



# **Work with the management node**

## Element Software

NetApp  
April 17, 2024

This PDF was generated from [https://docs.netapp.com/us-en/element-software/mnode/task\\_mnode\\_work\\_overview.html](https://docs.netapp.com/us-en/element-software/mnode/task_mnode_work_overview.html) on April 17, 2024. Always check docs.netapp.com for the latest.

# Table of Contents

- Work with the management node . . . . . 1
  - Management node overview . . . . . 1
  - Install or recover a management node . . . . . 2
  - Access the management node . . . . . 20
  - Change the management node default SSL certificate . . . . . 22
  - Work with the management node UI . . . . . 23
  - Work with the management node REST API . . . . . 27
  - Manage support connections . . . . . 44

# 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.



As a best practice, only associate one management node with one VMware vCenter instance, and avoid defining the same storage and compute resources or vCenter instances in multiple management nodes.

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](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](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 \(UI or REST API\)](#)

Change the default SSL certificate:

- [Change the management node default SSL certificate](#)

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:

- [Accessing storage nodes using SSH for basic troubleshooting](#)
  - [Enable remote NetApp Support connections](#)
  - [Manage SSH functionality on the management node](#)

## Find more information

- [NetApp Element Plug-in for vCenter Server](#)
- [SolidFire and Element Software Documentation](#)

# 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 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 virtual machine (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

### Download ISO or OVA and deploy the VM

1. Download the OVA or ISO for your installation from the [Element Software](#) page on the NetApp Support Site.
  - a. Select **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 VM from your hypervisor with the following configuration:
    - Six virtual CPUs
    - 24GB RAM
    - Storage adapter type set to LSI Logic Parallel



The default for your management node might be LSI Logic SAS. In the **New Virtual Machine** window, verify the storage adapter configuration by selecting **Customize hardware > Virtual Hardware**. If required, change LSI Logic SAS to **LSI Logic Parallel**.

- 400GB virtual disk, thin provisioned
- One virtual network interface with internet access and access to the storage MVIP.
- (Optional) 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 VM prior to the step indicating to do so later in this procedure.

- b. Attach the ISO to the VM 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 VM 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. If there is a Dynamic Host Configuration Protocol (DHCP) server on the network that assigns IPs with a maximum transmission unit (MTU) less than 1500 bytes, you must perform the following steps:
  - a. Temporarily put the management node on a vSphere network without DHCP, such as iSCSI.
  - b. Reboot the VM or restart the VM network.
  - c. Using the TUI, configure the correct IP on the management network with an MTU greater than or equal to 1500 bytes.
  - d. Re-assign the correct VM network to the VM.



A DHCP that assigns IPs with an MTU less than 1500 bytes can prevent you configuring the management node network or using the management node UI.

3. 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:



Starting with Element 12.3.1, substeps (a) to (e) are performed automatically. For management node 12.3.1, proceed to [substep \(f\)](#) to complete the time sync configuration.

- 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.



Do not edit the NTP after you complete the time sync configuration because it affects the NTP when you run the [setup command](#) on the management node.

## 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.

```
sudo /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://<ManagementNodeIP>/inventory/1/
```

