<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deciding whether to use this guide</td>
<td>5</td>
</tr>
<tr>
<td>Product overview</td>
<td>6</td>
</tr>
<tr>
<td>ONTAP Cloud for AWS overview</td>
<td>7</td>
</tr>
<tr>
<td>How an ONTAP Cloud HA configuration provides non-disruptive operations</td>
<td>8</td>
</tr>
<tr>
<td>How storage works in an ONTAP Cloud HA pair</td>
<td>9</td>
</tr>
<tr>
<td>Cloud Manager REST APIs</td>
<td>11</td>
</tr>
<tr>
<td>Installation and setup workflow</td>
<td>12</td>
</tr>
<tr>
<td>Preparing for installation and setup</td>
<td>13</td>
</tr>
<tr>
<td>Preparing your AWS environment</td>
<td>13</td>
</tr>
<tr>
<td>AWS networking requirements for Cloud Manager</td>
<td>14</td>
</tr>
<tr>
<td>AWS networking requirements for ONTAP Cloud</td>
<td>16</td>
</tr>
<tr>
<td>AWS networking requirements for ONTAP Cloud HA configurations</td>
<td>18</td>
</tr>
<tr>
<td>Sample VPC configurations for Cloud Manager and ONTAP Cloud</td>
<td>20</td>
</tr>
<tr>
<td>Granting AWS permissions to Cloud Manager</td>
<td>22</td>
</tr>
<tr>
<td>How AWS limits can impact ONTAP Cloud</td>
<td>25</td>
</tr>
<tr>
<td>Setting up AWS billing and cost management for Cloud Manager</td>
<td>25</td>
</tr>
<tr>
<td>Cloud Manager software requirements</td>
<td>27</td>
</tr>
<tr>
<td>Ways to encrypt ONTAP Cloud data</td>
<td>28</td>
</tr>
<tr>
<td>Key manager requirements for ONTAP Cloud encryption</td>
<td>29</td>
</tr>
<tr>
<td>Planning how to organize users and storage across tenants</td>
<td>31</td>
</tr>
<tr>
<td>Credentials that you need for Cloud Manager</td>
<td>32</td>
</tr>
<tr>
<td>Why you should link a tenant to your NetApp Support Site account</td>
<td>34</td>
</tr>
<tr>
<td>Installation and setup worksheet</td>
<td>34</td>
</tr>
<tr>
<td>Subscribing to ONTAP Cloud in AWS</td>
<td>36</td>
</tr>
<tr>
<td>Installing OnCommand Cloud Manager</td>
<td>37</td>
</tr>
<tr>
<td>Launching a Cloud Manager instance in a standard AWS region</td>
<td>37</td>
</tr>
<tr>
<td>Launching a Cloud Manager instance in the AWS GovCloud (US) region</td>
<td>38</td>
</tr>
<tr>
<td>Installing Cloud Manager on an existing Linux host</td>
<td>40</td>
</tr>
<tr>
<td>Setting up OnCommand Cloud Manager</td>
<td>42</td>
</tr>
<tr>
<td>Installing an HTTPS certificate for secure access</td>
<td>44</td>
</tr>
<tr>
<td>Creating tenants</td>
<td>44</td>
</tr>
<tr>
<td>Creating user accounts</td>
<td>45</td>
</tr>
<tr>
<td>Setting up Cloud Manager for ONTAP Cloud encryption</td>
<td>46</td>
</tr>
<tr>
<td>Understanding how ONTAP Cloud encryption works</td>
<td>47</td>
</tr>
<tr>
<td>Setting up Cloud Manager to be an intermediate CA</td>
<td>48</td>
</tr>
<tr>
<td>Adding key managers and CA certificates to Cloud Manager</td>
<td>48</td>
</tr>
<tr>
<td>What to do after installation and setup</td>
<td>50</td>
</tr>
<tr>
<td>Updating Cloud Manager</td>
<td>51</td>
</tr>
<tr>
<td>Enabling automatic updates</td>
<td>51</td>
</tr>
<tr>
<td>Updating Cloud Manager from 2.1 and later to 3.0</td>
<td>51</td>
</tr>
<tr>
<td>Updating Cloud Manager from 2.0 or earlier to 3.0</td>
<td>52</td>
</tr>
</tbody>
</table>
Deciding whether to use this guide

The *OnCommand Cloud Manager Installation and Setup Guide for Storage System Management* describes how to install and set up Cloud Manager in the Storage System View, which gives you full control of ONTAP Cloud systems and the data in your hybrid cloud storage environment.

The following image shows the Storage System View:

If you simply want to create volumes and would like Cloud Manager to handle storage management decisions for you, you should install and use Cloud Manager in the Volume View:

For instructions, see the *OnCommand Cloud Manager 3.0 Installation and User Guide for Volume Management.*
Product overview

OnCommand Cloud Manager provides simplified management of cloud storage environments built on NetApp. You can use Cloud Manager to manage data across your hybrid cloud, which includes full control of ONTAP Cloud systems, or you can simply provision volumes and let Cloud Manager handle the rest.

When you set up Cloud Manager, you can choose between two management views: the Storage System View and the Volume View.

Storage System View

You can use Cloud Manager in this view to have full control of ONTAP Cloud systems:

- Configure and launch ONTAP Cloud instances in Amazon Web Services (AWS)
- Provision NFS and CIFS storage
- Replicate data across a hybrid cloud environment: between on-premises ONTAP clusters, ONTAP Cloud systems, and NetApp Private Storage for Cloud configurations
- Manage ONTAP Cloud systems as needed, which includes capacity allocation decisions, simplified upgrades, cost monitoring, and several other tasks

Volume View

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

Where to deploy Cloud Manager

Cloud Manager can run in AWS or in your network. Cloud Manager must run in the AWS GovCloud (US) region if you want to launch ONTAP Cloud instances in AWS GovCloud (US).

Note: The Volume View is not supported in the AWS GovCloud (US) region.

The following image shows Cloud Manager running in AWS and managing an ONTAP Cloud system and data replication to and from ONTAP clusters:
ONTAP Cloud for AWS overview

ONTAP Cloud for Amazon Web Services (AWS) is a software-only storage appliance that runs the ONTAP data management software in the cloud. Building your cloud environment on ONTAP Cloud 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 ONTAP Cloud provides

ONTAP Cloud manages Amazon Elastic Block Store (EBS) volumes with the NetApp ONTAP software, which provides enterprise-class features:

- High availability (HA)
- 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 ONTAP Cloud.

How you deploy ONTAP Cloud

You must use OnCommand Cloud Manager to launch ONTAP Cloud as an Elastic Cloud Compute (EC2) instance in AWS. Cloud Manager launches EC2 instances and purchases the EBS volumes that ONTAP Cloud uses as back-end storage.

ONTAP Cloud configurations

ONTAP Cloud is available in two pricing options: pay-as-you-go and Bring Your Own License (BYOL). For pay-as-you-go, you can choose from three configurations: Explore, Standard, and Premium. For both pricing options, you can launch a single system or an HA pair.

<table>
<thead>
<tr>
<th></th>
<th>Explore ¹</th>
<th>Standard ¹</th>
<th>Premium ¹</th>
<th>BYOL</th>
</tr>
</thead>
<tbody>
<tr>
<td>EC2 instance types</td>
<td>m3.xlarge ²</td>
<td>m3.2xlarge ²</td>
<td>r3.2xlarge</td>
<td>m3.xlarge ²</td>
</tr>
<tr>
<td>for single node</td>
<td>m4.xlarge</td>
<td>m4.2xlarge</td>
<td></td>
<td>m3.2xlarge ²</td>
</tr>
<tr>
<td>systems</td>
<td></td>
<td>r3.xlarge</td>
<td></td>
<td>m4.xlarge</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>m4.2xlarge</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>r3.xlarge</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>r3.2xlarge</td>
</tr>
<tr>
<td>EC2 instance types</td>
<td>r3.xlarge</td>
<td>m4.2xlarge</td>
<td>r3.2xlarge</td>
<td>m4.2xlarge</td>
</tr>
<tr>
<td>for HA pairs</td>
<td></td>
<td></td>
<td></td>
<td>r3.xlarge</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>r3.2xlarge</td>
</tr>
<tr>
<td>EBS raw capacity</td>
<td>2 TB</td>
<td>10 TB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>limit per node</td>
<td></td>
<td></td>
<td></td>
<td>Single node systems:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• 368 TB for SSD</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• 46 TB for Magnetic</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Per node in an HA pair:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• 360 TB for SSD</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• 45 TB for Magnetic</td>
</tr>
<tr>
<td>Term</td>
<td>Hourly or annual</td>
<td></td>
<td></td>
<td>6 or 12 months</td>
</tr>
</tbody>
</table>

¹ The EC2 instance types are available in both pay-as-you-go and BYOL pricing options.
² The EBS raw capacity limit per node is the maximum amount of storage capacity that can be attached to an EC2 instance.

