

Run compute node health checks prior to upgrading compute firmware

HCI

dbag-personal, Dave Bagwell, amitha, Michael Wallis
August 25, 2020

This PDF was generated from https://docs.netapp.com/us-en/hci/docs/task_upgrade_compute_prechecks.html on October 18, 2020. Always check docs.netapp.com for the latest.

Table of Contents

- Run compute node health checks prior to upgrading compute firmware 1
 - Use NetApp Hybrid Cloud Control to run compute node health checks prior to upgrading firmware..... 1
 - Use API to run compute node health checks prior to upgrading firmware..... 2
 - Compute node health checks made by the service..... 5

Run compute node health checks prior to upgrading compute firmware

You must run health checks prior to upgrading compute firmware to ensure all compute nodes in your cluster are ready to be upgraded. Compute node health checks can only be run against compute clusters of one or more managed NetApp HCI compute nodes.

What you'll need

- You have updated to the latest management services bundle (2.11 or later).
- You are running management node 11.3 or later.
- Your storage cluster is running NetApp Element software 11.3 or later.

Health check options

You can run health checks using NetApp Hybrid Cloud Control (HCC) UI or HCC API:

- [Use NetApp Hybrid Cloud Control to run compute node health checks prior to upgrading firmware](#) (Preferred method)
- [Use API to run compute node health checks prior to upgrading firmware](#)

You can also find out more about compute node health checks that are run by the service:

- [Compute node health checks made by the service](#)

Use NetApp Hybrid Cloud Control to run compute node health checks prior to upgrading firmware


Using NetApp Hybrid Cloud Control (HCC), you can verify that a compute node is ready for a firmware upgrade.

Steps

1. Open a web browser and browse to the IP address of the management node:

```
https://<ManagementNodeIP>/hcc
```

2. Log in to NetApp Hybrid Cloud Control by providing the storage cluster administrator credentials.
3. Click **Upgrade** near the top right of the interface.
4. On the **Upgrades** page, select the **Compute firmware** tab.
- 5.

Click the health check  for the cluster you want to check for upgrade readiness.

6. On the **Compute Health Check** page, click **Run Health Check**.
7. If there are issues, the page provides a report. Do the following:
 - a. Go to the specific KB article listed for each issue or perform the specified remedy.
 - b. If a KB is specified, complete the process described in the relevant KB article.
 - c. After you have resolved cluster issues, click **Re-Run Health Check**.

After the health check completes without errors, the compute nodes in the cluster are ready to upgrade. See [Update compute node firmware](#) to proceed.

Use API to run compute node health checks prior to upgrading firmware

You can use REST API to verify that compute nodes in a cluster are ready to be upgraded. The health check verifies that there are no obstacles to upgrading, such as ESXi host issues or other vSphere issues. You will need to run compute node health checks for each compute cluster in your environment.

Steps

1. Locate the controller ID and cluster ID:
 - a. Open the inventory service REST API UI on the management node:

```
https://[management node IP]/inventory/1/
```
 - b. Click **Authorize** and complete the following:
 - i. Enter the cluster user name and password.
 - ii. Enter the client ID as `mnode-client` if the value is not already populated.
 - iii. Click **Authorize** to begin a session.
 - c. From the REST API UI, click **GET /installations**.
 - d. Click **Try it out**.
 - e. Click **Execute**.
 - f. From the code 200 response body, copy the `"id"` for the installation you plan to use for health checks.
 - g. From the REST API UI, click **GET /installations/{id}**.
 - h. Click **Try it out**.
 - i. Enter the installation ID.

- j. Click **Execute**.
- k. From the code 200 response body, copy the IDs for each of the following:
 - i. The cluster ID ("**clusterId**")
 - ii. A controller ID ("**controllerId**")

```
{
  "_links": {
    "collection": "https://10.117.187.199/inventory/1/installations",
    "self": "https://10.117.187.199/inventory/1/installations/xx94f6f0-12a6-412f-8b5e-4cf2z58329x0"
  },
  "compute": {
    "errors": [],
    "inventory": {
      "clusters": [
        {
          "clusterId": "domain-1",
          "controllerId": "abc12c3a-aa87-4e33-9f94-xx588c2cdcf6",
          "datacenterName": "NetApp-HCI-Datacenter-01",
          "installationId": "xx94f6f0-12a6-412f-8b5e-4cf2z58329x0",
          "installationName": "test-nde-mnode",
          "inventoryType": "managed",
          "name": "NetApp-HCI-Cluster-01",
          "summary": {
            "nodeCount": 2,
            "virtualMachineCount": 2
          }
        }
      ]
    }
  },
}
```

- 2. Run health checks on the compute nodes in the cluster:
 - a. Open the compute service REST API UI on the management node:

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

- b. Click **Authorize** and complete the following:
 - i. Enter the cluster user name and password.
 - ii. Enter the client ID as **mnode-client** if the value is not already populated.
 - iii. Click **Authorize** to begin a session.
 - c. Click **POST /compute/{CONTROLLER_ID}/health-checks**.
 - d. Click **Try it out**.

- e. Enter the **"controllerId"** you copied from the previous step in the **Controller_ID** parameter field.
- f. In the payload, enter the **"clusterId"** that you copied from the previous step as the **"cluster"** value and remove the **"nodes"** parameter.

```
{
  "cluster": "domain-1"
}
```

- g. Click **Execute** to run a health check on the cluster.

