# Table of Contents

Administer Cloud Manager ................................................................. 1
   Finding your Cloud Manager system ID ........................................ 1
   Manage Connectors ................................................................. 1
   Manage credentials ................................................................... 17
   Managing users, workspaces, Connectors, and subscriptions .......... 43
   Managing an HTTPS certificate for secure access ......................... 49
   Removing Cloud Volumes ONTAP working environments .............. 51
   Configuring a Connector to use a proxy server ............................. 52
   Overriding CIFS locks for Cloud Volumes ONTAP HA in Azure .......... 53
   Reference ................................................................................. 54
Administer Cloud Manager

Finding your Cloud Manager system ID

To help you get started, your NetApp representative might ask you for your Cloud Manager system ID. The ID is typically used for licensing and troubleshooting purposes.

*What you’ll need*

You need to create a Connector before you can change Cloud Manager settings. Learn how.

*Steps*

1. In the upper right of the Cloud Manager console, click the Settings icon.

2. Click **Support Dashboard**.

   Your system ID appears in the top right.

*Example*

<table>
<thead>
<tr>
<th>Account</th>
<th>Workspace</th>
<th>Connector</th>
<th>Support Website</th>
</tr>
</thead>
<tbody>
<tr>
<td>MyAccount</td>
<td>Test</td>
<td>Connector1</td>
<td></td>
</tr>
</tbody>
</table>

Manage Connectors

*Managing existing Connectors*

After you create one or more Connectors, you can manage them by switching between Connectors, connecting to the local user interface running on a Connector, and more.
Switching between Connectors

If you have multiple Connectors, you can switch between them to see the Working Environments that are associated with a specific Connector.

For example, let's say that you're working in a multi-cloud environment. You might have one Connector in AWS and another in Google Cloud. You'd need to switch between those Connectors to manage the Cloud Volumes ONTAP systems running in those clouds.

**Step**

1. Click the **Connector** drop-down, select another Connector, and then click **Switch**.

Cloud Manager refreshes and shows the Working Environments associated with the selected Connector.

Accessing the local UI

While you should perform almost all tasks from the SaaS user interface, a local user interface is still available on the Connector. This interface is needed for a few tasks that need to be performed from the Connector itself:

- Setting a proxy server
• Installing a patch (you'll typically work with NetApp personnel to install a patch)
• Downloading AutoSupport messages (usually directed by NetApp personnel when you have issues)

Steps

1. **Log in to the Cloud Manager SaaS interface** from a machine that has a network connection to the Connector instance.

   If the Connector doesn’t have a public IP address, you'll need a VPN connection or you'll need to connect from a jump host that's in the same network as the Connector.

2. Click the **Connector** drop-down, click the action menu for a Connector, and then click **Go to Local UI**.

   ![Connector interface](image)

   The Cloud Manager interface running on the Connector loads in a new browser tab.

Removing Connectors from Cloud Manager

If a Connector is inactive, you can remove it from the list of Connectors in Cloud Manager. You might do this if you deleted the Connector virtual machine or if you uninstalled the Connector software.

Note the following about removing a Connector:

• This action doesn't delete the virtual machine.

• This action can't be reverted—once you remove a Connector from Cloud Manager, you can't add it back to Cloud Manager.
Steps
1. Click the Connector drop-down from the Cloud Manager header.
2. Click the action menu for an inactive Connector and click **Remove Connector**.
3. Enter the name of the Connector to confirm and then click Remove.

Result
Cloud Manager removes the Connector from its records.

Uninstalling the Connector software
The Connector includes an uninstallation script that you can use to uninstall the software to troubleshoot issues or to permanently remove the software from the host.

Step
1. From the Linux host, run the uninstallation script:

   `/opt/application/netapp/cloudmanager/bin/uninstall.sh [silent]`

   *silent* runs the script without prompting you for confirmation.

What about software upgrades?
The Connector automatically updates its software to the latest version, as long as it has **outbound internet access** to obtain the software update.

More ways to create Connectors

Connector host requirements
The Connector software must run on a host that meets specific operating system requirements, RAM requirements, port requirements, and so on.
A dedicated host is required

The Connector is not supported on a host that is shared with other applications. The host must be a dedicated host.

CPU

4 cores or 4 vCPUs

RAM

14 GB

AWS EC2 instance type

An instance type that meets the CPU and RAM requirements above. We recommend t3.xlarge and use that instance type when you deploy the Connector directly from Cloud Manager.

Azure VM size

An instance type that meets the CPU and RAM requirements above. We recommend DS3 v2 and use that VM size when you deploy the Connector directly from Cloud Manager.

GCP machine type

An instance type that meets the CPU and RAM requirements above. We recommend n1-standard-4 and use that machine type when you deploy the Connector directly from Cloud Manager.

Supported operating systems

- CentOS 7.6
- CentOS 7.7
- Red Hat Enterprise Linux 7.6
- Red Hat Enterprise Linux 7.7

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 Connector installation.

The Connector 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?

Disk space in /opt

100 GB of space must be available

Outbound internet access

Outbound internet access is required to install the Connector and for the Connector to manage resources and processes within your public cloud environment. For a list of endpoints, see
Networking requirements for the Connector.

Creating a Connector from the AWS Marketplace

It’s best to create a Connector directly from Cloud Manager, but you can launch a Connector from the AWS Marketplace, if you’d rather not specify AWS access keys. After you create and set up the Connector, Cloud Manager will automatically use it when you create new working environments.

Steps
1. Create an IAM policy and role for the EC2 instance:
   a. Download the Cloud Manager IAM policy from the following location:
      
      NetApp Cloud Manager: AWS, Azure, and GCP 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. Now go to the Cloud Manager page on the AWS Marketplace to deploy Cloud Manager from an AMI.

   The IAM user must have AWS Marketplace permissions to subscribe and unsubscribe.

3. On the Marketplace page, click Continue to Subscribe and then click Continue to Configuration.
4. Change any of the default options and click Continue to Launch.

5. Under Choose Action, select Launch through EC2 and then click Launch.

These 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 isn’t possible using the Launch from Website action.

6. Follow the prompts to configure and deploy the instance:
   - Choose Instance Type: Depending on region availability, choose one of the supported instance types (t3.xlarge is recommended).
Review the instance requirements.

- **Configure Instance**: Select a VPC and subnet, choose the IAM role that you created in step 1, enable termination protection (recommended), and choose any other configuration options that meet your requirements.

![Instance Configuration Screenshot]

- **Add Storage**: Keep the default storage options.
- **Add Tags**: Enter tags for the instance, if desired.
- **Configure Security Group**: Specify the required connection methods for the Connector instance: SSH, HTTP, and HTTPS.
- **Review**: Review your selections and click **Launch**.

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

7. Open a web browser from a host that has a connection to the Connector instance and enter the following URL:

   http://ipaddress:80

8. After you log in, set up the Connector:

   a. Specify the Cloud Central account to associate with the Connector.

      Learn about Cloud Central accounts.
b. Enter a name for the system.

Result
The Connector is now installed and set up with your Cloud Central account. Cloud Manager will automatically use this Connector when you create new working environments. But if you have more than one Connector, you'll need to switch between them.

Creating a Connector from the Azure Marketplace

It's best to create a Connector directly from Cloud Manager, but you can launch a Connector from the Azure Marketplace, if you prefer. After you create and set up the Connector, Cloud Manager will automatically use it when you create new working environments.

Creating a Connector in Azure

Deploy the Connector in Azure using the image in the Azure Marketplace and then log in to the Connector to specify your Cloud Central account.

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 a VM size that meets CPU and RAM requirements. We recommend DS3 v2.
     
     Review the VM requirements.
   - For the network security group, the Connector requires inbound connections using SSH, HTTP, and HTTPS.
     
     Learn more about security group rules for the Connector.
   - Under **Management**, enable **System assigned managed identity** for the Connector by selecting **On**.
     
     This setting is important because a managed identity allows the Connector 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 Connector software should be running in approximately five minutes.

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

   http://ipaddress:80

6. After you log in, set up the Connector:
   
   a. Specify the Cloud Central account to associate with the Connector.
     