Product overview | 7
1. ONTAP Cloud pay-as-you-go configurations are not supported in the AWS GovCloud (US) region.
2. ONTAP Cloud encryption is not supported with M3 instances.

How an ONTAP Cloud HA configuration provides non-disruptive operations

An ONTAP Cloud HA configuration ensures high availability of your data in case of software, storage, and networking failures.

HA components

An ONTAP Cloud HA configuration includes the following components:

- Two ONTAP Cloud systems (nodes) whose data is synchronously mirrored between each other.
- A mediator instance that provides a communication channel between the nodes to assist in storage takeover and giveback processes.
  
  Note: The mediator instance runs the Linux operating system on a t2.micro instance and uses one EBS magnetic disk that is approximately 8 GB.
- Three floating IP addresses that can move between nodes, which enables storage failover for NFS and CIFS.
  
  Note: One floating IP address is for cluster management, one is for NFS/CIFS data on node 1, and one is for NFS/CIFS data on node 2. iSCSI data LIFs are created by default and use static IP addresses, rather than floating IP addresses.

The following image shows the relationship between these components:

![Diagram showing the relationship between ONTAP Cloud HA components](image)

Each of these components must be deployed properly in AWS.

AWS networking requirements for ONTAP Cloud HA configurations on page 18

Storage takeover and giveback

If a node goes down, the other node can serve data for its partner to provide continued data service. Clients can access the same data from the partner node because the data was synchronously mirrored to the partner.
When takeover occurs in a NAS configuration, the node’s floating IP address that clients use to access data moves to the other node. For iSCSI, ONTAP Cloud uses multipath I/O (MPIO) and Asymmetric Logical Unit Access (ALUA) to manage path failover between the active-optimized and non-optimized paths.

**Note:** For information about which specific host configurations support ALUA, see the *NetApp Interoperability Matrix Tool* and the Host Utilities *Installation and Setup Guide* for your host operating system.

The following image depicts storage takeover in a NAS configuration. If node 2 goes down, the floating IP address for node 2 moves to node 1.

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

**RPO and RTO**

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

- The recovery point objective (RPO) is 0 seconds.
  
  Your data is transactionally consistent with no data loss.

- The recovery time objective (RTO) is 60 seconds.
  
  In the event of an outage, data should be available in 60 seconds or less.

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

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

**Storage allocation**

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

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

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

Performance expectations for an ONTAP Cloud HA configuration

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

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


Client access to storage in an HA pair

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

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

You can easily identify the correct IP address from Cloud Manager:
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:

You can also find an overview, examples, and an API reference in the *OnCommand Cloud Manager 3.0 API Developer Guide.*
Installation and setup workflow

Deploying Cloud Manager involves preparing your environment, installing Cloud Manager, and then setting it up.

1. **Prepare for installation and setup**
   - Prepare your AWS environment.
   - Review Cloud Manager requirements.
   - Prepare key managers, if necessary.
   - Plan how to set up tenants.
   - Review the credentials that you will use.
   - Gather information for installation and setup.

2. **Install Cloud Manager**
   - The GovCloud region
     - Launch ONTAP Cloud in a standard region or in GovCloud?
       - Purchase an ONTAP Cloud license.
       - Launch the Cloud Manager instance in GovCloud.
   - A standard region
     - Subscribe to ONTAP Cloud in AWS.
     - New instance in AWS
       - Where do you want to run Cloud Manager?
         - Existing host in your network or in AWS
           - Download and install the Cloud Manager software.
         - Launch the Cloud Manager instance from the AMI.
   - Launch the Cloud Manager instance in GovCloud.

3. **Set up Cloud Manager**
   - Log in and set up Cloud Manager.
   - Install an HTTPS certificate, if necessary.
   - Create additional tenants, if necessary.
   - Create user accounts.
   - Set up ONTAP Cloud encryption, if necessary.
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 13
   Your AWS environment must meet a few requirements so that Cloud Manager and ONTAP Cloud operate correctly in AWS.

2. Review Cloud Manager requirements on page 27
   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 NetAppInteroperability 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 28
   You can choose whether to encrypt data on ONTAP Cloud systems when you create a new working environment. If data encryption is needed, you can choose between ONTAP Cloud encryption and Amazon EBS encryption.

4. Plan how to set up tenants on page 31
   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 32
   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 34
   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 so that Cloud Manager and ONTAP Cloud 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 14
   - *AWS networking requirements for ONTAP Cloud* on page 16
   - *AWS networking requirements for ONTAP Cloud HA configurations* on page 18

   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 device, or a VPC...
with a private subnet and VPN access. You can then use the pre-defined security groups that are available when you launch the Cloud Manager and ONTAP Cloud instances.

Sample VPC configurations for Cloud Manager and ONTAP Cloud on page 20

2. Grant the required permissions so Cloud Manager can perform operations in AWS.

Granting AWS permissions to Cloud Manager on page 22

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

How AWS limits can impact ONTAP Cloud on page 25

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

Setting up AWS billing and cost requirements on page 25

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 that Cloud Manager can launch ONTAP Cloud instances.

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet access</td>
<td>Cloud Manager requires Internet access to do the following:</td>
</tr>
<tr>
<td></td>
<td>• Access an S3 bucket that contains the ONTAP Cloud AMI manifest file and the</td>
</tr>
<tr>
<td></td>
<td>latest Cloud Manager installation packages</td>
</tr>
<tr>
<td></td>
<td>• Communicate with AWS services to launch and manage ONTAP Cloud instances</td>
</tr>
<tr>
<td></td>
<td>• Send AutoSupport messages to NetApp technical support</td>
</tr>
<tr>
<td></td>
<td>• Register ONTAP Cloud systems with NetApp technical support</td>
</tr>
<tr>
<td></td>
<td>If Cloud Manager is in your data center, you must set up a VPN connection to</td>
</tr>
<tr>
<td></td>
<td>the VPC and ensure that firewall policies allow traffic to the endpoints.</td>
</tr>
<tr>
<td></td>
<td>If Cloud Manager is in AWS, you must enable Internet access from your VPC by</td>
</tr>
<tr>
<td></td>
<td>using an Internet gateway, NAT device, or proxy server.</td>
</tr>
<tr>
<td></td>
<td>If you have a proxy, you must configure Cloud Manager to use it. You can do</td>
</tr>
<tr>
<td></td>
<td>so when using the Cloud Manager Setup wizard.</td>
</tr>
<tr>
<td></td>
<td>AWS Documentation: Adding an Internet Gateway to Your VPC</td>
</tr>
<tr>
<td></td>
<td>AWS Documentation: NAT</td>
</tr>
<tr>
<td>Requirement</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| A route to the subnets where you will deploy ONTAP Cloud and the mediator | Cloud Manager requires a connection to the subnets in which you will launch ONTAP Cloud instances and the mediator instance, if you deploy an HA configuration.  
Fedora                                                                                   | **AWS networking requirements for ONTAP Cloud HA configurations** on page 18  
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**                                           |
| 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.  
**AWS Documentation: Security Groups for Your VPC**                             |
| 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 either 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 |

