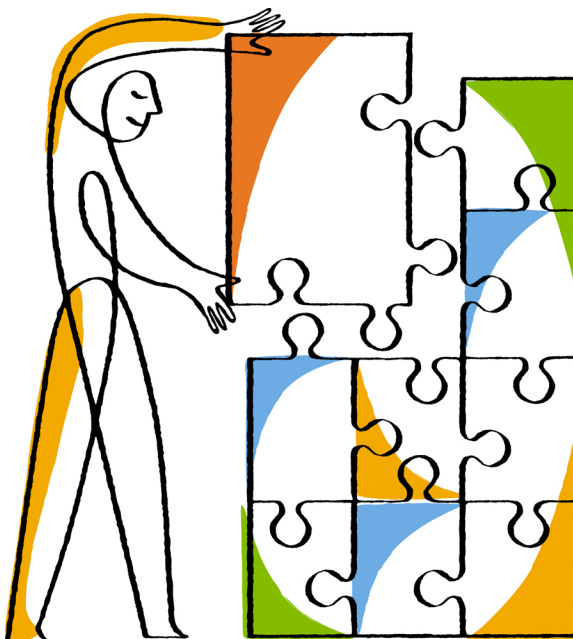




OnCommand® Cloud Manager 1.0

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: 215-09278_A0
November 2014

Contents

Product overview	5
Cloud ONTAP overview	6
What the NetApp Support instance is	7
NetApp Private Storage for AWS overview	8
Installation and setup workflow	9
Preparing for installation and setup	10
Preparing your AWS environment	10
AWS networking requirements for Cloud Manager	11
AWS networking requirements for Cloud ONTAP	13
AWS networking requirements for the NetApp Support instance	16
AWS networking requirements for NetApp Private Storage	17
Granting permissions to IAM users	17
How AWS limits can impact Cloud ONTAP	20
Setting up AWS billing and cost management for Cloud Manager	20
Cloud Manager requirements	23
Credentials that you need for Cloud Manager	24
Gathering information for installation and setup	26
Subscribing to Cloud ONTAP in AWS	28
Installing OnCommand Cloud Manager	29
Launching a Cloud Manager instance in AWS	29
Connecting to the Cloud Manager instance in AWS	30
Installing the Cloud Manager software	31
Setting up OnCommand Cloud Manager	32
Logging in to Cloud Manager	32
Overview of the Cloud Manager console	33
Adding your NetApp Private Storage configuration to Cloud Manager	35
Configuring Cloud Manager to use a proxy server	37
Defining tenants	38
Creating user accounts	38
What to do next	41
Copyright information	42
Trademark information	43

How to send your comments 44

Index 45

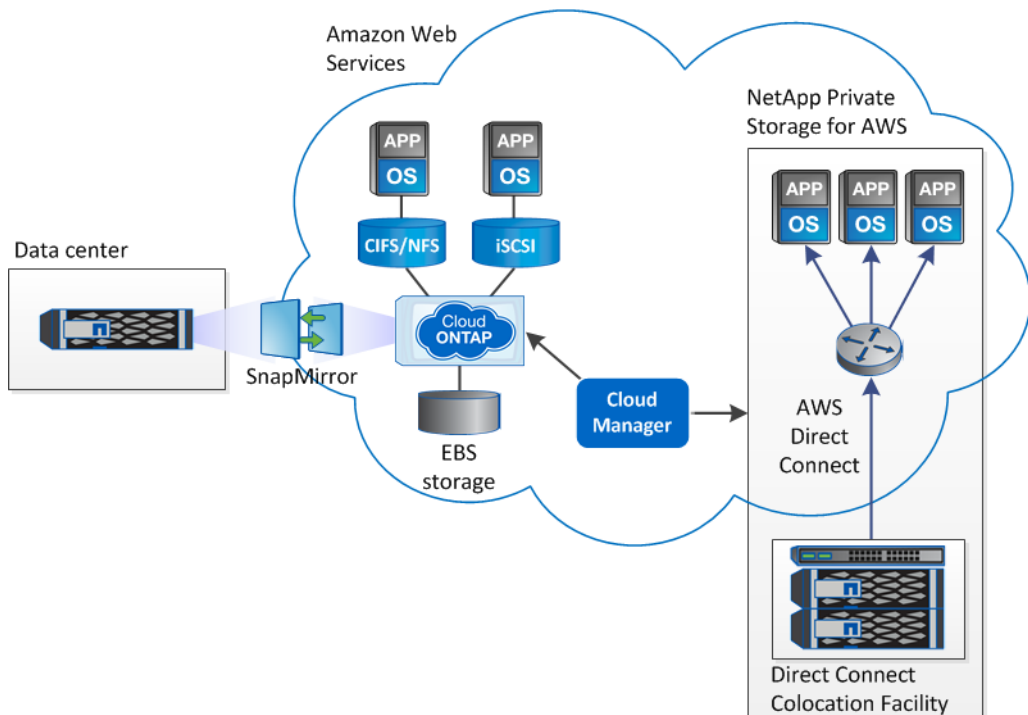
Product overview

OnCommand Cloud Manager helps you set up and manage 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 set up a network connection and Storage Virtual Machine (SVM) for NetApp Private Storage. Using clustered Data ONTAP in your data center and in the cloud gives you the enterprise standard for data management across your hybrid cloud.

Cloud Manager offers the following:

- Point-and-click deployments of Cloud ONTAP instances
- Simplified provisioning of cloud storage for Cloud ONTAP
- Cost monitoring of AWS storage and compute charges associated with Cloud ONTAP instances
- Network connection setup for NetApp Private Storage by connecting a FAS storage system in an AWS colocation facility to an AWS Direct Connect

You can run Cloud Manager in AWS or in your data center. The following graphic shows Cloud Manager running in AWS, managing a Cloud ONTAP instance and NetApp Private Storage:



Cloud ONTAP 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 allows you to easily replicate data between your data center and the cloud.

