Advanced deployment

Set up and administration

NetApp
September 22, 2022

Table of Contents

Advanced deployment

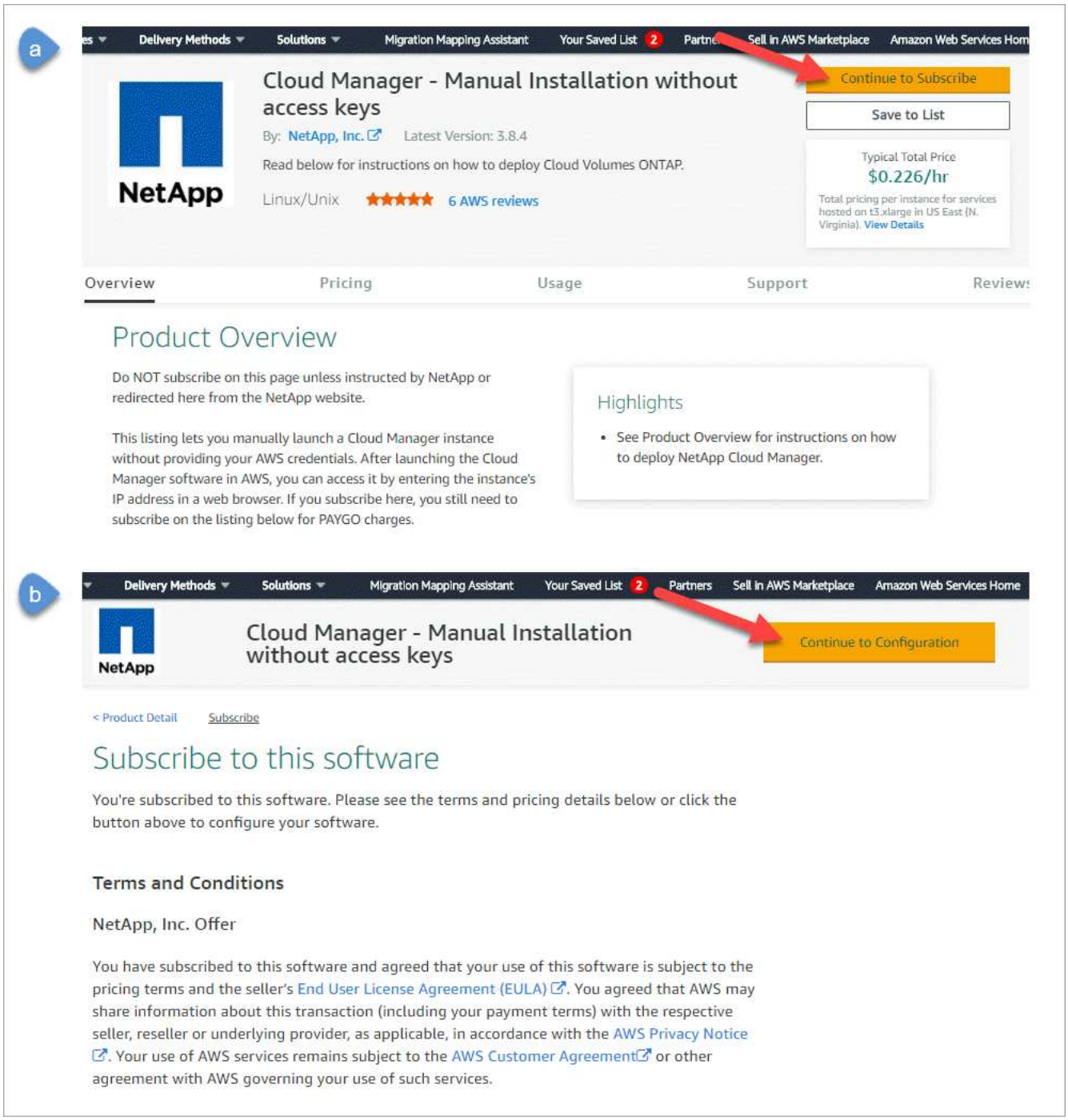
Create a Connector from the AWS Marketplace

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. 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. 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**.



