NetApp

Connectors

Set up and administration

NetApp
September 30, 2022

Table of Contents

Connectors

Advanced deployment

Create a Connector from the AWS Marketplace

For an AWS commercial region, it's best to create a Connector directly from Cloud Manager, but you can launch a Connector from the AWS Marketplace, if you prefer. For AWS Government regions, you can't deploy the Connector in a Government region from Cloud Manager's SaaS website, so the next best option is to do so from the AWS Marketplace.

> 💡 You can also download and install the Connector software on an existing Linux host in your network or in the cloud. Learn how to install the Connector on an existing Linux host.

Create the Connector in an AWS commercial region

You can launch the Connector instance in an AWS commercial region directly from the AWS Marketplace offering for Cloud Manager.

Before you get started

The IAM user who creates the Connector must have AWS Marketplace permissions to subscribe and unsubscribe.

Steps

1. Set up permissions in AWS:

    a. From the IAM console, create your own policy by copying and pasting the contents of the IAM policy for the Connector.

    b. Create an IAM role with the role type Amazon EC2 and attach the policy that you created in the previous step to the role.

2. Go to the Cloud Manager page on the AWS Marketplace to deploy Cloud Manager from an AMI:

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:

   ◦ **Name and tags**: Enter a name and tags for the instance.

   ◦ **Application and OS Image**: Skip this section. The Cloud Manager AMI is already selected.

   ◦ **Instance type**: Depending on region availability, choose one of the supported instance types (t3.xlarge

is recommended).

Review the instance requirements.

- **Key pair (login)**: Select the key pair that you want to use to securely connect to the instance.
- **Network settings**: Edit the network settings as needed:
    - Choose the desired VPC and subnet.
    - Specify whether the instance should have a public IP address.
    - Specify firewall settings that enable the required connection methods for the Connector instance: SSH, HTTP, and HTTPS.
- **Configure storage**: Keep the default storage options.
- **Advanced details**: Under **IAM intance profile**, choose the IAM role that you created in step 1.
- **Summary**: Review the summary and click **Launch instance**.

AWS launches the software with the specified settings. The Connector instance and software should be running in approximately five minutes.
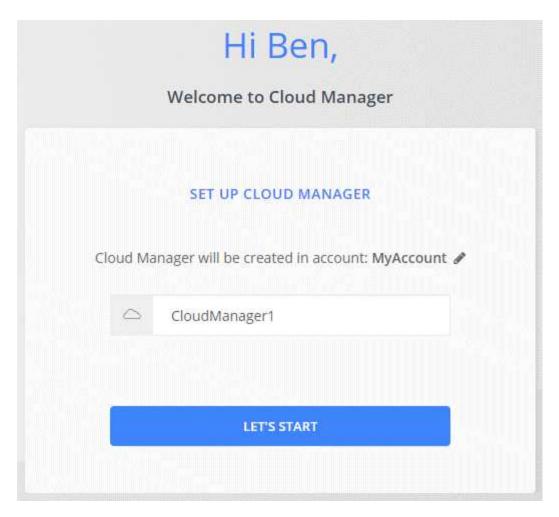
7. Open a web browser from a host that has a connection to the Connector instance and enter the following URL:

http://*ipaddress*:80

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

a. Specify the NetApp account to associate with the Connector.

Learn about NetApp accounts.

b. Enter a name for the system.

9. Open a web browser and go to https://cloudmanager.netapp.com to start using the Connector with Cloud Manager.

Result

The Connector is now installed and set up with your NetApp 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.

If you have Amazon S3 buckets in the same AWS account where you created the Connector, you'll see an Amazon S3 working environment appear on the Canvas automatically. Learn more about what you can do with this working environment.