- d. Select **Authorize** and complete the following:
  - i. Enter the cluster user name and password.
  - ii. Enter the client ID as `mnode-client`.
  - iii. Select **Authorize** to begin a session.
- e. From the REST API UI, select **GET /installations**.
- f. Select **Try it out**.
- g. Select **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. Add a vCenter controller asset for NetApp Hybrid Cloud Control 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://<ManagementNodeIP>/mnode
```

- b. Select **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. Select **Authorize** to begin a session.
  - iv. Close the window.
- c. Select **POST /assets/{asset\_id}/controllers** to add a controller sub-asset.



You should create a new NetApp HCC role in vCenter to add a controller sub-asset. This new NetApp HCC role will limit the management node services view to NetApp-only assets. See [Create a NetApp HCC role in vCenter](#).

- d. Select **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. Select **Execute**.

## Find more Information

- [Persistent volumes](#)
- [Add a controller asset to the management node](#)
- [Configure a storage NIC](#)
- [NetApp Element Plug-in for vCenter Server](#)
- [SolidFire and Element Software Documentation](#)

## Create a NetApp HCC role in vCenter

You should create a NetApp HCC role in vCenter to manually add vCenter assets (controllers) to the management node post installation or to modify existing controllers.

This NetApp HCC role limits your management node services view to NetApp-only assets.

### About this task

- This procedure describes the steps available in version 6.7 of vSphere. Your vSphere user interface might differ slightly from what is described depending on the version of vSphere installed. For additional help, see VMware vCenter documentation.
- To [create a new NetApp HCC role](#), you first set up a new user account in vCenter, create a NetApp HCC role, and then assign the user permissions.
- For NetApp ESXi host configurations, you should update the NDE-created user account to the new NetApp HCC role:
  - Use [this option](#) if your NetApp ESXi host does not exist inside a vCenter host cluster
  - Use [this option](#) if your NetApp ESXi host exists inside a vCenter host cluster
- You can [configure a controller asset](#) that already exists on the management node.
- Use the new NetApp HCC role to [add an asset](#) to the management node.

## Create a new NetApp HCC role

Set up a new user account in vCenter, create a NetApp HCC role, and then assign the user permissions.

### Set up a new user account in vCenter

Perform the following steps to set up a new user account in vCenter.

### Steps

1. Log into the vSphere Web Client as `administrator@vsphere.local` or equivalent.
2. From the Menu, select **Administration**.
3. In the **Single Sign On** section, select **Users and Groups**.
4. In the **Domain** list, select `vsphere.local` or your LDAP domain.

5. Select **Add User**.
6. Complete the **Add User** form.

### Create a new NetApp HCC role in vCenter

Perform the following steps to create a new NetApp HCC role in vCenter.

#### Steps

1. Select **Edit Role**, and assign the required permissions.
2. In the left navigation pane, select **Global**.
3. Select **Diagnostics** and **Licenses**.
4. In the left navigation pane, select **Hosts**.
5. Select **Maintenance**, **Power**, **Storage partition configuration**, and **Firmware**.
6. Save as NetApp Role.

### Assign user permissions to vCenter

Perform the following steps to assign the user permissions to the new NetApp HCC role in vCenter.

#### Steps

1. From the Menu, select **Hosts** and **Clusters**.
2. In the left navigation pane, select one of the following options:
  - The top level vCenter.
  - Your desired vCenter if you are in linked mode.



- Beginning with NetApp Element Plug-in for vCenter Server 5.0, to use [vCenter Linked Mode](#), you register the Element Plug-in from a separate management node for each vCenter Server that manages NetApp SolidFire storage clusters (recommended).
- Using NetApp Element Plug-in for vCenter Server 4.10 and earlier to manage cluster resources from other vCenter Servers using [vCenter Linked Mode](#) is limited to local storage clusters only.

3. In the right navigation pane, select **Permissions**.
4. Select the **+** icon to add the new user.

Add the following details in the **Add permission** window:

- a. Select `vsphere.local` or your LDAP domain
- b. Use the search to find the new user that you created in [Set up a new user account in vCenter](#).
- c. Select NetApp Role.



Do **NOT** select **Propagate to children**.

## Add Permission | satyabra-vccenter01.mgmt.ict.openengla... X

User: vsphere.local

Q netapp

Role: NetApp Role

☐ Propagate to children

CANCEL OK

### Assign user permissions to the datacenter

Perform the following steps to assign the user permissions to the datacenter in vCenter.

#### Steps

1. In the left pane, select **Datacenter**.
2. In the right navigation pane, select **Permissions**.
3. Select the + icon to add the new user.

Add the following details in the **Add permission** window:

- a. Select `vsphere.local` or your LDAP domain.
- b. Use the search to find the new HCC user that you created in [Set up a new user account in vCenter](#).
- c. Select `ReadOnly` role.



Do **NOT** select **Propagate to children**.

