Additional installation options

Cloud Manager 3.4

NetApp
June 06, 2022

Table of Contents

Additional installation options

Cloud Manager host requirements

If you install Cloud Manager on your own host, then you must verify support for your configuration, which includes operating system requirements, port requirements, and so on.

AWS EC2 instance type	t2.medium or m3.large
Azure VM size	A2 or D2_v2
Operating system	• CentOS 7.2 • CentOS 7.3 • CentOS 7.4 • Red Hat Enterprise Linux 7.2 • Red Hat Enterprise Linux 7.3 • Red Hat Enterprise Linux 7.4 Cloud Manager is supported on English-language versions of these operating systems.
Hypervisor	A bare metal or hosted hypervisor that is certified to run CentOS or Red Hat Enterprise Linux Red Hat Solution: Which hypervisors are certified to run Red Hat Enterprise Linux?
CPU	2.27 GHz or higher with two cores
RAM	4 GB
Free disk space	50 GB
Ports	The following ports must be available: • 80 for HTTP access • 443 for HTTPS access • 3306 for the Cloud Manager database • 8080 for the Cloud Manager API proxy

If other services are using these ports, Cloud Manager installation fails.

There is a potential conflict with port 3306. If another instance of MySQL is running on the host, it uses port 3306 by default. You must change the port that the existing MySQL instance uses.

You can change the default HTTP and HTTPS ports when you install Cloud Manager. You cannot change the default port for the MySQL database. If you change the HTTP and HTTPS ports, you must ensure that users can access the Cloud Manager web console from a remote host:

- Modify the security group to allow inbound connections through the ports.
- Specify the port when you enter the URL to the Cloud Manager web console.

Granting permissions when Cloud Manager is not launched from Cloud Central

If you cannot launch Cloud Manager in AWS from NetApp Cloud Central, then you must provide Cloud Manager with the permissions that it needs if you want to launch and manage ONTAP Cloud in AWS.

About this task

The Cloud Manager IAM policy defines the AWS actions and resources that Cloud Manager is allowed to use. You can grant the permissions defined in the IAM policy in one of two ways:

- You can attach an IAM role to the Cloud Manager instance in AWS.
- You can attach the IAM policy to IAM users or groups.

  You would then specify the AWS access keys for those users in Cloud Manager.

Steps

1. Download the Cloud Manager IAM policy from the following location:

   NetApp OnCommand Cloud Manager: AWS and Azure Policies

2. From the IAM console, create your own policy by copying and pasting the text from the Cloud Manager IAM policy.
3. Grant permissions to the Cloud Manager instance or to IAM users:

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

Result

Cloud Manager now has the permissions that it needs. If you attached the policy to IAM users, you must specify the AWS access keys for those IAM users when you set up user accounts in Cloud Manager.

Launching Cloud Manager from the AWS Marketplace

It is best to launch Cloud Manager in AWS using NetApp Cloud Central, but you can launch it from the AWS Marketplace, if needed.

Before you begin

If you want to assign a public IP address to the Cloud Manager instance and use the AWS 1-Click Launch option, the public subnet must be already enabled to automatically assign public IP addresses. Otherwise, you must use the Manual Launch option to assign a public IP address to the instance.

For details, refer to AWS Documentation: IP Addressing in Your VPC.

Steps

1. Set up an IAM role that includes the required permissions.

   Granting permissions when Cloud Manager is not launched from Cloud Central

2. Go to the Cloud Manager page on the AWS Marketplace.
3. Click **Continue**.
4. Launch the instance from the 1-Click Launch tab or the Custom Launch tab, depending on how you want to grant AWS permissions to Cloud Manager:

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

Result

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

After you finish

Log in to Cloud Manager by entering the public IP address or private IP address in a web browser and then complete the Setup wizard.

Installing Cloud Manager on an existing Linux host

If you want to run the Cloud Manager software on an existing host, you can download and install the software on a Linux host in your network or in the cloud.

About this task

- Root privileges are not required to install Cloud Manager.
- Cloud Manager installs the AWS command line tools (awscli) to enable recovery procedures from NetApp support.

  If you receive a message that installing the awscli failed, you can safely ignore the message. Cloud Manager can operate successfully without the tools.

Steps

1. Review networking requirements for your cloud service provider:
   - AWS networking requirements
   - Azure networking requirements
   - IBM Cloud networking requirements
2. Set up permissions for Cloud Manager:
   a. If you want to deploy ONTAP Cloud systems in AWS, set up an IAM role that includes the required permissions.
   b. If you want to deploy ONTAP Cloud systems in Azure, create and set up a service principal in Azure Active Directory.
3. Review Cloud Manager host requirements.
4. Download the software from the NetApp Support Site, and then copy it to the Linux host.

   For help with connecting and copying the file to an EC2 instance in AWS, see AWS Documentation: Connecting to Your Linux Instance Using SSH.

5. Assign permissions to execute the script.

   Example

   ```
   chmod +x OnCommandCloudManager-V3.4.0.sh
   ```

6. Run the installation script:

   ```
   ./OnCommandCloudManager-V3.4.0.sh [silent] [proxy=ipaddress] [proxyport=port]
   [proxyuser=user_name] [proxypwd=password]
   ```

   silent runs the installation without prompting you for information.

   proxy is required if the Cloud Manager host is behind a proxy server.

proxyport is the port for the proxy server.

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

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

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

   If you change the HTTP and HTTPS ports, you must ensure that users can access the Cloud Manager web console from a remote host:

   - Modify the security group to allow inbound connections through the ports.
   - Specify the port when you enter the URL to the Cloud Manager web console.

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

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

   https://*ipaddress*:*port*

   ipaddress can be localhost, a private IP address, or a public IP address, depending on the configuration of the Cloud Manager host. For example, if Cloud Manager is in the public cloud without a public IP address, you must enter a private IP address from a host that has a connection to the Cloud Manager host.

   port is required if you changed the default HTTP (80) or HTTPS (443) ports. For example, if the HTTPS port was changed to 8443, you would enter https://*ipaddress*:8443

9. Sign up for a NetApp Cloud Central account or log in if you already have one.
10. When you sign up or log in, Cloud Manager automatically adds your user account as the administrator for this system.
11. After you log in, enter a name for this Cloud Manager system.

After you finish

You can start creating ONTAP Cloud systems but you might want to perform additional setup first.

Installing Cloud Manager in an Azure US Gov region

To deploy Cloud Manager in an Azure US Gov region, you must download the Cloud Manager installer from the NetApp Support Site and install it on an existing CentOS 7.3 host.

About this task

For a list of supported Azure US Gov regions, see Supported Azure regions.

Steps

1. Review networking requirements for Azure.
2. Grant Azure permissions to Cloud Manager.
3. Create a CentOS 7.3 virtual machine from the Azure Marketplace.

While Cloud Manager supports other operating systems, it only supports CentOS 7.3 in the Azure US Gov regions.

4. Download and install Cloud Manager.

After you finish

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

Installing Cloud Manager in the Azure Germany region

The Azure Marketplace is not available in the Azure Germany region, so you must download the Cloud Manager installer from the NetApp Support Site and install it on an existing Linux host in the region.

Steps

1. Review networking requirements for Azure.
2. Grant Azure permissions to Cloud Manager.
3. Review Cloud Manager host requirements.
4. Download and install Cloud Manager.

After you finish

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