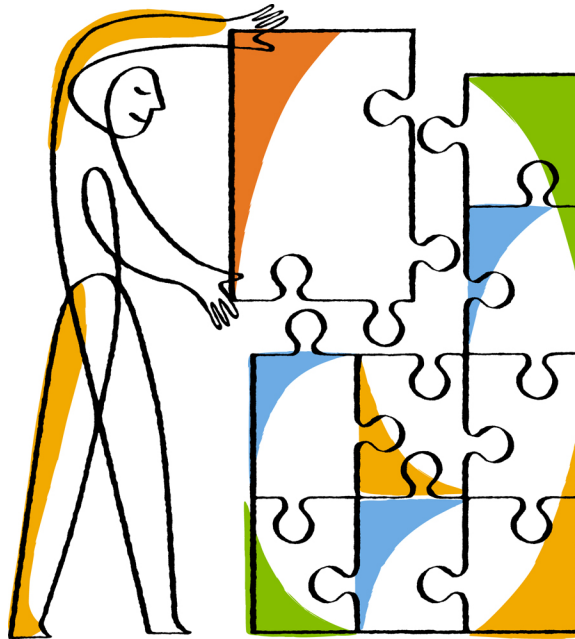




OnCommand® Cloud Manager 2.1

Installation and Setup 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: 215-10494_A0
December 2015

Contents

Product overview	5
Cloud ONTAP for AWS overview	6
Cloud Manager REST APIs	7
Installation and setup workflow	8
Preparing for installation and setup	9
Preparing your AWS environment	9
AWS networking requirements for Cloud Manager	10
AWS networking requirements for Cloud ONTAP	12
Sample VPC configurations for Cloud Manager and Cloud ONTAP	13
Granting permissions to IAM users	15
How AWS limits can impact Cloud ONTAP	17
Setting up AWS billing and cost management for Cloud Manager	17
Cloud Manager requirements	19
Ways to encrypt Cloud ONTAP data	20
Key manager requirements for Cloud ONTAP encryption	21
Planning how to organize users and storage across tenants	23
Credentials that you need for Cloud Manager	24
Installation and setup worksheet	26
Subscribing to Cloud ONTAP in AWS	27
Installing OnCommand Cloud Manager	28
Launching a Cloud Manager instance in AWS	28
Installing Cloud Manager on an existing Linux host	29
Setting up OnCommand Cloud Manager	30
Installing an HTTPS certificate for secure access	32
Defining tenants	32
Creating user accounts	33
Setting up Cloud Manager for Cloud ONTAP encryption	34
Understanding how Cloud ONTAP encryption works	35
Setting up Cloud Manager to be an intermediate CA	36
Adding key managers and CA certificates to Cloud Manager	36
What to do after installation and setup	38
Updating Cloud Manager to version 2.1	39
Installing OnCommand Cloud Manager	39
Launching a Cloud Manager instance in AWS	39
Installing Cloud Manager on an existing Linux host	40
Importing your Cloud Manager configuration	41
Configuring Cloud ONTAP to send configuration backups to Cloud Manager	42
Removing your previous Cloud Manager configuration	42
Terminating the Cloud Manager instance	42
Uninstalling the Cloud Manager software	43
Terminating the NetApp Support instance	43

Uninstalling Cloud Manager 44

Copyright information 45

Trademark information 46

How to send comments about documentation and receive update

notifications 47

Index 48

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:

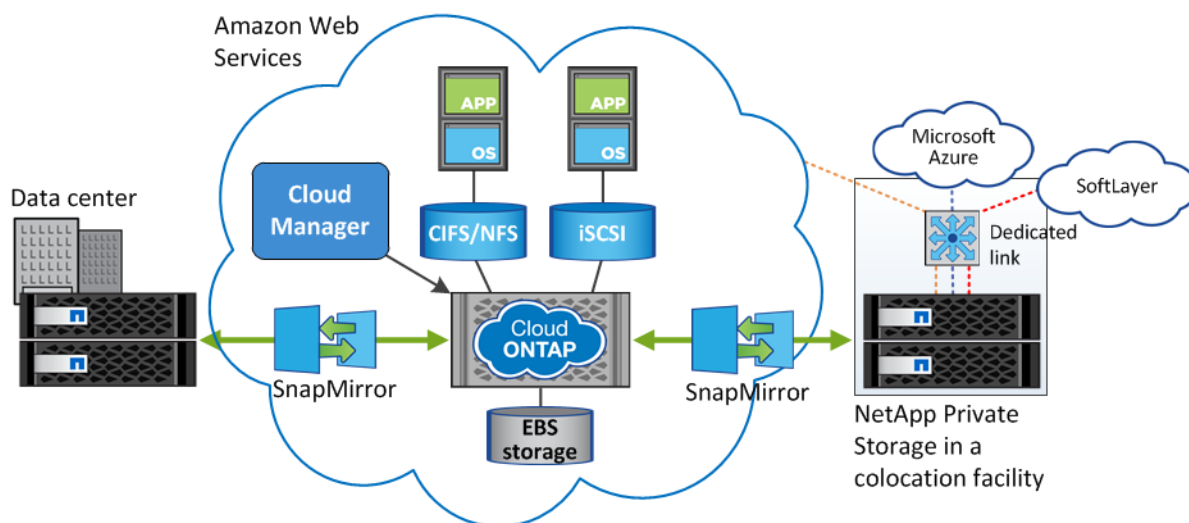
- Deploy Cloud ONTAP systems in approximately 25 minutes
- Set up Cloud ONTAP for data-at-rest encryption
- Provision NFS and CIFS storage using a simplified provisioning wizard
- Replicate data to and from the cloud
- Upgrade Cloud ONTAP systems to the latest version using an automated process
- Monitor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

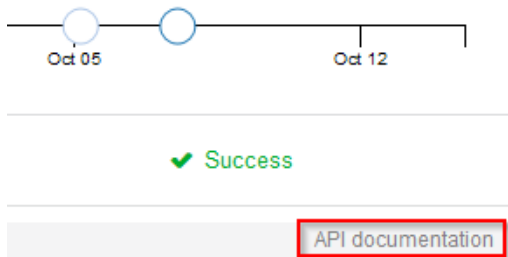
	Cloud ONTAP Explore	Cloud ONTAP Standard	Cloud ONTAP Premium	Cloud ONTAP BYOL
Cloud ONTAP encryption ¹	Not supported	Supported	Supported	Supported
EC2 instance types ²	• m3.xlarge • m4.xlarge	• m3.2xlarge • m4.2xlarge • r3.xlarge	r3.2xlarge	• m3.xlarge • m3.2xlarge • m4.xlarge • m4.2xlarge • r3.xlarge • 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.

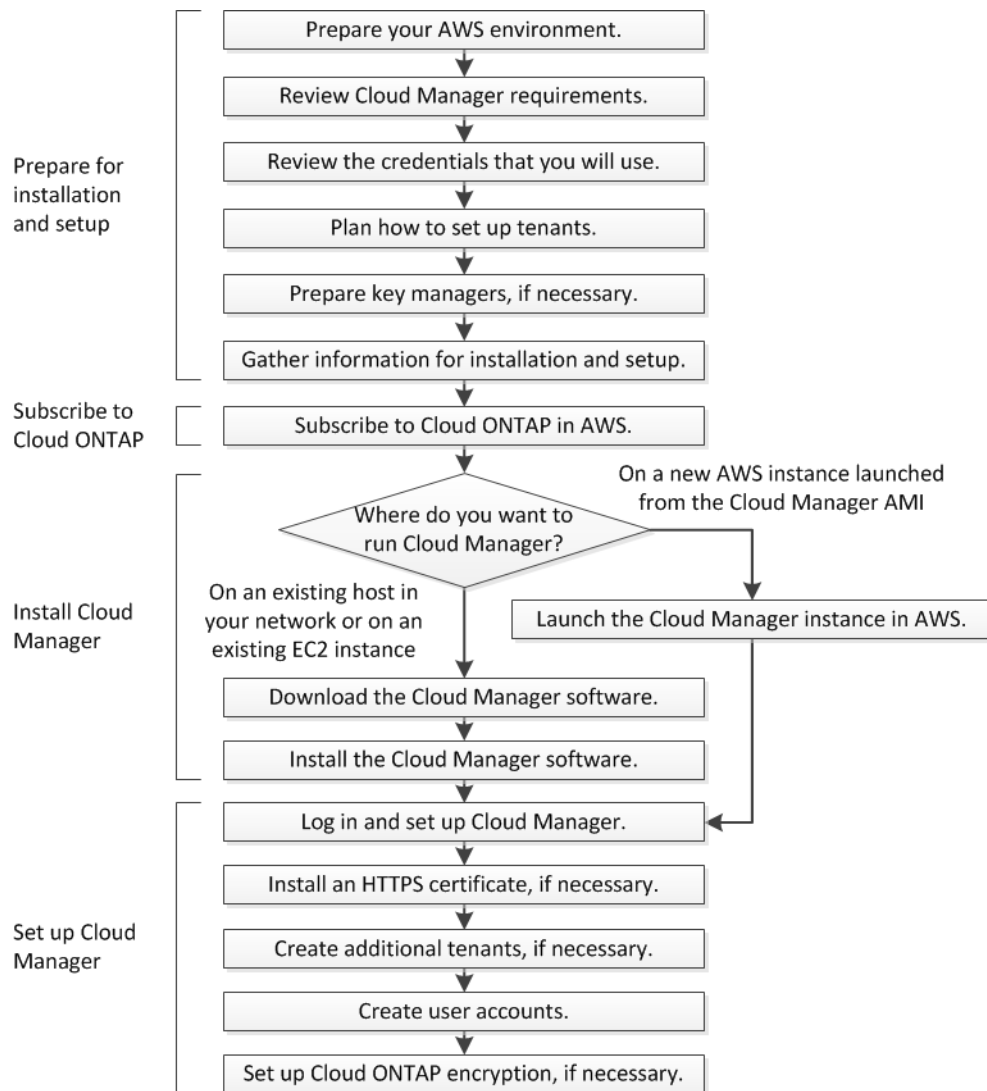
Cloud Manager provides interactive API documentation using the Swagger interface. A link to the API documentation is available in the lower-right corner of the console:



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

Installation and setup workflow

Deploying Cloud Manager involves preparing your environment, subscribing to Cloud ONTAP in the AWS Marketplace, installing Cloud Manager, and then setting it up.