### Assign user permissions to NetApp HCI datastores

Perform the following steps to assign the user permissions to the NetApp HCI datastores in vCenter.

#### Steps

1. In the left pane, select **Datacenter**.
2. Create a new storage folder. Right-click on **Datacenter** and select **Create storage folder**.
3. Transfer all the NetApp HCI datastores from the storage cluster and local to the compute node to the new

storage folder.

4. Select the new storage folder.
5. In the right navigation pane, select **Permissions**.
6. Select the **+** icon to add the new user.

Add the following details in the **Add permission** window:

- a. Select `vsphere.local` or your LDAP domain.
- b. Use the search to find the new HCC user that you created in [Set up a new user account in vCenter](#).
- c. Select `Administrator` role
- d. Select **Propagate to children**.

### Assign user permissions to a NetApp host cluster

Perform the following steps to assign the user permissions to a NetApp host cluster in vCenter.

#### Steps

1. In the left navigation pane, select the NetApp host cluster.
2. In the right navigation pane, select **Permissions**.
3. Select the **+** icon to add the new user.

Add the following details in the **Add permission** window:

- a. Select `vsphere.local` or your LDAP domain.
- b. Use the search to find the new HCC user that you created in [Set up a new user account in vCenter](#).
- c. Select `NetApp Role or Administrator`.
- d. Select **Propagate to children**.

### NetApp ESXi host configurations

For NetApp ESXi host configurations, you should update the NDE-created user account to the new NetApp HCC role.

#### NetApp ESXi host does not exist in a vCenter host cluster

If the NetApp ESXi host does not exist inside a vCenter host cluster, you can use the following procedure to assign the NetApp HCC role and user permissions in vCenter.

#### Steps

1. From the Menu, select **Hosts** and **Clusters**.
2. In the left navigation pane, select the NetApp ESXi host.
3. In the right navigation pane, select **Permissions**.
4. Select the **+** icon to add the new user.

Add the following details in the **Add permission** window:

- a. Select `vsphere.local` or your LDAP domain.

- b. Use the search to find the new user that you created in [Set up a new user account in vCenter](#).
  - c. Select `NetApp Role or Administrator`.
5. Select **Propagate to children**.

#### NetApp ESXi host exists in a vCenter host cluster

If a NetApp ESXi host exists inside a vCenter host cluster with other vendor ESXi hosts, you can use the following procedure to assign the NetApp HCC role and user permissions in vCenter.

1. From the Menu, select **Hosts** and **Clusters**.
2. In the left navigation pane, expand the desired host cluster.
3. In the right navigation pane, select **Permissions**.
4. Select the **+** icon to add the new user.

Add the following details in the **Add permission** window:

- a. Select `vsphere.local` or your LDAP domain.
- b. Use the search to find the new user that you created in [Set up a new user account in vCenter](#).
- c. Select `NetApp Role`.



Do **NOT** select **Propagate to children**.

5. In the left navigation pane, select a NetApp ESXi host.
6. In the right navigation pane, select **Permissions**.
7. Select the **+** icon to add the new user.

Add the following details in the **Add permission** window:

- a. Select `vsphere.local` or your LDAP domain.
  - b. Use the search to find the new user that you created in [Set up a new user account in vCenter](#).
  - c. Select `NetApp Role or Administrator`.
  - d. Select **Propagate to children**.
8. Repeat for remaining NetApp ESXi hosts in the host cluster.

#### Controller asset already exists on the management node

If a controller asset already exists on the management node, perform the following steps to configure the controller by using `PUT /assets /{asset_id} /controllers /{controller_id}`.

#### Steps

1. Access the mnode service API UI on the management node:

<https://<ManagementNodeIP>/mnode>

2. Select **Authorize** and enter the credentials to access the API calls.
3. Select `GET /assets` to get the parent ID.

4. Select `PUT /assets /{asset_id} /controllers /{controller_id}`.

- a. Enter the credentials created in account setup in the request body.

### Add an asset to the management node

If you need to manually add a new asset post installation, use the new HCC user account that you created in [Set up a new user account in vCenter](#). For more information, see [Add a controller asset to the management node](#).

### Find more information

- [NetApp Element Plug-in for vCenter Server](#)
- [SolidFire and Element Software Documentation](#)

## 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 a controller asset to the management node](#)
- [NetApp Element Plug-in for vCenter Server](#)
- [SolidFire and Element Software Documentation](#)

## 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 [Element software](#) page on the NetApp Support Site.
  - a. Select **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:



Beginning with Element 12.3.1, substeps (a) to (e) are performed automatically. For management node 12.3.1 or later, proceed to [substep \(f\)](#) to complete the time sync configuration.

- 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.



Do not edit the NTP after you complete the time sync configuration because it affects the NTP when you run the [redeploy command](#) on the management node.

## 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.