Create the Connector in an AWS Government region

To deploy the Connector in an AWS Government region, you need to go to the EC2 service and select the Cloud Manager offering from the AWS Marketplace.
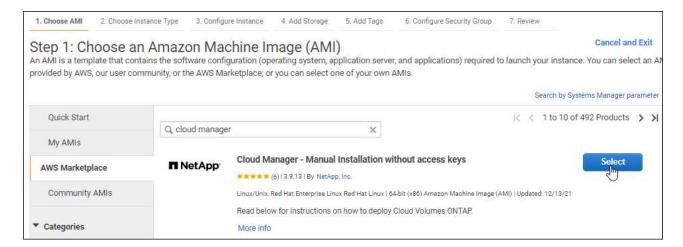
Steps

1. Set up permissions in AWS:

   a. From the IAM console, create your own policy by copying and pasting the contents of the IAM policy for the Connector.

   b. Create an IAM role with the role type Amazon EC2 and attach the policy that you created in the previous step to the role.

2. Go to the Cloud Manager offering in the AWS Marketplace.

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

   a. Open the EC2 service and select **Launch instance**.
   b. Select **AWS Marketplace**.
   c. Search for Cloud Manager and select the offering.

   d. Click **Continue**.
3. Follow the prompts to configure and deploy the instance:

   ◦ **Choose an Instance Type**: Depending on region availability, choose one of the supported instance types (t3.xlarge is recommended).

     Review the instance requirements.

   ◦ **Configure Instance Details**: 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.

- ◦ **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.
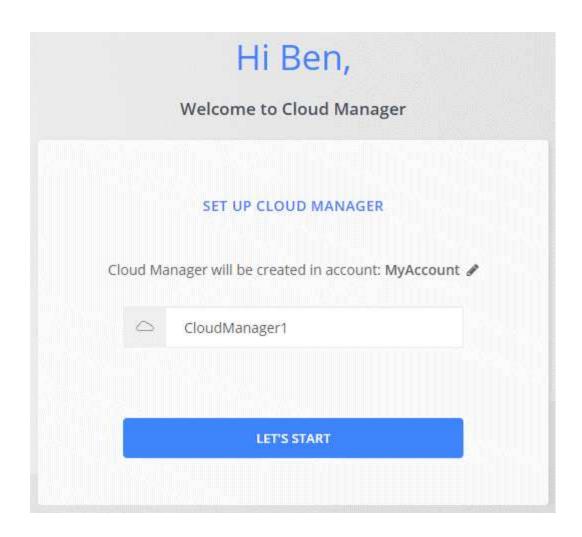
4. Open a web browser from a host that has a connection to the Connector instance and enter the following URL:

http://*ipaddress*:80

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

a. Specify the NetApp account to associate with the Connector.

Learn about NetApp accounts.

b. Enter a name for the system.

Result

The Connector is now installed and set up with your NetApp account.

Any time that you want to use Cloud Manager, open your web browser and connect to the IP address of the Connector instance: http://*ipaddress*:80

Since the Connector was deployed in a Government region, it's not accessible from https://cloudmanager.netapp.com.

Open port 3128 for AutoSupport messages

If you plan to deploy Cloud Volumes ONTAP systems in a subnet where an outbound internet connection won't be available, then Cloud Manager automatically configures Cloud Volumes ONTAP to use the Connector as a proxy server.

The only requirement is to ensure that the Connector's security group allows *inbound* connections over port 3128. You'll need to open this port after you deploy the Connector.

If you use the default security group for Cloud Volumes ONTAP, then no changes are needed to its security group. But if you plan to define strict outbound rules for Cloud Volumes ONTAP, then you'll also need to ensure that the Cloud Volumes ONTAP security group allows *outbound* connections over port 3128.

Create a Connector from the Azure Marketplace

For an Azure commercial region, it's best to create a Connector directly from Cloud Manager, but you can launch a Connector from the Azure Marketplace, if you prefer. For Azure Government regions, you can't deploy the Connector in a Government region from Cloud Manager's SaaS website, so the next best option is to do so from the Azure Marketplace.

> You can also download and install the Connector software on an existing Linux host in your network or in the cloud. Learn how to install the Connector on an existing Linux host.

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 NetApp account.

