Monitor your NetApp HCI system with NetApp Hybrid Cloud Control

HCI

NetApp
April 21, 2022

This PDF was generated from https://docs.netapp.com/us-en/hci/docs/task_hcc_dashboard.html on April 21, 2022. Always check docs.netapp.com for the latest.

Table of Contents

Monitor your NetApp HCI system with NetApp Hybrid Cloud Control . . . 1
Monitor storage and compute resources on the Hybrid Cloud Control Dashboard . . . 1
View your inventory on the Nodes page . . . 7
Edit Baseboard Management Controller connection information . . . 9
Monitor volumes on your storage cluster . . . 12
Monitor performance, capacity, and cluster health with SolidFire Active IQ . . . 14
Collect logs for troubleshooting . . . 15

Monitor your NetApp HCI system with NetApp Hybrid Cloud Control

Monitor storage and compute resources on the Hybrid Cloud Control Dashboard

With the NetApp Hybrid Cloud Control Dashboard, you can view all your storage and compute resources at a glance. Additionally, you can monitor storage capacity, storage performance, and compute utilization.

> When you launch a new NetApp Hybrid Cloud Control session for the first time, there might be a delay with loading the NetApp Hybrid Cloud Control Dashboard view when the management node is managing many clusters. The loading time varies depending on the number of clusters being actively managed by the management node. For subsequent launches, you will experience faster loading times.

Only compute nodes that are managed and clusters with at least one managed node in H-series hardware appear on the Hybrid Cloud Control Dashboard.

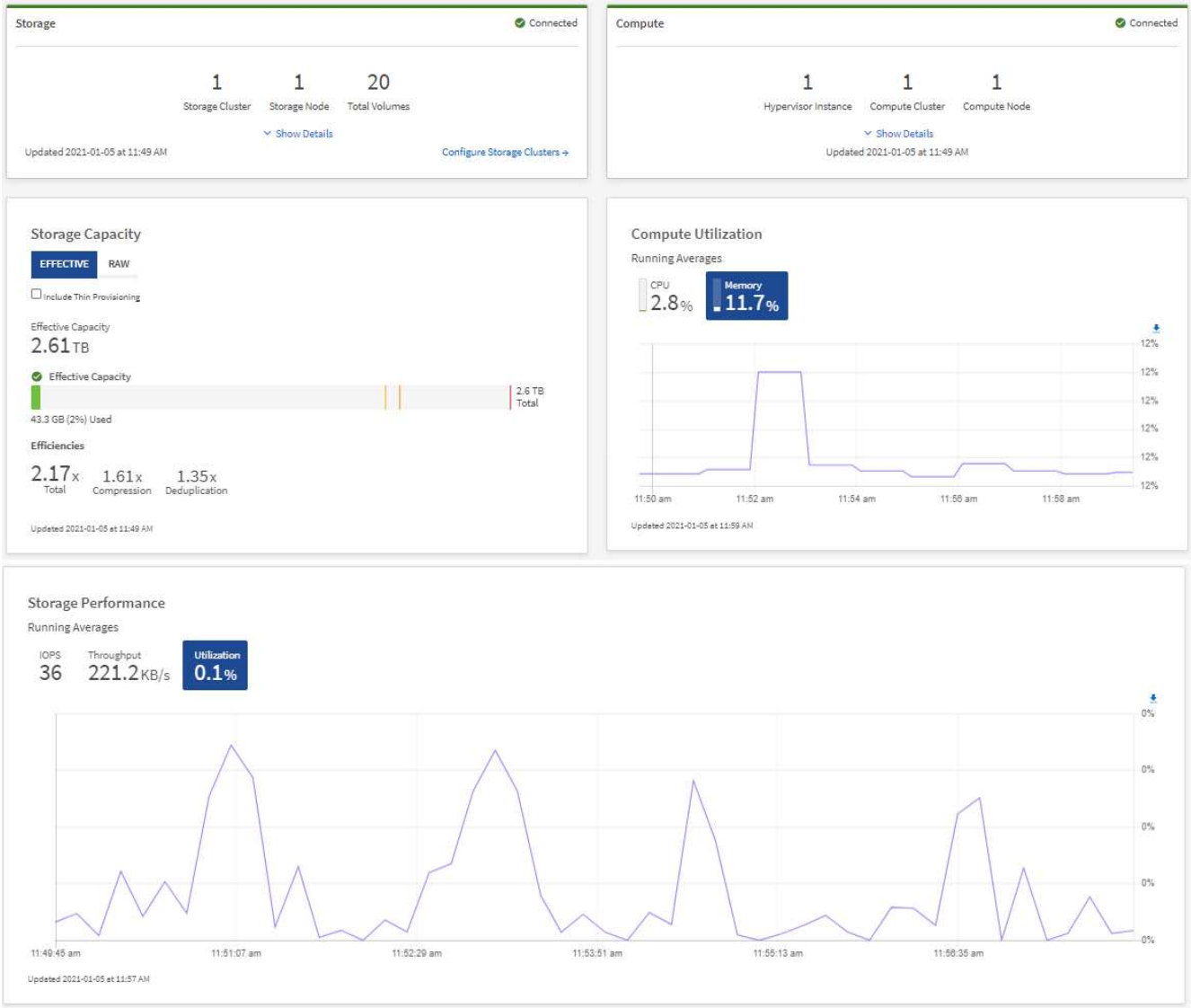
- Access the NetApp HCC Dashboard
- Monitor storage resources
- Monitor compute resources
- Monitor storage capacity
- Monitor storage performance
- Monitor compute utilization

