Getting started

Cloud Manager 3.4

NetApp
June 06, 2022

Table of Contents

Getting started

Deployment overview

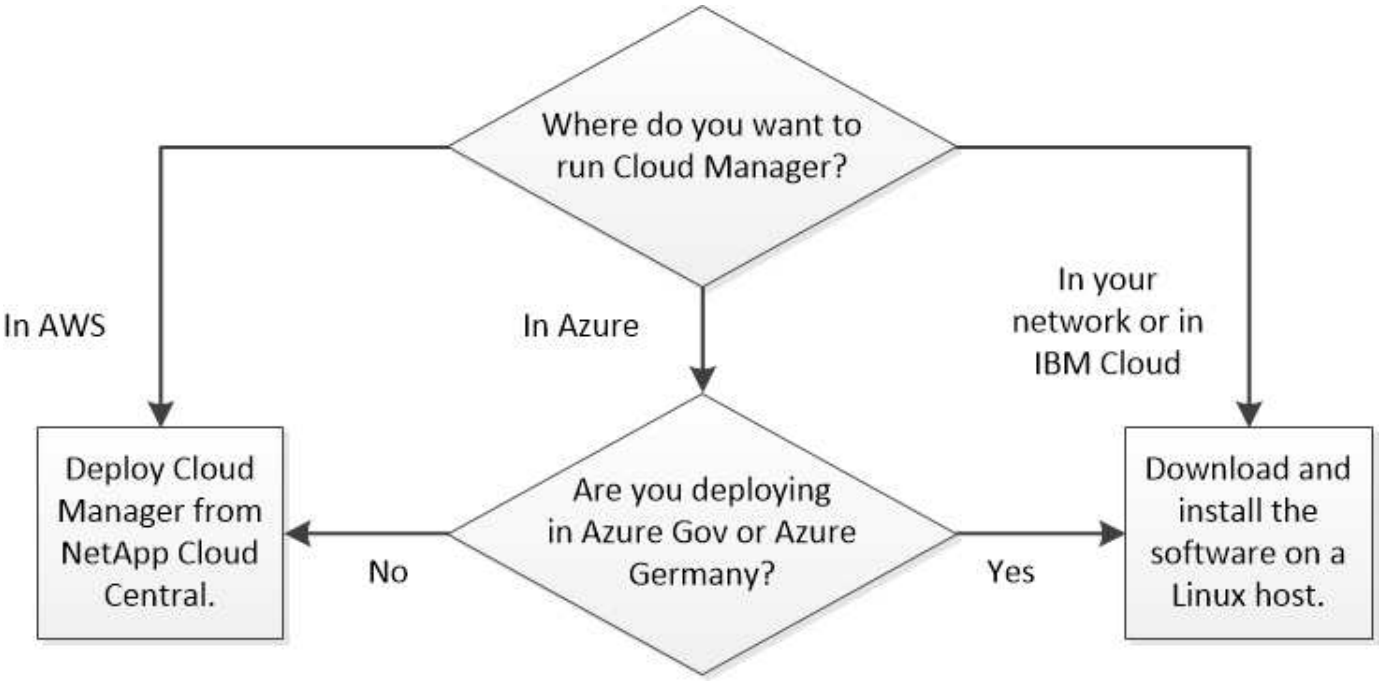
Before you get started, you might want to better understand your options for deploying OnCommand Cloud Manager and ONTAP Cloud.

Cloud Manager installation

Cloud Manager software is required to deploy and manage ONTAP Cloud systems. 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

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.

ONTAP Cloud deployment

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

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

- Planning your configuration
- Launching ONTAP Cloud in AWS
- Launching ONTAP Cloud in Azure

Getting started with ONTAP Cloud in AWS

Getting started with ONTAP Cloud includes preparing your AWS environment, launching the OnCommand Cloud Manager software from NetApp Cloud Central, and then launching ONTAP Cloud systems using Cloud Manager.

Verifying your networking

You must choose the AWS VPC and subnets in which you want to launch Cloud Manager and ONTAP Cloud. At a minimum, your networking must meet the following requirements:

- Outbound internet access

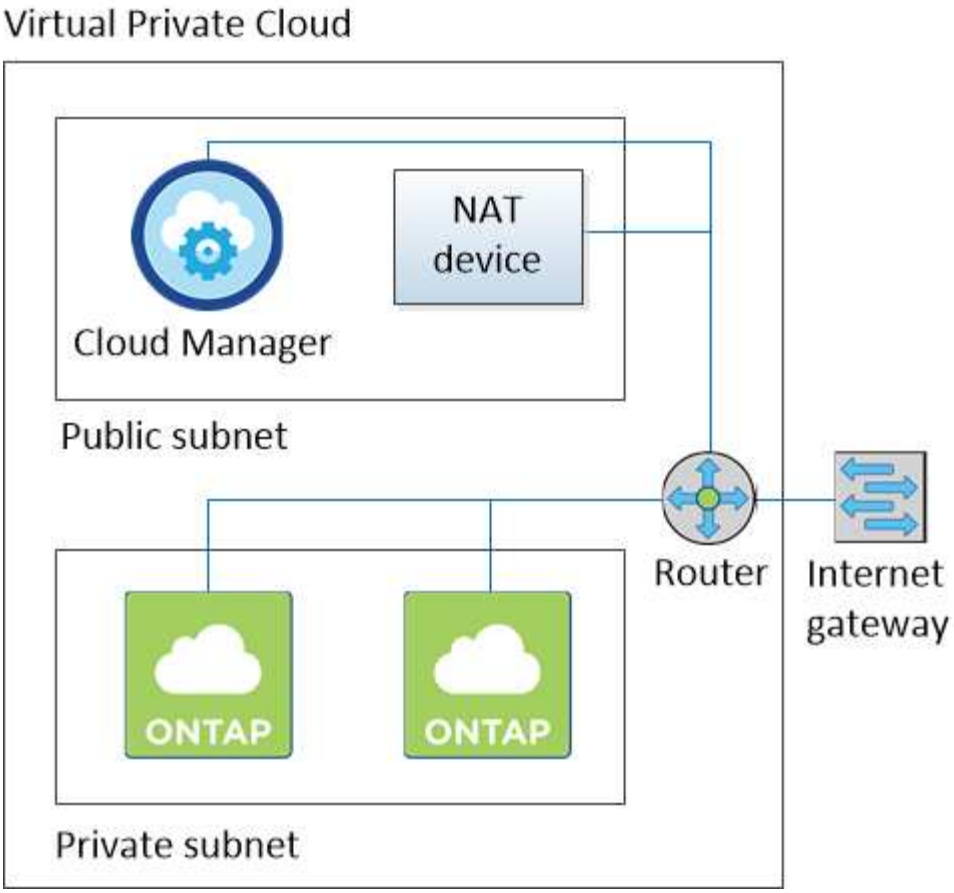
  The target VPC must have one or more subnets that have outbound internet access so Cloud Manager and ONTAP Cloud can contact several endpoints. To review the list of endpoints, see AWS networking requirements.

- Connections between networks
  - To deploy ONTAP Cloud systems in subnets or networks separate from Cloud Manager, connections between those networks must be in place.
  - To replicate data across a hybrid cloud or multi-cloud environment, VPN connections between networks must be in place. For details, refer to AWS Documentation: Setting Up an AWS VPN Connection.
- Endpoint to S3

  To reduce storage costs by using EBS as a performance tier and AWS S3 as a capacity tier, the VPC in which you launch ONTAP Cloud must have an endpoint to the S3 service. For details, refer to AWS Documentation: Creating a Gateway Endpoint.

For additional networking information, see AWS networking requirements.

The following sample VPC configuration shows public and private subnets and a NAT device that enables outbound internet access for the private subnet:



Subscribing to ONTAP Cloud in AWS

You must subscribe to ONTAP Cloud from the AWS Marketplace so you can launch ONTAP Cloud in AWS.

Steps

1. Go to the AWS Marketplace pages for ONTAP Cloud:
   - ONTAP Cloud for AWS (PayGo)
   - ONTAP Cloud for AWS (BYOL)
   - ONTAP Cloud for AWS - High Availability (PayGo)
   - ONTAP Cloud for AWS - High Availability (BYOL)
2. Click **Continue**, review the terms, and then click **Accept Software Terms**.

> You must not launch ONTAP Cloud instances from the AWS Marketplace. You must use Cloud Manager to launch ONTAP Cloud.

> Subscribing is not required to launch ONTAP Cloud in the AWS GovCloud (US) region.

Granting AWS permissions

When you launch Cloud Manager from NetApp Cloud Central, you must provide AWS credentials for a user that has specific AWS permissions. Cloud Central needs the credentials and permissions to launch the Cloud Manager instance on your behalf.

About this task

Providing the credentials is secure and private—NetApp does not save the credentials. It uses them only to launch the instance.

When you launch Cloud Manager, NetApp Cloud Central creates an IAM policy and an IAM role for the instance. This gives Cloud Manager permissions to deploy and manage ONTAP Cloud in AWS. To review the list of permissions, see AWS and Azure permissions for Cloud Manager.