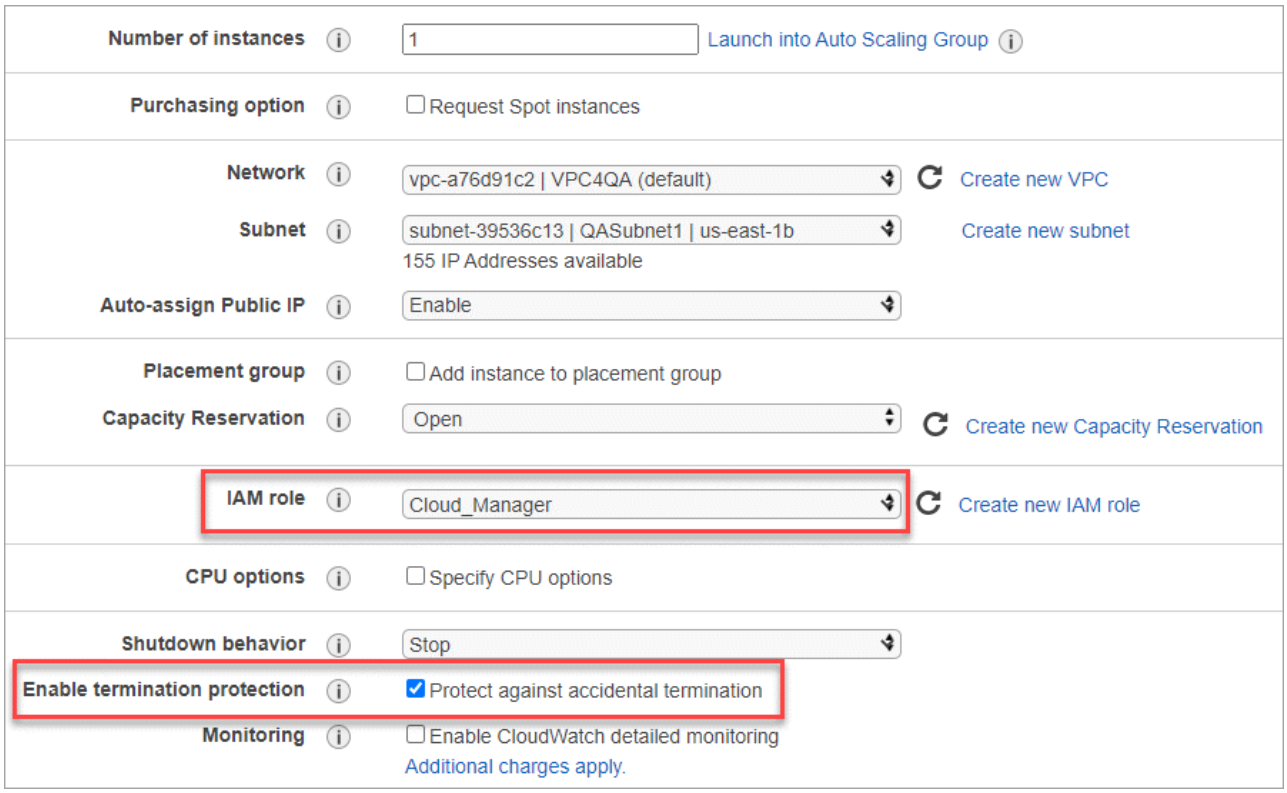
4. Change any of the default options and click **Continue to Launch**.
5. Under **Choose Action**, select **Launch through EC2** and then click **Launch**.

   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.



- **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.

