# Networking requirements for Cloud Manager

## Cloud Manager 3.5

Ben Cammett

11/01/2018

# Table of Contents

# 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.

## 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.

## 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 |
| --- | --- |
| AWS services (amazonaws.com):<br>• CloudFormation<br>• Elastic Compute Cloud (EC2)<br>• Key Management Service (KMS)<br>• Security Token Service (STS)<br>• Simple Storage Service (S3)<br>The exact endpoint depends on the region in which you deploy Cloud Volumes ONTAP. Refer to AWS documentation for details. | 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<br>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<br>https://support.netapp.com/ServiceGW/entitlement | Communication with NetApp for licensing and support registration. |
| Various third-party locations, for example:<br>• https://repo1.maven.org/maven2<br>• https://oss.sonatype.org/content/repositories<br>• https://repo.typesafe.org<br>Third-party locations are subject to change. | 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<br>https://login.microsoftonline.com | Enables Cloud Manager to deploy and manage Cloud Volumes ONTAP in most Azure regions. |
| https://management.microsoftazure.de<br>https://login.microsoftonline.de | Enables Cloud Manager to deploy and manage Cloud Volumes ONTAP in the Azure Germany regions. |
| https://management.usgovcloudapi.net<br>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<br>cognito-identity.us-east-1.amazonaws.com<br>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<br>https://support.netapp.com/ServiceGW/entitlement | Communication with NetApp for licensing and support registration. |
| Various third-party locations, for example:<br>• https://repo1.maven.org/maven2<br>• https://oss.sonatype.org/content/repositories<br>• https://repo.typesafe.org<br>Third-party locations are subject to change. | 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 | You must enter the host's IP address from a web browser to load the Cloud Manager console.<br><br>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:<br><br>• A jump host in the VPC that has a connection to Cloud Manager<br>• A host in your network that has a VPN connection to the private IP address |
| https://auth0.com<br>https://netapp-cloud-account.auth0.com<br>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

# 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.

**Copyright Information**

Copyright © 2019–2020 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system-without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

**Trademark Information**

NETAPP, the NETAPP logo, and the marks listed at http://www.netapp.com/TM are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.