**Security group rules for Cloud Manager**

**Inbound rules**

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

<table>
<thead>
<tr>
<th>Type</th>
<th>Port range</th>
<th>Used for</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSH</td>
<td>22</td>
<td>SSH connections to the Cloud Manager instance</td>
</tr>
<tr>
<td>HTTP</td>
<td>80</td>
<td>Accessing the Cloud Manager console</td>
</tr>
<tr>
<td>HTTPS</td>
<td>443</td>
<td>Accessing the Cloud Manager console</td>
</tr>
</tbody>
</table>

**Outbound rules**

<table>
<thead>
<tr>
<th>Type</th>
<th>Port range</th>
<th>Used for</th>
</tr>
</thead>
<tbody>
<tr>
<td>All TCP</td>
<td>All</td>
<td>All outbound traffic</td>
</tr>
<tr>
<td>All UDP</td>
<td>All</td>
<td>All outbound traffic</td>
</tr>
</tbody>
</table>
**AWS networking requirements for ONTAP Cloud**

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

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
</table>
| Internet access to send AutoSupport messages and to access an S3 bucket for upgrades | ONTAP Cloud 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 ONTAP Cloud software directly from Cloud Manager  
Because ONTAP Cloud is most likely running in a private subnet, you can use a NAT device, 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 ONTAP Cloud instances 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 ONTAP Cloud data encryption feature, ONTAP Cloud 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 that there is a route to the subnet in which you deploy ONTAP Cloud instances.  
If the key managers are in your network, a VPN connection provides a route to the subnets in a VPC.  
  *Ways to encrypt ONTAP Cloud data* on page 28                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 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*  

---

**Notes:**

- 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.
## Security group rules for ONTAP Cloud

### Inbound rules

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

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

### Outbound rules

<table>
<thead>
<tr>
<th>Type</th>
<th>Port range</th>
<th>Used for</th>
</tr>
</thead>
<tbody>
<tr>
<td>All ICMP</td>
<td>All</td>
<td>All outbound traffic (SnapMirror and SnapVault)</td>
</tr>
<tr>
<td>All TCP</td>
<td>All</td>
<td>All outbound traffic</td>
</tr>
<tr>
<td>All UDP</td>
<td>All</td>
<td>All outbound traffic</td>
</tr>
</tbody>
</table>
AWS networking requirements for ONTAP Cloud HA configurations

Additional AWS networking requirements apply to ONTAP Cloud HA configurations. You should review these requirements before you launch an ONTAP Cloud HA pair because you must enter the networking details in Cloud Manager.

Availability Zones

To ensure high availability of your data, you must use a dedicated Availability Zone for each ONTAP Cloud instance and the mediator instance, which provides a communication channel between the HA pair. Using the same Availability Zone for more than one instance is not supported. It does not provide high availability for all the required protection scenarios.

If your region does not have three Availability Zones, try to request more from AWS.

Outbound Internet access

The mediator instance must have outbound Internet access so it can communicate with AWS to assist with storage failover.

Floating IP addresses

ONTAP Cloud HA configurations use floating IP addresses for storage failover between nodes when using NFS and CIFS. You must specify three floating IP addresses that are outside of the CIDR blocks for all VPCs in the AWS region where you deploy the HA configuration. You can think of the floating IP addresses as a logical subnet that is outside of the VPCs in your region.

Note: One floating IP address is for cluster management, one is for NFS/CIFS data on node 1, and one is for NFS/CIFS data on node 2. iSCSI data LIFs are created by default and use static IP addresses, rather than floating IP addresses.

Note: If you use SnapDrive for Windows or SnapCenter with an ONTAP Cloud HA pair, a floating IP address is also required for the SVM management LIF. You must create this LIF after you launch the HA pair.

The following example shows the relationship between floating IP addresses and the VPCs in an AWS region. While the floating IP addresses are outside the CIDR blocks for all VPCs, they are routable to subnets through route tables.
You must manually enter the floating IP addresses in Cloud Manager when you create an ONTAP Cloud HA working environment. Cloud Manager allocates the IP addresses to the HA pair when it launches the system.

**Route tables**

After you specify the floating IP addresses in Cloud Manager, you must select the route tables that should include routes to the floating IP addresses. This enables client access to the ONTAP Cloud HA pair.

If you have just one route table for the subnets in your VPC (the main route table), then Cloud Manager automatically adds the floating IP addresses to that route table. If you have more than one route table, it is very important to select the correct route tables. Otherwise, some clients might not have access to the ONTAP Cloud HA pair.

For example, you might have two subnets that are associated with different route tables. If you select route table A, but not route table B, then clients in the subnet associated with route table A can access the HA pair, but clients in the subnet associated with route table B cannot access the HA pair.

*Amazon Web Services (AWS) Documentation: Route Tables*

**Connection to NetApp management tools**

ONTAP Cloud HA configurations use a private, floating IP address for the cluster management interface. Therefore, external routing is not available. If you want to use NetApp management tools with ONTAP Cloud HA configurations, they must be part of the same routing domain.

**Example configuration**

The following image shows an optimal ONTAP Cloud HA configuration in AWS operating as an active-passive configuration:
Sample VPC configurations for Cloud Manager and ONTAP Cloud

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

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

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


A VPC with public and private subnets and a NAT device

This VPC configuration includes public and private subnets, an Internet gateway that connects the VPC to the Internet, and a NAT gateway or 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 ONTAP Cloud instances in the private subnet.

Note: Instead of a NAT device, 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 single node ONTAP Cloud instances running in a private subnet:

AWS region

![Diagram of VPC with Private Subnet and VPN Connection]

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

This VPC configuration is a hybrid cloud configuration in which ONTAP Cloud 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 ONTAP Cloud 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 ONTAP Cloud systems in AWS, you should use a VPN connection so 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 single node ONTAP Cloud instances running in a private subnet:
Granting AWS permissions to Cloud Manager

Cloud Manager needs permissions to perform actions in AWS. The Cloud Manager IAM policy defines the AWS actions and resources that Cloud Manager is allowed to use. You must grant the permissions defined in the IAM policy by associating an IAM role with the Cloud Manager instance or by specifying AWS access keys for each Cloud Manager user account.

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

Setting up an IAM role for the Cloud Manager instance on page 22
Granting permissions to IAM users on page 23

Setting up an IAM role for the Cloud Manager instance

You can grant AWS permissions to Cloud Manager by associating an IAM role with the Cloud Manager instance when you launch it in AWS. Before you launch the instance, you must create an IAM policy and attach it to an IAM role.

About this task
You cannot associate an IAM role with an already running instance of Cloud Manager.

Steps
1. Download the Cloud Manager IAM policy from the following location:
   NetApp OnCommand Cloud Manager: AWS IAM Policy
2. From the IAM console, create your own policy by copying and pasting the text from the Cloud Manager IAM policy.
3. Create an IAM role with the role type Amazon EC2 and attach the policy that you created in the previous step.

Result
You now have an IAM role that you can associate with the Cloud Manager instance when you launch it in AWS.
**After you finish**

When you launch the Cloud Manager instance in a standard AWS region, you must choose Custom Launch to launch the instance from the EC2 console. Launching from the EC2 console enables you to associate the IAM role with the Cloud Manager instance.

*Note:* Launching from the EC2 console is the only option when launching the Cloud Manager instance in the GovCloud (US) region.

**Granting permissions to IAM users**

You can grant AWS permissions to Cloud Manager by specifying AWS access keys for IAM users when you create Cloud Manager user accounts. Before you create the Cloud Manager user accounts, you must grant the required permissions to those IAM users by using the Cloud Manager IAM policy.

**About this task**

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 the Cloud Manager IAM policy from the following location:
   
   *NetApp OnCommand Cloud Manager: AWS IAM Policy*

2. From the IAM console, create your own policy by copying and pasting the text from the Cloud Manager IAM policy.

3. Attach the policy to IAM users or groups.
   
   *AWS Documentation: Managing IAM Policies*

**Result**

IAM users now have the required permissions. When you create Cloud Manager user accounts, you must specify the AWS access keys for those IAM users.

