Work with the management node

HCI

NetApp
April 15, 2021

Table of Contents

Work with the management node

Management node overview

You can use the management node (mNode) to use system services, manage cluster assets and settings, run system tests and utilities, configure Active IQ for system monitoring, and enable NetApp Support access for troubleshooting.

For clusters running Element software version 11.3 or later, you can work with the management node by using one of two interfaces:

- With the management node UI (`https:// [mNode IP}:442`), you can make changes to network and cluster settings, run system tests, or use system utilities.
- With the built-in REST API UI (`https://[mNode IP}/mnode`), you can run or understand APIs relating to the management node services, including proxy server configuration, service level updates, or asset management.

Install or recover a management node:

- Install a management node
- Configure a storage Network Interface Controller (NIC)
- Recover a management node

Access the management node:

- Access the management node (UI or REST API)

Perform tasks with the management node UI:

- Management node UI overview

Perform tasks with the management node REST APIs:

- Management node REST API UI overview

Disable or enable remote SSH functionality or start a remote support tunnel session with NetApp Support to help you troubleshoot:

- Enable remote NetApp Support connections
- Manage SSH functionality on the management node

Find more information

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

Install or recover a management node

Install a management node

You can manually install the management node for your cluster running NetApp Element software using the appropriate image for your configuration.

This manual process is intended for SolidFire all-flash storage administrators and NetApp HCI administrators who are not using the NetApp Deployment Engine for management node installation.

What you'll need

- Your cluster version is running NetApp Element software 11.3 or later.
- Your installation uses IPv4. The management node 11.3 does not support IPv6.

  If you need to IPv6 support, you can use the management node 11.1.

- You have permission to download software from the NetApp Support Site.
- You have identified the management node image type that is correct for your platform:

Platform	Installation image type
Microsoft Hyper-V	.iso
KVM	.iso
VMware vSphere	.iso, .ova
Citrix XenServer	.iso
OpenStack	.iso

- (Management node 12.0 and later with proxy server) You have updated NetApp Hybrid Cloud Control to management services version 2.16 before configuring a proxy server.

About this task

The Element 12.2 management node is an optional upgrade. It is not required for existing deployments.

Prior to following this procedure, you should have an understanding of persistent volumes and whether or not you want to use them. Persistent volumes are optional but recommended for management node configuration data recovery in the event of a VM loss.

Steps

1. Download ISO or OVA and deploy the VM
2. Create the management node admin and configure the network
3. Configure time sync
4. Set up the management node
5. Configure controller assets
6. (NetApp HCI only) Configure compute node assets

Download ISO or OVA and deploy the VM

1. Download the OVA or ISO for your installation from the NetApp Support Site:

Element software: https://mysupport.netapp.com/site/products/all/details/element-software/downloads-tab
NetApp HCI: https://mysupport.netapp.com/site/products/all/details/netapp-hci/downloads-tab

a. Click **Download Latest Release** and accept the EULA.

b. Select the management node image you want to download.

2. If you downloaded the OVA, follow these steps:

   a. Deploy the OVA.

   b. If your storage cluster is on a separate subnet from your management node (eth0) and you want to use persistent volumes, add a second network interface controller (NIC) to the VM on the storage subnet (for example, eth1) or ensure that the management network can route to the storage network.

3. If you downloaded the ISO, follow these steps:

   a. Create a new 64-bit virtual machine from your hypervisor with the following configuration:

      - Six virtual CPUs
      - 24GB RAM
      - 400GB virtual disk, thin provisioned
      - One virtual network interface with internet access and access to the storage MVIP.
      - (Optional for SolidFire all-flash storage) One virtual network interface with management network access to the storage cluster. If your storage cluster is on a separate subnet from your management node (eth0) and you want to use persistent volumes, add a second network interface controller (NIC) to the VM on the storage subnet (eth1) or ensure that the management network can route to the storage network.

      Do not power on the virtual machine prior to the step indicating to do so later in this procedure.

   b. Attach the ISO to the virtual machine and boot to the .iso install image.

      Installing a management node using the image might result in 30-second delay before the splash screen appears.

4. Power on the virtual machine for the management node after the installation completes.

Create the management node admin and configure the network

1. Using the terminal user interface (TUI), create a management node admin user.

   To move through the menu options, press the Up or Down arrow keys. To move through the buttons, press Tab. To move from the buttons to the fields, press Tab. To navigate between fields, press the Up or Down arrow keys.

2. Configure the management node network (eth0).

   If you need an additional NIC to isolate storage traffic, see instructions on configuring another NIC: Configure a storage Network Interface Controller (NIC).