```
sudo /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 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](#).



SSH capability that provides [NetApp Support remote support tunnel \(RST\) session access](#) is disabled by default on management nodes running management services 2.18 and later. If you had previously enabled SSH functionality on the management node, you might need to [disable SSH again](#) on the recovered management node.

### Find more Information

- [Persistent volumes](#)
- [NetApp Element Plug-in for vCenter Server](#)
- [SolidFire and Element Software Documentation](#)

## 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
```

Management

### Network Settings - Management

Method :

static

Link Speed :

1000

IPv4 Address :

10.117.148.201

IPv4 Subnet Mask :

255.255.255.0

IPv4 Gateway Address :

10.117.151.254

IPv6 Address :

IPv6 Gateway Address :

MTU :

1500

DNS Servers :

10.117.20.40, 10.116.133.40

Search Domains :

den.scoloffine.net, one.den.scoloffine

Status :

UpAndRunning

Routes

+ Add

Reset Changes

Save Changes

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
```

## MANAGEMENT SERVICES API <sup>4.0</sup>

[ Base URL: /mnode ]  
<https://10.117.1.100/mnode/swagger/json>

The configuration REST service for MANAGEMENT SERVICES

[NetApp - Website](#)

[NetApp Commercial Software License](#)

Authorize 

### logs Log service

GET /logs Get logs from the MNODE service(s)

### assets Asset service

POST /assets Add a new asset

GET /assets Get all assets

GET /assets/compute-nodes Get all compute nodes

GET /assets/compute-nodes/{compute\_node\_id} Get a specific compute node by ID

GET /assets/controllers Get all controllers

GET /assets/controllers/{controller\_id} Get a specific controller by ID

GET /assets/storage-clusters Get all storage clusters

GET /assets/storage-clusters/{storage\_cluster\_id} Get a specific storage cluster by ID

PUT /assets/{asset\_id} Modify an asset with a specific ID

DELETE /assets/{asset\_id} Delete an asset with a specific ID

GET /assets/{asset\_id} Get an asset by it's ID

POST /assets/{asset\_id}/compute-nodes Add a compute asset

GET /assets/{asset\_id}/compute-nodes Get compute assets

PUT /assets/{asset\_id}/compute-nodes/{compute\_id} Update a specific compute node asset

DELETE /assets/{asset\_id}/compute-nodes/{compute\_id} Delete a specific compute node asset

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

## Find more Information

- [Enable Active IQ and NetApp monitoring](#)
- [NetApp Element Plug-in for vCenter Server](#)
- [SolidFire and Element Software Documentation](#)

## Change the management node default SSL certificate

You can change the default SSL certificate and private key of the management node using the NetApp Element API.

When you configure a management node, it creates a unique self-signed Secure Sockets Layer (SSL) certificate and private key that is used for all HTTPS communication by way of the the Element UI, per-node UI, or APIs. Element software supports self-signed certificates as well as certificates that are issued and verified by a trusted Certificate Authority (CA).



You can use the following API methods to get more information about the default SSL certificate and make changes.

- **GetNodeSSLCertificate**

You can use the [GetNodeSSLCertificate method](#) to retrieve information about the currently installed SSL certificate including all certificate details.

- **SetNodeSSLCertificate**

You can use the [SetNodeSSLCertificate method](#) to set the cluster and per-node SSL certificates to the certificate and private key you supply. The system validates the certificate and private key to prevent an invalid certificate from being applied.

- **RemoveNodeSSLCertificate**

This [RemoveNodeSSLCertificate method](#) removes the currently installed SSL certificate and private key. The cluster then generates a new self-signed certificate and private key.