What Cloud ONTAP provides

Cloud ONTAP manages EBS General Purpose (SSD) storage with NetApp's clustered Data ONTAP storage operating system, which provides enterprise-class features on top of EBS storage:

- Multiprotocol support (NFS, CIFS, and iSCSI)
- Data protection (Snapshot copies, SnapMirror technology, and SnapVault technology)
- Storage efficiency (thin provisioning, data deduplication, and data compression)

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

How you deploy Cloud ONTAP

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

Cloud ONTAP product models

To best fit your application needs, Cloud ONTAP is available in three product models:

Product model	EC2 instance type options	Maximum raw EBS capacity	Payment method
Explore (Hourly)	m3.xlarge	2 TB	Pay by the hour
Standard (Hourly)	m3.xlarge or m3.2xlarge	10 TB	Pay by the hour
Standard (BYOL)	m3.xlarge or m3.2xlarge	50 TB	Bring your own license

How you can use Cloud ONTAP

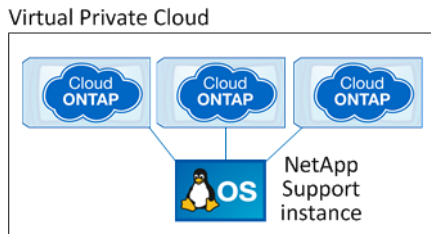
You can use Cloud ONTAP in the following ways:

- To serve data for cloud applications using NFS, CIFS, and iSCSI
- As a SnapMirror source or destination for data replication and disaster recovery
- As a SnapVault source or destination for data archiving

What the NetApp Support instance is

When you launch your first Cloud ONTAP instance in a Virtual Private Cloud (VPC), Cloud Manager also launches the NetApp Support instance in the VPC. The NetApp Support instance, which is an EC2 Linux instance, is the backup location for cluster configuration files and it provides tools for instance changes and for troubleshooting and repairing Cloud ONTAP instances. If you prefer, you can run the tools in your data center.

One NetApp Support instance supports all Cloud ONTAP instances in a VPC:



Cloud ONTAP periodically takes cluster configuration backups and sends them to the NetApp Support instance, which includes an FTP server. If the root volume for a Cloud ONTAP instance fails or becomes inaccessible, NetApp technical support can use the backups to restore the configuration.

Note: The user name for the destination FTP server is supportftp. The password is the ID of the VPC in which the instance is running.

The NetApp Support instance also includes the following tools:

- A script that you can use to change the EC2 instance type for Cloud ONTAP
- Recovery scripts that NetApp technical support can use to troubleshoot and repair Cloud ONTAP

Note: The NetApp Support instance installs the tools from a package available in a NetApp-managed S3 bucket. When you run a script, it automatically checks for a newer version of the tools in the S3 bucket, and if one is available, the script prompts you to upgrade.

The NetApp Support instance is a t1.micro instance that requires 8 GB of magnetic (standard) EBS storage. NetApp strongly recommends that you keep the instance running so that Cloud ONTAP can save the cluster configuration backups to a remote location. However, if you have your own FTP or HTTP server that you want to use for the backups, you can configure Cloud ONTAP to use that location. You can then optionally stop the instance and start it when you or technical support need to use the tools.

As an alternative, you can run the tools on a Linux host in your data center. For instructions, see the [OnCommand Cloud Manager 1.0 Administration Guide](#).

Note: Stopping the instance is the best way to stop accruing compute charges. If you delete the NetApp Support instance, Cloud Manager will launch another instance when you launch a Cloud ONTAP instance in that VPC.

NetApp Private Storage for AWS overview

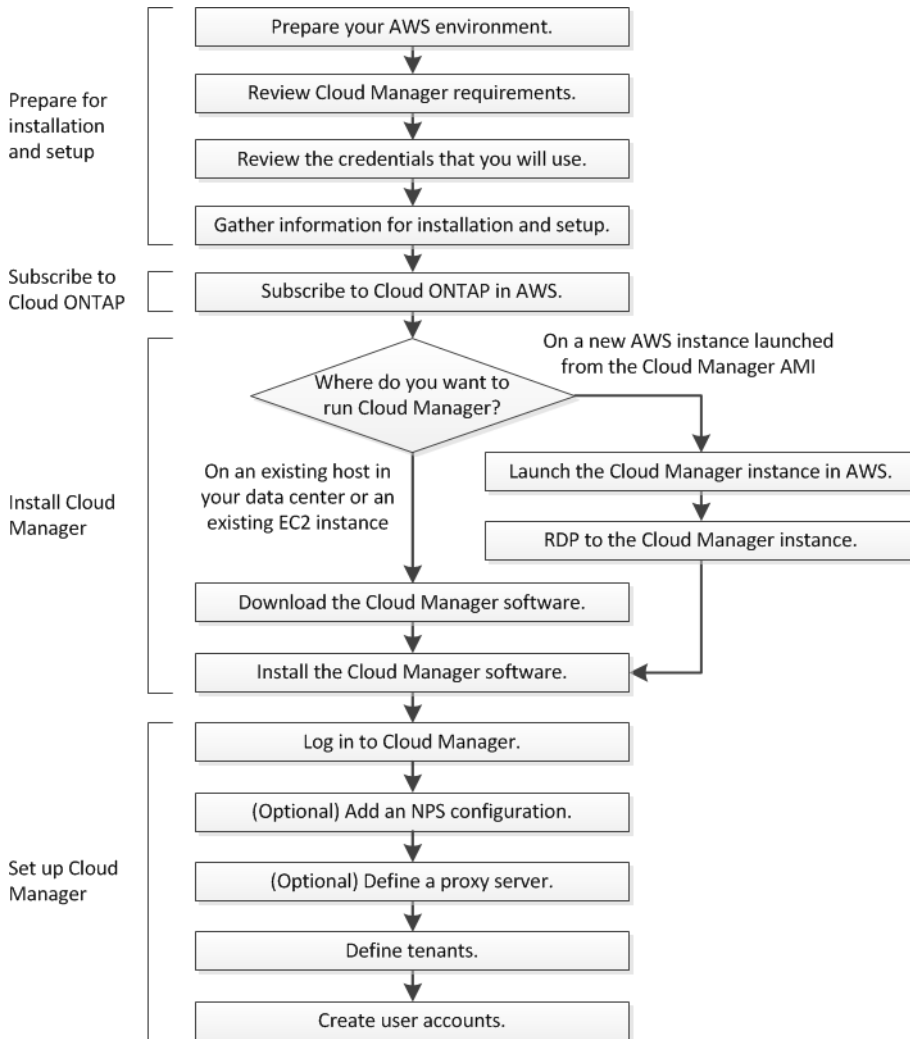
NetApp Private Storage for Amazon Web Services (AWS) combines compute resources from Amazon EC2 with NetApp storage hosted at an Amazon Direct Connect colocation facility. This configuration provides the elasticity and savings of AWS cloud compute with the performance and availability of dedicated enterprise storage.

Amazon Direct Connect provides a dedicated network connection from AWS to a colocation facility that is physically near Amazon data centers. Within the colocation facility, you provide a Layer 3 network switch or router and a NetApp storage system. You can then use OnCommand Cloud Manager to easily configure a connection from the AWS Direct Connect to a Storage Virtual Machine (SVM) on the storage system.

After the configuration is set up, you can connect virtual machines within Amazon EC2 to NetApp storage. This gives you a configuration that leverages cloud computing services and enables you to retain full control and mobility of your enterprise data.

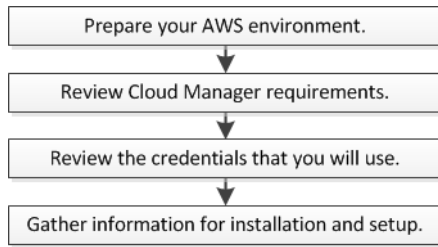
Installation and setup workflow

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 need to prepare your environment and understand the information that you will need for installation and setup.