Configure time sync

1. Ensure time is synced between the management node and the storage cluster using NTP:
   a. Log in to the management node using SSH or the console provided by your hypervisor.
   b. Stop NTPD:

```
sudo service ntpd stop
```

   c. Edit the NTP configuration file `/etc/ntp.conf`:
      i. Comment out the default servers (`server 0.gentoo.pool.ntp.org`) by adding a `#` in front of each.
      ii. Add a new line for each default time server you want to add. The default time servers must be the same NTP servers used on the storage cluster that you will use in a later step.

```
vi /etc/ntp.conf

#server 0.gentoo.pool.ntp.org
#server 1.gentoo.pool.ntp.org
#server 2.gentoo.pool.ntp.org
#server 3.gentoo.pool.ntp.org
server <insert the hostname or IP address of the default time
server>
```

      iii. Save the configuration file when complete.
   d. Force an NTP sync with the newly added server.

```
sudo ntpd -gq
```

   e. Restart NTPD.

```
sudo service ntpd start
```

   f. Disable time synchronization with host via the hypervisor (the following is a VMware example):

If you deploy the mNode in a hypervisor environment other than VMware, for example, from the .iso image in an Openstack environment, refer to the hypervisor documentation for the equivalent commands.

      i. Disable periodic time synchronization:

```
vmware-toolbox-cmd timesync disable
```

ii. Display and confirm the current status of the service:

```
vmware-toolbox-cmd timesync status
```

iii. In vSphere, verify that the `Synchronize guest time with host` box is un-checked in the VM options.

Do not enable this option if you make future changes to the VM.

Set up the management node

1. Configure and run the management node setup command:

You will be prompted to enter passwords in a secure prompt. If your cluster is behind a proxy server, you must configure the proxy settings so you can reach a public network.

```
/sf/packages/mnode/setup-mnode --mnode_admin_user [username]
--storage_mvip [mvip] --storage_username [username] --telemetry_active
[true]
```

a. Replace the value in [ ] brackets (including the brackets) for each of the following required parameters:

The abbreviated form of the command name is in parentheses ( ) and can be substituted for the full name.

- **--mnode_admin_user (-mu) [username]**: The username for the management node administrator account. This is likely to be the username for the user account you used to log into the management node.
- **--storage_mvip (-sm) [MVIP address]**: The management virtual IP address (MVIP) of the storage cluster running Element software. Configure the management node with the same storage cluster that you used during NTP servers configuration.
- **--storage_username (-su) [username]**: The storage cluster administrator username for the cluster specified by the `--storage_mvip` parameter.
- **--telemetry_active (-t) [true]**: Retain the value true that enables data collection for analytics by Active IQ.

b. (Optional): Add Active IQ endpoint parameters to the command:

- **--remote_host (-rh) [AIQ_endpoint]**: The endpoint where Active IQ telemetry data is sent to be processed. If the parameter is not included, the default endpoint is used.

c. (Recommended): Add the following persistent volume parameters. Do not modify or delete the account and volumes created for persistent volumes functionality or a loss in management capability will result.

- **--use_persistent_volumes (-pv) [true/false, default: false]**: Enable or disable persistent volumes. Enter the value true to enable persistent volumes functionality.
- **--persistent_volumes_account (-pva) [account_name]**: If `--use_persistent_volumes` is set to true, use this parameter and enter the storage account name that will be used for persistent volumes.

Use a unique account name for persistent volumes that is different from any existing account name on the cluster. It is critically important to keep the account for persistent volumes separate from the rest of your environment.

- **--persistent_volumes_mvip (-pvm) [mvip]**: Enter the management virtual IP address (MVIP) of the storage cluster running Element software that will be used with persistent volumes. This is only required if multiple storage clusters are managed by the management node. If multiple clusters are not managed, the default cluster MVIP will be used.

d. Configure a proxy server:

- **--use_proxy (-up) [true/false, default: false]**: Enable or disable the use of the proxy. This parameter is required to configure a proxy server.
- **--proxy_hostname_or_ip (-pi) [host]**: The proxy hostname or IP. This is required if you want to use a proxy. If you specify this, you will be prompted to input `--proxy_port`.
- **--proxy_username (-pu) [username]**: The proxy username. This parameter is optional.
- **--proxy_password (-pp) [password]**: The proxy password. This parameter is optional.
- **--proxy_port (-pq) [port, default: 0]**: The proxy port. If you specify this, you will be prompted to input the proxy host name or IP (`--proxy_hostname_or_ip`).
- **--proxy_ssh_port (-ps) [port, default: 443]**: The SSH proxy port. This defaults to port 443.

e. (Optional) Use parameter help if you need additional information about each parameter:

- **--help (-h)**: Returns information about each parameter. Parameters are defined as required or optional based on initial deployment. Upgrade and redeployment parameter requirements might vary.

f. Run the `setup-mnode` command.

Configure controller assets

1. Locate the installation ID:
   a. From a browser, log into the management node REST API UI:
   b. Go to the storage MVIP and log in. This action causes the certificate to be accepted for the next step.
   c. Open the inventory service REST API UI on the management node:

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

   d. 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.
   e. From the REST API UI, click **GET /installations**.
   f. Click **Try it out**.
   g. Click **Execute**.
   h. From the code 200 response body, copy and save the `id` for the installation for use in a later step.

Your installation has a base asset configuration that was created during installation or upgrade.