**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.

<table>
<thead>
<tr>
<th>Permissions</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;ec2:DescribeRouteTables&quot;, &quot;ec2:DescribeImages&quot;,</td>
<td>Launches an ONTAP Cloud HA configuration.</td>
</tr>
<tr>
<td>Permissions</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------</td>
<td>---------</td>
</tr>
<tr>
<td>&quot;ec2:CreateTags&quot;,</td>
<td>Tags every resource that Cloud Manager creates with the “WorkingEnvironment” and “WorkingEnvironmentId” tags. Cloud Manager uses these tags for maintenance and cost allocation.</td>
</tr>
<tr>
<td>&quot;ec2:DescribeSubnets&quot;, &quot;ec2:DescribeVpcs&quot;,</td>
<td>Gets the list of destination subnets and security groups, which is needed when creating a new working environment for ONTAP Cloud.</td>
</tr>
<tr>
<td>&quot;ec2:DescribeDhcpOptions&quot;,</td>
<td>Determines DNS servers and the default domain name when launching ONTAP Cloud instances.</td>
</tr>
<tr>
<td>&quot;ec2:CreateSnapshot&quot;, &quot;ec2:DeleteSnapshot&quot;, &quot;ec2:DescribeSnapshots&quot;,</td>
<td>Takes snapshots of EBS volumes during initial setup and whenever an ONTAP Cloud instance is stopped.</td>
</tr>
<tr>
<td>&quot;ec2:GetConsoleOutput&quot;,</td>
<td>Captures the ONTAP Cloud console, which is attached to AutoSupport messages.</td>
</tr>
<tr>
<td>&quot;ec2:DescribeKeyPairs&quot;,</td>
<td>Obtains the list of available key pairs when launching instances.</td>
</tr>
<tr>
<td>&quot;ec2:DescribeRegions&quot;,</td>
<td>Gets a list of available AWS regions.</td>
</tr>
<tr>
<td>Permissions</td>
<td>Purpose</td>
</tr>
<tr>
<td>---------------------------------------------------------------------------</td>
<td>---------------------------------------------------</td>
</tr>
<tr>
<td>&quot;iam:CreateInstanceProfile&quot;, &quot;iam:DeleteRolePolicy&quot;, &quot;iam:AddRoleToInstanceProfile&quot;,</td>
<td></td>
</tr>
<tr>
<td>&quot;iam:RemoveRoleFromInstanceProfile&quot;, &quot;iam:DeleteInstanceProfile&quot;,</td>
<td></td>
</tr>
<tr>
<td>&quot;s3:GetObject&quot;, &quot;s3:ListBucket&quot;</td>
<td>Obtains AWS cost data for ONTAP Cloud.</td>
</tr>
</tbody>
</table>

### How AWS limits can impact ONTAP Cloud

Amazon Web Services has several default limits that can impact your ability to use ONTAP Cloud 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 ONTAP Cloud 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, Cloud Manager must have permissions to access that S3 bucket, and AWS report tags must be enabled after you launch your first ONTAP Cloud instance.

**Before you begin**

You must have granted AWS permissions to Cloud Manager so it can access an S3 bucket.

*Granting AWS permissions to Cloud Manager* on page 22

**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 an ONTAP Cloud 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:
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**

<table>
<thead>
<tr>
<th>AWS Capacity</th>
<th>Allocated Capacity</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.13 TB</td>
<td>3.06 TB</td>
</tr>
</tbody>
</table>

**30% savings**

**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 create a user account, specify the S3 bucket that you created.

   *Creating user accounts* on page 45

   **Note:** If you grant AWS permissions to Cloud Manager by specifying AWS keys, you must create a user account and specify AWS keys for an IAM user created under the payer account or the AWS keys for the payer account itself.

4. After you launch your first ONTAP Cloud 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 ONTAP Cloud 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 software 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**

To run Cloud Manager on an existing host, the physical or virtual machine must meet minimum requirements:

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hypervisor</td>
<td>A bare metal or hosted hypervisor that is certified to run Red Hat Enterprise Linux</td>
</tr>
<tr>
<td></td>
<td><a href="#">Red Hat Solution: Which hypervisors are certified to run Red Hat Enterprise Linux?</a></td>
</tr>
<tr>
<td>Operating system</td>
<td>Red Hat Enterprise Linux 7.1 or 7.2</td>
</tr>
<tr>
<td>CPU</td>
<td>2.27 GHz or higher with two cores</td>
</tr>
<tr>
<td>Component</td>
<td>Requirement</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------</td>
</tr>
<tr>
<td>RAM</td>
<td>4 GB</td>
</tr>
<tr>
<td>Free disk space</td>
<td>50 GB</td>
</tr>
</tbody>
</table>

### Web browser requirements

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

<table>
<thead>
<tr>
<th>Web browser</th>
<th>Minimum supported version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google Chrome</td>
<td>48</td>
</tr>
<tr>
<td>Microsoft Edge</td>
<td>20</td>
</tr>
<tr>
<td>Microsoft Internet Explorer</td>
<td>11</td>
</tr>
<tr>
<td>Mozilla Firefox</td>
<td>43</td>
</tr>
</tbody>
</table>

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 must verify that the following ports are available. If other services are using these ports, Cloud Manager installation fails.

<table>
<thead>
<tr>
<th>Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>Provides HTTP access to the Cloud Manager web console.</td>
</tr>
<tr>
<td>443</td>
<td>Provides HTTPS access to the Cloud Manager web console.</td>
</tr>
<tr>
<td>3306</td>
<td>Used by a MySQL database that stores Cloud Manager data.</td>
</tr>
<tr>
<td>8080</td>
<td>Used by the Simplicator service, which is an API proxy for Cloud Manager.</td>
</tr>
</tbody>
</table>

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 ONTAP Cloud data

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

#### ONTAP Cloud encryption

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

Communication with key managers is always secure. ONTAP Cloud connects to key managers using a TLS connection and communicates using the Key Management Interoperability Protocol (KMIP).
ONTAP Cloud uses the XTS-AES algorithm, a mode of the Advanced Encryption Standard (AES), to protect data-at-rest. Before data is written to disk, it is encrypted using XTS-AES. When data is read from disk, the encrypted data is decrypted using XTS-AES before being sent to the requester.

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

You must set up a key management infrastructure to use ONTAP Cloud 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 ONTAP Cloud encryption

You need a supported key management infrastructure to use ONTAP Cloud 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 ONTAP Cloud systems using secure TLS connections. The following key managers are supported:

- SafeNet Virtual KeySecure for NetApp ONTAP Cloud
  SafeNet OS v8.2.1 is supported.
  AWS Marketplace: SafeNet Virtual KeySecure for NetApp ONTAP Cloud

- SafeNet KeySecure k460
  SafeNet OS v8.0.1 is supported.

Each ONTAP Cloud 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 ONTAP Cloud 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:

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key managers must have a server certificate</td>
<td>Key managers need a server certificate to authenticate with ONTAP Cloud 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 an ONTAP Cloud system, the same certificate authority (CA) must sign the server certificate for each key manager.</td>
</tr>
<tr>
<td>Key managers must trust the signing CA</td>
<td>The CA that signed the server certificate must be known and trusted by the key manager.</td>
</tr>
<tr>
<td>Requirement</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Key managers must have a KMIP server</td>
<td>Each key manager must have a KMIP server that uses SSL and a specific port. The default and recommended port for ONTAP Cloud is 5696. If needed, you can change this port when you set up Cloud Manager.</td>
</tr>
<tr>
<td>Key managers must have a network connection to ONTAP Cloud systems</td>
<td>If the key managers are in AWS, they must have a connection to the subnet in which ONTAP Cloud 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.</td>
</tr>
<tr>
<td>Key managers must trust the Cloud Manager CA and its root CA, if using client certificate authentication</td>
<td>When you set up Cloud Manager, you configure it to act as an intermediate CA so it can sign ONTAP Cloud 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.</td>
</tr>
<tr>
<td>Key managers must check a compatible user name field, if using client certificate authentication</td>
<td>If the key manager's KMIP server checks for a user name in client certificates, it must use a field compatible with ONTAP Cloud client certificates. Cloud Manager can create ONTAP Cloud client certificates that include a user name in the CN (Common Name), E (Email address), and OU (Organizational Unit) fields.</td>
</tr>
</tbody>
</table>

The following graphic depicts these requirements:

![Diagram showing network connections and certificate trust relationships between key managers, KMIP servers, and trusted CAs.]