Preparing for installation and setup

Before you install and set up Cloud Manager, you must prepare your environment and understand the information that you need for installation and setup.

Steps

1. [Prepare your AWS environment](#) on page 9
Your AWS environment must meet a few requirements to ensure that Cloud Manager and Cloud ONTAP operate correctly in AWS.
2. [Review Cloud Manager requirements](#) on page 19
You must verify support for your configuration, which includes host requirements, web browser requirements, EC2 instance requirements, and so on. Most of this information is available in the NetApp Interoperability Matrix; however, because you might not have a NetApp Support Site login, a minimum amount of information is provided to get you started.
3. [Decide whether you want to encrypt data and set up key managers, if necessary](#) on page 20
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.
4. [Plan how to set up tenants](#) on page 23
Cloud Manager enables you to provision and manage storage in isolated groups called *tenants*. You need to decide how to organize Cloud Manager users and their working environments across tenants.
5. [Review the credentials that you will use](#) on page 24
You must provide credentials for several accounts and components as you install and use Cloud Manager. Because there are quite a few credentials, it is helpful to understand which credentials you and your Cloud Manager users need to provide and when you need to provide them.
6. [Gather information for installation and setup](#) on page 26
You need to enter information about your environment when you install and set up Cloud Manager. You can use a worksheet to collect the information that you need.

Preparing your AWS environment

Your AWS environment must meet a few requirements to ensure that Cloud Manager and Cloud ONTAP operate correctly in AWS.

Before you begin

You should be familiar with AWS networking: Virtual Private Clouds (VPCs), subnets, and security groups. [AWS Documentation: Your VPC and Subnets](#).

Steps

1. Set up your VPC, subnets, and security groups according to the following requirements:
 - [AWS networking requirements for Cloud Manager](#) on page 10
 - [AWS networking requirements for Cloud ONTAP](#) on page 12

The easiest way to set up your AWS networking is to use the VPC wizard and choose one of the most common deployments: a VPC with public and private subnets and a NAT instance, or a VPC

with a private subnet and VPN access. You can then use the predefined security groups that are available when you launch the Cloud Manager and Cloud ONTAP instances.

[Sample VPC configurations for Cloud Manager and Cloud ONTAP](#) on page 13

2. Grant the required permissions to IAM users.

[Granting permissions to IAM users](#) on page 15

3. Review AWS default limits so that you do not reach limits that impact Cloud ONTAP instances.

[How AWS limits can impact Cloud ONTAP](#) on page 17

4. Optional: Set up AWS billing and cost management so that Cloud Manager can display compute and storage costs for Cloud ONTAP instances.

[Setting up AWS billing and cost requirements](#) on page 17

5. If you want to launch Cloud Manager in AWS, create an EC2 key pair, if you do not have one. You need a key pair to decrypt the login information for the Cloud Manager instance.

[AWS Documentation: Amazon EC2 Key Pairs](#)

AWS networking requirements for Cloud Manager

Whether you install Cloud Manager in AWS or in your data center, you must set up your AWS networking (Virtual Private Clouds, subnets, and security groups) so Cloud Manager can launch Cloud ONTAP instances.

Requirement	Description
Internet access	Cloud Manager requires Internet access to do the following: • Access an S3 bucket that contains the Cloud ONTAP AMI manifest file and the latest Cloud Manager installation packages • Communicate with AWS services to launch and manage Cloud ONTAP instances • Send AutoSupport messages to NetApp technical support • Register Cloud ONTAP systems with NetApp technical support If Cloud Manager is in your data center, you must set up a VPN connection to the VPC and ensure firewall policies allow traffic to the endpoints. If Cloud Manager is in AWS, you must enable Internet access from your VPC by using an Internet gateway, NAT instance, or proxy server. If you have a proxy, you must configure Cloud Manager to use it. You can do so when using the Cloud Manager Setup wizard. AWS Documentation: Adding an Internet Gateway to Your VPC AWS Documentation: NAT Instances
A route to the subnets where you will deploy Cloud ONTAP	Cloud Manager requires a connection to the subnets in which you will launch Cloud ONTAP instances. If you deploy Cloud Manager in your data center, a VPN connection provides a route to the subnets in a VPC. If you deploy Cloud Manager in AWS, subnets are routed together by default. However, if you changed the routing tables, you must either reroute the subnets or ensure that users do not use nonroutable subnets. AWS Documentation: Route Tables

Requirement	Description
A security group with the required rules	When you launch Cloud Manager in AWS, the AWS Marketplace page provides an option to create a security group that includes the required inbound and outbound rules. It is best to use that predefined security group, but if you want to use your own, then it must include the required inbound and outbound rules. <i>AWS Documentation: Security Groups for Your VPC</i>
Access to the Cloud Manager web console	Users must access Cloud Manager from a web browser. If you deploy Cloud Manager in AWS, the easiest way to provide access is by launching Cloud Manager in a public subnet with a public IP address. However, if you want to use a private IP address instead, users can access the console through any of the following: • A jump host in the VPC that has a connection to Cloud Manager • A host in your data center that has a VPN connection to the private IP address • An RDP connection to the Cloud Manager host

Security group rules for Cloud Manager

Inbound rules

Note: The source for inbound rules is 0.0.0.0/0.

Type	Port range	Used for
SSH	22	SSH connections to the Cloud Manager instance
HTTP	80	Accessing the Cloud Manager console
HTTPS	443	Accessing the Cloud Manager console

Outbound rules

Type	Port range	Used for
All TCP	All	All outbound traffic
All UDP	All	All outbound traffic

AWS networking requirements for Cloud ONTAP

You must set up your AWS networking so that Cloud ONTAP can operate properly.

Requirement	Description
Internet access to send AutoSupport messages and to access an S3 bucket for upgrades	Cloud ONTAP needs outbound Internet access to do the following: - Communicate with NetApp AutoSupport, which is a troubleshooting tool that proactively monitors the health of your system and automatically sends messages to NetApp technical support - Access a NetApp-managed S3 bucket to obtain the latest software image when users upgrade Cloud ONTAP software directly from Cloud Manager Because Cloud ONTAP is most likely running in a private subnet, you can use a NAT instance, VPN, or proxy server (in your network or in AWS) to enable Internet access. If you have a proxy, you must configure Cloud Manager to use it. You can do so when using the Cloud Manager Setup wizard. Note the following about providing Internet access for AutoSupport: - For a NAT instance, you must define an inbound security group rule that allows HTTPS traffic from the private subnet to the Internet. AWS Documentation: NAT Instances - For VPN configurations, routing and firewall policies must allow AWS HTTP/HTTPS traffic to support.netapp.com.
A security group with the required rules	When you launch a Cloud ONTAP instance from Cloud Manager, you can select a predefined security group that includes the required rules. It is best to use that predefined security group, but if you need to use your own, it must include the required inbound and outbound rules. AWS Documentation: Security Groups for Your VPC
Connection to key managers	If you want to use the Cloud ONTAP data encryption feature, Cloud ONTAP instances must have a connection to one or more key managers that are either in AWS or in your network. If the key managers are in AWS, make sure there is a route to the subnet in which you deploy Cloud ONTAP instances. If the key managers are in your network, a VPN connection provides a route to the subnets in a VPC. Ways to encrypt Cloud ONTAP data on page 20
DNS and Active Directory for CIFS	If you want to provision CIFS storage, you must set up DNS and Active Directory in AWS or extend your on-premises setup to AWS. The DNS server must provide name resolution services for the Active Directory environment. You can configure DHCP option sets to use the default EC2 DNS server, which must not be the DNS server used by the Active Directory environment. AWS: Active Directory Domain Services on the AWS Cloud Quick Start Reference Deployment

Security group rules for Cloud ONTAP

Inbound rules

Note: The source for inbound rules is 0.0.0.0/0.

Type	Port range	Used for
All ICMP	All	Pinging the instance
Custom TCP Rule	111	Portmapper
Custom TCP Rule	139	NetBIOS
Custom TCP Rule	161-162	SNMP
Custom TCP Rule	445	Microsoft SMB
Custom TCP Rule	635	NFS mount
Custom TCP Rule	749	Kerberos
Custom TCP Rule	2049	NFS
Custom TCP Rule	3260	iSCSI
Custom TCP Rule	4045-4046	NFS mountd
Custom TCP Rule	10000	NDMP
Custom TCP Rule	11104-11105	Intercluster management and data
Custom UDP Rule	111	Portmapper
Custom UDP Rule	161-162	SNMP
Custom UDP Rule	635	NFS mount
Custom UDP Rule	2049	NFS
Custom UDP Rule	4045-4046	NFS mountd
HTTP	80	System Manager access
HTTPS	443	System Manager access
SSH	22	SSH to the CLI

Outbound rules

Type	Port range	Used for
All ICMP	All	All outbound traffic (SnapMirror and SnapVault)
All TCP	All	All outbound traffic
All UDP	All	All outbound traffic

Sample VPC configurations for Cloud Manager and Cloud ONTAP

To better understand how you can deploy Cloud Manager and Cloud ONTAP in AWS, you should review the most common VPC configurations.

The most common VPC configurations for Cloud Manager and Cloud ONTAP include the following:

- A VPC with public and private subnets and a NAT instance
- A VPC with a private subnet and a VPN connection to your network

For information about advanced configurations, see [NetApp Technical Report 4352: Networking Configurations for NetApp Cloud ONTAP for Amazon Web Services](#).