2. (NetApp HCI only) Locate the hardware tag for your compute node in vSphere:
   a. Select the host in the vSphere Web Client navigator.
   b. Click the **Monitor** tab, and click **Hardware Health**.
   c. The node BIOS manufacturer and model number are listed. Copy and save the value for `tag` for use in a later step.
3. Add a vCenter controller asset for NetApp HCI monitoring (NetApp HCI installations only) and Hybrid Cloud Control (for all installations) to the management node known assets:
   a. Access the mnode service API UI on the management node by entering the management node IP address followed by `/mnode`:

      ```
      https://[management node IP]/mnode
      ```

   b. Click **Authorize** or any lock icon 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 window.
   c. Click **POST /assets/{asset_id}/controllers** to add a controller sub-asset.
   d. Click **Try it out**.
   e. Enter the parent base asset ID you copied to your clipboard in the **asset_id** field.
   f. Enter the required payload values with type `vCenter` and vCenter credentials.
   g. Click **Execute**.

(NetApp HCI only) Configure compute node assets

1. (For NetApp HCI only) Add a compute node asset to the management node known assets:
   a. Click **POST /assets/{asset_id}/compute-nodes** to add a compute node sub-asset with credentials for the compute node asset.
   b. Click **Try it out**.
   c. Enter the parent base asset ID you copied to your clipboard in the **asset_id** field.
   d. In the payload, enter the required payload values as defined in the Model tab. Enter `ESXi Host` as `type` and enter the hardware tag you saved during a previous step for `hardware_tag`.
   e. Click **Execute**.

Find more Information

- Persistent volumes
- Add an asset to the management node
- Configure a storage NIC
- NetApp Element Plug-in for vCenter Server

- NetApp HCI Resources Page

Configure a storage Network Interface Controller (NIC)

If you are using an additional NIC for storage, you can SSH in to the management node or use the vCenter console and run a curl command to set up a tagged or untagged network interface.

Before you begin

- You know your eth0 IP address.
- Your cluster version is running NetApp Element software 11.3 or later.
- You have deployed a management node 11.3 or later.

Configuration options

Choose the option that is relevant for your environment:

- Configure a storage Network Interface Controller (NIC) for an untagged network interface
- Configure a storage Network Interface Controller (NIC) for a tagged network interface

Configure a storage Network Interface Controller (NIC) for an untagged network interface

Steps

1. Open an SSH or vCenter console.
2. Replace the values in the following command template and run the command:

Values are represented by `$` for each of the required parameters for your new storage network interface. The `cluster` object in the following template is required and can be used for management node host name renaming. `--insecure` or `-k` options should not be used in production environments.

```
curl -u $mnode_user_name:$mnode_password --insecure -X POST \
https://$mnode_IP:442/json-rpc/10.0 \
-H 'Content-Type: application/json' \
-H 'cache-control: no-cache' \
-d ' {
     "params": {
                "network": {
                           "$eth1": {
                                    "#default" : false,
                                    "address" : "$storage_IP",
                                    "auto" : true,
                                    "family" : "inet",
                                    "method" : "static",
                                    "mtu" : "9000",
                                    "netmask" : "$subnet_mask",
                                    "status" : "Up"
                                    }
                           },
                "cluster": {
                           "name": "$mnode_host_name"
                           }
              },
    "method": "SetConfig"
}
'
```

Configure a storage Network Interface Controller (NIC) for a tagged network interface

Steps

1. Open an SSH or vCenter console.
2. Replace the values in the following command template and run the command:

Values are represented by `$` for each of the required parameters for your new storage network interface. The `cluster` object in the following template is required and can be used for management node host name renaming. `--insecure` or `-k` options should not be used in production environments.

```
curl -u $mnode_user_name:$mnode_password --insecure -X POST \
https://$mnode_IP:442/json-rpc/10.0 \
-H 'Content-Type: application/json' \
-H 'cache-control: no-cache' \
-d ' {
     "params": {
               "network": {
                         "$eth1": {
                                  "#default" : false,
                                  "address" : "$storage_IP",
                                  "auto" : true,
                                  "family" : "inet",
                                  "method" : "static",
                                  "mtu" : "9000",
                                  "netmask" : "$subnet_mask",
                                  "status" : "Up",
                                  "virtualNetworkTag" : "$vlan_id"
                                  }
                          },
               "cluster": {
                         "name": "$mnode_host_name",
                         "cipi": "$eth1.$vlan_id",
                         "sipi": "$eth1.$vlan_id"
                         }
             },
    "method": "SetConfig"
}
'
```

Find more Information

- Add an asset to the management node
- NetApp Element Plug-in for vCenter Server
- NetApp HCI Resources Page

Recover a management node

You can manually recover and redeploy the management node for your cluster running NetApp Element software if your previous management node used persistent volumes.

You can deploy a new OVA and run a redeploy script to pull configuration data from a previously installed management node running version 11.3 and later.

What you'll need

- Your previous management node was running NetApp Element software version 11.3 or later with

persistent volumes functionality engaged.