Access the NetApp HCC Dashboard

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

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

2. Log in to NetApp Hybrid Cloud Control by providing the NetApp HCI storage cluster administrator credentials.
3. View the Hybrid Cloud Control Dashboard.

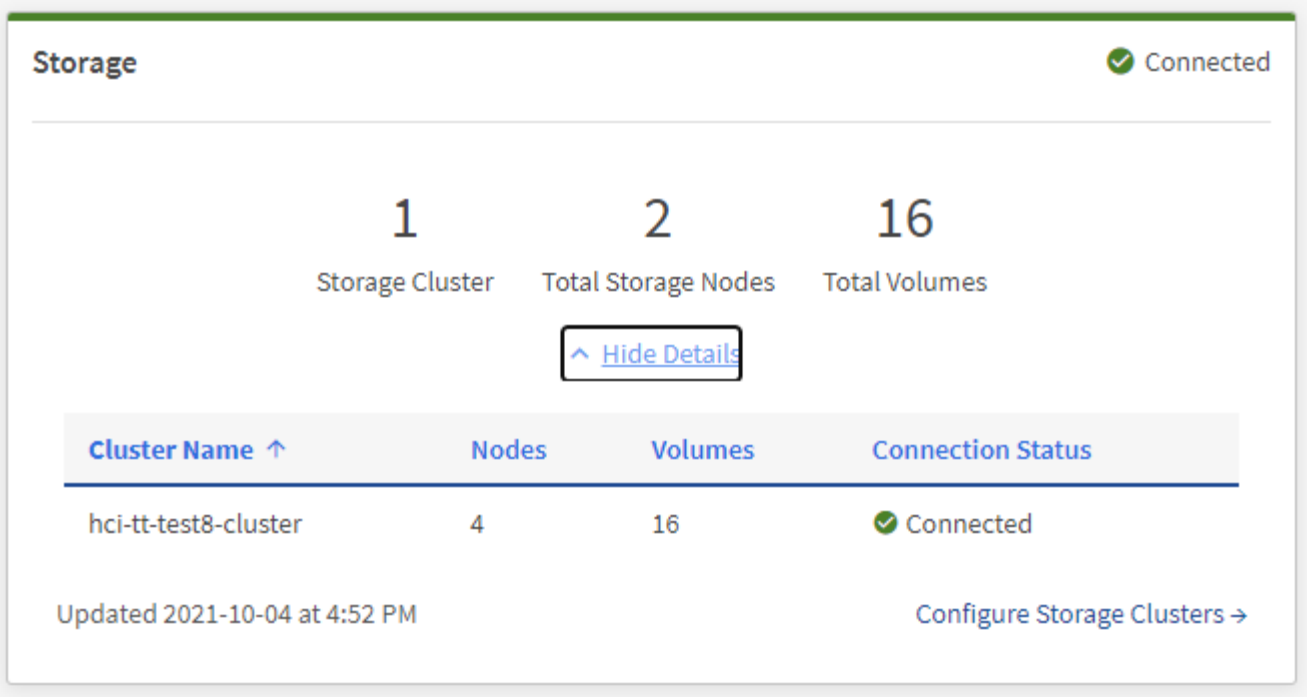


You might see some or all these panes, depending on your installation. For example, for storage-only installations, the Hybrid Cloud Control Dashboard shows only the Storage pane, the Storage Capacity pane, and the Storage Performance pane.

Monitor storage resources

Use the **Storage** pane to see your total storage environment. You can monitor the number of storage clusters, storage nodes, and total volumes.

To see details, in the Storage pane, select **Show Details**.



The Total Storage Nodes number does not include Witness Nodes from two-node storage clusters. The Witness Nodes are included in the Nodes number in the details section for that cluster.

To see the most recent storage cluster data, use the Storage Clusters page, where polling occurs more frequently than on the Dashboard.

Monitor compute resources

Use the **Compute** pane to see your total NetApp H-series compute environment. You can monitor the number of compute clusters and total compute nodes.

To see details, in the Compute panes, select **Show Details**.

Your vCenter instances only show in the Compute pane when at least one NetApp HCI compute node is associated with that instance. To list the vCenter instances linked in NetApp Hybrid Cloud Control, you can use the APIs.

