



Get started

Cloud Manager Automation

NetApp
October 07, 2021

Table of Contents

- Getting started 1
 - Before you begin 1
 - Get the client and account identifiers 2
 - Add NSS credentials key 3
 - Hello world 3
 - Understanding the workflow processes 4
 - Typical Cloud Manager deployment 8

Getting started

You can quickly get started using the Cloud Manager REST API by first preparing as described in [Before you begin](#). You'll also need a client identifier to test the curl sample in [Hello world](#). After that you can begin preparing to use the workflows and plan a deployment.

Before you begin

There are several things you should do to prepare before using the Cloud Manager REST API and associated workflows.

Review REST concepts and implementation

Make sure to review [REST implementation details](#) for information about REST concepts and the details of how the Cloud Manager REST API is designed.

Decide on the cloud provider and have credentials

Cloud Volumes ONTAP can be deployed in Amazon Web Services, Microsoft Azure, and Google Cloud Platform. You need to decide which of these providers you'll use and have the appropriate credentials.

Have Cloud Central credentials

You'll need a NetApp account (formerly NetApp Cloud Central) login to acquire an access token required for the workflow processes. See [Signing up to NetApp Cloud Central](#) for more information.

Be familiar with Cloud Volumes ONTAP concepts

If you intend to perform Cloud Volumes ONTAP administration tasks, you should be familiar with Cloud Volumes ONTAP concepts, terminology, and procedures. See [Learn about Cloud Volumes ONTAP](#) for more information.

Decide on the licensing model

You can create and manage Cloud Volumes ONTAP instances using a subscription PAYGO ("pay as you go") model or apply your own licenses with BYOL ("bring your own license"). You need to decide which licensing model you'll use and be ready to adjust the workflows as needed.

Prepare to use the workflow processes

Review [Understand the workflow processes](#) for more information about the organization and content of the workflows. Also see [Typical Cloud Manager deployment](#).



This documentation does not describe or use the Local UI.

Locate the client identifier

You'll need the `client_id` value for several of the workflows. For more information see [Get the client and account identifiers](#).

Get the client and account identifiers

You can sign into the Cloud Manager web user interface to retrieve the client and account identifiers to use with the workflows. You can use these identifiers to access the metadata, authentication, and security related information.



This page includes two tasks describing how to use the Cloud Manager web user interface to retrieve the ID values. You can also use the Cloud Manager REST API to get these values. See [Get supported services](#) for more information.

Get the client identifier

You can retrieve the client ID and use it with the `x-agent-id` HTTP request header.

About this task

You need to access the client ID which is unique for each Cloud Manager Connector and then use it as the agent identifier.

Before you begin

You must have a NetApp account (formerly Cloud Central account). You created this account when you first logged in to Cloud Manager and it's displayed at the top of the Cloud Manager user interface. [Learn more about NetApp accounts.](#)

Steps

1. Navigate to the Cloud Manager web site using a browser:

<https://cloudmanager.netapp.com>

2. Sign in using your NetApp account (formerly Cloud Central account) credentials.
3. Click **Connector** at the top right of the page and select **Manage Connectors**.
4. On the **Manage Connectors** page, click the ellipses (...) icon.
5. Select the **Connector ID**. This value is based on the **client ID**.

You can use the Connector ID in the `x-agent-id` HTTP request header as shown in the workflow curl examples, for example: `x-agent-id: uzJbMFKEnuzi2ryLaENbCP52KBTXx0aIclients`.

Get the account identifier

You can also retrieve the account ID.

About this task

You can create multiple accounts and access the unique identifier for each account.

Before you begin

You must have a NetApp account (formerly Cloud Central account). You created this account when you first logged in to Cloud Manager and it's displayed at the top of the Cloud Manager user interface. [Learn more about NetApp accounts.](#)

Steps

1. Navigate to the Cloud Manager web site using a browser:

<https://cloudmanager.netapp.com>

2. Sign in using your NetApp account (formerly Cloud Central account) credentials.
3. Click the **Account** drop-down and click **Manage Account** for the selected account.
4. In the **Overview** section copy the **Account ID** value.

Add NSS credentials key

You can sign in to the Cloud Manager web user interface to create a new NetApp Support Site (NSS) credentials key.