- You know the MVIP and SVIP of the cluster containing the persistent volumes.
- Your cluster version is running NetApp Element software 11.3 or later.
- Your installation uses IPv4. The management node 11.3 does not support IPv6.
- You have permission to download software from the NetApp Support Site.
- You have identified the management node image type that is correct for your platform:

Platform	Installation image type
Microsoft Hyper-V	.iso
KVM	.iso
VMware vSphere	.iso, .ova
Citrix XenServer	.iso
OpenStack	.iso

Steps

1. Download ISO or OVA and deploy the VM
2. Configure the network
3. Configure time sync
4. Configure the management node

Download ISO or OVA and deploy the VM

1. Download the OVA or ISO for your installation from the NetApp Support Site:

   Element software: https://mysupport.netapp.com/site/products/all/details/element-software/downloads-tab
   NetApp HCI: https://mysupport.netapp.com/site/products/all/details/netapp-hci/downloads-tab

   a. Click **Download Latest Release** and accept the EULA.
   b. Select the management node image you want to download.
2. If you downloaded the OVA, follow these steps:
   a. Deploy the OVA.
   b. If your storage cluster is on a separate subnet from your management node (eth0) and you want to use persistent volumes, add a second network interface controller (NIC) to the VM on the storage subnet (for example, eth1) or ensure that the management network can route to the storage network.
3. If you downloaded the ISO, follow these steps:
   a. Create a new 64-bit virtual machine from your hypervisor with the following configuration:
      - Six virtual CPUs
      - 24GB RAM
      - 400GB virtual disk, thin provisioned
      - One virtual network interface with internet access and access to the storage MVIP.
      - (Optional for SolidFire all-flash storage) One virtual network interface with management network access to the storage cluster. If your storage cluster is on a separate subnet from your

management node (eth0) and you want to use persistent volumes, add a second network interface controller (NIC) to the VM on the storage subnet (eth1) or ensure that the management network can route to the storage network.

Do not power on the virtual machine prior to the step indicating to do so later in this procedure.

b. Attach the ISO to the virtual machine and boot to the .iso install image.

Installing a management node using the image might result in 30-second delay before the splash screen appears.

4. Power on the virtual machine for the management node after the installation completes.

Configure the network

1. Using the terminal user interface (TUI), create a management node admin user.

To move through the menu options, press the Up or Down arrow keys. To move through the buttons, press Tab. To move from the buttons to the fields, press Tab. To navigate between fields, press the Up or Down arrow keys.

2. Configure the management node network (eth0).

If you need an additional NIC to isolate storage traffic, see instructions on configuring another NIC: Configure a storage Network Interface Controller (NIC).

Configure time sync

1. Ensure time is synced between the management node and the storage cluster using NTP:
   a. Log in to the management node using SSH or the console provided by your hypervisor.
   b. Stop NTPD:

```
sudo service ntpd stop
```

   c. Edit the NTP configuration file `/etc/ntp.conf`:
      i. Comment out the default servers (`server 0.gentoo.pool.ntp.org`) by adding a `#` in front of each.
      ii. Add a new line for each default time server you want to add. The default time servers must be the same NTP servers used on the storage cluster that you will use in a later step.

```
vi /etc/ntp.conf

#server 0.gentoo.pool.ntp.org
#server 1.gentoo.pool.ntp.org
#server 2.gentoo.pool.ntp.org
#server 3.gentoo.pool.ntp.org
server <insert the hostname or IP address of the default time
server>
```

iii. Save the configuration file when complete.

d. Force an NTP sync with the newly added server.

```
sudo ntpd -gq
```

e. Restart NTPD.

```
sudo service ntpd start
```

f. Disable time synchronization with host via the hypervisor (the following is a VMware example):

If you deploy the mNode in a hypervisor environment other than VMware, for example, from the .iso image in an Openstack environment, refer to the hypervisor documentation for the equivalent commands.

i. Disable periodic time synchronization:

```
vmware-toolbox-cmd timesync disable
```

ii. Display and confirm the current status of the service:

```
vmware-toolbox-cmd timesync status
```

iii. In vSphere, verify that the `Synchronize guest time with host` box is un-checked in the VM options.

Do not enable this option if you make future changes to the VM.

Configure the management node

1. Create a temporary destination directory for the management services bundle contents:

```
mkdir -p /sf/etc/mnode/mnode-archive
```

2. Download the management services bundle (version 2.15.28 or later) that was previously installed on the existing management node and save it in the `/sf/etc/mnode/` directory.
3. Extract the downloaded bundle using the following command, replacing the value in [ ] brackets (including the brackets) with the name of the bundle file:

```
tar -C /sf/etc/mnode -xvf /sf/etc/mnode/[management services bundle
file]
```

4. Extract the resulting file to the `/sf/etc/mnode-archive` directory:

```
tar -C /sf/etc/mnode/mnode-archive -xvf
/sf/etc/mnode/services_deploy_bundle.tar.gz
```

5. Create a configuration file for accounts and volumes:

```
echo '{"trident": true, "mvip": "[mvip IP address]", "account_name":
"[persistent volume account name]"}' | sudo tee /sf/etc/mnode/mnode-
archive/management-services-metadata.json
```

   a. Replace the value in [ ] brackets (including the brackets) for each of the following required parameters:
      - **[mvip IP address]**: The management virtual IP address of the storage cluster. Configure the management node with the same storage cluster that you used during NTP servers configuration.
      - **[persistent volume account name]**: The name of the account associated with all persistent volumes in this storage cluster.