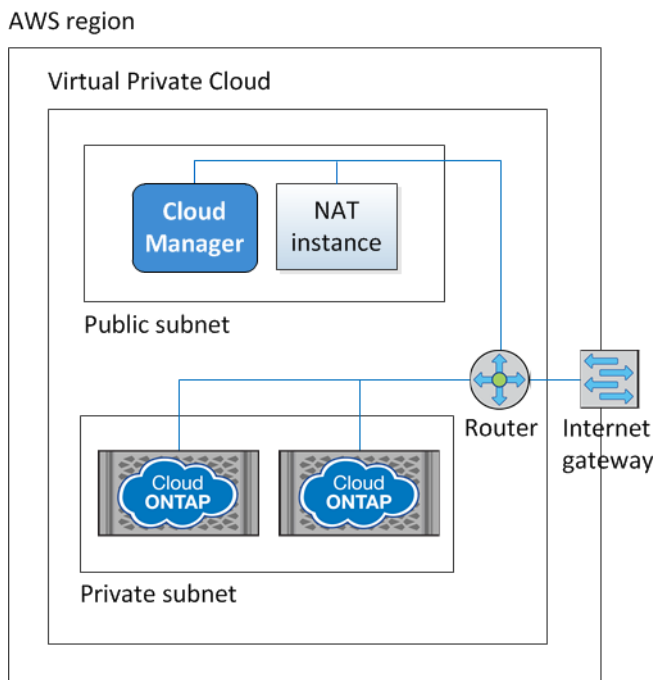
A VPC with public and private subnets and a NAT instance

This VPC configuration includes public and private subnets, an Internet gateway that connects the VPC to the Internet, and a NAT instance in the public subnet that enables outbound Internet traffic from the private subnet. In this configuration, you can run Cloud Manager in a public subnet or private subnet, but the public subnet is recommended because it allows access from hosts outside the VPC. You can then launch Cloud ONTAP instances in the private subnet.

Note: Instead of a NAT instance, you can use an HTTP proxy to provide Internet connectivity.

[AWS Documentation: Configuration Scenario 2 \(VPC with Public and Private Subnets\)](#)

The following graphic shows Cloud Manager running in a public subnet and Cloud ONTAP instances running in a private subnet:



A VPC with a private subnet and a VPN connection to your network

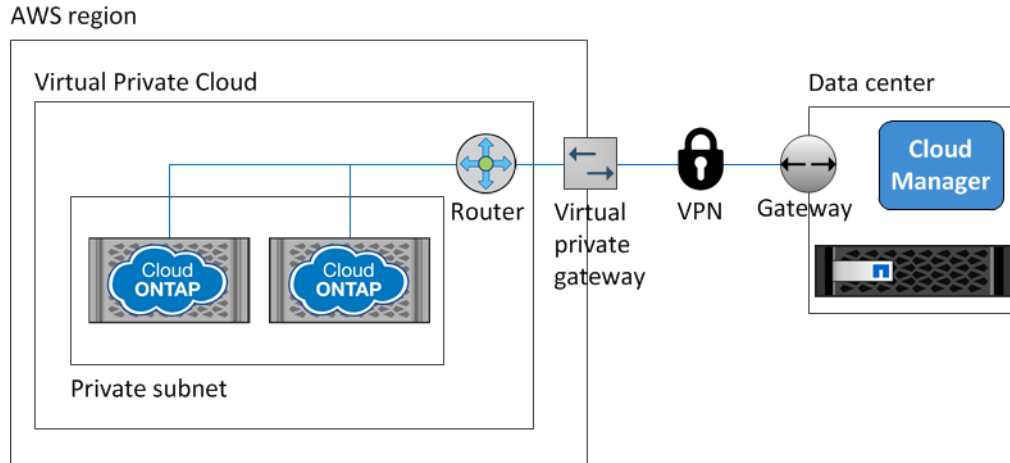
This VPC configuration is a hybrid cloud configuration in which Cloud ONTAP instances become an extension of your private environment. The configuration includes a private subnet and a virtual private gateway with a VPN connection to your network. Routing across the VPN tunnel allows EC2 instances to access the Internet through your network and firewalls. You can run Cloud Manager in the private subnet or in your data center. You would then launch Cloud ONTAP instances in the private subnet.

Note: You can also use a proxy server in this configuration to allow Internet access. The proxy server can be in your data center or in AWS.

If you want to replicate data between FAS systems in your data center and Cloud ONTAP systems in AWS, you should use a VPN connection to ensure that the link is secure.

[AWS Documentation: Configuration Scenario 4 \(VPC with a Private Subnet Only and Hardware VPN Access\)](#)

The following graphic shows Cloud Manager running in your data center and Cloud ONTAP instances running in a private subnet:



Granting permissions to IAM users

When you create Cloud Manager users, you must provide Cloud Manager with those users' AWS access keys so Cloud Manager can perform operations in AWS. AWS Identity and Access Management (IAM) users must have specific permissions defined in their account so Cloud Manager can perform the operations. You can download an IAM user policy that includes the required permissions.

About this task

If you provide any fewer than the permissions defined in the IAM user policy, then you need to perform any operations that Cloud Manager cannot perform. For example, if you do not allow an IAM user to delete AWS resources, then you need to delete those resources yourself.

Note: If you create a Cloud Manager user and enter access keys for an AWS root account user, then that user already has the required permissions.

Steps

1. Download an IAM user policy from the following location:
[NetApp OnCommand Cloud Manager: AWS IAM Policy](#)
2. From the **IAM** console, attach the policy to an IAM user or group.
[AWS Documentation: Managing IAM Policies](#)

What Cloud Manager does with AWS permissions

Cloud Manager uses an AWS account to make API calls to several AWS services, including EC2, S3, CloudFormation, and IAM. You might want to understand what Cloud Manager does with these permissions.

Permissions	Purpose
<pre>"ec2:StartInstances", "ec2:StopInstances", "ec2:DescribeInstances", "ec2:DescribeInstanceStatus", "ec2:RunInstances", "ec2:TerminateInstances", "ec2:ModifyInstanceAttribute", "ec2:DescribeInstanceAttribute",</pre>	Launches a Cloud ONTAP instance and stops, starts, and monitors the instance.

Permissions	Purpose
"ec2:CreateTags",	Tags every resource that Cloud Manager creates with the "WorkingEnvironment" and "WorkingEnvironmentId" tags. Cloud Manager uses these tags for maintenance and cost allocation.
"ec2:CreateVolume", "ec2:DescribeVolumes", "ec2:AttachVolume", "ec2:DeleteVolume", "ec2:DetachVolume",	Manages the EBS volumes that Cloud ONTAP uses as back-end storage.
"ec2:CreateSecurityGroup", "ec2:DeleteSecurityGroup", "ec2:DescribeSecurityGroups", "ec2:RevokeSecurityGroupEgress", "ec2:AuthorizeSecurityGroupEgress", "ec2:AuthorizeSecurityGroupIngress",	Creates predefined security groups for Cloud ONTAP.
"ec2:CreateNetworkInterface", "ec2:DescribeNetworkInterfaces", "ec2:DeleteNetworkInterface", "ec2:ModifyNetworkInterfaceAttribute",	Creates and manages network interfaces for Cloud ONTAP in the target subnet.
"ec2:DescribeSubnets", "ec2:DescribeVpcs",	Gets the list of destination subnets and security groups, which is needed when creating a new working environment for Cloud ONTAP.
"ec2:DescribeDhcpOptions",	Determines DNS servers and the default domain name when launching Cloud ONTAP instances.
"ec2:CreateSnapshot", "ec2:DeleteSnapshot", "ec2:DescribeSnapshots",	Takes snapshots of EBS volumes during initial setup and whenever a Cloud ONTAP instance is stopped.
"ec2:GetConsoleOutput",	Captures the Cloud ONTAP console, which is attached to AutoSupport messages.
"ec2:DescribeKeyPairs",	Obtains the list of available key pairs when launching instances.
"ec2:DescribeRegions",	Gets a list of available AWS regions.
"cloudformation:CreateStack", "cloudformation:DeleteStack", "cloudformation:DescribeStacks", "cloudformation:DescribeStackEvents", "cloudformation:DescribeStackResources", "cloudformation:GetTemplate", "cloudformation:ValidateTemplate",	Launches a Cloud ONTAP instance.

Permissions	Purpose
"iam:GetUser",	Validates AWS credentials when Cloud Manager saves and displays AWS keys for user accounts.
"s3:GetObject", "s3:ListBucket"	Obtains AWS cost data for Cloud ONTAP.

How AWS limits can impact Cloud ONTAP

Amazon Web Services has several default limits that can impact your ability to use Cloud ONTAP as you planned. Depending on your needs, you might need to request an increase to the default limits.

For example, you might need more instances and more total storage than you are currently allowed by AWS limits. By default, AWS limits your account to 20 instances and 20 TB of EBS storage.

Related information

[AWS Documentation: AWS Service Limits](#)

[AWS Documentation: Amazon EC2 Service Limits Report Now Available](#)

Setting up AWS billing and cost management for Cloud Manager

Cloud Manager can display the monthly compute costs and storage costs associated with running Cloud ONTAP in AWS. Before Cloud Manager can display the costs, users of AWS *payer* accounts must set up AWS to store billing reports in an S3 bucket, a Cloud Manager user account must have access to that S3 bucket, and AWS report tags must be enabled after you launch your first Cloud ONTAP instance.

About this task

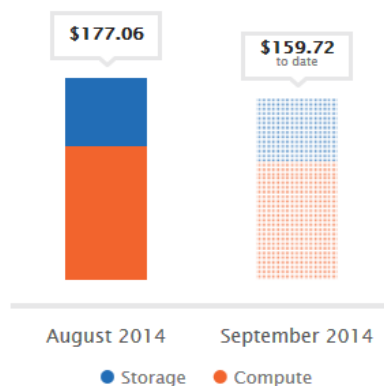
Users of AWS payer accounts must set up AWS to store billing reports in an S3 bucket. Cloud Manager uses the information from the reports to show monthly compute and storage costs associated with a Cloud ONTAP instance, as well as storage cost savings from NetApp product efficiency features (if they are enabled).

You should refer to AWS for final cost details.

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

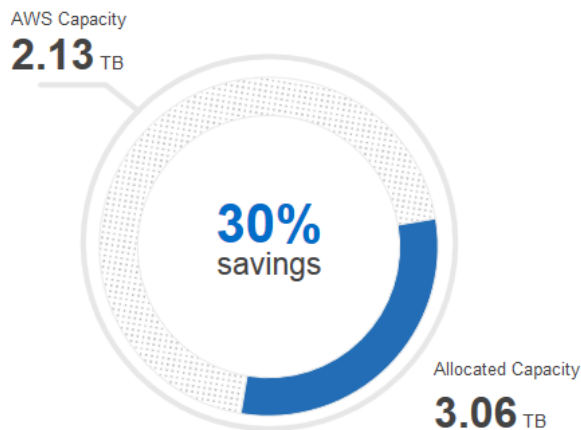


The following image shows an example of storage cost savings:

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](#)



Steps

1. Go to the **Amazon S3** console and set up an S3 bucket for the detailed billing reports:
 - a. Create an S3 bucket.
 - b. Apply a resource-based bucket policy to the S3 bucket to allow Billing and Cost Management to deposit the billing reports into the S3 bucket.