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 ONTAP Cloud encryption* on page 46
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 single ONTAP Cloud system or an HA pair
- An on-premises ONTAP cluster in your network
- An ONTAP cluster in a NetApp Private Storage configuration

The following image shows an ONTAP Cloud working environment:

![ONTAP Cloud working environment](image)

**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:

![Tenants](image)

**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:

<table>
<thead>
<tr>
<th>No.</th>
<th>Credentials</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>AWS instance credentials for a jump host</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>A jump host is also necessary to manage ONTAP Cloud using System Manager or the CLI. The jump host might be the Cloud Manager instance.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Both cases assume you do not have a VPN connection to the private IP addresses.</td>
</tr>
<tr>
<td>No.</td>
<td>Credentials</td>
<td>Purpose</td>
</tr>
<tr>
<td>-----</td>
<td>------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>2</td>
<td>Cloud Manager web console credentials</td>
<td>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.</td>
</tr>
<tr>
<td>3</td>
<td>AWS access keys for Cloud Manager users</td>
<td>When you create Cloud Manager users, you need to provide Cloud Manager with the AWS access keys for each user.</td>
</tr>
<tr>
<td>4</td>
<td>NetApp Support Site credentials</td>
<td>When you create a tenant, you should enter credentials for a NetApp Support Site account so Cloud Manager can manage licenses for BYOL instances, automatically register pay-as-you-go instances for support, and upgrade ONTAP Cloud software.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><em>Why you should link a tenant to your NetApp Support Site account</em> on page 34</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>No.</th>
<th>Credentials</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>ONTAP Cloud credentials</td>
<td>When users create ONTAP Cloud systems, they need to enter the password for the admin account, which they can use to manage ONTAP Cloud through System Manager or the CLI, if necessary.</td>
</tr>
<tr>
<td>6</td>
<td>ONTAP credentials</td>
<td>When users discover an ONTAP cluster that is in your network or part of a NetApp Private Storage configuration, they must enter the password for the admin account.</td>
</tr>
</tbody>
</table>

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

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

License management for BYOL systems

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

Support registration for pay-as-you-go instances

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

Software upgrades

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

NetApp Support Site account requirements

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

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.

<table>
<thead>
<tr>
<th>Information</th>
<th>Your value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance type</td>
<td></td>
</tr>
<tr>
<td>Virtual Private Cloud</td>
<td></td>
</tr>
<tr>
<td>Subnet</td>
<td></td>
</tr>
<tr>
<td>EC2 key pair</td>
<td></td>
</tr>
</tbody>
</table>
**Information needed to define tenants**

<table>
<thead>
<tr>
<th>Information</th>
<th>Your values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tenant name and NetApp Support Site account</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Information needed to set up Cloud Manager for ONTAP Cloud encryption**

<table>
<thead>
<tr>
<th>Key manager #1</th>
<th>Your value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td></td>
</tr>
<tr>
<td>IP address</td>
<td></td>
</tr>
<tr>
<td>(Optional) Field and key manager user name for client authentication</td>
<td></td>
</tr>
<tr>
<td>Key manager CA certificate available to copy and paste?</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Key manager #2</th>
<th>Your value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td></td>
</tr>
<tr>
<td>IP address</td>
<td></td>
</tr>
<tr>
<td>(Optional) Field and key manager user name for client authentication</td>
<td></td>
</tr>
<tr>
<td>Key manager CA certificate available to copy and paste?</td>
<td></td>
</tr>
</tbody>
</table>
Subscribing to ONTAP Cloud in AWS

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

About this task

- Subscribing to ONTAP Cloud means that you have accepted the terms of the product. Subscribing does not cost you anything until you launch an ONTAP Cloud 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.
- Subscribing to ONTAP Cloud is not necessary if you want to launch instances in the AWS GovCloud (US) region.

Steps

1. Go to the AWS Marketplace pages for ONTAP Cloud:
   
   - AWS Marketplace: ONTAP Cloud for AWS
   - AWS Marketplace: ONTAP Cloud for AWS (BYOL)
   - AWS Marketplace: ONTAP Cloud for AWS - High Availability
   - AWS Marketplace: ONTAP Cloud for AWS - High Availability (BYOL)

2. Review the terms, and then click Accept.

After you finish

You must use Cloud Manager to launch ONTAP Cloud instances. You must not launch ONTAP Cloud 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 (AWS) or by installing Cloud Manager on an existing Linux host. The standard method is to launch a Cloud Manager instance in AWS using the AMI.

Choices

- Launching a Cloud Manager instance in a standard AWS region on page 37
- Launching a Cloud Manager instance in the AWS GovCloud (US) region on page 38
- Installing Cloud Manager on an existing Linux host on page 40

Launching a Cloud Manager instance in a standard AWS region

You can use the Cloud Manager AMI from the AWS Marketplace to launch an EC2 instance in a standard AWS region (a region other than the AWS GovCloud (US) region). This gives you access to the Cloud Manager software, which 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.
  Amazon Web Services (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. Review the available delivery methods.
   Single AMI launches just the Cloud Manager instance (this is the standard delivery method). The advanced methods launch a stack of the software in a specific configuration: Cloud Manager, ONTAP Cloud, and EBS storage.
   No matter which method you choose, users can launch ONTAP Cloud instances after you set up Cloud Manager.

3. Under Pricing Details, choose a delivery method, review the estimated price, and then click Continue.

4. If you chose the Single AMI delivery method, launch the instance from the 1-Click Launch tab or the Custom Launch tab, depending on how you want to grant AWS permissions to Cloud Manager:
### Choice
You do not want to associate the instance with an IAM role. You want to specify AWS keys for each Cloud Manager user account.

<table>
<thead>
<tr>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. On the 1-Click Launch tab, specify settings for the instance. Note the following:</td>
</tr>
<tr>
<td>• The t2.medium instance type is recommended.</td>
</tr>
<tr>
<td>• Under security group, select Create new based on seller settings to create a pre-defined security group that includes the rules required by Cloud Manager.</td>
</tr>
<tr>
<td>b. Click Accept Terms and Launch with 1-Click.</td>
</tr>
</tbody>
</table>

You want to associate the instance with an IAM role.

<table>
<thead>
<tr>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. On the Custom Launch tab, click Launch with EC2 Console for your region.</td>
</tr>
<tr>
<td>b. Choose an instance type.</td>
</tr>
<tr>
<td>The t2.medium instance type is recommended.</td>
</tr>
<tr>
<td>c. Select a VPC, subnet, IAM role, and other configuration options that meet your requirements.</td>
</tr>
<tr>
<td>d. Keep the default storage options.</td>
</tr>
<tr>
<td>e. Enter tags for the instance, if desired.</td>
</tr>
<tr>
<td>f. Specify the required connection methods for the Cloud Manager instance: SSH, HTTP, and HTTPS.</td>
</tr>
<tr>
<td>g. Click Launch.</td>
</tr>
</tbody>
</table>

| 5. If you chose an advanced delivery method, specify settings for the instance and then launch the software: |
| a. On the Custom Launch tab, specify settings for the instance. |
| b. Click Launch with CloudFormation Console and follow the steps to launch a stack of the software. |

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

### After you finish
Log in to Cloud Manager by using a web browser and complete the Setup wizard.

### Related references
- AWS networking requirements for Cloud Manager on page 14

### Launching a Cloud Manager instance in the AWS GovCloud (US) region
Cloud Manager must run in the AWS GovCloud (US) region if you want to launch ONTAP Cloud instances in AWS GovCloud (US). You can gain access to the Cloud Manager software by launching
an EC2 instance from the Cloud Manager AMI. The Cloud Manager software is automatically installed on the instance.