     Learn about Cloud Central accounts.
   
   b. Enter a name for the system.
Result

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

Granting Azure permissions

When you deployed the Connector 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 Connector 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": [
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_3.8.7.json
```

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

2. Assign the role to the Connector 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 **Cloud Manager Operator** role.

     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 Connector virtual machine was created.

   - Select the Connector 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**

The Connector now has the permissions that it needs to manage resources and processes within your public cloud environment. Cloud Manager will automatically use this Connector when you create new working environments. But if you have more than one Connector, you’ll need to switch between them.

**Installing the Connector software on an existing Linux host**

The most common way to create a Connector is directly from Cloud Manager or from a cloud provider’s marketplace. But you have the option to download and install the Connector software on an existing Linux host in your network or in the cloud.
If you want to create a Cloud Volumes ONTAP system in Google Cloud, then you must have a Connector running in Google Cloud, as well. You can't use a Connector that’s running in another location.

Requirements

- The host must meet requirements for the Connector.
- 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 installation.
- The Connector installer accesses several URLs during the installation process. You must ensure that outbound internet access is allowed to these endpoints:
  - http://dev.mysql.com/get/mysql-community-release-el7-5.noarch.rpm

  The host might try to update operating system packages during installation. The host can contact different mirroring sites for these OS packages.

About this task

- Root privileges are not required to install the Connector.
- The installation 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. The Connector can operate successfully without the tools.

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

Steps

1. Download the Cloud Manager 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.

2. Assign permissions to execute the script.

   Example

   ```bash
   chmod +x OnCommandCloudManager-V3.8.4.sh
   ```
3. Run the installation script:

```
./OnCommandCloudManager-V3.8.4.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 host is behind a proxy server.

*proxyport* is the port for the proxy server.

*proxyuser* is the user name for the proxy server, if basic authentication is required.

*proxypwd* is the password for the user name that you specified.

4. Unless you specified the silent parameter, type Y to continue the script, and then enter the HTTP and HTTPS ports when prompted.

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

5. 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 host. For example, if the Connector 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 Connector 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

6. Sign up at NetApp Cloud Central or log in.

7. After you log in, set up Cloud Manager:
   a. Specify the Cloud Central account to associate with the Connector.
      
      Learn about Cloud Central accounts.
   
   b. Enter a name for the system.
Result

The Connector is now installed and set up with your Cloud Central account. Cloud Manager will automatically use this Connector when you create new working environments.

After you finish

Set up permissions so Cloud Manager can manage resources and processes within your public cloud environment:

- **AWS:** Set up an AWS account and then add it to Cloud Manager.
- **Azure:** Set up an Azure account and then add it to Cloud Manager.
- **GCP:** Set up a service account that has the permissions that Cloud Manager needs to create and manage Cloud Volumes ONTAP systems in projects.
  1. Create a role in GCP that includes the permissions defined in the Cloud Manager policy for GCP.
  2. Create a GCP service account and apply the custom role that you just created.
  3. Associate this service account with the Connector VM.
  4. If you want to deploy Cloud Volumes ONTAP in other projects, grant access by adding the service account with the Cloud Manager role to that project. You'll need to repeat this step for each project.
**Default configuration for the Connector**

If you need to troubleshoot the Connector, it might help to understand how it’s configured.

- If you deployed the Connector from Cloud Manager (or directly from a cloud provider’s marketplace), note the following:
  - In AWS, the user name for the EC2 Linux instance is ec2-user.
  - The operating system for the image is as follows:
    - AWS: Red Hat Enterprise Linux 7.5 (HVM)
    - Azure: Red Hat Enterprise Linux 7.6 (HVM)
    - GCP: CentOS 7.6
  
  The operating system does not include a GUI. You must use a terminal to access the system.

- The Connector installation folder resides in the following location:
  
  `/opt/application/netapp/cloudmanager`

- Log files are contained in the following folder:
  
  `/opt/application/netapp/cloudmanager/log`

- The Cloud Manager service is named occm.

- The occm service is dependent on the MySQL service.
  
  If the MySQL service is down, then the occm service is down too.

- Cloud Manager installs the following packages on the Linux host, if they are not already installed:
  - 7Zip
  - AWSCLI
  - Docker
  - Java
  - Kubectl
  - MySQL
  - Tridentctl
  - Pull
  - Wget

- The Connector uses the following ports on the Linux host:
  - 80 for HTTP access
- 443 for HTTPS access
- 3306 for the Cloud Manager database
- 8080 for the Cloud Manager API proxy
- 8666 for the Service Manager API
- 8777 for the Health-Checker Container Service API

Manage credentials

AWS

AWS credentials and permissions

Cloud Manager enables you to choose the AWS credentials to use when deploying Cloud Volumes ONTAP. You can deploy all of your Cloud Volumes ONTAP systems using the initial AWS credentials, or you can add additional credentials.

Initial AWS credentials

When you deploy a Connector from Cloud Manager, you need to use an AWS account that has permissions to launch the Connector instance. The required permissions are listed in the Connector deployment policy for AWS.

When Cloud Manager launches the Connector instance in AWS, it creates an IAM role and an instance profile for the instance. It also attaches a policy that provides Cloud Manager with permissions to manage resources and processes within that AWS account. Review how Cloud Manager uses the permissions.

Cloud Manager selects these AWS credentials by default when you create a new working environment for Cloud Volumes ONTAP:
Additional AWS credentials

If you want to launch Cloud Volumes ONTAP in different AWS accounts, then you can either provide AWS keys for an IAM user or the ARN of a role in a trusted account. The following image shows two additional accounts, one providing permissions through an IAM role in a trusted account and another through the AWS keys of an IAM user:

You would then add the account credentials to Cloud Manager by specifying the Amazon Resource Name (ARN) of the IAM role, or the AWS keys for the IAM user.

After you add another set of credentials, you can switch to them when creating a new working environment:
What about Marketplace deployments and on-prem deployments?

The sections above describe the recommended deployment method for the Connector, which is from Cloud Manager. You can also deploy a Connector in AWS from the AWS Marketplace and you can install the Connector on-premises.

If you use the Marketplace, permissions are provided in the same way. You just need to manually create and set up the IAM role, and then provide permissions for any additional accounts.

For on-premises deployments, you can’t set up an IAM role for the Cloud Manager system, but you can provide permissions just like you would for additional AWS accounts.
How can I securely rotate my AWS credentials?

As described above, Cloud Manager enables you to provide AWS credentials in a few ways: an IAM role associated with the Connector instance, by assuming an IAM role in a trusted account, or by providing AWS access keys.

With the first two options, Cloud Manager uses the AWS Security Token Service to obtain temporary credentials that rotate constantly. This process is the best practice—it’s automatic and it’s secure.

If you provide Cloud Manager with AWS access keys, you should rotate the keys by updating them in Cloud Manager at a regular interval. This is a completely manual process.

Managing AWS credentials and subscriptions for Cloud Manager

When you create a Cloud Volumes ONTAP system, you need to select the AWS credentials and subscription to use with that system. If you manage multiple AWS subscriptions, you can assign each one of them to different AWS credentials from the Credentials page.

Before you add AWS credentials to Cloud Manager, you need to provide the required permissions to that account. The permissions enable Cloud Manager to manage resources and processes within that AWS account. 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.

When you deployed a Connector from Cloud Manager, Cloud Manager automatically added AWS credentials for the account in which you deployed the Connector. This initial account is not added if you manually installed the Connector software on an existing system. Learn about AWS credentials and permissions.

Choices

• Granting permissions by providing AWS keys

• Granting permissions by assuming IAM roles in other accounts
How can I securely rotate my AWS credentials?

Cloud Manager enables you to provide AWS credentials in a few ways: an IAM role associated with the Connector instance, by assuming an IAM role in a trusted account, or by providing AWS access keys. Learn more about AWS credentials and permissions.

With the first two options, Cloud Manager uses the AWS Security Token Service to obtain temporary credentials that rotate constantly. This process is the best practice, it's automatic and it's secure.

If you provide Cloud Manager with AWS access keys, you should rotate the keys by updating them in Cloud Manager at a regular interval. This is a completely manual process.

Granting permissions by 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 Connector 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 Connector 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 Connector instance resides and select the IAM role that is attached to the instance.
   
a. Click Attach policies and then click Create policy.
   
b. Create a policy that includes the "sts:AssumeRole" action and the ARN of the role that you created in the target account.

   **Example**

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

   **Result**

   The account now has the required permissions. You can now add it to Cloud Manager.

Adding AWS credentials to Cloud Manager

After you provide an AWS account with the required permissions, you can add the credentials for that 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 Settings icon, and select **Credentials**.

2. Click **Add Credentials** and select **AWS**.

3. Provide AWS keys or the ARN of a trusted IAM role.

4. Confirm that the policy requirements have been met and click **Continue**.

5. Choose the pay-as-you-go subscription that you want to associate with the credentials, or click **Add Subscription** if you don’t have one yet.
To create a pay-as-you-go Cloud Volumes ONTAP system, AWS credentials must be associated with a subscription to Cloud Volumes ONTAP from the AWS Marketplace.