## Find more information

- [Change the Element software default SSL certificate](#)
- [What are the requirements around setting custom SSL certificates in Element Software?](#)
- [SolidFire and Element Software Documentation](#)
- [NetApp Element Plug-in for vCenter Server](#)

## 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](#)
- [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](#)
- [SolidFire and Element Software Documentation](#)

### Configure alert monitoring

The alert monitoring tools are configured for NetApp HCI alert monitoring. These tools are not configured or used for 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
```

For more information on configuring alert monitoring for NetApp HCI, see [Configure alert monitoring](#)

## Modify and test the management node network, cluster, and system settings

You can modify and test the management node network, cluster, and system settings.

- [Update management node network settings](#)
- [Update management node cluster settings](#)
- [Test the management node settings](#)

### Update management node network settings

On the Network Settings tab of the per-node management node UI, you can modify the management node network interface fields.

1. Open the per-node management node UI.
2. Select the **Network Settings** tab.
3. View or enter the following information:
  - a. **Method:** Choose one of the following methods to configure the interface:
    - **loopback:** Use to define the IPv4 loopback interface.
    - **manual:** Use to define interfaces for which no configuration is done by default.
    - **dhcp:** Use to obtain an IP address via DHCP.
    - **static:** Use to define Ethernet interfaces with statically allocated IPv4 addresses.
  - b. **Link Speed:** The speed negotiated by the virtual NIC.
  - c. **IPv4 Address:** The IPv4 address for the eth0 network.
  - d. **IPv4 Subnet Mask:** Address subdivisions of the IPv4 network.
  - e. **IPv4 Gateway Address:** Router network address to send packets out of the local network.
  - f. **IPv6 Address:** The IPv6 address for the eth0 network.
  - g. **IPv6 Gateway Address:** Router network address to send packets out of the local network.



The IPv6 options are not supported for 11.3 or later versions of the management node.

- h. **MTU:** Largest packet size that a network protocol can transmit. Must be greater than or equal to 1500. If you add a second storage NIC, the value should be 9000.
- i. **DNS Servers:** Network interface used for cluster communication.
- j. **Search Domains:** Search for additional MAC addresses available to the system.
- k. **Status:** Possible values:
  - UpAndRunning
  - Down

- Up
- l. **Routes:** Static routes to specific hosts or networks via the associated interface the routes are configured to use.

## Update management node cluster settings

On the Cluster Settings tab of the per-node UI for the management node, you can modify cluster interface fields when a node is in Available, Pending, PendingActive, and Active states.

1. Open the per-node management node UI.
2. Select the **Cluster Settings** tab.
3. View or enter the following information:
  - **Role:** Role the management node has in the cluster. Possible value: Management.
  - **Version:** Element software version running on the cluster.
  - **Default Interface:** Default network interface used for management node communication with the cluster running Element software.

## Test the management node settings

After you change management and network settings for the management node and commit the changes, you can run tests to validate the changes you made.

1. Open the per-node management node UI.
2. In the management node UI, select **System Tests**.
3. Complete any of the following:
  - a. To verify that the network settings you configured are valid for the system, select **Test Network Config**.
  - b. To test network connectivity to all nodes in the cluster on both 1G and 10G interfaces using ICMP packets, select **Test Ping**.
4. View or enter the following:
  - **Hosts:** Specify a comma-separated list of addresses or host names of devices to ping.
  - **Attempts:** Specify the number of times the system should repeat the test ping. Default: 5.
  - **Packet Size:** Specify the number of bytes to send in the ICMP packet that is sent to each IP. The number of bytes must be less than the maximum MTU specified in the network configuration.
  - **Timeout mSec:** Specify the number of milliseconds to wait for each individual ping response. Default: 500 ms.
  - **Total Timeout Sec:** Specify the time in seconds the ping should wait for a system response before issuing the next ping attempt or ending the process. Default: 5.
  - **Prohibit Fragmentation:** Enable the DF (do not fragment) flag for the ICMP packets.

## Find more Information

- [NetApp Element Plug-in for vCenter Server](#)
- [SolidFire and Element Software Documentation](#)

## Run system utilities from the management node

You can use the per-node UI for the management node to create or delete cluster support bundles, reset node configuration settings, or restart networking.

### Steps

1. Open the per-node management node UI using the management node admin credentials.
2. Select **System Utilities**.
3. Select the button for the utility that you want to run:
  - a. **Control Power**: Reboots, power cycles, or shuts down the node. Specify any of the following options.



This operation causes temporary loss of networking connectivity.

- **Action**: Options include `Restart` and `Halt` (power off).
  - **Wakeup Delay**: Any additional time before the node comes back online.
- b. **Create Cluster Support Bundle**: Creates the cluster support bundle to assist NetApp Support diagnostic evaluations of one or more nodes in a cluster. Specify the following options:
    - **Bundle Name**: Unique name for each support bundle created. If no name is provided, then "supportbundle" and the node name are used as the file name.
    - **Mvip**: The MVIP of the cluster. Bundles are gathered from all nodes in the cluster. This parameter is required if the `Nodes` parameter is not specified.
    - **Nodes**: The IP addresses of the nodes from which to gather bundles. Use either `Nodes` or `Mvip`, but not both, to specify the nodes from which to gather bundles. This parameter is required if `Mvip` is not specified.
    - **Username**: The cluster admin user name.
    - **Password**: The cluster admin password.
    - **Allow Incomplete**: Allows the script to continue to run if bundles cannot be gathered from one or more of the nodes.
    - **Extra Args**: This parameter is fed to the `sf_make_support_bundle` script. This parameter should be used only at the request of NetApp Support.
  - c. **Delete All Support Bundles**: Deletes any current support bundles on the management node.
  - d. **Reset Node**: Resets the management node to a new install image. This changes all settings except the network configuration to the default state. Specify the following options:
    - **Build**: The URL to a remote Element software image to which the node will be reset.
    - **Options**: Specifications for running the reset operations. Details are be provided by NetApp Support, if required.



This operation causes temporary loss of networking connectivity.

- e. **Restart Networking**: Restarts all networking services on the management node.



This operation causes temporary loss of networking connectivity.

### Find more Information

- [NetApp Element Plug-in for vCenter Server](#)
- [SolidFire and Element Software Documentation](#)

## 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 monitoring](#)
- [Configure a proxy server for the management node](#)
- [Configure NetApp Hybrid Cloud Control for multiple vCenters](#)
- [Add a controller asset to the management node](#)
- [Create and manage storage cluster assets](#)

#### Asset management

- [View or edit existing controller assets](#)
- [Create and manage storage cluster assets](#)
- [Use the REST API to collect Element system 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](#)
- [SolidFire and Element Software Documentation](#)

### 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.

### API command

