Manage SSH functionality on the management node

HCI

Dave Bagwell, Ann-Marie Grissino
February 18, 2021

This PDF was generated from https://docs.netapp.com/us-en/hci/docs/task_mnode_ssh_management.html on February 24, 2021. Always check docs.netapp.com for the latest.

Table of Contents

Manage SSH functionality on the management node 1
Disable or enable the SSH capability on the management node 1
Determine status of the SSH capability on the management node 2

Manage SSH functionality on the management node

You can disable, re-enable, or determine the status of the SSH capability on the management node (mNode) using the REST API. SSH capability that provides NetApp Support remote support tunnel (RST) session access is enabled on the management node by default.

What you'll need

- **Cluster administrator permissions**: You have permissions as administrator on the storage cluster.
- **Element software**: Your cluster is running NetApp Element software 11.3 or later.
- **Management node**: You have deployed a management node running version 11.3 or later.
- **Management services updates**: You have updated your management services bundle to version 2.17.

Options

You can do any of the following tasks after you authenticate:

- Disable or enable the SSH capability on the management node
- Determine status of the SSH capability on the management node

Disable or enable the SSH capability on the management node

You can disable or re-enable SSH capability on the management node. SSH capability that provides NetApp Support remote support tunnel (RST) session access is enabled on the management node by default. Disabling SSH does not terminate or disconnect existing SSH client sessions to the management node. If you disable SSH and elect to re-enable it at a later time, you can do so using the same API.

API command

```
curl -X PUT
"https://<managementNodeIP>/mnode/settings/ssh?enabled=<false/true>" -H
"accept: application/json" -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 management node API service by entering the management node IP address followed by `/mnode/`:

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

2. Select **Authorize** and complete the following:

a. Enter the cluster user name and password.

b. Enter the client ID as `mnode-client`.

c. Select **Authorize** to begin a session.

d. Close the window.

3. From the REST API UI, select **PUT /settings/ssh**.

a. Click **Try it out**.

b. Set the **enabled** parameter to `false` to disable SSH or `true` to re-enable SSH capability that you previously disabled.

c. Click **Execute**.

Determine status of the SSH capability on the management node

You can determine whether or not SSH capability is enabled on the management node using a management node service API. SSH is enabled by default on the management node.

API command

```
curl -X GET "https://<managementNodeIP>/mnode/settings/ssh" -H  "accept:
application/json" -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 management node API service by entering the management node IP address followed by `/mnode/`:

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

2. Select **Authorize** and complete the following:

a. Enter the cluster user name and password.

b. Enter the client ID as `mnode-client`.

c. Select **Authorize** to begin a session.

d. Close the window.

3. From the REST API UI, select **GET /settings/ssh**.

a. Click **Try it out**.

b. Click **Execute**.

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.