Work with the management node REST API

HCI

NetApp

April 15, 2021

Table of Contents

Work with the management node REST API

Management node REST API UI overview

By using the built-in REST API UI (`https://<managementNodeIP>/mnode`), you can run or understand APIs relating to the management node services, including proxy server configuration, service level updates, or asset management.

Tasks you can perform with REST APIs:

Authorization

- Get authorization to use REST APIs

Asset configuration

- Enable Active IQ and NetApp HCI monitoring
- Configure a proxy server for the management node
- Configure NetApp Hybrid Cloud Control for multiple vCenters
- Add compute and controller assets to the management node
- Create and manage storage cluster assets

Asset management

- View or edit existing controller assets
- Create and manage storage cluster assets
- Remove an asset from the management node
- Use the REST API to collect NetApp HCI logs
- Verify management node OS and services versions
- Getting logs from management services

Find more information

- Access the management node
- NetApp Element Plug-in for vCenter Server
- NetApp HCI Resources Page

Get authorization to use REST APIs

You must authorize before you can use APIs for management services in the REST API UI. You do this by obtaining an access token.

To obtain a token, you provide cluster admin credentials and a client ID. Each token lasts approximately ten minutes. After a token expires, you can authorize again for a new access token.

Authorization functionality is set up for you during management node installation and deployment. The token service is based on the storage cluster you defined during setup.

Before you begin

- Your cluster version should be running NetApp Element software 11.3 or later.
- You should have deployed a management node running version 11.3 or later.

Steps

1. Access the REST API UI for the service by entering the management node IP address followed by the service name, for example `/mnode/`:

```
https://<managementNodeIP>/mnode/
```

2. Click **Authorize**.

   Alternately, you can click on a lock icon next to any service API.

3. Complete the following:
   a. Enter the cluster user name and password.
   b. Enter the client ID as `mnode-client`.
   c. Do not enter a value for the client secret.
   d. Click **Authorize** to begin a session.
4. Close the **Available authorizations** dialog box.

   If you try to run a command after the token expires, a `401 Error: UNAUTHORIZED` message appears. If you see this, authorize again.

Find more information

- NetApp Element Plug-in for vCenter Server
- NetApp HCI Resources Page

Create and manage storage cluster assets

You can add new storage cluster assets to the management node, edit the stored credentials for known storage cluster assets, and delete storage cluster assets from the management node using the REST API.

What you'll need

- Ensure that your storage cluster version is running NetApp Element software 11.3 or later.
- Ensure that you have deployed a management node running version 11.3 or later.

Storage cluster asset management options

Choose one of the following options:

- Retrieve the installation ID and cluster ID of a storage cluster asset

- Add a new storage cluster asset
- Edit the stored credentials for a storage cluster asset
- Delete a storage cluster asset

Retrieve the installation ID and cluster ID of a storage cluster asset

You can use the REST API get the installation ID and the ID of the storage cluster. You need the installation ID to add a new storage cluster asset, and the cluster ID to modify or delete a specific storage cluster asset.

Steps

1. Access the REST API UI for the inventory service by entering the management node IP address followed by `/inventory/1/`:

   ```
   https://[management node IP]/inventory/1/
   ```

2. Click **Authorize** or any lock icon and complete the following:
   a. Enter the cluster user name and password.
   b. Enter the client ID as `mnode-client`.
   c. Click **Authorize** to begin a session.
   d. Close the window.
3. Click **GET /installations**.
4. Click **Try it out**.
5. Click **Execute**.

   The API returns a list of all known installations.

6. From the code 200 response body, save the value in the `id` field, which you can find in the list of installations. This is the installation ID. For example:

   ```
   "installations": [
       {
         "id": "1234a678-12ab-35dc-7b4a-1234a5b6a7ba",
         "name": "my-hci-installation",
         "_links": {
           "collection": "https://localhost/inventory/1/installations",
           "self": "https://localhost/inventory/1/installations/1234a678-
   12ab-35dc-7b4a-1234a5b6a7ba"
         }
       }
     ]
   ```

7. Access the REST API UI for the storage service by entering the management node IP address followed by `/storage/1/`:

```
https://[management node IP]/storage/1/
```

8. Click **Authorize** or any lock icon and complete the following:
   a. Enter the cluster user name and password.
   b. Enter the client ID as `mnode-client`.
   c. Click **Authorize** to begin a session.
   d. Close the window.
9. Click **GET /clusters**.
10. Click **Try it out**.
11. Enter the installation ID you saved earlier into the `installationId` parameter.
12. Click **Execute**.

