



# Cloud & Manager 3.5

Getting started

NetApp Docs

2020

# Table of Contents

1. Getting started .....	1
1.1. Deployment overview .....	1
1.2. Getting started with Cloud Volumes ONTAP in AWS .....	2
1.3. Getting started with Cloud Volumes ONTAP in Azure .....	3
1.4. Setting up Cloud Manager .....	5
1.5. Detailed networking requirements .....	11
1.6. Additional deployment options .....	22
1.7. Additional ways to provide permissions .....	30

# 1. Getting started

## 1.1. Deployment overview

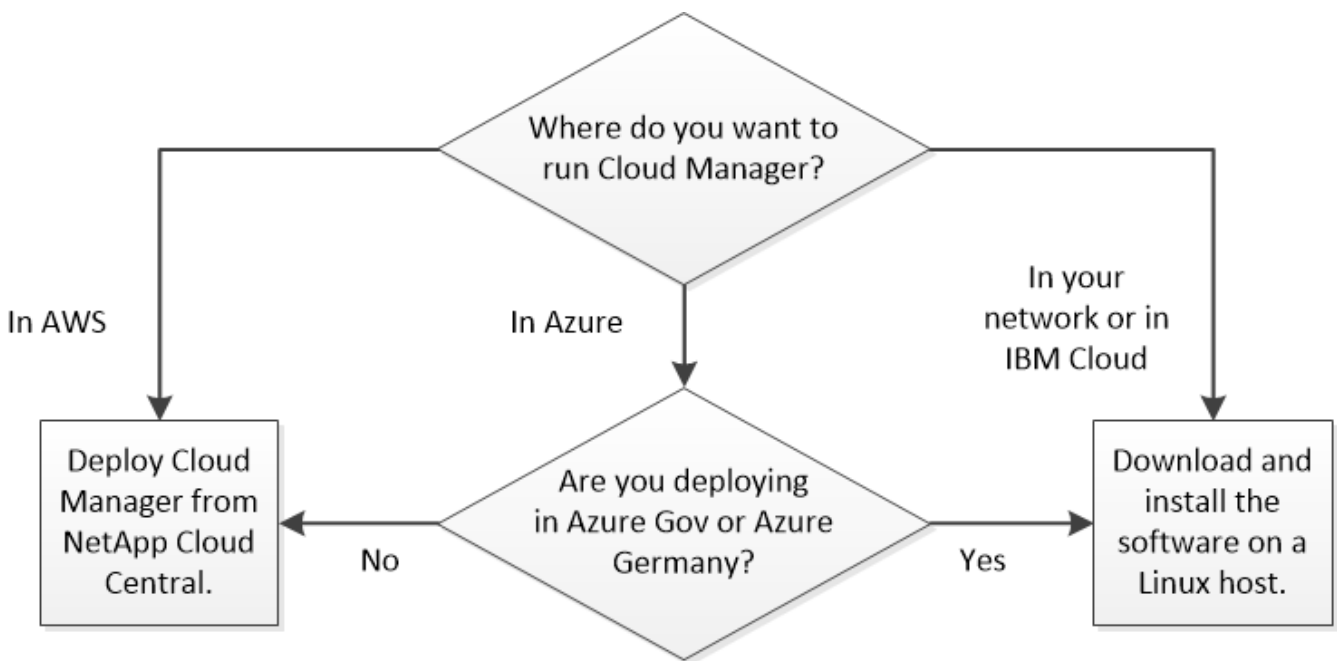
Before you get started, you might want to better understand your options for deploying OnCommand Cloud Manager and Cloud Volumes ONTAP.

### 1.1.1. Cloud Manager installation

Cloud Manager software is required to deploy and manage Cloud Volumes ONTAP. You can deploy Cloud Manager in any of the following locations:

- Amazon Web Services (AWS)
- Microsoft Azure
- IBM Cloud
- In your own network

How you deploy Cloud Manager depends on which location you choose:



Refer to the following for deploying Cloud Manager from NetApp Cloud Central:

- [Getting started in AWS](#)
- [Getting started in Azure](#)

For all other scenarios, refer to the following:

- [Installing Cloud Manager in an Azure US Gov region](#)
- [Installing Cloud Manager in the Azure Germany region](#)
- [Installing Cloud Manager on a Linux host](#)

### 1.1.2. Cloud Manager setup

You might want to perform additional setup after you install Cloud Manager, such as adding additional AWS accounts, installing an HTTPS certificate, and more. For instructions, see [Setting up Cloud Manager](#).

### 1.1.3. Cloud Volumes ONTAP deployment

After you get Cloud Manager up and running, you can start deploying Cloud Volumes ONTAP in AWS and in Microsoft Azure.

[Getting started in AWS](#) and [Getting started in Azure](#) provide instructions for getting Cloud Volumes ONTAP up and running quickly. For additional help, refer to the following:

- [Supported configurations for Cloud Volumes ONTAP 9.4](#)
- [Planning your configuration](#)
- [Launching Cloud Volumes ONTAP in AWS](#)
- [Launching Cloud Volumes ONTAP in Azure](#)

## 1.2. Getting started with Cloud Volumes ONTAP in AWS

You can get started with Cloud Volumes ONTAP in AWS by completing a few quick steps.



#### Set up your networking

- a. Enable outbound internet access from the target VPC so Cloud Manager and Cloud Volumes ONTAP can contact several endpoints.

This step is important because Cloud Manager cannot deploy Cloud Volumes ONTAP without outbound internet access. If you need to limit outbound connectivity, refer to the list of endpoints for [Cloud Manager](#) and [Cloud Volumes ONTAP](#).

- b. Set up a VPC endpoint to the S3 service.

A VPC endpoint is required if you want to tier cold data from Cloud Volumes ONTAP to low-cost object storage.



#### Subscribe to Cloud Volumes ONTAP from the AWS Marketplace

Subscribing from [the AWS Marketplace](#) is required to accept the software terms. You should only subscribe from the Marketplace. Launching Cloud Volumes ONTAP from anywhere but Cloud Manager is not supported.



### **Provide the required AWS permissions**

When you deploy Cloud Manager from NetApp Cloud Central, you need to use an AWS account that has permissions to deploy the instance.

- a. Go to the AWS IAM console and create a policy by copying and pasting the contents of the [NetApp-provided JSON file](#).
- b. Attach the policy to the IAM user.



### **Launch Cloud Manager from NetApp Cloud Central**


Cloud Manager software is required to deploy and manage Cloud Volumes ONTAP. It takes just a few minutes to launch a Cloud Manager instance from [Cloud Central](#).



### **Launch Cloud Volumes ONTAP using Cloud Manager**

Once Cloud Manager is ready, just click Create, select the type of system that you would like to launch, and complete the steps in the wizard. After 25 minutes, your first Cloud Volumes ONTAP system should be up and running.

Watch the following video for a walk through of these steps:

 | <https://img.youtube.com/vi/au5qQDiPuzo/maxresdefault.jpg>

#### *Related links*

- [Networking requirements for Cloud Manager](#)
- [Networking requirements for Cloud Volumes ONTAP in AWS](#)
- [Security group rules for AWS](#)
- [Setting up Cloud Manager](#)
- [Launching Cloud Volumes ONTAP in AWS](#)

## **1.3. Getting started with Cloud Volumes ONTAP in Azure**

You can get started with Cloud Volumes ONTAP in Azure by completing a few quick steps. Separate instructions are available to deploy Cloud Manager in [US Gov regions](#) and in [Azure Germany regions](#).



### **Set up your networking**

Enable outbound internet access from the target VNet so Cloud Manager and Cloud Volumes ONTAP can contact several endpoints.

This step is important because Cloud Manager cannot deploy Cloud Volumes ONTAP without outbound internet access. If you need to limit outbound connectivity, refer to the list of endpoints for [Cloud Manager](#) and [Cloud Volumes ONTAP](#).



## Provide the required Azure permissions

When you deploy Cloud Manager from NetApp Cloud Central, you need to use an Azure account that has permissions to deploy the Cloud Manager virtual machine.

- a. Download the [NetApp-provided JSON file](#).
- b. Modify the JSON file by adding your Azure subscription ID to the "AssignableScopes" field.
- c. Use the JSON file to create a custom role in Azure named *Azure SetupAsService*.

Example:            **az**            **role**            **definition**            **create**            **--role-definition**  
**C:\Policy\_for\_Setup\_As\_Service\_Azure.json**

- d. From the Azure portal, assign the custom role to the user who will deploy Cloud Manager from Cloud Central.