You need the NSS key when creating a working environment that uses BYOL ("bring your own") licensing.

Add the NSS key

You can create an NSS key and use it when creating a working environment.

Before you begin

You must have a NetApp account (formerly Cloud Central account). You created this account when you first logged in to Cloud Manager and it's displayed at the top of the Cloud Manager user interface. [Learn more about NetApp accounts.](#)

Steps

1. Navigate to the Cloud Manager web site using a browser:

<https://cloudmanager.netapp.com>

2. Sign in using your NetApp account (formerly Cloud Central account) credentials.
3. Click on the ? icon at the top right of the page and select **Support**.
4. Navigate to the **NSS Management** tab and click **Add NSS Account**.
5. Provide the NSS username and password and click **Register**. After successful registration, an NSS key ID will be generated.

Hello world

You can issue a curl command to get started using the Cloud Manager REST API and confirm its availability.



The example provided below is very simple. The workflow samples later in this guide use a more robust format. As a start, see [Understanding the workflow processes.](#)

Before you begin

You must do the following:

- Determine the identifier to use for the `x-agent-id` request header as well as the related client ID. See

Get the client and account identifiers.

- Acquire an access token for the `Authorization` request header. See [Create user token](#).

Curl example

The following curl command retrieves information about the Cloud Manager server.

```
curl --location --request GET
'https://cloudmanager.cloud.netapp.com/occm/api/occm/system/about'
--header 'Content-Type: application/json' --header 'x-agent-id:
<AGENT_ID>' --header 'Authorization: Bearer <ACCESS_TOKEN>'
```

Output example

Information about the system is provided in the following format.

```
{
  "version": "string",
  "build": "string",
  "buildTimestamp": "integer",
  "systemId": "string",
  "environment": "string",
  "siteIdentifier": {
    "company": "string",
    "host": "string",
    "site": "string"
  },
  "serverTimeZone": {
    "timeZoneName": "string",
    "formattedTimeZone": "string"
  },
  "beta": "boolean",
  "releaseNumber": "integer",
  "simplicatorUrl": "string",
  "migrationPerformed": "boolean",
  "demoMode": "boolean",
  "usingDockerInfra": "boolean",
  "privateIp": "string"
}
```

Understanding the workflow processes

You should be familiar with the high-level organization and format of the Cloud Manager workflow processes before using them with a live cloud deployment.

Introduction

A **workflow** is a sequence of one or more steps needed to accomplish a specific administrative task or goal. With the Cloud Manager workflows, each step can be one of the following:

- REST API call
- Invocation of another workflow
- Miscellaneous task such as deciding on the size of a new volume

The workflows provided include the minimum steps and parameters needed to accomplish each task. You can use these workflows as a starting point and customize them for your environment as needed.



All the workflow examples are designed to be used with NetApp Cloud Volumes ONTAP.

High level organization of the workflows

At a high level, the workflows are organized based on three primary attributes. The organization is reflected in the navigation sidebar.

1. Cloud provider

Most of the workflows can be performed with one cloud provider. The supported cloud platforms include:

- Amazon Web Services
- Microsoft Azure
- Google Cloud Platform

In addition, some workflows are not tied to a specific cloud provider and can be performed in any cloud environment. These workflows are considered to be **common** to all the cloud providers.

2. Functional category

The workflows for each cloud provider are placed in a specific functional category. The major categories as reflected in the navigation sidebar are presented below.

Working environments

A working environment is the context within which a Cloud Volumes ONTAP instance is deployed and runs. These workflows allow you to create workflows and perform related administration.

Aggregates

An aggregate is the low-level structure for Cloud Volumes ONTAP storage. These workflows allow you to create aggregates and perform related administration.

Volumes

The storage volumes can be exposed for use by your applications. These workflows allow you to create volumes and perform related administration.

Metadata

The metadata workflows allow you to view and administer the basic configuration of your cloud environment.

Miscellaneous

Workflows that are not clearly assigned to another functional category are considered miscellaneous.

3. Single node and High Availability workflows

Many of the workflows vary based on the type of the deployment.

Single node

The cluster consists of a single Cloud Volumes ONTAP instance or ONTAP node.