6. Click **Add**.

**Result**

You can now switch to a different set of credentials from the Details and Credentials page when creating a new working environment:

---

**Edit Account & Add Subscription**

**Credentials**

<table>
<thead>
<tr>
<th>Keyst</th>
<th>Account ID: [redacted]</th>
</tr>
</thead>
</table>

| Instance Profile | Account ID: [redacted] |

**Associate Subscription to Credentials**

To create a pay-as-you-go Cloud Volumes ONTAP system, you need to select AWS credentials that are associated with a subscription to Cloud Volumes ONTAP from the AWS Marketplace.

**Add Subscription**

---

**Associating an AWS subscription to credentials**

After you add your AWS credentials to Cloud Manager, you can associate an AWS Marketplace subscription with those credentials. The subscription enables you to create a pay-as-you-go Cloud Volumes ONTAP system, and to use other NetApp cloud services.
There are two scenarios in which you might associate an AWS Marketplace subscription after you’ve already added the credentials to Cloud Manager:

- You didn’t associate a subscription when you initially added the credentials to Cloud Manager.
- You want to replace an existing AWS Marketplace subscription with a new subscription.

What you’ll need

You need to create a Connector before you can change Cloud Manager settings. Learn how.

Steps

1. In the upper right of the Cloud Manager console, click the Settings icon, and select **Credentials**.
2. Hover over a set of credentials and click the action menu.
3. From the menu, click **Associate Subscription**.

4. Select a subscription from the down-down list or click **Add Subscription** and follow the steps to create a new subscription.

https://docs.netapp.com/us-en/occm/media/video_subscribing_aws.mp4 (video)

Azure

Azure credentials and permissions

Cloud Manager enables you to choose the Azure credentials to use when deploying Cloud Volumes ONTAP. You can deploy all of your Cloud Volumes ONTAP systems using the initial Azure credentials, or you can add additional credentials.

Initial Azure credentials

When you deploy a Connector from Cloud Manager, you need to use an Azure account that has permissions to deploy the Connector virtual machine. The required permissions are listed in the **Connector deployment policy for Azure**.
When Cloud Manager deploys the Connector virtual machine in Azure, it enables a system-assigned managed identity on virtual machine, creates a custom role, and assigns it to the virtual machine. The role provides Cloud Manager with permissions to manage resources and processes within that Azure subscription. Review how Cloud Manager uses the permissions.

Cloud Manager selects these Azure credentials by default when you create a new working environment for Cloud Volumes ONTAP:

<table>
<thead>
<tr>
<th>Details &amp; Credentials</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managed Service Identity</td>
</tr>
<tr>
<td>Credential Name</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

Additional Azure subscriptions for a managed identity

The managed identity is associated with the subscription in which you launched the Connector. If you want to select a different Azure subscription, then you need to associate the managed identity with those subscriptions.

Additional Azure credentials

If you want to deploy Cloud Volumes ONTAP using different Azure credentials, then you must grant the required permissions by creating and setting up a service principal in Azure Active Directory for each Azure account. The following image shows two additional accounts, each set up with a service principal and custom role that provides permissions:
You would then add the account credentials to Cloud Manager by providing details about the AD service principal.

After you add another set of credentials, you can switch to them when creating a new working environment:

What about Marketplace deployments and on-prem deployments?

The sections above describe the recommended deployment method for the Connector, which is from NetApp Cloud Central. You can also deploy a Connector in Azure from the Azure Marketplace, and you can install the Connector on-premises.

If you use the Marketplace, permissions are provided in the same way. You just need to manually create and set up the managed identity for the Connector, and then provide permissions for any additional accounts.

For on-premises deployments, you can't set up a managed identity for the Connector, but you can provide permissions just like you would for additional accounts by using a service principal.
Managing Azure credentials and subscriptions for Cloud Manager

When you create a Cloud Volumes ONTAP system, you need to select the Azure credentials and Marketplace subscription to use with that system. If you manage multiple Azure Marketplace subscriptions, you can assign each one of them to different Azure credentials from the Credentials page.

There are two ways to manage Azure credentials in Cloud Manager. First, if you want to deploy Cloud Volumes ONTAP in different Azure accounts, then you need to provide the required permissions and add the credentials to Cloud Manager. The second way is to associate additional subscriptions with the Azure managed identity.

When you deploy a Connector from Cloud Manager, Cloud Manager automatically adds the Azure account in which you deployed the Connector. An initial account is not added if you manually installed the Connector software on an existing system. Learn about Azure accounts and permissions.

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.
Steps

1. Create an Azure Active Directory application.
2. Assign the application to a role.
4. Get the application ID and directory ID.
5. Create a client secret.

Creating an Azure Active Directory application

Create an Azure Active Directory (AD) application and service principal that Cloud Manager can use for role-based access control.

Before you begin

You must have the right permissions in Azure to create an Active Directory application and to assign the application to a role. For details, refer to Microsoft Azure Documentation: Required permissions.

Steps

1. From the Azure portal, open the Azure Active Directory service.
2. In the menu, click **App registrations**.
3. Click **New registration**.
4. Specify details about the application:
   - **Name**: Enter a name for the application.
   - **Account type**: Select an account type (any will work with Cloud Manager).
   - **Redirect URI**: Select **Web** and then enter any URL—for example, https://url
5. Click **Register**.

**Result**
You’ve created the AD application and service principal.

**Assigning the application to a role**
You must bind the service principal to one or more Azure subscriptions and assign it the custom "OnCommand Cloud Manager Operator" role so Cloud Manager has permissions in Azure.

**Steps**
1. Create a custom role:
   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**

```json
"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_3.8.7.json
```

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

2. Assign the application to the role:
   a. From the Azure portal, open the **Subscriptions** service.
   b. Select the subscription.
   c. Click **Access control (IAM)** > **Add** > **Add role assignment**.
   d. Select the **Cloud Manager Operator** role.
   e. Keep **Azure AD user, group, or service principal** selected.
   f. Search for the name of the application (you can’t find it in the list by scrolling).
   
   ![Add role assignment](image)

   g. Select the application and click **Save**.

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

   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.

**Adding Windows Azure Service Management API permissions**

The service principal must have "Windows Azure Service Management API" permissions.

**Steps**

1. In the **Azure Active Directory** service, click **App registrations** and select the application.
2. Click **API permissions > Add a permission.**

3. Under **Microsoft APIs**, select **Azure Service Management.**

### Request API permissions

**Select an API**

<table>
<thead>
<tr>
<th>Microsoft APIs</th>
<th>APIs my organization uses</th>
<th>My APIs</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Commonly used Microsoft APIs</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Microsoft Graph</strong></td>
<td>Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.</td>
<td></td>
</tr>
<tr>
<td><strong>Azure Batch</strong></td>
<td>Schedule large-scale parallel and HPC applications in the cloud</td>
<td></td>
</tr>
<tr>
<td><strong>Azure Data Catalog</strong></td>
<td>Programmatic access to Data Catalog resources to register, annotate and search data assets</td>
<td></td>
</tr>
<tr>
<td><strong>Azure Data Explorer</strong></td>
<td>Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions</td>
<td></td>
</tr>
<tr>
<td><strong>Azure Data Lake</strong></td>
<td>Access to storage and compute for big data analytic scenarios</td>
<td></td>
</tr>
<tr>
<td><strong>Azure DevOps</strong></td>
<td>Integrate with Azure DevOps and Azure DevOps server</td>
<td></td>
</tr>
<tr>
<td><strong>Azure Import/Export</strong></td>
<td>Programmatic control of import/export jobs</td>
<td></td>
</tr>
<tr>
<td><strong>Azure Key Vault</strong></td>
<td>Manage your key vaults as well as the keys, secrets, and certificates within your Key Vault</td>
<td></td>
</tr>
<tr>
<td><strong>Azure Rights Management</strong></td>
<td>Allow validated users to read and write protected content</td>
<td></td>
</tr>
<tr>
<td><strong>Azure Service Management</strong></td>
<td><strong>Programmatic access to much of the functionality available through the Azure portal</strong></td>
<td><strong>Exclamation mark</strong></td>
</tr>
<tr>
<td><strong>Azure Storage</strong></td>
<td>Secure, massively scalable object and data lake storage for unstructured and semi-structured data</td>
<td></td>
</tr>
<tr>
<td><strong>Customer Insights</strong></td>
<td>Create profile and interaction models for your products</td>
<td></td>
</tr>
<tr>
<td><strong>Data Export Service for Microsoft Dynamics 365</strong></td>
<td>Export data from Microsoft Dynamics CRM organization to an external destination</td>
<td></td>
</tr>
</tbody>
</table>

4. Click **Access Azure Service Management as organization users** and then click **Add permissions.**
Getting the application ID and directory ID

When you add the Azure account to Cloud Manager, you need to provide the application (client) ID and the directory (tenant) ID for the application. Cloud Manager uses the IDs to programmatically sign in.