## Launch Cloud Manager from NetApp Cloud Central

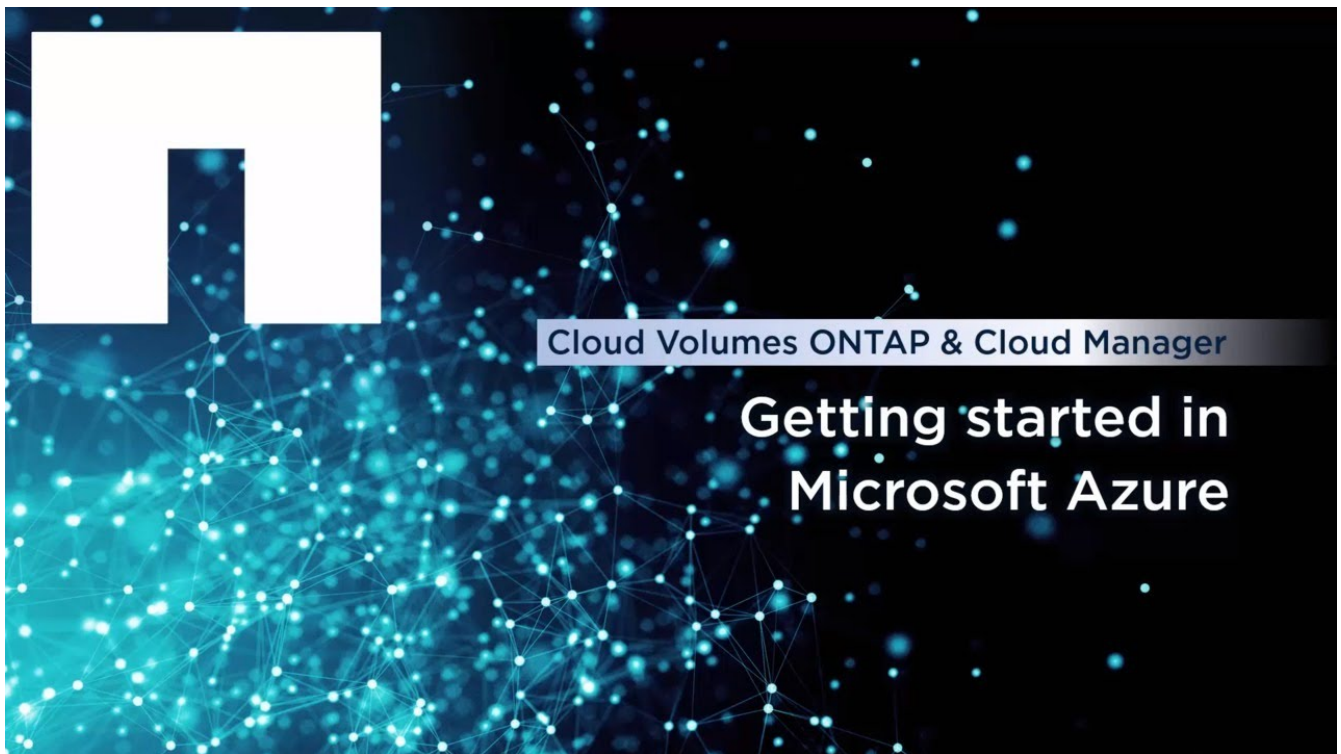
Cloud Manager software is required to deploy and manage Cloud Volumes ONTAP. It takes just a few minutes to launch a Cloud Manager instance from [Cloud Central](#).



## Launch Cloud Volumes ONTAP using Cloud Manager

Once Cloud Manager is ready, just click Create, select the type of system that you would like to deploy, and complete the steps in the wizard. After 25 minutes, your first Cloud Volumes ONTAP system should be up and running.

Watch the following video for a walk through of these steps:



#### *Related links*

- [Networking requirements for Cloud Manager](#)
- [Networking requirements for Cloud Volumes ONTAP in Azure](#)
- [Security group rules for Azure](#)
- [Setting up Cloud Manager](#)
- [Launching Cloud Volumes ONTAP in Azure](#)

## **1.4. Setting up Cloud Manager**

You can start creating Cloud Volumes ONTAP systems right after you deploy Cloud Manager. However, you might want to perform additional setup first by setting up the AWS Key Management Service, installing an HTTPS certificate, and more.

### **1.4.1. Adding additional Azure subscriptions to Cloud Manager**

If you want to deploy Cloud Volumes ONTAP systems in multiple Azure subscriptions, then you must add permissions for those subscriptions.

#### *About this task*

The following steps apply if you deployed Cloud Manager from NetApp Cloud Central. When you deployed Cloud Manager, Cloud Central created the OnCommand Cloud Manager Operator role and assigned it to the Cloud Manager virtual machine.

#### *Steps*

1. Log in to the Azure portal.

2. Open the **Subscriptions** service and then select the subscription in which you want to deploy Cloud Volumes ONTAP systems.
3. Click **Access control (IAM)**.
4. Click **Add** and then add the permissions:
  - Select the **OnCommand Cloud Manager Operator** role.
  - Assign access to a **Virtual Machine**.
  - Select the subscription in which the Cloud Manager virtual machine was created.
  - Select the Cloud Manager virtual machine.
  - Click **Save**.
5. Repeat these steps for additional subscriptions.

#### *Result*

When you create a new working environment, you should now have the ability to select from multiple Azure subscriptions.

[Shows the Details and Credentials page in the create new working environment wizard. A link is available to select a different Azure subscription.]

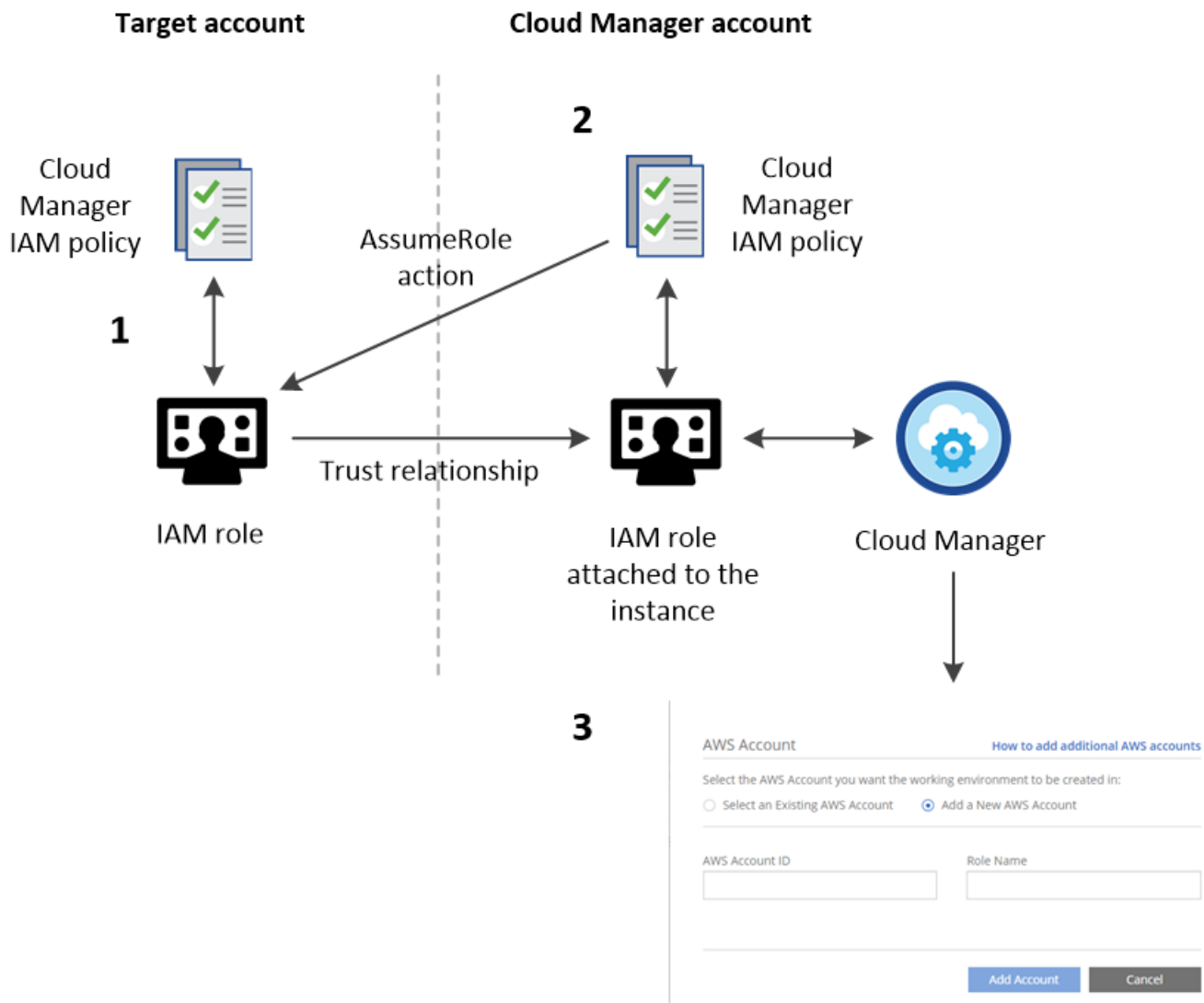
### **1.4.2. Adding additional AWS accounts to Cloud Manager**

When Cloud Manager is associated with an IAM role, it deploys Cloud Volumes ONTAP in the AWS account from which the Cloud Manager instance was created. If you want to deploy Cloud Volumes ONTAP in other AWS accounts, then you must delegate access across accounts.

#### *About this task*

The following image depicts the steps that you must complete below.





### Steps

1. Create an IAM role in the AWS account in which you want to deploy Cloud Volumes ONTAP.

The role must meet the following requirements:

- It must adhere to [Cloud Manager IAM policy requirements](#).
- It must have a trust relationship that allows the IAM role associated with the Cloud Manager instance to assume this new role.

