tenant.

When a Cloud Manager Admin or Tenant Admin creates a user account, they assign the user to a specific tenant. Working Environment Admins can also be assigned to specific working environments, and they can create their own working environments.

The following image shows the relationship between users, tenants, and working environments:

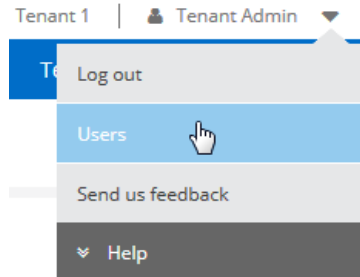


Changing your password

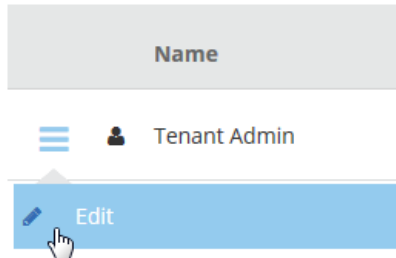
You might want to change your password after you log in to Cloud Manager for the first time because your administrator assigned your initial password for you.

Steps

1. In the upper right corner of the Cloud Manager console, click the task drop-down list, and then select **Users**:



2. In the **Users** table, position your cursor over your account name, select the menu icon, and then click **Edit**:



3. Click **Change Password**, enter your current password and new password, and then click **Save**.

Result

Cloud Manager saves your password. You can log out of the console and then log back in with your new password.

Creating Working Environment Admins

A tenant typically includes one or more Working Environment Admins who create and manage the working environments in that tenant. A Tenant Admin can create those Working Environment Admins, if the Cloud Manager Admin did not do so already.

Steps

1. In the upper right corner of the Cloud Manager console, click the task drop-down list, and then select **Users**.
2. In the **Users** page, click **New User**.
3. In the **New User** page, specify details for the new user account.

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

Field	Description
Email Address	Enter the email address that the user must use to log in to Cloud Manager. Cloud Manager does not send emails to this address.
Role	Assign the user to a tenant and, optionally, a working environment. If the selected tenant does not have a working environment, you can modify the assigned working environments at a later time. Note: Working Environment Admins automatically have privileges to the working environments that they create themselves.
AWS Access Key and Secret Key	Enter the access key and secret key assigned to the user in AWS. Cloud Manager uses the keys to perform AWS actions on the user's behalf. Identity and Access Management (IAM) users must have specific AWS permissions. You can use a NetApp-provided IAM policy that includes the required permissions. NetApp OnCommand Cloud Manager: AWS IAM Policy
AWS Cost S3 Bucket	Optionally enter the S3 bucket that contains detailed billing reports, if you specified keys for an AWS account under which the bucket was created. Giving Cloud Manager access to detailed billing reports enables users to see AWS storage and compute costs associated with Cloud ONTAP. If you are using AWS consolidated billing, you do not need to specify the bucket each time you create a user account. You just specify the bucket for one Cloud Manager user account that corresponds to an IAM user created under the AWS payer account, or the payer account itself. If you have not set up an S3 bucket and enabled billing reports, see the OnCommand Cloud Manager Installation and Setup Guide for details.

4. Click **Save**.

Result

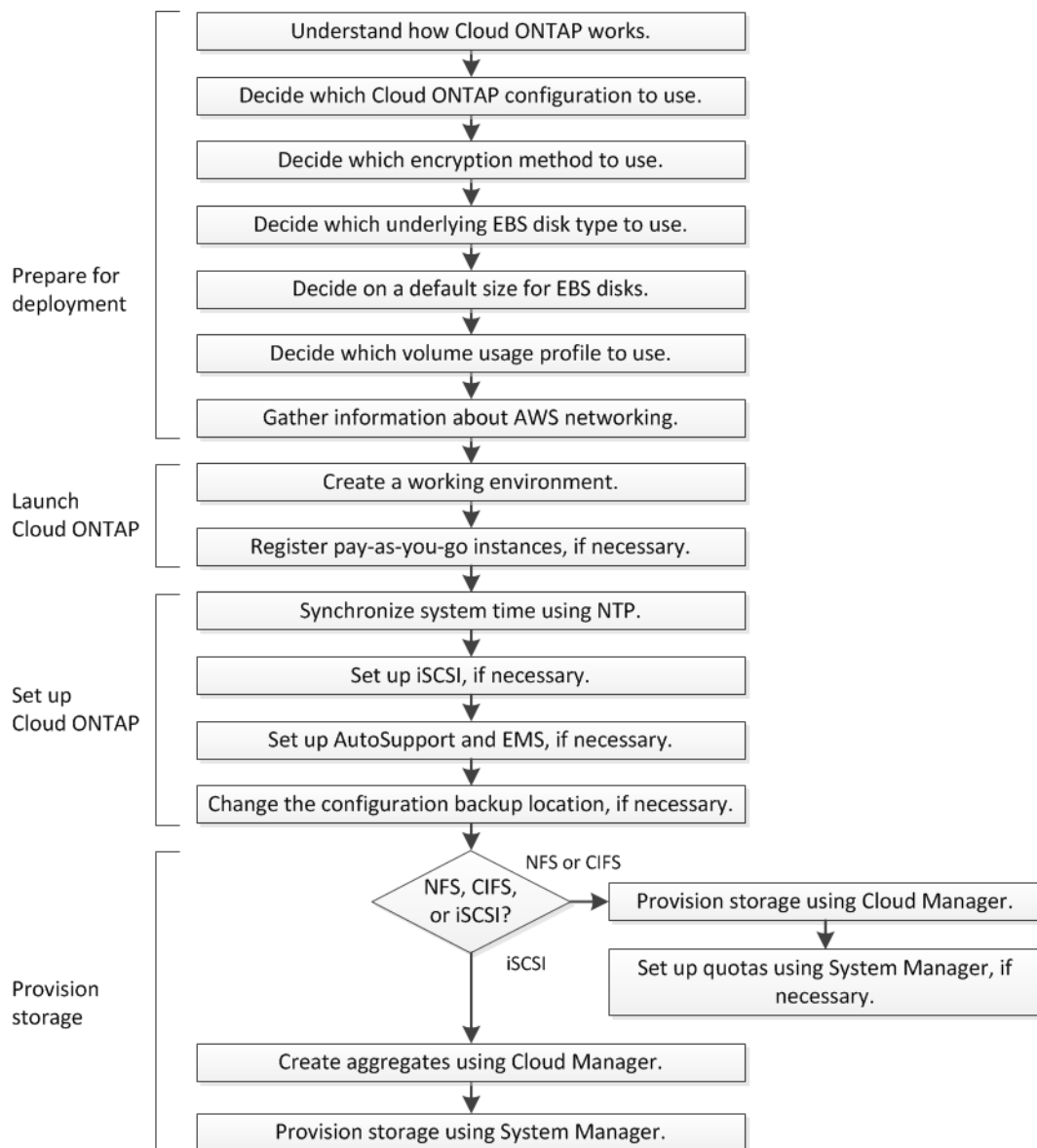
Cloud Manager creates the user account. The user can now log in to Cloud Manager.

Related information

[OnCommand Cloud Manager 2.1 Installation and Setup Guide](#)

Launching and setting up Cloud ONTAP instances

Getting Cloud ONTAP up and running involves preparing for deployment, launching instances, setting them up, and then provisioning storage. You can then use the instances to serve data and to replicate data to and from the cloud. After that, you can monitor AWS costs and manage the instances as needed.



Preparing to launch Cloud ONTAP instances

Before you launch a Cloud ONTAP instance, you should understand a few key concepts, decide how you want to set up the instance, and then gather AWS networking information.

Steps

1. Understand how Cloud ONTAP works.
[How Cloud ONTAP is configured by default](#) on page 15
[How Cloud ONTAP uses EBS storage](#) on page 16
2. Decide which Cloud ONTAP configuration to use.
[Cloud ONTAP configurations](#) on page 18
3. If you need to encrypt data, decide which data encryption method to use.
[Ways to encrypt Cloud ONTAP data](#) on page 18
4. Decide which underlying EBS disk type to use.
[Considerations for choosing an underlying EBS disk type](#) on page 19
5. Decide on a default size for EBS disks.
[Considerations for choosing EBS disk size](#) on page 19
6. Decide which volume usage profile you need.
[What volume usage profiles are](#) on page 20
7. Gather information about AWS networking.
[AWS network information worksheet](#) on page 21

How Cloud ONTAP is configured by default

Understanding how Cloud ONTAP is configured by default can help you set up and administer your systems, especially if you are familiar with clustered Data ONTAP because the default setup for Cloud ONTAP is different than clustered Data ONTAP.

- Cloud ONTAP is a single-node cluster. You cannot join other nodes to the cluster, which means that storage failover between an HA pair is not available.
- Cloud ONTAP supports a single Storage Virtual Machine (SVM). Cloud Manager creates this SVM when it launches an instance.

Note: Although you can create another SVM from System Manager or the CLI, using multiple SVMs is not supported.

- Several network interfaces are created by default:
 - A cluster management LIF
 - An intercluster LIF
 - A node management LIF
 - An iSCSI data LIF
 - A CIFS and NFS data LIF

Note: LIF failover is disabled by default for Cloud ONTAP due to EC2 requirements. Migrating a LIF to a different port breaks the external mapping between IP addresses and network interfaces on the instance, making the LIF inaccessible.

- Cloud Manager sets up Cloud ONTAP for NFS and CIFS. iSCSI requires further configuration.
- Cloud ONTAP sends configuration backups to Cloud Manager using HTTPS.
When logged in to Cloud Manager, the backups are accessible from `https://ipaddress/occm/offboxconfig/`
- Cloud Manager sets a few volume attributes differently than other management tools (System Manager or the CLI, for example).

The following table lists the volume attributes that Cloud Manager sets differently from the default values:

Attribute	Value set by Cloud Manager
Autosize mode	grow
Maximum autosize	1,000 percent Note: The Cloud Manager Admin can modify this value from the Settings page.
Security style	NTFS for CIFS volumes UNIX for NFS volumes
Space guarantee style	none
UNIX permissions (NFS only)	777

See the `volume create` man page for information about these attributes.

Related tasks

[Setting up Cloud ONTAP for iSCSI](#) on page 29

Related information

[NetApp Data ONTAP Operating System](#)

[Clustered Data ONTAP 8.3.2 man page: volume create - Create a new volume](#)

How Cloud ONTAP uses EBS storage

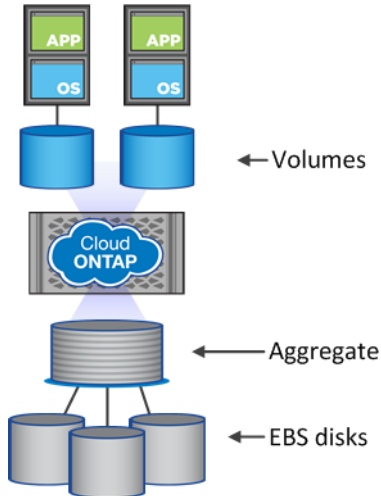
Cloud Manager makes storage provisioning easy by purchasing the AWS EBS disks that you need to provision volumes for Cloud ONTAP. Knowing how Cloud ONTAP uses EBS storage can help you understand your storage costs.

Cloud ONTAP user data

Cloud ONTAP uses EBS volumes as back-end storage. It sees these volumes as disks and groups them into one or more aggregates. Aggregates, which can include up to six EBS disks, provide storage to one or more Cloud ONTAP volumes.