To manage a compute node in NetApp Hybrid Cloud Control, you must add the compute node to a vCenter host cluster.

Monitor storage capacity

Monitoring the storage capacity of your environment is critical. Using the Storage Capacity pane, you can determine your storage capacity efficiency gains with or without compression, deduplication, and thin provisioning features enabled.

You can see the total physical storage space available in your cluster on the **RAW** tab, and information about the provisioned storage on the **EFFECTIVE** tab.

To view cluster health, also look at the SolidFire Active IQ Dashboard. See Monitor performance, capacity, and cluster health in NetApp SolidFire Active IQ.

Steps

1. Select the **RAW** tab, to see the total physical storage space used and available in your cluster.

   Look at the vertical lines to determine whether your used capacity is less than the total or less than Warning, Error, or Critical thresholds. Hover over the lines to see details.

   You can set the threshold for Warning, which defaults to 3% below the Error threshold. The Error and Critical thresholds are preset and not configurable by design. The Error threshold indicates that less than one node of capacity remains in the cluster. For steps on setting the threshold, see Setting cluster full threshold.

   For details about the related cluster thresholds Element API, see "getClusterFullThreshold" in the *Element software API documentation*. To view details about block and metadata capacity, see Understanding cluster fullness levels in the *Element software documentation*.

2. Select the **EFFECTIVE** tab, to see information about total storage provisioned to connected hosts and to see efficiency ratings.
   a. Optionally, check **Include Thin Provisioning** to see thin provisioning efficiency rates in the Effective Capacity bar chart.
   b. **Effective Capacity bar chart**: Look at the vertical lines to determine whether your used capacity is less than the total or less than Warning, Error, or Critical thresholds. Similar to the Raw tab, you can hover over the vertical lines to see details.
   c. **Efficiencies**: Look at these ratings to determine your storage capacity efficiency gains with compression, deduplication, and thin provisioning features enabled. For example, if compression shows as "1.3x", this means that storage efficiency with compression enabled is 1.3 times more efficient than without it.

      Total Efficiencies equals (maxUsedSpace * efficiency factor) / 2, where efficiencyFactor = (thinProvisioningFactor * deDuplicationFactor * compressionFactor). When Thin Provisioning is unchecked, it is not included in the Total Efficiency.

d. If the effective storage capacity nears an Error or Critical threshold, consider clearing the data on your system. Alternatively, consider expanding your system.

   See Expansion overview.

3. For further analysis and historical context, look at NetApp SolidFire Active IQ details.

Monitor storage performance

You can look at how much IOPS or throughput you can get out of a cluster without surpassing the useful performance of that resource by using the Storage Performance pane. Storage performance is the point at which you get the maximum utilization before latency becomes an issue.

The Storage Performance pane helps you identify whether the performance is reaching the point where the performance might degrade if the workloads increase.

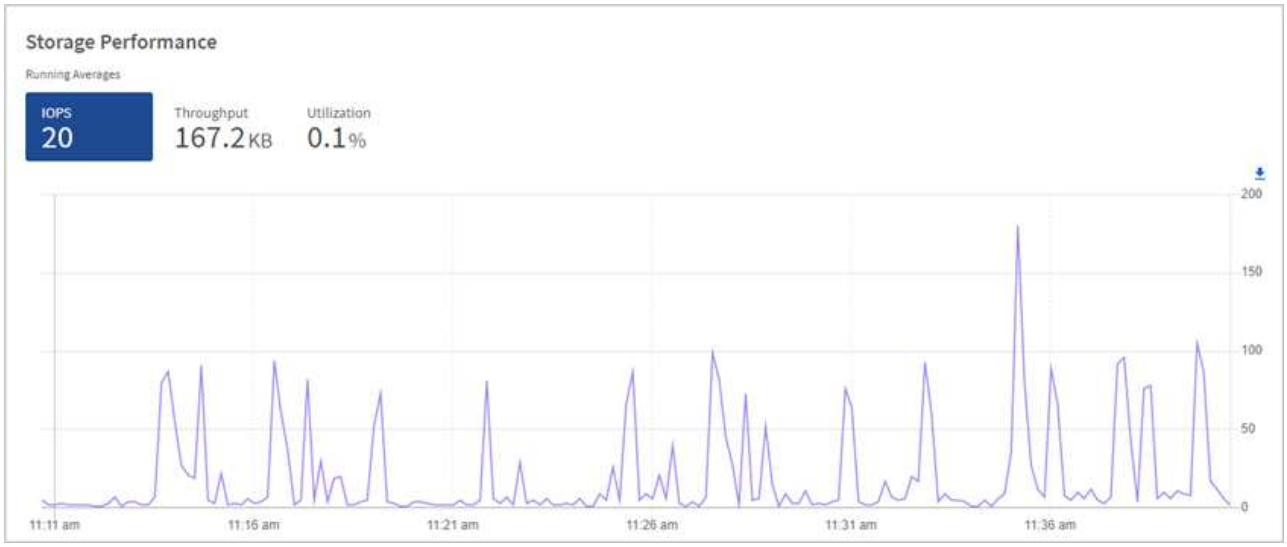
The information on this pane refreshes every 10 seconds and shows an average of all the points on the graph.