2. Add a permission to the Cloud Manager IAM role policy that enables it to assume the IAM role that you just created.



You can find the name of the Cloud Manager IAM role from the EC2 console by viewing a description of the instance.

3. When you create a new working environment, add the target account in the Details & Credentials page by specifying the AWS account ID of the target account and the name of the IAM role in that account.



As always, you must ensure network connectivity between Cloud Manager and the location of the target Cloud Volumes ONTAP systems. This is important when the instances are created by different accounts.

For additional background about this process, refer to [AWS Documentation: Tutorial: Delegate Access Across AWS Accounts Using IAM Roles](#). In this tutorial, the production account is similar to the target account and the development account is similar to the Cloud Manager account.

*After you finish*

If you have additional accounts, complete these steps for those accounts, as well.

### 1.4.3. Setting up the AWS KMS

If you want to use Amazon encryption with Cloud Volumes ONTAP, then you must set up the AWS Key Management Service (KMS).

*Steps*

1. Ensure that an active CMK exists in your account.

The CMK can be an AWS-managed CMK or a customer-managed CMK.

2. Add the IAM role associated with the Cloud Manager instance to the list of key users for a CMK.

This gives Cloud Manager permissions to use the CMK with Cloud Volumes ONTAP.

### 1.4.4. 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, install a certificate by generating a certificate signing request (CSR) or by installing your own CA-signed certificate:

Option	Description
Generate a CSR	<p>a. Enter the host name or DNS of the Cloud Manager host (its Common Name), and then click <b>Generate CSR</b>.</p> <p>Cloud Manager displays a certificate signing request.</p> <p>b. Use the CSR to submit an SSL certificate request to a CA.</p> <p>The certificate must use the Privacy Enhanced Mail (PEM) Base-64 encoded X.509 format.</p> <p>c. Copy the contents of the signed certificate, paste it in the Certificate field, and then click <b>Install</b>.</p>
Install your own CA-signed certificate	<p>a. Select <b>Install CA-signed certificate</b>.</p> <p>b. Load both the certificate file and the private key and then click <b>Install</b>.</p> <p>The certificate must use the Privacy Enhanced Mail (PEM) Base-64 encoded X.509 format.</p>

#### *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:

[Screen shot: Shows the HTTPS Setup page after you install a signed certificate. The page shows the certificate properties and an option to renew the certificate.]

### 1.4.5. Adding users to Cloud Manager

If additional users need to use your Cloud Manager system, they must sign up for an account in NetApp Cloud Central. You can then add the users to Cloud Manager.

#### *Steps*

1. If the user does not yet have an account in NetApp Cloud Central, send them a link to your Cloud Manager system and have them sign up.

Wait until the user confirms that they have signed up for an account.

2. In Cloud Manager, click the user icon and then click **View Users**.
3. Click **New User**.
4. Enter the email address associated with the user account, select a role, and click **Add**.

#### *After you finish*

Inform the user that they can now log in to the Cloud Manager system.

### 1.4.6. Linking tenants to a NetApp Support Site account

You should link a tenant to a NetApp Support Site account so Cloud Manager can manage licenses for BYOL systems, register pay-as-you-go instances for support, and upgrade Cloud Volumes ONTAP software. For more information about these benefits, [watch this video](#).

#### *Before you begin*

Each NetApp Support Site account that you link to a tenant must meet the following requirements:

- The account must be a NetApp customer-level account (not a guest or temp account).
- If you purchased a secure BYOL subscription, then a *secure* NetApp Support Site account is required to upload the license file.

Contact your NetApp account team for further information about secure BYOL subscriptions.

- The account must be authorized to access the serial numbers of any BYOL systems deployed in the tenant.

If you do not have an account, you can create one from the [NetApp Support Site](#).

#### *Steps*

1. Click the tenants icon and then click **Switch Tenant**.

[Screen shot: Shows the tenant icon (a push pin) and the Switch Tenant button]

2. Click the edit icon for the tenant that you want to link to a NetApp Support Site account.

[Screen shot: Shows the edit icon (a pencil) which is available when hovering over a tenant.]

3. Click **Change NSS account**.
4. Enter the user name and password for the account and click **Save**.

#### *Result*

Cloud Manager registers all existing and future Cloud Volumes ONTAP systems in the tenant with NetApp support.

### 1.4.7. Setting up AWS billing and cost management for Cloud Manager

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

#### *Before you begin*

You must have granted AWS permissions to Cloud Manager so it can access an S3 bucket. For details, see [Granting AWS permissions to Cloud Manager](#).

#### *About this task*

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

### Steps

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

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

2. From the Billing and Cost Management console, go to Preferences and enable the reports:
  - a. Enable **Receive Billing Reports** and specify the S3 bucket.
  - b. Enable **Cost allocation report**.
3. When you set up a user account in Cloud Manager, specify the S3 bucket that you created.



If you grant AWS permissions to Cloud Manager by specifying AWS keys, you must set up a Cloud Manager user account by specifying 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 Cloud Volumes ONTAP instance, go back to Billing and Cost Management **Preferences**, click **Manage report tags**, and enable the **WorkingEnvironmentId** tag.

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

### Result

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

### After you finish

Repeat these steps for other AWS payer accounts for which cost reporting is needed. For details about how to view the cost information, see [Monitoring AWS storage and compute costs](#).

## 1.5. Detailed networking requirements

### 1.5.1. Networking requirements for Cloud Manager

You must set up your networking so that Cloud Manager can deploy Cloud

Volumes ONTAP systems in AWS or in Microsoft Azure. The most important step is ensuring outbound internet access to various endpoints.



If your network uses a proxy server for all communication to the internet, Cloud Manager prompts you to specify the proxy during setup. You can also specify the proxy server from the Settings page. Refer to [Configuring Cloud Manager to use a proxy server](#).

### Connection to target networks

Cloud Manager requires a network connection to the AWS VPCs and Azure VNets in which you want to deploy Cloud Volumes ONTAP.

For example, if you install Cloud Manager in your corporate network, then you must set up a VPN connection to the AWS VPC or Azure VNet in which you launch Cloud Volumes ONTAP.

### Outbound internet access

Cloud Manager requires outbound internet access to deploy and manage Cloud Volumes ONTAP. Outbound internet access is also required when accessing Cloud Manager from your web browser and when running the Cloud Manager installer on a Linux host.

The following sections identify the specific endpoints.

### Outbound internet access to manage Cloud Volumes ONTAP in AWS

Cloud Manager requires outbound internet access to contact the following endpoints when deploying and managing Cloud Volumes ONTAP in AWS:

Endpoints	Purpose
<p>AWS services (amazonaws.com):</p> <ul style="list-style-type: none"><li>• CloudFormation</li><li>• Elastic Compute Cloud (EC2)</li><li>• Key Management Service (KMS)</li><li>• Security Token Service (STS)</li><li>• Simple Storage Service (S3)</li></ul> <p>The exact endpoint depends on the region in which you deploy Cloud Volumes ONTAP. <a href="#">Refer to AWS documentation for details.</a></p>	Enables Cloud Manager to deploy and manage Cloud Volumes ONTAP in AWS.
api.services.cloud.netapp.com:443	API requests to NetApp Cloud Central.
cloud.support.netapp.com.s3.us-west-1.amazonaws.com	Provides access to software images, manifests, and templates.

Endpoints	Purpose
cognito-idp.us-east-1.amazonaws.com cognito-identity.us-east-1.amazonaws.com	Enables Cloud Manager to access and download manifests, templates, and Cloud Volumes ONTAP upgrade images.
kinesis.us-east-1.amazonaws.com	Enables NetApp to stream data from audit records.
https://netapp-cloud-account.auth0.com	Communication with NetApp Cloud Central for centralized user authentication.
https://mysupport.netapp.com	Communication with NetApp AutoSupport.
https://support.netapp.com/svcgw https://support.netapp.com/ServiceGW/entitlement	Communication with NetApp for licensing and support registration.
<p>Various third-party locations, for example:</p> <ul style="list-style-type: none"> <li>• https://repo1.maven.org/maven2</li> <li>• https://oss.sonatype.org/content/repositories</li> <li>• https://repo.typesafe.org</li> </ul> <p>Third-party locations are subject to change.</p>	During upgrades, Cloud Manager downloads the latest packages for third-party dependencies.

### Outbound internet access to manage Cloud Volumes ONTAP in Azure

Cloud Manager requires outbound internet access to contact the following endpoints when deploying and managing Cloud Volumes ONTAP in Microsoft Azure:

Endpoints	Purpose
https://management.azure.com https://login.microsoftonline.com	Enables Cloud Manager to deploy and manage Cloud Volumes ONTAP in most Azure regions.
https://management.microsoftazure.de https://login.microsoftonline.de	Enables Cloud Manager to deploy and manage Cloud Volumes ONTAP in the Azure Germany regions.
https://management.usgovcloudapi.net https://login.microsoftonline.com	Enables Cloud Manager to deploy and manage Cloud Volumes ONTAP in the Azure US Gov regions.
api.services.cloud.netapp.com:443	API requests to NetApp Cloud Central.
cloud.support.netapp.com.s3.us-west-1.amazonaws.com	Provides access to software images, manifests, and templates.
cognito-idp.us-east-1.amazonaws.com cognito-identity.us-east-1.amazonaws.com sts.amazonaws.com	Enables Cloud Manager to access and download manifests, templates, and Cloud Volumes ONTAP upgrade images.