The underlying EBS disk type can be either General Purpose (SSD) or Magnetic. You choose the disk type and the default disk size when you launch a Cloud ONTAP instance.

The following graphic shows the relationship between EBS disks and Cloud ONTAP storage:



When you launch a Cloud ONTAP instance, Cloud Manager purchases one to four EBS disks. The number of disks depends on the size of the Cloud ONTAP volume that you create. If you do not create a volume when you launch an instance, Cloud Manager purchases one EBS disk.

Although aggregates can include up to six EBS disks, Cloud Manager does not create new volumes on the last two disks. It uses the last two disks for existing volumes that need room to grow (Cloud Manager sets the autosize mode to *grow* for all read-write volumes).

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

Cloud ONTAP boot and root data

In addition to the storage for user data, Cloud Manager also purchases the following EBS storage:

- One Provisioned IOPS (SSD) disk for Cloud ONTAP boot data, which is approximately 42 GB and 1,250 PIOPS
- One General Purpose (SSD) disk for Cloud ONTAP root data, which is approximately 140 GB
- Two EBS snapshots for the Cloud ONTAP boot disk and root disk

Where the EBS disks reside

Cloud Manager lays out the storage from the EBS disks as follows:

- Boot data resides on an EBS disk attached to the instance under `/dev/sda1`. This disk, which contains the boot image, is not available to Cloud ONTAP.
- Root data, which contains the system configuration and logs, resides in `aggr0`.
- The Storage Virtual Machine (SVM) root volume resides in `aggr1`.
- Data volumes also reside in `aggr1`.

Related tasks

[Provisioning storage](#) on page 29

Cloud ONTAP configurations

Because application needs are different, Cloud ONTAP is available in several configurations that provide different options for EC2 instance types, EBS storage types, maximum raw EBS capacity, and terms. You need to choose a configuration when you launch an instance.

Cloud ONTAP is available in a pay-as-you-go AMI and a BYOL AMI. You can choose between three pay-as-you-go configurations: Explore, Standard, and Premium.

	Cloud ONTAP Explore	Cloud ONTAP Standard	Cloud ONTAP Premium	Cloud ONTAP BYOL
Cloud ONTAP encryption ¹	Not supported	Supported	Supported	Supported
EC2 instance types ²	- m3.xlarge - m4.xlarge	- m3.2xlarge - m4.2xlarge - r3.xlarge	r3.2xlarge	- m3.xlarge - m3.2xlarge - m4.xlarge - m4.2xlarge - r3.xlarge - r3.2xlarge
EBS storage type	General Purpose (SSD) or Magnetic	General Purpose (SSD) or Magnetic	General Purpose (SSD) or Magnetic	General Purpose (SSD) or Magnetic
EBS raw capacity limit	2 TB	10 TB	368 TB for SSD disks 46 TB for Magnetic disks	368 TB for SSD disks 46 TB for Magnetic disks
Term	Hourly or annual	Hourly or annual	Hourly or annual	6 or 12 months

1. Cloud ONTAP encryption is not supported with M3 instances and with m4.xlarge instances.
2. M4 instances are supported starting with Cloud ONTAP 8.3.2.

You can view pricing details from the AWS Marketplace pages.

Related information

[AWS Marketplace: Cloud ONTAP for AWS](#)

[AWS Marketplace: Cloud ONTAP for AWS \(BYOL\)](#)

Ways to encrypt Cloud ONTAP data

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

Cloud ONTAP encryption

You can protect your data from unauthorized access by using data-at-rest encryption provided by Cloud ONTAP. 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. Cloud ONTAP connects to key managers using a TLS connection and communicates using the Key Management Interoperability Protocol (KMIP).

Cloud ONTAP 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 a Cloud ONTAP 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 a key management infrastructure to use Cloud ONTAP encryption and Cloud Manager must be configured as an intermediate CA. See the [OnCommand Cloud Manager 2.1 Installation and Setup Guide](#) for more details.

Amazon EBS encryption

Amazon EBS encryption also protects your data-at-rest. However, AWS handles key management for you. This is a good option if you want added security, but do not need to control your own key management infrastructure. Refer to AWS documentation for more information.

[Amazon Web Services \(AWS\) Documentation: EBS Encryption](#)

Considerations for choosing an underlying EBS disk type

When you launch a Cloud ONTAP instance, you need to choose the underlying EBS disk type for user data: either General Purpose (SSD) disks or Magnetic disks. The differences between the two include cost, performance, and maximum capacity.

At a high level, General Purpose (SSD) disks are a good choice when performance is more important than cost (the data is frequently accessed). Magnetic disks are a good choice when cost is more important than performance (the data is infrequently accessed). For details about EBS performance, see [AWS Documentation: EBS Volume Types](#).

In addition to cost and performance, you must take maximum storage capacity into consideration if you are using Cloud ONTAP Premium or Cloud ONTAP BYOL. The EBS raw capacity limit is higher when you use General Purpose (SSD) disks. For details, see [Cloud ONTAP configurations](#) on page 18.

Considerations for choosing EBS disk size

You must choose the EBS disk size to use in an aggregate when you launch a Cloud ONTAP instance and when you use the advanced allocation option. You should consider the disk size carefully because it impacts cost, performance, and total volume and system capacity.

When you launch a Cloud ONTAP instance, you must choose the default EBS 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 an EBS disk size different from the default by using the advanced allocation option.

[How you can provision Cloud ONTAP storage in Cloud Manager](#) on page 29

When choosing disk size, you should take several factors into consideration. The disk size impacts how much you pay for AWS storage, the size of volumes that you can create in an aggregate, the total capacity available to Cloud ONTAP, and performance, if you use General Purpose (SSD) disks.

Different disk sizes are available for Magnetic disks and for General Purpose (SSD) disks. Note that all EBS disks in an aggregate must be the same size.

Considerations for choosing Magnetic disk size

When you choose a disk size for Magnetic disks, you size your aggregates for the *capacity* that you need. You can choose from 100 GB, 500 GB, or 1 TB disks. For more information about Magnetic disks, see [AWS Documentation: EBS Volume Types](#).

Considerations for choosing General Purpose (SSD) disk size

When you choose a disk size for General Purpose (SSD) disks, you size your aggregates for the capacity *and the performance* that you need. You can choose from the following disk sizes:

100 GB

Provides a small amount of storage with lower performance. You might choose this size to start out with something small or if you have low performance requirements.

500 GB

Provides the best price to performance ratio.

1 TB or 2 TB

Provides higher sustained performance.

4 TB or 8 TB

Provides the best sustained performance.

Note: Larger aggregates can enhance the value of NetApp storage efficiency features (deduplication and compression), which work at the aggregate level.

Although you pay for the *amount* of storage that you buy, you should be aware of the *performance* differences between these disks. To understand the relationship between size and IOPS, see [AWS Documentation: EBS Volume Types](#).

You should take the following into consideration when looking at the performance of EBS disks:

- In a FAS storage system, more spindles is better, but that is not always the case with General Purpose (SSD) disks.
You can get better sustained performance from larger disks and you can get a higher maximum burst duration and less time to refill an empty credit balance.
- 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 (for example, r3.2xlarge) can reach its bandwidth limit.

Ultimately, you should choose the disk size that gives you the *sustained* performance that you need.

What volume usage profiles are

Cloud ONTAP and clustered Data ONTAP include 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 from usage profiles that enable or disable thin provisioning, deduplication, and compression. You should learn more about these profiles to help you decide which to use.

Cloud Manager provides three usage profiles:

Usage profile	Description	Efficiency features
Highest performance	Recommended for applications that require low latency	None
Performance with efficiency	Provides good performance with NetApp storage efficiency	Thin provisioning and deduplication
Most efficient	Best for storing a large amount of data	Thin provisioning, deduplication, and compression

NetApp efficiency features provide the following benefits:

Thin provisioning

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

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

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

Related information

[NetApp Storage Efficiency: Overview](#)

AWS network information worksheet

When you launch a Cloud ONTAP instance, you need to specify the AWS region, VPC, subnet, and security group for the instance. You can use a worksheet to collect the information from your administrator.

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

Launching Cloud ONTAP instances

You launch a Cloud ONTAP instance by creating a working environment in Cloud Manager. If you launch a Cloud ONTAP pay-as-you-go instance in a tenant that is not linked to a NetApp Support Site account, you should register it with NetApp to enable support.

Creating a Cloud ONTAP working environment

If you want to launch a Cloud ONTAP instance in AWS, you need to create a Cloud ONTAP 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.
[Preparing to launch Cloud ONTAP instances](#) on page 15
- If you want to launch a Cloud ONTAP BYOL instance, you must have the license key. If you do not have it, [NetApp Software License Search](#) contains the instructions for obtaining your license key.
- If you want to use CIFS, you must have set up DNS and Active Directory. For details about this requirement, see the [OnCommand Cloud Manager 2.1 Installation and Setup Guide](#).

Steps

1. On the **Working Environments** page, click **Add environment**.

- Under **Create**, select **Cloud ONTAP**.
- On the **Details** page, enter a name and description for the working environment, add AWS tags if needed, 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
Name	Cloud Manager uses the working environment name to name both the Cloud 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.
AWS tags	AWS tags are metadata for your AWS resources. Cloud Manager adds the tags to the Cloud ONTAP instance and each AWS resource associated with the instance. AWS Documentation: Tagging your Amazon EC2 Resources

Note: If AWS keys were not specified for your Cloud Manager account, you are prompted to enter them after you click **Continue**. You need to enter them before you can proceed.

- On the **Data Security** page, choose no data encryption, Cloud ONTAP-managed encryption, or AWS-managed encryption.

[Ways to encrypt Cloud ONTAP data](#) on page 18

Note: If Cloud Manager was not set up for encryption, the Cloud Manager Admin must follow the steps in the [OnCommand Cloud Manager 2.1 Installation and Setup Guide](#).

- If you chose Cloud ONTAP encryption, select one to four key managers, select the certificate of the CA that signed the server certificate for each key manager, and then click **Continue**.

Note: The key manager CA certificate is for all selected key managers, which means the same certificate authority (CA) must have signed the server certificate for each key manager.

- On the **VPC** page, enter the network information that you recorded in the AWS worksheet, select the checkbox to confirm network connectivity, and then click **Continue**.

The following image shows the VPC page filled out:

The screenshot displays the VPC configuration interface. At the top, there are two dropdown menus: 'AWS Region' set to 'US East | N. Virginia' and 'VPC' set to 'vpc-ead2918f | 10.0.0.0/16'. Below these, a card shows details for the selected VPC: 'vpc-ead2918f', '10.0.0.0/16', and 'Name: VPC1', with a 'View Tags' link. Underneath the card, there are two more dropdowns: 'Subnet' set to '10.0.0.0/24' and 'Security group' set to 'Use generated Security Group'. At the bottom, a checkbox labeled 'Networking connectivity is verified between the Cloud Manager server and the selected VPC.' is checked.

- On the **Licensing** page, change the Cloud ONTAP version as needed, select a license and an instance type, and then click **Continue**.

[Cloud ONTAP configurations](#) on page 18

If your needs change after you launch the instance, you can modify the license or instance type later. See [Changing the configuration of Cloud ONTAP instances](#) on page 43.

8. If the **NetApp Support Site credentials** page is displayed, enter your NetApp Support Site credentials to enable Cloud Manager to automatically register future Cloud ONTAP pay-as-you-go instances created in the tenant.

Otherwise, you need to register each instance manually.