Steps

1. Go to the NetApp Connector VM page in the Azure Marketplace.

   ◦ Azure Marketplace page for commercial regions

   ◦ Azure Marketplace page for Azure Government regions

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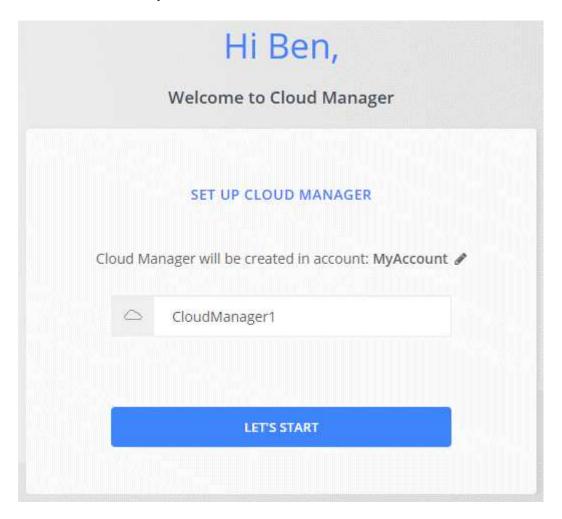
5. Open a web browser from a host that has a connection to the Connector virtual machine and enter the following URL:

   http://*ipaddress*:80

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

   a. Specify the NetApp account to associate with the Connector.

      Learn about NetApp accounts.

   b. Enter a name for the system.

Result

The Connector is now installed and set up with your NetApp account.

If the Connector is in an Azure commercial region, open a web browser and go to https://cloudmanager.netapp.com to start using the Connector with Cloud Manager.

If the Connector is in an Azure Government region, you can use Cloud Manager by opening your web browser and connecting to the IP address of the Connector instance: http://*ipaddress*:80

Since the Connector was deployed in a Government region, it's not accessible from https://cloudmanager.netapp.com.

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:

   a. Copy the contents of the custom role permissions for the Connector and save them in a JSON file.

   b. Modify the JSON file by adding Azure subscription IDs to the assignable scope.

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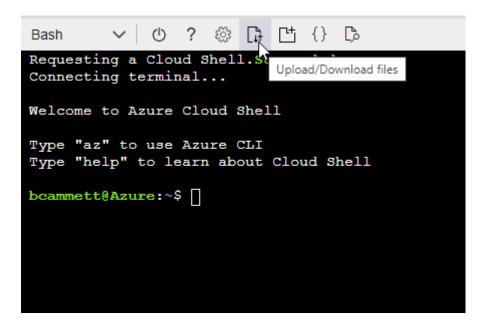
   Example

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

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

   The following steps describe how to create the role by using Bash in Azure Cloud Shell.

   - Start Azure Cloud Shell and choose the Bash environment.
   - Upload the JSON file.

   - Enter the following Azure CLI command:

   ```
   az role definition create --role-definition
   Policy_for_Setup_As_Service_Azure.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)** > **Add** > **Add role assignment**.

   c. In the **Role** tab, select the **Cloud Manager Operator** role and click **Next**.

   > (i) 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.

   d. In the **Members** tab, complete the following steps:

      - Assign access to a **Managed identity**.
      - Click **Select members**, select the subscription in which the Connector virtual machine was created, choose **Virtual machine**, and then select the Connector virtual machine.
      - Click **Select**.
      - Click **Next**.

   e. Click **Review + assign**.

   f. 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.

If you have Azure Blob storage in the same Azure account where you created the Connector, you'll see an Azure Blob working environment appear on the Canvas automatically. Learn more about what you can do with this working environment.

Open port 3128 for AutoSupport messages

If you plan to deploy Cloud Volumes ONTAP systems in a subnet where an outbound internet connection won't be available, then Cloud Manager automatically configures Cloud Volumes ONTAP to use the Connector as a proxy server.

The only requirement is to ensure that the Connector's security group allows *inbound* connections over port 3128. You'll need to open this port after you deploy the Connector.

If you use the default security group for Cloud Volumes ONTAP, then no changes are needed to its security group. But if you plan to define strict outbound rules for Cloud Volumes ONTAP, then you'll also need to ensure that the Cloud Volumes ONTAP security group allows *outbound* connections over port 3128.

Install the Connector on an existing Linux host that has internet access

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. These steps are specific to hosts that have internet access.

Learn about other ways to deploy a Connector.

ℹ️ If you want to create a Cloud Volumes ONTAP system in Google Cloud, then you must have a Connector that's running in Google Cloud as well. You can't use a Connector that's running in AWS, Azure, or on-prem.

Verify 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

16 GB

AWS EC2 instance type

An instance type that meets the CPU and RAM requirements above. We recommend t3.xlarge.

Azure VM size

An instance type that meets the CPU and RAM requirements above. We recommend DS3 v2.

GCP machine type

An instance type that meets the CPU and RAM requirements above. We recommend n2-standard-4.

The Connector is supported in Google Cloud on a VM instance with an OS that supports Shielded VM features

Supported operating systems

- CentOS 7.6
- CentOS 7.7
- CentOS 7.8
- CentOS 7.9
- Red Hat Enterprise Linux 7.6
- Red Hat Enterprise Linux 7.7
- Red Hat Enterprise Linux 7.8
- Red Hat Enterprise Linux 7.9

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 GiB of space must be available

Disk space in /var

20 GiB of space must be available

Outbound internet access

The installer for the Connector must access the following URLs during the installation process:

- https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm

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

- https://*.blob.core.windows.net or https://hub.docker.com

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

Install the Connector

After you verify that you have a supported Linux host, you can obtain the Connector software and then install it.

Required privileges

Root privileges are required to install the Connector.

About this task

- 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 run the script.

   ```
   chmod +x OnCommandCloudManager-V3.9.19.sh
   ```

3. Run the installation script.

   If you have a proxy server, you will need to enter the command parameters as shown below. The installer

doesn't prompt you to provide information about a proxy.

```
  ./OnCommandCloudManager-V3.9.19.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, enter **Y** to continue with the installation.

   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*

   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.

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

7. If you installed the Connector in Google Cloud, set up a service account that has the permissions that Cloud Manager needs to create and manage Cloud Volumes ONTAP systems in projects.

   a. Create a role in GCP that includes the permissions defined in the Connector policy for GCP.

   b. Create a GCP service account and apply the custom role that you just created.

   c. Associate this service account with the Connector VM.

   d. 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.

8. After you log in, set up Cloud Manager:

   a. Specify the NetApp account to associate with the Connector.

      Learn about NetApp accounts.

   b. Enter a name for the system.

Result

The Connector is now installed and set up with your NetApp 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
- Google Cloud: See step 7 above

Install the Connector on-prem without internet access

You can install the Connector on an on-premises Linux host that doesn't have internet access. You can then discover on-prem ONTAP clusters, replicate data between them, back up volumes using Cloud Backup, and scan them with Cloud Data Sense.

These installation instructions are specifically for the use case described above. Learn about other ways to deploy a Connector.

Verify 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

16 GB

Supported operating systems

- CentOS 7.6
- CentOS 7.7
- CentOS 7.8
- CentOS 7.9
- Red Hat Enterprise Linux 7.6
- Red Hat Enterprise Linux 7.7
- Red Hat Enterprise Linux 7.8
- Red Hat Enterprise Linux 7.9

  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 type

An SSD is required

Disk space in /opt

100 GiB of space must be available

Disk space in /var

20 GiB of space must be available

Docker Engine

Docker Engine version 19 or later is required on the host before you install the Connector. View installation instructions.

Install the Connector

After you verify that you have a supported Linux host, you can obtain the Connector software and then install it.

Required privileges

Root privileges are required to install the Connector.

