



Getting started

Cloud Manager 3.6

NetApp
October 27, 2021

This PDF was generated from https://docs.netapp.com/us-en/occm36/reference_deployment_overview.html on October 27, 2021. Always check docs.netapp.com for the latest.

Table of Contents

- Getting started 1
- Deployment overview 1
- Getting started with Cloud Volumes ONTAP in AWS 2
- Getting started with Cloud Volumes ONTAP in Azure 3
- Setting up Cloud Manager 4
- Networking requirements 19
- Additional deployment options 32

Getting started

Deployment overview

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

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:

Location	How to deploy Cloud Manager
AWS	Deploy Cloud Manager from NetApp Cloud Central
AWS C2S	Deploy Cloud Manager from the AWS Intelligence Community Marketplace
Azure generally available region	Deploy Cloud Manager from NetApp Cloud Central
Azure Government	Deploy Cloud Manager from the Azure US Government Marketplace
Azure Germany	Download and install the software on a Linux host
IBM Cloud	Download and install the software on a Linux host
On-premises network	Download and install the software on a Linux host

Cloud Manager setup

You might want to perform additional setup after you install Cloud Manager, such as adding additional cloud provider accounts, installing an HTTPS certificate, and more.

- [Adding Cloud Provider Accounts to Cloud Manager](#)
- [Installing an HTTPS certificate](#)
- [Setting up users and tenants](#)
- [Setting up the AWS KMS](#)

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 9.5](#)
- [Planning your configuration](#)
- [Launching Cloud Volumes ONTAP in AWS](#)
- [Launching Cloud Volumes ONTAP in Azure](#)

Getting started with Cloud Volumes ONTAP in AWS

You can get started with Cloud Volumes ONTAP in AWS from NetApp Cloud Central.



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 Cloud Central policy for AWS](#).
- 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](#).

5

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.

Related links

- [Evaluating](#)
- [Networking requirements for Cloud Manager](#)
- [Networking requirements for Cloud Volumes ONTAP in AWS](#)
- [Security group rules for AWS](#)
- [Adding Cloud Provider Accounts to Cloud Manager](#)
- [What Cloud Manager does with AWS permissions](#)
- [Launching Cloud Volumes ONTAP in AWS](#)
- [Launching Cloud Manager from the AWS Marketplace](#)

Getting started with Cloud Volumes ONTAP in Azure

You can get started with Cloud Volumes ONTAP in Azure from NetApp Cloud Central. Separate instructions are available to deploy Cloud Manager in [Azure US Government regions](#) and in [Azure Germany regions](#).

1

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](#).

2

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 Cloud Central policy for Azure](#).
- 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.

Related links

- [Evaluating](#)
- [Networking requirements for Cloud Manager](#)
- [Networking requirements for Cloud Volumes ONTAP in Azure](#)
- [Security group rules for Azure](#)
- [Adding Cloud Provider Accounts to Cloud Manager](#)
- [What Cloud Manager does with Azure permissions](#)
- [Launching Cloud Volumes ONTAP in Azure](#)
- [Launching Cloud Manager from the Azure Marketplace](#)

Setting up Cloud Manager

Adding cloud provider accounts to Cloud Manager

If you want to deploy Cloud Volumes ONTAP in different cloud accounts, then you need to provide the required permissions to those accounts and then add the details to Cloud Manager.

When you deploy Cloud Manager from Cloud Central, Cloud Manager automatically adds a [cloud provider account](#) for the account in which you deployed Cloud Manager. An initial cloud provider account is not added if you manually installed the Cloud Manager software on an existing system.

Setting up and adding AWS accounts to Cloud Manager

If you want to deploy Cloud Volumes ONTAP in different AWS accounts, then you need to provide the required permissions to those accounts and then add the details to Cloud Manager. How you provide the permissions depends on whether you want to provide Cloud Manager with AWS keys or the ARN of a role in a trusted account.

- [Granting permissions when providing AWS keys](#)
- [Granting permissions by assuming IAM roles in other accounts](#)

Granting permissions when providing AWS keys

If you want to provide Cloud Manager with AWS keys for an IAM user, then you need to grant the required

permissions to that user. The Cloud Manager IAM policy defines the AWS actions and resources that Cloud Manager is allowed to use.

Steps

1. Download the Cloud Manager IAM policy from the [Cloud Manager Policies page](#).
2. From the IAM console, create your own policy by copying and pasting the text from the Cloud Manager IAM policy.

[AWS Documentation: Creating IAM Policies](#)

3. Attach the policy to an IAM role or an IAM user.
 - [AWS Documentation: Creating IAM Roles](#)
 - [AWS Documentation: Adding and Removing IAM Policies](#)

Result

The account now has the required permissions. [You can now add it to Cloud Manager](#).

Granting permissions by assuming IAM roles in other accounts

You can set up a trust relationship between the source AWS account in which you deployed the Cloud Manager instance and other AWS accounts by using IAM roles. You would then provide Cloud Manager with the ARN of the IAM roles from the trusted accounts.

Steps

1. Go to the target account where you want to deploy Cloud Volumes ONTAP and create an IAM role by selecting **Another AWS account**.

Be sure to do the following:

- Enter the ID of the account where the Cloud Manager instance resides.
- Attach the Cloud Manager IAM policy, which is available from the [Cloud Manager Policies page](#).

2. Go to the source account where the Cloud Manager instance resides and select the IAM role that is attached to the instance.
 - a. Click **Trust Relationships > Edit trust relationship**.
 - b. Add the "sts:AssumeRole" action and the ARN of the role that you created in the target account.