6. Configure and run the management node redeploy command to connect to persistent volumes hosted on the cluster and start services with previous management node configuration data:

   You will be prompted to enter passwords in a secure prompt. If your cluster is behind a proxy server, you must configure the proxy settings so you can reach a public network.

```
/sf/packages/mnode/redeploy-mnode --mnode_admin_user [username]
```

   a. Replace the value in [ ] brackets (including the brackets) with the user name for the management node administrator account. This is likely to be the username for the user account you used to log into the management node.

      You can add the user name or allow the script to prompt you for the information.

   b. Run the `redeploy-mnode` command. The script displays a success message when the redeployment is complete.

c. If you access Element or NetApp HCI web interfaces (such as the management node or NetApp Hybrid Cloud Control) using the Fully Qualified Domain Name (FQDN) of the system, reconfigure authentication for the management node.

If you had previously disabled SSH functionality on the management node, you need to disable SSH again on the recovered management node. SSH capability that provides NetApp Support remote support tunnel (RST) session access is enabled on the management node by default.

Find more Information

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

Access the management node

Beginning with NetApp Element software version 11.3, the management node contains two UIs: a UI for managing REST-based services and a per-node UI for managing network and cluster settings and operating system tests and utilities.

For clusters running Element software version 11.3 or later, you can make use one of two interfaces:

- By using the management node UI (`https:// [mNode IP}:442`), you can make changes to network and cluster settings, run system tests, or use system utilities.
- By using the built-in REST API UI (`https://[mNode IP}/mnode`), you can run or understand APIs relating to the management node services, including proxy server configuration, service level updates, or asset management.

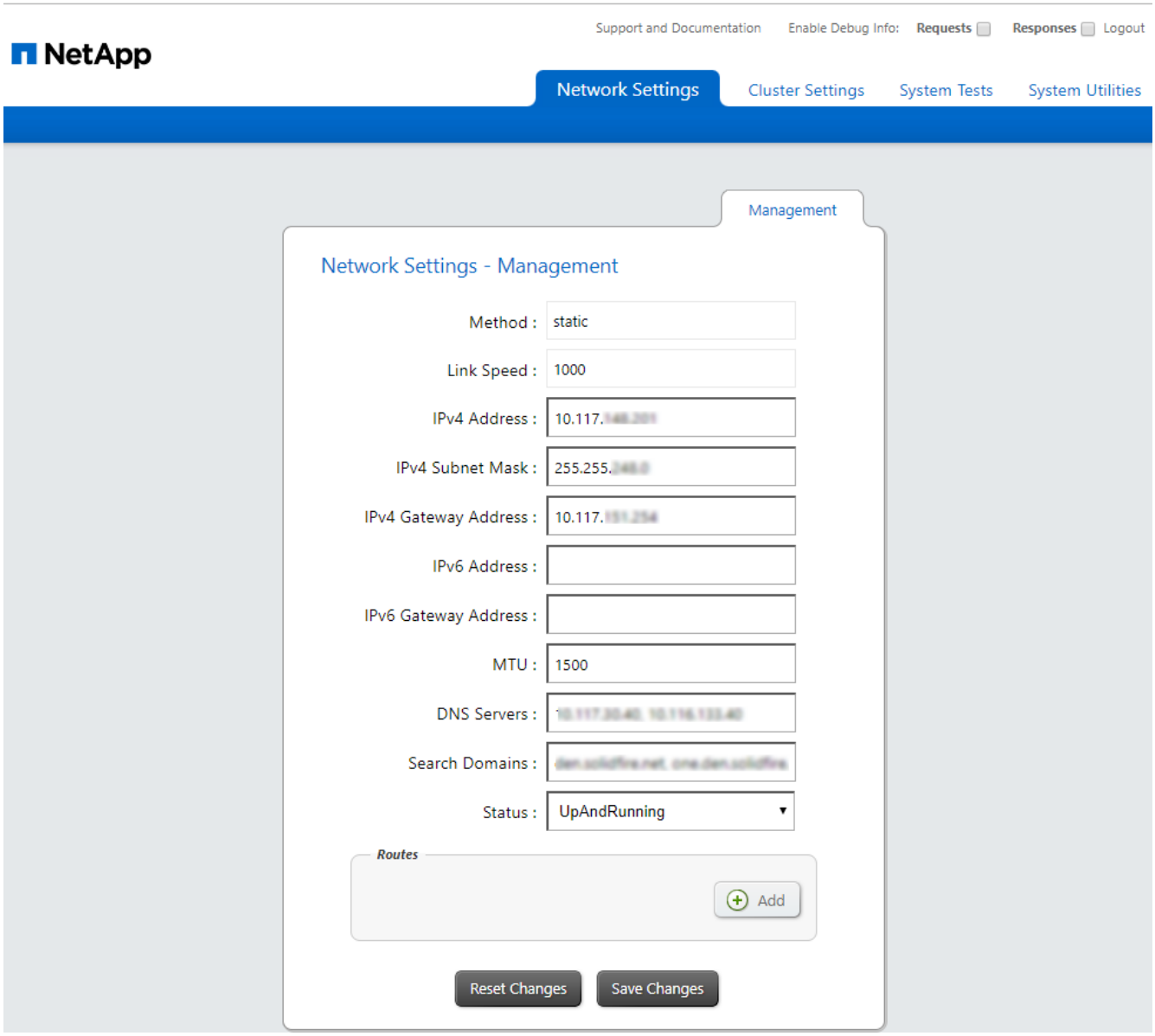
Access the management node per-node UI

From the per-node UI, you can access network and cluster settings and utilize system tests and utilities.