Steps

1. From the AWS IAM console, create your own policy by copying and pasting the contents of the NetApp Cloud Central IAM policy.
2. Attach the policy that you just created to the IAM user.

   The following video shows this process.

   ► https://docs.netapp.com/us-en/occm34//media/video_setup_portal_policy.mp4 *(video)*

Launching Cloud Manager in AWS

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

Steps

1. Go to NetApp Cloud Central and sign up or log in.
2. Under **ONTAP Cloud**, click **Start Free Trial**.
3. Follow the prompts to deploy the Cloud Manager instance and software in AWS.

   You should keep the page open until the deployment is complete. The portal redirects you to the Cloud Manager system when it is available.

   ⓘ If a proxy server is required for internet connectivity in the subnet, Cloud Manager prompts you to add the proxy details.

   The following video shows how to launch Cloud Manager.

   ► https://docs.netapp.com/us-en/occm34//media/video_launch_occm.mp4 *(video)*

Result

Cloud Manager is now installed and set up so users can launch ONTAP Cloud instances.

Launching ONTAP Cloud in AWS

You can launch ONTAP Cloud in AWS to provide enterprise-class features for your cloud storage. You can choose a single-node configuration, or an HA pair to provide nondisruptive operations and fault tolerance in AWS.

Steps

1. On the Working Environments page in Cloud Manager, click **Create**.
2. Under Create, select **ONTAP Cloud** or **ONTAP Cloud HA**.
3. Complete the steps in the wizard to launch the instance.

Note the following as you complete the wizard:

- The predefined security group includes the rules that ONTAP Cloud needs to operate successfully. If you need to use your own, refer to Security group rules.
- The underlying AWS disk type is for the initial ONTAP Cloud volume. You can choose a different disk type for subsequent volumes.
- The performance of AWS disks is tied to disk size. You should choose the disk size that gives you the sustained performance that you need. For details, refer to AWS Documentation: Amazon EBS Volume Types.
- The disk size is the default size for all disks on the system.

If you need a different size later, you can use the **Advanced allocation** option to create an aggregate that uses disks of a specific size.

The following video shows how to launch a single-node configuration.

► https://docs.netapp.com/us-en/occm34//media/video_launch_otc_aws.mp4 *(video)*

Result

Cloud Manager launches the ONTAP Cloud instance in AWS. You can track the progress in the timeline.

Getting started with ONTAP Cloud in Azure

Getting started with ONTAP Cloud includes preparing your Azure environment, launching the OnCommand Cloud Manager software from NetApp Cloud Central, and then launching ONTAP Cloud systems using Cloud Manager.

Verifying your networking

You must choose the Azure VNet and subnets in which you want to deploy Cloud Manager and ONTAP Cloud. At a minimum, your networking must meet the following requirements:

- Outbound internet access

  The target VNet must have one or more subnets that have outbound internet access so Cloud Manager and ONTAP Cloud can contact several endpoints. To review the list of endpoints, see Azure networking requirements.

- Connections between networks
  - To deploy ONTAP Cloud systems in subnets or networks separate from Cloud Manager, connections between those networks must be in place.
  - To replicate data across a hybrid cloud or multi-cloud environment, VPN connections between networks must be in place. For details, refer to Microsoft Azure Documentation: Create a Site-to-Site connection in the Azure portal.

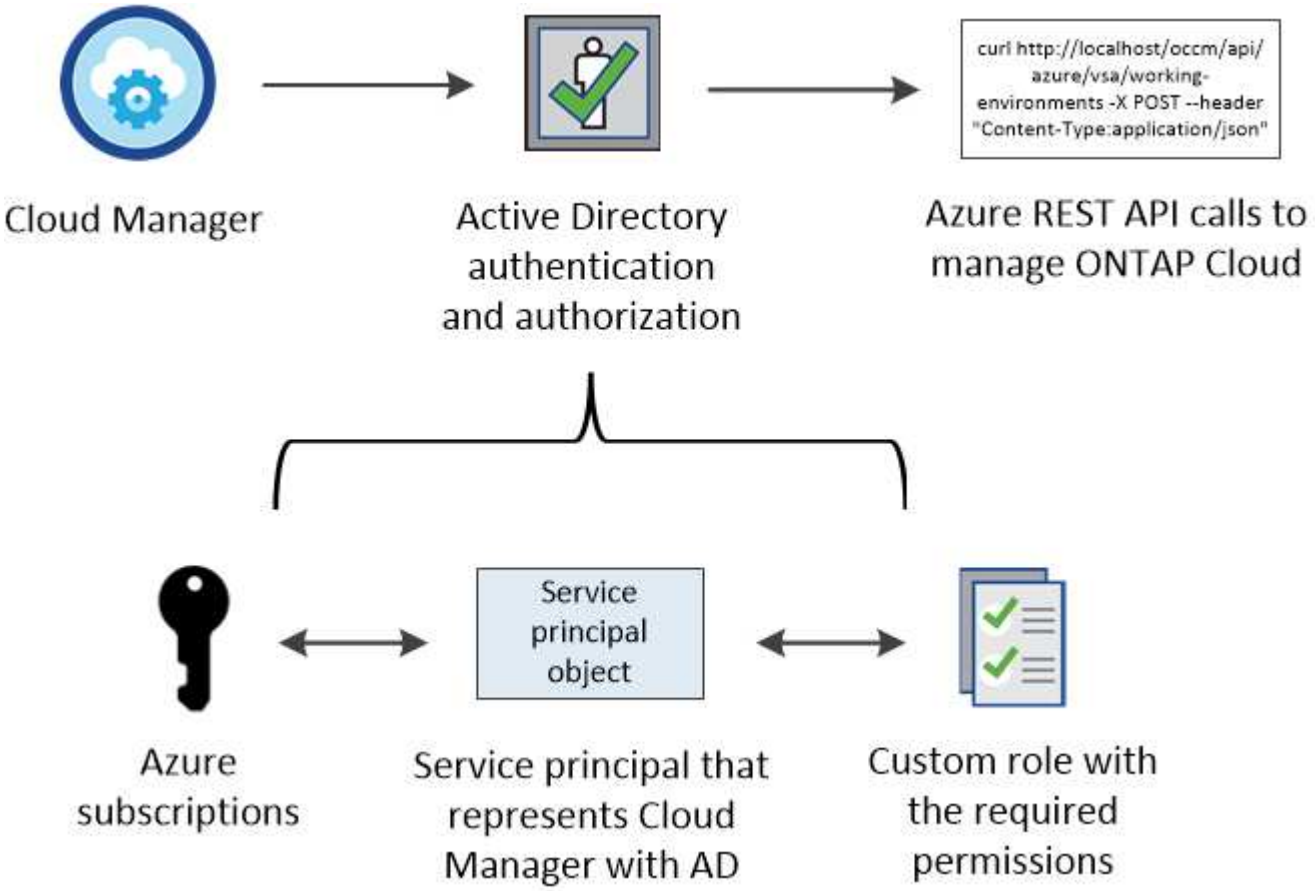
For additional networking information, see Azure networking requirements.

Granting Azure permissions to Cloud Manager

Cloud Manager needs permissions to perform actions in Azure. You must 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.

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 ONTAP Cloud 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 ONTAP Cloud 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_4_5.json

Result

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

Creating an Active Directory service principal

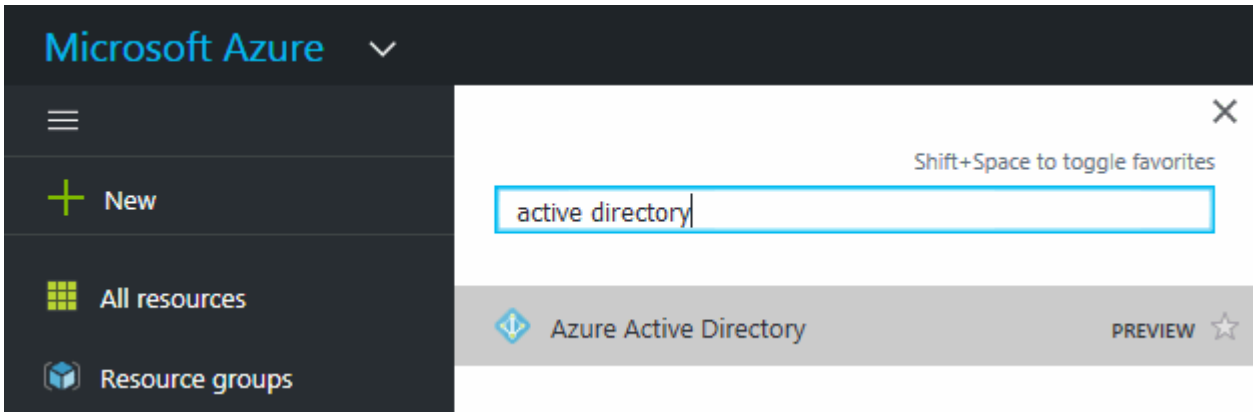
You must create an Active Directory service principal so Cloud Manager can authenticate with Azure Active Directory.

