



Update vCenter and ESXi credentials

HCI

Ann-Marie Grissino, Dave Bagwell
August 16, 2021

Table of Contents

- Update vCenter and ESXi credentials 1
 - Update vCenter password by using the management node REST API 1
 - Update the ESXi password by using the management node REST API 1

Update vCenter and ESXi credentials

To maintain full functionality of NetApp Hybrid Cloud Control for your NetApp HCI installation, when you change your credentials in vCenter and ESXi hosts, you also need to update those credentials in the asset service on the management node.

About this task

NetApp Hybrid Cloud Control communicates with vCenter and the individual compute nodes running VMware vSphere ESXi to retrieve information for the dashboard and to facilitate rolling upgrades of firmware, software and drivers. NetApp Hybrid Cloud Control and its related services on the management node use credentials (username/password) to authenticate against VMware vCenter and ESXi.

If communication between these components fails, NetApp Hybrid Cloud Control and vCenter display error messages when authentication problems occur. NetApp Hybrid Cloud Control will display a red error banner if it cannot communicate with the associated VMware vCenter instance in the NetApp HCI installation. VMware vCenter will display ESXi account lockout messages for individual ESXi hosts as a result of NetApp Hybrid Cloud Control using outdated credentials.

The management node in NetApp HCI refers to these components using the following names:

- "Controller assets" are vCenter instances associated with your NetApp HCI installation.
- "Compute node assets" are the ESXi hosts in your NetApp HCI installation.

During the initial installation of NetApp HCI using the NetApp Deployment Engine, the management node stored the credentials for the administrative user you specified for vCenter and the "root" account password on ESXi servers.

Update vCenter password by using the management node REST API

Follow the steps to update the controller assets. See [View or edit existing controller assets](#).

Update the ESXi password by using the management node REST API

Steps

1. To gain an overview of the Management node REST API user interface, see the [Management node REST API user interface overview](#).
2. Access the REST API UI for management services on the management node:

```
https://<management node IP>/mnode
```

Replace <management node IP> with the IPv4 address of your management node on the management network used for NetApp HCI.

3. Click **Authorize** or any lock icon and complete the following:
 - a. Enter the NetApp SolidFire cluster administrative user name and password.

- b. Enter the client ID as `mnode-client`.
 - c. Click **Authorize** to begin a session.
 - d. Close the window.
4. From the REST API UI, click **GET /assets/compute_nodes**.

This retrieves the records of compute node assets that are stored in the management node.

Here is the direct link to this API in the UI:

```
https://<management node  
IP>/mnode/#/assets/routes.v1.assets_api.get_compute_nodes
```

5. Click **Try it out**.
6. Click **Execute**.
7. From the response body, identify the compute node asset records that need updated credentials. You can use the “ip” and “host_name” properties to find the correct ESXi host records.

```
"config": { },  
"credentialid": <credential_id>,  
"hardware_tag": <tag>,  
"host_name": <host_name>,  
"id": <id>,  
"ip": <ip>,  
"parent": <parent>,  
"type": ESXi Host
```



The next step uses the “parent” and “id” fields in the compute asset record to reference the record to be updated.

8. Configure the specific compute node asset:
 - a. Click **PUT /assets/{asset_id}/compute-nodes/{compute_id}**.

Here is the direct link to the API in the UI:

```
https://<management node  
IP>/mnode/#/assets/routes.v1.assets_api.put_assets_compute_id
```

- b. Click **Try it out**.
- c. Enter the “asset_id” with the “parent” information.
- d. Enter the “compute_id” with the “id” information.
- e. Modify the request body in the user interface to update only the password and user name parameters in the compute asset record:

```
{
  "password": "<password>",
  "username": "<username>"
}
```

- f. Click **Execute**.
- g. Validate that the response is HTTP 200, which indicates that the new credentials have been stored in the referenced compute asset record
9. Repeat the previous two steps for additional compute node assets that need to be updated with a new password.
10. Navigate to https://<mNode_ip>/inventory/1/.
 - a. Click **Authorize** or any lock icon and complete the following:
 - i. Enter the NetApp SolidFire cluster administrative user name and password.
 - ii. Enter the client ID as `mnode-client`.
 - iii. Click **Authorize** to begin a session.
 - iv. Close the window.
 - b. From the REST API UI, click **GET /installations**.
 - c. Click **Try it out**.
 - d. Select **True** from the refresh description drop-down list.
 - e. Click **Execute**.
 - f. Validate that the response is HTTP 200.
11. Wait for about 15 minutes for the account lockout message in vCenter to disappear.

Find more information

- [NetApp Element Plug-in for vCenter Server](#)
- [NetApp HCI Resources Page](#)

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.