For details about using an S3 bucket for detailed billing reports and to use an example bucket policy, see [AWS Documentation: Understand Your Usage with Detailed Billing Reports](#).

2. From the **Billing and Cost Management** console, go to **Preferences** and enable the reports:
 - a. Enable **Receive Billing Reports** and specify the S3 bucket.
 - b. Enable **Cost allocation report**.
3. When you set up Cloud Manager, create a user account that Cloud Manager can use to access the reports:
 - a. Specify the AWS keys for an IAM user created under the payer account or the AWS keys for the payer account itself.

The IAM user must have the required permissions to access the billing information. If you used an IAM user policy provided by NetApp, the IAM user already has the required permissions. For details, see [Granting permissions to IAM users](#) on page 15.

- b. Specify the S3 bucket that you created.

[Creating user accounts](#) on page 33

4. After you launch your first Cloud ONTAP instance, go back to Billing and Cost Management **Preferences**, click **Manage report tags**, and enable the **WorkingEnvironmentId** tag.

This tag is not available in AWS until you create your first Cloud ONTAP working environment using any account under the AWS payer account.

Result

Cloud Manager updates the cost information at each 12-hour polling interval.

After you finish

Repeat these steps for other AWS payer accounts for which cost reporting is needed.

Related information

[AWS Documentation: Setting Up Your Monthly Cost Allocation Report](#)

[AWS Documentation: Controlling Access to Your Billing Information](#)

Cloud Manager requirements

You must verify support for your configuration, which includes host requirements, web browser requirements, EC2 instance requirements, and so on. Most of this information is available in the NetApp Interoperability Matrix; however, because you might not have a NetApp Support Site login, a minimum amount of information is provided to get you started.

If you have a NetApp Support Site login, go to the [NetApp Interoperability Matrix Tool](#) to search for supported Cloud Manager configurations.

EC2 instance requirements

Cloud Manager is supported on the t2.medium and m3.medium instance types. Cloud Manager can run on other EC2 instance types, but they are not supported.

Host requirements

A physical or virtual machine must meet minimum requirements to run Cloud Manager:

Component	Minimum requirement
Hypervisor	A bare metal or hosted hypervisor that is certified to run Red Hat Enterprise Linux. Red Hat Solution: Which hypervisors are certified to run Red Hat Enterprise Linux?
Operating system	Red Hat Enterprise Linux 7.1
CPU	2.27 GHz or higher with two cores
RAM	4 GB
Free disk space	50 GB

Web browser requirements

You need to access the Cloud Manager console from a supported web browser:

Web browser	Minimum supported version
Google Chrome	43
Microsoft Edge	20
Microsoft Internet Explorer	11

Web browser	Minimum supported version
Mozilla Firefox	38

For the full list of supported web browser versions, see the [NetApp Interoperability Matrix Tool](#).

Port requirements

Before you install Cloud Manager on an existing host, you should verify that the following ports are available. If other services are using these ports, Cloud Manager installation fails.

Port	Purpose
80	Provides HTTP access to the Cloud Manager web console.
443	Provides HTTPS access to the Cloud Manager web console.
3306	Used by a MySQL database that stores Cloud Manager data.
8080	Used by the Simplicator service, which is an API proxy for Cloud Manager.

There is a potential conflict with port 3306. If another instance of MySQL is running on the host, it uses port 3306 by default. You must change the port that the existing MySQL instance uses.

You can change the default HTTP and HTTPS ports when you install Cloud Manager. You cannot change the default port for the MySQL database. If you change the HTTP and HTTPS ports, you must ensure that users can access the Cloud Manager web console from a remote host:

- In AWS, modify the instance's security group to allow inbound connections through the ports.
- Specify the port when you enter the URL to the Cloud Manager web console.

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.

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](#)

Key manager requirements for Cloud ONTAP encryption

You need a supported key management infrastructure to use Cloud ONTAP encryption.

Supported key managers

An external key manager is a system in your network or in AWS that securely stores authentication keys and provides them upon demand to Cloud ONTAP systems using secure TLS connections. The following key managers are supported:

- SafeNet Virtual KeySecure for NetApp Cloud ONTAP
SafeNet OS v8.2.1 is supported.
[AWS Marketplace: SafeNet Virtual KeySecure for NetApp Cloud ONTAP](#)
- SafeNet KeySecure k460
SafeNet OS v8.0.1 is supported.

Each Cloud ONTAP system supports up to four key managers. You should use multiple key managers in a clustered configuration for redundancy.

Key manager configuration requirements

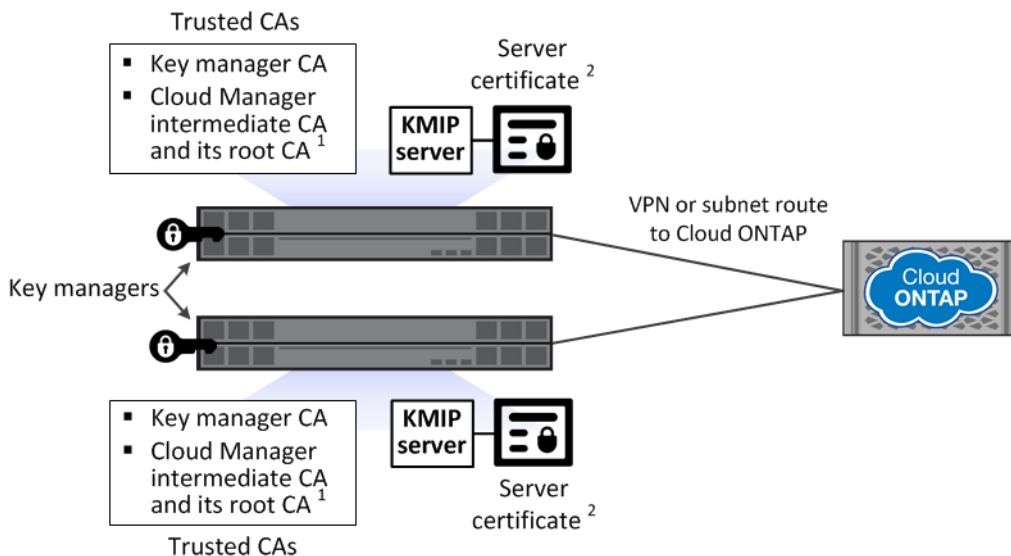
Each key manager must have several certificates, a KMIP server, and a network connection to Cloud ONTAP systems. The key manager must also meet specific requirements if using client certificate authentication. Note that Cloud Manager does not communicate with key managers, so a network connection between Cloud Manager and key managers is not required.

A description of the key manager requirements follows:

Requirement	Description
Key managers must have a server certificate	Key managers need a server certificate to authenticate with Cloud ONTAP systems. The SSL certificate must use the Privacy Enhanced Mail (PEM) Base-64 encoded X.509 format. You select this server certificate when you configure the KMIP server on the key manager. If you plan to use two to four key managers with a Cloud ONTAP system, the same certificate authority (CA) must sign the server certificate for each key manager.
Key managers must trust the signing CA	The CA that signed the server certificate must be known and trusted by the key manager.
Key managers must have a KMIP server	Each key manager must have a KMIP server that uses SSL and a specific port. The default and recommended port for Cloud ONTAP is 5696. If needed, you can change this port when you set up Cloud Manager.
Key managers must have a network connection to Cloud ONTAP systems	If the key managers are in AWS, they must have a connection to the subnet in which Cloud ONTAP instances are running. If the key managers are in your network, a VPN connection to the VPC provides the required connection. Firewall settings must allow communication through the KMIP port.

Requirement	Description
Key managers must trust the Cloud Manager CA and its root CA, if using client certificate authentication	When you set up Cloud Manager, you configure it to act as an intermediate CA so it can sign Cloud ONTAP client certificates. If a KMIP server requires client certificate authentication, then the Cloud Manager intermediate CA must be known and trusted by key managers. The root CA that signed the Cloud Manager certificate must also be known and trusted by the key manager.
Key managers must check a compatible user name field, if using client certificate authentication	If the key manager's KMIP server checks for a user name in client certificates, it must use a field compatible with Cloud ONTAP client certificates. Cloud Manager can create Cloud ONTAP client certificates that include a user name in the CN (Common Name), E (Email address), and OU (Organizational Unit) fields.

The following graphic depicts these requirements:



Notes:

1. The Cloud Manager intermediate CA and its root CA must be trusted only if the KMIP server requires client certificate authentication.
2. The same CA must have signed the server certificate for both key managers. This CA is called the *key manager CA*.

Related tasks

[Setting up Cloud Manager for Cloud ONTAP encryption](#) on page 34

Planning how to organize users and storage across tenants

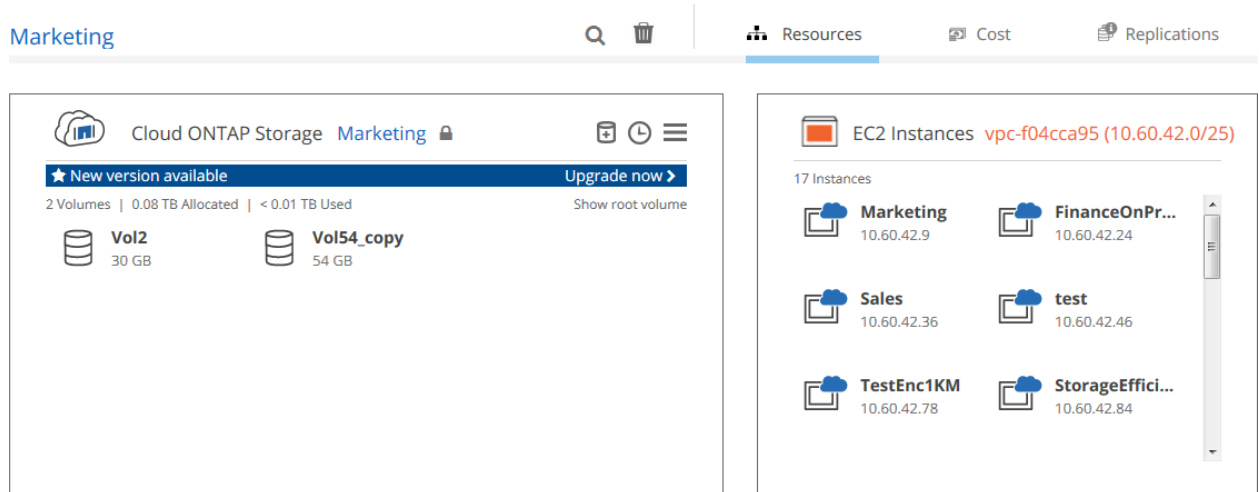
Cloud Manager enables you to provision and manage storage in isolated groups called *tenants*. You need to decide how to organize Cloud Manager users and their working environments across tenants.