Steps

1. In the Azure Active Directory service, click App registrations and select the application.
2. Copy the Application (client) ID and the Directory (tenant) ID.

Creating a client secret

You need to create a client secret and then provide Cloud Manager with the value of the secret so Cloud Manager can use it to authenticate with Azure AD.

When you add the account to Cloud Manager, Cloud Manager refers to the client secret as the Application Key.
Steps
1. Open the Azure Active Directory service.
2. Click App registrations and select your application.
3. Click Certificates & secrets > New client secret.
4. Provide a description of the secret and a duration.
5. Click Add.
6. Copy the value of the client secret.

Result
Your service principal is now setup and you should have copied the application (client) ID, the directory (tenant) ID, and the value of the client secret. You need to enter this information in Cloud Manager when you add an Azure account.

Adding Azure credentials to Cloud Manager

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

What you'll need
You need to create a Connector before you can change Cloud Manager settings. Learn how.

Steps
1. In the upper right of the Cloud Manager console, click the Settings icon, and select Credentials.
2. Click Add Credentials and select Microsoft Azure.
3. Enter information about the Azure Active Directory service principal that grants the required permissions:
   - Application (client) ID: See Getting the application ID and directory ID.
Directory (tenant) ID: See Getting the application ID and directory ID.

Client Secret: See Creating a client secret.

4. Confirm that the policy requirements have been met and then click Continue.

5. Choose the pay-as-you-go subscription that you want to associate with the credentials, or click Add Subscription if you don’t have one yet.

To create a pay-as-you-go Cloud Volumes ONTAP system, Azure credentials must be associated with a subscription to Cloud Volumes ONTAP from the Azure Marketplace.

6. Click Add.

Result
You can now switch to different set of credentials from the Details and Credentials page when creating a new working environment:

Edit Account & Add Subscription

<table>
<thead>
<tr>
<th>cloud-manager-app</th>
<th>Application ID: 57c42424-88a0-480a</th>
</tr>
</thead>
</table>

Managed Service Identity

OCCM QA1 (Default)

Associating an Azure Marketplace subscription to credentials

After you add your Azure credentials to Cloud Manager, you can associate an Azure Marketplace subscription to those credentials. The subscription enables you to create a pay-as-you-go Cloud Volumes ONTAP system, and to use other NetApp cloud services.

There are two scenarios in which you might associate an Azure Marketplace subscription after you’ve already added the credentials to Cloud Manager:

- You didn’t associate a subscription when you initially added the credentials to Cloud Manager.
- You want to replace an existing Azure Marketplace subscription with a new subscription.

What you’ll need
You need to create a Connector before you can change Cloud Manager settings. Learn how.
**Steps**

1. In the upper right of the Cloud Manager console, click the Settings icon, and select **Credentials**.

2. Hover over a set of credentials and click the action menu.

3. From the menu, click **Associate Subscription**.

![Associate Subscription](https://docs.netapp.com/us-en/occm/media/video_subscribing_azure.mp4)

4. Select a subscription from the down-down list or click **Add Subscription** and follow the steps to create a new subscription.

   The following video starts from the context of the working environment wizard, but shows you the same workflow after you click **Add Subscription**:

   ![Video Link](https://docs.netapp.com/us-en/occm/media/video_subscribing_azure.mp4) (video)

**Associating additional Azure subscriptions with a managed identity**

Cloud Manager enables you to choose the Azure credentials and Azure 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 Azure account** when you deploy a Connector from Cloud Manager. When you deployed the Connector, Cloud Manager created the Cloud Manager Operator role and assigned it to the Connector 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.

3. Click **Access control (IAM)**.
   a. Click **Add > Add role assignment** and then add the permissions:
      - Select the **Cloud Manager Operator** role.
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 Connector virtual machine was created.
- Select the Connector 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.

---

**GCP**

**Google Cloud projects, permissions, and accounts**

A service account provides Cloud Manager with permissions to deploy and manage Cloud Volumes ONTAP systems in the same project as Cloud Manager, or in different projects.
Project and permissions for Cloud Manager

Before you can deploy Cloud Volumes ONTAP in Google Cloud, you must first deploy a Connector in a Google Cloud project. The Connector can’t be running on your premises, or in a different cloud provider.

Two sets of permissions must be in place before you deploy a Connector directly from Cloud Manager:

1. You need to deploy a Connector using a Google account that has permissions to launch the Connector VM instance from Cloud Manager.

2. When deploying the Connector, you are prompted to select a service account for the VM instance. Cloud Manager gets permissions from the service account to create and manage Cloud Volumes ONTAP systems on your behalf. Permissions are provided by attaching a custom role to the service account.

We have set up two YAML files that include the required permissions for the user and the service account. Learn how to use the YAML files to set up permissions.

The following image depicts the permission requirements described in numbers 1 and 2 above:

![Permission Diagram]

Project for Cloud Volumes ONTAP

Cloud Volumes ONTAP can reside in the same project as the Connector, or in a different project. To deploy Cloud Volumes ONTAP in a different project, you need to first add the Connector service account and role to that project.

- Learn how to set up service account (see step 2).
- Learn how to deploy Cloud Volumes ONTAP in GCP and select a project.
Account for data tiering

Cloud Manager requires a GCP account for Cloud Volumes ONTAP 9.6, but not for 9.7 and later. If you want to use data tiering with Cloud Volumes ONTAP 9.7, then follow step 4 in Getting started with Cloud Volumes ONTAP in Google Cloud Platform.

Adding a Google Cloud account to Cloud Manager is required to enable data tiering on a Cloud Volumes ONTAP 9.6 system. Data tiering automatically tiers cold data to low-cost object storage, enabling you to reclaim space on your primary storage and shrink secondary storage.

When you add the account, you need to provide Cloud Manager with a storage access key for a service account that has Storage Admin permissions. Cloud Manager uses the access keys to set up and manage a Cloud Storage bucket for data tiering.

After you add a Google Cloud account, you can then enable data tiering on individual volumes when you create, modify, or replicate them.

- Learn how to set up and add GCP accounts to Cloud Manager.
- Learn how to tier inactive data to low-cost object storage.

Managing GCP credentials and subscriptions for Cloud Manager

You can manage two types of Google Cloud Platform credentials from Cloud Manager: the credentials that are associated with the Connector VM instance and storage access keys used with a Cloud Volumes ONTAP 9.6 system for data tiering.

Associating a Marketplace subscription with GCP credentials

When you deploy a Connector in GCP, Cloud Manager creates a default set of credentials that are associated with the Connector VM instance. These are the credentials that Cloud Manager uses to deploy Cloud Volumes ONTAP.

At any time, you can change the Marketplace subscription that’s associated with these credentials. The subscription enables you to create a pay-as-you-go Cloud Volumes ONTAP system, and to use other NetApp cloud services.

Steps

1. In the upper right of the Cloud Manager console, click the Settings icon, and select Credentials.
2. Hover over a set of credentials and click the action menu.
3. From the menu, click Associate Subscription.
4. Select a Google Cloud project and subscription from the down-down list or click **Add Subscription** and follow the steps to create a new subscription.

5. Click **Associate**.

**Setting up and adding GCP accounts for data tiering with Cloud Volumes ONTAP 9.6**

If you want to enable a Cloud Volumes ONTAP 9.6 system for **data tiering**, you need to provide Cloud Manager with a storage access key for a service account that has Storage Admin permissions. Cloud Manager uses the access keys to set up and manage a Cloud Storage bucket for data tiering.

If you want to use data tiering with Cloud Volumes ONTAP 9.7, then follow step 4 in **Getting started with Cloud Volumes ONTAP in Google Cloud Platform**.

**Setting up a service account and access keys for Google Cloud Storage**

A service account enables Cloud Manager to authenticate and access Cloud Storage buckets used for data tiering. The keys are required so that Google Cloud Storage knows who is making the request.

**Steps**

1. Open the GCP IAM console and create a service account that has the Storage Admin role.
2. Go to GCP Storage Settings.
3. If you're prompted, select a project.
4. Click the Interoperability tab.
5. If you haven’t already done so, click Enable interoperability access.
6. Under Access keys for service accounts, click Create a key for a service account.
7. Select the service account that you created in step 1.
8. Click **Create Key**.

9. Copy the access key and secret.

   You’ll need to enter this information in Cloud Manager when you add the GCP account for data tiering.

### Adding a GCP account to Cloud Manager

Now that you have an access key for a service account, you can add it to Cloud Manager.

**What you’ll need**

You need to create a Connector before you can change Cloud Manager settings. [Learn how](#).