Steps

1. Verify that docker is enabled and running.

   ```
   sudo sysctl enable docker && sudo sysctl start docker
   ```

2. Download the Cloud Manager software from the NetApp Support Site.
3. Copy the installer to the Linux host.
4. Assign permissions to run the script.

   ```
   chmod +x /path/cloud-manager-connector-offline-v3.9.19
   ```

5. Run the installation script:

   ```
   sudo /path/cloud-manager-connector-offline-v3.9.19
   ```

6. Open a web browser and enter https://*ipaddress* where *ipaddress* is the IP address of the Linux host.

   You should see the following screen.

7. Click **Set Up New Cloud Manager** and follow the prompts to set up the system.
   ◦ **System Details**: Enter a name for the Cloud Manager system and your company name.

- ◦ **Create Admin User**: Create the admin user for the system.

  This user account runs locally on the system. There's no connection to NetApp Cloud Central.

- ◦ **Review**: Review the details, accept the license agreement, and then click **Set Up**.

8. Log in to Cloud Manager using the admin user that you just created.

Result

The Connector is now installed and you can start using the Cloud Manager features that are available in a dark site deployment.

What's next?

- • Discover on-prem ONTAP clusters
- • Replicate data between on-prem ONTAP clusters
- • Back up on-prem ONTAP volume data to StorageGRID using Cloud Backup
- • Scan on-prem ONTAP volume data using Cloud Data Sense

When new versions of the Connector software are available, they'll be posted to the NetApp Support Site. Learn how to upgrade the Connector.

Finding the system ID for a Connector

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

Steps

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

2. Click **Support > Connector**.

   The system ID appears at the top.

   Example

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.

Switch 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.

Access 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. If you're accessing Cloud Manager from a Government region or a site that doesn't have outbound internet access, then you need to use the local user interface running on the Connector.

Steps

1. Open a web browser and enter the following URL:

   https://*ipaddress*

   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.

2. Enter your user name and password to log in.

Download or send an AutoSupport message

If you're having problems, NetApp personnel might ask you to send an AutoSupport message to NetApp support for troubleshooting purposes.

Steps

1. Connect to the Connector local UI, as described in the section above.

2. In the upper right of the Cloud Manager console, click the Help icon, and select **Support**.

3. Click **Connector**.

4. Depending on how you need to send the information to NetApp support, choose one of the following options:

   a. Select the option to download the AutoSupport message to your local machine. You can then send it to NetApp Support using a preferred method.

   b. Click **Send AutoSupport** to directly send the message to NetApp Support.

Connect to the Linux VM

If you need to connect to the Linux VM that the Connector runs on, you can do so by using the connectivity options available from your cloud provider.

AWS

When you created the Connector instance in AWS, you provided an AWS access key and secret key. You can use this key pair to SSH to the instance.

AWS Docs: Connect to your Linux instance

Azure

When you created the Connector VM in Azure, you chose to authenticate with a password or SSH public key. Use the authentication method that you chose to connect to the VM.

Azure Docs: SSH into your VM

Google Cloud

You can't specify an authentication method when you create a Connector in Google Cloud. However, you can connect to the Linux VM instance using the Google Cloud Console or Google Cloud CLI (gcloud).

Google Cloud Docs: Connect to Linux VMs

Apply security updates

Update the operating system on the Connector to ensure that it's patched with the latest security updates.

Steps

1. Access the CLI shell on the Connector host.

2. Run the following commands with elevated privileges:

```
sudo -s
service service-manager stop
yum -y update --security
service service-manager start
```

Change the IP address for a Connector

If it's required for your business, you can change the internal IP address and public IP address of the Connector instance that is automatically assigned by your cloud provider.

Steps

1. Follow the instructions from your cloud provider to change the local IP address or public IP address (or both) for the Connector instance.

2. If you changed the public IP address and you need to connect to the local user interface running on the Connector, restart the Connector instance to register the new IP address with Cloud Manager.