Preparing your AWS environment

You need to make sure that your AWS environment meets a few requirements to ensure that Cloud Manager can 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. Review AWS networking requirements:
 - [AWS networking requirements for Cloud Manager](#) on page 11
 - [AWS networking requirements for Cloud ONTAP](#) on page 13
 - [AWS networking requirements for the NetApp Support instance](#) on page 16
 - [AWS networking requirements for NetApp Private Storage](#) on page 17
2. Grant the required permissions to IAM users.
[Granting permissions to IAM users](#) on page 17
3. Review AWS default limits so that you do not reach limits that can impact Cloud ONTAP instances.
[How AWS limits can impact Cloud ONTAP](#) on page 20
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 20

5. If you want to launch Cloud Manager in AWS, create an EC2 key pair, if you do not have one already.

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 need to set up your AWS networking (Virtual Private Clouds, subnets, and security groups) so Cloud Manager can launch Cloud ONTAP instances and configure NetApp Private Storage connections.

Requirement	Description
Internet access to AWS services	Cloud Manager needs Internet access to communicate with AWS services so it can launch and manage Cloud ONTAP instances and configure a NetApp Private Storage connection. It also uses an Internet connection to send AutoSupport messages to NetApp technical support. If you deploy Cloud Manager in your data center, set up a VPN connection to the VPC. If you deploy Cloud Manager in AWS, enable Internet access from your VPC by using an Internet gateway, NAT instance, or proxy server. Note: If you have a proxy, you must configure Cloud Manager to use it. See <i>Configuring Cloud Manager to use a proxy server</i> on page 37. <i>AWS Documentation: Adding an Internet Gateway to Your VPC</i> <i>AWS Documentation: NAT Instances</i>
A route to the subnets where you will deploy Cloud ONTAP	Cloud Manager needs 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, either reroute the subnets or ensure that users do not use non-routable subnets for Cloud ONTAP instances. <i>AWS Documentation: Route Tables</i>
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 need to use your own, then it must include the required inbound and outbound rules. <i>AWS Documentation: Security Groups for Your VPC</i>

Requirement	Description
Access to the Cloud Manager web console	Users need to 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 need 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
HTTP	80	Access to the Cloud Manager console
HTTPS	443	Access to the Cloud Manager console
RDP	3389	RDP connections to the Cloud Manager instance

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 need to set up your AWS networking so that Cloud ONTAP can operate properly.

Requirement	Description
Internet access to send AutoSupport messages	Cloud ONTAP needs outbound Internet access to 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. You can use a NAT instance, VPN, or proxy server (in your data center or in AWS) to enable outbound traffic to AutoSupport. For a NAT instance, you must define an inbound security group rule that allows HTTPS traffic from the private subnet to the internet. <i>AWS Documentation: NAT Instances</i> Note: If you have a proxy, you must configure Cloud Manager to use it. See <i>Configuring Cloud Manager to use a proxy server</i> on page 37.
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, then it must include the required inbound and outbound rules. <i>AWS Documentation: Security Groups for Your VPC</i>
DNS and Active Directory for CIFS	If you want to provision CIFS storage, you need to 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. <i>AWS: Active Directory Domain Services on the AWS Cloud Quick Start Reference Deployment</i>

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

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

Sample VPC configurations for 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:

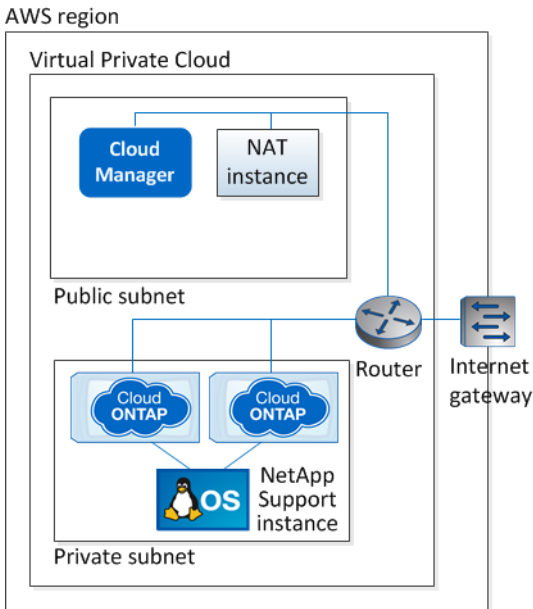
- A VPC with public and private subnets and a NAT instance
- A VPC with a private subnet and hardware VPN access

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 that runs in the public subnet. The NAT instance enables instances in the private subnet to initiate outbound Internet traffic. In this configuration, you can run Cloud Manager in a public subnet or private subnet. You would then launch Cloud ONTAP instances in the private subnet.

[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:



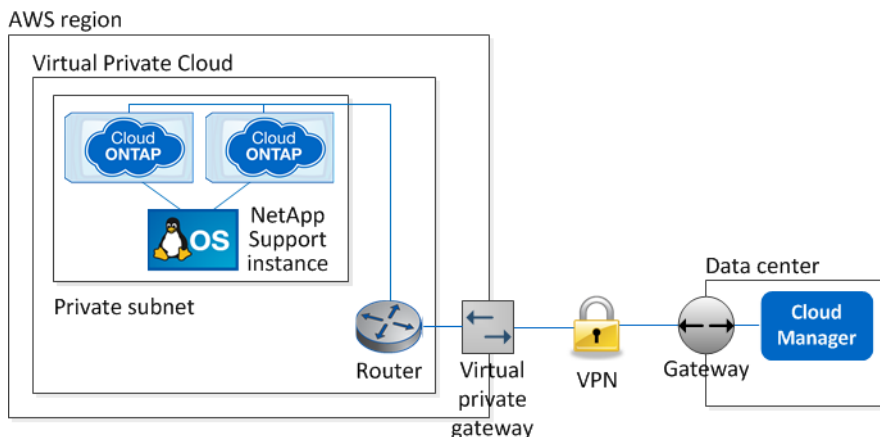
A VPC with a private subnet and hardware VPN access

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 corporate 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.

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:



AWS networking requirements for the NetApp Support instance

You need to set up your AWS networking so the NetApp Support instance can operate properly.

Requirement	Description
Internet access	The NetApp Support instance needs Internet access to communicate with AWS services to run a script for instance changes and scripts to troubleshoot and repair Cloud ONTAP instances. In addition, the instance also needs Internet access to download package updates from an S3 bucket in AWS. Similar to Cloud ONTAP, you can use a NAT instance, VPN, or proxy server (in your data center or in AWS) to enable outbound traffic. AWS Documentation: NAT Instances
A security group with the required rules	Cloud Manager automatically creates a security group for the NetApp Support instance. If you need to use your own security group, then it must include the required inbound and outbound rules. AWS Documentation: Security Groups for Your VPC

Security group rules for the NetApp Support instance

Inbound rules

Note: FTP connections are accepted from only the VPC in which the NetApp Support instance is running. SSH connections are accepted from any source (0.0.0.0/0.)