**Steps**

1. In the upper right of the Cloud Manager console, click the Settings icon, and select **Credentials**.

2. Click **Add Credentials** and select **Google Cloud**.

3. Enter the access key and secret for the service account.

   The keys enable Cloud Manager to set up a Cloud Storage bucket for data tiering.

4. Confirm that the policy requirements have been met and then click **Create Account**.

**What’s next?**

You can now enable data tiering on individual volumes on a Cloud Volumes ONTAP 9.6 system when you create, modify, or replicate them. For details, see [Tiering inactive data to low-cost object storage](#).

But before you do, be sure that the subnet in which Cloud Volumes ONTAP resides is configured for Private Google Access. For instructions, refer to [Google Cloud Documentation: Configuring Private Google Access](#).

### 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.
What you’ll need
You need to create a Connector before you can change Cloud Manager settings. Learn how.

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 Settings icon, and select Credentials.
3. Click Add Credentials 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.
Managing users, workspaces, Connectors, and subscriptions

After you perform initial setup, you might need to administer your account settings later by managing users, workspaces, Connectors, and subscriptions.

Learn more about how Cloud Central accounts work.

Adding users

Associate Cloud Central users with the Cloud Central account so those users can create and manage working environments in Cloud Manager.

Steps

1. If the user hasn't already done so, ask the user to go to NetApp Cloud Central and sign up.
2. From the top of Cloud Manager, click the Account drop-down.
3. Click Manage Account next to the currently selected account.
4. From the Users tab, click **Associate User**.

5. Enter the user’s email address and select a role for the user:
   - **Account Admin**: Can perform any action in Cloud Manager.
   - **Workspace Admin**: Can create and manage resources in assigned workspaces.
   - **Compliance Viewer**: Can only view compliance information and generate reports for workspaces that they have permission to access.

6. If you selected Workspace Admin or Compliance Viewer, select one or more workspaces to associate with that user.
7. Click **Associate User**.

**Result**
The user should receive an email from NetApp Cloud Central titled "Account Association." The email includes the information needed to access Cloud Manager.

**Removing users**

Disassociating a user makes it so they can no longer access the resources in a Cloud Central account.

**Steps**
1. From the top of Cloud Manager, click the **Account** drop-down and click **Manage Account**.
2. From the Users tab, click the action menu in the row that corresponds to the user.

3. Click **Disassociate User** and click **Disassociate** to confirm.

**Result**

The user can no longer access the resources in this Cloud Central account.

**Managing a Workspace Admin’s workspaces**

You can associate and disassociate Workspace Admins with workspaces at any time. Associating the user enables them to create and view the working environments in that workspace.

**Steps**

1. From the top of Cloud Manager, click the **Account** drop-down and click **Manage Account**.
2. From the Users tab, click the action menu in the row that corresponds to the user.

3. Click **Manage Workspaces**.

4. Select the workspaces to associate with the user and click **Apply**.

**Result**
The user can now access those workspaces from Cloud Manager, as long as the Connector was also associated with the workspaces.

**Managing workspaces**
Manage your workspaces by creating, renaming, and deleting them. Note that you can’t delete a workspace if it contains any resources. It must be empty.

**Steps**
1. From the top of Cloud Manager, click the **Account** drop-down and click **Manage Account**.
2. Click **Workspaces**.
3. Choose one of the following options:
   - Click **Add New Workspace** to create a new workspace.
   - Click **Rename** to rename the workspace.
Managing a Connector’s workspaces

You need to associate the Connector with workspaces so Workspace Admins can access those workspaces from Cloud Manager.

If you only have Account Admins, then associating the Connector with workspaces isn’t required. Account Admins have the ability to access all workspaces in Cloud Manager by default.

Learn more about users, workspaces, and Connectors.

Steps

1. From the top of Cloud Manager, click the Account drop-down and click Manage Account.
2. Click Connector.
3. Click Manage Workspaces for the Connector that you want to associate.
4. Select the workspaces to associate with the Connector and click Apply.

Managing subscriptions

After you subscribe from a cloud provider’s marketplace, each subscription is available from the Account Settings widget. You have the option to rename a subscription and to disassociate the subscription from one or more accounts.

For example, let’s say that you have two accounts and each is billed through separate subscriptions. You might disassociate a subscription from one of the accounts so the users in that account don’t accidentally choose the wrong subscription when creating a Cloud Volume ONTAP working environment.

Learn more about subscriptions.

Steps

1. From the top of Cloud Manager, click the Account drop-down and click Manage Account.
2. Click Subscriptions.

You’ll only see the subscriptions that are associated with the account that you’re currently viewing.

3. Click the action menu in the row that corresponds to the subscription that you want to manage.
4. Choose to rename the subscription or to manage the accounts that are associated with the subscription.

**Changing the account name**

Change your account name at any time to change it to something meaningful for you.

*Steps*

1. From the top of Cloud Manager, click the Account drop-down and click **Manage Account**.
2. In the **Overview** tab, click the edit icon next to the account name.
3. Type a new account name and click **Save**.

**Enabling or disabling the SaaS platform**

We don’t recommend disabling the SaaS platform unless you need to in order to comply with your company’s security policies. Disabling the SaaS platform limits your ability to use NetApp’s integrated cloud services.

The following services aren’t available from Cloud Manager if you disable the SaaS platform:

- Cloud Compliance
- Kubernetes
- Cloud Tiering
- Global File Cache
- Monitoring (Cloud Insights)

*Steps*

1. From the top of Cloud Manager, click the Account drop-down and click **Manage Account**.
2. In the **Overview** tab, toggle the option to enable use the SaaS platform.

**Managing 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.

**Before you get started**

You need to create a Connector before you can change Cloud Manager settings. [Learn how.](#)

**Installing an HTTPS certificate**

Install a certificate signed by a CA for secure access.

**Steps**

1. In the upper right of the Cloud Manager console, click the Settings icon, and 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:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Generate a CSR              | a. Enter the host name or DNS of the Connector 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 | 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. |
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

Renewing the Cloud Manager HTTPS certificate

You should renew the Cloud Manager HTTPS certificate before it expires to ensure secure access to the Cloud Manager web console. If you do not renew the certificate before it expires, a warning appears when users access the web console using HTTPS.

**Steps**

1. In the upper right of the Cloud Manager console, click the Settings icon, and select **HTTPS Setup**.

   Details about the Cloud Manager certificate displays, including the expiration date.

2. Click **Renew HTTPS Certificate** and follow the steps to generate a CSR or install your own CA-signed certificate.

**Result**

Cloud Manager uses the new CA-signed certificate to provide secure HTTPS access.

Removing Cloud Volumes ONTAP working environments

The Account Admin can remove a Cloud Volumes ONTAP working environment to move it to another system or to troubleshoot discovery issues.

**About this task**

Removing a Cloud Volumes ONTAP working environment removes it from Cloud Manager. It does not delete the Cloud Volumes ONTAP system. You can later rediscover the working environment.
Removing a working environment from Cloud Manager enables you to do the following:

- Rediscover it in another workspace
- Rediscover it from another Cloud Manager system
- Rediscover it if you had problems during the initial discovery

Steps
1. In the upper right of the Cloud Manager console, click the Settings icon, and select **Tools**.

2. From the Tools page, click **Launch**.
3. Select the Cloud Volumes ONTAP working environment that you want to remove.
4. On the Review and Approve page, click **Go**.

Result
Cloud Manager removes the working environment. Users can rediscover this working environment from the Working Environments page at any time.

**Configuring a Connector to use a proxy server**

If your corporate policies dictate that you use a proxy server for all HTTP communication to the internet, then you must configure your Connectors to use that proxy server. The proxy server can be in the cloud or in your network.

When you configure a Connector to use a proxy server, that Connector and the Cloud Volumes ONTAP systems that it manages (including any HA mediators), all use the proxy server.

Steps
1. **Log in to the Cloud Manager SaaS interface** from a machine that has a network connection to the Connector instance.

   If the Connector doesn’t have a public IP address, you’ll need a VPN connection or you’ll need to connect from a jump host that’s in the same network as the Connector.

2. Click the **Connector** drop-down and then click **Go to local UI** for a specific Connector.
The Cloud Manager interface running on the Connector loads in a new browser tab.

3. In the upper right of the Cloud Manager console, click the Settings icon, and select **Cloud Manager Settings**.

4. Under HTTP Proxy, enter the server using the syntax `http://address:port`, specify a user name and password if basic authentication is required for the server, and then click **Save**.

   Cloud Manager doesn’t support passwords that include the @ character.

