Getting started checklist

Cloud Manager

Ben Cammett
July 06, 2021

This PDF was generated from https://docs.netapp.com/us-en/occm/reference_checklist_cm.html on September 14, 2021. Always check docs.netapp.com for the latest.

Table of Contents

Getting started checklist 1

Getting started checklist

This checklist describes what's needed to get up and running with Cloud Manager.

A NetApp Cloud Central login

You need to sign up to NetApp Cloud Central so you can access Cloud Manager and other cloud services.

Network access from a web browser to several endpoints

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

Endpoints	Purpose
https://cloudmanager.cloud.netapp.com	To connect you to the Cloud Manager SaaS interface.
https://api.services.cloud.netapp.com	To contact Cloud Central APIs.
https://auth0.com https://cdn.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.
https://widget.intercom.io	For in-product chat that enables you to talk to NetApp cloud experts.

A network location for a Connector

After logging in to Cloud Manager, an Account Admin will need to deploy a *Connector* in a cloud provider or in your on-premises network. The Connector enables Cloud Manager to manage resources and processes within your public cloud environment. A Connector isn't required for Azure NetApp Files, Cloud Volumes Service, or Cloud Sync, but it is required for all other services and features in Cloud Manager. Learn more about Connectors and how they work.

- The network location must have an outbound internet connection.

  The Connector requires outbound internet access to manage resources and processes within your public cloud environment. Outbound internet access is also required if you want to manually install the Connector on a Linux host or access the local UI running on the Connector.

  View the specific endpoints that the Connector contacts.

- There's no incoming traffic to the Connector, unless you initiate it.

  HTTP (80) and HTTPS (443) provide access to the local UI, which you'll use in rare circumstances. SSH (22) is only needed if you need to connect to the host for troubleshooting.

Cloud provider permissions

You need an account that has permissions to deploy the Connector in your cloud provider directly from Cloud Manager.

There are alternative ways to create a Connector. You also have the option to create a Connector from the AWS Marketplace, Azure Marketplace, or to manually install the software.

Location	High-level steps	Detailed steps
AWS	1. Use a JSON file that includes the required permissions to create an IAM policy in AWS. 2. Attach the policy to the IAM user who will create the Connector from Cloud Manager. 3. When you create the Connector, provide Cloud Manager with the AWS access key and secret key for the IAM user that has the required permissions.	Click here to view detailed steps.
Azure	1. Use a JSON file that includes the required permissions to create a custom role in Azure. 2. Assign the role to the user who will create the Connector from Cloud Manager. 3. When you create the Connector, log in with the Microsoft account that has the required permissions (the login prompt that is owned and hosted by Microsoft).	Click here to view detailed steps.
Google Cloud	1. Use a YAML file that includes the required permissions to create a custom role in Google Cloud. 2. Attach that role to the user who will create the Connector from Cloud Manager. 3. If you plan to use Cloud Volumes ONTAP, set up a service account that has the required permissions. 4. Enable Google Cloud APIs. 5. When you create the Connector, log in with the Google account that has the required permissions (the login prompt is owned and hosted by Google).	Click here to view detailed steps.

Networking for individual services

Now that your setup is complete, you're ready to start using the services available from Cloud Manager. Note that each service has its own networking requirements. Refer to the following pages for more details.

- Cloud Volumes ONTAP for AWS
- Cloud Volumes ONTAP for Azure
- Cloud Volumes ONTAP for GCP
- Data replication between ONTAP systems
- Cloud Data Sense for Cloud Volumes ONTAP, on-premises ONTAP, or Azure NetApp Files
- Cloud Data Sense for Amazon S3
- Cloud Data Sense for generic S3 object storage
- Cloud Data Sense for non-NetApp NFS or CIFS file shares
- Cloud Data Sense for databases
- Cloud Data Sense for OneDrive accounts

- On-prem ONTAP clusters
  - Data tiering from ONTAP clusters to Amazon S3
  - Data tiering from ONTAP clusters to Azure Blob storage
  - Data tiering from ONTAP clusters to Google Cloud Storage
  - Data tiering from ONTAP clusters to StorageGRID
  - Data backup from ONTAP clusters to Amazon S3 or Azure Blob storage

Copyright Information

Copyright © 2021 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.