Working environments

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

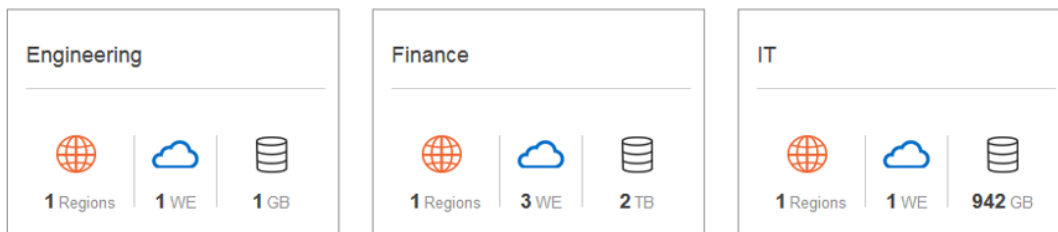
- A Cloud ONTAP system
- An on-premises Data ONTAP cluster in your network
- A Data ONTAP cluster in a NetApp Private Storage configuration

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:



User management of tenants and working environments

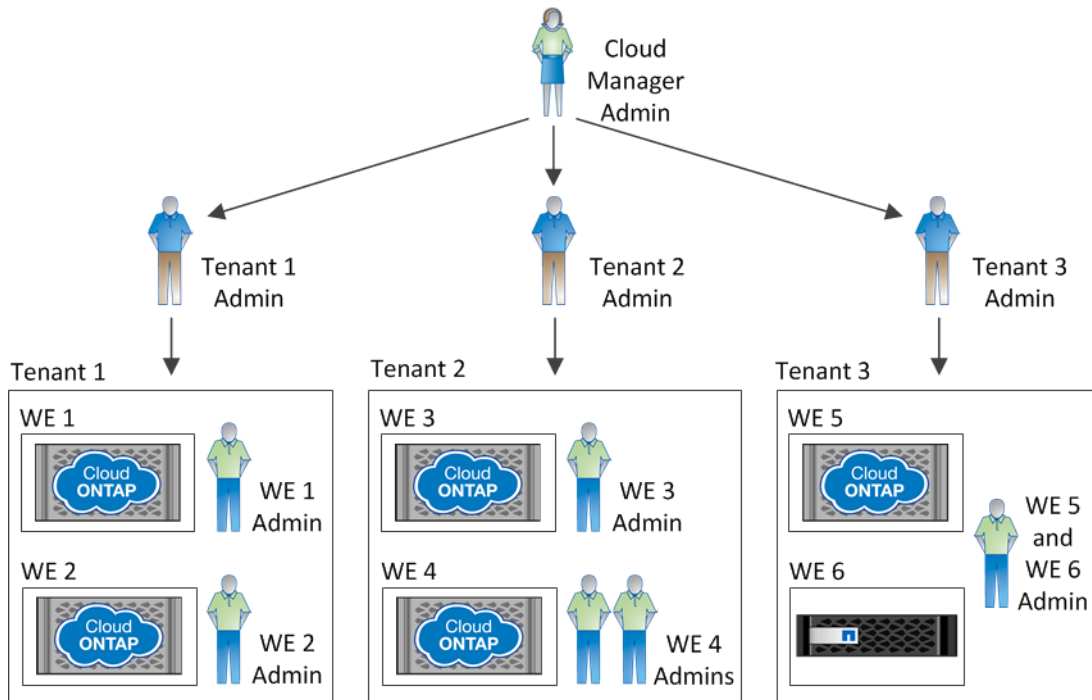
The tenants and working environments that Cloud Manager users can manage depends on user role and assignments. The three distinct user roles are as follows:

- **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.

You assign Tenant Admins and Working Environment Admins to a specific tenant when creating the user accounts. You can also assign Working Environment Admins to specific working environments, if the tenant has preexisting working environments. Working Environment Admins can also create their own working environments.

Example of how you might create tenants and users

If your organization has departments that operate independently, it is best to have a tenant for each department. For example, you might create three tenants for three separate departments. You would then create a Tenant Admin for each tenant. Within each tenant would be one or more Working Environment Admins who manage working environments. The following image depicts this scenario:



Credentials that you need for Cloud Manager

You must provide credentials for several accounts and components as you install and use Cloud Manager. Because there are quite a few credentials, it is helpful to understand which credentials you and your Cloud Manager users need to provide and when you need to provide them.

As you install and set up Cloud Manager, you might need to provide or create the following credentials:

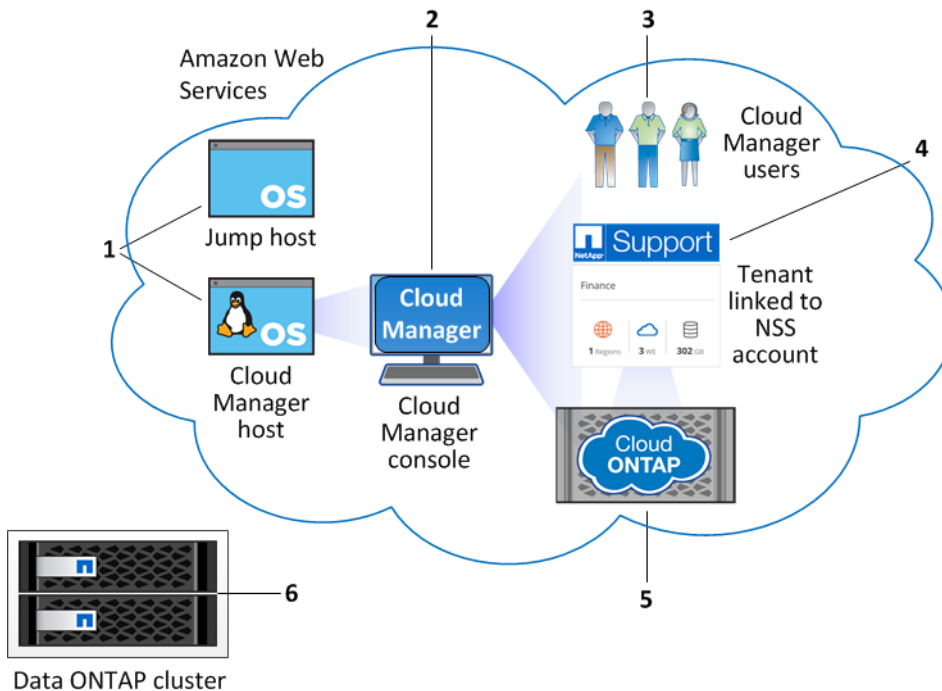
No.	Credentials	Purpose
1	AWS instance credentials for a jump host or the Cloud Manager instance	You might use a jump host to connect to the Cloud Manager web console if the Cloud Manager instance does not have a public IP address in AWS. A jump host is also necessary to manage Cloud ONTAP using System Manager or the CLI. The jump host might be the Cloud Manager instance. Both cases assume you do not have a VPN connection to the private IP addresses.

No.	Credentials	Purpose
2	Cloud Manager web console credentials	When you set up Cloud Manager, you create the credentials that you, as the Cloud Manager Admin, will use to log in to Cloud Manager.
3	AWS access keys for Cloud Manager users	When you create Cloud Manager users, you need to provide Cloud Manager with the AWS access keys for each user.
4	NetApp Support Site credentials	When you create a tenant, you can enter credentials for a NetApp Support Site account so Cloud Manager automatically registers and activates support for each Cloud ONTAP pay-as-you-go instance created in the tenant. If you do not enter credentials, then you need to manually register each instance.

After you set up Cloud Manager, Cloud Manager users can work with the following credentials:

No.	Credentials	Purpose
5	Cloud ONTAP credentials	When users create a Cloud ONTAP system, they need to enter the password for the admin account, which they can use to manage Cloud ONTAP through System Manager or the CLI, if necessary.
6	Clustered Data ONTAP credentials	When users discover a Data ONTAP cluster that is in your network or part of a NetApp Private Storage configuration, they must enter the password for the admin account.

The following graphic shows an AWS environment and identifies the components or users for which you need to provide credentials. The numbers correspond to the previous tables.



Installation and setup worksheet

You need to enter information about your environment when you install and set up Cloud Manager. You can use a worksheet to collect the information that you need.

Information needed to launch the Cloud Manager instance in AWS

Information	Your value
Instance type	
Virtual Private Cloud	
Subnet	
Security Group (if using your own)	
EC2 key pair	

Information needed to define tenants

Information	Your values
Tenant name and NetApp Support Site account for automatic registration of Cloud ONTAP pay-as-you-go instances	

Information needed to set up Cloud Manager for Cloud ONTAP encryption

Key manager #1	Your value
Name	
IP address	
(Optional) Field and key manager user name for client authentication	
Key manager CA certificate available to copy and paste?	

Key manager #2	Your value
Name	
IP address	
(Optional) Field and key manager user name for client authentication	
Key manager CA certificate available to copy and paste?	

Subscribing to Cloud ONTAP in AWS

Before you can launch Cloud ONTAP instances, you must subscribe to Cloud ONTAP in AWS. If you do not subscribe, then you cannot launch a Cloud ONTAP instance from Cloud Manager. You should subscribe to each Cloud ONTAP product that you plan to use.

About this task

Subscribing to Cloud ONTAP means that you have accepted the terms of the product. Subscribing does not cost you anything until you launch a Cloud ONTAP instance.

If the AWS master account (or IAM administrative user) subscribes to the software, then IAM users are also subscribed, if they have appropriate permissions.

Steps

1. Go to the AWS Marketplace pages for Cloud ONTAP:

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

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

2. Review the terms, and then click **Accept**.

After you finish

You must use Cloud Manager to launch Cloud ONTAP instances. You must not launch Cloud ONTAP instances from the EC2 console.