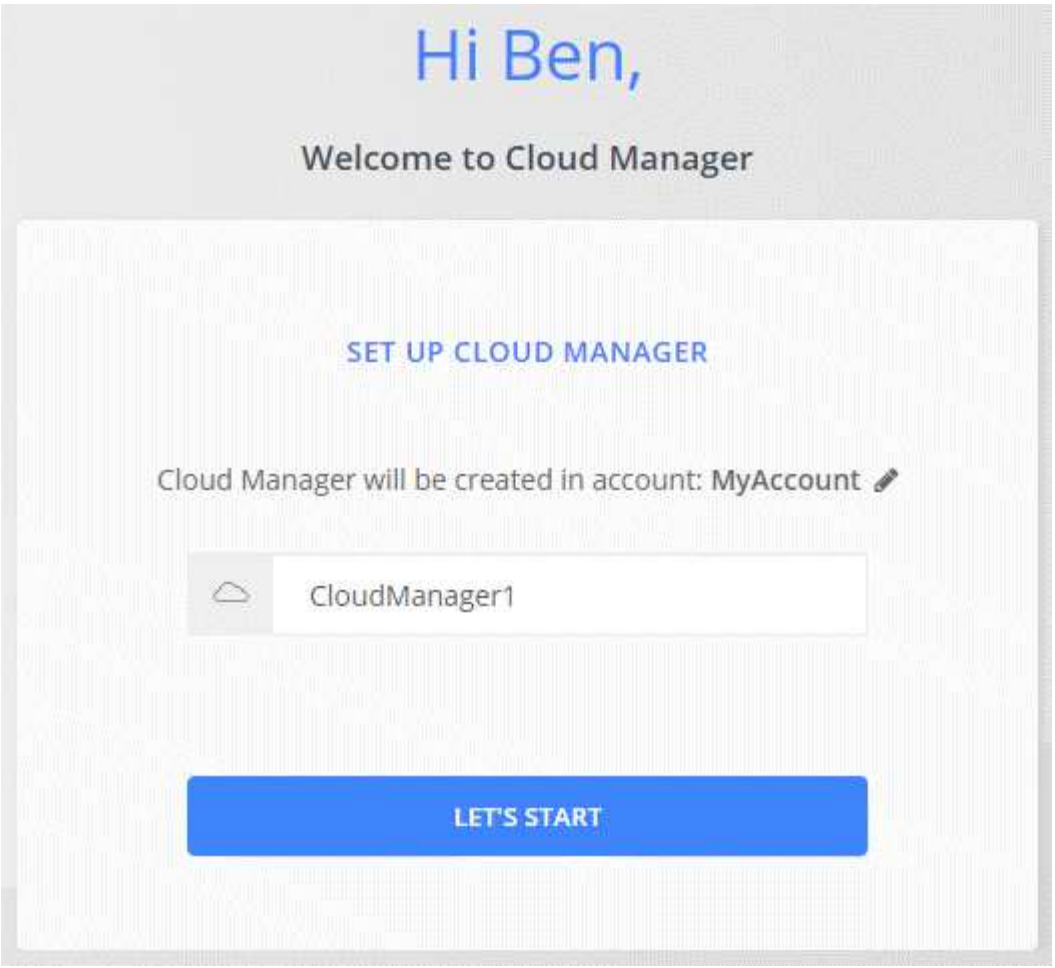
7. Open a web browser from a host that has a connection to the Connector instance and enter the following URL:

   http://*ipaddress*:80

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

After you finish

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

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 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.