9. On the **Cloud ONTAP Settings** page, specify system credentials, the underlying AWS disk type, and the default disk size:

Field	Description
Credentials	These are the credentials for the Cloud ONTAP cluster admin account. You can use these credentials to connect to Cloud ONTAP through OnCommand System Manager or its CLI.
Underlying AWS Disk	For guidance on choosing a disk type, see Considerations for choosing an underlying EBS disk type on page 19. For guidance on choosing a disk size, see Considerations for choosing EBS disk size on page 19. Note the following: - You cannot change the underlying EBS disk type or the default disk size after you create the system. - The disk size is the default size 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 EBS disk size by using the advanced allocation option.

10. On the **Create Volume** page, enter details for the new volume, and then click **Continue**.

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. For an example, see How you can provision Cloud ONTAP storage in Cloud Manager on page 29.
Access control (for NFS only)	An export policy defines the EC2 instances 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 <i>access control lists</i> 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 <i>domain\username</i> .
Usage Profile	Usage profiles define the NetApp storage efficiency features that are enabled for a volume. For more information, see Understanding volume usage profiles on page 20.

Field	Description
Protection	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.

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

Details

Volume Name:

Protocol:

Size (GB): *

Share name:

Permissions:

Users / Groups:

Valid users and groups separated by a semicolon

Usage Profile

☐ **Highest Performance**
Recommended for applications requiring lowest latency.

☒ **Performance with Efficiency**
Good performance with ONTAP storage efficiency™.

☐ **Most Efficient**
Best for storing the most data.

For more information regarding usage profiles, see OnCommand Cloud Manager documentation.

Protection

Snapshot Policy:

- Every **hour**, keep the last **6** copies
- Once a **day**, keep the last **2** copies
- Once a **week**, keep the last **2** copies

11. If you chose the CIFS protocol, set up a CIFS server on the **Cloud ONTAP CIFS Setup** page:

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 ONTAP Storage Virtual Machine (SVM). In most cases, the domain is the same as the AD domain.

12. On the **Review & Approve** page, review and confirm your selections:
- Review details about the configuration.
 - Click **More information** to review details about support and the AWS resources that Cloud Manager will purchase.
 - Select the **I understand...** check boxes.

- d. Click **Go**.

Result

Cloud Manager launches the Cloud ONTAP instance. The working environment should be ready in approximately 25 minutes. You can track the progress in the timeline.

If you experience any issues launching the Cloud ONTAP instance, verify that your AWS environment meets the requirements. For details, see the [OnCommand Cloud Manager 2.1 Installation and Setup Guide](#).

For additional help, go to [NetApp Cloud ONTAP Support](#).

After you finish

- If you launched a Cloud ONTAP pay-as-you-go instance and the tenant is not linked to a NetApp Support Site account, manually register the instance with NetApp to enable support. Support from NetApp is included with your Cloud ONTAP instance. To activate support, you must first register the instance with NetApp. [Registering Cloud ONTAP instances](#) on page 25
- 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.
- If this is the first Cloud ONTAP instance launched in AWS, remind your administrator to finish setting up AWS billing and cost requirements by enabling the **WorkingEnvironmentId** tag. This tag is not available in AWS until after you create your first Cloud ONTAP working environment under the AWS payer account. For details, see the [OnCommand Cloud Manager 2.1 Installation and Setup Guide](#).

Registering Cloud ONTAP pay-as-you-go instances

Support from NetApp is included with Cloud ONTAP Explore, Standard, and Premium instances, but you must first activate that support by registering the instances with NetApp, if you have not set up automatic registration.

Before you begin

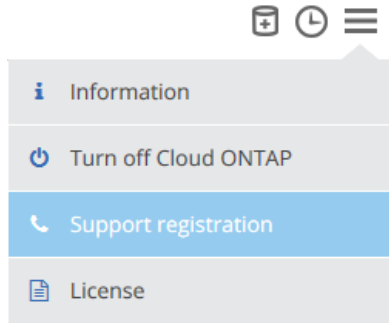
The host from which you are logged in to Cloud Manager must have Internet access. If it does not, you can register from another location by going to [NetApp Cloud ONTAP Registration](#).

About this task

If a tenant is linked to a NetApp Support Site account, Cloud Manager automatically registers the instance with that account. However, if the tenant is not linked to an account, then you should register instances with NetApp after you launch them.

Steps

1. On the **Working Environments** page, double-click the name of the instance that you want to register.
2. In the **Cloud ONTAP Storage** pane, click the menu icon, and then click **Support registration**:



The information that you need to register an instance is displayed:

- Instance ID
 - Serial number
 - Account ID
3. To automatically register future instances in the tenant, click the link to enter your NetApp Support Site credentials.
 4. To register this instance with NetApp support, click the link and then click **Register to NetApp support**.
Following this link automatically completes the instance ID, serial number, and account ID in the registration form.
 5. Follow the instructions to register your Cloud ONTAP instance.

Setting up Cloud ONTAP

After you launch Cloud ONTAP, you can set it up by synchronizing the system time using NTP, and then by optionally setting up iSCSI, configuring AutoSupport and EMS, and changing the backup location of cluster configuration files to an existing FTP or HTTP server. You must perform these tasks from either System Manager or the CLI.

Task	Description
Synchronize the system time using NTP	Cloud ONTAP needs a Network Time Protocol (NTP) server to synchronize the time with clients and peered clusters. Problems can occur when the time is inaccurate. You can configure the NTP server using System Manager or the CLI. For instructions, see the System Manager Help or the Clustered Data ONTAP 8.3 System Administration Guide .
Optional: Set up iSCSI	If you want to use iSCSI, you must start the iSCSI server. Setting up Cloud ONTAP for iSCSI on page 29
Optional: Configure AutoSupport	AutoSupport proactively monitors the health of your system and automatically sends messages to NetApp technical support by default. If you want messages sent to your internal support organization, you must set the correct options and have a valid mail host. If the Cloud Manager Admin added a proxy server to Cloud Manager before you launched your instance, Cloud ONTAP is configured to use that proxy server for AutoSupport messages. You can configure AutoSupport using System Manager or the CLI. For instructions, see the System Manager Help or the Clustered Data ONTAP 8.3 System Administration Guide .

Task	Description
Optional: Configure EMS	The Event Management System (EMS) collects and displays information about events that occur on a Cloud ONTAP system. 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 Clustered Data ONTAP 8.3 EMS Configuration Express Guide.
Optional: Change the backup location of configuration files	Cloud ONTAP automatically creates configuration backup files that contain information about the configurable options that it needs to operate properly. By default, Cloud 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 Clustered Data ONTAP 8.3 System Administration Guide.

Related tasks

[Connecting to OnCommand System Manager](#) on page 27

[Connecting to the Cloud ONTAP CLI](#) on page 28

Connecting to OnCommand System Manager

You might need to perform some Cloud ONTAP tasks from OnCommand System Manager, which is a browser-based management tool that runs on the Cloud ONTAP instance. For example, you need to use System Manager to configure the iSCSI protocol.

Before you begin

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

Steps

1. From the **Working Environments** page, double-click the name of the instance that you want to manage with System Manager.
2. In the **Cloud ONTAP Storage** pane, 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 ONTAP.

Connecting to the Cloud ONTAP CLI

The Cloud 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 ONTAP must have a network connection to the Cloud ONTAP instance. For example, you might need to use SSH from the Cloud Manager instance or from a jump host in AWS.

Steps

1. In Cloud Manager, identify the IP address of the cluster management interface:
 - a. On the **Working Environments** page, double-click the name of the instance.
 - b. In the **Cloud ONTAP Storage** pane, click the menu icon, and then click **Information**.
 - c. Copy the cluster management IP address:

Information

Cluster Management :	192.168.111.5
----------------------	---------------

Intercluster :	192.168.111.217
----------------	-----------------

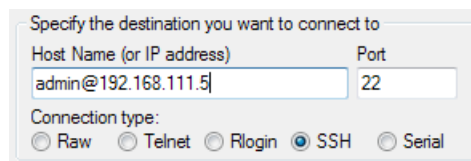
Node Management :	192.168.111.50
-------------------	----------------