Example

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "sts:AssumeRole",
    "Resource": "arn:aws:iam::ACCOUNT-B-ID:role/ACCOUNT-B-ROLENAME"
  }
}
```

Result

The account now has the required permissions. [You can now add it to Cloud Manager.](#)

Adding AWS accounts to Cloud Manager

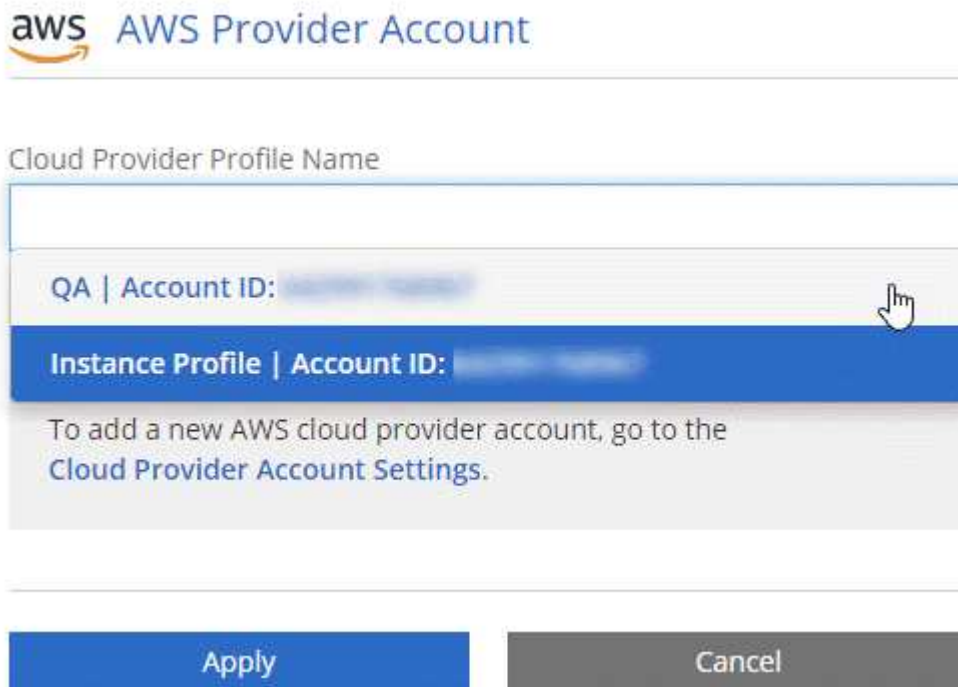
After you provide an AWS account with the required permissions, you can add the account to Cloud Manager. This enables you to launch Cloud Volumes ONTAP systems in that account.

Steps

1. In the upper right of the Cloud Manager console, click the task drop-down list, and then select **Account Settings**.
2. Click **Add New Account** and select **AWS**.
3. Choose whether you want to provide AWS keys or the ARN of a trusted IAM role.
4. Confirm that the policy requirements have been met and then click **Create Account**.

Result

You can now switch to another account from the Details and Credentials page when creating a new working environment:



Setting up and adding Azure accounts to Cloud Manager

If you want to deploy Cloud Volumes ONTAP in different Azure accounts, then you need to provide the required permissions to those accounts and then add details about the accounts to Cloud Manager.

- [Granting Azure permissions using a service principal](#)
- [Adding Azure accounts to Cloud Manager](#)

Granting Azure permissions using a service principal

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

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_3.6.1.json
```

Result

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

Creating an Active Directory service principal

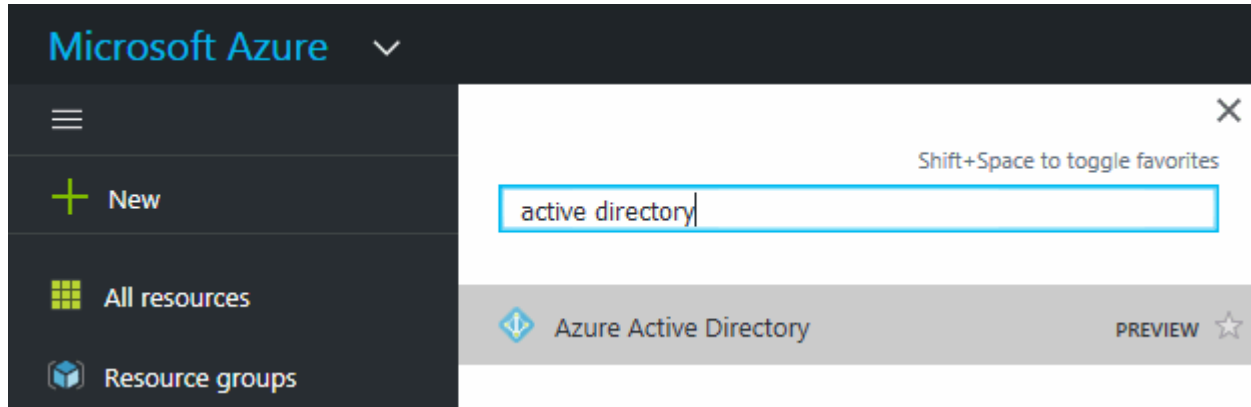
You must create an Active Directory service principal so Cloud Manager can authenticate with Azure Active Directory.

Before you begin

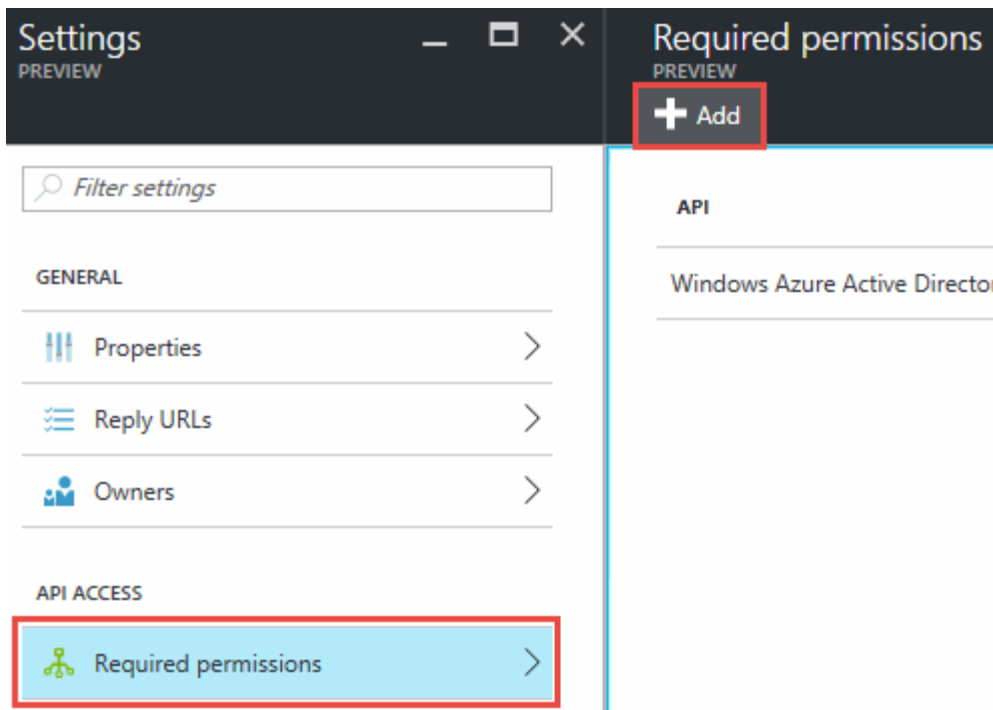
You must have the appropriate permissions in Azure to create an Active Directory application and to assign the application to a role. For details, refer to [Microsoft Azure Documentation: Use portal to create Active Directory application and service principal that can access resources](#).