    The API returns a list of all known storage clusters in this installation.

13. From the code 200 response body, find the correct storage cluster and save the value in the cluster's `storageId` field. This is the storage cluster ID.

Add a new storage cluster asset

You can use the REST API to add one or more new storage cluster assets to the management node inventory. When you add a new storage cluster asset, it is automatically registered with the management node.

What you'll need

- You have copied the storage cluster ID and installation ID for any storage clusters you want to add.
- If you are adding more than one storage node, you have read and understood the limitations of the authoritative cluster and multiple storage cluster support.

> All users defined on the authoritative cluster are defined as users on all other clusters tied to the Hybrid Cloud Control instance.

Steps

1. Access the REST API UI for the storage service by entering the management node IP address followed by `/storage/1/`:

```
https://[management node IP]/storage/1/
```

2. Click **Authorize** or any lock icon and complete the following:
   a. Enter the cluster user name and password.
   b. Enter the client ID as `mnode-client`.
   c. Click **Authorize** to begin a session.
   d. Close the window.
3. Click **POST /clusters**.

4. Click **Try it out**.
5. Enter the new storage cluster's information in the following parameters in the **Request body** field:

```
{
  "installationId": "a1b2c34d-e56f-1a2b-c123-1ab2cd345d6e",
  "mvip": "10.0.0.1",
  "password": "admin",
  "userId": "admin"
}
```

Parameter	Type	Description
`installationId`	string	The installation in which to add the new storage cluster. Enter the installation ID you saved earlier into this parameter.
`mvip`	string	The IPv4 management virtual IP address (MVIP) of the storage cluster.
`password`	string	The password used to communicate with the storage cluster.
`userId`	string	The user ID used to communicate with the storage cluster (the user must have administrator privileges).

6. Click **Execute**.

   The API returns an object containing information about the newly added storage cluster asset, such as the name, version, and IP address information.

Edit the stored credentials for a storage cluster asset

You can edit the stored credentials that the management node uses to log in to a storage cluster. The user you choose must have cluster admin access.

Ensure you have followed the steps in Retrieve the installation ID and cluster ID of a storage cluster asset before continuing.

Steps

1. Access the REST API UI for the storage service by entering the management node IP address followed by `/storage/1/`:

```
https://[management node IP]/storage/1/
```

2. Click **Authorize** or any lock icon and complete the following:
   a. Enter the cluster user name and password.
   b. Enter the client ID as `mnode-client`.
   c. Click **Authorize** to begin a session.
   d. Close the window.
3. Click **PUT /clusters/{storageId}**.
4. Click **Try it out**.
5. Paste the storage cluster ID you copied earlier into the `storageId` parameter.
6. Change one or both of the following parameters in the **Request body** field:

```
{
  "password": "adminadmin",
  "userId": "admin"
}
```

Parameter	Type	Description
`password`	string	The password used to communicate with the storage cluster.
`userId`	string	The user ID used to communicate with the storage cluster (the user must have administrator privileges).

7. Click **Execute**.

Delete a storage cluster asset

You can delete a storage cluster asset if the storage cluster is no longer in service. When you remove a storage cluster asset, it is automatically unregistered from the management node.

Ensure you have followed the steps in Retrieve the installation ID and cluster ID of a storage cluster asset before continuing.

Steps

1. Access the REST API UI for the storage service by entering the management node IP address followed by `/storage/1/`:

```
https://[management node IP]/storage/1/
```

2. Click **Authorize** or any lock icon and complete the following:
   a. Enter the cluster user name and password.

   b. Enter the client ID as `mnode-client`.
   c. Click **Authorize** to begin a session.
   d. Close the window.
3. Click **DELETE /clusters/{storageId}**.
4. Click **Try it out**.
5. Enter the storage cluster ID you copied earlier in the `storageId` parameter.
6. Click **Execute**.

   Upon success, the API returns an empty response.

Find more information

* Authoritative cluster
* NetApp Element Plug-in for vCenter Server
* NetApp HCI Resources Page

Configure a proxy server

If your cluster is behind a proxy server, you must configure the proxy settings so that you can reach a public network.

A proxy server is used for telemetry collectors and reverse tunnel connections. You can enable and configure a proxy server using the REST API UI if you did not already configure a proxy server during installation or upgrade. You can also modify existing proxy server settings or disable a proxy server.