Data (iscsi) :	192.168.111.219
----------------	-----------------

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: :>
```

Setting up Cloud ONTAP for iSCSI

If you want to provision iSCSI LUNs for Cloud ONTAP, you need to start the iSCSI server from System Manager.

About this task

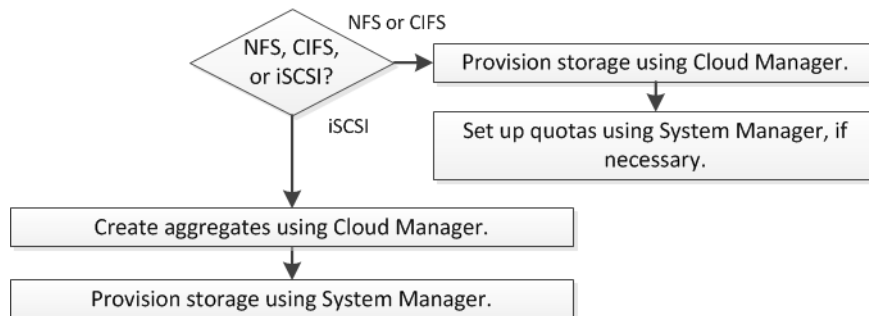
You do not need to create an iSCSI data LIF because Cloud Manager created one by default when you launched the Cloud ONTAP instance.

Steps

1. Log in to System Manager.
[Connecting to OnCommand System Manager](#) on page 27
2. Select the Storage Virtual Machine and click **Configuration** > **Protocols** > **iSCSI**.
3. Click **Start**.

Provisioning storage

You can provision additional NFS and CIFS storage for your Cloud ONTAP instances from Cloud Manager by managing volumes and aggregates. If you need to create iSCSI storage, you should do so from System Manager.



How you can provision Cloud ONTAP storage in Cloud Manager

Cloud Manager makes storage provisioning easy by purchasing EBS 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.

How Cloud Manager provisions storage using the simple provisioning option

Aggregates provide EBS storage to Cloud ONTAP volumes. Cloud Manager creates aggregates for you when you launch an instance, and when you provision additional volumes by clicking the new volume icon .

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 EBS disks for that aggregate (up to a total of four disks).
- It purchases up to four EBS disks for a new aggregate and places the volume on that aggregate.

Note: Although aggregates can include up to six EBS disks, Cloud Manager does not create new volumes on the last two disks. It uses the last two disks for existing volumes that need room to grow (Cloud Manager sets the autosize mode to *grow* for all read-write volumes).

Cloud Manager determines where to place a new volume by looking at several factors: an aggregate's maximum size, whether thin provisioning is enabled, an aggregate's free space threshold (10 percent by default), and an aggregate's overcommitment threshold (500 percent by default).

Note: The Cloud Manager Admin can modify these thresholds. For details, see the [OnCommand Cloud Manager 2.1 Administration Guide](#).

The size of the volume that you can create largely depends on whether you enable thin provisioning. For example, if you create a volume using the Highest Performance usage profile, which does not enable thin provisioning, the maximum size for the volume is approximately 1.51 TB. This is because 12 to 14 percent of the new aggregate's capacity is reserved for overhead and 10 percent is reserved for free space. If you want to create a larger volume, you either need to choose a profile that enables thin provisioning, or you need to create an aggregate yourself, which enables you to add up to six EBS disks in an aggregate and use disks larger than 500 GB.

How you can provision storage using the advanced allocation option

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 contain up to six disks, add EBS disks to an existing aggregate, and create volumes in specific aggregates.

The benefit in managing aggregates yourself is that you can choose an underlying EBS disk size that is different from the default size. Note that all EBS disks in an aggregate must be the same size.

Related tasks

[Managing existing aggregates](#) on page 36

Provisioning volumes

If you need more storage after you launch a Cloud ONTAP instance, you can provision new NFS and CIFS volumes from Cloud Manager.

Before you begin

If you want to use CIFS, you must have set up DNS and Active Directory. For details about this requirement, see the [OnCommand Cloud Manager 2.1 Installation and Setup Guide](#).

Steps

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

To...	Do this...
Create a new volume and let Cloud Manager choose the containing aggregate	Click the create new volume icon: 
Create a new volume on a specific aggregate	a. Click the menu icon, and then click Advanced > Advanced allocation. b. Select an aggregate. c. Click Create volume.

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

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. For an example, see How you can provision Cloud ONTAP storage in Cloud Manager on page 29.
Access control (for NFS only)	An export policy defines the EC2 instances 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 <i>access control lists</i> 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 <i>domain\username</i> .
Usage Profile	Usage profiles define the NetApp storage efficiency features that are enabled for a volume. For more information, see Understanding volume usage profiles on page 20.
Protection	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.

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.
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 ONTAP Storage Virtual Machine (SVM). In most cases, the domain is the same as the AD domain.

5. When prompted, click **Approve**.

Result

Cloud 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 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 EBS 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 ONTAP instance on which you want to manage aggregates.
2. In the **Cloud ONTAP Storage** pane, click the menu icon, and then click **Advanced > Advanced allocation**.
3. Click the + icon, and then create the aggregate:
 - a. Enter an aggregate name, select the number of EBS disks, and then select the EBS disk size.
Considerations for choosing EBS disk size on page 19
 - b. Click **Create**, and then click **Approve and Purchase**.

Related tasks

Managing existing aggregates on page 36

Provisioning iSCSI LUNs

If you want to create iSCSI LUNs, you need to do so from System Manager.

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.
Managing aggregates on page 36

Steps

1. Log in to System Manager.
Connecting to OnCommand System Manager on page 27
2. Select the Storage Virtual Machine and click **Storage > LUNs > Create**.

3. Follow the prompts in the **Create LUN** wizard to create the LUN.
4. Connect to the LUN from the host.

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

Related information

[NetApp Documentation: Host Utilities \(current releases\)](#)

Managing Cloud ONTAP

You might need to perform several management and maintenance tasks as you use Cloud ONTAP. For example, you might need to upgrade Cloud ONTAP software, change license and instance types, and manage encryption settings.

Monitoring AWS storage and compute costs

You can view the cost associated with running a Cloud ONTAP instance in AWS. The monthly cost consists of the compute purchased from AWS to run Cloud ONTAP and the disks purchased from AWS for Cloud ONTAP use.

Before you begin

The AWS payer account must meet specific billing and cost requirements and your Cloud Manager account must be associated with the AWS cost S3 bucket. For details, see the [OnCommand Cloud Manager 2.1 Installation and Setup Guide](#).

About this task

Cloud Manager updates the storage and compute costs every 12 hours.

You should refer to AWS for final cost details.

Step

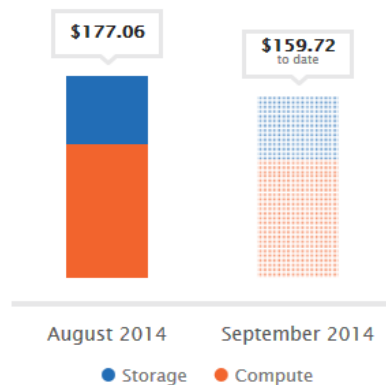
1. On the **Working Environments** page, select the Cloud ONTAP instance and then click **Cost**.

The Cost page displays costs for the current and previous months and shows your storage costs savings, if you enabled NetApp's efficiency features on volumes. If the cost information is not available, verify that the Cloud Manager Admin met the prerequisites listed earlier.

The following image shows an example of the AWS costs per month:

So far this month you've spent \$159.72

Last updated: 9/1/2014 2:23 AM

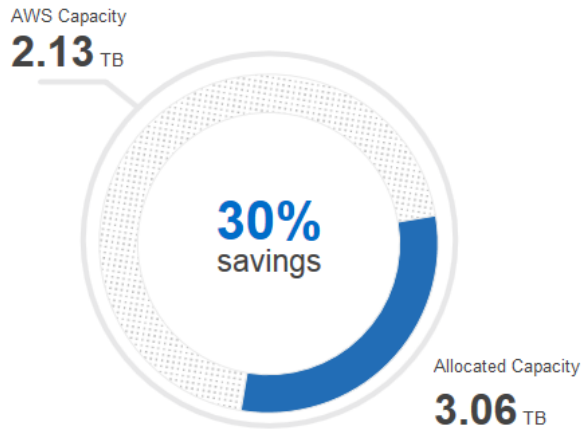


The following image shows an example of storage cost savings:

30% storage cost savings

Your savings are enabled by ONTAP's advanced technologies such as Thin Provisioning, Deduplication and Compression. The savings are based on the difference between your allocated capacity (3.06 TB) and the purchased AWS capacity (only 2.13 TB).

[Show calculation](#)



Managing storage

You can manage Cloud ONTAP volumes and aggregates as your storage needs change, and you can modify the CIFS server, if your configuration changed.

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 name of the Cloud ONTAP instance 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 .
Edit a volume (read-write volumes only)	a. Select a volume, and then click Edit. b. Modify the volume's Snapshot policy, NFS access control list, or share permissions, and then click Update.

Task	Action
Clone a volume	- Select a volume, and then click Clone. - Modify the clone name as needed, and then click Clone. This process creates a <i>FlexClone</i> volume. To learn about <i>FlexClone</i> volumes, see the Clustered Data ONTAP 8.3 Logical Storage Management Guide.
Restore data from a Snapshot copy to a new volume	- Select a volume, and then click Restore from Snapshot copy. - Select a Snapshot copy, enter a name for the new volume, and then click Restore.
Delete a volume	- Select a volume, and then click Delete. - Click Delete again to confirm.

Related tasks

[Provisioning volumes](#) on page 30

Managing existing aggregates

If you want to manage existing aggregates yourself, you can add disks to aggregates, view information about aggregates, and delete 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.

[Connecting to OnCommand System Manager](#) on page 27

Steps

- On the **Working Environments** page, double-click the name of the Cloud ONTAP instance on which you want to manage aggregates.
- In the **Cloud ONTAP Storage** pane, click the menu icon, and then click **Advanced > Advanced allocation**.
- Manage your aggregates:

Task	Action
View information about an aggregate	Select an aggregate, and then click Info .
Add disks to an aggregate	- Select an aggregate, and then click Add AWS disks. - Select the number of disks that you want to add, and then click Add.

Task	Action
Delete an aggregate	a. Select an aggregate that does not contain any volumes, and then click Delete. b. Click Delete again to confirm.

Related tasks

[Creating aggregates](#) on page 32

Modifying the CIFS server

If you change your DNS servers or Active Directory domain, you need to modify the CIFS server in Cloud 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:

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 ONTAP Storage Virtual Machine (SVM). In most cases, the domain is the same as the AD domain.

3. Click **Save**.

Result

Cloud ONTAP updates the CIFS server with the changes.

Managing the state of Cloud ONTAP instances

You can stop and start Cloud ONTAP instances from Cloud Manager to manage your EC2 costs. You can also terminate instances, if you no longer need them.

Scheduling automatic shutdowns of Cloud ONTAP instances

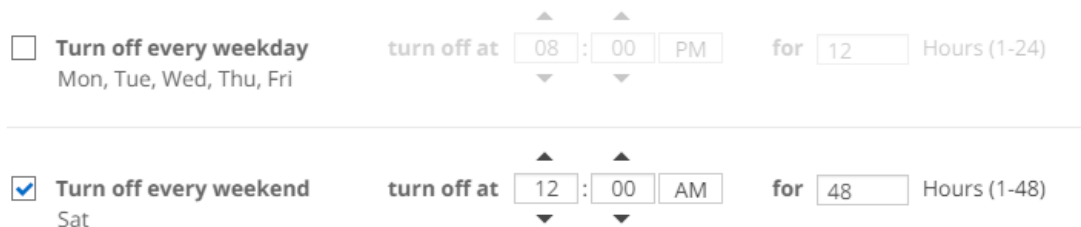
You might want to shut down Cloud ONTAP instances during specific time intervals to lower your AWS costs. Rather than do this manually, you can configure Cloud Manager to automatically shut down and then restart instances at specific times.

Steps

1. From the working environment, click the clock icon: 
2. Specify the shutdown schedule:
 - a. Choose whether you want to shut down the instance every weekday, every weekend, or both.
 - b. Specify when you want to turn off the instance and for how long you want it turned off.

Example

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



☐ **Turn off every weekday**
Mon, Tue, Wed, Thu, Fri turn off at 08 : 00 PM for 12 Hours (1-24)

☒ **Turn off every weekend**
Sat turn off at 12 : 00 AM for 48 Hours (1-48)

3. Click **Save**.

Result

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

Stopping a Cloud ONTAP instance

