Create and manage storage cluster assets

HCI

Michael Wallis, Dave Bagwell
December 14, 2020

This PDF was generated from https://docs.netapp.com/us-en/hci/docs/task_mnode_manage_storage_cluster_assets.html on December 14, 2020. Always check docs.netapp.com for the latest.

NetApp®

Table of Contents

Create and manage storage cluster assets 1
- Retrieve the installation ID and cluster ID of a storage cluster asset 1
- Add a new storage cluster asset 3
- Edit the stored credentials for a storage cluster asset 4
- Delete a storage cluster asset 5

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

Copyright Information

Copyright © 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.