The command to configure a proxy server updates and then returns the current proxy settings for the management node. The proxy settings are used by Active IQ, the NetApp HCI monitoring service that is deployed by the NetApp Deployment Engine, and other Element software utilities that are installed on the management node, including the reverse support tunnel for NetApp Support.

Before you begin

* You should know host and credential information for the proxy server you are configuring.
* Ensure that your cluster version is running NetApp Element software 11.3 or later.
* Ensure that you have deployed a management node running version 11.3 or later.
* (Management node 12.0 and later) You have updated NetApp Hybrid Cloud Control to management services version 2.16 before configuring a proxy server.

Steps

1. Access the REST API UI on the management node by entering the management node IP address followed by `/mnode`:

   ```
   https://[management node IP]/mnode
   ```

2. Click **Authorize** or any lock icon and complete the following:

a. Enter the cluster user name and password.
b. Enter the client ID as `mnode-client`.
c. Click **Authorize** to begin a session.
d. Close the window.

3. Click **PUT /settings**.
4. Click **Try it out**.
5. To enable a proxy server, you must set `use_proxy` to true. Enter the IP or host name and proxy port destinations.

   The proxy user name, proxy password, and SSH port are optional and should be omitted if not used.

```
{
"proxy_ip_or_hostname": "[IP or name]",
"use_proxy": [true/false],
"proxy_username": "[username]",
"proxy_password": "[password]",
"proxy_port": [port value],
"proxy_ssh_port": [port value: default is 443]
}
```

6. Click **Execute**.

Find more information

- NetApp Element Plug-in for vCenter Server
- NetApp HCI Resources Page

Verify management node OS and services versions

You can verify the version numbers of the management node OS, management services bundle, and individual services running on the management node using the REST API in the management node.

What you'll need

- Your cluster is running NetApp Element software 11.3 or later.
- You have deployed a management node running version 11.3 or later.

Options

- API commands
- REST API UI steps

API commands

- Get version information about the management node OS, the management services bundle, and the management node API (mnode-api) service that are running on the management node:

```
curl -X GET "https://<managementNodeIP>/mnode/about" -H  "accept:
application/json"
```

- Get version information about individual services running on the management node:

```
curl -X GET "https://<managementNodeIP>/mnode/services?status=running"
-H  "accept: */*" -H  "Authorization: Bearer <ID>"
```

> You can find the bearer ID used by the API by running a GET command and retrieving it from the curl response.

REST API UI steps

1. Access the REST API UI for the service by entering the management node IP address followed by `/mnode/`:

```
https://<managementNodeIP>/mnode/
```

2. Do one of the following:
   - Get version information about the management node OS, the management services bundle, and the management node API (mnode-api) service that are running on the management node:
     a. Select **GET /about**.
     b. Select **Try it out**.
     c. Select **Execute**.

        The management services bundle version (`"mnode_bundle_version"`), management node OS version (`"os_version"`), and management node API version (`"version"`) are indicated in the response body.
   - Get version information about individual services running on the management node:
     a. Select **GET /services**.
     b. Select **Try it out**.
     c. Select the status as **Running**.
     d. Select **Execute**.

        The services that are running on the management node are indicated in the response body.

Find more information

- NetApp Element Plug-in for vCenter Server
- NetApp HCI Resources Page

Getting logs from management services

You can retrieve logs from the services running on the management node using the REST API. You can pull logs from all public services or specify specific services and use query parameters to better define the return results.

What you'll need

- Your cluster version is running NetApp Element software 11.3 or later.
- You have deployed a management node running version 11.3 or later.

Steps

1. Open the REST API UI on the management node:

   ```
   https://[managementNodeIP]/mnode
   ```

2. Select **Authorize** or any lock icon and complete the following:
   a. Enter the cluster user name and password.
   b. Enter the client ID as mnode-client if the value is not already populated.
   c. Select **Authorize** to begin a session.
   d. Close the window.
3. Select **GET /logs**.
4. Select **Try it out**.
5. Specify the following parameters:
   - `Lines`: Enter the number of lines you want the log to return. This parameter is an integer that defaults to 1000.

     Avoid requesting the entire history of log content by setting Lines to 0.

   - `since`: Adds a ISO-8601 timestamp for the service logs starting point.

     Use a reasonable `since` parameter when gathering logs of wider timespans.

   - `service-name`: Enter a service name.

     Use the `GET /services` command to list services on the management node.

   - `stopped`: Set to `true` to retrieve logs from stopped services.
6. Select **Execute**.

Find more Information

- NetApp Element Plug-in for vCenter Server
- NetApp HCI Resources Page