*Result*

After you specify the proxy server, new Cloud Volumes ONTAP systems are automatically configured to use the proxy server when sending AutoSupport messages. If you didn't specify the proxy server before users create Cloud Volumes ONTAP systems, then they must use System Manager to manually set the proxy server in the AutoSupport options for each system.

**Overriding CIFS locks for Cloud Volumes ONTAP HA in Azure**

The Account Admin can enable a setting in Cloud Manager that prevents issues
with Cloud Volumes ONTAP storage failover during Azure maintenance events. When you enable this setting, Cloud Volumes ONTAP vetoes CIFS locks and resets active CIFS sessions.

About this task
Microsoft Azure schedules periodic maintenance events on its virtual machines. When a maintenance event occurs on a node in a Cloud Volumes ONTAP HA pair, the HA pair initiates storage takeover. If there are active CIFS sessions during this maintenance event, the locks on CIFS files can prevent storage failover.

If you enable this setting, Cloud Volumes ONTAP will veto the locks and reset the active CIFS sessions. As a result, the HA pair can complete storage failover during these maintenance events.

This process might be disruptive to CIFS clients. Data that is not committed from CIFS clients could be lost.

What you'll need
You need to create a Connector before you can change Cloud Manager settings. Learn how.

Steps
1. In the upper right of the Cloud Manager console, click the Settings icon, and select Cloud Manager Settings.

2. Under HA CIFS Locks, select the checkbox and click Save.

Reference

Roles
The Account Admin, Workspace Admin, and Cloud Compliance Viewer roles provide specific permissions to users.

<table>
<thead>
<tr>
<th>Task</th>
<th>Account Admin</th>
<th>Workspace Admin</th>
<th>Cloud Compliance Viewer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage working environments</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Enable services on working environments</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Task</td>
<td>Account Admin</td>
<td>Workspace Admin</td>
<td>Cloud Compliance Viewer</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>---------------</td>
<td>-----------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>View data replication status</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>View the timeline</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Switch between workspaces</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>View Compliance scan results</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Delete working environments</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Connect Kubernetes clusters to working environments</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Receive the Cloud Volumes ONTAP report</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Create Connectors</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Manage Cloud Central accounts</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Manage credentials</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Modify Cloud Manager settings</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>View and manage the Support Dashboard</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Remove working environments from Cloud Manager</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Install an HTTPS certificate</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Related links**

- Setting up workspaces and users in the Cloud Central account
- Managing workspaces and users in the Cloud Central account

**How Cloud Manager uses cloud provider permissions**

Cloud Manager requires permissions to perform actions in your cloud provider. These permissions are included in the policies provided by NetApp. You might want to understand what Cloud Manager does with these permissions.

**What Cloud Manager does with AWS permissions**

Cloud Manager uses an AWS account to make API calls to several AWS services, including EC2, S3, CloudFormation, IAM, the Security Token Service (STS), and the Key Management Service (KMS).
<table>
<thead>
<tr>
<th>Actions</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;ec2:StartInstances&quot;, &quot;ec2:StopInstances&quot;, &quot;ec2:DescribeInstances&quot;,</td>
<td>Launches a Cloud Volumes ONTAP instance and stops, starts, and monitors</td>
</tr>
<tr>
<td>&quot;ec2:DescribeInstanceStatus&quot;, &quot;ec2:RunInstances&quot;, &quot;ec2:TerminateInstances&quot;,</td>
<td>the instance.</td>
</tr>
<tr>
<td>&quot;ec2:ModifyInstanceAttribute&quot;,</td>
<td></td>
</tr>
<tr>
<td>&quot;ec2:DescribeInstanceAttribute&quot;,</td>
<td>Verifies that enhanced networking is enabled for supported instance types.</td>
</tr>
<tr>
<td>&quot;ec2:DescribeRouteTables&quot;, &quot;ec2:DescribeImages&quot;,</td>
<td>Launches a Cloud Volumes ONTAP HA configuration.</td>
</tr>
<tr>
<td>&quot;ec2:CreateTags&quot;,</td>
<td></td>
</tr>
<tr>
<td>&quot;ec2:CreateVolume&quot;, &quot;ec2:DescribeVolumes&quot;, &quot;ec2:ModifyVolumeAttribute&quot;,</td>
<td>Manages the EBS volumes that Cloud Volumes ONTAP uses as back-end storage.</td>
</tr>
<tr>
<td>&quot;ec2:AttachVolume&quot;, &quot;ec2:DeleteVolume&quot;, &quot;ec2:DetachVolume&quot;,</td>
<td></td>
</tr>
<tr>
<td>&quot;ec2:DescribeSubnets&quot;, &quot;ec2:DescribeVpcs&quot;,</td>
<td></td>
</tr>
<tr>
<td>&quot;ec2:DescribeDhcpOptions&quot;,</td>
<td>Gets the list of destination subnets and security groups, which is needed when creating a new working environment for Cloud Volumes ONTAP.</td>
</tr>
<tr>
<td>&quot;ec2:DescribeDhcpOptions&quot;,</td>
<td></td>
</tr>
<tr>
<td>&quot;ec2:DescribeDhcpOptions&quot;,</td>
<td>Determines DNS servers and the default domain name when launching Cloud Volumes ONTAP instances.</td>
</tr>
<tr>
<td>Actions</td>
<td>Purpose</td>
</tr>
<tr>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>&quot;ec2:CreateSnapshot&quot;, &quot;ec2:DeleteSnapshot&quot;, &quot;ec2:DescribeSnapshots&quot;</td>
<td>Takes snapshots of EBS volumes during initial setup and whenever a CloudVolumes ONTAP instance is stopped.</td>
</tr>
<tr>
<td>&quot;ec2:GetConsoleOutput&quot;</td>
<td>Captures the Cloud Volumes ONTAP console, which is attached to AutoSupport messages.</td>
</tr>
<tr>
<td>&quot;ec2:DescribeKeyPairs&quot;</td>
<td>Obtains the list of available key pairs when launching instances.</td>
</tr>
<tr>
<td>&quot;ec2:DescribeRegions&quot;</td>
<td>Gets a list of available AWS regions.</td>
</tr>
<tr>
<td>&quot;ec2:DeleteTags&quot;, &quot;ec2:DescribeTags&quot;</td>
<td>Manages tags for resources associated with Cloud Volumes ONTAP instances.</td>
</tr>
<tr>
<td>&quot;s3:GetBucketTagging&quot;, &quot;s3:GetBucketLocation&quot;, &quot;s3:ListAllMyBuckets&quot;, &quot;s3:ListBucket&quot;</td>
<td>Obtains information about AWS S3 buckets so Cloud Manager can integrate with the NetApp Data Fabric Cloud Sync service.</td>
</tr>
<tr>
<td>Actions</td>
<td>Purpose</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>&quot;s3:CreateBucket&quot;, &quot;s3:DeleteBucket&quot;, &quot;s3:GetLifecycleConfiguration&quot;,</td>
<td>Manages the S3 bucket that a Cloud Volumes ONTAP system uses as a capacity tier for data tiering.</td>
</tr>
<tr>
<td>&quot;s3:PutLifecycleConfiguration&quot;, &quot;s3:PutBucketTagging&quot;, &quot;s3:ListBucket</td>
<td></td>
</tr>
<tr>
<td>Versions&quot;, &quot;s3:GetBucketPolicyStatus&quot;, &quot;s3:GetBucketPublicAccessBlock&quot;,</td>
<td></td>
</tr>
<tr>
<td>&quot;s3:GetBucketAcl&quot;, &quot;s3:GetBucketPolicy&quot;, &quot;s3:PutBucketPublicAccessBlock&quot;</td>
<td></td>
</tr>
<tr>
<td>&quot;kms:List*&quot;, &quot;kms:ReEncrypt*&quot;, &quot;kms:Describe*&quot;, &quot;kms:CreateGrant&quot;,</td>
<td>Enables data encryption of Cloud Volumes ONTAP using the AWS Key Management Service (KMS).</td>
</tr>
<tr>
<td>&quot;ce:GetReservationUtilization&quot;, &quot;ce:GetDimensionValues&quot;, &quot;ce:GetCostAndUsage&quot;,</td>
<td>Obtains AWS cost data for Cloud Volumes ONTAP.</td>
</tr>
<tr>
<td>&quot;ce:GetTags&quot;</td>
<td></td>
</tr>
<tr>
<td>&quot;ec2:CreatePlacementGroup&quot;, &quot;ec2:DeletePlacementGroup&quot;</td>
<td>When you deploy an HA configuration in a single AWS Availability Zone, Cloud Manager launches the two HA nodes and the mediator in an AWS spread placement group.</td>
</tr>
<tr>
<td>&quot;ec2:DescribeReservedInstancesOfferings&quot;</td>
<td>Cloud Manager uses the permission as part of Cloud Compliance deployment to choose which instance type to use.</td>
</tr>
<tr>
<td>&quot;s3:DeleteBucket&quot;, &quot;s3:GetLifecycleConfiguration&quot;, &quot;s3:PutLifecycle</td>
<td>Cloud Manager uses these permissions when you enable the Backup to S3 service.</td>
</tr>
<tr>
<td>Configuration&quot;, &quot;s3:PutBucketTagging&quot;, &quot;s3:ListBucketVersions&quot;, &quot;s3:</td>
<td></td>
</tr>
<tr>
<td>GetObject&quot;, &quot;s3:ListBucket&quot;, &quot;s3:ListAllMyBuckets&quot;, &quot;s3:GetBucket</td>
<td></td>
</tr>
<tr>
<td>Tagging&quot;, &quot;s3:GetBucketLocation&quot; &quot;s3:GetBucketPolicyStatus&quot;, &quot;s3:GetBucketPublicAccessBlock&quot;,</td>
<td></td>
</tr>
<tr>
<td>&quot;s3:GetBucketAcl&quot;, &quot;s3:GetBucketPolicy&quot;, &quot;s3:PutBucketPublicAccessBlock&quot;</td>
<td></td>
</tr>
</tbody>
</table>
What Cloud Manager does with Azure permissions