Related information

[*AWS Documentation: Controlling Access to AWS Marketplace Subscriptions*](#)

Installing OnCommand Cloud Manager

You can install the Cloud Manager software by launching a Cloud Manager instance in Amazon Web Services or by installing Cloud Manager on an existing Linux host.

Choices

- [Launching a Cloud Manager instance in AWS](#) on page 28
- [Installing Cloud Manager on an existing Linux host](#) on page 29

Launching a Cloud Manager instance in AWS

To run Cloud Manager in Amazon Web Services (AWS), you must subscribe to Cloud Manager and launch an EC2 instance from the Cloud Manager AMI, which is available on the AWS Marketplace. The Cloud Manager software is automatically installed on the instance.

Before you begin

- You must have an EC2 key pair.
AWS uses the key pair to secure the instance's login information.
[Amazon Web Services \(AWS\) Documentation: Amazon EC2 Key Pairs](#)
- If you want to assign a public IP address to the Cloud Manager instance and use the AWS **1-Click Launch** option, the public subnet must be already enabled to automatically assign public IP addresses.
[AWS Documentation: IP Addressing in Your VPC](#)
Otherwise, you must use the **Manual Launch** option to assign a public IP address to the instance.

Steps

1. Go to the Cloud Manager page on the AWS Marketplace.
[AWS Marketplace: OnCommand Cloud Manager](#)
2. Click **Continue**.
3. On the **1-Click Launch** tab, specify the settings for the instance.
Note: You can also launch the instance from the Manual Launch tab; however, using 1-Click Launch provides the default settings and is typically faster. If you choose a manual launch, you must accept the terms, which subscribes you and gives you access to the Cloud Manager software.

Note the following when you choose settings for the Cloud Manager instance:
 - The **t2.medium** and **m3.medium** instance types are supported.
t2.medium is recommended.
 - When you select a security group, the **Create new based on seller settings** option creates a pre-defined security group that includes the rules required by Cloud Manager.
If you use your own security group, it must include the required inbound and outbound rules.
[AWS networking requirements for Cloud Manager](#) on page 10
4. Subscribe to Cloud Manager and launch the instance by clicking **Accept Terms and Launch with 1-Click**.

Result

AWS launches the Cloud Manager instance with the specified settings. The instance and Cloud Manager software should be running in approximately five minutes.

After you finish

Log in to Cloud Manager using a web browser and complete the Setup wizard. For first time setup, see [Setting up OnCommand Cloud Manager](#) on page 30. For importing an existing configuration, see [Importing your Cloud Manager configuration](#) on page 41.

Installing Cloud Manager on an existing Linux host

You can install the Cloud Manager software on an existing Linux host in your network or in AWS. This is an alternative to running Cloud Manager on a new AWS instance launched from the Cloud Manager AMI.

About this task

Root privileges are not required to install Cloud Manager.

Steps

1. Download the software from the NetApp Support Site and copy it to the Linux host.

For help with connecting and copying the file to an EC2 instance in AWS, see [AWS Documentation: Connecting to Your Linux Instance Using SSH](#).

2. Assign permissions to execute the script.

Example

```
chmod +x OnCommandCloudManager-V2.1.0.sh
```

3. Run the installation script:

```
./OnCommandCloudManager-V2.1.0.sh [silent] [proxy=ipaddress]
[proxyport=port]
```

`silent` runs the installation without prompting you for information.

`proxy` is required if the Cloud Manager host is behind a proxy server.

`proxyport` is the port for the proxy server.

4. Unless you specified the `silent` parameter, type **Y** to continue the script and then enter the HTTP and HTTPS ports when prompted.

If you change the HTTP and HTTPS ports, you must ensure that users can access the Cloud Manager web console from a remote host:

- In AWS, modify the instance's security group to allow inbound connections through the ports.
- Specify the port when you enter the URL to the Cloud Manager web console.

After you finish

Log in to Cloud Manager using a web browser and complete the Setup wizard. For first time setup, see [Setting up OnCommand Cloud Manager](#) on page 30. For importing an existing configuration, see [Importing your Cloud Manager configuration](#) on page 41.

Setting up OnCommand Cloud Manager

The Cloud Manager Setup wizard appears when you access the web console for the first time. The wizard enables you to perform essential setup tasks.

Before you begin

You should have prepared for Cloud Manager setup.

[Preparing for installation and setup](#) on page 9

About this task

If you recently launched a Cloud Manager instance in Amazon Web Services (AWS), the Cloud Manager console should be available a few minutes after the AWS instance starts.

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 Setup wizard appears:

Welcome to OnCommand Cloud Manager

This is NetApp's most advanced solution for managing your storage

Just a quick setup wizard and you'll be ready to create your first working environment!

Set up new Cloud Manager

OR

Restore from existing Cloud Manager

2. Complete the steps in the **Setup** wizard:

On this page...	Do this...
Welcome	Click Set up new Cloud Manager .
EULA	Read the End User License Agreement and, if you approve, click I read and approve the EULA .

On this page...	Do this...
Proxy Setup	Optionally, enter the location to a proxy server using the syntax http://address:port. If your corporate policies dictate that you use a proxy server for all HTTP communication to the Internet, then you must configure Cloud Manager to use that proxy server. The proxy server can be in AWS or in your network. You can set the proxy server later from the Cloud Manager Settings page. After you specify the proxy server, new Cloud ONTAP systems are automatically configured to use the proxy server when sending AutoSupport messages. If you do not specify the proxy server before users create Cloud ONTAP systems, then they must use System Manager to manually set the proxy server in the AutoSupport options for each system.
Let us know who you are	Specify your site and company name.
Create an admin user	Specify details to create an administrator user for Cloud Manager. You use this user account to log in to Cloud Manager. Your user name is your email address. Cloud Manager does not send emails to this address.
AWS Credentials	Specify AWS keys that Cloud Manager should use for the administrator user account and specify an S3 bucket that contains detailed billing reports, if you entered keys for an AWS account under which the bucket was created. You can add this information later by editing the user account. Note the following: - Cloud Manager uses the keys to perform AWS actions on your behalf. 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 - 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. Setting up AWS billing and cost management on page 17
Create your first tenant	Enter a name, description, and cost center for your first tenant. Planning how to organize users and storage across tenants on page 23
NetApp Support Site credentials	Enter credentials for a NetApp Support Site account so Cloud Manager can automatically register and activate support for each Cloud ONTAP pay-as-you-go instance created in the tenant. If you do not specify credentials for a tenant, Cloud Manager users need to manually register each instance individually after they are launched.

After you finish

Continue setting up Cloud Manager by doing the following:

- Installing a TLS certificate for secure HTTPS access
- Creating additional tenants
- Creating user accounts so other users can access Cloud Manager
- Setting up Cloud Manager so users can use Cloud ONTAP encryption

Installing an HTTPS certificate for secure access

By default, Cloud Manager uses a self-signed certificate for HTTPS access to the web console. You can install a certificate signed by a certificate authority (CA), which provides better security protection than a self-signed certificate.

Steps

1. In the upper right of the Cloud Manager console, click the task drop-down list, and then select **HTTPS Setup**.
2. In the **HTTPS Setup** page, enter the host name or DNS of the Cloud Manager host (its Common Name), and then click **Generate CSR**.

Cloud Manager displays a certificate signing request.

3. Use the CSR to submit an SSL certificate request to a CA.
The certificate must use the Privacy Enhanced Mail (PEM) Base-64 encoded X.509 format.
4. Copy the content of the signed certificate, paste it in the **Certificate** field, and then click **Install**.

Result

Cloud Manager now uses the CA-signed certificate to provide secure HTTPS access. The following image shows a Cloud Manager system that is configured for secure access:

Cloud Manager HTTPS certificate

Expiration:	 Oct 27, 2016 05:13:28 am
Issuer:	CN=localhost, O=NetApp, OU=Tel-Aviv, EMAILADDRESS=admin@example.com
Subject:	EMAILADDRESS=admin@example.com, OU=Tel-Aviv, O=NetApp, CN=localhost
 View Certificate	
Renew HTTPS Certificate	

Defining tenants

You can create additional tenants beyond the single tenant that you created when using the Setup wizard. Using tenants enables you to easily organize and isolate storage resources in groups.

Steps

1. In Cloud Manager, click **Tenants**.
2. Click the + icon.
3. In the **New Tenant** page, specify details for the tenant:
 - a. Enter a name, description, and cost center for the tenant.

The Description and Cost Center fields are optional.

- b. Enter credentials for a NetApp Support Site account so Cloud Manager can automatically register and activate support for each Cloud ONTAP pay-as-you-go instance created in the tenant.

If you do not specify credentials for a tenant, Cloud Manager users need to manually register each instance individually after they are launched.

4. Click **Save**.

Result

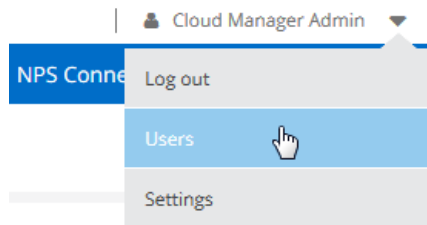
Cloud Manager creates the tenant. Users can create and discover working environments in the tenant.

Creating user accounts

If multiple people in your organization need to use Cloud Manager, then you need to create Cloud Manager user accounts for each user. You can create several types of users: Cloud Manager administrators, tenant administrators, and working environment administrators.

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.

Most 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	Select one of the three roles: • 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 you create a Working Environment Admin user, you need to 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 later. Note: Working Environment Admin users automatically have privileges to the working environments that they create.

Field	Description
AWS Access Key and AWS 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.

4. Click **Save**.

Result

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

Related tasks

[Setting up AWS billing and cost management for Cloud Manager](#) on page 17

Setting up Cloud Manager for Cloud ONTAP encryption

The Cloud Manager Admin user must set up Cloud Manager before other users can enable Cloud ONTAP encryption on new Cloud ONTAP systems. Setup involves configuring Cloud Manager to be an intermediate certificate authority (CA), entering information about key managers, and adding CA certificates for key managers.

Before you begin

You must have set up key managers and gathered the required information.