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

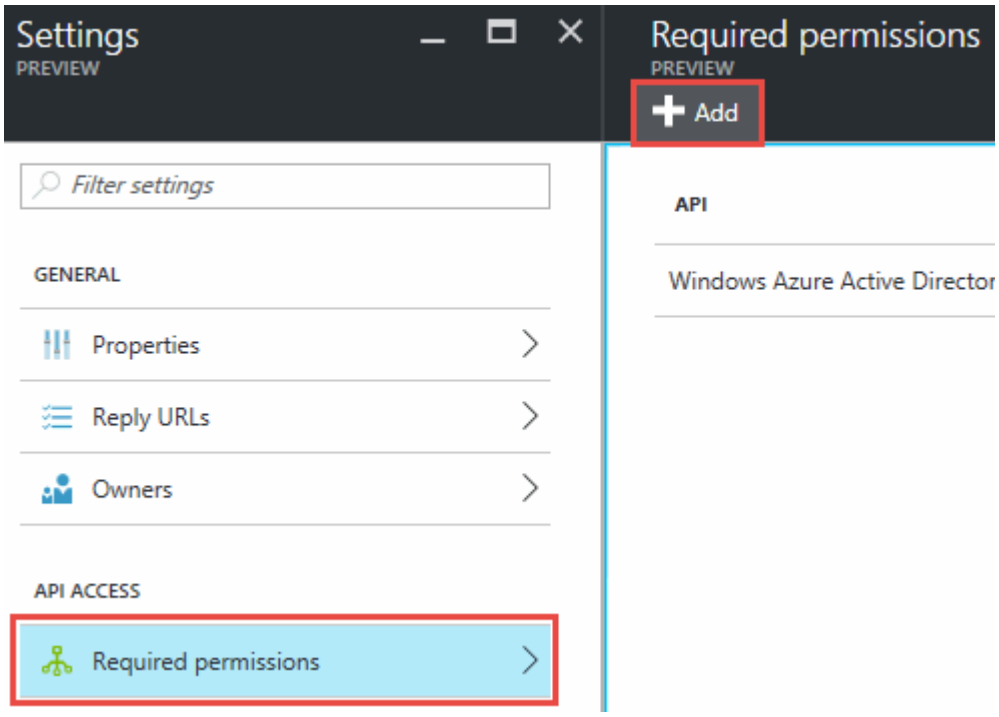
1. From the Azure portal, open the **Azure Active Directory** service.



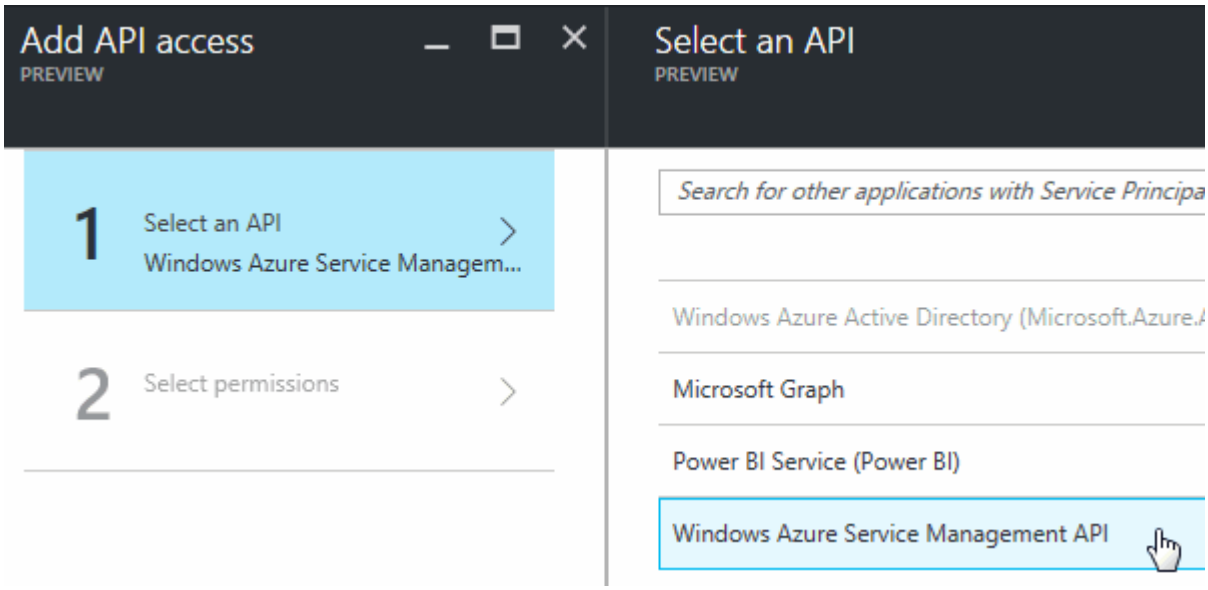
2. In the menu, click **App registrations**.
3. Create the service principal:
   a. Click **New application registration**.
   b. Enter a name for the application, keep **Web app / API** selected, and then enter any URL—for example, http://url

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**.

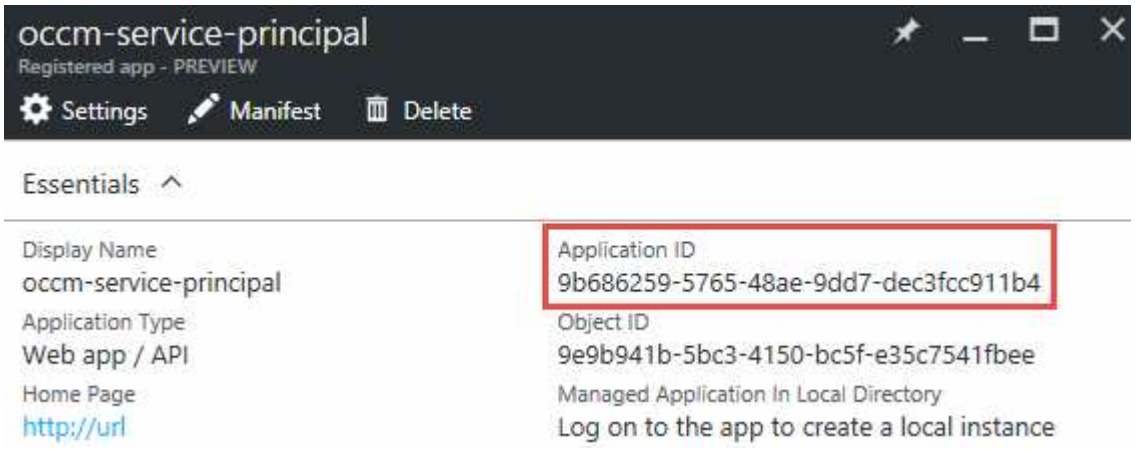
5. Create a key for the service principal:
   a. Under Settings, click **Keys**.
   b. Enter a description, select a duration, and then click **Save**.

c. Copy the key value.

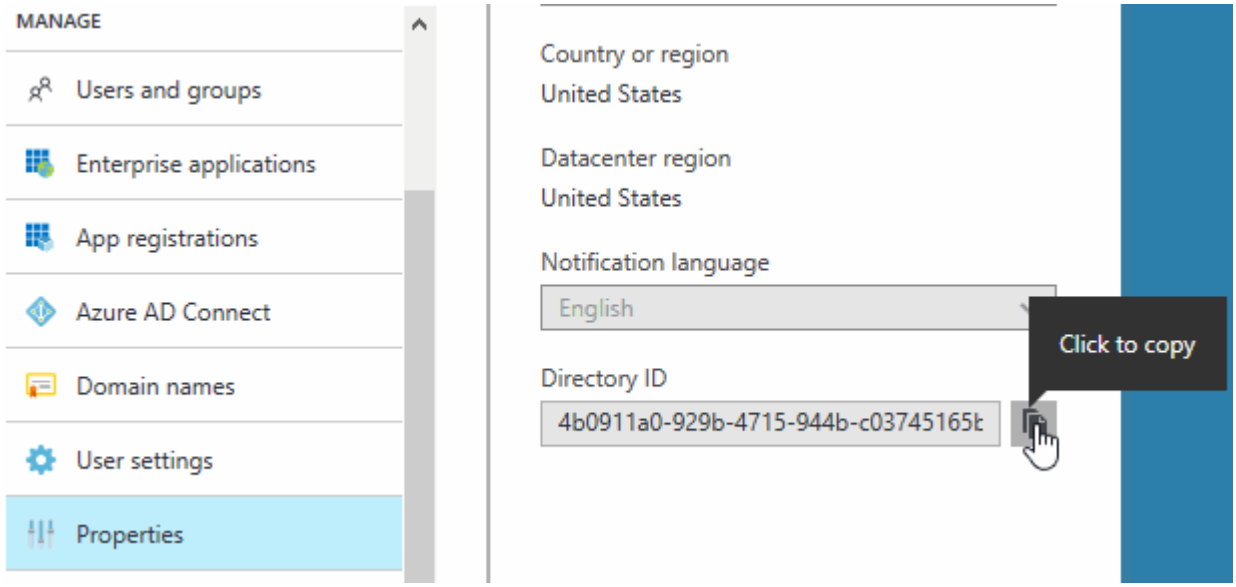
   You need to enter the key value in Cloud Manager when you create user accounts for this subscription.