The Cloud Manager Azure policy includes the permissions that Cloud Manager needs to deploy and manage Cloud Volumes ONTAP in Azure.

<table>
<thead>
<tr>
<th>Actions</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;Microsoft.Compute/locations/operations/read&quot;,</td>
<td>Creates Cloud Volumes ONTAP and stops, starts, deletes, and obtains the</td>
</tr>
<tr>
<td>&quot;Microsoft.Compute/locations/vmSizes/read&quot;,</td>
<td>status of the system.</td>
</tr>
<tr>
<td>&quot;Microsoft.Compute/operations/read&quot;,</td>
<td></td>
</tr>
<tr>
<td>&quot;Microsoft.Compute/virtualMachines/instanceView/read&quot;,</td>
<td></td>
</tr>
<tr>
<td>&quot;Microsoft.Compute/virtualMachines/powerOff/action&quot;,</td>
<td></td>
</tr>
<tr>
<td>&quot;Microsoft.Compute/virtualMachines/read&quot;,</td>
<td></td>
</tr>
<tr>
<td>&quot;Microsoft.Compute/virtualMachines/restart/action&quot;,</td>
<td></td>
</tr>
<tr>
<td>&quot;Microsoft.Compute/virtualMachines/start/action&quot;,</td>
<td></td>
</tr>
<tr>
<td>&quot;Microsoft.Compute/virtualMachines/deallocate/action&quot;,</td>
<td></td>
</tr>
<tr>
<td>&quot;Microsoft.Compute/virtualMachines/vmSizes/read&quot;,</td>
<td></td>
</tr>
<tr>
<td>&quot;Microsoft.Compute/virtualMachines/write&quot;,</td>
<td></td>
</tr>
<tr>
<td>&quot;Microsoft.Compute/images/write&quot;,</td>
<td>Enables Cloud Volumes ONTAP deployment from a VHD.</td>
</tr>
<tr>
<td>&quot;Microsoft.Compute/images/read&quot;,</td>
<td></td>
</tr>
<tr>
<td>&quot;Microsoft.Compute/disks/delete&quot;,</td>
<td>Manages Azure storage accounts and disks, and attaches the disks to</td>
</tr>
<tr>
<td>&quot;Microsoft.Compute/disks/read&quot;,</td>
<td>Cloud Volumes ONTAP.</td>
</tr>
<tr>
<td>&quot;Microsoft.Compute/disks/write&quot;,</td>
<td></td>
</tr>
<tr>
<td>&quot;Microsoft.Storage/checknameavailability/read&quot;,</td>
<td></td>
</tr>
<tr>
<td>&quot;Microsoft.Storage/operations/read&quot;,</td>
<td></td>
</tr>
<tr>
<td>&quot;Microsoft.Storage/storageAccounts/listkeys/action&quot;,</td>
<td></td>
</tr>
<tr>
<td>&quot;Microsoft.Storage/storageAccounts/read&quot;,</td>
<td></td>
</tr>
<tr>
<td>&quot;Microsoft.Storage/storageAccounts/regeneratekey/action&quot;,</td>
<td></td>
</tr>
<tr>
<td>&quot;Microsoft.Storage/storageAccounts/write&quot;</td>
<td></td>
</tr>
<tr>
<td>&quot;Microsoft.Storage/storageAccounts/delete&quot;,</td>
<td></td>
</tr>
<tr>
<td>&quot;Microsoft.Storage/usages/read&quot;,</td>
<td></td>
</tr>
<tr>
<td>&quot;Microsoft.Network/networkInterfaces/read&quot;,</td>
<td>Creates and manages network interfaces for Cloud Volumes ONTAP in the</td>
</tr>
<tr>
<td>&quot;Microsoft.Network/networkInterfaces/join/action&quot;</td>
<td></td>
</tr>
<tr>
<td>Actions</td>
<td>Purpose</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| "Microsoft.Network/networkSecurityGroups/read",
| "Microsoft.Network/networkSecurityGroups/write",
| Creates predefined network security groups for Cloud Volumes ONTAP.     |
| "Microsoft.Resources/subscriptions/locations/read",
| "Microsoft.Network/locations/operationResults/read",
| "Microsoft.Network/locations/operations/read",
| "Microsoft.Network/virtualNetworks/read",
| "Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read",
| "Microsoft.Network/virtualNetworks/subnets/read",
| "Microsoft.Network/virtualNetworks/subnets/virtualMachines/read",
| "Microsoft.Network/virtualNetworks/virtualMachines/read",
| "Microsoft.Network/virtualNetworks/subnets/join/action",
| Gets network information about regions, the target VNet and subnet, and adds Cloud Volumes ONTAP to VNets. |
| "Microsoft.Network/virtualNetworks/subnets/write",
| "Microsoft.Network/routeTables/join/action",
| Enables VNet service endpoints for data tiering.                        |
| "Microsoft.Resources/deployments/operations/read",
| "Microsoft.Resources/deployments/read",
| "Microsoft.Resources/deployments/write",
<p>| Deploys Cloud Volumes ONTAP from a template.                            |</p>
<table>
<thead>
<tr>
<th>Actions</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;Microsoft.Resources/deployments/operations/read&quot;,</td>
<td>Creates and manages resource groups for Cloud Volumes ONTAP.</td>
</tr>
<tr>
<td>&quot;Microsoft.Resources/deployments/read&quot;,</td>
<td></td>
</tr>
<tr>
<td>&quot;Microsoft.Resources/deployments/write&quot;,</td>
<td></td>
</tr>
<tr>
<td>&quot;Microsoft.Resources/resources/read&quot;,</td>
<td></td>
</tr>
<tr>
<td>&quot;Microsoft.Resources/subscriptions/operations/results/read&quot;,</td>
<td></td>
</tr>
<tr>
<td>&quot;Microsoft.Resources/subscriptions/resourceGroups/delete&quot;,</td>
<td></td>
</tr>
<tr>
<td>&quot;Microsoft.Resources/subscriptions/resourceGroups/read&quot;,</td>
<td></td>
</tr>
<tr>
<td>&quot;Microsoft.Resources/subscriptions/resourceGroups/resources/read&quot;,</td>
<td></td>
</tr>
<tr>
<td>&quot;Microsoft.Resources/subscriptions/resourceGroups/write&quot;,</td>
<td></td>
</tr>
<tr>
<td>&quot;Microsoft.Compute/snapshots/read&quot;,</td>
<td></td>
</tr>
<tr>
<td>&quot;Microsoft.Compute/disks/beginGetAccess/action&quot;</td>
<td></td>
</tr>
<tr>
<td>&quot;Microsoft.Compute/availabilitySets/write&quot;,</td>
<td></td>
</tr>
<tr>
<td>&quot;Microsoft.Compute/availabilitySets/read&quot;,</td>
<td></td>
</tr>
<tr>
<td>&quot;Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/write&quot;</td>
<td></td>
</tr>
<tr>
<td>&quot;Microsoft.Network/loadBalancers/write&quot;,</td>
<td></td>
</tr>
<tr>
<td>&quot;Microsoft.Network/loadBalancers/delete&quot;,</td>
<td></td>
</tr>
<tr>
<td>&quot;Microsoft.Network/loadBalancers/backendAddressPools/read&quot;,</td>
<td></td>
</tr>
<tr>
<td>&quot;Microsoft.Network/loadBalancers/backendAddressPools/join/action&quot;,</td>
<td></td>
</tr>
<tr>
<td>&quot;Microsoft.Network/loadBalancers/frontendIPConfigurations/read&quot;,</td>
<td></td>
</tr>
<tr>
<td>&quot;Microsoft.Network/loadBalancers/loadBalancingRules/read&quot;,</td>
<td></td>
</tr>
<tr>
<td>&quot;Microsoft.Network/loadBalancers/probes/read&quot;,</td>
<td></td>
</tr>
<tr>
<td>&quot;Microsoft.Network/loadBalancers/probes/join/action&quot;,</td>
<td></td>
</tr>
<tr>
<td>Actions</td>
<td>Purpose</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>&quot;Microsoft.Resources/deployments/operationStatuses/read&quot;</td>
<td>Azure requires this permission for some virtual machine deployments (it depends on the underlying physical hardware that's used during deployment).</td>
</tr>
<tr>
<td>&quot;Microsoft.Protocols/azure/privaterangex/local circumcision&quot;</td>
<td>Enables Cloud Manager to encrypt Azure managed disks on single node Cloud Volumes ONTAP systems using external keys from another account. This feature is supported using APIs.</td>
</tr>
</tbody>
</table>
What Cloud Manager does with GCP permissions