Type	Port Range	Used for
Custom TCP Rule	20-21	FTP
Custom TCP Rule	12000-12100	Passive FTP
SSH	22	SSH

Outbound rules

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

AWS networking requirements for NetApp Private Storage

Before you can use Cloud Manager to set up connections for your NetApp Private Storage configuration, the NetApp storage system and switch should be installed and configured in the colocation facility. You then need to set up your AWS networking, which includes a VPC with a subnet and a Direct Connect network connection. The deployment steps are captured in NetApp Technical Report 4133.

Related information

[*NetApp Technical Report 4133: NetApp Private Storage for Amazon Web Services \(AWS\) Solution Architecture and Deployment Guide*](#)

Granting permissions to IAM users

When you create Cloud Manager users, you need to 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 IAM user policies that include the required permissions.

About this task

To quickly provide your IAM users with the appropriate permissions for Cloud Manager, you can grant them “Power User” permissions. However, if you need to grant just the permissions that are required, use the NetApp-provided IAM policies that include the required permissions. You can use a policy that defines permissions for Cloud ONTAP, NetApp Private Storage, or both.

If you provide any less than the permissions defined in these policies, you will 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 will 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 one of the IAM user policies from the following location:

[*NetApp: AWS IAM User Policies for Cloud Manager*](#)

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, IAM, and Direct Connect (NetApp Private Storage only). You might want to understand what Cloud Manager does with these permissions.

Permissions	Purpose
"directconnect:*VirtualInterface", "directconnect:Describe*",	Creates a virtual interface and sets up a NetApp Private Storage connection.
"ec2:StartInstances", "ec2:StopInstances", "ec2:DescribeInstances", "ec2:DescribeInstanceStatus", "ec2:RunInstances", "ec2:TerminateInstances", "ec2:ModifyInstanceAttribute",	Launches a Cloud ONTAP instance and stops, starts, and monitors the instance.
"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.

Permissions	Purpose
"ec2:CreateSecurityGroup", "ec2:DeleteSecurityGroup", "ec2:DescribeSecurityGroups", "ec2:RevokeSecurityGroupEgress", "ec2:AuthorizeSecurityGroupEgress", "ec2:AuthorizeSecurityGroupIngress",	Creates predefined security groups for Cloud ONTAP, the NetApp Support instance, and NetApp Private Storage.
"ec2:CreateNetworkInterface", "ec2:DescribeNetworkInterfaces", "ec2:DeleteNetworkInterface", "ec2:ModifyNetworkInterfaceAttribute",	Creates a virtual private gateway (VGW) for NetApp Private Storage and attaches it to the VPC, if a VGW is not already present. The VGW is required to connect a subnet to a Direct Connect connection using a virtual interface.
"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 or NetApp Private Storage.
"ec2:DescribeVpnGateways", "ec2:CreateVpnGateway", "ec2:AttachVpnGateway", "ec2:DetachVpnGateway", "ec2:EnableVgwRoutePropagation", "ec2:DescribeRouteTables",	Connects a subnet to a Direct Connect connection using a virtual interface for NetApp Private Storage.
"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",	Launches a NetApp Support instance.

Permissions	Purpose
<pre>"cloudformation:CreateStack", "cloudformation:DeleteStack", "cloudformation:DescribeStacks", "cloudformation:DescribeStackEvents", "cloudformation:DescribeStackResources", "cloudformation:GetTemplate", "cloudformation:ValidateTemplate",</pre>	Launches a Cloud ONTAP instance or a NetApp Support instance.
<pre>"iam:GetUser",</pre>	Issues a private virtual interface request to the account that owns the Direct Connect connection for NetApp Private Storage.
<pre>"s3:GetObject", "s3:ListBucket"</pre>	Gets AWS cost data for Cloud ONTAP.

How AWS limits can impact Cloud ONTAP

AWS 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 general purpose SSD 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

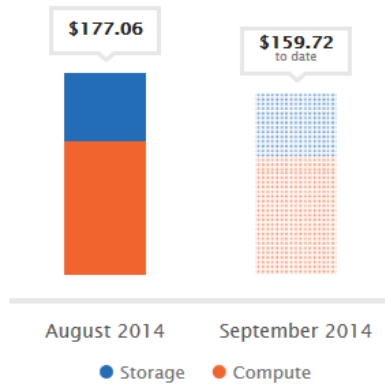
Users of AWS payer accounts must set up AWS to store billing reports in an S3 bucket. Cloud Manager uses the information from the reports to show monthly compute and storage costs associated with a Cloud ONTAP instance, as well as storage cost savings from NetApp's efficiency features (if they are enabled).

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:

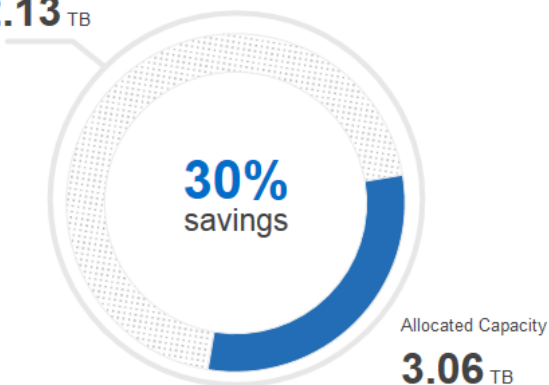
30% storage cost savings

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](#)

AWS Capacity

2.13 TB



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. Create a Cloud Manager 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 17.
 - b. Specify the S3 bucket that you created.

[Creating user accounts](#) on page 38

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 need to verify support for your configuration, which includes host requirements, web browser requirements, supported NetApp Private Storage configurations, 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 at this time, 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 supported by Microsoft
Operating system	Windows Server 2012 R2 (Standard or Datacenter)
CPU	2.27 GHz or higher with 2 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	36
Microsoft Internet Explorer	11
Mozilla Firefox	31

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

Port requirements

Cloud Manager uses the following ports:

- 80 for HTTP access to Cloud Manager
- 443 for HTTPS access to Cloud Manager
- 3306 for the MySQL database that stores Cloud Manager data

Before you install Cloud Manager on an existing Windows host, you should verify that these ports are available. If other services are using these ports, Cloud Manager installation will fail.

You can change the default HTTP and HTTPS ports when you install Cloud Manager. You cannot change the default port for the Cloud Manager MySQL database. If you change the HTTP and HTTPS ports, you must ensure that users can access the Cloud Manager web console. For details about changing the default ports, see [Installing the Cloud Manager software](#) on page 31.