Endpoints	Purpose
kinesis.us-east-1.amazonaws.com	Enables NetApp to stream data from audit records.
https://netapp-cloud-account.auth0.com	Communication with NetApp Cloud Central for centralized user authentication.
https://mysupport.netapp.com	Communication with NetApp AutoSupport.
https://support.netapp.com/svcgw https://support.netapp.com/ServiceGW/entitlement	Communication with NetApp for licensing and support registration.
<p>Various third-party locations, for example:</p> <ul style="list-style-type: none"> <li>• https://repo1.maven.org/maven2</li> <li>• https://oss.sonatype.org/content/repositories</li> <li>• https://repo.typesafe.org</li> </ul> <p>Third-party locations are subject to change.</p>	During upgrades, Cloud Manager downloads the latest packages for third-party dependencies.

### Outbound internet access from your web browser

Users must access Cloud Manager from a web browser. The machine running the web browser must have connections to the following endpoints:

Endpoints	Purpose
The Cloud Manager host	<p>You must enter the host's IP address from a web browser to load the Cloud Manager console.</p> <p>If you deploy Cloud Manager in AWS, the easiest way to provide access is by allocating 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:</p> <ul style="list-style-type: none"> <li>• A jump host in the VPC that has a connection to Cloud Manager</li> <li>• A host in your network that has a VPN connection to the private IP address</li> </ul>
https://auth0.com https://netapp-cloud-account.auth0.com https://services.cloud.netapp.com	Your web browser connects to these endpoints for centralized user authentication through NetApp Cloud Central.



## Outbound internet access to install Cloud Manager on a Linux host

The Cloud Manager installer must access the following URLs during the installation process:

- <http://dev.mysql.com/get/mysql-community-release-el7-5.noarch.rpm>
- <https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm>
- <https://s3.amazonaws.com/aws-cli/awscli-bundle.zip>

## Ports and security groups

- If you deploy Cloud Manager from Cloud Central or from the marketplace images, refer to the following:
  - [Security group rules for Cloud Manager in AWS](#)
  - [Security group rules for Cloud Manager in Azure](#)
- If you install Cloud Manager on an existing Linux host, see [Cloud Manager host requirements](#).

## 1.5.2. Networking requirements for Cloud Volumes ONTAP in AWS

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

Looking for the list of endpoints to which Cloud Manager requires access? They're now maintained in a single location. [Click here for details](#).

## General AWS networking requirements for Cloud Volumes ONTAP

The following requirements must be met in AWS.

### Outbound internet access for Cloud Volumes ONTAP nodes

Cloud Volumes ONTAP nodes require outbound internet access to send messages to NetApp AutoSupport, which proactively monitors the health of your storage.

Routing and firewall policies must allow AWS HTTP/HTTPS traffic to [mysupport.netapp.com](https://mysupport.netapp.com).

If you have a NAT instance, you must define an inbound security group rule that allows HTTPS traffic from the private subnet to the internet.

### Outbound internet access for the HA mediator

The HA mediator instance must have an outbound connection to the AWS EC2 service so it can assist with storage failover. To provide the connection, you can add a public IP address, specify a proxy server, or use a manual option.

The manual option can be a NAT gateway or an interface VPC endpoint from the target subnet to the AWS EC2 service. For details about VPC endpoints, refer to [AWS Documentation: Interface VPC Endpoints \(AWS PrivateLink\)](#).

## Security groups

You do not need to create security groups because Cloud Manager does that for you. If you need to use your own, refer to [Security group rules](#).

## Connection from Cloud Volumes ONTAP to AWS S3 for data tiering

If you want to use EBS as a performance tier and AWS S3 as a capacity tier, you must ensure that Cloud Volumes ONTAP has a connection to S3. The best way to provide that connection is by creating a VPC Endpoint to the S3 service. For instructions, see [AWS Documentation: Creating a Gateway Endpoint](#).

When you create the VPC Endpoint, be sure to select the region, VPC, and route table that corresponds to the Cloud Volumes ONTAP instance. You must also modify the security group to add an outbound HTTPS rule that enables traffic to the S3 endpoint. Otherwise, Cloud Volumes ONTAP cannot connect to the S3 service.

If you experience any issues, see [AWS Support Knowledge Center: Why can't I connect to an S3 bucket using a gateway VPC endpoint?](#).

## Connections to ONTAP systems in other networks

To replicate data between a Cloud Volumes ONTAP system in AWS and ONTAP systems in other networks, you must have a VPN connection between the AWS VPC and the other network—for example, an Azure VNet or your corporate network. For instructions, see [AWS Documentation: Setting Up an AWS VPN Connection](#).

## 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.

For instructions, refer to [AWS Documentation: Active Directory Domain Services on the AWS Cloud Quick Start Reference Deployment](#).

## AWS networking requirements for Cloud Volumes ONTAP HA in multiple AZs

Additional AWS networking requirements apply to Cloud Volumes ONTAP HA configurations that use multiple Availability Zones (AZs). You should review these requirements before you launch an HA pair because you must enter the networking details in Cloud Manager.

To understand how HA pairs work, see [High-availability pairs](#).

## Availability Zones

This HA deployment model uses multiple AZs to ensure high availability of your data. You should use a dedicated AZ for each Cloud Volumes ONTAP instance and the mediator instance, which provides a communication channel between the HA pair.

## Floating IP addresses for NAS data access

Cloud Volumes ONTAP HA configurations in multiple AZs use floating IP addresses for NAS client access from within the VPC. These IP addresses can migrate between nodes when failures occur.

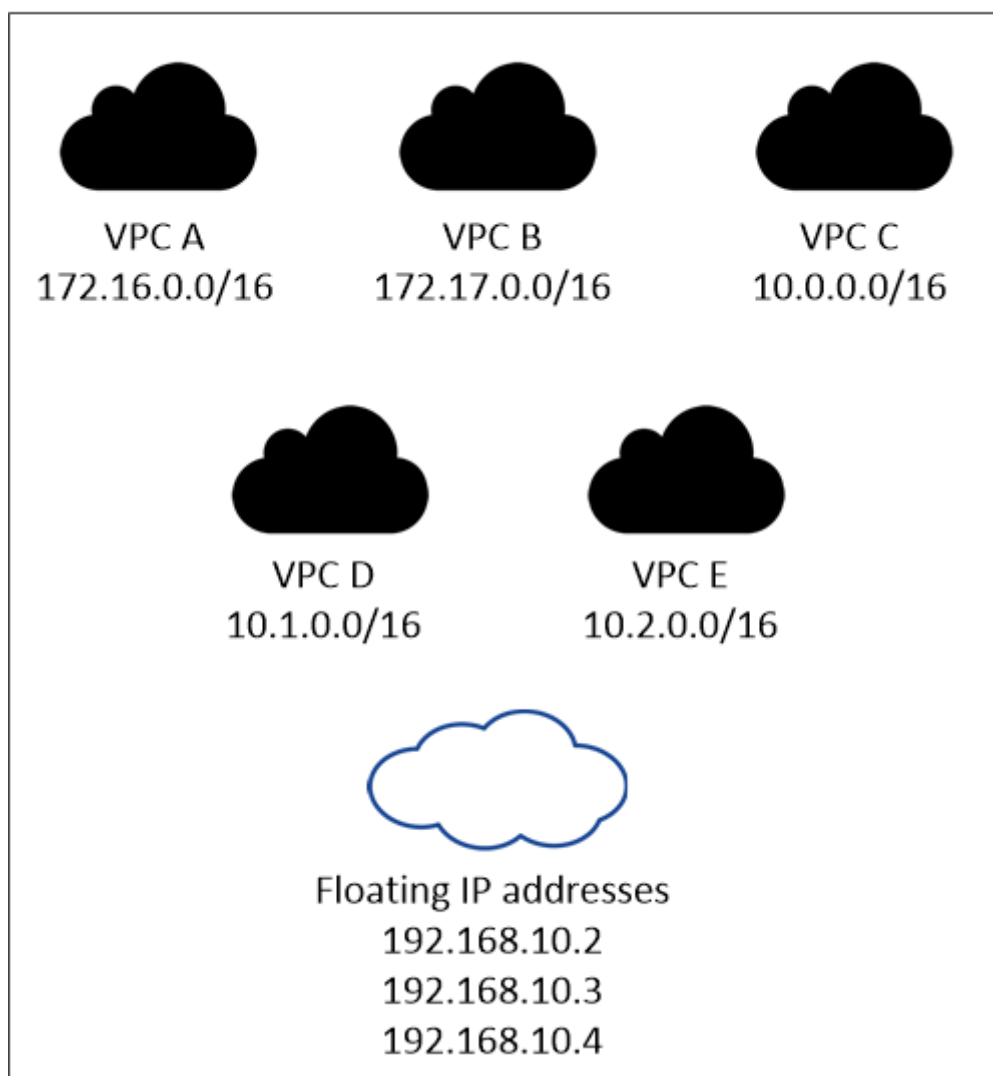
You must specify three floating IP addresses that are outside of the CIDR blocks for all VPCs in the AWS region in which you deploy the HA configuration. You can think of the floating IP addresses as a logical subnet that is outside of the VPCs in your region.