3. If you changed the private IP address, update the backup location for Cloud Volumes ONTAP configuration files so that the backups are being sent to the new private IP address on the Connector.

   a. Run the following command from the Cloud Volumes ONTAP CLI to remove the current backup target:

   ```
   system configuration backup settings modify -destination ""
   ```

   b. Go to Cloud Manager and open the working environment.

   c. Click the menu and select **Advanced > Configuration Backups**.

   d. Click **Set Backup Target**.

Edit a Connector's URIs

Add and remove the URIs for a Connector.

Steps

1. Click the **Connector** drop-down from the Cloud Manager header.

2. Click **Manage Connectors**.

3. Click the action menu for a Connector and click **Edit URIs**.

4. Add and remove URIs and then click **Apply**.

Fix download failures when using a Google Cloud NAT gateway

The Connector automatically downloads software updates for Cloud Volumes ONTAP. The download can fail if your configuration uses a Google Cloud NAT gateway. You can correct this issue by limiting the number of parts that the software image is divided into. This step must be completed by using the Cloud Manager API.

Step

1. Submit a PUT request to /occm/config with the following JSON as body:

   ```
   {
     "maxDownloadSessions": 32
   }
   ```

The value for *maxDownloadSessions* can be 1 or any integer greater than 1. If the value is 1, then the downloaded image will not be divided.

Note that 32 is an example value. The value that you should use depends on your NAT configuration and the number of sessions that you can have simultaneously.

Learn more about the /occm/config API call.

Upgrade the Connector on-prem without internet access

If you installed the Connector on an on-premises host that doesn't have internet access, you can upgrade the Connector when a newer version is available from the NetApp Support Site.

The Connector needs to restart during the upgrade process so the user interface will be unavailable during the

upgrade.

Steps

1. Download the Cloud Manager software from the NetApp Support Site.

2. Copy the installer to the Linux host.

3. Assign permissions to run the script.

```
chmod +x /path/cloud-manager-connector-offline-v3.9.14
```

4. Run the installation script:

```
sudo /path/cloud-manager-connector-offline-v3.9.14
```

5. After the upgrade is complete, you can verify the Connector's version by going to **Help > Support > Connector**.

> ### What about software upgrades on hosts that have internet access?
>
> The Connector automatically updates its software to the latest version, as long as it has outbound internet access to obtain the software update.

Remove 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 **Manage Connectors**.
3. Click the action menu for an inactive Connector and click **Remove Connector**.

4. Enter the name of the Connector to confirm and then click Remove.

Result

Cloud Manager removes the Connector from its records.

Uninstall the Connector software

Uninstall the Connector software to troubleshoot issues or to permanently remove the software from the host. The steps that you need to use depends on whether you installed the Connector on a host that has internet access or a host in a restricted network that doesn't have internet access.

Uninstall from a host with internet access

The online Connector includes an uninstallation script that you can use to uninstall the software.

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.

Uninstall from a host without internet access

Use these commands if you downloaded the Connector software from the NetApp Support Site and installed it in a restricted network that doesn't have internet access.

Step

1. From the Linux host, run the following commands:

```
docker-compose -f /opt/application/netapp/ds/docker-compose.yml down -v
rm -rf /opt/application/netapp/ds
```

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:

Option	Description
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. Upload the certificate file 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.

Result

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

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 **Change 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.

Configuring a Connector to use an HTTP proxy server

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

(i)   Cloud Manager doesn't support using an HTTPS proxy with the Connector.

Configuring the Connector to use an HTTP proxy server provides outbound internet access if a public IP address or a NAT gateway isn't available. This proxy server provides only the Connector with an outbound connection. It doesn't provide any connectivity for Cloud Volumes ONTAP systems.

If Cloud Volumes ONTAP systems don't have an outbound internet connection to send AutoSupport messages, Cloud Manager automatically configures those Cloud Volumes ONTAP systems to use a proxy server that's

included with the Connector. The only requirement is to ensure that the Connector's security group allows inbound connections over port 3128. You'll need to open this port after you deploy the Connector.