**Before you begin**

You should have purchased one or more licenses for ONTAP Cloud.

Instructions are available at *NetApp ONTAP Cloud for GovCloud.*

**Steps**

1. Log in to the AWS Management Console for the AWS GovCloud (US) region.
2. Select the EC2 service.
3. From the **EC2 Dashboard**, click **Launch Instance**:

   ![Launch Instance](image)

4. Click **Community AMIs** and then search for Cloud Manager or ONTAP Cloud.
5. To the right of the AMI name, click **Select**:

   ![Select AMI](image)

6. Complete the pages to launch the instance:

<table>
<thead>
<tr>
<th>On this page...</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Choose Instance Type</td>
<td>Select the <strong>t2.medium</strong> or <strong>m3.medium</strong> instance type. <strong>t2.medium</strong> is recommended.</td>
</tr>
<tr>
<td>Configure Instance</td>
<td>Select a VPC and subnet, and then choose other configuration options that meet your requirements.</td>
</tr>
<tr>
<td>On this page...</td>
<td>Do this...</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------</td>
</tr>
<tr>
<td>Add Storage</td>
<td>Keep the default settings.</td>
</tr>
<tr>
<td>Tag Instance</td>
<td>Enter tags for the instance, if desired.</td>
</tr>
<tr>
<td>Configure</td>
<td>Create a new security group or choose an existing security group. The security group must include the required rules.</td>
</tr>
<tr>
<td>Security Group</td>
<td>Source networking requirements for Cloud Manager on page 14</td>
</tr>
<tr>
<td>Review</td>
<td>Review the instance launch details, make changes if necessary, and then click Launch.</td>
</tr>
</tbody>
</table>

**Result**

AWS launches the Cloud Manager instance with the specified settings. The instance and the 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.

*Setting up OnCommand Cloud Manager* on page 42

**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.
- Cloud Manager installs the AWS command line tools (awscli) to enable recovery procedures from NetApp support.
  - If you receive a message that installing the awscli failed, you can safely ignore the message. Cloud Manager can operate successfully without the tools.

**Steps**

1. Download the software from the NetApp Support Site, and then copy it to the Linux host.
   
   *NetApp Downloads: Software*
   
   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-V3.0.0.sh`

3. Run the installation script:

   `./OnCommandCloudManager-V3.0.0.sh [silent] [proxy=ipaddress] [proxyport=port] [proxyuser=user_name] [proxypwd=password]`

   *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.
proxyuser is the user name for the proxy server, if basic authentication is required.
proxypwd is the password for the user name that you specified.

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.

**Result**

Cloud Manager is now installed. At the end of the installation, the Cloud Manager service (occm) restarts twice if you specified a proxy server.

**After you finish**

Log in to Cloud Manager using a web browser, and then complete the Setup wizard.
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 13

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.png)

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

<table>
<thead>
<tr>
<th>On this page...</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Welcome</td>
<td>Click <strong>Storage System View</strong>.</td>
</tr>
<tr>
<td>Cloud Manager</td>
<td>Click <strong>Set up new Cloud Manager</strong>.</td>
</tr>
<tr>
<td>On this page...</td>
<td>Do this...</td>
</tr>
<tr>
<td>----------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Proxy Setup</td>
<td>If the host does not have access to the Internet, enter the location to a proxy server using the syntax <a href="http://address:port">http://address:port</a> and specify a user name and password if basic authentication is required for the 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 network.</td>
</tr>
<tr>
<td>Let us know who you are</td>
<td>Specify your site and company name.</td>
</tr>
<tr>
<td>Create an admin user</td>
<td>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.</td>
</tr>
</tbody>
</table>
| Credentials          | • Specify AWS keys for the administrator user account (unless you associated the Cloud Manager instance with an IAM role). Granting AWS permissions to Cloud Manager on page 22  
                        • Confirm that you have adhered to IAM policy requirements. NetApp OnCommand Cloud Manager: AWS IAM Policy  
                        • To see AWS storage and compute costs in Cloud Manager, specify an S3 bucket that contains detailed billing reports. Setting up AWS billing and cost management on page 25 |
| 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 31                                                                 |
| NetApp Support Site credentials | Enter credentials for a NetApp Support Site account. Why you should link a tenant to your NetApp Support Site account on page 34                                                                 |
| Review               | Enable automatic updates to make sure that you are running the latest version, read and accept the End User License Agreement, choose a capacity management mode, and then click Go. Note the following about the capacity management modes:  
                        • To automate storage capacity decisions, choose Automatic Mode. Cloud Manager automatically purchases new AWS disks for ONTAP Cloud instances when more capacity is needed, deletes unused collections of disks (aggregates), and moves volumes between aggregates, as needed.  
                          Important: In Automatic Mode, Cloud Manager allocates the appropriate EBS resources as needed, without asking for approval.  
                        • If you want users to make those decisions, then choose Manual Mode. Cloud Manager displays Action Required messages when capacity decisions must be made. It is up to the user to accept the actions. |

**After you finish**

Continue setting up Cloud Manager by doing the following:

- Installing an HTTPS certificate for secure access
- Creating additional tenants
- Creating user accounts so that other users can access Cloud Manager
• Setting up Cloud Manager so that users can use ONTAP Cloud 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:

Creating tenants

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

Steps

1. 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.
   *Why you should link a tenant to your NetApp Support Site account* on page 34

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**.

![Cloud Manager Admin](image)

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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email Address</td>
<td>Enter the email address that the user must use to log in to Cloud Manager. Cloud Manager does not send emails to this address.</td>
</tr>
<tr>
<td>Role</td>
<td>Select one of the three roles:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Cloud Manager Admin</strong>: Administers the product and has access to all tenants and working environments.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Tenant Admin</strong>: Administers a single tenant. Can create and manage all working environments and users in the tenant.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Working Environment Admin</strong>: Administers one or more working environments in a tenant.</td>
</tr>
</tbody>
</table>

   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, unless you associated an IAM role with the Cloud Manager instance. 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. Giving Cloud Manager access to detailed billing reports enables users to see AWS storage and compute costs associated with ONTAP Cloud. If you are using AWS consolidated billing and you specified AWS keys, 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 25

### Setting up Cloud Manager for ONTAP Cloud encryption

The Cloud Manager Admin user must set up Cloud Manager before other users can enable ONTAP Cloud encryption on new ONTAP Cloud 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 ONTAP Cloud encryption* on page 29

**Steps**
1. **Understand how ONTAP Cloud encryption works** on page 47
   Understanding how ONTAP Cloud encryption works can help you set up and use the feature.
2. **Set up Cloud Manager to be an intermediate CA** on page 48
   Cloud Manager must be an intermediate certificate authority (CA) because it needs to create client certificates for ONTAP Cloud. 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 48
   Cloud Manager needs information about your key managers and CA certificates so users can select them for use with ONTAP Cloud systems.
Understanding how ONTAP Cloud encryption works

Understanding how ONTAP Cloud 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 ONTAP Cloud instances with encryption enabled. Cloud Manager sets up ONTAP Cloud by installing the key manager CA certificate, generating and installing a client certificate, configuring the KMIP client, and linking the system to one or more key managers.
   
   **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, ONTAP Cloud generates and sends an encryption key to key managers.