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.

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.

### AWS region



You must manually enter the floating IP addresses in Cloud Manager when you create a Cloud Volumes ONTAP HA working environment. Cloud Manager allocates the IP addresses to the HA pair when it launches the system.



Cloud Manager automatically creates static IP addresses for iSCSI access and for NAS access from clients outside the VPC. You do not need to meet any requirements for these types of IP addresses.

### **Floating IP address for SVM management**

If you use SnapDrive for Windows or SnapCenter with an HA pair, a floating IP address is also required for the SVM management LIF. Cloud Manager prompts you to specify the IP address when you launch the HA pair. If you did not specify the IP address, you can create the SVM Management LIF later. For details, see [Setting up Cloud Volumes ONTAP](#).

### **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 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 when launching the HA pair. Otherwise, some clients might not have access to Cloud Volumes ONTAP.

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.

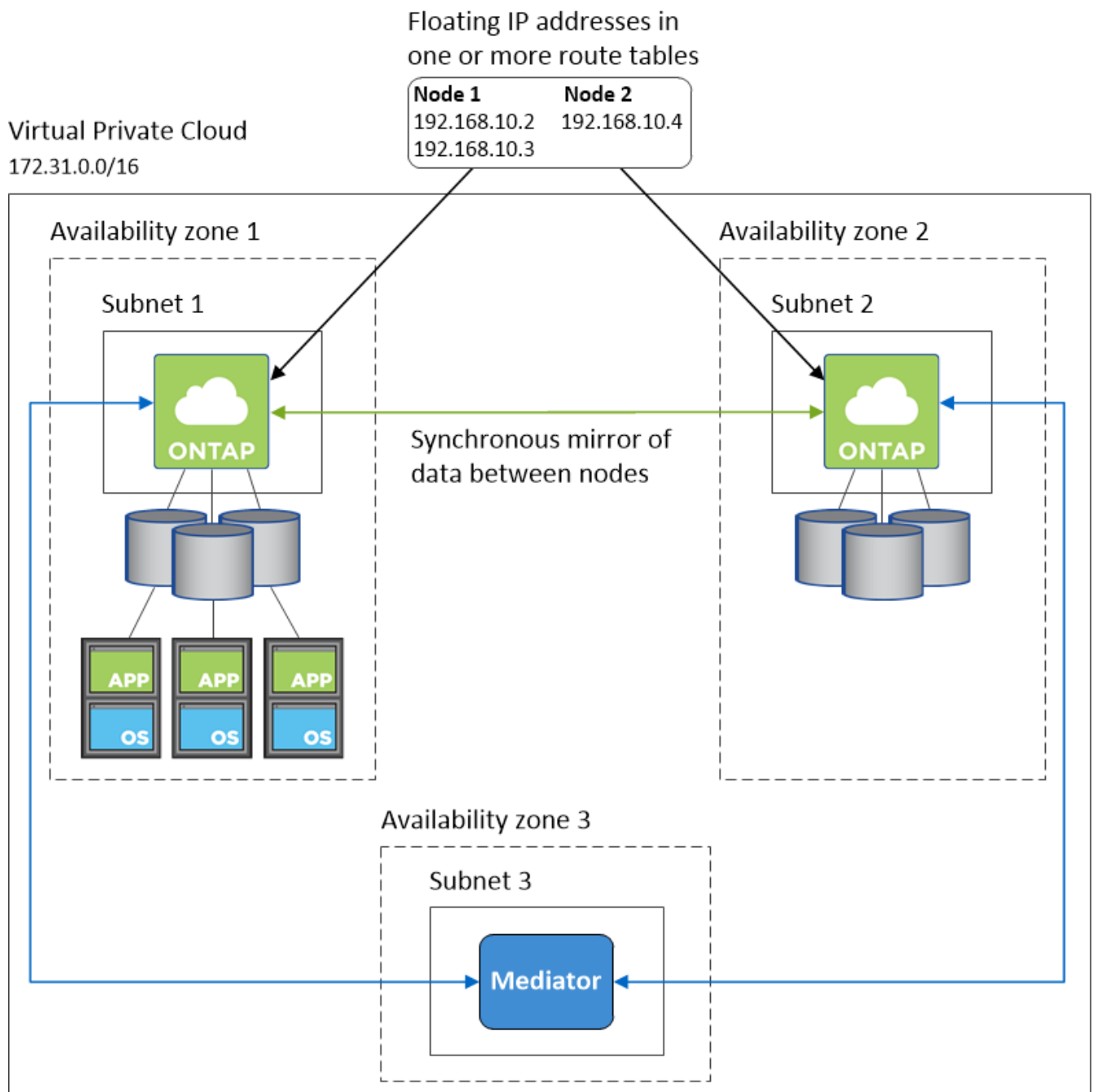
For more information about route tables, refer to [AWS Documentation: Route Tables](#).

### **Connection to NetApp management tools**

When deployed in multiple AZs, Cloud Volumes ONTAP HA configurations use a floating IP address for the cluster management interface, which means external routing is not available. If you want to use NetApp management tools with HA configurations, they must be in the same VPC with similar routing configuration as NAS clients.

### **Example configuration**

The following image shows an optimal HA configuration in AWS operating as an active-passive configuration:



## Sample VPC configurations

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

- 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 Cloud Volumes ONTAP instances in the private

subnet.

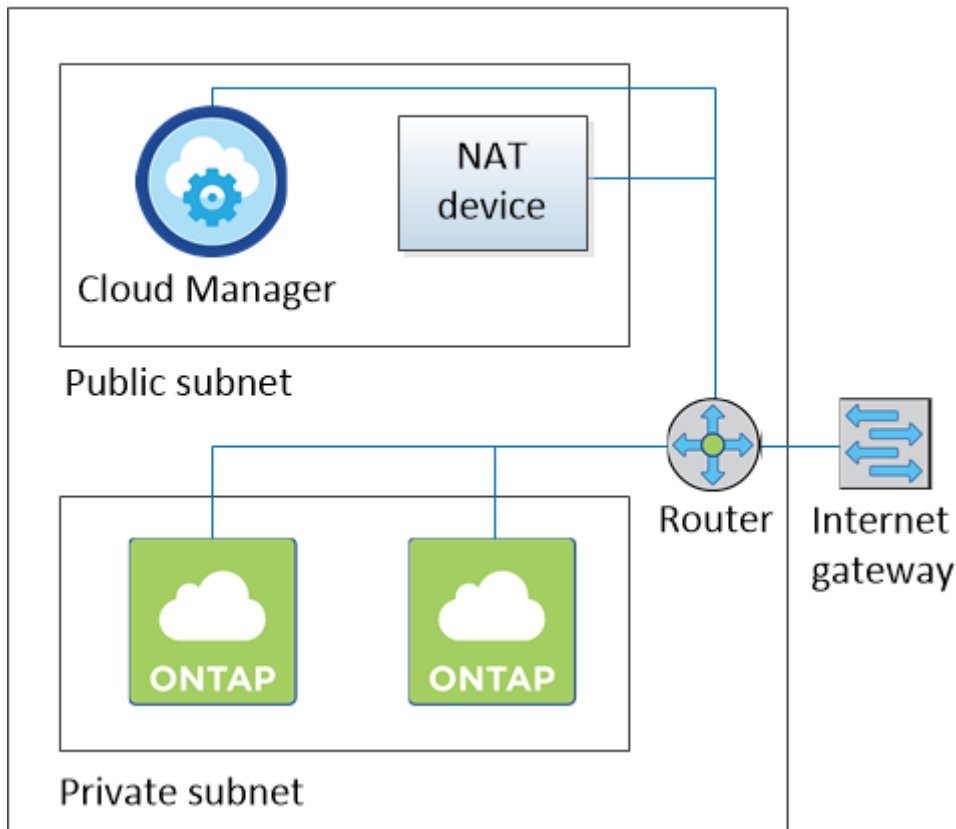


Instead of a NAT device, you can use an HTTP proxy to provide internet connectivity.

For more details about this scenario, refer to [AWS Documentation: Scenario 2: VPC with Public and Private Subnets \(NAT\)](#).