[Key manager requirements for Cloud ONTAP encryption](#) on page 21

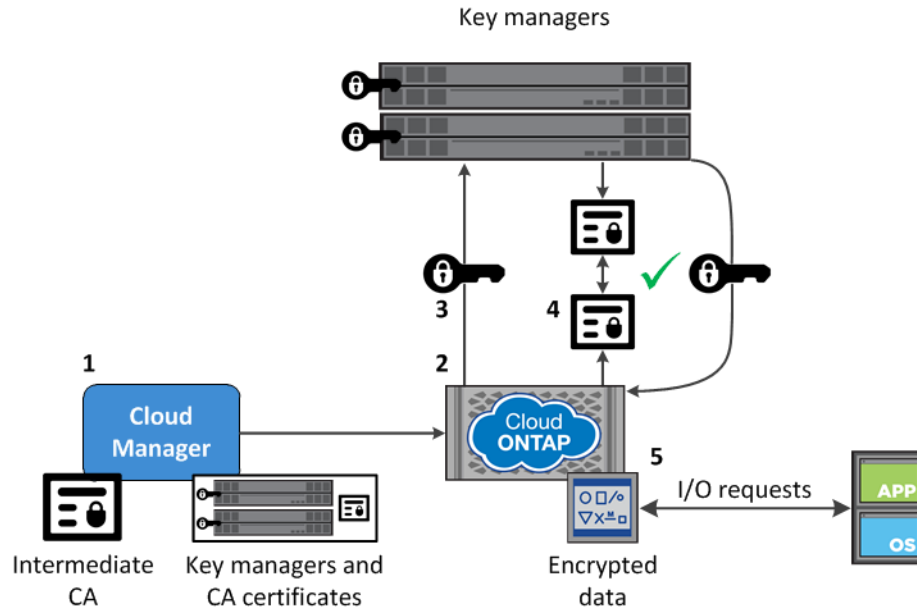
Steps

1. [Understand how Cloud ONTAP encryption works](#) on page 35
Understanding how Cloud ONTAP encryption works can help you set up and use the feature.
2. [Set up Cloud Manager to be an intermediate CA](#) on page 36
Cloud Manager must be an intermediate certificate authority (CA) because it needs to create client certificates for Cloud ONTAP. You set up Cloud Manager to be an intermediate CA by generating a certificate signing request (CSR), getting the CSR signed by a root CA, and then installing the certificate in Cloud Manager.
3. [Add key managers and their CA certificates to Cloud Manager](#) on page 36
Cloud Manager needs information about your key managers and CA certificates so users can select them for use with Cloud ONTAP systems.

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.
4. 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.
5. Before data is written to disk, it is encrypted using XTS-AES.
 When data is read from disk, the encrypted data is decrypted using XTS-AES before being sent.

Setting up Cloud Manager to be an intermediate CA

Cloud Manager must be an intermediate certificate authority (CA) because it needs to create client certificates for Cloud ONTAP. You set up Cloud Manager to be an intermediate CA by generating a certificate signing request (CSR), getting the CSR signed by a root CA, and then installing the certificate in Cloud Manager.

Steps

1. In the upper-right corner of the Cloud Manager console, click the task drop-down list, and then select **Encryption Setup**.
2. In the **Intermediate CA** tab, click **Generate CSR**.
Cloud Manager displays a certificate signing request.
3. Use the CSR to submit a certificate request to a CA.
The intermediate CA certificate must use the Privacy Enhanced Mail (PEM) Base-64 encoded X.509 format.
4. Copy the content of the signed certificate and paste it in the **Cloud Manager certificate** field.
5. Click **Install Cloud Manager Certificate**.

Result

Cloud Manager is now an intermediate CA—it can sign client certificates for Cloud ONTAP systems. The following image shows a Cloud Manager system that is configured to be an intermediate CA:

Cloud Manager is configured as an Intermediate CA



Cloud Manager certificate

Expiration:	Sep 22, 2016 04:33:30 am
Issuer:	C=il, ST=Some-State, L=tlv, O=netapp, OU=occm, CN=yh1
Subject:	CN=OCCM, O=NetApp, OU=Tel-Aviv, E=cloudmgr@netapp.com

[View Certificate](#)

[Resume renewal process](#)

After you finish

If a KMIP server requires client certificate authentication, add the Cloud Manager intermediate CA and its root CA to the key manager's list of trusted CAs. This step is necessary because the key manager must verify that Cloud ONTAP client certificates were signed by a trusted CA.

Adding key managers and CA certificates to Cloud Manager

Cloud Manager needs information about your key managers and CA certificates so users can select them for use with Cloud ONTAP systems.

Steps

1. In the **Encryption Setup** page, click **Key Manager**.
2. If your key managers use a KMIP port other than 5696, change the port and then click **Save**.
Cloud Manager configures Cloud ONTAP systems to connect to key managers using this port.

3. In the **Key Managers** table, click **Add**.
4. In the **Add Key Manager** dialog box, enter details about the key manager, and then click **Add**:

In this field...	Do this...
Key Manager Name	Enter a unique name to distinguish the key manager.
IP Address	Enter the IP address of the key manager.
User Name for Client Certificate Authentication	If the key manager is enabled for client certificate authentication by having the key manager verify a user name from client certificates, specify the field and user name: - Select the field in which the key manager should look for a user name. - Enter a user name that is defined in the key manager. Cloud Manager generates Cloud ONTAP client certificates with the value defined in the user name field.

5. In the **Key Managers' CA Certificates** table, click **Add**.
6. Paste the certificate of the certificate authority (CA) that signed the key manager's server certificate and then click **Add**.
7. Repeat the steps for any additional key managers and their CA certificates.

Result

Cloud Manager is now set up to create Cloud ONTAP systems with encryption enabled.

What to do after installation and setup

After you set up Cloud Manager, users can launch Cloud ONTAP instances, discover Data ONTAP clusters, and replicate data to and from the cloud. When necessary, you can also administer Cloud Manager and use online resources to get help.

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

Tasks	Resources
Create and manage working environments using the web console: - Launch Cloud ONTAP instances - Provision storage for Cloud ONTAP - Discover on-premises FAS systems and existing NetApp Private Storage configurations - Replicate data to and from the cloud	OnCommand Cloud Manager 2.1 Storage Management Guide
Administer Cloud Manager using the web console: - Back up Cloud Manager - Manage user accounts - Configure Cloud Manager settings - Troubleshoot issues	OnCommand Cloud Manager 2.1 Administration Guide
Use REST APIs for automation	Swagger interface available from http://server/occm/api-doc/ OnCommand Cloud Manager 2.1 API Getting Started Guide
Review release-specific information (known issues, limitations, and so on) for Cloud Manager and Cloud ONTAP	OnCommand Cloud Manager 2.1 Release Notes Find the Release Notes for your version of Cloud ONTAP
View more documentation and videos for Cloud ONTAP and Cloud Manager	NetApp Cloud ONTAP Resources
Get help	NetApp Cloud ONTAP Support NetApp Community: Hybrid Cloud

Updating Cloud Manager to version 2.1

Because Cloud Manager 2.1 is supported on Linux only, you cannot directly upgrade from a previous release. You must set up Cloud Manager 2.1 on a new host or instance and import your existing configuration. You should then set Cloud Manager as the cluster configuration backup target, remove your previous Cloud Manager configuration, and then terminate the NetApp Support instance.

Steps

1. [Install Cloud Manager 2.1](#) on page 39
You can install the Cloud Manager software by launching a Cloud Manager instance in Amazon Web Services or by installing Cloud Manager on an existing Linux host.
2. [Import your existing Cloud Manager configuration](#) on page 41
After you install Cloud Manager on a new host, you can import an existing configuration to the new Cloud Manager database. This step is required when updating to version 2.1.
3. [Set Cloud Manager as the target for Cloud ONTAP configuration backups](#) on page 42
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.
4. [Remove your previous Cloud Manager configuration](#) on page 42
You no longer need your previous Cloud Manager configuration after you import the database into your new configuration. You can terminate the instance in AWS or uninstall the software.
5. [Terminate the NetApp Support instance](#) on page 43
You can terminate the NetApp Support instance from the EC2 console after you upgrade to Cloud Manager 2.1 and configure Cloud ONTAP instances to send configuration backups to Cloud Manager.

Installing OnCommand Cloud Manager

You can install the Cloud Manager software by launching a Cloud Manager instance in Amazon Web Services or by installing Cloud Manager on an existing Linux host.

Choices

- [Launching a Cloud Manager instance in AWS](#) on page 39
- [Installing Cloud Manager on an existing Linux host](#) on page 40

Launching a Cloud Manager instance in AWS

To run Cloud Manager in Amazon Web Services (AWS), you must subscribe to Cloud Manager and launch an EC2 instance from the Cloud Manager AMI, which is available on the AWS Marketplace. The Cloud Manager software is automatically installed on the instance.

Before you begin

- You must have an EC2 key pair.
AWS uses the key pair to secure the instance's login information.
[Amazon Web Services \(AWS\) Documentation: Amazon EC2 Key Pairs](#)
- If you want to assign a public IP address to the Cloud Manager instance and use the AWS **1-Click Launch** option, the public subnet must be already enabled to automatically assign public IP addresses.

[AWS Documentation: IP Addressing in Your VPC](#)

Otherwise, you must use the **Manual Launch** option to assign a public IP address to the instance.

Steps

1. Go to the Cloud Manager page on the AWS Marketplace.

[AWS Marketplace: OnCommand Cloud Manager](#)

2. Click **Continue**.
3. On the **1-Click Launch** tab, specify the settings for the instance.

Note: You can also launch the instance from the Manual Launch tab; however, using 1-Click Launch provides the default settings and is typically faster. If you choose a manual launch, you must accept the terms, which subscribes you and gives you access to the Cloud Manager software.

Note the following when you choose settings for the Cloud Manager instance:

- The **t2.medium** and **m3.medium** instance types are supported. **t2.medium** is recommended.
- When you select a security group, the **Create new based on seller settings** option creates a pre-defined security group that includes the rules required by Cloud Manager. If you use your own security group, it must include the required inbound and outbound rules. [AWS networking requirements for Cloud Manager](#) on page 10

4. Subscribe to Cloud Manager and launch the instance by clicking **Accept Terms and Launch with 1-Click**.

Result

AWS launches the Cloud Manager instance with the specified settings. The instance and Cloud Manager software should be running in approximately five minutes.