For details about the associated Element API method, see the GetClusterStats method in the *Element software API documentation*.

Steps

1. View the Storage Performance pane. For details, hover over points in the graph.

   a. **IOPS** tab: See the current operations per second. Look for trends in data or spikes. For example, if you see that the maximum IOPS is 160K and 100K of that is free or available IOPS, you might consider adding more workloads to this cluster. On the other hand, if you see that only 140K is available, you might consider offloading workloads or expanding your system.



   b. **Throughput** tab: Monitor patterns or spikes in throughput. Also monitor for continuously high throughput values, which might indicate that you are nearing the maximum useful performance of the resource.

c. **Utilization** tab: Monitor the utilization of IOPS in relation to the total IOPS available summed up at the cluster level.

2. For further analysis, look at storage performance by using the NetApp Element Plug-in for vCenter Server.

   Performance shown in the NetApp Element Plug-in for vCenter Server.

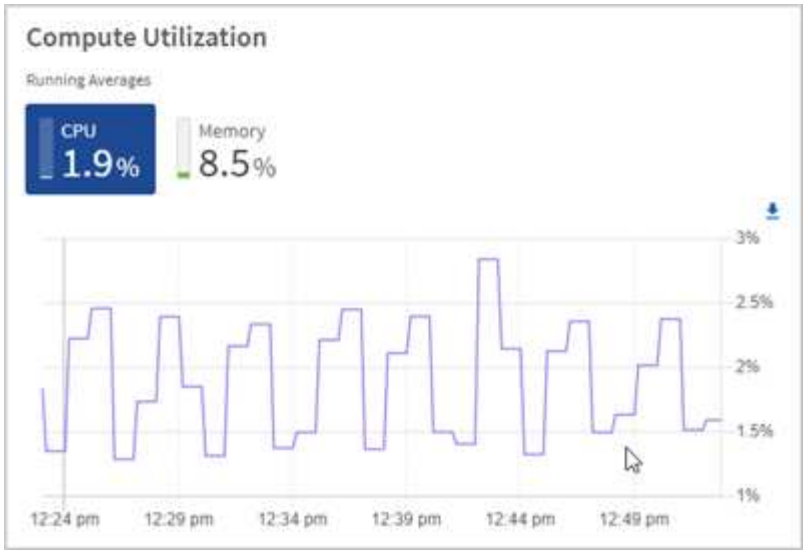
Monitor compute utilization

In addition to monitoring IOPS and throughput of your storage resources, you also might want to view the CPU and memory usage of your compute assets. The total IOPS that a node can provide is based on the physical characteristics of the node, for example, the number of CPUs, the CPU speed, and the amount of RAM.

Steps

1. View the **Compute Utilization** pane. Using both the CPU and Memory tabs, look for patterns or spikes in utilization. Also look for continuously high usage, indicating that you might be nearing the maximum utilization for the compute clusters.

   This pane shows data only for those compute clusters managed by this installation.



a. **CPU** tab: See the current average of CPU utilization on the compute cluster.
b. **Memory** tab: See the current average memory usage on the compute cluster.

2. For further analysis on compute information, see NetApp SolidFire Active IQ for historical data.

Find more information

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

View your inventory on the Nodes page

You can view both your storage and compute assets in your system and determine their IP addresses, names, and software versions.

You can view storage information for your multiple node systems and any NetApp HCI Witness Nodes associated with two-node or three-node clusters. If custom protection domains are assigned, you can see which protection domains are assigned to specific nodes.

Witness Nodes manage quorum within the cluster; they are not used for storage. Witness Nodes are applicable only to NetApp HCI and not to all-flash storage environments.

For more information about Witness Nodes, see Nodes definitions.

For SolidFire Enterprise SDS nodes, you can monitor inventory on the Storage tab.