The following are known conflicts with the default Cloud Manager ports:

- If Internet Information Services (IIS) is installed on the Windows host, it uses port 80 by default. You need to change the default TCP port for IIS services, or you need to change the default HTTP port when you install Cloud Manager.
- If another instance of MySQL is running on the Windows host, it uses port 3306 by default. You need to change the port that the existing MySQL instance uses.

Cloud Manager installation will fail if these conflicts are not resolved.

Credentials that you need for Cloud Manager

You need to 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 use or create the following credentials:

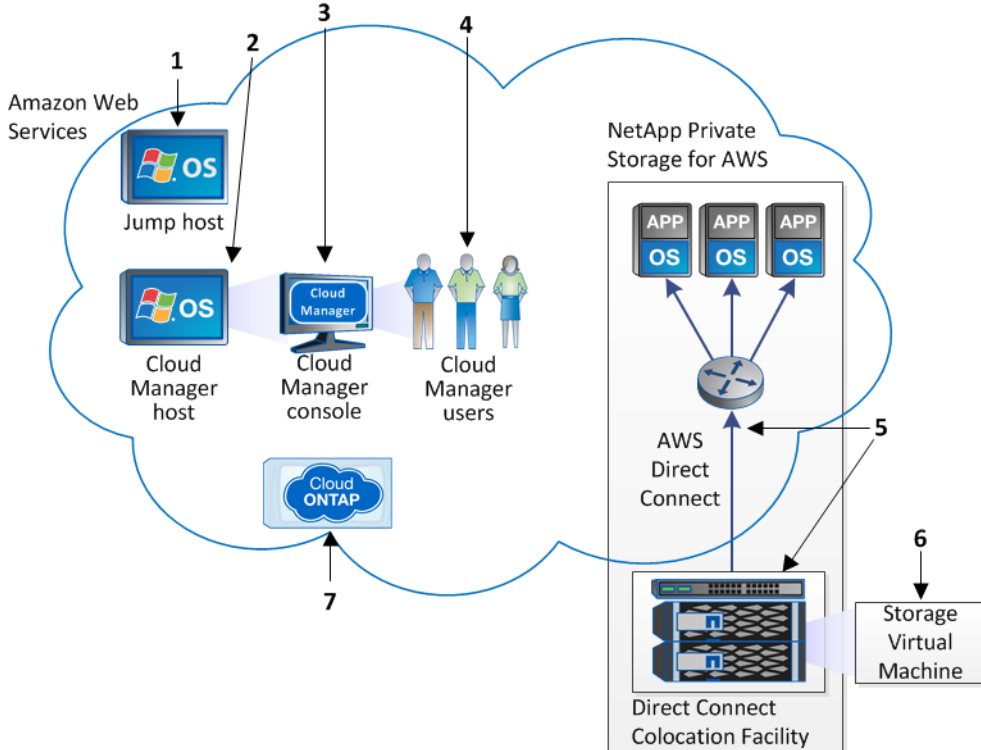
No.	Credentials	Purpose
1	Jump host credentials	If you do not assign a public IP address to the Cloud Manager instance, you need to connect to the instance from another instance in AWS (a jump host).
2	Cloud Manager host credentials	You need to connect to the host on which you want to install Cloud Manager. In AWS, this involves using a key pair to obtain the credentials.
3	Cloud Manager credentials	When you install Cloud Manager, you create the credentials that you, as the Cloud Manager Admin, will use to log in to Cloud Manager.
4	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.

No.	Credentials	Purpose
5	NetApp Private Storage connection credentials	When you add your NetApp Private Storage configuration to Cloud Manager, you need to enter credentials for the cluster, the network switch, and the access keys for the account associated with the Direct Connect connection.

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

No.	Credentials	Purpose
6	SVM credentials for a NetApp Private Storage configuration	When users create a Storage Virtual Machine (SVM) for NetApp Private Storage, they need to enter credentials for the SVM account.
7	Cloud ONTAP credentials	When users launch a Cloud ONTAP instance, they need to enter the password for the admin account, which they can use to connect to Cloud ONTAP through OnCommand System Manager or the CLI.

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.



Gathering information for installation and setup

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 add a NetApp Private Storage configuration

Cluster information	Your value
Cluster Management IP address	
admin user name	
admin password	
Ports connected to the network switch	

Network switch information	Your value
Network switch IP address	
User name	
Password	
Initial CIDR	
VLAN range	

Direct Connect information	Your value
Region	
Access and secret keys	
Connection	

Information needed to define tenants

Information	Your values
Tenant names	

Subscribing to Cloud ONTAP in AWS

Before you can launch Cloud ONTAP instances, you need to 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: Explore \(Hourly\)](#)
 - [AWS Marketplace: Cloud ONTAP for AWS: Standard \(Hourly\)](#)
 - [AWS Marketplace: Cloud ONTAP for AWS: Standard \(BYOL\)](#)
2. Review the terms, and then click **Accept**.

After you finish

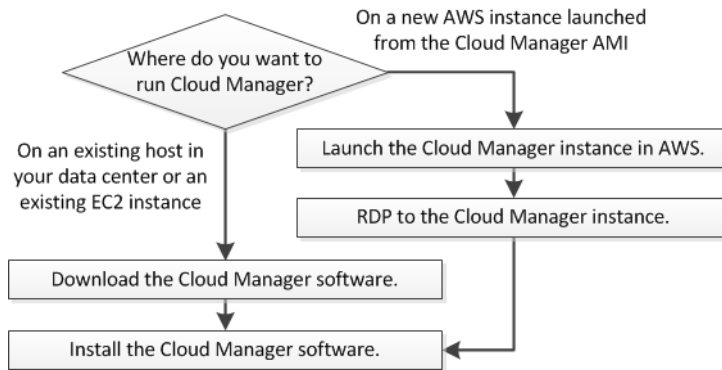
Attention: You must use Cloud Manager to launch Cloud ONTAP instances. You must not launch Cloud ONTAP instances from the EC2 console.

Related information

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

Installing OnCommand Cloud Manager

You can install Cloud Manager on an EC2 instance that you launch from the Cloud Manager AMI, or you can download the Cloud Manager software from the NetApp Support Site and install it on a host in your data center or on an existing EC2 instance in AWS.



Launching a Cloud Manager instance in AWS

If you want to run Cloud Manager in AWS, you need to subscribe to Cloud Manager and launch an EC2 instance from the Cloud Manager Amazon Machine Image (AMI), which is available on the AWS Marketplace.

Before you begin

- You should have an EC2 key pair. You need a key pair to decrypt the login information for the Cloud Manager instance.
- If you want to assign a public IP address to the Cloud Manager instance, the public subnet must be enabled to automatically assign public IP addresses if you want to use the **1-Click Launch** option.