Steps

1. Access the per-node UI for the management node by entering the management node IP address followed by :442

```
https://[IP address]:442
```



2. Enter the management node user name and password when prompted.

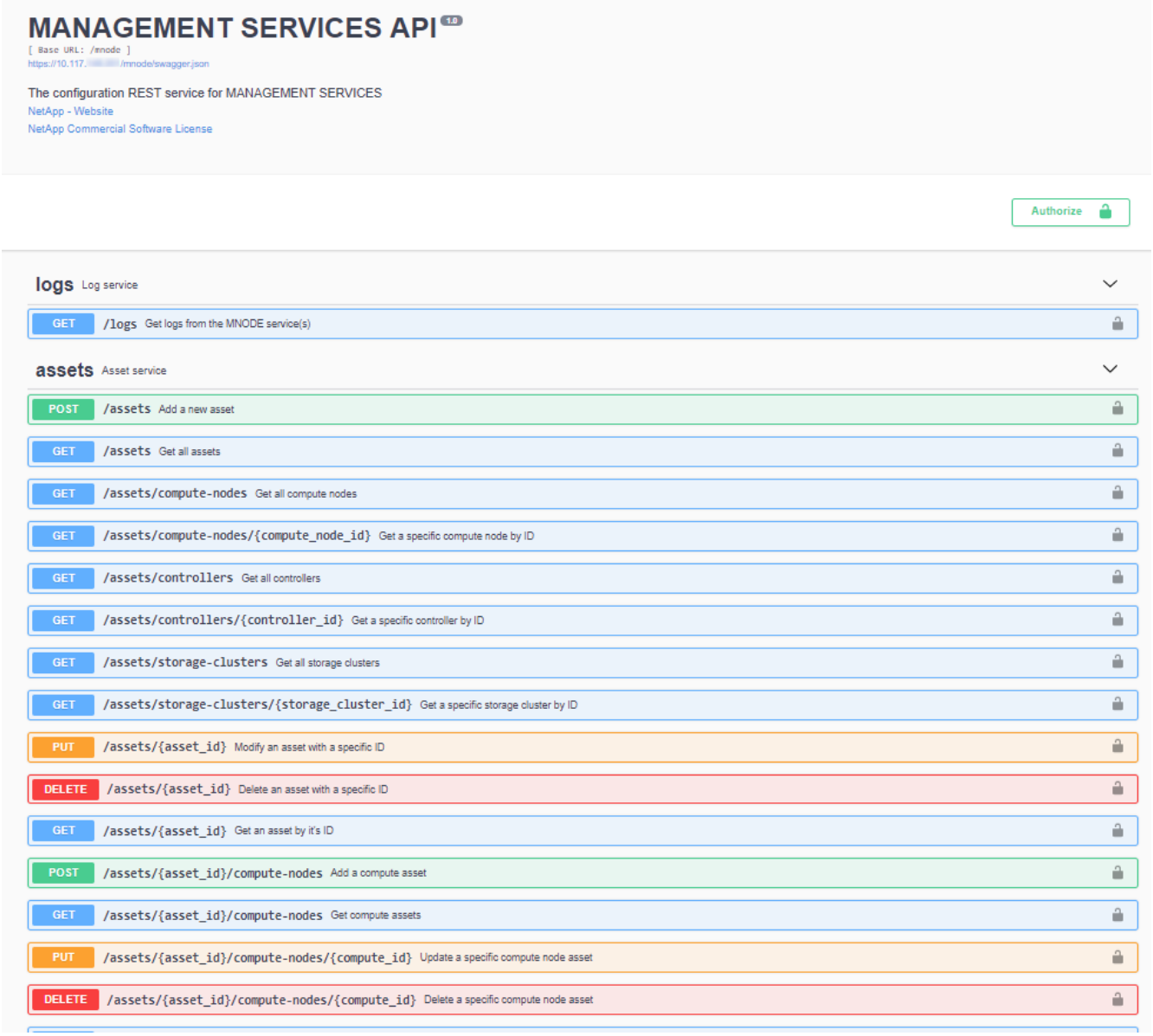
Access the management node REST API UI

From the REST API UI, you can access a menu of service-related APIs that control management services on the management node.

Steps

1. To access the REST API UI for management services, enter the management node IP address followed by `/mnode`:

```
https://[IP address]/mnode
```



2. Click **Authorize** or any lock icon and enter cluster admin credentials for permissions to use APIs.

Find more Information

- Enable the Active IQ collector service for SolidFire all-flash storage
- NetApp Element Plug-in for vCenter Server
- NetApp HCI Resources Page

Work with the management node UI

Management node UI overview

With the management node UI (`https://<managementNodeIP>:442`), you can make changes to network and cluster settings, run system tests, or use system utilities.