The following graphic shows Cloud Manager running in a public subnet and single node systems running in a private subnet:

### Virtual Private Cloud



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

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

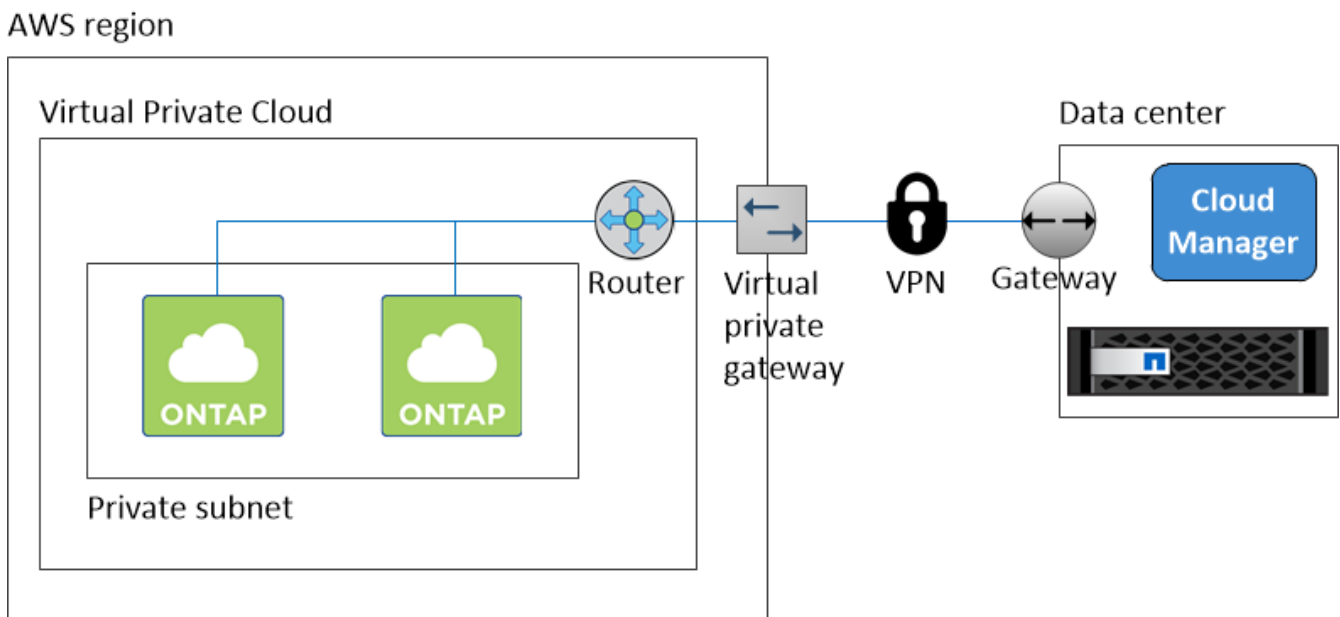


You can also use a proxy server in this configuration to allow internet access. The proxy server can be in your data center or in AWS.

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

For more details about this scenario, refer to [AWS Documentation: Scenario 4: VPC with a Private Subnet Only and AWS Managed VPN Access](#).

The following graphic shows Cloud Manager running in your data center and single node systems running in a private subnet:



### 1.5.3. Networking requirements for Cloud Volumes ONTAP in Azure

You must set up your Azure networking so Cloud Volumes ONTAP systems can operate properly.

Looking for the list of endpoints to which Cloud Manager requires access? They're now maintained in a single location. [Click here for details](#).

#### Outbound internet access for Cloud Volumes ONTAP

Cloud Volumes ONTAP requires outbound internet access to send messages to NetApp AutoSupport, which proactively monitors the health of your storage.

Routing and firewall policies must allow Azure HTTP/HTTPS traffic to [mysupport.netapp.com](#) so Cloud Volumes ONTAP can send AutoSupport messages.

#### Security groups

You do not need to create security groups because Cloud Manager does that for you. If you need to use your own, refer to [Security group rules](#).

#### Connection from Cloud Volumes ONTAP to Azure Blob storage for data tiering

If you want to tier cold data to Azure Blob storage, you do not need to set up a VNet service endpoint as long as Cloud Manager has the required permission:

"Microsoft.Network/virtualNetworks/subnets/write",

That permission is included in the latest Cloud Manager policy. For details about providing permissions, see [Granting Azure permissions](#).

For details about setting up data tiering, see [Tiering cold data to low-cost object storage](#).



If your network configuration uses route tables, then Cloud Manager also requires the following permission: Microsoft.Network/routeTables/join/action

### Connections to ONTAP systems in other networks

To replicate data between a Cloud Volumes ONTAP system in Azure and ONTAP systems in other networks, you must have a VPN connection between the Azure VNet and the other network—for example, an AWS VPC or your corporate network.

For instructions, refer to [Microsoft Azure Documentation: Create a Site-to-Site connection in the Azure portal](#).

## 1.6. Additional deployment options

### 1.6.1. Cloud Manager host requirements

If you install Cloud Manager on your own host, then you must verify support for your configuration, which includes operating system requirements, port requirements, and so on.

#### Supported AWS EC2 instance types

t2.medium or m4.large

#### Supported Azure VM sizes

A2 or D2\_v2

#### Supported operating systems

- CentOS 7.2
- CentOS 7.3
- CentOS 7.4
- Red Hat Enterprise Linux 7.2
- Red Hat Enterprise Linux 7.3
- Red Hat Enterprise Linux 7.4

The Red Hat Enterprise Linux system must be registered with Red Hat Subscription Management. If it is not registered, the system cannot access repositories to update required 3rd party software during Cloud Manager installation.

Cloud Manager is supported on English-language versions of these operating systems.



## Hypervisor

A bare metal or hosted hypervisor that is certified to run CentOS or Red Hat Enterprise Linux

[Red Hat Solution: Which hypervisors are certified to run Red Hat Enterprise Linux?](#)

## CPU

2.27 GHz or higher with two cores

## RAM

4 GB

## Free disk space

50 GB

## Outbound internet access

Outbound internet access is required when installing Cloud Manager and when using Cloud Manager to deploy Cloud Volumes ONTAP. For a list of endpoints, see [Networking requirements for Cloud Manager](#).

## Ports

The following ports must be available:

- 80 for HTTP access
- 443 for HTTPS access
- 3306 for the Cloud Manager database
- 8080 for the Cloud Manager API proxy

If other services are using these ports, Cloud Manager installation fails.



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:

- Modify the security group to allow inbound connections through the ports.
- Specify the port when you enter the URL to the Cloud Manager web console.

### 1.6.2. Installing Cloud Manager on an existing Linux host

If you want to run the Cloud Manager software on an existing host, you can download and install the software on a Linux host in your network or in the cloud.

### *Before you begin*

- A Red Hat Enterprise Linux system must be registered with Red Hat Subscription Management. If it is not registered, the system cannot access repositories to update required 3rd party software during Cloud Manager installation.
- The Cloud Manager installer accesses several URLs during the installation process. You must ensure that outbound internet access is allowed to those endpoints. Refer to [Networking requirements for Cloud Manager](#).

### *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. Review networking requirements:
  - [Networking requirements for Cloud Manager](#)
  - [Networking requirements for Cloud Volumes ONTAP for AWS](#)
  - [Networking requirements for Cloud Volumes ONTAP for Azure](#)
2. Set up permissions for Cloud Manager:
  - a. If you want to deploy Cloud Volumes ONTAP in AWS, [set up an IAM role that includes the required permissions](#).
  - b. If you want to deploy Cloud Volumes ONTAP in Azure, [create and set up a service principal in Azure Active Directory](#).
3. Review [Cloud Manager host requirements](#).
4. Download the software from the [NetApp Support Site](#), and then copy it to the Linux host.