After you finish

Log in to Cloud Manager using a web browser and complete the Setup wizard. For first time setup, see [Setting up OnCommand Cloud Manager](#) on page 30. For importing an existing configuration, see [Importing your Cloud Manager configuration](#) on page 41.

Installing Cloud Manager on an existing Linux host

You can install the Cloud Manager software on an existing Linux host in your network or in AWS. This is an alternative to running Cloud Manager on a new AWS instance launched from the Cloud Manager AMI.

About this task

Root privileges are not required to install Cloud Manager.

Steps

1. Download the software from the NetApp Support Site and copy it to the Linux host.

For help with connecting and copying the file to an EC2 instance in AWS, see [AWS Documentation: Connecting to Your Linux Instance Using SSH](#).

2. Assign permissions to execute the script.

Example

```
chmod +x OnCommandCloudManager-V2.1.0.sh
```

3. Run the installation script:

```
./OnCommandCloudManager-V2.1.0.sh [silent] [proxy=ipaddress]
[proxyport=port]
```

`silent` runs the installation without prompting you for information.

`proxy` is required if the Cloud Manager host is behind a proxy server.

`proxyport` is the port for the proxy server.

4. Unless you specified the `silent` parameter, type **Y** to continue the script and then enter the HTTP and HTTPS ports when prompted.

If you change the HTTP and HTTPS ports, you must ensure that users can access the Cloud Manager web console from a remote host:

- In AWS, modify the instance's security group to allow inbound connections through the ports.
- Specify the port when you enter the URL to the Cloud Manager web console.

After you finish

Log in to Cloud Manager using a web browser and complete the Setup wizard. For first time setup, see [Setting up OnCommand Cloud Manager](#) on page 30. For importing an existing configuration, see [Importing your Cloud Manager configuration](#) on page 41.

Importing your Cloud Manager configuration

After you install Cloud Manager on a new host, you can import an existing configuration to the new Cloud Manager database. This step is required when updating to version 2.1.

Before you begin

The new Cloud Manager host must have connectivity to the existing Cloud Manager host. If the host does not have connectivity, you must manually back up your existing configuration, choose the option to set up a new Cloud Manager configuration, and then import the backup into the new Cloud Manager configuration.

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`

2. Click **Restore from existing Cloud Manager**.
3. Enter the host name or IP address of your existing Cloud Manager host, enter your Cloud Manager user name and password, accept the EULA, and then click **Restore**.

Result

The new Cloud Manager configuration accesses your previous Cloud Manager configuration, generates a backup, and then imports the configuration.

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.

Removing your previous Cloud Manager configuration

You no longer need your previous Cloud Manager configuration after you import the database into your new configuration. You can terminate the instance in AWS or uninstall the software.

Choices

- [Terminating the Cloud Manager instance](#) on page 42
- [Uninstalling the Cloud Manager software](#) on page 43

Terminating the Cloud Manager instance

When you no longer need the Cloud Manager instance in AWS, you can terminate it from the EC2 console.

Step

1. From the AWS EC2 console, select the Cloud Manager instance and click **Terminate**.

Uninstalling the Cloud Manager software

You can uninstall Cloud Manager when you want to update to the latest version or when you no longer need the software.

Steps

1. In the Windows Control Panel, open the **Programs and Features** application, and then select **NetApp OnCommand Cloud Manager**.
2. Click **Uninstall** and then follow the prompts to uninstall the software.

Terminating the NetApp Support instance

You can terminate the NetApp Support instance from the EC2 console after you upgrade to Cloud Manager 2.1 and configure Cloud ONTAP instances to send configuration backups to Cloud Manager.

About this task

The NetApp Support instance is no longer launched by Cloud Manager because Cloud ONTAP instances launched from Cloud Manager 2.1 and later automatically send configuration backups to Cloud Manager using HTTPS.

Step

1. From the AWS EC2 console, select the NetApp Support instance and click **Terminate**.

Uninstalling Cloud Manager

Cloud Manager includes an uninstallation script that you can use to uninstall the software to troubleshoot issues or to permanently remove the software from the host.

Steps

1. If you are going to reinstall Cloud Manager, back up the database before you uninstall the software:
 - a. In the upper-right corner of the Cloud Manager console, click the task drop-down list, and then select **Tools**.
 - b. Click **Backup** and save the backup file to your local machine.
2. From the Linux host, run the uninstallation script:
`/opt/application/netapp/cloudmanager/bin/uninstall.sh [silent]`
`silent` runs the script without prompting you for confirmation.

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

- accounts
 - creating Cloud Manager users [33](#)
 - credentials for [24](#)
- Amazon Web Services
 - billing and cost requirements [17](#)
 - default limits [17](#)
 - encryption overview [20](#)
 - granting permissions to IAM users [15](#)
 - launching Cloud Manager in [28](#), [39](#)
 - networking requirements for Cloud Manager [10](#)
 - networking requirements for Cloud ONTAP [12](#)
 - preparing [9](#)
 - sample VPC configurations [13](#)
 - subscribing to Cloud ONTAP software from [27](#)
 - what Cloud Manager does with permissions [15](#)
- APIs
 - overview of [7](#)
- AWS
 - See* Amazon Web Services

B

- backups, cluster configuration
 - sending to Cloud Manager [42](#)
- billing and cost requirements
 - verifying IAM user access to billing information [17](#)

C

- certificate signing request
 - generating [36](#)
- certificates
 - adding CA certificates to Cloud Manager [36](#)
 - installing Cloud Manager certificate [36](#)
 - installing HTTPS certificate [32](#)
 - requirements [21](#)
- Chrome
 - supported versions [19](#)
- Cloud Manager
 - See* OnCommand Cloud Manager
- Cloud ONTAP
 - AWS networking requirements for [12](#)
 - encryption overview [20](#)
 - product models [6](#)
 - sending configuration backups to Cloud Manager [42](#)
 - subscribing to the software in AWS [27](#)
 - what it is [6](#)
- Cloud ONTAP encryption
 - understanding how it works [35](#)
- cluster configuration backups
 - sending to Cloud Manager [42](#)
- comments
 - how to send feedback about documentation [47](#)
- components
 - credentials for [24](#)
- configuration, Cloud Manager

importing [41](#)

- cost
 - requirements to display in Cloud Manager [17](#)
- CPU
 - required for Cloud Manager [19](#)
- credentials
 - types of and purposes [24](#)

D

- disk space
 - required for Cloud Manager [19](#)
- documentation
 - how to receive automatic notification of changes to [47](#)
 - how to send feedback about [47](#)
 - where to find additional [38](#)

E

- encryption
 - deciding whether to use [20](#)
 - key manager requirements [21](#)
 - setting up Cloud Manager for [34](#)
 - understanding how it works in Cloud ONTAP [35](#)

F

- feedback
 - how to send comments about documentation [47](#)
- Firefox
 - supported versions [19](#)

H

- HTTPS certificate
 - installing [32](#)

I

- IAM users
 - granting permissions to [15](#)
 - what Cloud Manager does with permissions [15](#)
- information
 - how to send feedback about improving documentation [47](#)
- installation
 - gathering information for [26](#)
 - preparing for OnCommand Cloud Manager [9](#)
 - what to do after [38](#)
 - worksheets [26](#)
- installing OnCommand Cloud Manager
 - on existing hosts [29](#), [40](#)
 - workflow [8](#)
- instance
 - terminating, Cloud Manager [42](#)
 - terminating, NetApp Support [43](#)
- instance limits

- for AWS [17](#)
- intermediate CA
 - setting up Cloud Manager [36](#)
- Internet Explorer
 - supported versions [19](#)

K

- key managers
 - adding to Cloud Manager [36](#)
 - requirements [21](#)
- KMIP server
 - requirements [21](#)

N

- NetApp Support instance
 - terminating [43](#)

O

- OnCommand Cloud Manager
 - AWS networking requirements for [10](#)
 - billing and cost requirements [17](#)
 - creating admin user of [33](#)
 - creating user accounts [33](#)
 - EC2 instance requirements [19](#)
 - host requirements [19](#)
 - importing an existing configuration [41](#)
 - information needed to launch in AWS [26](#)
 - installation and setup workflow [8](#)
 - installing [29, 40](#)
 - launching in AWS [28, 39](#)
 - preparing for installation and setup [9](#)
 - setting up [30](#)
 - setting up to be intermediate CA [36](#)
 - supported web browsers [19](#)
 - terminating the instance [42](#)
 - uninstalling [43, 44](#)
 - what it is [5](#)
- operating system
 - required for Cloud Manager [19](#)

P

- permissions
 - granting to IAM users [15](#)
 - purposes of [15](#)
- ports
 - requirements for Cloud Manager [10](#)
 - requirements for Cloud ONTAP [12](#)
- proxy server
 - configuring Cloud Manager to use [30](#)

R

- RAM
 - required for Cloud Manager [19](#)

S

- security groups
 - requirements for Cloud Manager [10](#)
 - requirements for Cloud ONTAP [12](#)
- setup
 - credentials used for OnCommand Cloud Manager [24](#)
 - gathering information for [26](#)
 - preparing for OnCommand Cloud Manager [9](#)
 - what to do after [38](#)
 - workflow [8](#)
 - worksheets [26](#)
- SSL certificates
 - requirements [21](#)
- storage limits
 - for AWS [17](#)
- subnets
 - requirements for Cloud Manager [10](#)
 - requirements for Cloud ONTAP [12](#)
- suggestions
 - how to send feedback about documentation [47](#)

T

- tenants
 - creating admin user of [33](#)
 - defining in Cloud Manager [32](#)
 - definition of [23](#)
 - how to use [23](#)
- troubleshooting
 - uninstalling software first [44](#)
- twitter
 - how to receive automatic notification of documentation changes [47](#)

U

- uninstalling
 - OnCommand Cloud Manager [44](#)
- updates
 - importing an existing configuration [41](#)
- user accounts
 - creating [33](#)
- users
 - definition of [23](#)

V

- Virtual Private Clouds
 - requirements for Cloud Manager [10](#)
 - requirements for Cloud ONTAP [12](#)
 - sample configurations [13](#)

W

- web browsers
 - supported versions [19](#)
- working environments
 - creating admin user of [33](#)
 - defining tenants for Cloud Manager [32](#)
 - definition of [23](#)