The code 200 response gives a **"resourceLink"** URL with the task ID appended that is needed to confirm the health check results.

```
{
  "resourceLink": "https://10.117.150.84/vcenter/1/compute/tasks/[This is the task ID for health check task results]",
  "serviceName": "vcenter-v2-svc",
  "taskId": "ab12c345-06f7-42d7-b87c-7x64x56x321x",
  "taskName": "VCenter service health checks"
}
```

- h. Copy the task ID portion of the **"resourceLink"** URL to verify the task result.
3. Verify the result of the health checks:
- a. Return to the compute service REST API UI on the management node:

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

- b. Click **GET /compute/tasks/{task_id}**.
- c. Click **Try it out**.
- d. Enter the task ID portion of the **"resourceLink"** URL from the **POST /compute/{CONTROLLER_ID}/health-checks** code 200 response in the **task_id** parameter field.
- e. Click **Execute**.
- f. If the **status** returned indicates that there were problems regarding compute node health, do the following:
 - i. Go to the specific KB article (**KBLink**) listed for each issue or perform the specified remedy.
 - ii. If a KB is specified, complete the process described in the relevant KB article.
 - iii. After you have resolved cluster issues, run **POST /compute/{CONTROLLER_ID}/health-checks** again (see step 2).

If health checks complete without issues, the response code 200 indicates a successful result.

Compute node health checks made by the service

Compute health checks, whether performed by HCC or API methods, make the following checks per node. Depending on your environment, some of these checks might be skipped. You should re-run health checks after resolving any detected issues.

Check description	Node/cluster	Action needed to resolve	Knowledgebase article with procedure
Is DRS enabled and fully automated?	Cluster	Turn on DRS and make sure it is fully automated.	See this KB . NOTE: If you have standard licensing, put the ESXi host into maintenance mode and ignore this health check failure warning.
Is DPM disabled in vSphere?	Cluster	Turn off Distributed Power Management.	See this KB .
Is HA admission control disabled in vSphere?	Cluster	Turn off HA admission control.	See this KB .
Is FT enabled for a VM on a host in the cluster?	Node	Suspend Fault Tolerance on any affected virtual machines.	See this KB .
Are there critical alarms in vCenter for the cluster?	Cluster	Launch vSphere and resolve and/or acknowledge any alerts before proceeding.	No KB needed to resolve issue.
Are there generic/global informational alerts in vCenter?	Cluster	Launch vSphere and resolve and/or acknowledge any alerts before proceeding.	No KB needed to resolve issue.
Are management services up to date?	HCI system	You must update management services before you perform an upgrade or run pre-upgrade health checks.	No KB needed to resolve issue. See this article for more information.
Are there errors on the current ESXi node in vSphere?	Node	Launch vSphere and resolve and/or acknowledge any alerts before proceeding.	No KB needed to resolve issue.

Check description	Node/cluster	Action needed to resolve	Knowledgebase article with procedure
Is virtual media mounted to a VM on a host in the cluster?	Node	Unmount all virtual media disks (CD/DVD/floppy) from the VMs.	No KB needed to resolve issue.
Is BMC version the minimum required version that has RedFish support?	Node	Manually update your BMC firmware.	No KB needed to resolve issue.
Is ESXi host up and running?	Node	Start your ESXi host.	No KB needed to resolve issue.
Do any virtual machines reside on local ESXi storage?	Node/VM	Remove or migrate local storage attached to virtual machines.	No KB needed to resolve issue.
Is BMC up and running?	Node	Power on your BMC and ensure it is connected to a network this management node can reach.	No KB needed to resolve issue.
Are there partner ESXi host(s) available?	Node	Make one or more ESXi host(s) in cluster available (not in maintenance mode) to migrate virtual machines.	No KB needed to resolve issue.
Are you able to connect with BMC via IPMI protocol?	Node	Enable IPMI protocol on Baseboard Management Controller (BMC).	No KB needed to resolve issue.
Is ESXi host mapped to hardware host (BMC) correctly?	Node	The ESXi host is not mapped to the Baseboard Management Controller (BMC) correctly. Correct the mapping between ESXi host and hardware host.	No KB needed to resolve issue. See this article for more information.

Check description	Node/cluster	Action needed to resolve	Knowledgebase article with procedure
What is the status of the Witness Nodes in the cluster? None of the witness nodes identified are up and running.	Node	A Witness Node is not running on an alternate ESXi host. Power on the Witness Node on an alternate ESXi host and re-run the health check. One Witness Node must be running in the HCI installation at all times.	See this KB
What is the status of the Witness Nodes in the cluster? The witness node is up and running on this ESXi host and the alternate witness node is not up and running.	Node	A Witness Node is not running on an alternate ESXi host. Power on the Witness Node on an alternate ESXi host. When you are ready to upgrade this ESXi host, shut down the witness node running on this ESXi host and re-run the health check. One Witness Node must be running in the HCI installation at all times.	See this KB
What is the status of the Witness Nodes in the cluster? Witness node is up and running on this ESXi host and the alternate node is up but is running on the same ESXi host.	Node	Both Witness Nodes are running on this ESXi host. Relocate one Witness Node to an alternate ESXi host. When you are ready to upgrade this ESXi host, shut down the Witness Node remaining on this ESXi host and re-run the health check. One Witness Node must be running in the HCI installation at all times.	See this KB

Check description	Node/cluster	Action needed to resolve	Knowledgebase article with procedure
What is the status of the Witness Nodes in the cluster? Witness node is up and running on this ESXi host and the alternate witness node is up and running on another ESXi host.	Node	A Witness Node is running locally on this ESXi host. When you are ready to upgrade this ESXi host, shut down the Witness Node only on this ESXi host and re-run the health check. One Witness Node must be running in the HCI installation at all times.	See this KB

Find more information

- [NetApp HCI Documentation Center](#)
- [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.