



Networking requirements for Cloud Manager

Cloud Manager 3.5

NetApp
11/01/2018

Table of Contents

1. Networking requirements for Cloud Manager	1
1.1. Connection to target networks	1
1.2. Outbound internet access	1
1.3. Ports and security groups	4

1. Networking requirements for Cloud Manager

You must set up your networking so that Cloud Manager can deploy Cloud Volumes ONTAP systems in AWS or in Microsoft Azure. The most important step is ensuring outbound internet access to various endpoints.



If your network uses a proxy server for all communication to the internet, Cloud Manager prompts you to specify the proxy during setup. You can also specify the proxy server from the Settings page. Refer to [Configuring Cloud Manager to use a proxy server](#).

1.1. Connection to target networks

Cloud Manager requires a network connection to the AWS VPCs and Azure VNets in which you want to deploy Cloud Volumes ONTAP.

For example, if you install Cloud Manager in your corporate network, then you must set up a VPN connection to the AWS VPC or Azure VNet in which you launch Cloud Volumes ONTAP.

1.2. Outbound internet access

Cloud Manager requires outbound internet access to deploy and manage Cloud Volumes ONTAP. Outbound internet access is also required when accessing Cloud Manager from your web browser and when running the Cloud Manager installer on a Linux host.

The following sections identify the specific endpoints.

Outbound internet access to manage Cloud Volumes ONTAP in AWS

Cloud Manager requires outbound internet access to contact the following endpoints when deploying and managing Cloud Volumes ONTAP in AWS:

Endpoints	Purpose
<p>AWS services (amazonaws.com):</p> <ul style="list-style-type: none"> • CloudFormation • Elastic Compute Cloud (EC2) • Key Management Service (KMS) • Security Token Service (STS) • Simple Storage Service (S3) <p>The exact endpoint depends on the region in which you deploy Cloud Volumes ONTAP. Refer to AWS documentation for details.</p>	Enables Cloud Manager to deploy and manage Cloud Volumes ONTAP in AWS.
api.services.cloud.netapp.com:443	API requests to NetApp Cloud Central.
cloud.support.netapp.com.s3.us-west-1.amazonaws.com	Provides access to software images, manifests, and templates.
cognito-idp.us-east-1.amazonaws.com cognito-identity.us-east-1.amazonaws.com	Enables Cloud Manager to access and download manifests, templates, and Cloud Volumes ONTAP upgrade images.
kinesis.us-east-1.amazonaws.com	Enables NetApp to stream data from audit records.
https://netapp-cloud-account.auth0.com	Communication with NetApp Cloud Central for centralized user authentication.
https://mysupport.netapp.com	Communication with NetApp AutoSupport.
https://support.netapp.com/svcgw https://support.netapp.com/ServiceGW/entitlement	Communication with NetApp for licensing and support registration.
<p>Various third-party locations, for example:</p> <ul style="list-style-type: none"> • https://repo1.maven.org/maven2 • https://oss.sonatype.org/content/repositories • https://repo.typesafe.org <p>Third-party locations are subject to change.</p>	During upgrades, Cloud Manager downloads the latest packages for third-party dependencies.

Outbound internet access to manage Cloud Volumes ONTAP in Azure

Cloud Manager requires outbound internet access to contact the following endpoints when deploying and managing Cloud Volumes ONTAP in Microsoft Azure:

Endpoints	Purpose
https://management.azure.com https://login.microsoftonline.com	Enables Cloud Manager to deploy and manage Cloud Volumes ONTAP in most Azure regions.
https://management.microsoftazure.de https://login.microsoftonline.de	Enables Cloud Manager to deploy and manage Cloud Volumes ONTAP in the Azure Germany regions.
https://management.usgovcloudapi.net https://login.microsoftonline.com	Enables Cloud Manager to deploy and manage Cloud Volumes ONTAP in the Azure US Gov regions.
api.services.cloud.netapp.com:443	API requests to NetApp Cloud Central.
cloud.support.netapp.com.s3.us-west-1.amazonaws.com	Provides access to software images, manifests, and templates.
cognito-idp.us-east-1.amazonaws.com cognito-identity.us-east-1.amazonaws.com sts.amazonaws.com	Enables Cloud Manager to access and download manifests, templates, and Cloud Volumes ONTAP upgrade images.
kinesis.us-east-1.amazonaws.com	Enables NetApp to stream data from audit records.
https://netapp-cloud-account.auth0.com	Communication with NetApp Cloud Central for centralized user authentication.
https://mysupport.netapp.com	Communication with NetApp AutoSupport.
https://support.netapp.com/svcgw https://support.netapp.com/ServiceGW/entitlement	Communication with NetApp for licensing and support registration.
<p>Various third-party locations, for example:</p> <ul style="list-style-type: none"> • https://repo1.maven.org/maven2 • https://oss.sonatype.org/content/repositories • https://repo.typesafe.org <p>Third-party locations are subject to change.</p>	During upgrades, Cloud Manager downloads the latest packages for third-party dependencies.

Outbound internet access from your web browser

Users must access Cloud Manager from a web browser. The machine running the web browser must have connections to the following endpoints:

Endpoints	Purpose
The Cloud Manager host	<p>You must enter the host's IP address from a web browser to load the Cloud Manager console.</p> <p>If you deploy Cloud Manager in AWS, the easiest way to provide access is by allocating a public IP address. However, if you want to use a private IP address instead, users can access the console through either of the following:</p> <ul style="list-style-type: none"> • A jump host in the VPC that has a connection to Cloud Manager • A host in your network that has a VPN connection to the private IP address
https://auth0.com https://netapp-cloud-account.auth0.com https://services.cloud.netapp.com	Your web browser connects to these endpoints for centralized user authentication through NetApp Cloud Central.

Outbound internet access to install Cloud Manager on a Linux host

The Cloud Manager installer must access the following URLs during the installation process:

- <http://dev.mysql.com/get/mysql-community-release-el7-5.noarch.rpm>
- <https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm>
- <https://s3.amazonaws.com/aws-cli/awscli-bundle.zip>

1.3. Ports and security groups

- If you deploy Cloud Manager from Cloud Central or from the marketplace images, refer to the following:
 - [Security group rules for Cloud Manager in AWS](#)
 - [Security group rules for Cloud Manager in Azure](#)
- If you install Cloud Manager on an existing Linux host, see [Cloud Manager host requirements](#).