Manage Connectors
Cloud Manager
NetApp
October 21, 2020

This PDF was generated from https://docs.netapp.com/us-en/occm/task_managing_connectors.html on October 21, 2020. Always check docs.netapp.com for the latest.
# Table of Contents

**Manage Connectors** ........................................................................................................... 1
  - Managing existing Connectors ....................................................................................... 1
  - More ways to create Connectors .................................................................................. 4
  - Default configuration for the Connector ...................................................................... 15
# 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**.

![Image of Connectors](image.png)
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**.

   ![Cloud Manager 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:

   ```bash
   /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](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.

<table>
<thead>
<tr>
<th><strong>Number of instances</strong></th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Purchasing option</strong></td>
<td>✔ Request Spot instances</td>
</tr>
<tr>
<td><strong>Network</strong></td>
<td>vpc-a75d91c2</td>
</tr>
<tr>
<td><strong>Subnet</strong></td>
<td>subnet-39538c13</td>
</tr>
<tr>
<td><strong>Auto-assign Public IP</strong></td>
<td>Enable</td>
</tr>
<tr>
<td><strong>Placement group</strong></td>
<td>✔ Add instance to placement group</td>
</tr>
<tr>
<td><strong>Capacity Reservation</strong></td>
<td>Open</td>
</tr>
<tr>
<td><strong>IAM role</strong></td>
<td>Cloud_Manager</td>
</tr>
<tr>
<td><strong>CPU options</strong></td>
<td>✔ Specify CPU options</td>
</tr>
<tr>
<td><strong>Shutdown behavior</strong></td>
<td>Stop</td>
</tr>
<tr>
<td><strong>Enable termination protection</strong></td>
<td>✔ Protect against accidental termination</td>
</tr>
</tbody>
</table>

- **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
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:

```bash
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
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
  ◦ https://s3.amazonaws.com/aws-cli/awscli-bundle.zip

   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
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