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

Steps

1. From the working environment, click the menu icon and then click **Turn off Cloud ONTAP**.
2. Keep the option to create EBS snapshots enabled because the snapshots can enable system recovery.
3. Click **Turn off**.

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

Deleting a Cloud ONTAP working environment

It is best to terminate a Cloud ONTAP instance from Cloud Manager, rather than from AWS. For example, if you terminate a licensed Cloud ONTAP instance from AWS, you cannot use the license

key for another instance. You must delete the Cloud ONTAP working environment from Cloud Manager to release the license.

About this task

When you delete a working environment, Cloud Manager terminates the instance, deletes EBS disks, and EBS snapshots.

Important: Cloud ONTAP instances have termination protection enabled to help prevent accidental termination from AWS. However, if you do terminate a Cloud 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

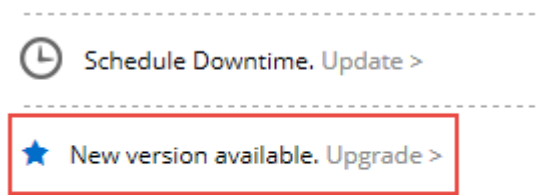
1. From the working environment, click the **Delete** icon.
2. Select **I understand...** and then click **Delete**.

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

Updating Cloud ONTAP software

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

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



You can start the upgrade process from this notification, which automates the upgrade process by obtaining the software image from an S3 bucket, installing the image, and then restarting the system.

Advanced options for software updates

Cloud Manager also provides the following advanced options for updating Cloud 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.
- 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.

Transitioning Cloud ONTAP to an earlier release in the same release family (8.3.x to 8.3.y) is referred to as a *downgrade*. You can downgrade without assistance when downgrading new or test clusters, but you should call technical support if you want to downgrade a production cluster.

Preparing to update Cloud ONTAP software

Before performing an upgrade or downgrade, you must verify that the cluster is ready and make any required configuration changes.

Steps

1. [Review version requirements for SnapMirror source and destination systems](#) on page 40
If any of your systems have active SnapMirror relationships, you should review SnapMirror version requirements before you upgrade. The version requirements have changed starting with the 8.3 release.
2. [Suspend SnapMirror transfers](#) on page 40
If a Cloud ONTAP system has active SnapMirror relationships, it is best to suspend transfers before you update the Cloud ONTAP software. Suspending the transfers prevents SnapMirror failures. You must suspend the transfers from the destination system.
3. [Verify that aggregates are online](#) on page 41
Cloud ONTAP aggregates 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.

Version requirements for SnapMirror source and destination systems

If any of your systems have active SnapMirror relationships, you should review SnapMirror version requirements before you upgrade. The version requirements have changed starting with the 8.3 release.

If you want to replicate data between Cloud ONTAP systems and clustered Data ONTAP systems running a version prior to 8.3, then the destination system must run a version that is equal to or later than that of the source system. This requirement applies to SnapMirror. It does not apply to SnapVault.

For example, replication from a Cloud ONTAP 8.3 system to a clustered Data ONTAP 8.2.3 system is not supported because the destination is running an earlier version. Conversely, replication from an 8.2.3 system to an 8.3 system is supported because the destination is running a later version.

Starting with clustered Data ONTAP 8.3, there are no version requirements for source and destination systems in SnapMirror relationships. The systems can run different versions, if they are both running 8.3 or later.

Suspending SnapMirror transfers

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

Steps

1. Log in to System Manager from the destination system.
[Connecting to OnCommand System Manager](#) on page 27
2. Select the Storage Virtual Machine (SVM) and click **Protection**.
3. Select the relationship and click **Operations > Quiesce**.

Verifying that aggregates are online

Cloud ONTAP aggregates 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.

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.

aggr1		
Aggregate Capacity:	88.57 GB	
Used Aggregate Capacity:	1.07 GB	
Volumes:	2	▼
AWS Disks:	1	▼
State:	online	

3. If the aggregate is offline, use System Manager to bring the aggregate online:
 - a. Log in to System Manager.
[Connecting to OnCommand System Manager](#) on page 27
 - b. Select the cluster, and then click **Storage > Aggregates**.
 - c. Select the aggregate, and then click **Status > Online**.

Upgrading Cloud ONTAP to the latest version

You can upgrade to the latest version of Cloud ONTAP directly from Cloud Manager. Cloud Manager notifies you when a new version is available.

Before you begin

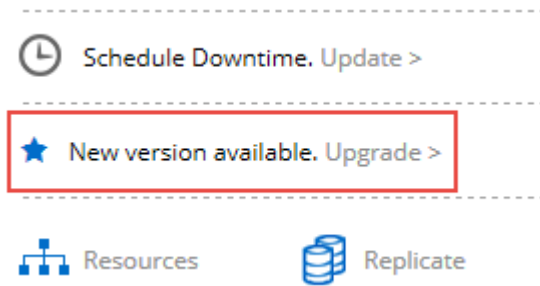
Cloud Manager operations such as volume or aggregate creation must not be in progress for the Cloud ONTAP system.

About this task

The upgrade process takes the Cloud ONTAP system offline for up to 25 minutes, during which I/O is interrupted.

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 Cloud ONTAP 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. The Cloud ONTAP system and working environment should be available in approximately 25 minutes.

After you finish

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

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

You can place the Cloud 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.

About this task

The upgrade or downgrade process takes the Cloud ONTAP system offline for up to 25 minutes, during which I/O is interrupted.

Steps

1. Set up an HTTP server or FTP server that can host the Cloud ONTAP software image.
If you have a VPN connection to the VPC, you can place the Cloud 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 AWS.
2. If you use your own security group for Cloud ONTAP instances, ensure that the outbound rules allow HTTP or FTP connections so Cloud ONTAP can access the software image.
Note: The predefined Cloud ONTAP security group allows outbound HTTP and FTP connections by default.
3. Obtain the software image.
[NetApp Downloads: Software](#)
4. Copy the software image to the directory on the HTTP or FTP server from which the file will be served.

5. From the working environment in Cloud Manager, click the menu icon, and then click **Advanced > Update Cloud ONTAP software**.
6. On the **Update Cloud ONTAP software** page, choose **Select an image available from a URL**, enter the URL, and then click **Change Image**.
7. Click **Proceed** to confirm.

Result

Cloud Manager starts the software update. The Cloud ONTAP system and working environment should be available in approximately 25 minutes.

After you finish

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

Downgrading Cloud ONTAP by using a local image

Each Cloud 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 ONTAP, if you are experiencing issues with the current image.

About this task

The downgrade process takes the Cloud ONTAP system offline for up to 25 minutes, during which time I/O is interrupted.

Steps

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

Result

Cloud Manager starts the software update. The Cloud ONTAP system and working environment should be available in approximately 25 minutes.

After you finish

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

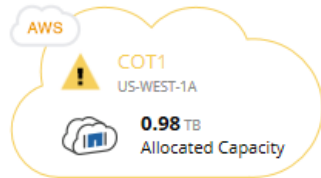
Changing the configuration of Cloud ONTAP instances

You might need to change the configuration of a Cloud ONTAP instance as your storage needs change. You can change between pay-as-you-go configurations, change the instance type, move to an alternate subscription, and view details about the configuration and license.

How Cloud Manager enforces Cloud ONTAP BYOL subscriptions

Cloud Manager warns you 30 days before your subscription to a Cloud ONTAP BYOL instance is due to expire, and again when the subscription expires. If you do not renew the subscription in time, Cloud Manager stops the instance.

Cloud Manager displays the warnings in the Working Environments page:



You can select the working environment to review the message.

If Cloud Manager stops an instance after the subscription expires, you must renew the subscription and then restart the instance. You cannot restart the instance until you renew the subscription.

If you do not want to renew your subscription, but you want to retrieve data from the instance, then you must contact NetApp technical support.

Related information

[NetApp Global Sales and Subscription Contacts](#)

Viewing Cloud ONTAP configuration details

You might need to view the configuration of a Cloud ONTAP instance. For example, you must know the cluster management IP address to connect to Cloud ONTAP using SSH. You might also want to see the version of Cloud ONTAP that you are running. Or you might need to find your Cloud ONTAP serial number or account ID.

Steps

1. From the working environment, click the menu icon and then click **Information**.
The IP addresses of the various interfaces and the user who created the working environment appears. If you want to understand more about the interfaces, see the [Clustered Data ONTAP 8.3 Network Management Guide](#).
2. To view more information about the instance, click **Advanced Information**.
The advanced information appears and displays information such as the instance ID, serial number, and account ID.

Viewing Cloud ONTAP license information

You can view licensing information about a Cloud ONTAP instance, which includes the license type, instance type, capacity limit, and current attached and allocated capacities.

Step

1. From the working environment, click the menu icon and then click **License**.

Changing a Cloud ONTAP instance type

You can choose from several instance types when you launch a Cloud ONTAP instance. After you launch the instance, you can change the instance type at any time if you determine that it is undersized or oversized for your requirements.

About this task

- The operation restarts Cloud ONTAP, which means that I/O is interrupted.
- Changing the instance type affects AWS service charges.

Steps

1. From the working environment, click the menu icon, and then click **Change AWS instance type**.
2. Select an instance type, select the check box to confirm that you understand the implications of changing the instance type, and then click **Change**.

Result

Cloud Manager stops the instance and sends an AWS request to change the instance type.

Changing between pay-as-you-go configurations

After you launch a pay-as-you-go Cloud ONTAP instance, you can change between the Explore, Standard, and Premium configurations at any time by modifying the license. Changing the license increases or decreases the EBS raw capacity limit and enables you to choose from different EC2 instance types.

About this task

Changing between pay-as-you-go configurations is possible only with the new Cloud ONTAP products introduced with Cloud ONTAP 8.3.1. If you want to move an existing 8.3 instance to one of the new product licenses, you must launch a new instance and then replicate the data.

[Moving to an alternate Cloud ONTAP subscription](#) on page 45

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

- The operation restarts Cloud ONTAP, which means that I/O is interrupted.
- Changing the instance type affects AWS service charges.

Steps