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.



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 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 ONTAP Cloud 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 ONTAP Cloud.

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.

Installing and setting up Cloud Manager in Azure

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

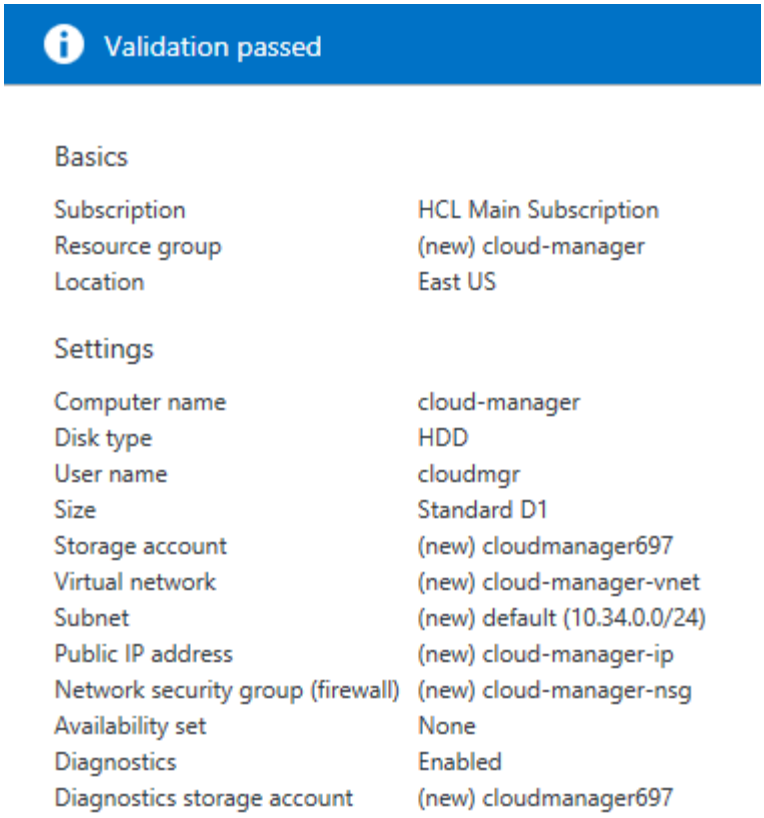
Steps

1. Go to NetApp Cloud Central and sign up or log in.
2. Under **ONTAP Cloud**, click **Start Free Trial**.
3. Select **Microsoft Azure** to deploy Cloud Manager from the Azure Marketplace.
4. Click **Get it now** and then click **Continue**.
5. 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.
6. Review your selections and click **OK**.

   Example



7. Click **Purchase**.

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

8. 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.

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

Result

Cloud Manager is now installed and set up so users can deploy ONTAP Cloud in Azure.

Deploying ONTAP Cloud in Azure

You can deploy ONTAP Cloud in Azure to provide enterprise-class features for your cloud storage.

Steps

1. On the Working Environments page in Cloud Manager, click **Create**.
2. Under Create, select **ONTAP Cloud for Azure**.
3. Complete the steps in the wizard to launch the system.

   Note the following as you complete the wizard:

- The predefined network security group includes the rules that ONTAP Cloud needs to operate successfully. If you need to use your own, refer to Security group rules.
- The underlying Azure disk type is for the initial ONTAP Cloud volume. You can choose a different disk type for subsequent volumes.
- The performance of Azure Premium Storage is tied to the disk size. Larger disks provide higher IOPS and throughput.
- The disk size is the default size for all disks on the system.

If you need a different size later, you can use the **Advanced allocation** option to create an aggregate that uses disks of a specific size.

The following video shows how to deploy ONTAP Cloud in Azure.

► https://docs.netapp.com/us-en/occm34//media/video_launch_otc_azure.mp4 *(video)*

Result

Cloud Manager deploys the ONTAP Cloud system. You can track the progress in the timeline.

Setting up Cloud Manager

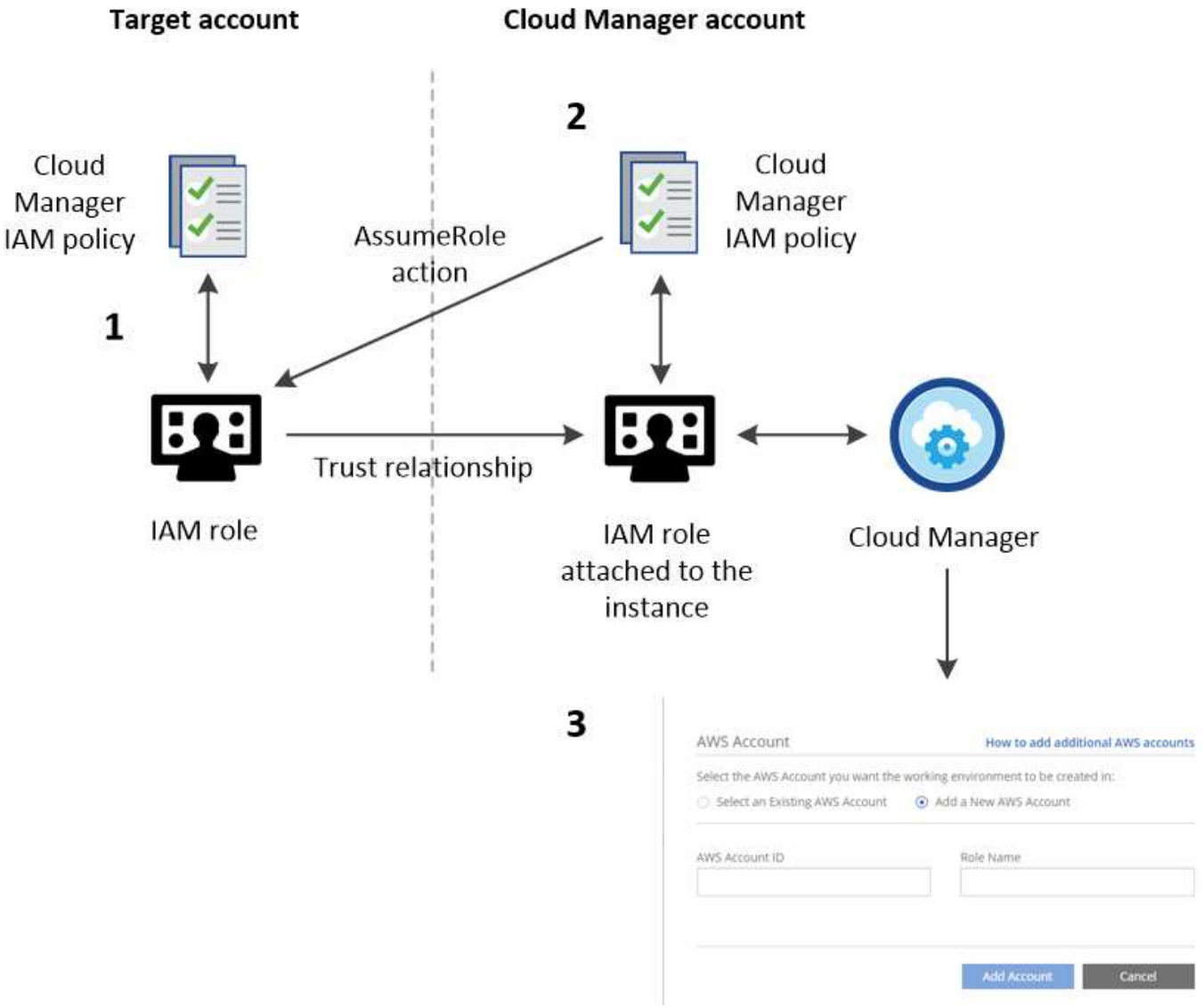
You can start creating ONTAP Cloud systems right after you deploy Cloud Manager. However, you might want to perform additional setup first by setting up the AWS Key Management Service, installing an HTTPS certificate, and more.

Adding additional AWS accounts to Cloud Manager

When Cloud Manager is associated with an IAM role, it deploys ONTAP Cloud systems in the AWS account from which the Cloud Manager instance was created. If you want to deploy ONTAP Cloud systems 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 ONTAP Cloud systems.

   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 ONTAP Cloud 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.

Setting up the AWS KMS

If you want to use Amazon encryption with ONTAP Cloud, 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 ONTAP Cloud systems.