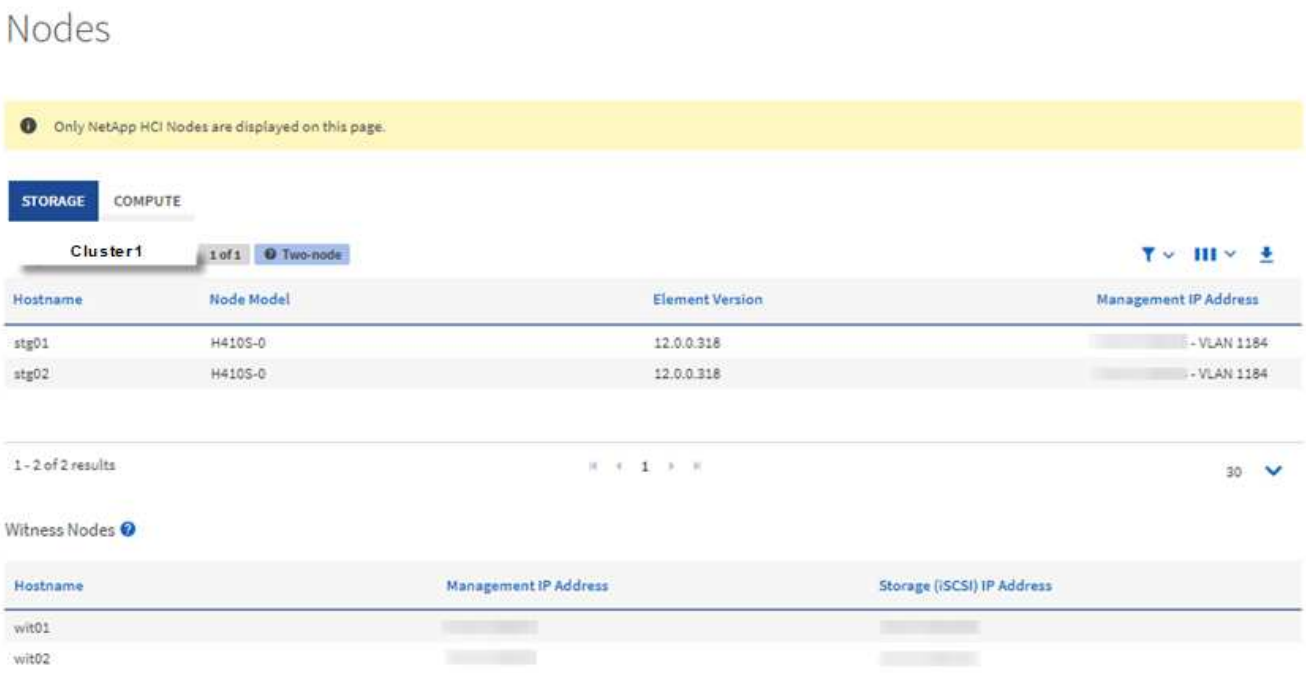
Steps

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

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

2. Log in to NetApp Hybrid Cloud Control by providing the NetApp HCI storage cluster administrator credentials.

3. In the left navigation, click **Nodes**.



> When you launch a new NetApp Hybrid Cloud Control session for the first time, there might be a delay with loading the NetApp Hybrid Cloud Control Nodes page when the management node is managing many clusters. The loading time varies depending on the number of clusters being actively managed by the management node. For subsequent launches, you will experience faster loading times.

4. On the **Storage** tab of the Nodes page, review the following information:
   a. Two-node clusters: A “two-node” label appears on the Storage tab and the associated Witness Nodes are listed.
   b. Three-node clusters: The storage nodes and associated Witness Nodes are listed. Three-node clusters have a Witness Node deployed on standby to maintain high availability in the case of node failure.
   c. Clusters with four nodes or more: Information for clusters with four or more nodes appears. Witness Nodes do not apply. If you started with two or three storage nodes and added more nodes, the Witness Nodes still appear. Otherwise, the Witness Nodes table does not appear.
   d. The firmware bundle version: Starting with management services version 2.14, if you have clusters running Element 12.0 or later, you can see the firmware bundle version for these clusters. If the nodes in a cluster have different firmware versions on them, you can see **Multiple** in the **Firmware Bundle Version** column.
   e. Custom protection domains: If custom protection domains are in use on the cluster, you can see custom protection domain assignments for each node in the cluster. If custom protection domains are not enabled, this column does not appear.
5. To view compute inventory information, click **Compute**.
6. You can manipulate the information on these pages in several ways:
   a. To filter the list of items in the results, click the **Filter** icon and select the filters. You can also enter text for the filter.
   b. To show or hide columns, click the **Show/Hide Columns** icon.

c. To download the table, click the **Download** icon.

d. To add or edit the stored BMC credentials for a compute node with BMC connection errors, click **Edit connection settings** in the error message text in the **BMC Connection Status** column. Only if the connection attempt fails for a compute node, an error message is displayed in this column for that node.

To view the number of storage and compute resources, look at the NetApp Hybrid Cloud Control (HCC) Dashboard. See Monitor storage and compute resources with the HCC Dashboard.

To manage a compute node in NetApp Hybrid Cloud Control, you must add the compute node to a vCenter host cluster.

Find more information

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

Edit Baseboard Management Controller connection information

You can change Baseboard Management Controller (BMC) administrator credentials in NetApp Hybrid Cloud Control for each of your compute nodes. You might need to change credentials prior to upgrading BMC firmware or to resolve a `Hardware ID not available` or `Unable to Detect` error indicated in NetApp Hybrid Cloud Control.