1. From the working environment, click the menu icon, and then click **License**.
2. Click **Change License**.
3. Select a license type and instance type, select the check box to confirm that you understand the implications of changing the instance type, and then click **OK**.

Result

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

Moving to an alternate Cloud ONTAP subscription

If you want to move to one of the Cloud ONTAP products introduced with Cloud ONTAP 8.3.1, you can launch a new instance and then replicate data from the existing instance to the new instance. You

can use this same process to move from a pay-as-you-go subscription to a BYOL subscription, and vice versa.

Steps

1. Launch a new Cloud ONTAP instance by creating a working environment.
Creating a Cloud ONTAP working environment on page 21
2. If you launched a Cloud ONTAP pay-as-you-go instance and the tenant does not have a NetApp Support Site account assigned to it, manually register the instance with NetApp.
Support from NetApp is included with your Cloud ONTAP instance. To activate support, you must first register the instance with NetApp.
Registering Cloud ONTAP instances on page 25
3. Set up one-time data replication between the systems for each volume that you must replicate.
Replicating data between systems on page 57
4. Terminate the Cloud ONTAP instance that you no longer need by deleting the original working environment.
Deleting a Cloud ONTAP working environment on page 38

Adding existing Cloud ONTAP instances to Cloud Manager

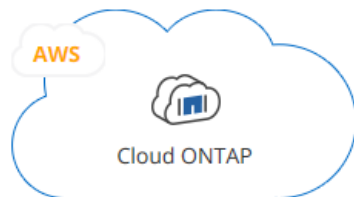
You can discover and add existing Cloud ONTAP instances to Cloud Manager. You might do this if your Cloud Manager instance became unusable and you launched a new instance, but you could not restore all Cloud ONTAP instances from a recent Cloud Manager backup.

Before you begin

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

Steps

1. On the **Working Environments** page, click **Add environment**.
2. Under **Discover**, select **Cloud ONTAP**.



3. On the **Region** page, choose the region where the instance is running, and then select the instance.
4. On the **Credentials** page, enter the password for the Cloud ONTAP admin user, and then click **Go**.

Result

Cloud Manager adds the Cloud ONTAP instance to the tenant.

Managing Cloud ONTAP encryption

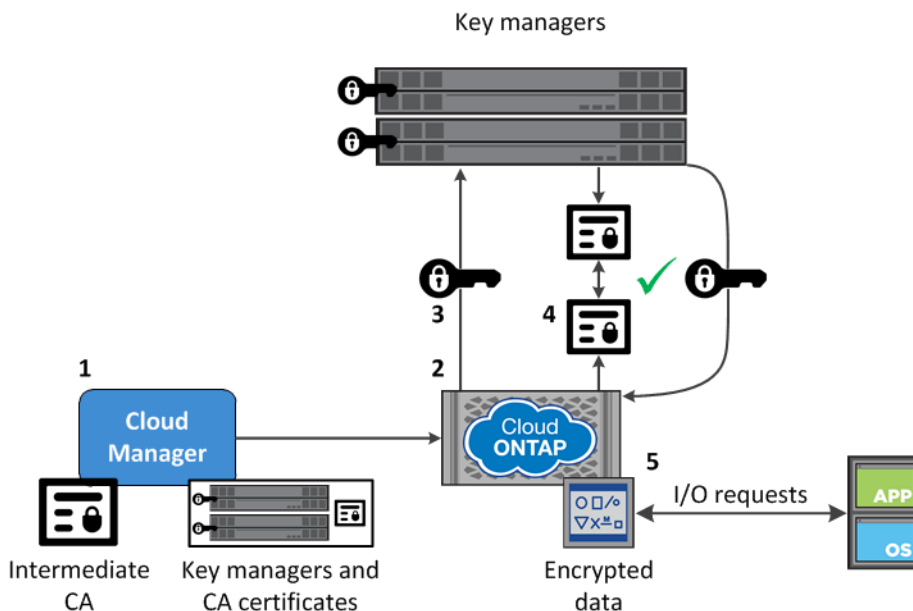
If you enabled Cloud ONTAP encryption, you can manage the key managers and certificates associated with specific Cloud ONTAP systems. Cloud Manager also enables you to find the encryption keys for aggregates which can help you manage the keys on your key managers.

Note: If you want to manage encryption settings for Cloud Manager, see the [OnCommand Cloud Manager 2.1 Administration Guide](#). Cloud Manager encryption settings include the Cloud Manager certificate, and the key managers and CA certificates available to use with Cloud ONTAP systems. Only the Cloud Manager Admin can manage those settings.

Understanding how Cloud ONTAP encryption works

Understanding how Cloud ONTAP encryption works can help you set up and use the feature.

The following graphic shows the steps and components involved in the encryption process:



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 Cloud ONTAP instances with encryption enabled.
Cloud Manager sets up Cloud ONTAP 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.

Note:

 - Users can enable encryption only when launching a new instance in AWS; it cannot be enabled afterward.
 - All data on the system is encrypted, except for the root aggregate, which does not contain user data.
3. For each aggregate, Cloud ONTAP generates and sends an encryption key to key managers.

- Each time Cloud ONTAP boots, it authenticates with key managers to obtain encryption keys, which are then stored in cache and never displayed in cleartext.
Note: Cloud ONTAP communicates with key managers when it boots and when new aggregates are created. It does not communicate with key managers at any other time.
- 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.

Managing key managers and certificates for Cloud ONTAP

You must update encryption settings for Cloud ONTAP as you make changes in your key management infrastructure and when certificates are about to expire.

Before you begin

You must have enabled Cloud ONTAP encryption when you launched the instance.

Steps

- In the working environment, click the menu icon and then click **Encryption settings**.
- Manage encryption settings as needed:

To perform this task...	Do this...
Configure Cloud ONTAP to use a new key manager	Click the + icon, select the key manager, and click Save . The key manager CA certificate selected for this Cloud ONTAP system must have signed the server certificate for this new key manager.
Stop Cloud ONTAP from using an existing key manager	Select the key manager, click Delete , and then click OK .
View details about certificates	Click View details for either the client certificate or key manager CA certificate.
Renew a client certificate that has expired	Click Renew and then click OK .
Use a different key manager CA certificate	Click Update , select the certificate, and then click Save . The certificate must be for the CA that signed the server certificate for each key manager configured with this Cloud ONTAP system. Those key managers must trust this CA.

Finding the encryption key for an aggregate

Cloud ONTAP creates an encryption key for each aggregate on the system and sends it to key managers. You can view the ID for those keys from Cloud Manager. You might do this before you delete an aggregate or a Cloud ONTAP instance, because the keys are not automatically deleted from key managers. You must delete the keys yourself.

Before you begin

You must have enabled Cloud ONTAP encryption when you launched the instance.

About this task

If you want to find the key ID for an aggregate or Cloud ONTAP instance that you already deleted, you can find the information in the Cloud Manager timeline.

Steps

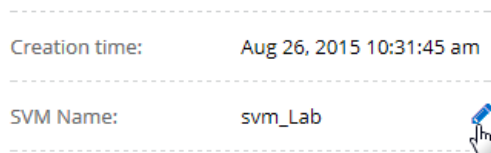
1. In the working environment, click the menu icon, and then click **Advanced > Advanced allocation**.
2. Select the aggregate, and then click **Info**.
The Key ID field shows the first 12 characters of the encryption key.
3. To view the entire encryption key, position your cursor over the first 12 characters of the encryption key.
A tooltip displays the entire contents of the key.
4. To copy the entire encryption key, double-click the first 12 characters, copy the text to your clipboard, and then paste it in a text editor.

Modifying the Storage Virtual Machine name

Cloud Manager automatically names the Storage Virtual Machine (SVM) for a Cloud ONTAP system. 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 Data ONTAP clusters.

Steps

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



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

Changing the password for a Cloud ONTAP instance

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

About this task

Important: 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.

Configuring Cloud ONTAP to send configuration backups to Cloud Manager

You should configure Cloud ONTAP to send configuration backups to Cloud Manager if the target location is currently the NetApp Support instance, or if you added a new working environment to Cloud Manager by discovering an existing Cloud ONTAP instance.

About this task

Cloud ONTAP instances launched from Cloud Manager 2.1 and later automatically send configuration backups to Cloud Manager using HTTPS. Cloud ONTAP instances launched from a previous release of Cloud Manager send the files to the NetApp Support instance. The NetApp Support instance is no longer launched by Cloud Manager starting in version 2.1.

The configuration backup files contain information about the configurable options that Cloud ONTAP needs to operate properly. You can use the files with the help of NetApp technical support to restore a configuration.

Steps

1. From the working environment, click the menu icon and then click **Advanced > Configuration backups**.
2. Click **Set Backup Target**.
3. Click **OK** to confirm.
4. Repeat the steps for other Cloud ONTAP instances.

Result

Cloud ONTAP is now configured to send the configuration backups to Cloud Manager every eight hours.

Discovering and managing Data ONTAP clusters

Cloud Manager can discover the Data ONTAP clusters in your on-premises environment and the clusters that belong to a NetApp Private Storage configuration in Amazon Web Services, Microsoft Azure, or SoftLayer. Discovering these clusters enables you to easily replicate data across your hybrid cloud environment: between on-premises Data ONTAP clusters, Cloud ONTAP systems, and NetApp Private Storage clusters.

Discovering Data ONTAP clusters

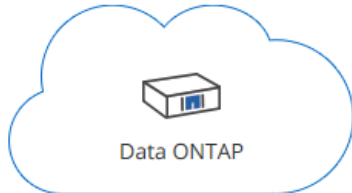
Discovering a Data ONTAP cluster that is in your network or in a NetApp Private Storage configuration enables you to replicate data to and from the cloud.

Before you begin

You must have the cluster management IP address and the password for the admin user account to add the cluster to Cloud Manager.

Steps

1. On the **Working Environments** page, click **Add environment**.
2. Under **Discover**, select **Data ONTAP**.



3. On the **Data ONTAP Cluster Details** page, enter the cluster management IP address and the password for the admin user account, and then select the type of working environment: an on-premises cluster or a NetApp Private Storage configuration.
4. On the **Details** page, enter a name and description for the working environment, and then click **Go**.

Result

Cloud Manager discovers the cluster. You can now create volumes, replicate data to and from the cluster, and launch OnCommand System Manager to perform advanced tasks.

Provisioning volumes for Data ONTAP clusters

Cloud Manager enables you to provision NFS and CIFS volumes on NetApp Private Storage clusters, as well as on-premises Data ONTAP clusters.

Before you begin

NFS or CIFS must be set up on the cluster. You can set up NFS and CIFS using System Manager or the CLI.

Steps

1. On the **Working Environments** page, double-click the name of the Data ONTAP cluster on which you want to provision volumes.
2. Click the create new volume icon.
3. On the **Create New Volume** page, enter details for the volume, and then click **Create**.

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 EC2 instances 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 <i>access control lists</i> 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 <i>domain\username</i> .
Usage Profile	Usage profiles define the NetApp storage efficiency features that are enabled for a volume. For more information, see Understanding volume usage profiles on page 20.
Protection	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.

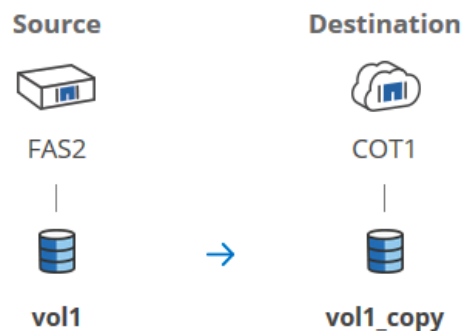
Replicating data to and from the cloud

You can replicate data between Cloud ONTAP systems and Data ONTAP clusters that are in your network or part of a NetApp Private Storage configuration. Cloud Manager uses SnapMirror and SnapVault technology to replicate data at the volume level. You can choose a one-time data replication to move data to and from the cloud, or a recurring schedule for disaster recovery or long-term retention.

About this task

Cloud Manager simplifies data replication between volumes on separate systems. 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 AWS disks, configures relationships, applies the replication policy, and then initiates the baseline transfer between volumes.

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



Steps

1. [Decide which type of replication policy to use](#) on page 54