Steps

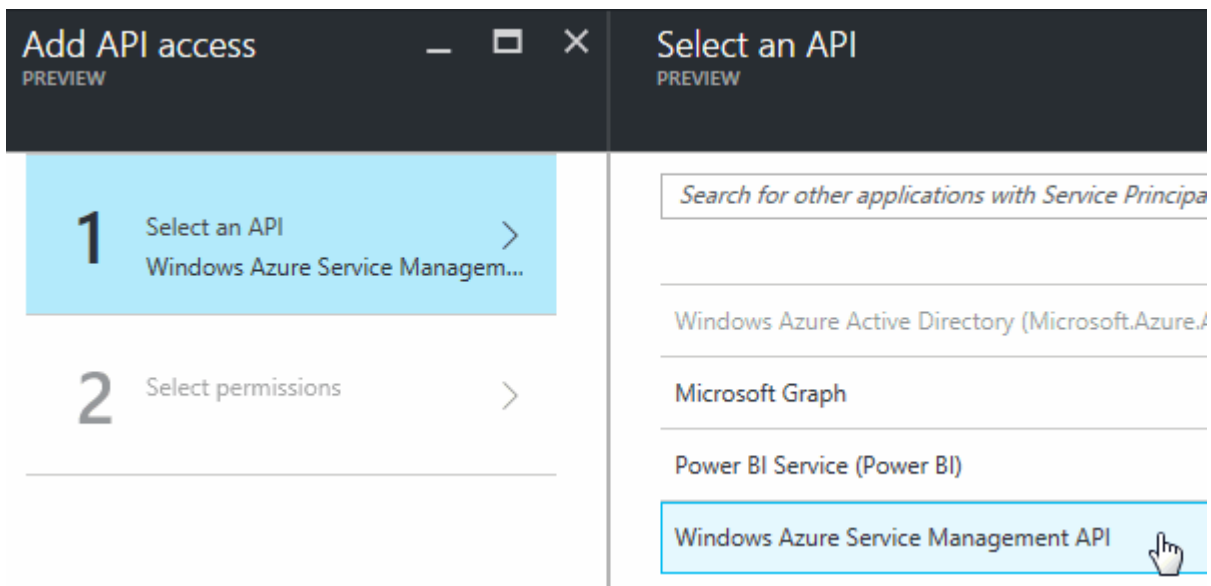
1. From the Azure portal, open the **Azure Active Directory** service.



2. In the menu, click **App registrations (Legacy)**.
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**.



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



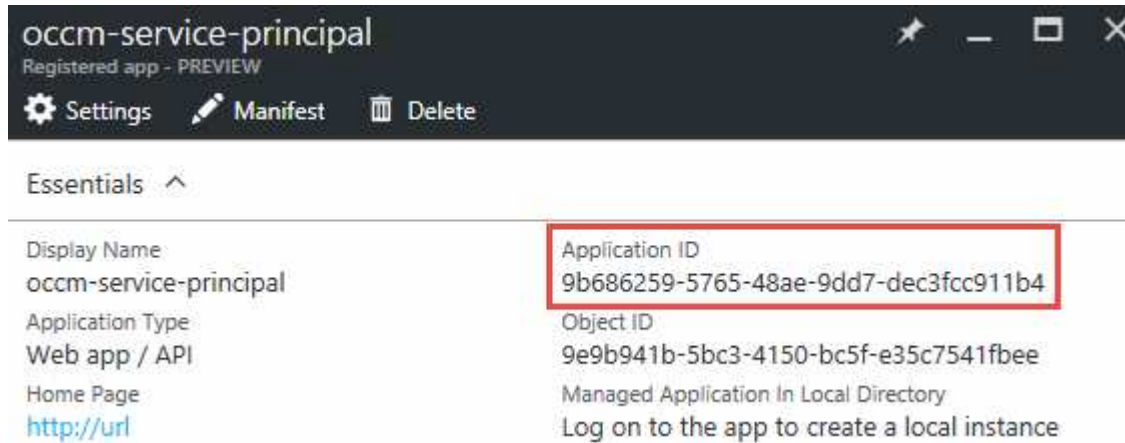
- d. Click **Access Azure Service Management as organization users**, click **Select** and then click **Done**.
5. Create a key for the service principal:
- a. Under Settings, click **Keys**.
 - b. Enter a description, select a duration, and then click **Save**.
 - c. Copy the key value.

You need to enter the key value when you add a cloud provider account to Cloud Manager.

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

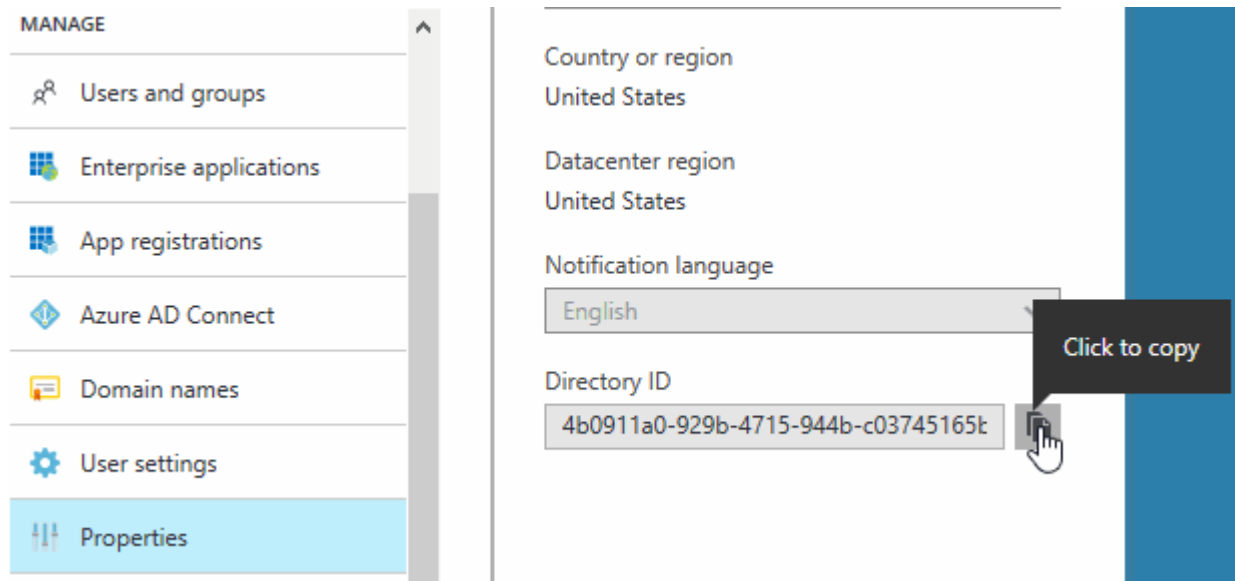
Similar to the key value, you need to enter the application ID in Cloud Manager when you add a cloud

provider account to Cloud Manager.