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

5. Before data is written to disk, it is encrypted using XTS-AES.
   When data is read from disk, the encrypted data is decrypted using XTS-AES before being sent.
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 ONTAP Cloud. 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 ONTAP Cloud systems. The following image shows a Cloud Manager system that is configured to be an intermediate 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 ONTAP Cloud 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 ONTAP Cloud 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**:

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

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 ONTAP Cloud systems with encryption enabled.
# What to do after installation and setup

After you set up Cloud Manager, users can launch ONTAP Cloud instances, discover 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:

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create and manage working environments using the web console:</td>
<td>* OnCommand Cloud Manager 3.0 Storage System Management Guide</td>
</tr>
<tr>
<td>• Launch ONTAP Cloud instances</td>
<td></td>
</tr>
<tr>
<td>• Provision storage for ONTAP Cloud</td>
<td></td>
</tr>
<tr>
<td>• Discover on-premises FAS systems and existing NetApp Private Storage</td>
<td></td>
</tr>
<tr>
<td>• Replicate data to and from the cloud</td>
<td></td>
</tr>
<tr>
<td>Administer Cloud Manager using the web console:</td>
<td>* OnCommand Cloud Manager 3.0 Administration Guide</td>
</tr>
<tr>
<td>• Back up Cloud Manager</td>
<td></td>
</tr>
<tr>
<td>• Manage user accounts</td>
<td></td>
</tr>
<tr>
<td>• Configure Cloud Manager settings</td>
<td></td>
</tr>
<tr>
<td>• Troubleshoot issues</td>
<td></td>
</tr>
<tr>
<td>Review release-specific information (known issues, limitations, and so</td>
<td>* OnCommand Cloud Manager 3.0 Release Notes</td>
</tr>
<tr>
<td>on) for Cloud Manager and ONTAP Cloud</td>
<td>* Find the Release Notes for your version of ONTAP Cloud</td>
</tr>
<tr>
<td>View more documentation and videos for ONTAP Cloud and Cloud Manager</td>
<td>* NetApp ONTAP Cloud Resources</td>
</tr>
<tr>
<td>Get help</td>
<td>* NetApp ONTAP Cloud Support</td>
</tr>
<tr>
<td></td>
<td>* NetApp Community: Hybrid Cloud</td>
</tr>
</tbody>
</table>
## Updating Cloud Manager

You can update Cloud Manager to the latest version or with a patch that NetApp personnel shared with you. How you update Cloud Manager depends on which version you are currently running.

### Choices
- Enabling automatic updates on page 51
- Updating Cloud Manager from 2.1 and later to 3.0 on page 51
- Updating Cloud Manager from 2.0 or earlier to 3.0 on page 52
- Updating Cloud Manager with a patch on page 57

### Enabling automatic updates

Cloud Manager can automatically update itself when a new version is available. This ensures that you are running the latest version.

**About this task**

Cloud Manager automatically updates at 12:00 midnight if no operations are running. Major updates (for example, 3.0 to 4.0) are not automatically installed. You must manually update Cloud Manager when a new major version is available.

**Steps**

1. In the upper right of the Cloud Manager console, click the task drop-down list, and then select **Settings**.
2. Select the checkbox under **Automatic Update** and then click **Save**.

### Updating Cloud Manager from 2.1 and later to 3.0

You can update Cloud Manager to the latest version directly from the web console. Cloud Manager obtains the software update from a NetApp-owned S3 bucket in AWS.

**Before you begin**

You should have reviewed the *OnCommand Cloud Manager Release Notes* to identify new requirements and changes in support.

**About this task**

The software update takes a few minutes. Cloud Manager will not be available during the update.

**Steps**

1. Check whether a new version is available by looking at the lower-right corner of the console:

   ![New version available](image)

2. If a new version is available, click **Timeline** to determine whether any tasks are in progress. If any tasks are in progress, wait for them to finish before you proceed to the next step.
3. In the lower-right of the console, click **New version available**.

4. On the **Cloud Manager Software Update** page, click **Update** next to the version that you want.

5. Complete the confirmation dialog box, and then click **OK**:

   a. Keep the option to download a backup because you can use it to restore your Cloud Manager configuration, if necessary.

   b. Read the terms and conditions, and then select the **I read and approve the terms and conditions (EULA)** check box.

6. When prompted, save the Cloud Manager backup.

**Result**

Cloud Manager starts the update process. You can log in to the console after a few minutes.

### Updating Cloud Manager from 2.0 or earlier to 3.0

Cloud Manager 3.0 is supported on Linux only. You cannot directly upgrade to 3.0 from 2.0 or earlier because those releases supported Windows only. You must set up Cloud Manager 3.0 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 3.0** on page 52
   
   You can install the Cloud Manager software by launching a Cloud Manager instance in Amazon Web Services (AWS) or by installing Cloud Manager on an existing Linux host. The standard method is to launch a Cloud Manager instance in AWS using the AMI.

2. **Import your existing Cloud Manager configuration** on page 55
   
   After you install Cloud Manager on a new host, you can import an existing configuration to the new Cloud Manager database.

3. **Set Cloud Manager as the target for ONTAP Cloud configuration backups** on page 56
   
   You should configure ONTAP Cloud to send configuration backups to Cloud Manager if the target location is currently the NetApp Support instance, or if you added new working environments to Cloud Manager by discovering existing ONTAP Cloud instances.

4. **Remove your previous Cloud Manager configuration** on page 56
   
   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 57
   
   You should terminate the NetApp Support instance from the EC2 console after you update Cloud Manager to version 2.2 or later and configure ONTAP Cloud 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 (AWS) or by installing Cloud Manager on an existing Linux host. The standard method is to launch a Cloud Manager instance in AWS using the AMI.

**Choices**

- **Launching a Cloud Manager instance in a standard AWS region** on page 53
• Installing Cloud Manager on an existing Linux host on page 54

Launching a Cloud Manager instance in a standard AWS region

You can use the Cloud Manager AMI from the AWS Marketplace to launch an EC2 instance in a standard AWS region (a region other than the AWS GovCloud (US) region). This gives you access to the Cloud Manager software, which 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.
  Amazon Web Services (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. Review the available delivery methods.
  Single AMI launches just the Cloud Manager instance (this is the standard delivery method). The advanced methods launch a stack of the software in a specific configuration: Cloud Manager, ONTAP Cloud, and EBS storage.

  No matter which method you choose, users can launch ONTAP Cloud instances after you set up Cloud Manager.

3. Under Pricing Details, choose a delivery method, review the estimated price, and then click Continue.

4. If you chose the Single AMI delivery method, launch the instance from the 1-Click Launch tab or the Custom Launch tab, depending on how you want to grant AWS permissions to Cloud Manager:

<table>
<thead>
<tr>
<th>Choice</th>
<th>Steps</th>
</tr>
</thead>
</table>
| You do not want to associate the instance with an IAM role. You want to specify AWS keys for each Cloud Manager user account. | a. On the 1-Click Launch tab, specify settings for the instance. Note the following:  
• The t2.medium instance type is recommended.  
• Under security group, select Create new based on seller settings to create a pre-defined security group that includes the rules required by Cloud Manager.  
  b. Click Accept Terms and Launch with 1-Click. |
You want to associate the instance with an IAM role.

a. On the Custom Launch tab, click Launch with EC2 Console for your region.

b. Choose an instance type. The t2.medium instance type is recommended.

c. Select a VPC, subnet, IAM role, and other configuration options that meet your requirements.

d. Keep the default storage options.

e. Enter tags for the instance, if desired.

f. Specify the required connection methods for the Cloud Manager instance: SSH, HTTP, and HTTPS.

g. Click Launch.

5. If you chose an advanced delivery method, specify settings for the instance and then launch the software:

   a. On the Custom Launch tab, specify settings for the instance.

   b. Click Launch with CloudFormation Console and follow the steps to launch a stack of the software.

Result

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

After you finish

Log in to Cloud Manager by using a web browser and complete the Setup wizard.

Related references

AWS networking requirements for Cloud Manager on page 14

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.
- Cloud Manager installs the AWS command line tools (awscli) to enable recovery procedures from NetApp support.
  If you receive a message that installing the awscli failed, you can safely ignore the message. Cloud Manager can operate successfully without the tools.

Steps

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

   NetApp Downloads: Software
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**
   ```bash
   chmod +x OnCommandCloudManager-V3.0.0.sh
   ```

3. Run the installation script:

   ```bash
   ./OnCommandCloudManager-V3.0.0.sh [silent] [proxy=ipaddress] [proxyport=port] [proxyuser=user_name] [proxypwd=password]
   ```

   - `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.
   - `proxyuser` is the user name for the proxy server, if basic authentication is required.
   - `proxypwd` is the password for the user name that you specified.

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.

**Result**

Cloud Manager is now installed. At the end of the installation, the Cloud Manager service (occm) restarts twice if you specified a proxy server.