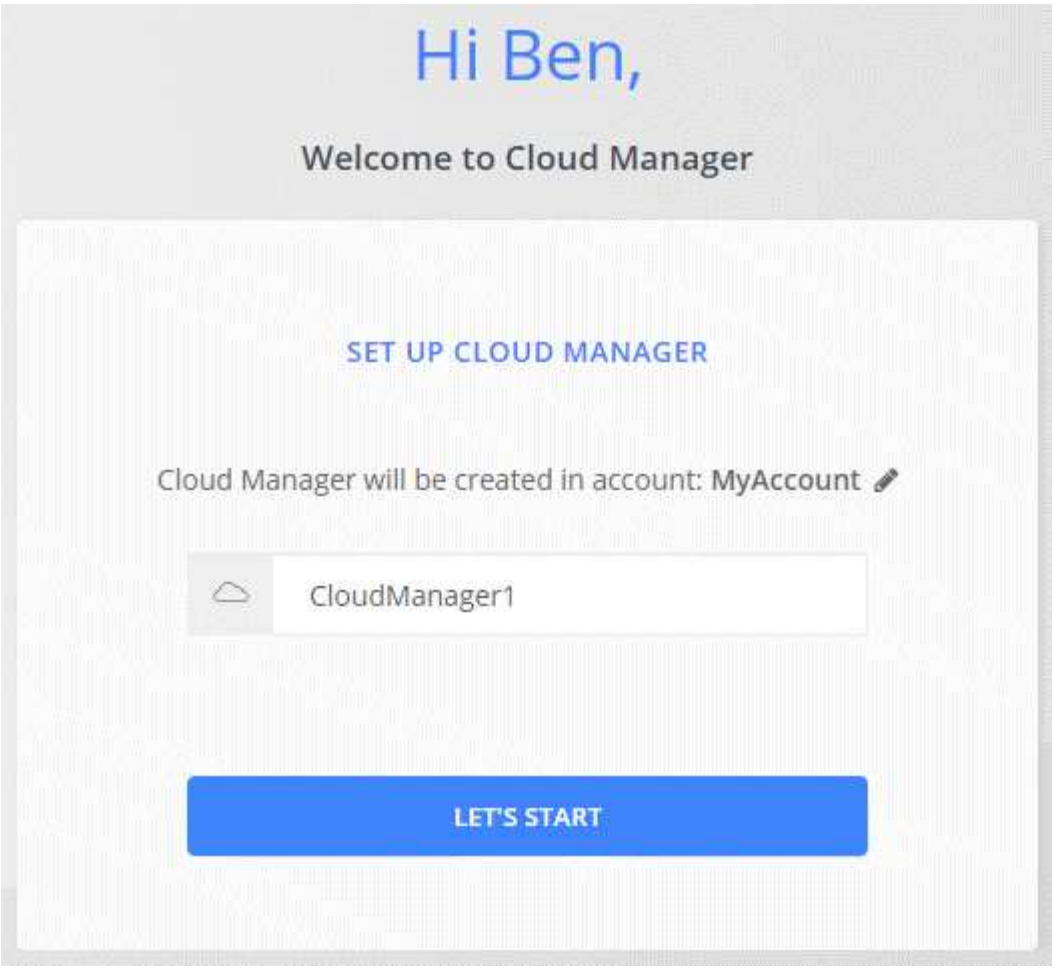
5. Open a web browser from a host that has a connection to the Connector virtual machine and enter the following URL:

   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. 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:
   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.