[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 it gets your Cloud Manager instance up and running faster. If you do choose a manual launch, you need to 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 security group that includes the inbound and outbound rules required by Cloud Manager. If you want to use your own security group, it must meet the Cloud Manager port requirements.
4. To subscribe to Cloud Manager and launch the instance, click **Accept Terms and Launch with 1-Click**.

Result

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

Related references

[AWS networking requirements for Cloud Manager](#) on page 11

Related information

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

Connecting to the Cloud Manager instance in AWS

After you launch the Cloud Manager instance, connect to it using RDP to install the Cloud Manager software on the instance.

Steps

1. From the Amazon EC2 console, select the Cloud Manager instance, and then click **Connect**.
2. Follow the prompts to get the password and the remote desktop file.
3. Use the remote desktop file to log in to the instance.

Related information

[AWS Documentation: Connecting to Your Windows Instance Using RDP](#)

Installing the Cloud Manager software

You install Cloud Manager on a Windows host by using an installation wizard.

Steps

1. If you are installing Cloud Manager on an existing host, download the software from the NetApp Support Site.

[NetApp Downloads: Software](#)

If you launched the Cloud Manager instance in AWS, the product installer is on the desktop.

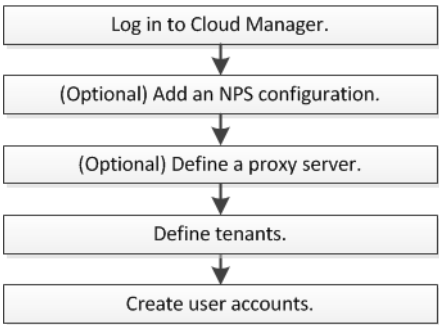
2. Double-click the .exe file.
3. Complete the steps in the installation wizard to install Cloud Manager.

Most of the pages in the wizard are self-explanatory. The following table describes pages for which you might need guidance:

In this page...	Do this...
Server Configuration	Change or keep the default HTTP and HTTPS ports. If you change the ports, ensure that users can log in to the Cloud Manager web console from a remote host: • In AWS, modify the instance's security group to allow inbound connections through the ports. • Configure Windows Firewall to allow inbound connections through the ports. • Specify the port when you enter the URL to the Cloud Manager web console. Logging in to Cloud Manager on page 32
Customer Information	Specify your site and company name, which AutoSupport uses to identify who you are.
Administrator User	Specify details to create the administrator user for Cloud Manager. You use this user account to log in to Cloud Manager after the installation completes. Note: Your user name is your email address. Cloud Manager does not send emails to this address.

Setting up OnCommand Cloud Manager

After you install Cloud Manager, you need to set it up so that users can log in and provision NetApp storage for the cloud.



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 one of the following URLs:

If you are on...	Enter...
The Cloud Manager host	https://localhost:port
A host that has a connection to the Cloud Manager host	https://ipaddress:port

ipaddress can be either 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 need to enter a private IP address from a host in AWS that has a connection to the Cloud Manager host.

port is necessary only if the default HTTP (80) or HTTPS (443) ports were changed. For example, if the HTTPS port was changed to 8443, you need to enter **https://localhost:8443**

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



Welcome to OnCommand Cloud Manager

Email

Password

Log in

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

The Working Environments page appears.



Working Environments

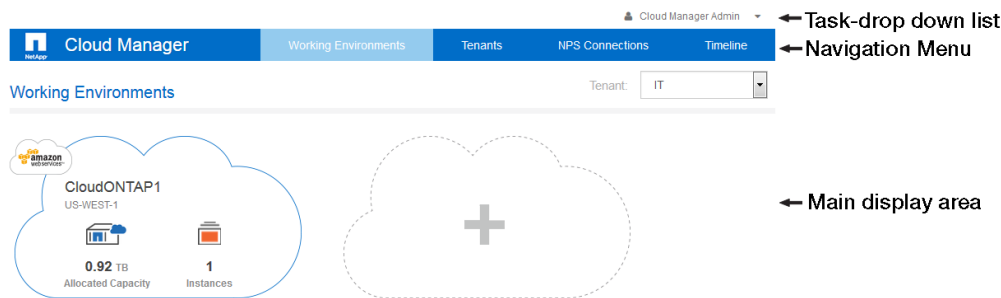


Overview of the Cloud Manager console

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

Major components of the console

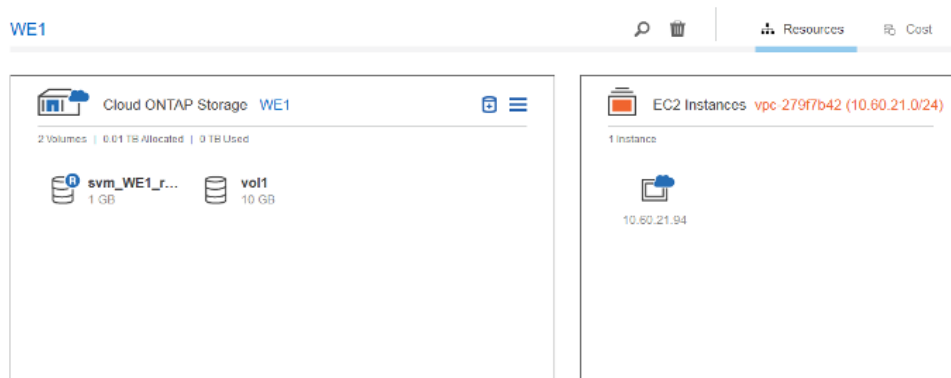
The console consists of a task drop-down list, a navigation menu, and a main display area:



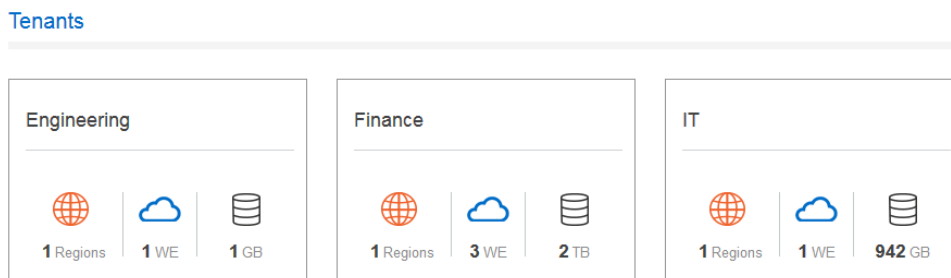
Working environments and tenants

The console organizes storage by working environments and tenants.