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

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



Just like the application ID and application key, you must enter the Active Directory tenant ID when you add a cloud provider account to Cloud Manager.

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 add a cloud provider account.

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.

Adding Azure accounts to Cloud Manager

After you provide an Azure account with the required permissions, you can add the account to Cloud Manager. This enables you to launch Cloud Volumes ONTAP systems in that account.

Steps

1. In the upper right of the Cloud Manager console, click the task drop-down list, and then select **Account Settings**.
2. Click **Add New Account** and select **Microsoft Azure**.
3. Enter information about the Azure Active Directory service principal that grants the required permissions.
4. Confirm that the policy requirements have been met and then click **Create Account**.

Result

You can now switch to another account from the Details and Credentials page when creating a new working environment:



Cloud Provider Profile Name

Azure Keys | Application ID: ...
Dev Keys | Application ID: ...
Managed Service Identity

To add a new Azure cloud provider account, go to the [Cloud Provider Account Settings](#).

Apply

Cancel

Associating additional Azure subscriptions with a managed identity

Cloud Manager enables you to choose the Azure account and subscription in which you want to deploy Cloud Volumes ONTAP. You can't select a different Azure subscription for the managed identity profile unless you associate the [managed identity](#) with those subscriptions.

About this task

A managed identity is the initial [cloud provider account](#) when you deploy 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)**.
 - a. Click **Add > Add role assignment** 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**.

4. 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 for the managed identity profile.

Microsoft Azure Provider Account

Cloud Provider Profile Name
Managed Service Identity

Azure Subscription

OCCM Dev

OCCM QA1 (Default)

To add a new Azure cloud provider account, go to the [Cloud Provider Account Settings](#).

Apply Cancel

Adding NetApp Support Site accounts to Cloud Manager

Adding your NetApp Support Site account to Cloud Manager is required to deploy a BYOL system. It's also required to register pay-as-you-go systems and to upgrade ONTAP software.

Watch the following video to learn how to add NetApp Support Site accounts to Cloud Manager. Or scroll down to read the steps.



Steps

1. If you don't have a NetApp Support Site account yet, [register for one](#).
2. In the upper right of the Cloud Manager console, click the task drop-down list, and then select **Account Settings**.
3. Click **Add New Account** and select **NetApp Support Site**.
4. Specify a name for the account and then enter the user name and password.
 - The account must be a customer-level account (not a guest or temp account).
 - If you plan to deploy BYOL systems:
 - The account must be authorized to access the serial numbers of the BYOL systems.
 - If you purchased a secure BYOL subscription, then a secure NSS account is required.
5. Click **Create Account**.

What's next?

Users can now select the account when creating new Cloud Volumes ONTAP systems and when registering existing systems.

- [Launching Cloud Volumes ONTAP in AWS](#)
- [Launching Cloud Volumes ONTAP in Azure](#)
- [Registering pay-as-you-go systems](#)
- [Learn how Cloud Manager manages license files](#)

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	<ol style="list-style-type: none">a. 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.b. 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.c. Copy the contents of the signed certificate, paste it in the Certificate field, and then click Install.
Install your own CA-signed certificate	<ol style="list-style-type: none">a. Select Install CA-signed certificate.b. Load both the certificate file and the private key and then click Install. The certificate must use the Privacy Enhanced Mail (PEM) Base-64 encoded X.509 format.

Result

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

Cloud Manager HTTPS certificate

Expiration:

 Oct 27, 2016 05:13:28 am

Issuer:

CN=localhost, O=NetApp, OU=Tel-Aviv,
EMAILADDRESS=admin@example.com

Subject:

EMAILADDRESS=admin@example.com,
OU=Tel-Aviv, O=NetApp, CN=localhost

 [View Certificate](#)

 [Renew HTTPS Certificate](#)

Setting up users and tenants

Cloud Manager enables you to add additional Cloud Central users to Cloud Manager and to isolate working environments by using tenants.

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**.

What's next?

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

Creating tenants

Tenants enable you to isolate your working environments into separate groups. You create one or more working environments within a tenant. [Learn more about tenants](#).

Steps

1. Click the tenants icon and then click **Add Tenant**.
2. Enter a name, description, and cost center, if needed.
3. Click **Save**.

What's next?

You can now switch to this new tenant and add Tenant Admins and Working Environment Admins to this tenant.

Setting up the AWS KMS

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

Steps

1. Ensure that an active Customer Master Key (CMK) exists.

The CMK can be an AWS-managed CMK or a customer-managed CMK. It can be in the same AWS account as Cloud Manager and Cloud Volumes ONTAP or in a different AWS account.

[AWS Documentation: Customer Master Keys \(CMKs\)](#)

2. Modify the key policy for each CMK by adding the IAM role that provides permissions to Cloud Manager as a *key user*.

Adding the IAM role as a key user gives Cloud Manager permissions to use the CMK with Cloud Volumes ONTAP.

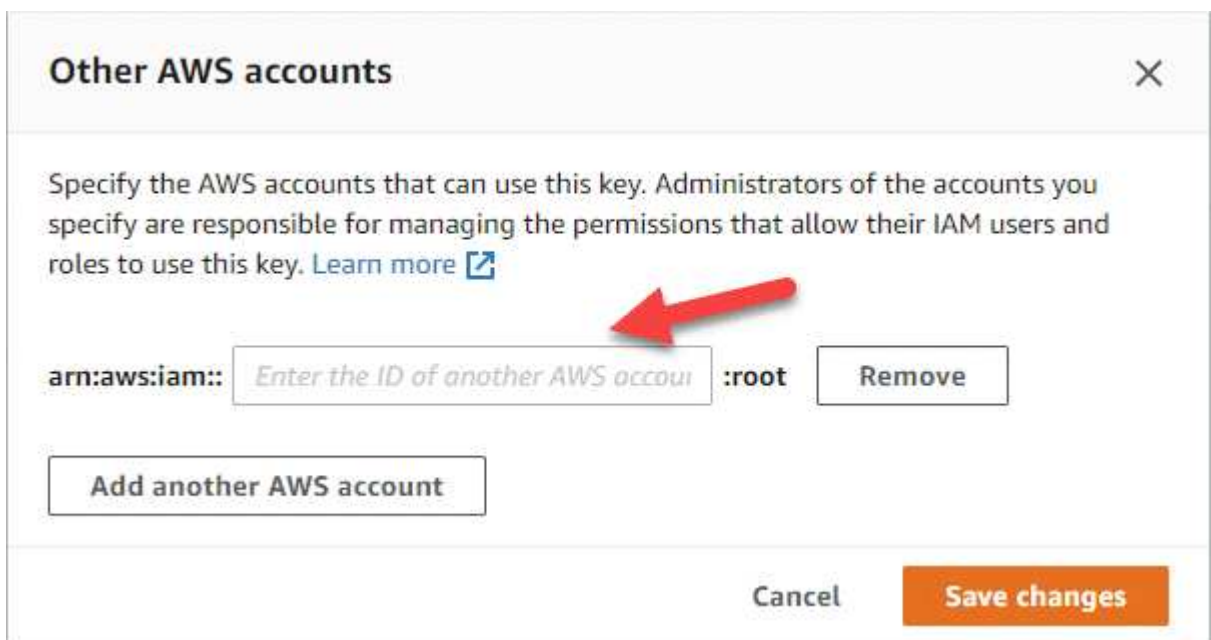
[AWS Documentation: Editing Keys](#)