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

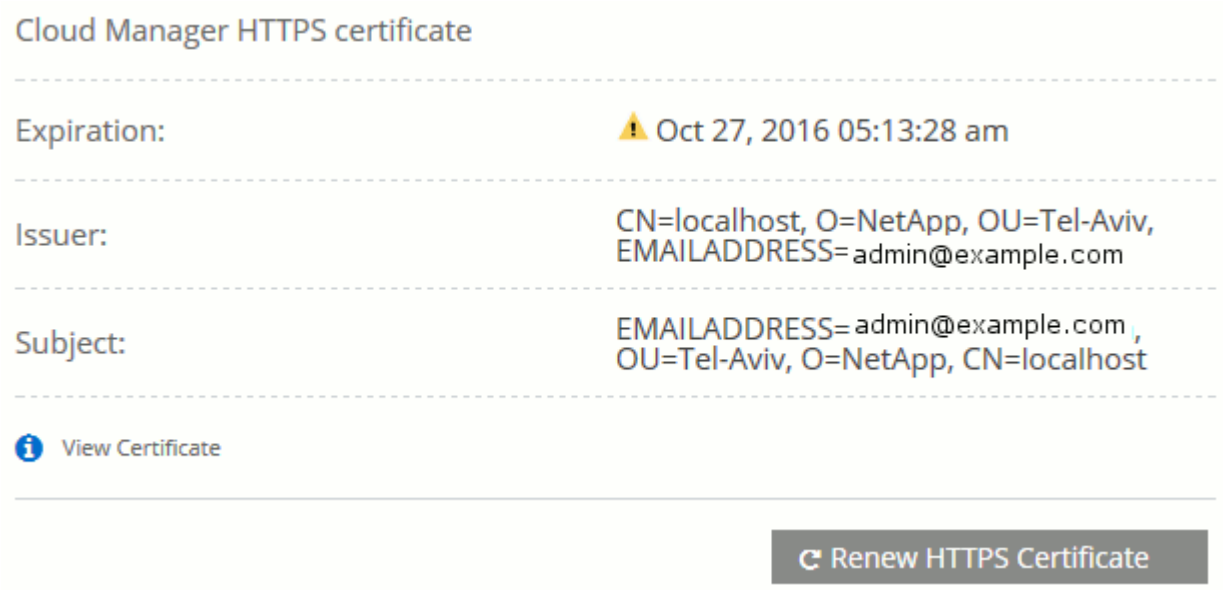
1. In the upper right of the Cloud Manager console, click the task drop-down list, and then select **HTTPS Setup**.
2. In the HTTPS Setup page, install a certificate by generating a certificate signing request (CSR) or by installing your own CA-signed certificate:

Option	Description
Generate a CSR	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**.

Option	Description
Install your own CA-signed certificate	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:



Adding users to Cloud Manager

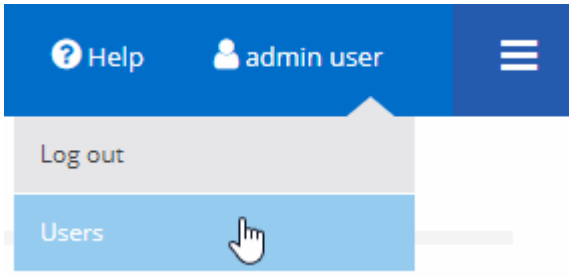
If additional users need to use your Cloud Manager system, they must sign up for an account in NetApp Cloud Central. You can then add the users to Cloud Manager.

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 **Users**.



3. Click **Add 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.

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 ONTAP Cloud software.

Steps

1. Click **Tenants**.
2. Select the tenant that you want to link to a NetApp Support Site account.
3. Click **Change NSS account**.
4. Enter the user name and password for a NetApp customer-level account (not a guest or temp account) and click **Save**.

Result

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

Setting up AWS billing and cost management for Cloud Manager

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

Before you begin

You must have granted AWS permissions to Cloud Manager so it can access an S3 bucket. 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 an ONTAP Cloud instance, as well as storage cost savings from NetApp product efficiency features (if they are enabled). For an example, see 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 ONTAP Cloud instance, go back to Billing and Cost Management **Preferences**, click **Manage report tags**, and enable the **WorkingEnvironmentId** tag.

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

Result

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

After you finish

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

Setting up ONTAP Cloud encryption

The Cloud Manager Admin user must set up Cloud Manager before other users can enable ONTAP Cloud encryption on new ONTAP Cloud systems in AWS.

Steps

1. Implement a supported key management infrastructure.
2. Set up Cloud Manager as an intermediate CA.
3. Add key managers and their CA certificates to Cloud Manager.

Key manager requirements

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

Supported key managers

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

- SafeNet Virtual KeySecure k150v
- SafeNet KeySecure k460
- Vormetric Data Security Manager

See the NetApp Interoperability Matrix Tool for supported software versions.

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

Vormetric configuration requirements

See NetApp KB article 000033069.

> The Encryption Setup page in Cloud Manager pertains to SafeNet key managers only. You must refer to the KB article to set up ONTAP Cloud with Vormetric key managers. The rest of this section describes setup for SafeNet key managers.

SafeNet configuration requirements

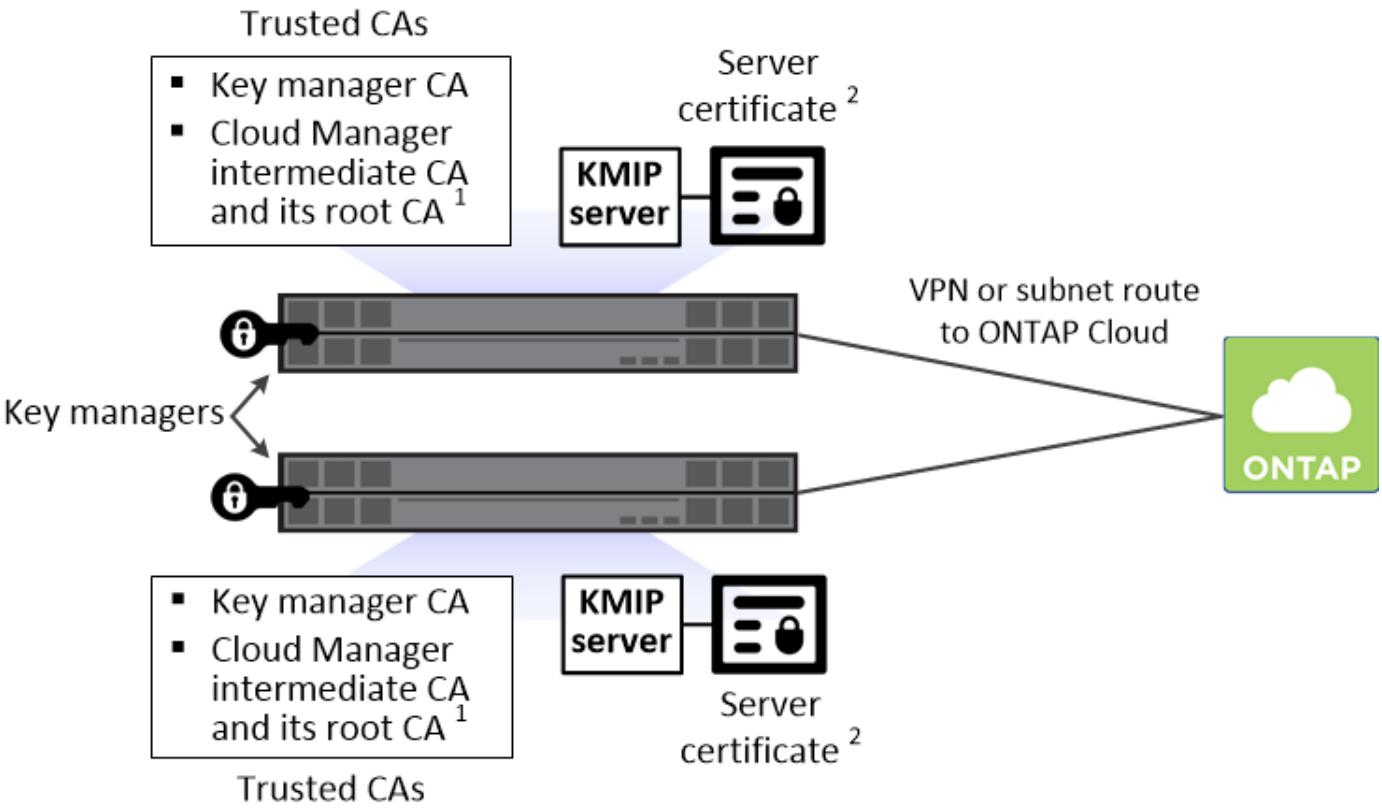
Each SafeNet key manager must have several certificates, a KMIP server, and a network connection to ONTAP Cloud systems. The key manager must also meet specific requirements if using client certificate authentication. Note that Cloud Manager does not communicate with key managers, so a network connection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

A description of the key manager requirements follows:

Requirement	Description
Key managers must have a server certificate	Key managers need a server certificate to authenticate with ONTAP Cloud systems. The SSL certificate must use the Privacy Enhanced Mail (PEM) Base-64 encoded X.509 format. You select this server certificate when you configure the KMIP server on the key manager. If you plan to use two to four key managers with an ONTAP Cloud system, the same certificate authority (CA) must sign the server certificate for each key manager.
Key managers must trust the signing CA	The CA that signed the server certificate must be known and trusted by the key manager. Key managers must have a KMIP server Each key manager must have a KMIP server that uses SSL and a specific port. The default and recommended port for ONTAP Cloud is 5696. If needed, you can change this port when you set up Cloud Manager.
Key managers must have a network connection to ONTAP Cloud systems	If the key managers are in AWS, they must have a connection to the subnet in which ONTAP Cloud instances are running. If the key managers are in your network, a VPN connection to the VPC provides the required connection. Firewall settings must allow communication through the KMIP port.
Key managers must trust the Cloud Manager CA and its root CA, if using client certificate authentication	When you set up Cloud Manager, you configure it to act as an intermediate CA so it can sign ONTAP Cloud client certificates. If a KMIP server requires client certificate authentication, then the Cloud Manager intermediate CA must be known and trusted by key managers. The root CA that signed the Cloud Manager certificate must also be known and trusted by the key manager.
Key managers must check a compatible user name field, if using client certificate authentication	If the key manager's KMIP server checks for a user name in client certificates, it must use a field compatible with ONTAP Cloud client certificates. Cloud Manager can create ONTAP Cloud client certificates that include a user name in the CN (Common Name), E (Email address), and OU (Organizational Unit) fields.