A *working environment* includes a Cloud ONTAP instance or a NetApp Private Storage configuration and the AWS EC2 compute instances in the VPC. The following image shows a Cloud ONTAP working environment:



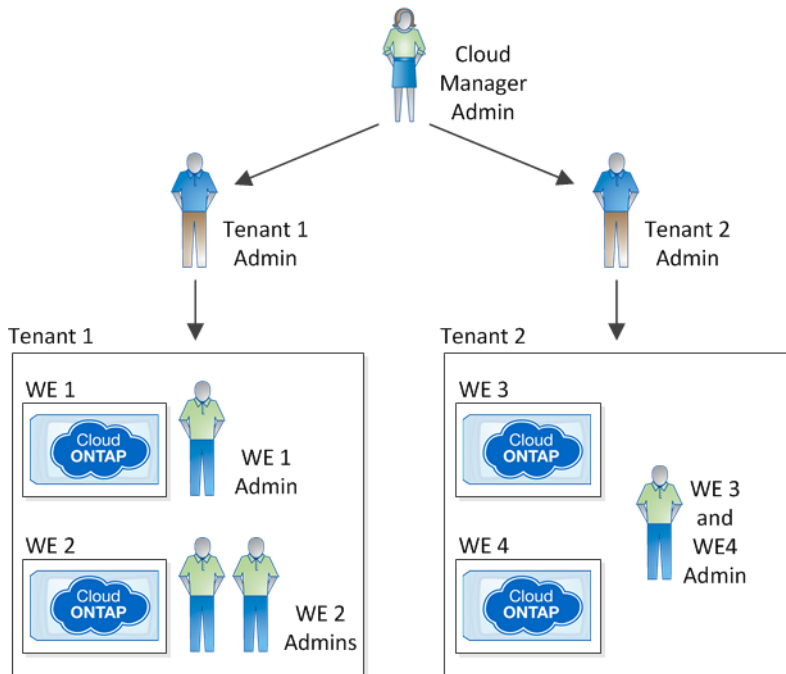
A *tenant* represents a group in your organization. You create one or more working environments within a tenant. The following image shows three tenants defined in Cloud Manager:



How Cloud Manager users relate to tenants and working environments

The tasks that you can perform in the console depend on your user role. The three distinct user roles are: Cloud Manager Admin (who administers the product), Tenant Admin (who administers a specific tenant), and Working Environment Admin (who administers one or more working environments).

The following image shows the relationship between Cloud Manager user roles, tenants, and working environments:



Adding your NetApp Private Storage configuration to Cloud Manager

If you want to use Cloud Manager to manage a NetApp Private Storage for AWS configuration, you need to provide Cloud Manager with details about the storage system, the network switch, and the AWS Direct Connect configuration.

Steps

1. In Cloud Manager, click **NPS Connections**.
2. In the **NPS Connections** page, click the + icon.

3. In the **New NPS Connection** page, enter a name and description for the connection, and then specify details about the cluster, network switch, and AWS Direct Connect.

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

Field	Description
Ports	Choose the ports that are connected to the network switch and designated for data traffic.
Initial CIDR	Specify the CIDR network that matches your IP address plan. Cloud Manager automatically displays the next available CIDR.
VLAN range	Specify the VLAN range that matches your IP address plan. Cloud Manager automatically displays the next available VLAN.
AWS Access Key and AWS Secret Key	Enter the keys for the AWS account associated with the Direct Connect configuration.

The following image shows the New NPS Connection page filled out:

The screenshot shows the 'New NPS Connection' page with three main sections: Cluster, Network Switch, and Direct Connect. Each section has several input fields.

- Cluster:**
 - Management IP: 192.168.1.20
 - User Name: admin
 - Password: (masked with dots)
 - Ports: A dropdown menu showing 'x e0g (sv5-cluster1-01)' and 'x e0h (sv5-cluster1-01)'.
- Network Switch:**
 - IP: 192.168.1.1
 - User Name: admin
 - Password: (masked with dots)
 - Initial CIDR: 192.168.2.0/29
 - VLAN range: 100-200
- Direct Connect:**
 - Region: us-west-1 (dropdown menu)
 - AWS Access Key: AAAA77777B88888888
 - AWS Secret Key: (masked with dots)
 - Connection: SV1 10GbE (dropdown menu)

4. Click **Verify**.

Cloud Manager attempts to connect to the NetApp Private Storage configuration. If the information is valid, a blue check mark appears next to the cluster, network switch, and Direct Connect information. If the information is not valid, an error appears on the page. If this happens, review the error and verify the information that you entered.

5. Click **Save**.

Result

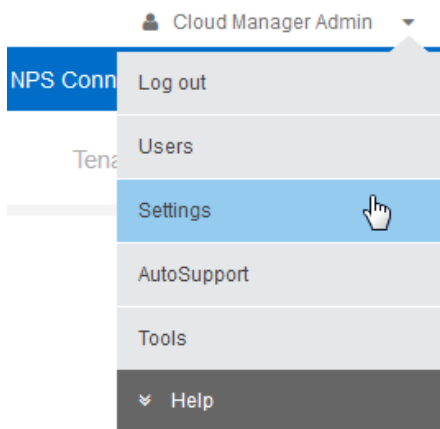
Cloud Manager saves the configuration. After you define your tenants, users can create a Data ONTAP working environment for NetApp Private Storage using the configuration that you added.

Configuring Cloud Manager to use a proxy server

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 data center.

Steps

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



2. Under **HTTP Proxy**, enter the server using the syntax **http://address:port**, and then click **Save**.

Example

HTTP Proxy

Set up Proxy configuration to allow Cloud Manager and Cloud ONTAP instances to access the Internet.

Enter an empty value to disable the proxy.

Save

Result

After you set the proxy option in Cloud Manager, new Cloud ONTAP instances are automatically configured to use the proxy server for AutoSupport messages. If you set the proxy option after launching Cloud ONTAP instances, you need to manually set the proxy in the AutoSupport options for each instance.

Defining tenants

You can use the default tenant (“Tenant 1”) or you can define your own tenants. A tenant represents a business group that contains Cloud ONTAP and NetApp Private Storage working environments. 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, enter a name, description, and cost center for the tenant.
The Description and Cost Center fields are optional.
4. Click **Save**.

Result

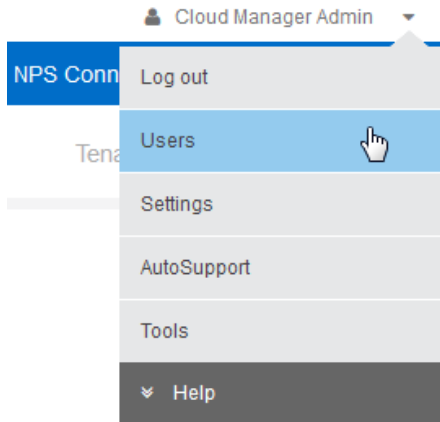
Cloud Manager creates the tenant. Users can create Cloud ONTAP and NetApp Private Storage working environments in the new tenant.