**After you finish**

Log in to Cloud Manager using a web browser, and then complete the Setup wizard.

**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.

**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. On the Welcome page, click Storage System View, and then 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 ONTAP Cloud to send configuration backups to Cloud Manager
You should configure ONTAP Cloud to send configuration backups to Cloud Manager if the target location is currently the NetApp Support instance, or if you added new working environments to Cloud Manager by discovering existing ONTAP Cloud instances.

About this task
ONTAP Cloud instances launched from Cloud Manager 2.1 and later automatically send configuration backups to Cloud Manager using HTTPS. ONTAP Cloud 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 ONTAP Cloud 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 ONTAP Cloud instances.

Result
ONTAP Cloud 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 57
• Uninstalling the Cloud Manager software on page 57
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 should terminate the NetApp Support instance from the EC2 console after you update Cloud Manager to version 2.2 or later and configure ONTAP Cloud instances to send configuration backups to Cloud Manager.

**About this task**

The NetApp Support instance is no longer launched by Cloud Manager because ONTAP Cloud 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**.

Updating Cloud Manager with a patch

If NetApp shared a patch with you, you can update Cloud Manager with the supplied patch directly from the Cloud Manager web console.

**About this task**

The patch update typically takes a few minutes. Cloud Manager will not be available during the update.

**Steps**
1. In the upper-right hand corner of the Cloud Manager console, click the task drop-down list, and then select **Update**.
2. Click the link to update Cloud Manager with the supplied patch.
3. Complete the confirmation dialog box and then click **OK**:
   a. Keep the option to download a backup enabled because you can use it to restore your Cloud Manager configuration, if necessary.
   b. Read the terms and conditions and then select the **I read and approve the terms and conditions (EULA)** check box.

4. Select the patch that you were provided.

5. When prompted, save the Cloud Manager backup.

**Result**

Cloud Manager applies the patch. You can log in to the console after a few minutes.
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 © 1994–2016 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.

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.

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

about this guide
  deciding whether to use 5
accounts
  creating Cloud Manager users 45
  credentials for 32
Amazon Web Services
  billing and cost requirements 25
  default limits 25
  encryption overview 28
  granting permissions to IAM users 23
  launching Cloud Manager in standard region 37, 53
  launching Cloud Manager in the AWS GovCloud (US) region 38
  networking requirements for Cloud Manager 14
  networking requirements for ONTAP Cloud 16
  preparing the environment 13
  sample VPC configurations 20
  setting up an IAM role 22
  subscribing to ONTAP Cloud software from 36
  what Cloud Manager does with permissions 23
APIs
  overview of 11
  audience
    for this guide 5
AWS
  See Amazon Web Services

B

backups, cluster configuration
  sending to Cloud Manager 56
billing and cost requirements
  verifying IAM user access to billing information 25

C

certificate signing request
  generating 48
  certificates
    adding CA certificates to Cloud Manager 48
    installing Cloud Manager certificate 48
    installing HTTPS certificate 44
    requirements 29
Chrome
  supported versions 27
Cloud Manager
  enabling automatic updates of 51
  introduction to updating 51, 52
  See also OnCommand Cloud Manager
cluster configuration backups
  sending to Cloud Manager 56
comments
  how to send feedback about documentation 62
  components
    credentials for 32
    configuration, Cloud Manager
  importing 55
  cost
    requirements to display in Cloud Manager 25
CPU
  required for Cloud Manager 27
credentials
  types of and purposes 32

D

disk space
  required for Cloud Manager 27
documentation
  how to receive automatic notification of changes to 62
  how to send feedback about 62
  where to find additional 50

E

encryption
  deciding whether to use 28
  key manager requirements 29
  setting up Cloud Manager for 46
  understanding how it works in ONTAP Cloud 47

F

feedback
  how to send comments about documentation 62
Firefox
  supported versions 27

G

GovCloud
  launching Cloud Manager in 38

H

HA configurations
  best practices 18
  how storage works 9
  how they work 8
  requirements 18
high availability
  See HA configurations
hosts, Linux
  installing OnCommand Cloud Manager on existing 40, 54
HTTPS certificate
  installing 44

I

IAM roles
  setting up for Cloud Manager 22
IAM users
  granting permissions to 23
  what Cloud Manager does with permissions 23
information
  how to send feedback about improving documentation 62
installation
  gathering information for 34
  preparing for OnCommand Cloud Manager 13
  what to do after 50
  worksheets 34
installing OnCommand Cloud Manager
  on existing Linux hosts 40, 54
  workflow 12
instance
  terminating, Cloud Manager 57
  terminating, NetApp Support 57
instance limits
  for AWS 25
intermediate CA
  setting up Cloud Manager 48
Internet Explorer
  supported versions 27

K
key managers
  adding to Cloud Manager 48
  requirements 29
KMIP server
  requirements 29

L
Linux hosts
  installing OnCommand Cloud Manager on existing 40, 54

N
NetApp Support instance
  terminating 57
NetApp Support Site account
  how Cloud Manager uses an account 34
  requirements 34

O
OnCommand Cloud Manager
  AWS networking requirements for 14
  billing and cost requirements 25
  creating admin user of 45
  creating user accounts 45
  EC2 instance requirements 27
  granting AWS permissions to 22
  host requirements 27
  importing an existing configuration 55
  information needed to launch in AWS 34
  installation and setup workflow 12
  installing on an existing Linux host 40, 54
  launching in AWS 37, 53
  launching in the AWS GovCloud (US) region 38
  preparing for installation and setup 13
  setting up 42
  setting up an IAM role for 22
  setting up to be intermediate CA 48
  supported web browsers 27
  terminating the instance 57
  uninstalling 57, 59
  updating to the latest version 51
  updating with a patch 57
  what it is 6
ONTAP Cloud
  AWS networking requirements for 16
  encryption overview 28
  HA best practices 18
  HA configuration overview 8
  HA configuration requirements 18
  HA storage overview 9
  product models 7
  sending configuration backups to Cloud Manager 56
  subscribing to the software in AWS 36
  what it is 7
ONTAP Cloud BYOL
  NetApp Support Site account requirements 34
ONTAP Cloud encryption
  understanding how it works 47
  operating system
    required for Cloud Manager 27

P
patches
  updating Cloud Manager with 57
pay-as-you-go instances
  NetApp Support Site account requirements 34
permissions
  granting to IAM users 23
  purposes of 23
ports
  requirements for Cloud Manager 14
  requirements for ONTAP Cloud 16
proxy server
  configuring Cloud Manager to use 42

R
RAM
  required for Cloud Manager 27
  requirements
    OnCommand Cloud Manager 27

S
security groups
  requirements for Cloud Manager 14
  requirements for ONTAP Cloud 16
setup
  credentials used for OnCommand Cloud Manager 32
  gathering information for 34
  preparing for OnCommand Cloud Manager 13
  what to do after 50
  workflow 12
  worksheets 34
SSL certificates
  requirements 29
storage
  how it works in an HA pair 9
storage limits
  for AWS 25
subnets
  requirements for Cloud Manager 14
  requirements for ONTAP Cloud 16
suggestions
  how to send feedback about documentation 62

T
  tenants
    creating 44
    creating admin user of 45
    definition of 31
    how to use 31
troubleshooting
  uninstalling software first 59
Twitter
  how to receive automatic notification of documentation changes 62

U
  uninstalling
    OnCommand Cloud Manager 59
updates
  enabling automatic updates 51
importing an existing Cloud Manager configuration 55
introduction to updating Cloud Manager 51
introduction to updating Cloud Manager to the latest version 52
updating Cloud Manager to the latest version 51
updating Cloud Manager with a patch 57
user accounts
  creating 45
users
  definition of 31

V
  Virtual Private Clouds
    requirements for Cloud Manager 14
    requirements for ONTAP Cloud 16
    sample configurations 20

W
  web browsers
    supported versions 27
working environments
  creating admin user of 45
  creating tenants for 44
  definition of 31
worksheets
  installation and setup 34