A replication policy defines how the storage system replicates data from a source volume to a destination volume. You must choose a replication policy when you set up data replication in Cloud Manager.
2. [Understand what happens when you replicate data to and from encrypted systems](#) on page 56
You can replicate encrypted or unencrypted data between Data ONTAP clusters and Cloud ONTAP systems. When you replicate data from an encrypted system, the data is decrypted before it is replicated. Data is encrypted on the destination system if encryption is enabled on that system.
3. [Verify that your systems meet data replication requirements](#) on page 56
Before you can replicate data, you should confirm that specific requirements are met for both Cloud ONTAP systems and Data ONTAP clusters.
4. [Replicate data between systems](#) on page 57
You can replicate data between Cloud ONTAP systems and Data 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.
5. [Manage data protection schedules and relationships](#) on page 59
After you set up data replication between two systems, you can manage the data replication schedule and relationship from Cloud Manager.

Considerations for choosing a replication policy

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

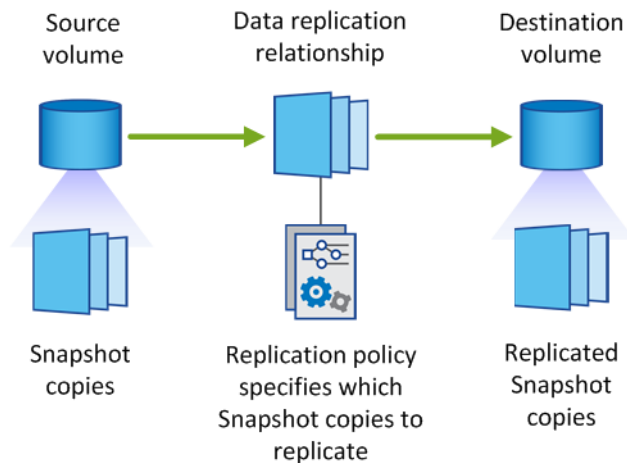
What replication policies do

The Cloud ONTAP and clustered Data ONTAP operating systems automatically create 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.

Note: Replication policies are also referred to as *protection policies* because they are part of SnapMirror and SnapVault technologies that provide disaster recovery protection and disk-to-disk backup and recovery.

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



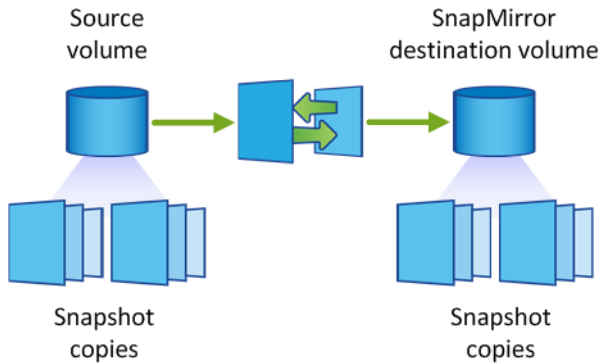
Types of replication policies

There are three types of replication policies:

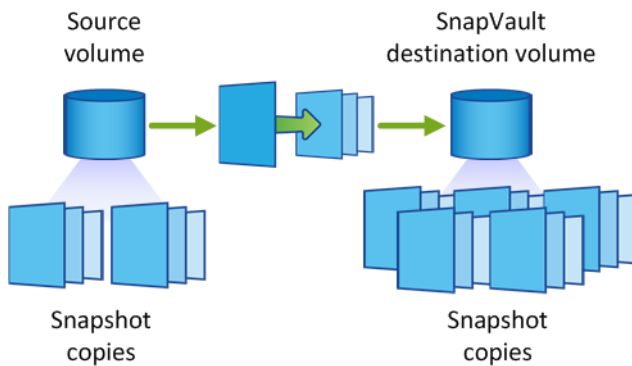
- A *SnapMirror policy* replicates newly created Snapshot copies to a destination volume. You can use these Snapshot copies to protect the source volume in preparation for disaster recovery or for one-time data replication. You can activate the destination volume for data access at any time.
- A *SnapVault 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.
[How SnapVault policies work](#) on page 55
- A *SnapMirror and SnapVault policy* provides both disaster recovery and long-term retention.

Each system includes default SnapMirror and SnapVault policies, which work 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 SnapMirror and SnapVault. A SnapMirror policy mirrors the Snapshot copies available on the source volume.



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



How SnapVault policies work

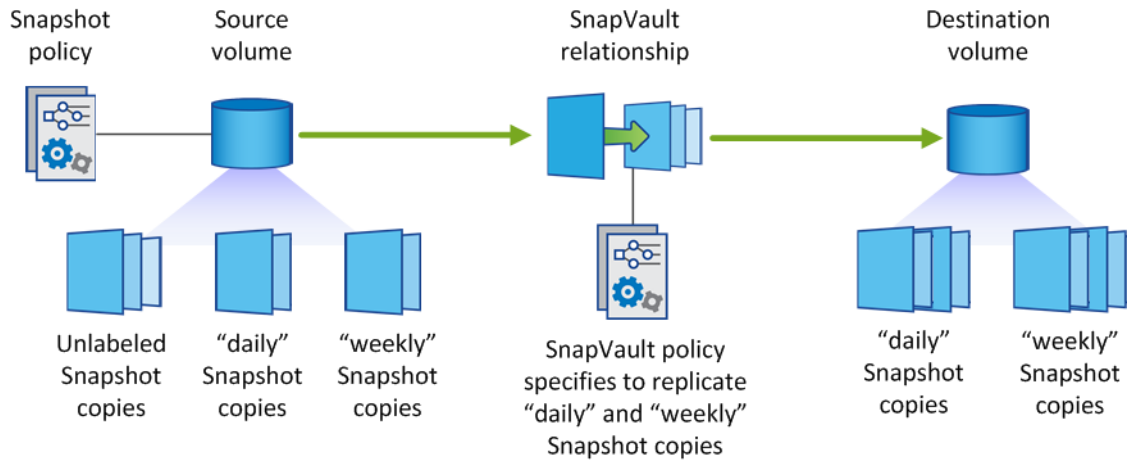
Unlike SnapMirror, SnapVault replicates *specific* Snapshot copies to a destination volume, as defined by a SnapVault policy. It is important to understand how SnapVault policies work if you want to use your own policies instead of the default policies.

Understanding the relationship between Snapshot copy labels and SnapVault 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 *SnapVault 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 SnapVault policy must match one or more labels defined in a Snapshot policy. Otherwise, the system cannot replicate any Snapshot copies.

For example, a SnapVault 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 SnapVault policy with the default Snapshot policy. The default SnapVault 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.

What happens when you replicate data to and from encrypted systems

You can replicate encrypted or unencrypted data between Data ONTAP clusters and Cloud ONTAP systems. When you replicate data from an encrypted system, the data is decrypted before it is replicated. Data is encrypted on the destination system if encryption is enabled on that system.

For example, if you use the NetApp Storage Encryption feature with a Data ONTAP cluster and enable Cloud ONTAP-managed encryption on a Cloud ONTAP system, the data that you replicate between those systems is decrypted before it is replicated and then re-encrypted after it is replicated.

Data replication requirements

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

General requirements

- If you want to replicate data between Cloud ONTAP systems and clustered Data ONTAP systems running a version prior to 8.3, then the destination system must run a version that is equal to or later than that of the source system. This requirement applies to SnapMirror. It does not apply to SnapVault.

For example, replication from a Cloud ONTAP 8.3 system to a clustered Data ONTAP 8.2.3 system is not supported because the destination is running an earlier version. Conversely, replication from an 8.2.3 system to an 8.3 system is supported because the destination is running a later version.

Starting with clustered Data ONTAP 8.3, there are no version requirements for source and destination systems in SnapMirror relationships. The systems can run different versions, if they are both running 8.3 or later.

- Each cluster must have a unique name.
You cannot create a cluster peering relationship with any cluster that has the same name or is in a peer relationship with a cluster of the same name.

Requirements specific to Cloud ONTAP

- The instance's security group must include the required inbound and outbound rules: specifically, rules for ICMP and ports 10000, 11104, and 11105.
These rules are included in the predefined security group.
For more details about security group requirements, see the [OnCommand Cloud Manager 2.1 Installation and Setup Guide](#).
- When replicating data between two Cloud ONTAP systems in different AWS subnets, the subnets must be routed together (this is the default setting).

Requirements specific to Data ONTAP clusters

- The clustered Data ONTAP version must be 8.2.1 or later.
- 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, which is typically a VPN connection.
- Data ONTAP clusters must meet additional subnet, port, firewall, and cluster requirements.
For details, see the *Cluster Peering Express Guide* or *Data Protection Guide* for your version of clustered Data ONTAP.

Related information

[Clustered Data ONTAP 8.3 Cluster Peering Express Guide](#)
[Clustered Data ONTAP 8.3 Data Protection Guide](#)

Replicating data between systems

You can replicate data between Cloud ONTAP systems and Data 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 and fanout data protection configurations, but it does not support cascade 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, which can be SnapMirror or SnapVault destinations.

Note: Only one SnapVault relationship is allowed in a fanout configuration.

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

If you want to use a cascade configuration, then you must set it up using the CLI. For more information about data protection configurations, see the [Clustered Data ONTAP 8.3 Data Protection Guide](#).

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. On the **Source and Destination Peering Setup** pages, 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 a Data 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, and then click **Continue**.
4. On the **Destination Volume** page, specify the destination volume name, and then click **Advanced options** if you want to specify the maximum rate (in kilobytes per second) at which data can be transferred (for example, 10240 KB/s).

Note the following:

- If the destination is a Data ONTAP cluster, you must also specify the destination SVM and aggregate.
 - If Cloud ONTAP is the destination, you can also choose a specific aggregate for the destination volume when you click **Advanced options**.
5. On the **Replication Policy** page, choose one of the default policies or click **Additional Policies**, and then select one of the advanced policies.

[Considerations for choosing a replication policy](#) on page 54

If you choose a custom SnapVault policy, the labels associated with the policy must match the labels of the Snapshot copies on the source volume.

[How SnapVault policies work](#) on page 55
 6. 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.
 7. On the **Review** page, review your selections, and then click **Go**.

Result

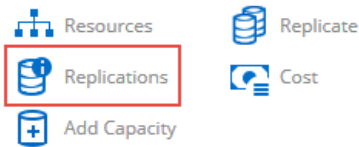
Cloud Manager starts the data replication process. You can view details about the replication in the Replication Status page.

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

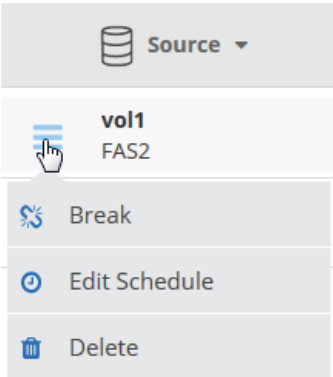
1. On the **Working Environments** page, view the replication status for all assigned working environments in the tenant or for a specific working environment:

For...	Do this...
All assigned working environments in the tenant	Click Replication Status from the navigation bar. 
A specific working environment	Select the working environment and click Replications. 

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

Note: 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 SnapMirror relationship between the source and destination volumes, and activates the destination volume for data access. This option is typically used when the source volume is unable to 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 Clustered Data ONTAP 8.3 Volume Disaster Recovery Express Guide.
Resync	Reestablishes a broken SnapMirror relationship between volumes and resumes data replication according to the defined schedule. Important: 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 Clustered Data ONTAP 8.3 Volume Disaster Recovery Express Guide.
Edit Schedule	Enables you to choose a different schedule for data replication.
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.
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.

Result

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

What to do after using Cloud Manager

After you set up Cloud ONTAP and you start replicating data to and from the cloud, you might want to manage and protect your data with other NetApp storage software, or get help with Cloud ONTAP.

You can perform the following tasks and use the following resources for help:

Tasks	Resources
Identify the NetApp storage software supported with Cloud ONTAP	<i>NetApp Interoperability Matrix Tool</i>
Activate and configure a destination SnapMirror volume for data access	<i>Clustered Data ONTAP 8.3 Volume Disaster Recovery Express Guide</i>
Restore a volume from a SnapVault backup	<i>Clustered Data ONTAP 8.3 Volume Restore Using SnapVault Express Guide</i>
Review release-specific information (known issues, limitations, and so on) for Cloud Manager and Cloud ONTAP	<i>OnCommand Cloud Manager 2.1 Release Notes</i> <i>Find the Release Notes for your version of Cloud ONTAP</i>
View more documentation and videos for Cloud ONTAP and Cloud Manager	<i>NetApp Cloud ONTAP Resources</i>
Get help	<i>NetApp Cloud ONTAP Support</i> <i>NetApp Community: Hybrid Cloud</i>

Copyright information

Copyright © 1994–2015 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, Go Further, Faster, AltaVault, ASUP, AutoSupport, Campaign Express, Cloud ONTAP, Clustered Data ONTAP, Customer Fitness, Data ONTAP, DataMotion, Fitness, Flash Accel, Flash Cache, Flash Pool, FlashRay, FlexArray, FlexCache, FlexClone, FlexPod, FlexScale, FlexShare, FlexVol, FPolicy, GetSuccessful, LockVault, Manage ONTAP, Mars, MetroCluster, MultiStore, NetApp Insight, OnCommand, ONTAP, ONTAPI, RAID DP, RAID-TEC, SANtricity, SecureShare, Simplicity, Simulate ONTAP, Snap Creator, SnapCenter, SnapCopy, SnapDrive, SnapIntegrator, SnapLock, SnapManager, SnapMirror, SnapMover, SnapProtect, SnapRestore, Snapshot, SnapValidator, SnapVault, StorageGRID, Tech OnTap, Unbound Cloud, and WAFL and other names are trademarks or registered trademarks of NetApp, Inc., in the United States, and/or other countries. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such. A current list of NetApp trademarks is available on the web at <http://www.netapp.com/us/legal/netapptmlist.aspx>.