HA pair

The cluster consists of two linked Cloud Volumes ONTAP instances which together provide the ONTAP high availability (HA) feature.



If both versions of a workflow exist for an administrative task they are included on the same page.

Base URLs and REST endpoint paths

The REST API calls in the workflows use different URLs and URL formats depending on the desired service and resource.



Every API call used in the workflows includes the resource path to the REST endpoint. The path is relative and appended to the appropriate **base** URL. Unless otherwise indicated for a specific API call, the base URL addresses the NetApp Cloud Manager service. You should always carefully review the curl examples provided in the workflows before using them.

Cloud Manager endpoints

The majority of the workflow REST API calls are made to the **NetApp Cloud Manager** service. The base URL of the SaaS interface is:

<https://cloudmanager.netapp.com/>

Auth0 authentication service

Some of the REST API calls used in the identity workflows are made to the **Auth0** token authentication service. The base URL is:

<https://netapp-cloud-account.auth0.com/>

Common parameters and variables

There are several parameters or variables common among the workflows.

Request headers

Nearly all the REST API calls used in the workflows require the following two request headers.



Rather than cite these headers as a prerequisite in every REST API call, they are considered a universal requirement. If a workflow does not use these headers or has different prerequisites, the section **Before you begin** is included at the top of the workflow and describes the prerequisites.

Authorization request header

To get a bearer token for this header, perform the appropriate workflow at [Create user token](#) and extract the `access_token` value.

x-agent-id request header

This header contains the agent ID which is based on the client ID. See [Get client and account identifiers](#) for information about creating this value.

Presentation of common tokens and identifiers

Most of the variable tokens, identifiers, and other variables used in the sample REST API calls consist of long strings of letters, numbers, and special characters. They are considered *opaque* with no easily discernible content or meaning. Therefore, rather than including the actual original strings, smaller reserved keywords are used instead. This has several benefits:

- The curl and JSON samples are simpler and easier to understand.
- Because all keywords use the same format (including capital letters), you can quickly identify the content to insert or extract.
- No value is lost because the original values cannot be copied and used with an actual deployment.

A list of the keywords used in the workflow curl examples is presented in the table below.

Keyword	Description
<ACCESS_TOKEN>	An access token is a temporary string which establishes identity and access based on the OAuth2 standard.
<ID_TOKEN>	The ID token contains additional identity information for the user based on OpenID Connect (OIDC).
<CLIENT_ID>	This value uniquely identifies the user within a specific authorization domain.
<AGENT_ID>	The agent identifier is based on the client ID and is used to identify the user agent.
<ACCOUNT_ID>	This value identifies your NetApp account.
<NSS_KEY_ID>	This value identifies an entitlement key and is used by NetApp support.
<WORKING_ENV_ID>	This value identifies a working environment for the ONTAP runtime and so is synonymous with a Cloud Volumes ONTAP instance.
<SVM_NAME>	The name used for an ONTAP storage virtual machine.
<VOLUME_NAME>	The name used for an ONTAP storage volume.
<AGGR_NAME>	The aggregate name for a disk operation.
<REQUEST_ID>	This value is returned to the caller in the HTTP response and uniquely identifies the request.
<PROVIDER>	Abbreviation for the cloud provider.

Keyword	Description
<CLOUD_ACC_ID>	Account ID for the cloud provider.
<REFRESH_TOKEN>	NetApp refresh token used for federated authentication.

JSON input for curl command

In many cases, a workflow step accepts JSON input in the request body of the REST API call. This input is indicated in the curl command through the `-d` option, with the corresponding sample included in the **JSON input example** section.

Working environment status requirements

Many of the workflows require the working environment to have a specific status (such as `ON` or `DEGRADED`) before the REST API call can be performed. Review the [API reference content](#) for details about the requirements for each API call.

Typical Cloud Manager deployment

A summary of the major steps needed to deploy and administer a Cloud Volumes ONTAP instance using the Cloud Manager REST API is presented below.

Plan the deployment including cloud provider, licensing model, and size.



Obtain the required Cloud Manager and cloud provider accounts.



Create a connector using the Cloud Manager web user interface.



Get the required identifiers and prepare the common request headers.



Create a working environment using the appropriate REST API workflow.



Administer the storage for the CVO instance using the REST API workflows.

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.