3. If the CMK is in a different AWS account, complete the following steps:
 - a. Go to the KMS console from the account where the CMK resides.
 - b. Select the key.
 - c. In the **General configuration** pane, copy the ARN of the key.

You'll need to provide the ARN to Cloud Manager when you create the Cloud Volumes ONTAP system.

- d. In the **Other AWS accounts** pane, add the AWS account that provides Cloud Manager with permissions.

In most cases, this is the account where Cloud Manager resides. If Cloud Manager wasn't installed in AWS, it would be the account for which you provided AWS access keys to Cloud Manager.



- e. Now switch to the AWS account that provides Cloud Manager with permissions and open the IAM console.

- f. Create an IAM policy that includes the permissions listed below.
- g. Attach the policy to the IAM role or IAM user that provides permissions to Cloud Manager.

The following policy provides the permissions that Cloud Manager needs to use the CMK from the external AWS account. Be sure to modify the region and account ID in the "Resource" sections.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowUseOfTheKey",
      "Effect": "Allow",
      "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
      ],
      "Resource": [
        "arn:aws:kms:us-east-1:externalaccountid:key/externalkeyid"
      ]
    },
    {
      "Sid": "AllowAttachmentOfPersistentResources",
      "Effect": "Allow",
      "Action": [
        "kms:CreateGrant",
        "kms:ListGrants",
        "kms:RevokeGrant"
      ],
      "Resource": [
        "arn:aws:kms:us-east-1:externalaccountid:key/externalaccountid"
      ],
      "Condition": {
        "Bool": {
          "kms:GrantIsForAWSResource": true
        }
      }
    }
  ]
}
```

For additional details about this process, see [AWS Documentation: Allowing External AWS Accounts to](#)

Networking requirements

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">• CloudFormation• Elastic Compute Cloud (EC2)• Key Management Service (KMS)• Security Token Service (STS)• Simple Storage Service (S3) <p>The exact endpoint depends on the region in which you deploy Cloud Volumes ONTAP. Refer to AWS documentation for details.</p>	<p>Enables Cloud Manager to deploy and manage Cloud Volumes ONTAP in AWS.</p>
<p>https://api.services.cloud.netapp.com:443</p>	<p>API requests to NetApp Cloud Central.</p>

Endpoints	Purpose
https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com	Provides access to software images, manifests, and templates.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com	Enables Cloud Manager to access and download manifests, templates, and Cloud Volumes ONTAP upgrade images.
https://kinesis.us-east-1.amazonaws.com	Enables NetApp to stream data from audit records.
https://cloudmanager.cloud.netapp.com	Communication with the Cloud Manager service, which includes Cloud Central accounts.
https://netapp-cloud-account.auth0.com	Communication with NetApp Cloud Central for centralized user authentication.
https://support.netapp.com/aods/asupmessage https://support.netapp.com/asupprod/post/1.0/postAsup	Communication with NetApp AutoSupport.
https://support.netapp.com/svcgw https://support.netapp.com/ServiceGW/entitlement	Communication with NetApp for licensing and support registration.
https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/	Required to connect Cloud Volumes ONTAP systems with a Kubernetes cluster. The endpoints enable installation of NetApp Trident.
<p>Various third-party locations, for example:</p> <ul style="list-style-type: none"> • https://repo1.maven.org/maven2 • https://oss.sonatype.org/content/repositories • https://repo.typesafe.org <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.

Endpoints	Purpose
https://api.services.cloud.netapp.com:443	API requests to NetApp Cloud Central.
https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com	Provides access to software images, manifests, and templates.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://sts.amazonaws.com	Enables Cloud Manager to access and download manifests, templates, and Cloud Volumes ONTAP upgrade images.
https://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.
https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/	Required to connect Cloud Volumes ONTAP systems with a Kubernetes cluster. The endpoints enable installation of NetApp Trident.