Requirement	Description
KMIP Cryptographic Usage Mask must be set to no	If you use SafeNet OS v8.6, you must do the following: 1. Connect to the CLI using the admin user 2. Enter the following commands: **config** **no kmip cryptographicusagemask** 3. Restart the NAE Server from the user interface

The following graphic depicts these requirements:



Notes:

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

After you meet these requirements, you must set up Cloud Manager so users can enable ONTAP Cloud encryption.

Setting up Cloud Manager as an intermediate CA

Cloud Manager must be an intermediate certificate authority (CA) because it needs to create client certificates for ONTAP Cloud. You set up Cloud Manager to be an intermediate CA by generating a certificate signing

request (CSR), getting the CSR signed by a root CA, and then installing the certificate in Cloud Manager.

Steps

1. In the upper-right corner of the Cloud Manager console, click the task drop-down list, and then select **Encryption Setup**.
2. In the Intermediate CA tab, click **Generate CSR**.

   Cloud Manager displays a certificate signing request.

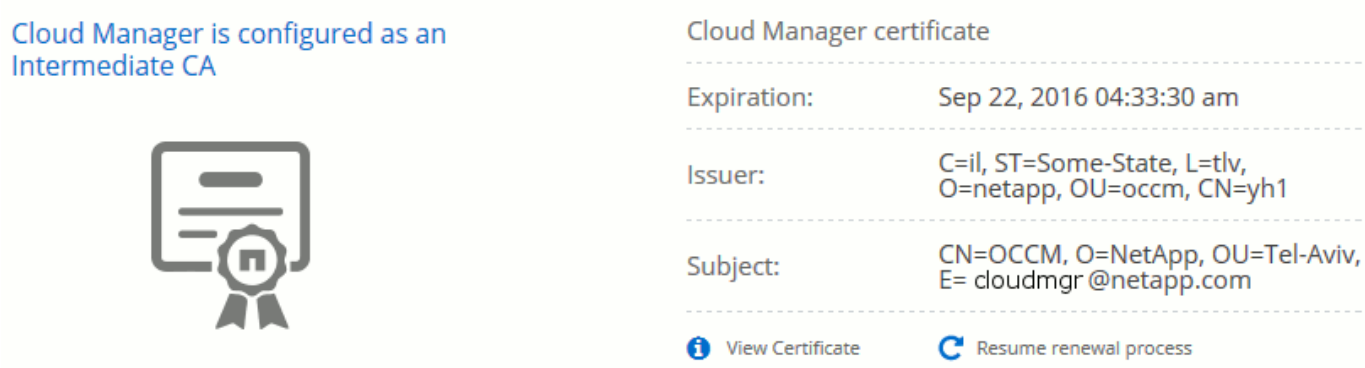
3. Use the CSR to submit a certificate request to a CA.

   The intermediate CA certificate must use the Privacy Enhanced Mail (PEM) Base-64 encoded X.509 format.

4. Copy the content of the signed certificate and paste it in the Cloud Manager certificate field.
5. Click **Install Cloud Manager Certificate**.

Result

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



After you finish

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

Adding key managers and CA certificates to Cloud Manager

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

Steps

1. In the Encryption Setup page, click **Key Manager**.
2. If your key managers use a KMIP port other than 5696, change the port and then click Save.

   Cloud Manager configures ONTAP Cloud systems to connect to key managers using this port.

3. In the Key Managers table, click **Add**.

   In the Add Key Manager dialog box, enter details about the key manager, and then click **Add**:

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

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

Result

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

Detailed networking requirements

AWS networking requirements

You must set up your AWS networking so that Cloud Manager can deploy ONTAP Cloud systems and so those systems can operate properly.

General networking requirements

The following requirements must be met in AWS.

Outbound internet access for Cloud Manager

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

Endpoints	Purpose
AWS services (amazonaws.com): • CloudFormation • Elastic Compute Cloud (EC2) • Key Management Service (KMS) • Security Token Service (STS) • Simple Storage Service (S3) The exact endpoint depends on the region in which you deploy ONTAP Cloud. Refer to AWS documentation for details.	Enables Cloud Manager to deploy and manage ONTAP Cloud systems in AWS.
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	Enables Cloud Manager to access and download manifests, templates, and ONTAP Cloud 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.
Various third-party locations, for example: https://repo1.maven.org/maven2 https://oss.sonatype.org/content/repositories https://repo.typesafe.org Third-party locations are subject to change.	During upgrades, Cloud Manager downloads the latest packages for third-party dependencies.

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.

Outbound internet access for ONTAP Cloud

ONTAP Cloud 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 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).

Outbound internet access from your web browser

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

Endpoint	Purpose
The Cloud Manager host	You must enter the host's IP address from a web browser to load the Cloud Manager console. 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: • A jump host in the VPC that has a connection to Cloud Manager • A host in your network that has a VPN connection to the private IP address
https://netapp-cloud-account.auth0.com	Your web browser connects to this endpoint for centralized user authentication through NetApp Cloud Central.

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 between Cloud Manager and ONTAP Cloud subnets

Cloud Manager requires a connection to the subnets in which you launch ONTAP Cloud systems, including the HA mediator.

If Cloud Manager is not installed in the target VPC, it must have network connectivity to that VPC. For example, if you install Cloud Manager in Azure or in your corporate network, then you must set up a VPN connection to the VPC in which you launch ONTAP Cloud systems.

Connection from ONTAP Cloud 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 ONTAP Cloud 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 ONTAP Cloud instance. You must also modify the security group to add an outbound HTTPS rule that enables traffic to the S3 endpoint. Otherwise, ONTAP Cloud 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 an ONTAP Cloud 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.

Connection to key managers

If you want to use the ONTAP Cloud data encryption feature, ONTAP Cloud instances must have a connection to one or more key managers that are either in AWS or in your network. For instructions, see Setting up ONTAP Cloud encryption.

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.

Networking requirements for ONTAP Cloud HA in multiple AZs

Additional AWS networking requirements apply to ONTAP Cloud 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 ONTAP Cloud instance and the mediator instance, which provides a communication channel between the HA pair.

