Work with the management node

HCI

NetApp
August 10, 2020

Table of Contents

Work with the management node

Management node overview

You can use the management node (mNode) to upgrade 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)

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

Tasks you can perform with the management node REST APIs:

- Get authorization to use REST APIs
- Enable Active IQ and NetApp HCI monitoring
- Add compute and controller assets to the management node
- Change the storage cluster administrator password
- Configure a proxy server for the management node
- Use the REST API to collect NetApp HCI logs

Enable remote NetApp Support connections to help you troubleshoot:

- Enable remote NetApp Support connections

Find more information

- NetApp HCI Documentation Center
- 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.

Before you begin

- 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

About this task

Prior to following this procedure, you should have an understanding of persistent volumes and whether or not you want to use them.

Steps

1. Download ISO or OVA and deploy the VM

2. Create the management node admin and configure the network
3. Configure the management node
4. Configure controller assets
5. (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
      - 12GB 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 the management node

1. SSH into the management node.
2. Using SSH, run the following command to gain root privileges. Enter your password when prompted:

```
sudo su
```

3. Ensure time is synced (NTP) between the management node and the storage cluster.

In vSphere, the **Synchronize guest time with host** box should be checked in the VM options. Do not disable this option if you make future changes to the VM.

4. 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.
- **--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. (Optional): 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.

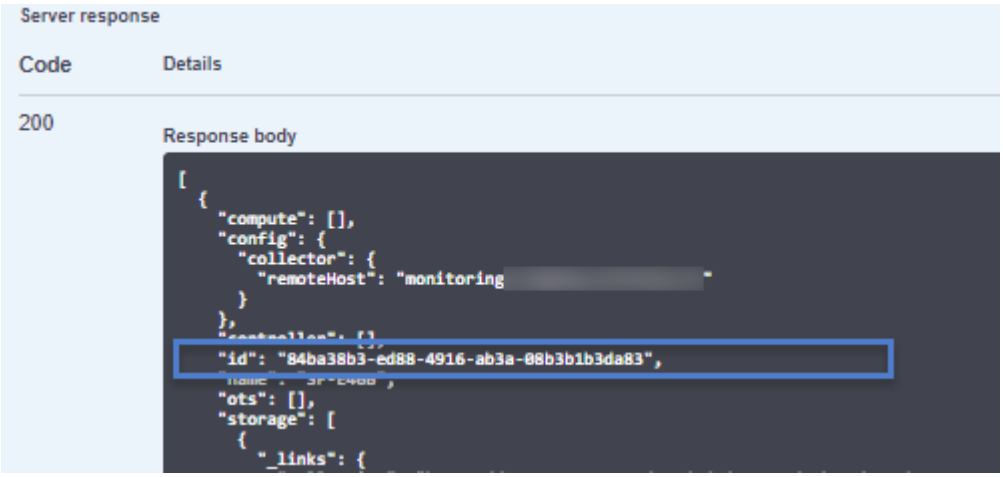
f. Run the `setup-mnode` command.

Configure controller assets

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

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

2. From the management node REST API UI, 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. Run **GET /assets** to find the base asset ID that you will need for the next steps:
   1. Click **GET /assets**.
   2. Click **Try it out**.
   3. Click **Execute**.
   4. Copy the value for `"id"` for the base asset to your clipboard:



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

4. 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. Click **POST /assets/{asset_id}/controllers** to add a controller sub-asset.
   b. Click **Try it out**.
   c. Enter the required payload values as defined in the **Model** tab with type vCenter and vCenter credentials.
   d. Enter the parent base asset ID you copied to your clipboard in the **asset_id** field.
   e. 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. In the payload, enter the required payload values as defined in the Model tab. Use type `ESXi Host` and remove the `"hardware_tag"` parameter.
   d. Enter the parent base asset ID you copied to your clipboard in the **asset_id** field.
   e. Click **Execute**.

Find more Information

- Persistent volumes
- Add an asset to the management node
- Configure a storage NIC
- NetApp HCI Documentation Center
- 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 that 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.

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. The `--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"
}
'
```

Find more Information

- Add an asset to the management node
- NetApp HCI Documentation Center
- 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.

Before you begin

- 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

About this task

Prior to completing this procedure, you should have an understanding of persistent volumes and whether or not you want to use them.

- Download ISO or OVA and deploy the VM
- Configure the network
- 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
      - 12GB 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 the management node

1. SSH into the management node or use the console provided by your hypervisor.
2. Using SSH, run the following command to gain root privileges. Enter your password when prompted:

```
sudo su
```

3. Ensure time is synced (NTP) between the management node and the storage cluster.

In vSphere, the **Synchronize guest time with host** box should be checked in the VM options. Do not disable this option if you make future changes to the VM.

4. 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) 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. You can add the following required parameters or allow the script to prompt you for the information.

- **--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 with the persistent volumes that contain management node data for recovery.
- **--storage_username (-su) [username]**: The storage cluster administrator username for the cluster specified by the `--storage_mvip` parameter.

- **--persistent_volumes_account (-pva) [account_name]**: Enter the storage account name from the cluster containing the persistent volumes. This is the exact name of the storage user account that owns the volumes in the cluster.

b. (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.

c. Run the `redeploy-mnode` command.

Find more Information

- Persistent volumes
- NetApp HCI Documentation Center
- 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.

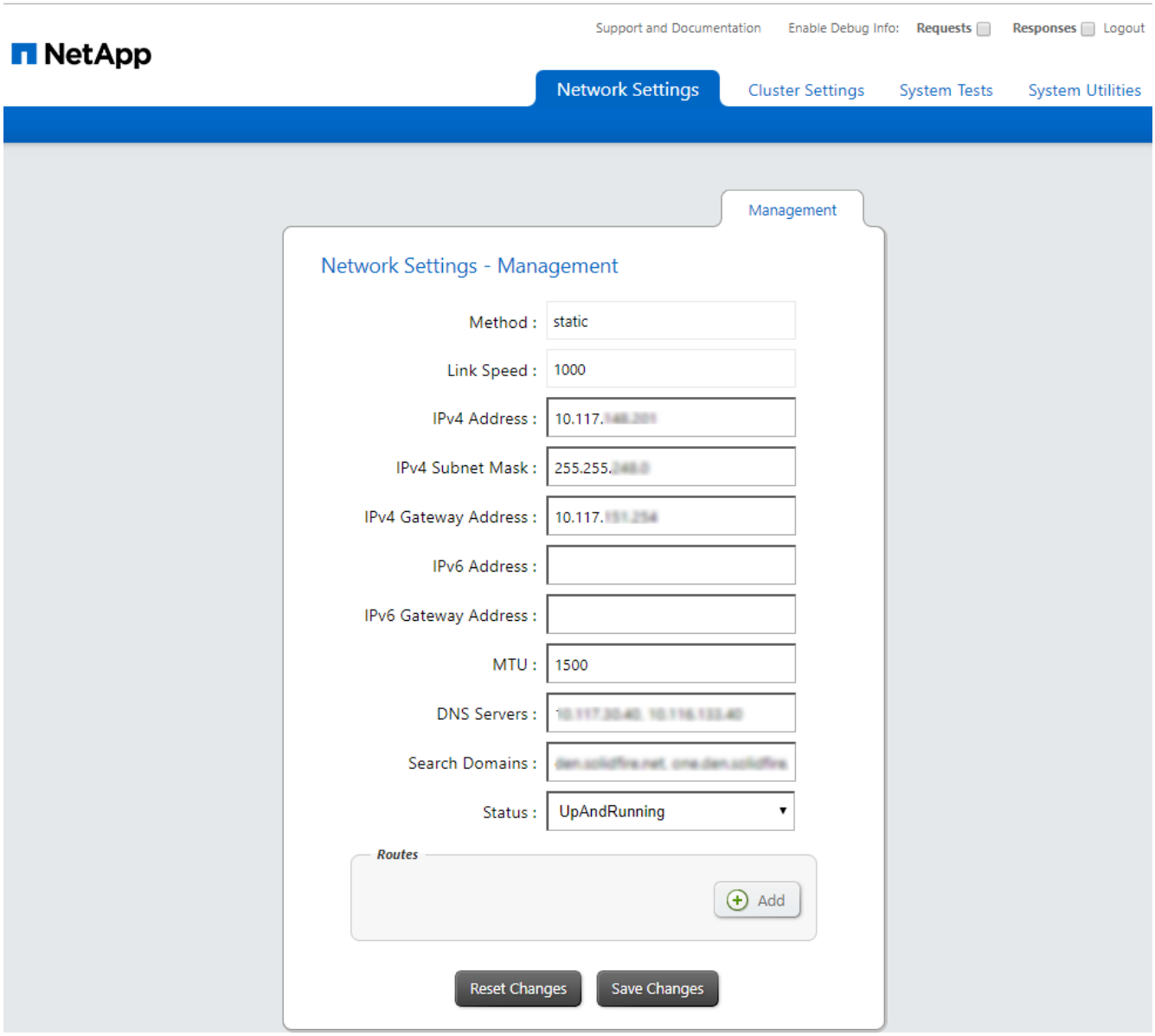
Access the management node per-node UI

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.

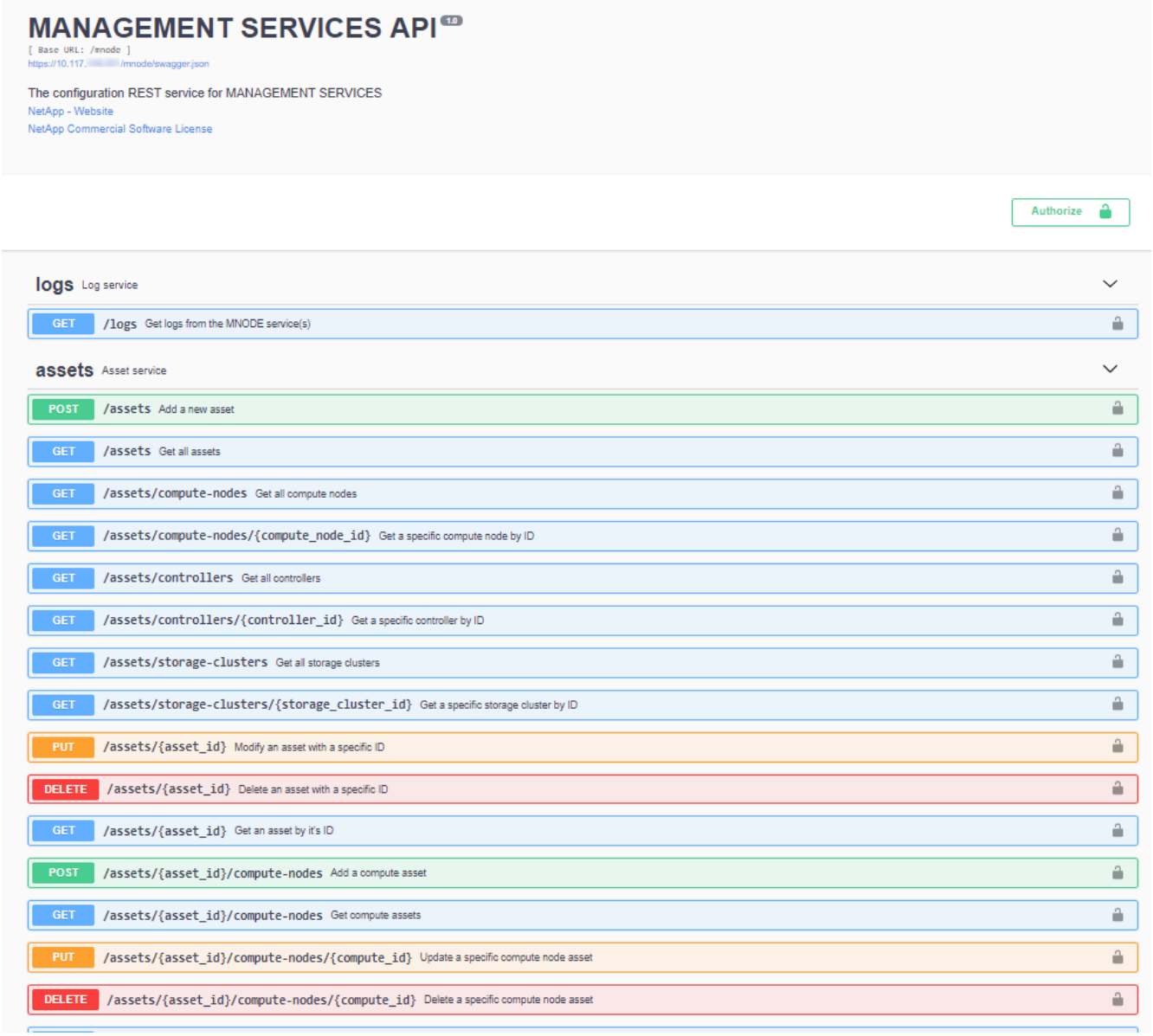
Access the management node REST API UI

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 HCI Documentation Center
- NetApp HCI Resources Page

Work with the management node UI

Management node UI overview

With the management node UI (`https://[management node IP]: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 HCI Documentation Center
- 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

options	Description
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`.
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 HCI Documentation Center
- 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://[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.

Tasks you can perform with REST APIs:

- Get authorization to use REST APIs
- Enable Active IQ and NetApp HCI monitoring
- Add compute and controller assets to the management node

- Change the storage cluster administrator password
- Configure a proxy server for the management node
- Use the REST API to collect NetApp HCI logs

Find more information

- Access the management node
- NetApp HCI Documentation Center
- 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. Open the REST API UI on the management node:

   ```
   https://[management node IP address]/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. Select **Request body** from the Type drop-down list.

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

   d. Do not enter a value for the client secret.

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

If the error message `Auth Error TypeError: Failed to fetch` is returned after you attempt to authorize, you might need to accept the SSL certificate for the MVIP of your cluster. Copy the IP in the Token URL, paste the IP into another browser tab, and authorize again.

The Available authorizations screen indicates **Authorized**.

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 HCI Documentation Center
- 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.

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 HCI Documentation Center
- NetApp HCI Resources Page

Enable remote NetApp Support connections

If you require technical support for your NetApp Element software-based storage system, NetApp Support can connect remotely with your system if you enable remote access. To 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

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 HCI Documentation Center
- NetApp HCI Resources Page