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

5. Assign permissions to execute the script.

### **Example**

```
chmod +x OnCommandCloudManager-V3.5.0.sh
```

6. Run the installation script:

```
./OnCommandCloudManager-V3.5.0.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.

7. 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:

- Modify the security group to allow inbound connections through the ports.
- Specify the port when you enter the URL to the Cloud Manager web console.

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

8. 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 in the public cloud without a public IP address, you must enter a private IP address from a host 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`

9. Sign up for a NetApp Cloud Central account or log in if you already have one.
10. When you sign up or log in, Cloud Manager automatically adds your user account as the administrator for this system.
11. After you log in, enter a name for this Cloud Manager system.

*After you finish*

You can start creating Cloud Volumes ONTAP systems but you might want to perform additional setup first.

### **1.6.3. Launching Cloud Manager from the AWS Marketplace**

It is best to launch Cloud Manager in AWS using [NetApp Cloud Central](#), but you can launch it from the AWS Marketplace, if needed.



If you launch Cloud Manager from the AWS Marketplace, Cloud Manager is still integrated with NetApp Cloud Central. [Learn more about the integration.](#)

### *Before you begin*

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

For details, refer to [AWS Documentation: IP Addressing in Your VPC](#).

### *Steps*

1. Set up an IAM role that includes the required permissions.

#### [Granting permissions when Cloud Manager is not launched from Cloud Central](#)

2. Go to the [Cloud Manager page on the AWS Marketplace](#).
3. Click **Continue**.
4. 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	Steps
You want to associate the instance with an IAM role.	<ol style="list-style-type: none"><li>a. On the Custom Launch tab, click <b>Launch with EC2 Console</b> for your region.</li><li>b. Choose the t2.medium or m4.large instance type.</li><li>c. Select a VPC, subnet, IAM role, and other configuration options that meet your requirements.</li><li>d. Keep the default storage options.</li><li>e. Enter tags for the instance, if desired.</li><li>f. Specify the required connection methods for the Cloud Manager instance: SSH, HTTP, and HTTPS.</li><li>g. Click <b>Launch</b>.</li></ol>
You do not want to associate the instance with an IAM role. You want to specify AWS keys for each Cloud Manager user account.	<ol style="list-style-type: none"><li>a. On the 1-Click Launch tab, specify settings for the instance. Note the following:<ul style="list-style-type: none"><li>◦ The t2.medium and m4.large instance types are supported.</li><li>◦ Under security group, select <b>Create new based on seller settings</b> to create a pre-defined security group that includes the rules required by Cloud Manager.</li></ul></li><li>b. Click <b>Accept Terms and Launch with 1-Click</b>.</li></ol>

### *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 entering the public IP address or private IP address in a web browser and then complete the Setup wizard.

### 1.6.4. Deploying Cloud Manager from the Azure Marketplace

It is best to deploy Cloud Manager in Azure using [NetApp Cloud Central](#), but you can deploy it from the Azure Marketplace, if needed.



If you deploy Cloud Manager from the Azure Marketplace, Cloud Manager is still integrated with NetApp Cloud Central. [Learn more about the integration.](#)

#### Deploying Cloud Manager in Azure

You need to install and set up Cloud Manager so you can use it to launch Cloud Volumes ONTAP in Azure.

##### *Steps*

1. [Go to the Azure Marketplace page for Cloud Manager.](#)
2. Click **Get it now** and then click **Continue**.
3. From the Azure portal, click **Create** and follow the steps to configure the virtual machine.

Note the following as you configure the virtual machine:

- Cloud Manager can perform optimally with either HDD or SSD disks.
- You should choose one of the recommended virtual machine sizes: A2 or D2\_v2.
- For the network security group, it is best to choose **Advanced**.

The **Advanced** option creates a new security group that includes the required inbound rules for Cloud Manager. If you choose Basic, refer to [Security group rules](#) for the list of required rules.

- Under the settings, enable **Managed Service Identity** for Cloud Manager by selecting **Yes**.

This setting is important because a Managed Service Identity allows a Cloud Manager virtual machine to identify itself to Azure Active Directory without providing any credentials. This method is simpler than [manually setting up an Azure service principal and providing the credentials to Cloud Manager](#).

For more information about Managed Service Identities, refer to [Azure documentation](#).

4. On the summary page, review your selections and click **Create** to start the deployment.

Azure deploys the virtual machine with the specified settings. The virtual machine and Cloud Manager software should be running in approximately five minutes.

5. Open a web browser from a host that has a connection to the Cloud Manager virtual machine and enter the following URL:

`http://ipaddress:80`

When you log in, Cloud Manager automatically adds your user account as the administrator for this system.

6. After you log in, enter a name for the Cloud Manager system.

### *Result*

Cloud Manager is now installed and set up. You must grant Azure permissions before users can deploy Cloud Volumes ONTAP in Azure.

## **Granting Azure permissions to Cloud Manager**

When you deployed Cloud Manager in Azure, you should have enabled a Managed Service Identity. You must now grant the required Azure permissions by creating a custom role and then by assigning the role to the Cloud Manager virtual machine for one or more subscriptions.

### *Steps*

1. Create a custom role using the Cloud Manager policy:
  - a. Download the [Cloud Manager Azure policy](#).
  - b. Modify the JSON file by adding Azure subscription IDs to the assignable scope.

You should add the ID for each Azure subscription from which users will create Cloud Volumes ONTAP systems.

### **Example**

```
"AssignableScopes": [  
  "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",  
  "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",  
  "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
```

- c. Use the JSON file to create a custom role in Azure.

The following example shows how to create a custom role using the Azure CLI 2.0:

```
az           role           definition           create           --role-definition  
C:\Policy_for_Cloud_Manager_Azure_3_5_2.json
```

You should now have a custom role called OnCommand Cloud Manager Operator that you can assign to the Cloud Manager virtual machine.

2. Assign the role to the Cloud Manager virtual machine for one or more subscriptions:
  - a. Open the **Subscriptions** service and then select the subscription in which you want to deploy Cloud Volumes ONTAP systems.
  - b. Click **Access control (IAM)**.

c. Click **Add** and then add the permissions:

- Select the **OnCommand Cloud Manager Operator** role.



OnCommand Cloud Manager Operator is the default name provided in the [Cloud Manager policy](#). If you chose a different name for the role, then select that name instead.

- Assign access to a **Virtual Machine**.
- Select the subscription in which the Cloud Manager virtual machine was created.
- Select the Cloud Manager virtual machine.
- Click **Save**.

d. If you want to deploy Cloud Volumes ONTAP from additional subscriptions, switch to that subscription and then repeat these steps.

#### *Result*

Cloud Manager now has the permissions that it needs to deploy and manage Cloud Volumes ONTAP in Azure.

### 1.6.5. Installing Cloud Manager in an Azure US Gov region

To deploy Cloud Manager in an Azure US Gov region, you must download the Cloud Manager installer from the NetApp Support Site and install it on an existing CentOS 7.3 host.

#### *About this task*

For a list of supported Azure US Gov regions, see [Supported Azure regions](#).

#### *Steps*

1. [Review networking requirements for Azure](#).
2. Create a CentOS 7.3 virtual machine from the Azure Marketplace.

While Cloud Manager supports other operating systems, it only supports CentOS 7.3 in the Azure US Gov regions.

3. [Download and install Cloud Manager](#).
4. [Grant Azure permissions to Cloud Manager using a service principal and credentials](#).



Managed Service Identities are not supported in the US Gov regions.

#### *After you finish*

Cloud Manager is now ready to deploy Cloud Volumes ONTAP in an Azure US Gov region, just like any other region. However, you might want to perform additional setup first.

### 1.6.6. Installing Cloud Manager in an Azure Germany region

The Azure Marketplace is not available in the Azure Germany regions, so you must download the Cloud Manager installer from the NetApp Support Site and install it on an existing Linux host in the region.

#### *Steps*

1. [Review networking requirements for Azure.](#)
2. [Review Cloud Manager host requirements.](#)
3. [Download and install Cloud Manager.](#)
4. [Grant Azure permissions to Cloud Manager using a service principal and credentials.](#)



Managed Service Identities are not supported in the Azure Germany regions.

#### *After you finish*

Cloud Manager is now ready to deploy Cloud Volumes ONTAP in the Azure Germany region, just like any other region. However, you might want to perform additional setup first.

## 1.7. Additional ways to provide permissions

### 1.7.1. Granting permissions when Cloud Manager is not launched from Cloud Central

If you cannot launch Cloud Manager in AWS from [NetApp Cloud Central](#), then you must provide Cloud Manager with the permissions that it needs if you want to launch and manage Cloud Volumes ONTAP in AWS.

#### *About this task*

The Cloud Manager IAM policy defines the AWS actions and resources that Cloud Manager is allowed to use. You can grant the permissions defined in the IAM policy in one of two ways:

- You can attach an IAM role to the Cloud Manager instance in AWS.
- You can attach the IAM policy to IAM users or groups.

You would then specify the AWS access keys for those users in Cloud Manager.

#### *Steps*

1. Download the Cloud Manager IAM policy from the following location:

[NetApp OnCommand Cloud Manager: AWS and Azure Policies](#)

2. From the IAM console, create your own policy by copying and pasting the text from the Cloud Manager IAM policy.
3. Grant permissions to the Cloud Manager instance or to IAM users:



Option	Description
Grant permissions to the Cloud Manager instance	<ol style="list-style-type: none"> <li>Create an IAM role with the role type Amazon EC2 and attach the policy that you created in the previous step to the role.</li> <li>Attach the IAM role to Cloud Manager when you launch it from the AWS Marketplace (choose <b>Custom Launch</b>) or by modifying an existing instance from the EC2 console.</li> </ol>
Grant permissions to IAM users	Attach the policy to IAM users or groups. For instructions, refer to <a href="#">AWS Documentation: Managing IAM Policies</a> .

### *Result*

Cloud Manager now has the permissions that it needs. If you attached the policy to IAM users, you must specify the AWS access keys for those IAM users when you set up user accounts in Cloud Manager.

## **1.7.2. Granting Azure permissions to Cloud Manager using a service principal and credentials**

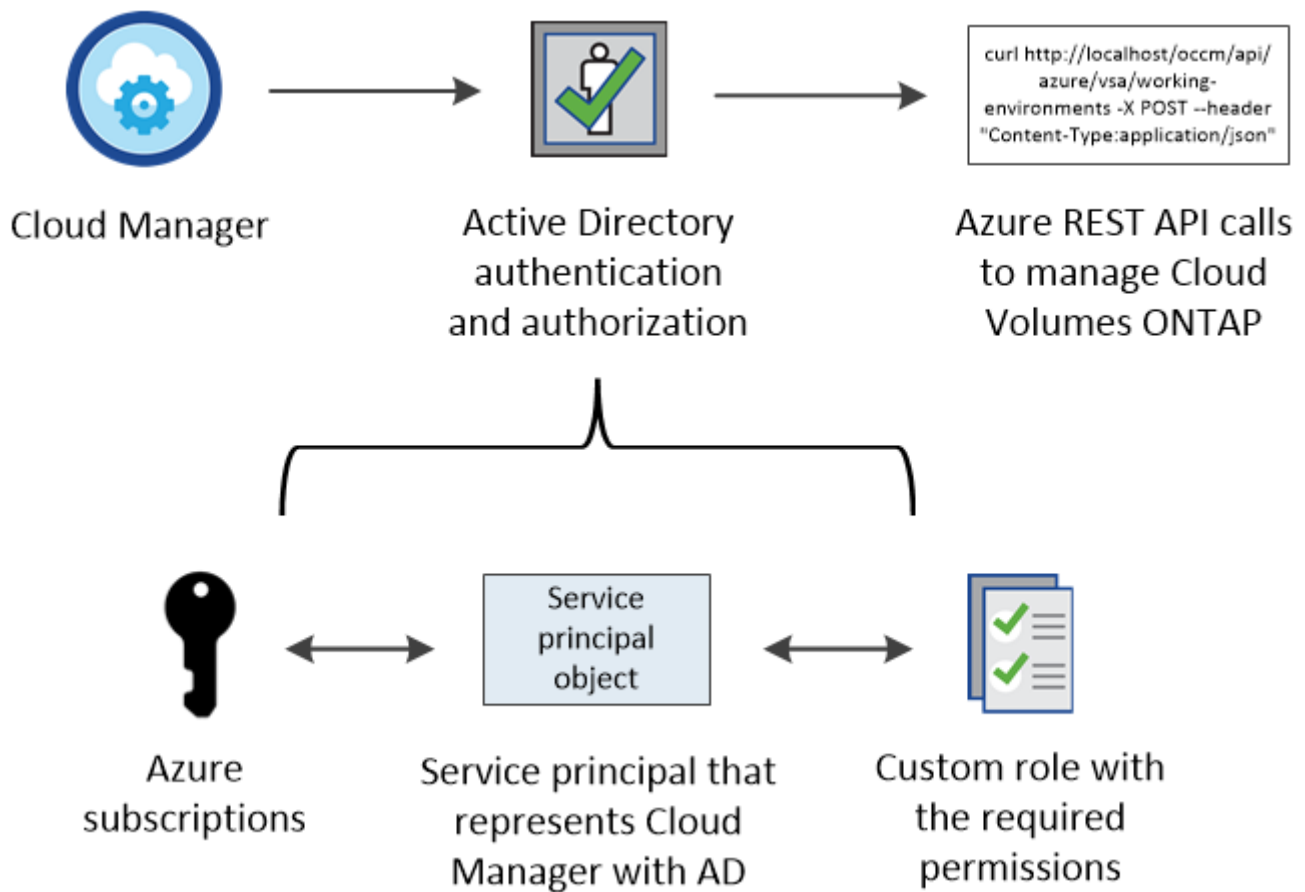
Cloud Manager needs permissions to perform actions in Azure. You can grant the required permissions by creating and setting up a service principal in Azure Active Directory and by obtaining the Azure credentials that Cloud Manager needs.

### *Before you begin*

Using a service principal and credentials is an alternative to using a Managed Service Identity, which is simpler and does not require credentials. To use a Managed Service Identity with Cloud Manager instead, follow [instructions for new Cloud Manager virtual machines](#) or [instructions for existing Cloud Manager virtual machines](#).

### *About this task*

The following image depicts how Cloud Manager obtains permissions to perform operations in Azure. A service principal object, which is tied to one or more Azure subscriptions, represents Cloud Manager in Azure Active Directory and is assigned to a custom role that allows the required permissions.



The following steps use the new Azure portal. If you experience any issues, you should use the Azure classic portal.

#### Steps

1. [Create a custom role with the required Cloud Manager permissions.](#)
2. [Create an Active Directory service principal.](#)
3. [Assign the custom Cloud Manager Operator role to the service principal.](#)

### Creating a custom role with the required Cloud Manager permissions

A custom role is required to provide Cloud Manager with the permissions that it needs to launch and manage Cloud Volumes ONTAP in Azure.

#### Steps

1. Download the [Cloud Manager Azure policy](#).
2. Modify the JSON file by adding Azure subscription IDs to the assignable scope.

You should add the ID for each Azure subscription from which users will create Cloud Volumes ONTAP systems.

#### Example