What you'll need

Cluster administrator permissions to change BMC credentials.

If you set BMC credentials during a health check, there can be a delay of up to 2 minutes before the change is reflected on the **Nodes** page.

Options

Choose one of the following options to change BMC credentials:

- Use NetApp Hybrid Cloud Control to edit BMC information
- Use the REST API to edit BMC information

Use NetApp Hybrid Cloud Control to edit BMC information

You can edit the stored BMC credentials using the NetApp Hybrid Cloud Control Dashboard.

Steps

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

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

2. Log in to NetApp Hybrid Cloud Control by providing the NetApp HCI storage cluster administrator credentials.
3. In the left navigation blue box, select the NetApp HCI installation.

   The NetApp Hybrid Cloud Control Dashboard appears.

4. In the left navigation, click **Nodes**.
5. To view compute inventory information, click **Compute**.

   A list of your compute nodes appears. The **BMC Connection Status** column shows the result of BMC connection attempts for each compute node. If the connection attempt fails for a compute node, an error message is displayed in this column for that node.

6. To add or edit the stored BMC credentials for a compute node with BMC connection errors, click **Edit connection settings** in the error message text.
7. In the dialog that appears, add the correct administrator user name and password for the BMC of this compute node.
8. Click **Save**.
9. Repeat steps 6 through 8 for any compute node that has missing or incorrect stored BMC credentials.

> Updating BMC information refreshes the inventory and ensures that management node services are aware of all hardware parameters needed to complete the upgrade.

Use the REST API to edit BMC information

You can edit the stored BMC credentials using the NetApp Hybrid Cloud Control REST API.

Steps

1. Locate the compute node hardware tag and BMC information:
   a. Open the inventory service REST API UI on the management node:

   ```
   https://<ManagementNodeIP>/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`.
      iii. Click **Authorize** to begin a session.
      iv. Close the authorization window.
   c. From the REST API UI, click **GET /installations**.
   d. Click **Try it out**.
   e. Click **Execute**.
   f. From the response, copy the installation asset ID (`id`).
   g. From the REST API UI, click **GET /installations/{id}**.
   h. Click **Try it out**.

i. Paste the installation asset ID into the **id** field.

j. Click **Execute**.

k. From the response, copy and save the node asset id (`id`), BMC IP address (`bmcAddress`), and node serial number (`chassisSerialNumber`) for use in a later step.

```
"nodes": [
  {
    "bmcDetails": {
      "bmcAddress": "10.117.1.111",
      "credentialsAvailable": false,
      "credentialsValidated": false
    },
    "chassisSerialNumber": "221111019323",
    "chassisSlot": "C",
    "hardwareId": null,
    "hardwareTag": "00000000-0000-0000-0000-ac1f6ab4ecf6",
    "id": "8cd91e3c-1b1e-1111-b00a-4c9c4900b000",
```

2. Open the hardware service REST API UI on the management node:

```
https://<ManagementNodeIP>/hardware/2/
```

3. Click **Authorize** 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. Click **Authorize** to begin a session.
   d. Close the window.
4. Click **PUT /nodes/{hardware_id}**.
5. Click **Try it out**.
6. Enter the node asset id that you saved earlier in the `hardware_id` parameter.
7. Enter the following information in the payload:

Parameter	Description
`assetId`	The installation asset id (`id`) that you saved in step 1(f).
`bmcIp`	The BMC IP address (`bmcAddress`) that you saved in step 1(k).
`bmcPassword`	An updated password to log into the BMC.
`bmcUsername`	An updated user name to log into the BMC.
`serialNumber`	The chassis serial number of the hardware.

Example payload:

```
{
  "assetId": "7bb41e3c-2e9c-2151-b00a-8a9b49c0b0fe",
  "bmcIp": "10.117.1.111",
  "bmcPassword": "mypassword1",
  "bmcUsername": "admin1",
  "serialNumber": "221111019323"
}
```

8. Click **Execute** to update BMC credentials.
   A successful result returns a response similar to the following:

```
{
  "credentialid": "33333333-cccc-3333-cccc-333333333333",
  "host_name": "hci-host",
  "id": "8cd91e3c-1b1e-1111-b00a-4c9c4900b000",
  "ip": "1.1.1.1",
  "parent": "abcd01y3-ab30-1ccc-11ee-11f123zx7d1b",
  "type": "BMC"
}
```

Find more information

- Known issues and workarounds for compute node upgrades
- NetApp Element Plug-in for vCenter Server
- NetApp HCI Resources Page

Monitor volumes on your storage cluster

The SolidFire system provisions storage using volumes. Volumes are block devices accessed over the network by iSCSI or Fibre Channel clients. You can monitor details about access groups, accounts, initiators, used capacity, Snapshot data protection status, number of iSCSI sessions, and the Quality of Service (QoS) policy associated with the volume.

You can also see details on active and deleted volumes.

With this view, you might first want to monitor the Used capacity column.

You can access this information only if you have NetApp Hybrid Cloud Control administrative privileges.

Steps

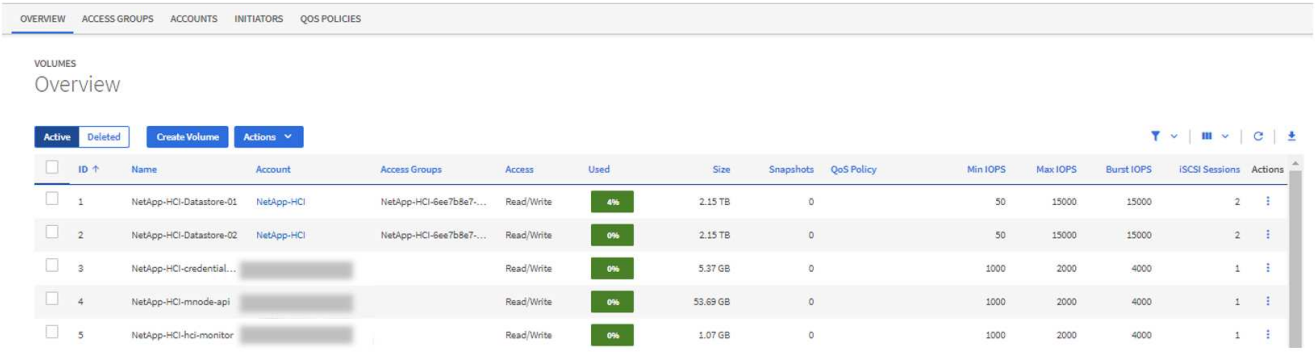
1. Open a web browser and browse to the IP address of the management node. For example:

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

2. Log in to NetApp Hybrid Cloud Control by providing the NetApp HCI storage cluster administrator credentials.
3. In the left navigation blue box, select the NetApp HCI installation.

   The Hybrid Cloud Control Dashboard appears.

4. In the left navigation, select the cluster and select **Storage** > **Volumes**.



5. On the Volumes page, use the following options:

   a. Filter the results by clicking the **Filter** icon.
   b. Hide or show columns by clicking the **Hide/Show** icon.
   c. Refresh data by clicking the **Refresh** icon.
   d. Download a CSV file by clicking on the **Download** icon.
6. Monitor the Used capacity column. If Warning, Error, or Critical thresholds are reached, the color represents the used capacity status:
   a. Warning - Yellow
   b. Error - Orange
   c. Critical - Red
7. From the Volumes view, click the tabs to see additional details about the volumes:
   a. **Access Groups**: You can see the volume access groups that are mapped from initiators to a collection of volumes for secured access.

      See information about volume access groups.

   b. **Accounts**: You can see the user accounts, which enable clients to connect to volumes on a node. When you create a volume, it is assigned to a specific user account.

      See information about NetApp HCI user accounts.

   c. **Initiators**: You can see the iSCSI initiator IQN or Fibre Channel WWPNs for the volume. Each IQN added to an access group can access each volume in the group without requiring CHAP

authentication. Each WWPN added to an access group enables Fibre Channel network access to the volumes in the access group.

d. **QoS Policies**: You can see the QoS policy applied to the volume. A QoS policy applies standardized settings for minimum IOPS, maximum IOPS, and burst IOPS to multiple volumes.

   See information about performance and QoS policies.

Find more information

- SolidFire and Element documentation
- NetApp Element Plug-in for vCenter Server
- NetApp HCI Resources Page

Monitor performance, capacity, and cluster health with SolidFire Active IQ

By using SolidFire Active IQ, you can monitor the events, performance, and capacity of your clusters. You can access SolidFire Active IQ from the NetApp Hybrid Cloud Control Dashboard.

Before you begin

- You must have a NetApp Support account to take advantage of this service.
- You must have authorization to use management node REST APIs.
- You have deployed a management node running version 12.0 or later.
- Your cluster version is running NetApp Element software 12.0 or later.
- You have Internet access. The Active IQ collector service cannot be used from dark sites.

About this task

You can obtain continually updated historical views of cluster-wide statistics. You can set up notifications to alert you about specified events, thresholds, or metrics on a cluster so that they can be addressed quickly.

As part of your normal support contract, NetApp Support monitors this data and alerts you to potential system issues.

Steps

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

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

2. Log in to NetApp Hybrid Cloud Control by providing the NetApp HCI storage cluster administrator credentials.
3. From the Dashboard, click the menu on the upper right.
4. Select **View Active IQ**.

   The SolidFire Active IQ Dashboard appears.

5. To learn about SolidFire Active IQ, from the Dashboard, click the menu icon on the upper right and click **Documentation**.
6. From the SolidFire Active IQ interface, verify that the NetApp HCI compute and storage nodes are reporting telemetry correctly to Active IQ:
   a. If you have more than one NetApp HCI installation, click **Select a Cluster** and choose the cluster from the list.
   b. In the left navigation pane, click **Nodes**.
7. If a node or nodes are missing from the list, contact NetApp Support.

> To view the number of storage and compute resources, look at the Hybrid Cloud Control (HCC) Dashboard. See Monitor storage and compute resources with the HCC Dashboard.

Find more information