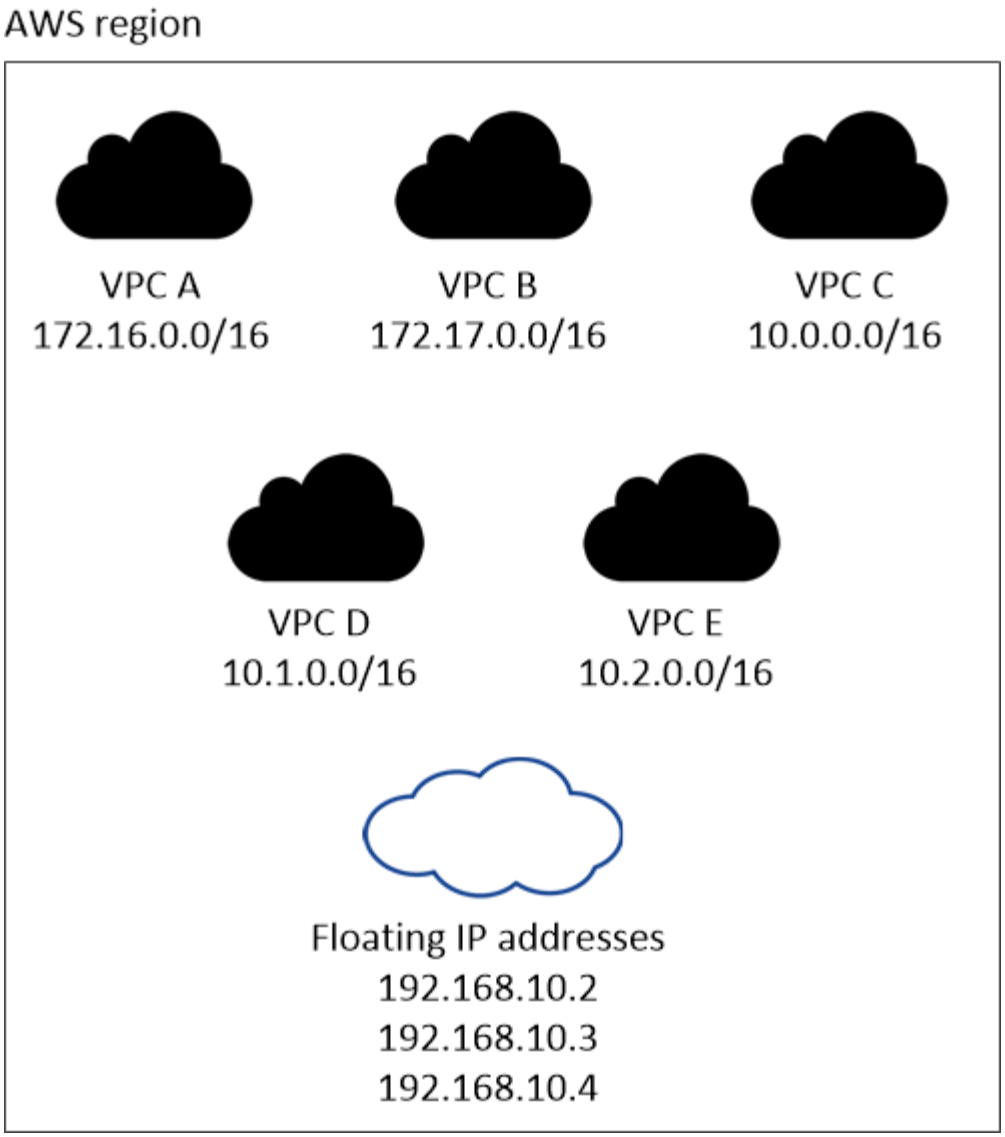
Floating IP addresses for NAS data access

ONTAP Cloud 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.



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

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 ONTAP Cloud HA pair, a floating IP address is also required for the SVM management LIF. You must create this LIF after you launch the HA pair. For details, see Setting up ONTAP Cloud.

Route tables

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

If you have just one route table for the subnets in your VPC (the main route table), then Cloud Manager automatically adds the floating IP addresses to that route table. If you have more than one route table, it is

very important to select the correct route tables when launching the HA pair. Otherwise, some clients might not have access to ONTAP Cloud.

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.

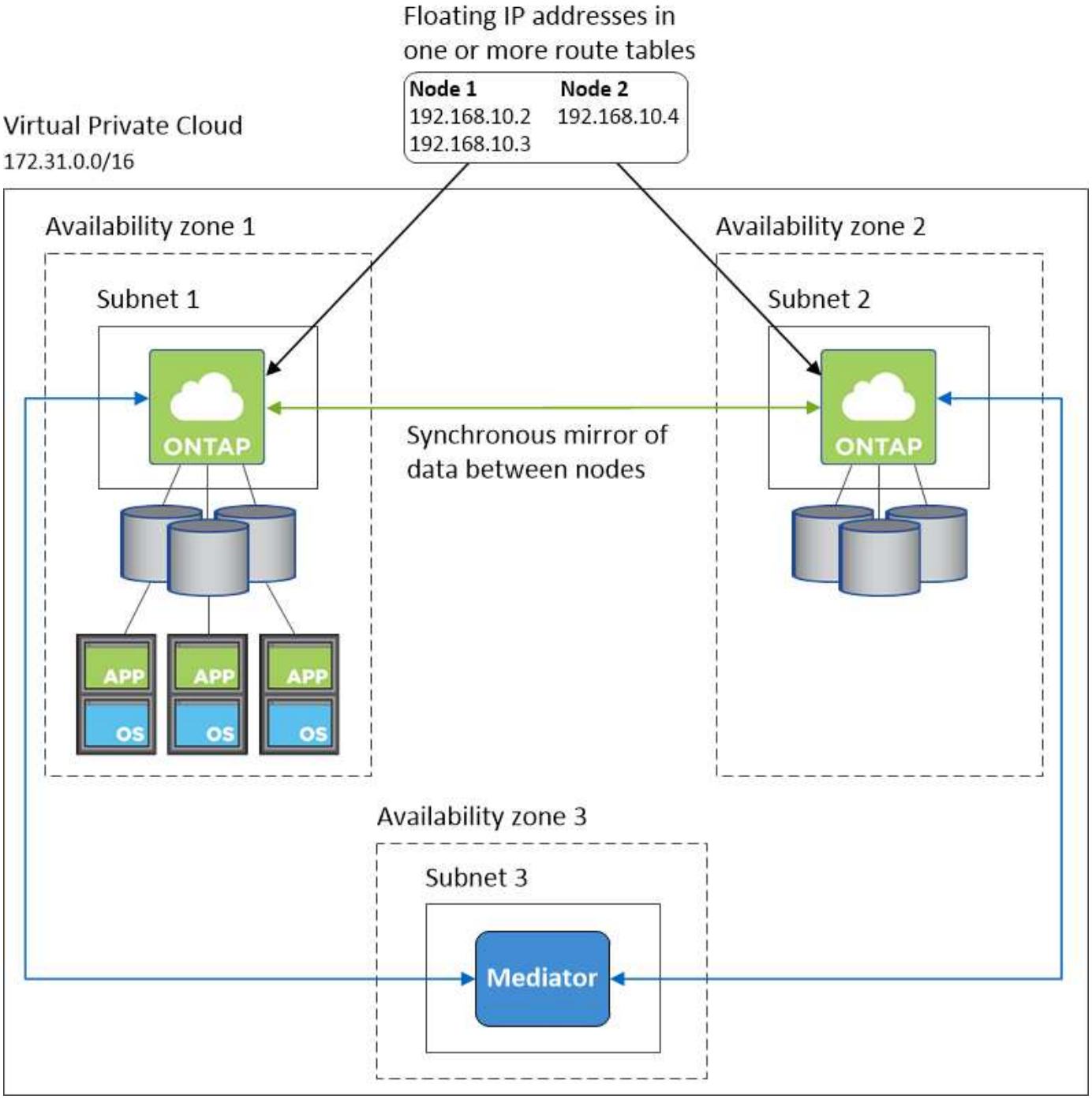
For more information about route tables, refer to AWS Documentation: Route Tables.

Connection to NetApp management tools

When deployed in multiple AZs, ONTAP Cloud 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 ONTAP Cloud HA configurations, they must be in the same VPC with similar routing configuration as NAS clients.

Example configuration

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



Sample VPC configurations

To better understand how you can deploy Cloud Manager and ONTAP Cloud 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

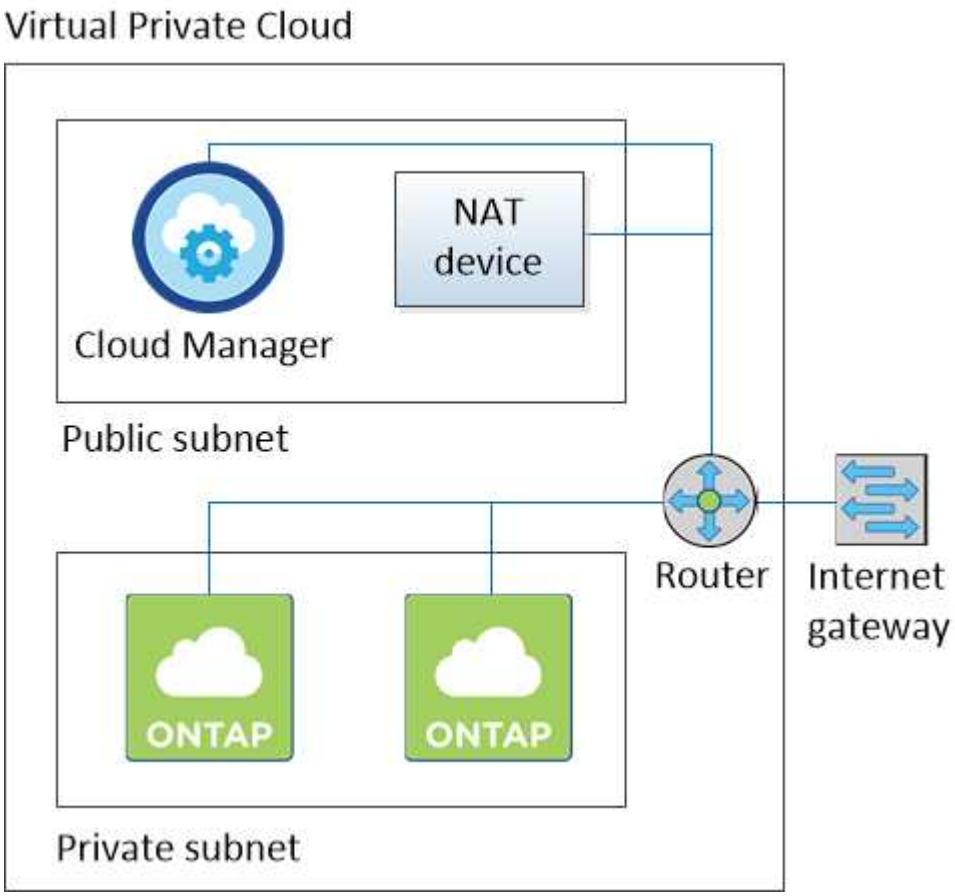
This VPC configuration includes public and private subnets, an internet gateway that connects the VPC to the internet, and a NAT gateway or NAT instance in the public subnet that enables outbound internet traffic from