Various third-party locations, for example: <ul style="list-style-type: none"> • https://repo1.maven.org/maven2 • https://oss.sonatype.org/content/repositories • https://repo.typesafe.org <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>Depending on your connectivity to your cloud provider, you can use the private IP or a public IP assigned to the host:</p> <ul style="list-style-type: none"> • A private IP works if you have a VPN and direct connect access to your virtual network • A public IP works in any networking scenario <p>In any case, you should secure network access by ensuring that security group rules allow access from only authorized IPs or subnets.</p>
https://auth0.com https://cdn.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.
https://widget.intercom.io	For in-product chat that enables you to talk to NetApp cloud experts.

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](#).

Networking requirements for Cloud Volumes ONTAP in AWS

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 the following endpoints so Cloud Volumes ONTAP can send AutoSupport messages:

- <https://support.netapp.com/aods/asupmessage>
- <https://support.netapp.com/asupprod/post/1.0/postAsup>

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 and cluster/SVM management

HA configurations in multiple AZs use floating IP addresses that migrate between nodes if failures occur. They are not natively accessible from outside the VPC, unless you [set up an AWS transit gateway](#).

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. A fourth floating IP address for SVM management is optional.



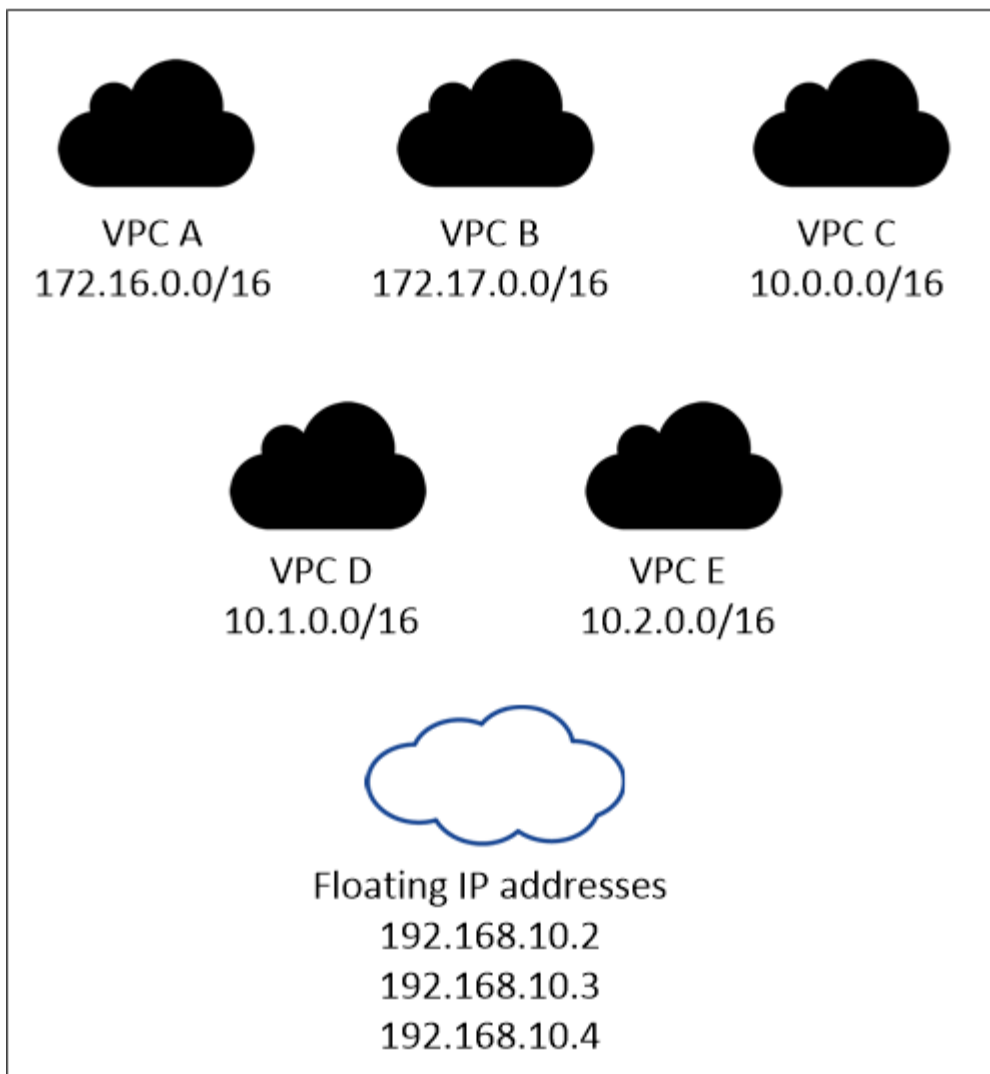
A floating IP address is required for the SVM management LIF if you use SnapDrive for Windows or SnapCenter with the HA pair. If you don't specify the IP address when you deploy the system, you can create the LIF later. For details, see [Setting up Cloud Volumes ONTAP](#).

You need to 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.

The floating IP addresses must be outside of the CIDR blocks for all VPCs in the AWS region in which you deploy the HA configuration. Think of the floating IP addresses as a logical subnet that's outside of the VPCs in your region.

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're routable to subnets through route tables.

AWS region



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

Transit gateway to enable floating IP access from outside the VPC

[Set up an AWS transit gateway](#) to enable access to an HA pair's floating IP addresses from outside the VPC where the HA pair resides.

Route tables

After you specify the floating IP addresses in Cloud Manager, you need to 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's 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 can't.

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

Connection to NetApp management tools

To use NetApp management tools with HA configurations that are in multiple AZs, you have two connection options:

1. Deploy the NetApp management tools in a different VPC and [set up an AWS transit gateway](#). The gateway enables access to the floating IP address for the cluster management interface from outside the VPC.
2. Deploy the NetApp management tools in the same VPC with a 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:

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:

Setting up an AWS transit gateway for HA pairs in multiple AZs

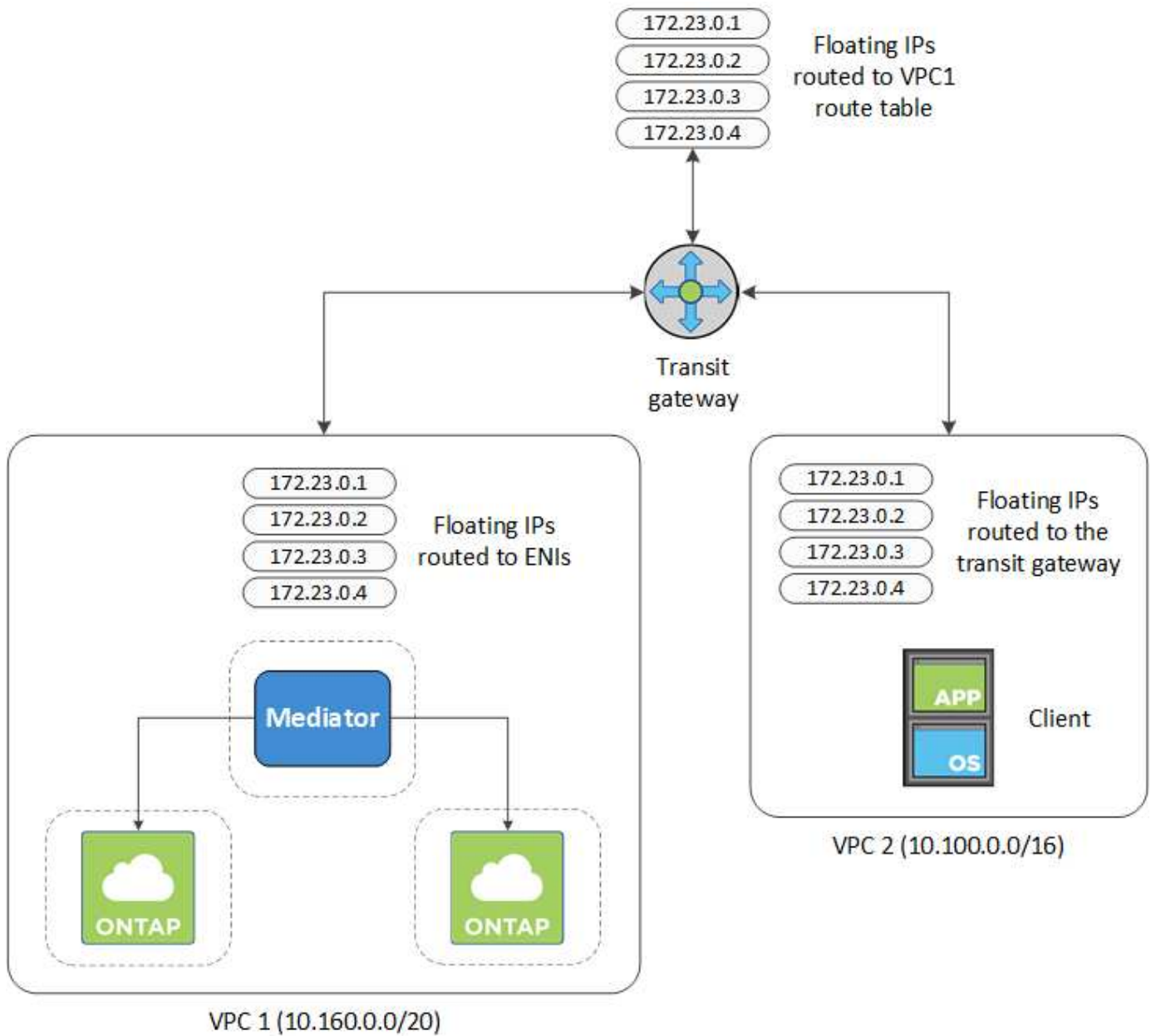
Set up an AWS transit gateway to enable access to an HA pair's floating IP addresses from outside the VPC where the HA pair resides.

When a Cloud Volumes ONTAP HA configuration is spread across multiple AWS Availability Zones, floating IP addresses are required for NAS data access from within the VPC. These floating IP addresses can migrate between nodes when failures occur, but they are not natively accessible from outside the VPC. Separate private IP addresses provide data access from outside the VPC, but they don't provide automatic failover.

Floating IP addresses are also required for the cluster management interface and the optional SVM management LIF.

If you set up an AWS transit gateway, you enable access to the floating IP addresses from outside the VPC where the HA pair resides. That means NAS clients and NetApp management tools outside the VPC can access the floating IPs.

Here's an example that shows two VPCs connected by a transit gateway. An HA system resides in one VPC, while a client resides in the other. You could then mount a NAS volume on the client using the floating IP address.