- NetApp SolidFire Active IQ Documentation
- NetApp Element Plug-in for vCenter Server
- NetApp HCI Resources Page

Collect logs for troubleshooting

If you have trouble with your NetApp HCI or SolidFire all-flash storage installation, you can collect logs to send to NetApp Support to help with diagnosis. You can either use NetApp Hybrid Cloud Control or the REST API to collect logs on NetApp HCI or Element systems.

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.

Log collection options

Choose one of the following options:

- Use NetApp Hybrid Cloud Control to collect logs
- Use the REST API to collect logs

Use NetApp Hybrid Cloud Control to collect logs

You can access the log collection area from the NetApp Hybrid Cloud Control Dashboard.

Steps

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

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

2. Log in to NetApp Hybrid Cloud Control by providing the NetApp HCI or Element storage cluster administrator credentials.

3. From the Dashboard, click the menu on the upper right.
4. Select **Collect Logs**.

   The **Collect Logs** page appears. If you have collected logs before, you can download the existing log package, or begin a new log collection.

5. Select a date range in the **Date Range** drop-down menu to specify what dates the logs should include.

   If you specify a custom start date, you can select the date to begin the date range. Logs will be collected from that date up to the present time.

6. In the **Log Collection** section, select the types of log files the log package should include.

   For storage and compute logs, you can expand the list of storage or compute nodes and select individual nodes to collect logs from (or all nodes in the list).

7. Click **Collect Logs** to start log collection.

   Log collection runs in the background, and the page shows the progress.

   > Depending on the logs you collect, the progress bar might remain at a certain percentage for several minutes, or progress very slowly at some points.

8. Click **Download Logs** to download the log package.

   The log package is in a compressed UNIX .tgz file format.

Use the REST API to collect logs

You can use REST API to collect NetApp HCI or Element logs.

Steps

1. Locate the storage cluster ID:
   a. Open the management node REST API UI on the management node:

      ```
      https://<ManagementNodeIP>/logs/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.
2. Collect logs from NetApp HCI or Element:
   a. Click **POST /bundle**.
   b. Click **Try it out**.
   c. Change the values of the following parameters in the **Request body** field depending on which type of logs you need to collect and for what time range:

Parameter	Type	Description
`modifiedSince`	Date string	Only include logs modified after this date and time. For example, the value "2020-07-14T20:19:00.000Z" defines a start date of July 14, 2020 at 20:19 UTC.
`computeLogs`	Boolean	Set this parameter to `true` to include compute node logs.
`computeIds`	UUID array	If `computeLogs` is set to `true`, populate this parameter with the management node asset IDs of compute nodes to limit log collection to those specific compute nodes. Use the `GET` `https://<ManagementNodeIP>/logs/1/bundle/options` endpoint to see all possible node IDs you can use.
`mnodeLogs`	Boolean	Set this parameter to `true` to include management node logs.
`storageCrashDumps`	Boolean	Set this parameter to `true` to include storage node crash debug logs.
`storageLogs`	Boolean	Set this parameter to `true` to include storage node logs.
`storageNodeIds`	UUID array	If `storageLogs` is set to `true`, populate this parameter with the storage cluster node IDs to limit log collection to those specific storage nodes. Use the `GET` `https://<ManagementNodeIP>/logs/1/bundle/options` endpoint to see all possible node IDs you can use.

d. Click **Execute** to begin log collection.
The response should return a response similar to the following:

```
{
  "_links": {
    "self": "https://10.1.1.5/logs/1/bundle"
  },
  "taskId": "4157881b-z889-45ce-adb4-92b1843c53ee",
  "taskLink": "https://10.1.1.5/logs/1/bundle"
}
```

3. Check on the status of the log collection task:
   a. Click **GET /bundle**.
   b. Click **Try it out**.
   c. Click **Execute** to return a status of the collection task.
   d. Scroll to the bottom of the response body.

      You should see a `percentComplete` attribute detailing the progress of the collection. If the collection is complete, the `downloadLink` attribute contains the full download link including the file name of the log package.

   e. Copy the file name at the end of the `downloadLink` attribute.
4. Download the collected log package:
   a. Click **GET /bundle/{filename}**.
   b. Click **Try it out**.
   c. Paste the file name you copied earlier into the `filename` parameter text field.
   d. Click **Execute**.

      After execution, a download link appears in the response body area.

   e. Click **Download file** and save the resulting file to your computer.

      The log package is in a compressed UNIX .tgz file format.

Find more information

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

Copyright Information

Copyright © 2022 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.