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 ONTAP Cloud 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 ONTAP Cloud instances running in a private subnet:



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

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

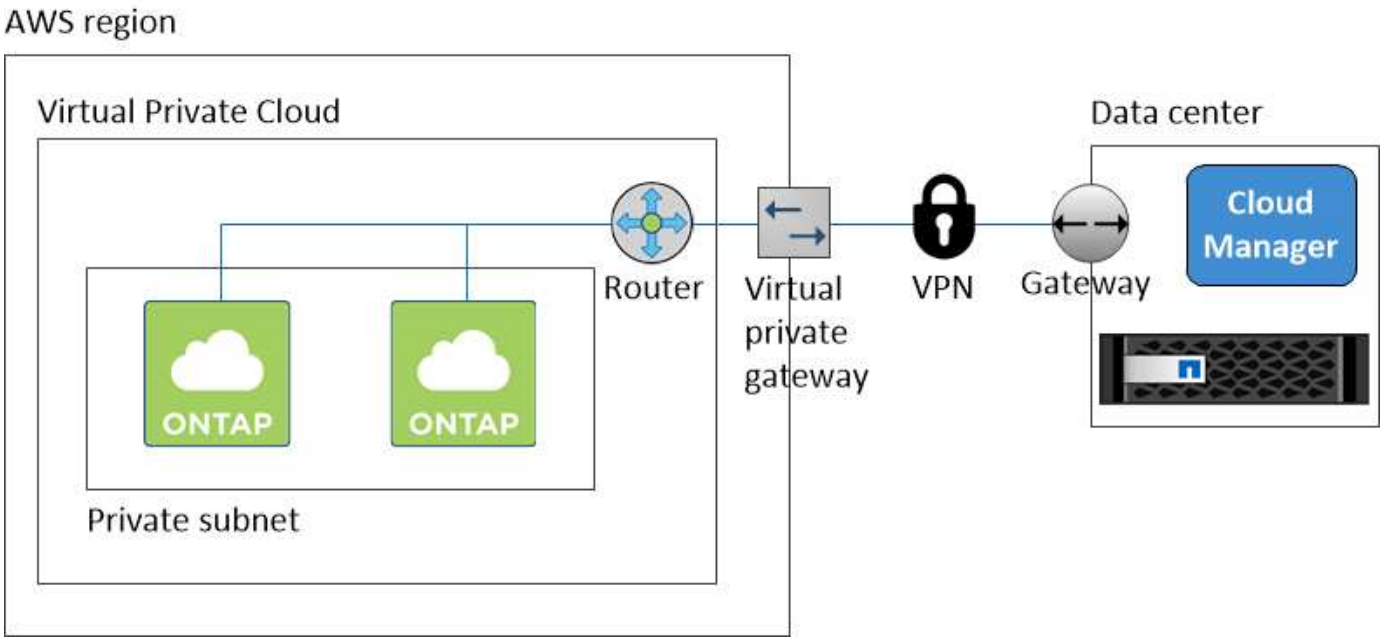
You can also use a proxy server in this configuration to allow internet access. The proxy server can be in your data center or in AWS.

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

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 ONTAP Cloud instances running in a private subnet:



Azure networking requirements

You must set up your Azure networking so that Cloud Manager can deploy ONTAP Cloud systems and so those systems can operate properly.

Outbound internet access for Cloud Manager

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

Endpoints	Purpose
https://management.azure.com https://login.microsoftonline.com	Enables Cloud Manager to deploy and manage ONTAP Cloud systems in most Azure regions.
https://management.microsoftazure.de https://login.microsoftonline.de	Enables Cloud Manager to deploy and manage ONTAP Cloud systems in the Azure Germany regions.
https://management.usgovcloudapi.net https://login.microsoftonline.com	Enables Cloud Manager to deploy and manage ONTAP Cloud systems in the Azure US Gov regions.
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 ONTAP Cloud upgrade images.
kinesis.us-east-1.amazonaws.com	Enables NetApp to stream data from audit records.

Endpoints	Purpose
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.
Various third-party locations, for example: https://repo1.maven.org/maven2 https://oss.sonatype.org/content/repositories https://repo.typesafe.org Third-party locations are subject to change.	During upgrades, Cloud Manager downloads the latest packages for third-party dependencies.

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.

Outbound internet access for ONTAP Cloud

ONTAP Cloud 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 ONTAP Cloud can send AutoSupport messages.

Outbound internet access from your web browser

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

Endpoint	Purpose
The Cloud Manager host	You must enter the host's IP address from a web browser to load the Cloud Manager console. If you deploy Cloud Manager in Azure, 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: • A jump host in the VNet that has a connection to Cloud Manager • A host in your network that has a VPN connection to the private IP address
https://netapp-cloud-account.auth0.com	Your web browser connects to this endpoint for centralized user authentication through NetApp Cloud Central.

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 between Cloud Manager and ONTAP Cloud subnets

Cloud Manager requires a connection to the subnets in which you deploy ONTAP Cloud systems.

If Cloud Manager is not installed in the target VNet, it must have network connectivity to that VNet. For example, if you install Cloud Manager in AWS or in your corporate network, you must set up a VPN connection to the VNet in which you deploy ONTAP Cloud systems.

Connections to ONTAP systems in other networks

To replicate data between an ONTAP Cloud 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.

IBM Cloud networking requirements

If you want to install Cloud Manager in the IBM Cloud, then the environment must meet a few requirements.

While you can install Cloud Manager in the IBM Cloud, ONTAP Cloud is not supported in the IBM Cloud.

Outbound internet access

Cloud Manager needs outbound internet access to communicate with AWS and Azure services when deploying ONTAP Cloud, to access software images for upgrades, and to enable technical support from NetApp.

For details about the specific endpoints, see AWS networking requirements and Azure networking requirements.

Connection between Cloud Manager and ONTAP Cloud subnets

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

Connection to the Cloud Manager web console

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

Endpoint	Purpose
The Cloud Manager host	You must enter the host's IP address from a web browser to load the Cloud Manager console. 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: • A jump host that has a connection to Cloud Manager • A host in your network that has a VPN connection to the private IP address

Endpoint	Purpose
https://netapp-cloud-account.auth0.com	Your web browser connects to this endpoint for centralized user authentication through NetApp Cloud Central.

Additional installation 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.

AWS EC2 instance type

t2.medium or m3.large

Azure VM size

A2 or D2_v2

Operating system

- 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

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

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.

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 ONTAP Cloud 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	a. Create an IAM role with the role type Amazon EC2 and attach the policy that you created in the previous step to the role. b. Attach the IAM role to Cloud Manager when you launch it from the AWS Marketplace (choose **Custom Launch**) or by modifying an existing instance from the EC2 console.
Grant permissions to IAM users	Attach the policy to IAM users or groups. For instructions, refer to AWS Documentation: Managing IAM Policies.

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.

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.

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.	a. On the Custom Launch tab, click **Launch with EC2 Console** for your region. b. Choose the t2.medium or m3.large instance type. c. Select a VPC, subnet, IAM role, and other configuration options that meet your requirements. d. Keep the default storage options. e. Enter tags for the instance, if desired. f. Specify the required connection methods for the Cloud Manager instance: SSH, HTTP, and HTTPS. g. Click **Launch**.
You do not want to associate the instance with an IAM role. You want to specify AWS keys for each Cloud Manager user account.	a. On the 1-Click Launch tab, specify settings for the instance. Note the following: ◦ The t2.medium and m3.large instance types are supported. ◦ Under security group, select **Create new based on seller settings** to create a pre-defined security group that includes the rules required by Cloud Manager. b. Click **Accept Terms and Launch with 1-Click**.

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.

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.

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 for your cloud service provider:
   - AWS networking requirements
   - Azure networking requirements
   - IBM Cloud networking requirements
2. Set up permissions for Cloud Manager:
   a. If you want to deploy ONTAP Cloud systems in AWS, set up an IAM role that includes the required permissions.
   b. If you want to deploy ONTAP Cloud systems 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-V3.4.0.sh
   ```

6. Run the installation script:

   ```
   ./OnCommandCloudManager-V3.4.0.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 ONTAP Cloud systems but you might want to perform additional setup first.

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. Grant Azure permissions to Cloud Manager.
3. 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.

4. Download and install Cloud Manager.

After you finish

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

Installing Cloud Manager in the Azure Germany region

The Azure Marketplace is not available in the Azure Germany region, 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. Grant Azure permissions to Cloud Manager.
3. Review Cloud Manager host requirements.
4. Download and install Cloud Manager.

After you finish

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