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 Can perform all tasks in Cloud Manager. Tenant Admin Can create and manage all working environments in a tenant and can manage users in that tenant. Working Environment Admin Can create and manage one or more working environments in a single 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 make requests to AWS. If the user is an IAM user, the account must have specific AWS permissions. You can use NetApp-provided IAM policies that include the required permissions. NetApp Cloud ONTAP: AWS IAM User Policies for Cloud Manager Note: Cloud Manager validates the keys when the user creates and manages working environments.
AWS Cost S3 Bucket	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 billings reports enables it to display AWS storage and compute costs associated with Cloud ONTAP instances. If you are using AWS consolidated billing, you do not need to specify the bucket each time you create a Cloud Manager user account. You just need to 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

[Granting permissions to IAM users](#) on page 17

[Setting up AWS billing and cost management for Cloud Manager](#) on page 20

What to do next

After you set up Cloud Manager, users can launch Cloud ONTAP instances, move data in and out of Cloud ONTAP, and set up connections for a NetApp Private Storage configuration. When necessary, you can also administer Cloud Manager and view online resources to get help.

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

If you want to...	Open these resources...
Create and manage working environments: • Launch Cloud ONTAP instances • Provision storage for Cloud ONTAP • Replicate data to and from Cloud ONTAP • Provision and connect a Storage Virtual Machine (SVM) to an AWS Direct Connect for NetApp Private Storage	<i>OnCommand Cloud Manager 1.0 User Guide</i>
Administer Cloud Manager by backing it up, managing user accounts, configuring settings, troubleshooting, and using APIs.	<i>OnCommand Cloud Manager 1.0 Administration Guide</i>
Review release-specific information (known issues, limitations, and so on) for Cloud Manager and Cloud ONTAP	<i>OnCommand Cloud Manager 1.0 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 © 1994–2014 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, 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, SANtricity, SecureShare, Simplicity, Simulate ONTAP, Snap Creator, SnapCopy, SnapDrive, SnapIntegrator, SnapLock, SnapManager, SnapMirror, SnapMover, SnapProtect, SnapRestore, Snapshot, SnapValidator, SnapVault, StorageGRID, Tech OnTap, Unbound Cloud, and WAFL are trademarks or registered trademarks of NetApp, Inc., in the United States, and/or other countries. A current list of NetApp trademarks is available on the web at <http://www.netapp.com/us/legal/netapptmlist.aspx>.

Cisco and the Cisco logo are trademarks of Cisco in the U.S. and other countries. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such.

How to send your comments

You can help us to improve the quality of our documentation by sending us your feedback.

Your feedback is important in helping us to provide the most accurate and high-quality information. 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.

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 [38](#)
- credentials for [24](#)

Amazon Web Services

- billing and cost requirements [20](#)
- connecting to Cloud Manager instance [30](#)
- default limits [20](#)
- granting permissions to IAM users [17](#)
- launching Cloud Manager in [29](#)
- networking requirements for Cloud Manager [11](#)
- networking requirements for Cloud ONTAP [13](#)
- networking requirements for NetApp Private Storage [17](#)
- networking requirements for NetApp Support instance [16](#)
- preparing [10](#)
- sample VPC configurations [14](#)
- subscribing to Cloud ONTAP software from [28](#)
- what Cloud Manager does with permissions [18](#)

B

billing and cost requirements

- verifying IAM user access to billing information [20](#)

C

Chrome

- supported versions [23](#)

Cloud Manager

- See* OnCommand Cloud Manager

Cloud ONTAP

- AWS networking requirements for [13](#)
- product models [6](#)
- subscribing to the software in AWS [28](#)
- what it is [6](#)
- what the NetApp Support instance is [7](#)

comments

- how to send feedback about documentation [44](#)

components

- credentials for [24](#)

console

- logging in to Cloud Manager [32](#)
- understanding [33](#)

cost

- requirements to display in Cloud Manager [20](#)

CPU

- required for Cloud Manager [23](#)

D

Direct Connect

- adding to Cloud Manager [35](#)

disk space

- required for Cloud Manager [23](#)

documentation

- how to send feedback about [44](#)
- where to find additional documentation [41](#)

F

feedback

- how to send comments about documentation [44](#)

Firefox

- supported versions [23](#)

I

IAM users

- granting permissions to [17](#)
- what Cloud Manager does with permissions [18](#)

information

- how to send feedback about improving documentation [44](#)

installation

- gathering information for [26](#)
- preparing for OnCommand Cloud Manager [10](#)

installing OnCommand Cloud Manager

- using an installation wizard [31](#)
- workflow [9](#)

instance limits

- for AWS [20](#)

Internet Explorer

- supported versions [23](#)

L

logging in

- to Cloud Manager [32](#)

N

NetApp Private Storage

- adding configuration to Cloud Manager [35](#)
- AWS requirements for [17](#)
- information needed to add configuration [26](#)
- overview [8](#)

NetApp Support instance

- AWS networking requirements for [16](#)
- what it is [7](#)

O

OnCommand Cloud Manager

- adding NetApp Private Storage configuration to [35](#)
 - AWS networking requirements for [11](#)
 - billing and cost requirements [20](#)
 - configuring to use a proxy server [37](#)
 - connecting to Cloud Manager instance [30](#)
 - creating admin user of [38](#)
 - creating user accounts [38](#)
 - EC2 instance requirements [23](#)
 - host requirements [23](#)
 - information needed to launch in AWS [26](#)
 - installation and setup workflow [9](#)
 - installing [31](#)
 - launching in AWS [29](#)
 - logging in [32](#)
 - overview of the console [33](#)
 - overview of where to install [29](#)
 - preparing for installation and setup [10](#)
 - setting up [32](#)
 - supported web browsers [23](#)
 - what it is [5](#)
- operating system
 - required for Cloud Manager [23](#)

P

ports

- requirements for Cloud Manager [11](#)
- requirements for Cloud ONTAP [13](#)
- requirements for NetApp Support instance [16](#)

proxy servers

- configuring Cloud Manager to use [37](#)

R

RAM

- required for Cloud Manager [23](#)

S

security groups

- requirements for Cloud Manager [11](#)
- requirements for Cloud ONTAP [13](#)
- requirements for NetApp Support instance [16](#)

setup

- credentials used for OnCommand Cloud Manager [24](#)
- gathering information for [26](#)
- preparing for OnCommand Cloud Manager [10](#)
- workflow [9](#)

storage limits

- for AWS [20](#)

subnets

- requirements for Cloud Manager [11](#)
- requirements for Cloud ONTAP [13](#)
- requirements for NetApp Support instance [16](#)

suggestions

- how to send feedback about documentation [44](#)

T

tenants

- creating admin user of [38](#)
- defining in Cloud Manager [38](#)
- definition of [33](#)

U

user accounts

- creating [38](#)

V

Virtual Private Clouds

- requirements for Cloud Manager [11](#)
- requirements for Cloud ONTAP [13](#)
- requirements for NetApp Private Storage [17](#)
- requirements for NetApp Support instance [16](#)
- sample configurations [14](#)

W

web browsers

- supported versions [23](#)

working environments

- creating admin user of [38](#)
- defining tenants for Cloud Manager [38](#)