Enable a proxy on a Connector

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.
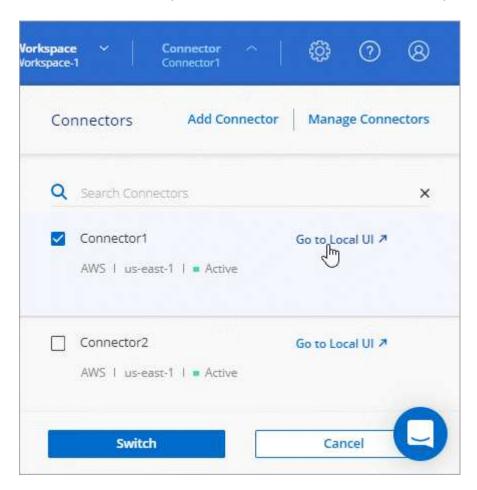
Note that this operation restarts the Connector. Ensure that the Connector isn't performing any operations before you proceed.

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 **Connector Settings**.

4. Under **General**, click **HTTP Proxy Configuration**.

5. Set up the proxy:

   a. Click **Enable Proxy**.

   b. Specify the server using the syntax http://*address:port*

   c. Specify a user name and password if basic authentication is required for the server

   d. Click **Save**.

   > ⓘ   Cloud Manager doesn't support passwords that include the @ character.

Enable direct API traffic

If you configured a proxy server, you can send API calls directly to Cloud Manager without going through the proxy. This option is supported with Connectors that are running in AWS, in Azure, or in Google Cloud.

Steps

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

2. Under **General**, click **Support Direct API Traffic**.

3. Click the checkbox to enable the option and then click **Save**.

Default configuration for the Connector

You might want to learn more about the Connector before you deploy it, or if you need to troubleshoot any issues.

Default configuration with internet access

The following configuration details apply if you deployed the Connector from Cloud Manager, from your cloud provider's marketplace, or if you manually installed the Connector on an on-premises Linux host that has internet access.

AWS details

If you deployed the Connector from Cloud Manager or from the cloud provider's marketplace, note the following:

• The EC2 instance type is t3.xlarge.

• The operating system for the image is Red Hat Enterprise Linux 7.6 (HVM).

The operating system does not include a GUI. You must use a terminal to access the system.

- The user name for the EC2 Linux instance is ec2-user.
- The default system disk is a 100 GiB gp2 disk.

Azure details

If you deployed the Connector from Cloud Manager or from the cloud provider's marketplace, note the following:

- The VM type is DS3 v2.
- The operating system for the image is CentOS 7.6.

  The operating system does not include a GUI. You must use a terminal to access the system.

- The default system disk is a 100 GiB premium SSD disk.

Google Cloud details

If you deployed the Connector from Cloud Manager or from the cloud provider's marketplace, note the following:

- The VM instance is n2-standard-4.
- The operating system for the image is CentOS 7.9.

  The operating system does not include a GUI. You must use a terminal to access the system.

- The default system disk is a 100 GiB SSD persistent disk.

Installation folder

The Connector installation folder resides in the following location:

/opt/application/netapp/cloudmanager

Log files

Log files are contained in the following folders:

- /opt/application/netapp/cloudmanager/log

  The logs in this folder provide details about the Connector and docker images.

- /opt/application/netapp/cloudmanager/docker_occm/data/log

  The logs in this folder provide details about cloud services and the Cloud Manager service that runs on the Connector.

Connector service

- 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.

Packages

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

Ports

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

Default configuration without internet access

The following configuration applies if you manually installed the Connector on an on-premises Linux host that doesn't have internet access. Learn more about this installation option.

- The Connector installation folder resides in the following location:

  /opt/application/netapp/ds

- Log files are contained in the following folders:

  /var/lib/docker/volumes/ds_occmdata/_data/log

  The logs in this folder provide details about the Connector and docker images.

- All services are running inside docker containers

  The services are dependent on the docker runtime service running

- The Connector uses the following ports on the Linux host:
  - 80 for HTTP access

- 443 for HTTPS access