```
"AssignableScopes": [  
  "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",  
  "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
```

"/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"

3. Use the JSON file to create a custom role in Azure.

The following example shows how to create a custom role using the Azure CLI 2.0:

```
az role definition create --role-definition C:\Policy_for_Cloud_Manager_Azure_3_5_2.json
```

### Result

You should now have a custom role called OnCommand Cloud Manager Operator.

## Creating an Active Directory service principal

You must create an Active Directory service principal so Cloud Manager can authenticate with Azure Active Directory.

## Before you begin

You must have the appropriate permissions in Azure to create an Active Directory application and to assign the application to a role. For details, refer to [Microsoft Azure Documentation: Use portal to create Active Directory application and service principal that can access resources](#)

### Steps

1. From the Azure portal, open the **Azure Active Directory** service.

[Shows the Active Directory service in Microsoft Azure.]

2. In the menu, click **App registrations**.
3. Create the service principal:
  - a. Click **New application registration**.
  - b. Enter a name for the application, keep **Web app / API** selected, and then enter any URL—for example, <http://url>
  - c. Click **Create**.
4. Modify the application to add the required permissions:
  - a. Select the created application.
  - b. Under Settings, click **Required permissions** and then click **Add**.

[Shows the settings for an Active Directory application in Microsoft Azure and highlights the option to add required permissions for API access.]

- c. Click **Select an API**, select **Windows Azure Service Management API**, and then click **Select**.

[Shows the API to select in Microsoft Azure when adding API access to the Active Directory application. The API is the Windows Azure Service Management API.]

- d. Click **Access Azure Service Management as organization users**, click **Select** and then click **Done**.

5. Create a key for the service principal:

- a. Under Settings, click **Keys**.
- b. Enter a description, select a duration, and then click **Save**.
- c. Copy the key value.

You need to enter the key value in Cloud Manager when you create user accounts for this subscription.

- d. Click **Properties** and then copy the application ID for the service principal.

Similar to the key value, you need to enter the application ID in Cloud Manager when you create user accounts for this subscription.

[Shows the application ID for an Azure Active Directory service principal.]

6. Obtain the Active Directory tenant ID for your organization:

- a. In the Active Directory menu, click **Properties**.
- b. Copy the Directory ID.

[Shows the Active Directory properties in the Azure portal and the Directory ID that you need to copy.]

Just like the application ID and application key, you must enter the Active Directory tenant ID when you create Cloud Manager user accounts.

### *Result*

You should now have an Active Directory service principal and you should have copied the application ID, the application key, and the Active Directory tenant ID. You need to enter this information in Cloud Manager when you set up user accounts.

## **Assigning the Cloud Manager Operator role to the service principal**

You must bind the service principal to one or more Azure subscriptions and assign it the Cloud Manager Operator role so Cloud Manager has permissions in Azure.

### *About this task*

If you want to deploy Cloud Volumes ONTAP from multiple Azure subscriptions, then you must bind the service principal to each of those subscriptions. Cloud Manager enables you to select the subscription that you want to use when deploying Cloud Volumes ONTAP.

### *Steps*

1. From the Azure portal, select **Subscriptions** in the left pane.
2. Select the subscription.
3. Click **Access control (IAM)** and then click **Add**.
4. Select the **OnCommand Cloud Manager Operator** role.
5. Search for the name of the application (you cannot find it in the list by scrolling).

6. Select the application, click **Select**, and then click **OK**.

#### *Result*

The service principal for Cloud Manager now has the required Azure permissions.

### 1.7.3. Providing Azure permissions to an existing Cloud Manager virtual machine using a Managed Service Identity

You can provide Azure permissions to Cloud Manager by using a Managed Service Identity. A Managed Service Identity allows the Cloud Manager virtual machine to identify itself to Azure Active Directory without providing any credentials.



Managed Service Identities are not supported in the Azure US Gov regions and in the Germany regions. You must [grant Azure permissions to Cloud Manager using a service principal and credentials](#).

#### *About this task*

If you currently provide Cloud Manager with Azure permissions through a service principal, you can change to using a Managed Service Identity instead. This method is simpler than manually setting up an Azure service principal and providing the credentials to Cloud Manager.

For more information about Managed Service Identities, refer to [Azure documentation](#).

#### *Steps*

1. Log in to the Azure portal using an account that is associated with the Cloud Manager virtual machine.
2. Enable a Managed Service Identity on the virtual machine:
  - a. Navigate to the virtual machine.
  - b. Under Settings, select **Configuration**.
  - c. Click **Yes** next to Managed Service Identity and then click **Save**.
3. Provide permissions to the Cloud Manager virtual machine for one or more subscriptions:
  - a. Open the **Subscriptions** service and then select the subscription in which you want to deploy Cloud Volumes ONTAP systems.
  - b. Click **Access control (IAM)**.
  - c. Click **Add** and then add the permissions:
    - Select the **OnCommand Cloud Manager Operator** role.



OnCommand Cloud Manager Operator is the default name provided in the [Cloud Manager policy](#). If you chose a different name for the role, then select that name instead.

If you have not yet created this role, follow [these instructions](#).

- Assign access to a **Virtual Machine**.
  - Select the subscription in which the Cloud Manager virtual machine was created.
  - Select the Cloud Manager virtual machine.
  - Click **Save**.
- d. If you want to deploy Cloud Volumes ONTAP from additional subscriptions, click **Subscriptions** again, select a subscription, and then repeat the steps for that subscription.

#### *Result*

Cloud Manager now has permissions that are controlled by a Managed Service Identity. If you repeated the steps for several subscriptions, then you can choose a different subscription when creating a new working environment.

[Screen shot: Shows the link to select a different subscription in the Details and Credentials page.]