The Cloud Manager policy for GCP includes the permissions that Cloud Manager needs to deploy and manage Cloud Volumes ONTAP.

<table>
<thead>
<tr>
<th>Actions</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| - compute.disks.create  
- compute.disks.createSnapshot  
- compute.disks.delete  
- compute.disks.get  
- compute.disks.list  
- compute.disks.setLabels  
- compute.disks.use | To create and manage disks for Cloud Volumes ONTAP. |
| - compute.firewalls.create  
- compute.firewalls.delete  
- compute.firewalls.get  
- compute.firewalls.list | To create firewall rules for Cloud Volumes ONTAP. |
| - compute.globalOperations.get | To get the status of operations. |
| - compute.images.get  
- compute.images.getFromFamily  
- compute.images.list  
- compute.images.useReadOnly | To get images for VM instances. |
| - compute.instances.attachDisk  
- compute.instances.detachDisk | To attach and detach disks to Cloud Volumes ONTAP. |
| - compute.instances.create  
- compute.instances.delete | To create and delete Cloud Volumes ONTAP VM instances. |
| - compute.instances.get | To list VM instances. |
| - compute.instances.getSerialPortOutput | To get console logs. |
| - compute.instances.list | To retrieve the list of instances in a zone. |
| - compute.instances.setDeletionProtection | To set deletion protection on the instance. |
| - compute.instances.setLabels | To add labels. |
| - compute.instances.setMachineType | To change the machine type for Cloud Volumes ONTAP. |
| - compute.instances.setMetadata | To add metadata. |
| - compute.instances.setTags | To add tags for firewall rules. |
| - compute.instances.start  
- compute.instances.stop  
- compute.instances.updateDisplayDevice | To start and stop Cloud Volumes ONTAP. |
<p>| - compute.machineTypes.get | To get the numbers of cores to check quotas. |</p>
<table>
<thead>
<tr>
<th>Actions</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>- compute.projects.get</td>
<td>To support multi-projects.</td>
</tr>
</tbody>
</table>
| - compute.snapshots.create  
- compute.snapshots.delete  
- compute.snapshots.get  
- compute.snapshots.list  
- compute.snapshots.setLabels | To create and manage persistent disk snapshots. |
| - compute.networks.get  
- compute.networks.list  
- compute.regions.get  
- compute.regions.list  
- compute.subnetworks.get  
- compute.subnetworks.list  
- compute.zoneOperations.get  
- compute.zones.get  
- compute.zones.list | To get the networking information needed to create a new Cloud Volumes ONTAP virtual machine instance. |
| - deploymentmanager.compositeTypes.get  
- deploymentmanager.compositeTypes.list  
- deploymentmanager.deployments.create  
- deploymentmanager.deployments.delete  
- deploymentmanager.deployments.get  
- deploymentmanager.deployments.list  
- deploymentmanager.manifests.get  
- deploymentmanager.manifests.list  
- deploymentmanager.operations.get  
- deploymentmanager.operations.list  
- deploymentmanager.resources.get  
- deploymentmanager.resources.list  
- deploymentmanager.typeProviders.get  
- deploymentmanager.typeProviders.list  
- deploymentmanager.types.get  
- deploymentmanager.types.list | To deploy the Cloud Volumes ONTAP virtual machine instance using Google Cloud Deployment Manager. |
| - logging.logEntries.list  
- logging.privateLogEntries.list | To get stack log drives. |
| - resourcemanager.projects.get | To support multi-projects. |
| - storage.buckets.create  
- storage.buckets.delete  
- storage.buckets.get  
- storage.buckets.list  
- storage.buckets.update | To create and manage a Google Cloud Storage bucket for data tiering. |
<table>
<thead>
<tr>
<th>Actions</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>- cloudkms.cryptoKeyVersions.useToEncrypt</td>
<td>To use customer-managed encryption keys from the Cloud Key Management Service with Cloud Volumes ONTAP.</td>
</tr>
<tr>
<td>- cloudkms.cryptoKeys.get</td>
<td></td>
</tr>
<tr>
<td>- cloudkms.cryptoKeys.list</td>
<td></td>
</tr>
<tr>
<td>- cloudkms.keyRings.list</td>
<td></td>
</tr>
<tr>
<td>- compute.instances.setServiceAccount</td>
<td>To set a service account on the Cloud Volumes ONTAP instance. This service account provides permissions for data tiering to a Google Cloud Storage bucket.</td>
</tr>
<tr>
<td>- iam.serviceAccounts.getIamPolicy</td>
<td></td>
</tr>
<tr>
<td>- iam.serviceAccounts.list</td>
<td></td>
</tr>
</tbody>
</table>

**AWS Marketplace pages for Cloud Manager and Cloud Volumes ONTAP**

Several offerings are available in the AWS Marketplace for Cloud Manager and Cloud Volumes ONTAP. If need help understanding the purpose of each page, read the descriptions below.

In all cases, remember that you can't launch Cloud Volumes ONTAP in AWS from the AWS Marketplace. You need to launch it directly from Cloud Manager.
<table>
<thead>
<tr>
<th>Goal</th>
<th>AWS Marketplace page to use</th>
<th>More information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable the use of Cloud Volumes ONTAP PAYGO, Cloud Tiering, Cloud Compliance, and other add-on services</td>
<td>Cloud Manager - Deploy &amp; Manage NetApp Cloud Data Services</td>
<td>This subscription enables charging for the PAYGO version of Cloud Volumes ONTAP 9.6 and later. It also enables charging for Cloud Tiering, Cloud Compliance, and other add-on services. You should subscribe to this offering when Cloud Manager prompts you and redirects you to the page. Cloud Manager prompts you in the Working Environment wizard or when you add new credentials in the Settings. This page doesn’t enable you to launch Cloud Manager in AWS. That should be done from NetApp Cloud Central, or alternatively using the AMI listed in row 3 of this table.</td>
</tr>
<tr>
<td>Enable the use of Cloud Volumes ONTAP PAYGO, Cloud Tiering, Cloud Compliance, and other add-on services using an annual contract</td>
<td>Cloud Manager (Contracts) - Deploy &amp; Manage NetApp Cloud Data Services</td>
<td>This subscription is an alternative to the subscription in the first row. It enables you to get an annual upfront payment for the listings. It’s mostly for NetApp partners.</td>
</tr>
<tr>
<td>Deploy Cloud Manager from the AWS Marketplace using an AMI</td>
<td>Cloud Manager - Manual installation without access keys</td>
<td>We recommend that you launch Cloud Manager in AWS from NetApp Cloud Central, but you can launch it from this AWS Marketplace page, if you prefer.</td>
</tr>
<tr>
<td>Goal</td>
<td>AWS Marketplace page to use</td>
<td>More information</td>
</tr>
<tr>
<td>---------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Enable deployment of Cloud Volumes ONTAP PAYGO (9.5 or earlier)</td>
<td>• Cloud Volumes ONTAP for AWS</td>
<td>These AWS Marketplace pages enable you to subscribe to the single node or HA versions of Cloud Volumes ONTAP PAYGO for versions 9.5 and earlier.</td>
</tr>
<tr>
<td></td>
<td>• Cloud Volumes ONTAP for AWS - High Availability</td>
<td>Starting with version 9.6, you need to subscribe through the AWS Marketplace page listed in row 1 of this table for PAYGO deployments.</td>
</tr>
</tbody>
</table>
Copyright Information

Copyright © 2020 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.