Tasks you can perform with the management node UI:

- Configure alert monitoring on NetApp HCI
- Modify and test the management node network, cluster, and system settings
- Run system utilities from the management node

Find more information

- Access the management node
- NetApp Element Plug-in for vCenter Server
- NetApp HCI Resources Page

Configure alert monitoring on NetApp HCI

You can configure settings to monitor alerts on your NetApp HCI system.

NetApp HCI alert monitoring forwards NetApp HCI storage cluster system alerts to vCenter Server, enabling you to view all alerts for NetApp HCI from the vSphere Web Client interface.

These tools are not configured or used for storage-only clusters, such as SolidFire all-flash storage. Running the tools for these clusters results in the following 405 error, which is expected given the configuration: `webUIParseError : Invalid response from server. 405`

1. Open the per-node management node UI (`https://[IP address]:442`).
2. Click the **Alert Monitor** tab.
3. Configure the alert monitoring options.

Alert monitoring options

options	Description
Run Alert Monitor Tests	Runs the monitor system tests to check for the following: • NetApp HCI and VMware vCenter connectivity • Pairing of NetApp HCI and VMware vCenter through datastore information supplied by the QoSSIOC service • Current NetApp HCI alarm and vCenter alarm lists
Collect Alerts	Enables or disables the forwarding of NetApp HCI storage alarms to vCenter. You can select the target storage cluster from the drop-down list. The default setting for this option is `Enabled`.

options	Description
Collect Best Practice Alerts	Enables or disables the forwarding of NetApp HCI storage Best Practice alerts to vCenter. Best Practice alerts are faults that are triggered by a sub-optimal system configuration. The default setting for this option is `Disabled`. When disabled, NetApp HCI storage Best Practice alerts do not appear in vCenter.
Send Support Data To AIQ	Controls the flow of support and monitoring data from VMware vCenter to NetApp SolidFire Active IQ. Options are the following: • Enabled: All vCenter alarms, NetApp HCI storage alarms, and support data are sent to NetApp SolidFire Active IQ. This enables NetApp to proactively support and monitor the NetApp HCI installation, so that possible problems can be detected and resolved before affecting the system. • Disabled: No vCenter alarms, NetApp HCI storage alarms, or support data are sent to NetApp SolidFire Active IQ.  If you turned off the **Send data to AIQ** option using NetApp Deployment Engine, you need to enable telemetry again using the management node REST API to configure the service from this page.

options	Description
Send Compute Node Data To AIQ	Controls the flow of support and monitoring data from the compute nodes to NetApp SolidFire Active IQ. Options are the following: • Enabled: Support and monitoring data about the compute nodes is transmitted to NetApp SolidFire Active IQ to enable proactive support for the compute node hardware. • Disabled: Support and monitoring data about the compute nodes is not transmitted to NetApp SolidFire Active IQ. If you turned off the **Send data to AIQ** option using NetApp Deployment Engine, you need to enable telemetry again using the management node REST API to configure the service from this page.

Find more Information

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

Work with the management node REST API

Management node REST API UI overview

By using the built-in REST API UI (`https://<managementNodeIP>/mnode`), you can run or understand APIs relating to the management node services, including proxy server configuration, service level updates, or asset management.

Tasks you can perform with REST APIs:

Authorization

- Get authorization to use REST APIs

Asset configuration

- Enable Active IQ and NetApp HCI monitoring
- Configure a proxy server for the management node
- Configure NetApp Hybrid Cloud Control for multiple vCenters
- Add compute and controller assets to the management node

- Create and manage storage cluster assets

Asset management

- View or edit existing controller assets
- Create and manage storage cluster assets
- Remove an asset from the management node
- Use the REST API to collect NetApp HCI logs
- Verify management node OS and services versions
- Getting logs from management services

Find more information

- Access the management node
- NetApp Element Plug-in for vCenter Server
- NetApp HCI Resources Page

Get authorization to use REST APIs

You must authorize before you can use APIs for management services in the REST API UI. You do this by obtaining an access token.

To obtain a token, you provide cluster admin credentials and a client ID. Each token lasts approximately ten minutes. After a token expires, you can authorize again for a new access token.

Authorization functionality is set up for you during management node installation and deployment. The token service is based on the storage cluster you defined during setup.

Before you begin

- Your cluster version should be running NetApp Element software 11.3 or later.
- You should have deployed a management node running version 11.3 or later.

Steps

1. Access the REST API UI for the service by entering the management node IP address followed by the service name, for example `/mnode/`:

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

2. Click **Authorize**.

   Alternately, you can click on a lock icon next to any service API.

3. Complete the following:
   a. Enter the cluster user name and password.
   b. Enter the client ID as `mnode-client`.
   c. Do not enter a value for the client secret.

d. Click **Authorize** to begin a session.

4. Close the **Available authorizations** dialog box.

If you try to run a command after the token expires, a `401 Error: UNAUTHORIZED` message appears. If you see this, authorize again.

Find more information

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

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.