How to send comments about documentation and receive update notifications

You can help us to improve the quality of our documentation by sending us your feedback. You can receive automatic notification when production-level (GA/FCS) documentation is initially released or important changes are made to existing production-level documents.

If you have suggestions for improving this document, send us your comments by email to doccomments@netapp.com. To help us direct your comments to the correct division, include in the subject line the product name, version, and operating system.

If you want to be notified automatically when production-level documentation is released or important changes are made to existing production-level documents, follow Twitter account @NetAppDoc.

You can also contact us in the following ways:

- NetApp, Inc., 495 East Java Drive, Sunnyvale, CA 94089 U.S.
- Telephone: +1 (408) 822-6000
- Fax: +1 (408) 822-4501
- Support telephone: +1 (888) 463-8277

Index

A

- account ID
 - viewing [44](#)
- Active Directory domains
 - modifying the CIFS server in Cloud ONTAP after changing [37](#)
- aggregates
 - adding disks to [36](#)
 - considerations for choosing EBS disk size [19](#)
 - creating [32](#), [36](#)
 - deleting [36](#)
 - finding encryption keys for [48](#)
 - how they are created [29](#)
 - provisioning a volume for Cloud ONTAP [30](#)
 - viewing [36](#)
- aggregates, Cloud ONTAP
 - verifying that they are online [41](#)
- Amazon Web Services
 - considerations for choosing an EBS disk type [19](#)
 - costs [34](#)
 - discovering NetApp Private Storage clusters [51](#)
 - encryption overview [18](#)
 - monitoring [34](#)
- Amazon Web Services storage
 - how Cloud ONTAP uses [16](#)
- APIs
 - overview of [8](#)
- automatic shutdowns
 - scheduling for Cloud ONTAP [38](#)

B

- backups, cluster configuration
 - sending to Cloud Manager [50](#)

C

- CA certificate
 - updating [48](#)
- capacity
 - moving to a higher capacity subscription [45](#)
- certificates
 - renewing [48](#)
 - updating [48](#)
 - viewing details for [48](#)
- CIFS servers
 - modifying in Cloud ONTAP [37](#)
- CIFS volumes
 - provisioning for Data ONTAP clusters using Cloud Manager [51](#)
- CLI
 - connecting to Cloud ONTAP [28](#)
- client certificate
 - renewing [48](#)
- Cloud Manager
 - adding existing Cloud ONTAP instances to [46](#)
 - See also* OnCommand Cloud Manager

Cloud ONTAP

- adding existing instances to Cloud Manager [46](#)
- automatically shutting down [38](#)
- changing instance types for [45](#)
- changing license types for [45](#)
- completing the AWS network information worksheet [21](#)
- connecting to the CLI [28](#)
- considerations for choosing an EBS disk type for [19](#)
- creating a working environment [21](#)
- data replication requirements [56](#)
- differences among products [18](#)
- downgrade preparation [40](#)
- downgrading from HTTP or FTP server [42](#)
- downgrading using local image [43](#)
- encryption overview [18](#)
- expired subscriptions to [44](#)
- how it is configured by default [15](#)
- how it uses AWS storage [16](#)
- how to provision AWS storage for [29](#)
- identifying who created it [44](#)
- introduction to launching instances of [21](#)
- introduction to preparing to launch [15](#)
- managing from System Manager [27](#)
- moving to an alternate subscription [45](#)
- overview of software updates [39](#)
- product models [7](#)
- registering pay-as-you-go instances [25](#)
- replicating data [57](#)
- requirements before launching [5](#)
- sending configuration backups to Cloud Manager [50](#)
- stopping an instance [38](#)
- terminating [38](#)
- upgrade preparation [40](#)
- upgrading [41](#)
- upgrading from HTTP or FTP server [42](#)
- viewing configuration details [44](#)
- viewing costs for [34](#)
- ways to configure after launch [26](#)
- what it is [7](#)
- workflow for deploying [14](#)
- Cloud ONTAP aggregates
 - verifying that they are online [41](#)
- Cloud ONTAP encryption
 - understanding how it works [47](#)
- Cloud ONTAP volume usage profiles
 - differences between [20](#)
- cluster admin account
 - changing the password for [49](#)
- cluster configuration backups
 - sending to Cloud Manager [50](#)
- clusters
 - adding to Cloud Manager [51](#)
- clusters, NetApp Private Storage
 - provisioning volumes for, using Cloud Manager [51](#)
- clusters, on-premises Data ONTAP
 - provisioning volumes for, using Cloud Manager [51](#)
- comments
 - how to send feedback about documentation [64](#)

- compression
 - defined [20](#)
- configurations, Cloud ONTAP
 - differences among [18](#)
- configurations, default
 - Cloud ONTAP [15](#)
- configurations, pay-as-you-go
 - changing between [45](#)
- console
 - components of [9](#)
 - logging in to Cloud Manager [9](#)
 - understanding [9](#)
- costs
 - viewing for Cloud ONTAP [34](#)

D

- Data ONTAP clusters
 - adding to Cloud Manager [51](#)
 - provisioning volumes for, using Cloud Manager [51](#)
- data replication
 - how it works in Cloud Manager [53](#)
 - managing [59](#)
 - requirements [56](#)
 - viewing status of [59](#)
 - what happens to encrypted data [56](#)
 - workflow [53](#)
- deduplication
 - defined [20](#)
- default configurations
 - Cloud ONTAP [15](#)
- destination systems, SnapMirror
 - version requirements for upgrades [40](#)
- disks, EBS
 - considerations for choosing for Cloud ONTAP [19](#)
 - considerations for choosing size [19](#)
 - how Cloud ONTAP uses [16](#)
 - understanding the performance of [19](#)
- DNS servers
 - modifying the CIFS server in Cloud ONTAP after changing [37](#)
- documentation
 - how to receive automatic notification of changes to [64](#)
 - how to send feedback about [64](#)
 - where to find additional documentation [61](#)

E

- EBS disks
 - considerations for choosing for Cloud ONTAP [19](#)
 - considerations for choosing size [19](#)
 - how Cloud ONTAP uses [16](#)
 - understanding the performance of [19](#)
- EBS snapshots
 - creating for root and boot disks [38](#)
- encryption
 - deciding whether to use [18](#)
 - how data is replicated [56](#)
 - understanding how it works in Cloud ONTAP [47](#)
- encryption keys
 - finding for aggregates [48](#)

- environments, working
 - creating for Cloud ONTAP [21](#)
- existing Cloud ONTAP instances
 - adding to Cloud Manager [46](#)

F

- FAS clusters
 - adding to Cloud Manager [51](#)
 - data replication requirements [56](#)
 - replicating data [57](#)
- feedback
 - how to send comments about documentation [64](#)

G

- General Purpose (SSD) disk size
 - considerations for choosing [19](#)

I

- information
 - how to send feedback about improving documentation [64](#)
- instance types
 - changing for Cloud ONTAP [45](#)
- instances
 - shutting down through a schedule [38](#)
 - stopping [38](#)
- IP addresses
 - viewing for Cloud ONTAP [44](#)
- iSCSI
 - provisioning storage for [32](#)
 - setting up Cloud ONTAP for [29](#)

K

- key managers
 - adding [48](#)
 - deleting [48](#)
- keys, encryption
 - finding for aggregates [48](#)

L

- license
 - viewing information about [44](#)
- license types
 - changing for Cloud ONTAP [45](#)
- logging in
 - to Cloud Manager [9](#)

M

- Magnetic disk size
 - considerations for choosing [19](#)
- Microsoft Azure
 - discovering NetApp Private Storage clusters [51](#)
- models, Cloud ONTAP
 - differences among [18](#)

N

- NetApp Private Storage
 - discovering existing configurations [51](#)
 - provisioning volumes for, using Cloud Manager [51](#)
 - requirements before creating working environment [5](#)
- network interfaces
 - default configurations for Cloud ONTAP [15](#)
- NFS volumes
 - provisioning for Data ONTAP clusters using Cloud Manager [51](#)

O

- on-premises Data ONTAP clusters
 - discovering existing configurations [51](#)
 - provisioning volumes for, using Cloud Manager [51](#)
- OnCommand Cloud Manager
 - changing your password [12](#)
 - how to provision storage for Cloud ONTAP [29](#)
 - logging in [9](#)
 - overview of the console [9](#)
 - what it is [6](#)

P

- passwords
 - changing for Cloud Manager [12](#)
 - changing for Cloud ONTAP [49](#)
- pay-as-you-go configurations
 - changing between [45](#)
- policies, replication
 - considerations for choosing [54](#)
- policies, Snapshot
 - how they work [55](#)
- policies, SnapVault
 - how they work [55](#)
- product models, Cloud ONTAP
 - differences among [18](#)

R

- relationships, SnapMirror
 - version requirements for upgrades [40](#)
- replication policies
 - considerations for choosing [54](#)
- replication, data
 - how it works on Cloud Manager [53](#)
 - managing [59](#)
 - viewing status of [59](#)
 - what happens to encrypted data [56](#)
 - workflow [53](#)
- requirements, version
 - for upgrading SnapMirror source and destination systems [40](#)

S

- schedules, data replication
 - managing [59](#)
- serial number
 - viewing [44](#)

- setup, Cloud ONTAP
 - ways to configure after launch [26](#)
- shutdowns, automatic
 - scheduling for Cloud ONTAP [38](#)
- SnapMirror
 - requirements [56](#)
 - suspending transfers [40](#)
 - using to replicate data [57](#)
 - version requirements for upgrades [40](#)
 - what happens to encrypted data [56](#)
- SnapMirror policies
 - considerations for choosing [54](#)
- Snapshot policies
 - how they work [55](#)
- snapshots
 - creating for root and boot disks [38](#)
- SnapVault
 - using to replicate data [57](#)
- SnapVault policies
 - considerations for choosing [54](#)
 - how they work [55](#)
 - relationship between Snapshot copy labels [55](#)
- SoftLayer
 - discovering NetApp Private Storage clusters [51](#)
- source systems, SnapMirror
 - version requirements for upgrades [40](#)
- SSH
 - using to access the Cloud ONTAP CLI [28](#)
- Storage Virtual Machine
 - modifying the name of [49](#)
- Storage Virtual Machines
 - adding iSCSI access to [29](#)
- storage, Amazon Web Services
 - how Cloud ONTAP uses [16](#)
- storage, Cloud ONTAP
 - how to provision [29](#)
- suggestions
 - how to send feedback about documentation [64](#)
- support
 - registering pay-as-you-go Cloud ONTAP instances [25](#)
- suspending SnapMirror transfers
 - prior to software upgrade [40](#)
- SVMs
 - number supported with Cloud ONTAP [15](#)
- System Manager
 - connecting to [27](#)
- systems, SnapMirror source and destination
 - version requirements for upgrades [40](#)

T

- tenants
 - definition of [9](#)
- thin provisioning
 - defined [20](#)
- transfers
 - suspending [40](#)
- twitter
 - how to receive automatic notification of documentation changes [64](#)

U

- upgrades
 - version requirements for SnapMirror source and destination systems [40](#)
- upgrading
 - Cloud ONTAP using HTTP or FTP server [42](#)
- usage profiles, volume
 - defined [20](#)
 - differences between [20](#)
- user accounts
 - changing your Cloud Manager password [12](#)
 - creating Working Environment Admins [12](#)

V

- version requirements
 - for upgrading SnapMirror source and destination systems [40](#)
- volume usage profiles
 - differences between [20](#)
- volumes
 - cloning [35](#)

- deleting [35](#)
- editing [35](#)
- provisioning for Cloud ONTAP [30](#)
- provisioning for Data ONTAP clusters using Cloud Manager [51](#)
- provisioning for iSCSI [32](#)
- restoring from [35](#)
- viewing [35](#)

W

- warnings
 - expired subscriptions [44](#)
- working environment
 - identifying who created it [44](#)
- Working Environment Admins
 - creating [12](#)
- working environments
 - automatically shutting down [38](#)
 - creating for Cloud ONTAP [21](#)
 - requirements before creating [5](#)
- worksheets, AWS network information
 - completing for Cloud ONTAP [21](#)