The following steps illustrate how to set up a similar configuration.

Steps

1. [Create a transit gateway and attach the VPCs to the gateway.](#)
2. Create routes in the transit gateway's route table by specifying the HA pair's floating IP addresses.

You can find the floating IP addresses on the Working Environment Information page in Cloud Manager. Here's an example:

NFS & CIFS access from within the VPC using Floating IP

Auto failover

Cluster Management : 172.23.0.1

Data (nfs,cifs) : Node 1: 172.23.0.2 | Node 2: 172.23.0.3

Access

SVM Management : 172.23.0.4

The following sample image shows the route table for the transit gateway. It includes routes to the CIDR blocks of the two VPCs and four floating IP addresses used by Cloud Volumes ONTAP.

Transit Gateway Route Table: tgw-rtb-0ea8ee291c7aeddd3

Details Associations Propagations **Routes** Tags

The table below will return a maximum of 1000 routes. Narrow the filter or use export routes to view more routes.

Create route Replace route Delete route

Filter by attributes or search by keyword

<input type="checkbox"/>	CIDR	Attachment	Resource type	Route type	Route state
<input type="checkbox"/>	10.100.0.0/16	tgw-attach-05e77bd34e2ff91f8 vpc-0b2bc30e0dc8e0db1	VPC2	propagated	active
<input type="checkbox"/>	10.160.0.0/20	tgw-attach-00eba3eac3250d7db vpc-673ae603	VPC1	propagated	active
<input type="checkbox"/>	172.23.0.1/32	tgw-attach-00eba3eac3250d7db vpc-673ae603	VPC	static	active
<input type="checkbox"/>	172.23.0.2/32	tgw-attach-00eba3eac3250d7db vpc-673ae603	VPC	static	active
<input type="checkbox"/>	172.23.0.3/32	tgw-attach-00eba3eac3250d7db vpc-673ae603	VPC	static	active
<input type="checkbox"/>	172.23.0.4/32	tgw-attach-00eba3eac3250d7db vpc-673ae603	VPC	static	active

Floating IP Addresses

3. Modify the route table of VPCs that need to access the floating IP addresses.
 - a. Add route entries to the floating IP addresses.
 - b. Add a route entry to the CIDR block of the VPC where the HA pair resides.

The following sample image shows the route table for VPC 2, which includes routes to VPC 1 and the floating IP addresses.

Route Table: rtb-0569a1bd740ed033f

Summary Routes Subnet Associations Route Propagation Tags

Edit routes

View All routes

Destination	Target	Status	Propagated
10.100.0.0/16	local	active	No
0.0.0.0/0	igw-07250bd01781e67df	active	No
10.160.0.0/20	tgw-015b7c249661ac279	active	No
172.23.0.1/32	tgw-015b7c249661ac279	active	No
172.23.0.2/32	tgw-015b7c249661ac279	active	No
172.23.0.3/32	tgw-015b7c249661ac279	active	No
172.23.0.4/32	tgw-015b7c249661ac279	active	No

VPC1
Floating IP Addresses

- Modify the route table for the HA pair's VPC by adding a route to the VPC that needs access to the floating IP addresses.

This step is important because it completes the routing between the VPCs.

The following sample image shows the route table for VPC 1. It includes a route to the floating IP addresses and to VPC 2, which is where a client resides. Cloud Manager automatically added the floating IPs to the route table when it deployed the HA pair.

Summary Routes Subnet Associations Route Propagation Tags

Edit routes

View All routes

Destination	Target	Status
10.160.0.0/20	local	active
pl-68a54001 (com.amazonaws.us-west-2.s3, 54.231.160.0/19, 52.218.128.0/17, 52.92.32.0/22)	vpce-cb51a0a2	active
0.0.0.0/0	igw-b2182dd7	active
10.60.29.0/25	pcx-589c3331	active
10.100.0.0/16	tgw-015b7c249661ac279	active
10.129.0.0/20	pcx-ff7e1396	active
172.23.0.1/32	eni-0854d4715559c3cdb	active
172.23.0.2/32	eni-0854d4715559c3cdb	active
172.23.0.3/32	eni-0f76681216c3108ed	active
172.23.0.4/32	eni-0854d4715559c3cdb	active

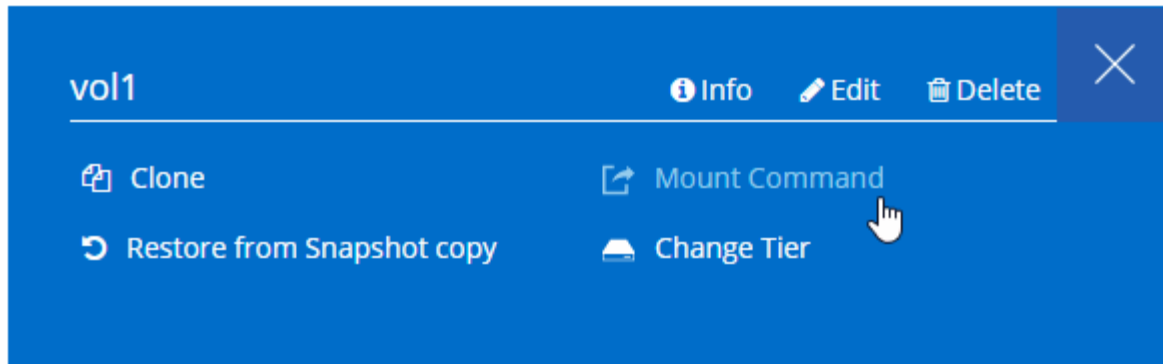
VPC2
Floating act IP Addresses

- Mount volumes to clients using the floating IP address.

You can find the correct IP address in Cloud Manager by selecting a volume and clicking **Mount Command**.

Volumes

2 Volumes | 0.22 TB Allocated | < 0.01 TB Used (0 TB in S3)



Related links

- [High-availability pairs in AWS](#)
- [Networking requirements for Cloud Volumes ONTAP in AWS](#)

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 AWS HTTP/HTTPS traffic to the following endpoints so Cloud Volumes ONTAP can send AutoSupport messages:

- <https://support.netapp.com/aods/asupmessage>
- <https://support.netapp.com/asupprod/post/1.0/postAsup>

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 permissions:

```
"Microsoft.Network/virtualNetworks/subnets/write",  
"Microsoft.Network/routeTables/join/action",
```

These permissions are included in the latest [Cloud Manager policy](#).

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

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](#).

Additional deployment options

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

t3.medium (recommended), t2.medium, and m4.large

Supported Azure VM sizes

A2, D2 v2, or D2 v3 (based on availability)

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.

Installing Cloud Manager on an existing Linux host

The most common way to deploy Cloud Manager is from Cloud Central or from a cloud provider's marketplace. But you have the option to download and install the Cloud Manager software on an existing 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.

- The installer that is available on the NetApp Support Site might be an earlier version. After installation, Cloud Manager automatically updates itself if a new version is available.

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. Review [Cloud Manager host requirements](#).
3. 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](#).

4. Assign permissions to execute the script.

Example

```
chmod +x OnCommandCloudManager-V3.6.3.sh
```

5. Run the installation script:

```
./OnCommandCloudManager-V3.6.3.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.

6. 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.

7. 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`

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

After you finish

Set up permissions for your AWS and Azure accounts so Cloud Manager can deploy Cloud Volumes ONTAP:

- If you want to deploy Cloud Volumes ONTAP in AWS, [set up an AWS account and then add it to Cloud Manager](#).
- If you want to deploy Cloud Volumes ONTAP in Azure, [set up an Azure account and then add it to Cloud Manager](#).

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](#).

About this task

The following steps describe how to launch the instance from the EC2 Console because the console enables you to attach an IAM role to the Cloud Manager instance. This is not possible using the 1-Click option.

Steps

1. Create an IAM policy and role for the EC2 instance:
 - a. Download the Cloud Manager IAM policy from the following location:
[NetApp OnCommand Cloud Manager: AWS and Azure Policies](#)
 - b. From the IAM console, create your own policy by copying and pasting the text from the Cloud Manager IAM policy.

- c. Create an IAM role with the role type Amazon EC2 and attach the policy that you created in the previous step to the role.
2. Go to the [Cloud Manager page on the AWS Marketplace](#).
3. Click **Continue**.
4. On the Custom Launch tab, click **Launch with EC2 Console** for your region, and then make your selections:
 - a. Depending on region availability, choose the t3.medium (recommended), t2.medium, or m4.large instance type.
 - b. Select a VPC, subnet, IAM role, and other configuration options that meet your requirements.
 - c. Keep the default storage options.
 - d. Enter tags for the instance, if desired.
 - e. Specify the required connection methods for the Cloud Manager instance: SSH, HTTP, and HTTPS.
 - f. Click **Launch**.

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.

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.

Separate instructions are available to deploy Cloud Manager in [Azure US Government regions](#) and in [Azure Germany regions](#).



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 VM:

- Cloud Manager can perform optimally with either HDD or SSD disks.
- Choose one of the recommended virtual machine sizes: A2, D2 v2, or D2 v3 (based on availability).

- For the network security group, Cloud Manager requires inbound connections using SSH, HTTP, and HTTPS.

[Learn more about security group rules for Cloud Manager.](#)

- Under **Management**, enable **System assigned managed identity** for Cloud Manager by selecting **On**.

This setting is important because a managed identity allows the Cloud Manager virtual machine to identify itself to Azure Active Directory without providing any credentials. [Learn more about managed identities for Azure resources.](#)

4. On the **Review + create** 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 [system-assigned managed 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_3.6.1.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 > Add role assignment** 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.

Deploying Cloud Manager in an Azure US Government region

To get Cloud Manager up and running in a US Government region, first deploy Cloud Manager from the Azure Government Marketplace. Then provide the permissions that Cloud Manager needs to deploy and manage Cloud Volumes ONTAP systems.

For a list of supported Azure US Government regions, see [Cloud Volumes Global Regions](#).

Deploying Cloud Manager from the Azure US Government Marketplace

Cloud Manager is available as an image in the Azure US Government Marketplace.

Steps

1. Search for OnCommand Cloud Manager in the Azure US Government portal.
2. 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, D2 v2, or D2 v3 (based on availability).
- 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.

3. 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.

4. 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.

5. 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 using a managed identity

The easiest way to provide permissions is by enabling a [managed identity](#) on the Cloud Manager virtual machine and then by assigning the required permissions to the virtual machine. If preferred, an alternative way is to [grant Azure permissions using a service principal](#).

Steps

1. Enable a managed identity on the Cloud Manager virtual machine:
 - a. Navigate to the Cloud Manager virtual machine and select **Identity**.
 - b. Under **System Assigned**, click **On** and then click **Save**.
2. 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_3.6.1.json
```

You should now have a custom role called OnCommand Cloud Manager Operator that you can assign

to the Cloud Manager virtual machine.

3. 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**, click **Add role assignment**, 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.
 - Type the name of the virtual machine and then select it.
 - 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.

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](#).

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.

Copyright Information

Copyright © 2021 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, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.