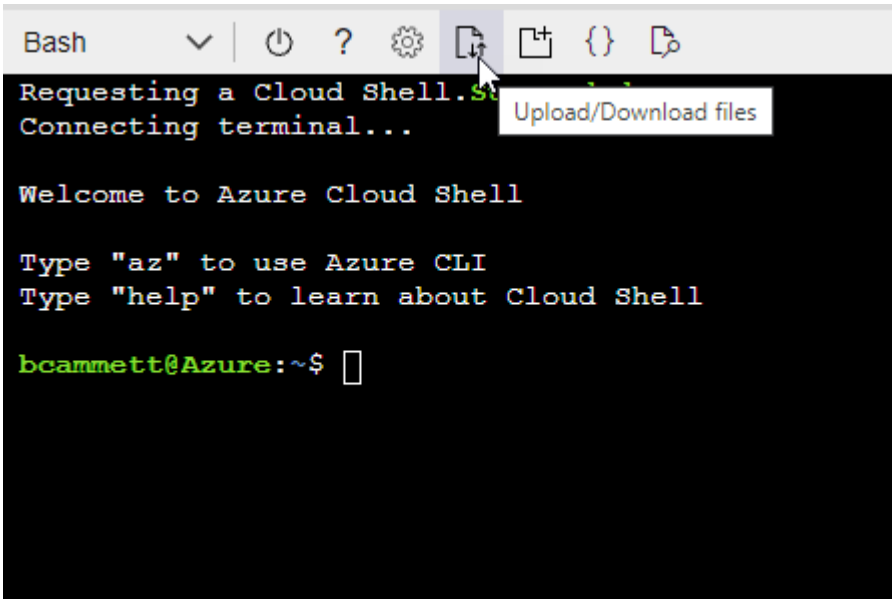
      Example

```
"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**.

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.

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:

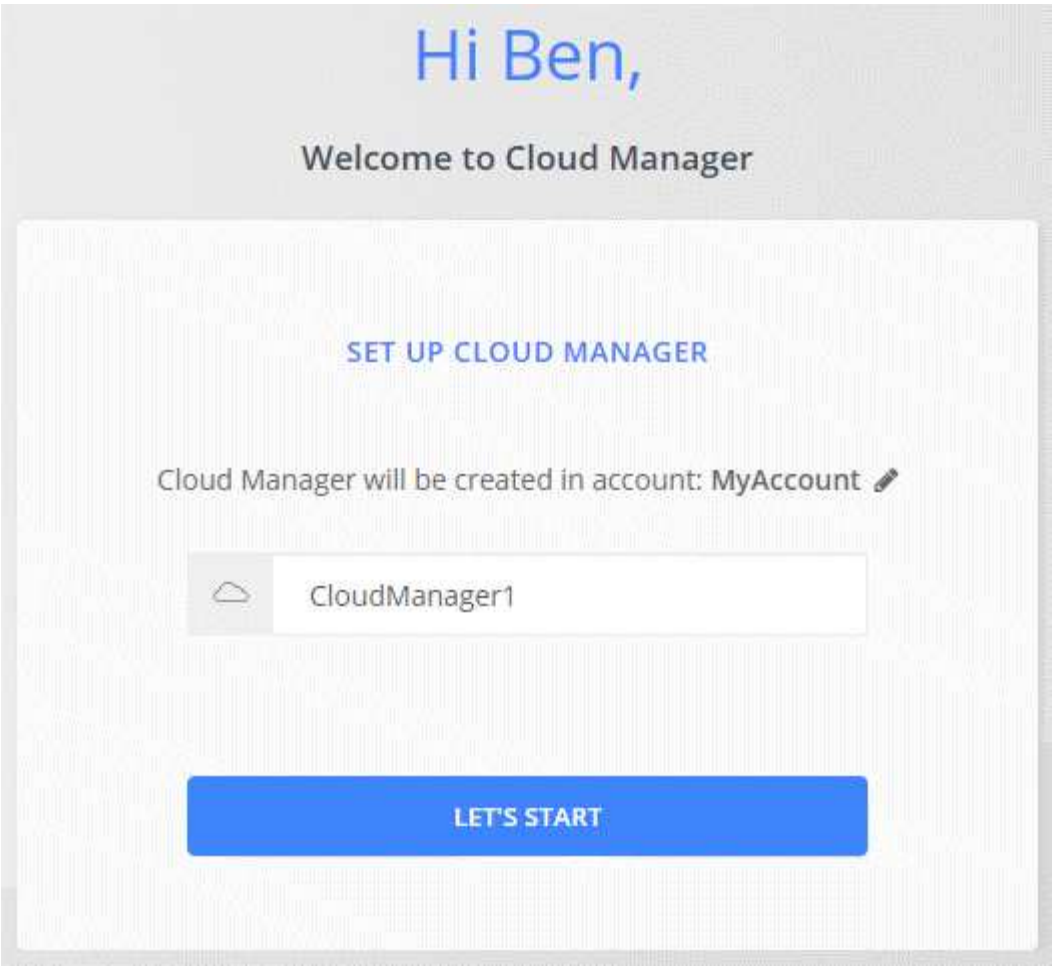
   https://*ipaddress*

   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:

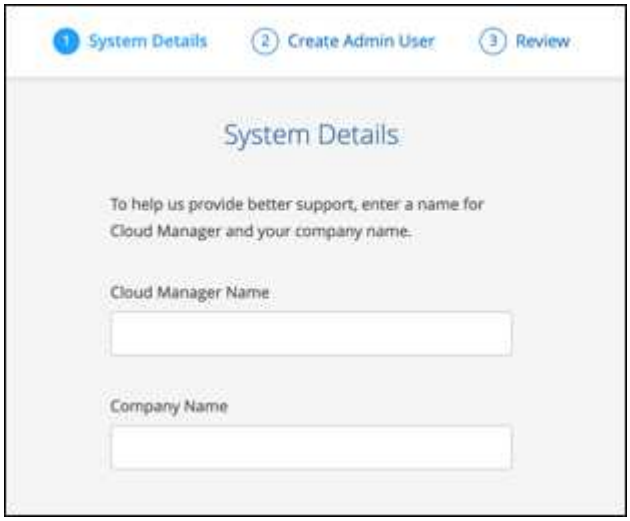
```
sudo /path/cloud-manager-connector-offline-v3.9.19
```

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.