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).

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

Configure a proxy server

If your cluster is behind a proxy server, you must configure the proxy settings so that you can reach a public network.

A proxy server is used for telemetry collectors and reverse tunnel connections. You can enable and configure a proxy server using the REST API UI if you did not already configure a proxy server during installation or upgrade. You can also modify existing proxy server settings or disable a proxy server.

The command to configure a proxy server updates and then returns the current proxy settings for the management node. The proxy settings are used by Active IQ, the NetApp HCI monitoring service that is deployed by the NetApp Deployment Engine, and other Element software utilities that are installed on the management node, including the reverse support tunnel for NetApp Support.

Before you begin

- You should know host and credential information for the proxy server you are configuring.
- Ensure that your 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.
- (Management node 12.0 and later) You have updated NetApp Hybrid Cloud Control to management services version 2.16 before configuring a proxy server.

Steps

1. Access the REST API UI on the management node by entering the management node IP address followed by `/mnode`:

   ```
   https://[management node IP]/mnode
   ```

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 /settings**.
4. Click **Try it out**.
5. To enable a proxy server, you must set `use_proxy` to true. Enter the IP or host name and proxy port destinations.

   The proxy user name, proxy password, and SSH port are optional and should be omitted if not used.

```
{
"proxy_ip_or_hostname": "[IP or name]",
"use_proxy": [true/false],
"proxy_username": "[username]",
"proxy_password": "[password]",
"proxy_port": [port value],
"proxy_ssh_port": [port value: default is 443]
}
```

6. Click **Execute**.

Find more information

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

Verify management node OS and services versions

You can verify the version numbers of the management node OS, management services bundle, and individual services running on the management node using the REST API in the management node.

What you'll need

- Your cluster is running NetApp Element software 11.3 or later.
- You have deployed a management node running version 11.3 or later.

Options

- API commands
- REST API UI steps

API commands

- Get version information about the management node OS, the management services bundle, and the management node API (mnode-api) service that are running on the management node:

```
curl -X GET "https://<managementNodeIP>/mnode/about" -H  "accept:
application/json"
```

- Get version information about individual services running on the management node:

```
curl -X GET "https://<managementNodeIP>/mnode/services?status=running"
-H  "accept: */*" -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 service by entering the management node IP address followed by `/mnode/`:

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

2. Do one of the following:
   - Get version information about the management node OS, the management services bundle, and the management node API (mnode-api) service that are running on the management node:
     a. Select **GET /about**.
     b. Select **Try it out**.
     c. Select **Execute**.

     The management services bundle version (`"mnode_bundle_version"`), management node OS version (`"os_version"`), and management node API version (`"version"`) are indicated in the response body.
   - Get version information about individual services running on the management node:
     a. Select **GET /services**.
     b. Select **Try it out**.
     c. Select the status as **Running**.
     d. Select **Execute**.

     The services that are running on the management node are indicated in the response body.

Find more information

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

Getting logs from management services

You can retrieve logs from the services running on the management node using the REST API. You can pull logs from all public services or specify specific services and use query parameters to better define the return results.

What you'll need

- Your cluster version is running NetApp Element software 11.3 or later.
- You have deployed a management node running version 11.3 or later.

Steps

1. Open the REST API UI on the management node:

```
https://[managementNodeIP]/mnode
```

2. Select **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 if the value is not already populated.
   c. Select **Authorize** to begin a session.
   d. Close the window.
3. Select **GET /logs**.
4. Select **Try it out**.
5. Specify the following parameters:
   - `Lines`: Enter the number of lines you want the log to return. This parameter is an integer that defaults to 1000.

     Avoid requesting the entire history of log content by setting Lines to 0.
   - `since`: Adds a ISO-8601 timestamp for the service logs starting point.

     Use a reasonable `since` parameter when gathering logs of wider timespans.
   - `service-name`: Enter a service name.

     Use the `GET /services` command to list services on the management node.
   - `stopped`: Set to `true` to retrieve logs from stopped services.
6. Select **Execute**.

Find more Information

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

Manage support connections

Start a remote NetApp Support session

If you require technical support for your NetApp HCI or SolidFire all-flash storage system, NetApp Support can connect remotely with your system. To start a session and gain remote access, NetApp Support can open a reverse Secure Shell (SSH) connection to your environment.

About this task

You can open a TCP port for an SSH reverse tunnel connection with NetApp Support. This connection enables

NetApp Support to log in to your management node. If your management node is behind a proxy server, the following TCP ports are required in the sshd.config file:

TCP port	Description	Connection direction
443	API calls/HTTPS for reverse port forwarding via open support tunnel to the web UI	Management node to storage nodes
22	SSH login access	Management node to storage nodes or from storage nodes to management node

By default, the capability for remote access is enabled on the management node. To disable remote access functionality, see Manage SSH functionality on the management node. You can enable remote access functionality again, if needed.

Steps

- Log in to your management node and open a terminal session.
- At a prompt, enter the following:

```
rst -r sfsupport.solidfire.com -u element -p <port_number>
```

- To close the remote support tunnel, enter the following:

```
rst --killall
```

Find more information

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

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