```
TOKEN=`curl -k -X POST https://MVIP/auth/connect/token -F client_id=mnode-client -F grant_type=password -F username=CLUSTER_ADMIN -F password=CLUSTER_PASSWORD|awk -F': ' '{print $2}'|awk -F',' '{print $1}'|sed s/\"//g`
```

### REST API UI 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. Select **Authorize**.



Alternately, you can select 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. Select **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](#)
- [SolidFire and Element Software Documentation](#)

## Enable Active IQ and NetApp monitoring

You can enable Active IQ storage monitoring if you did not already do so during installation or upgrade. You might need to use this procedure if you did not set up SolidFire Active IQ during installation for a SolidFire all-flash storage system.

The Active IQ collector service forwards configuration data and Element software-based cluster performance metrics to SolidFire Active IQ for historical reporting and near real-time performance monitoring. The NetApp monitoring service enables forwarding of storage cluster faults to vCenter for alert notification.

### Before you begin

- Some functions in Active IQ, for example, quality of service (QoS), require Element 11.3 or later to work correctly. To confirm that you have the capability to use all Active IQ functions, NetApp recommends the following:
  - Your storage cluster is running NetApp Element software 11.3 or later.
  - You have deployed a management node running version 11.3 or later.
- You have internet access. The Active IQ collector service cannot be used from dark sites that do not have external connectivity.

### Steps

1. Get the base asset ID for the installation:
  - a. Open the inventory service REST API UI on the management node:

```
https://<ManagementNodeIP>/inventory/1/
```

- b. Select **Authorize** and complete the following:
  - i. Enter the cluster user name and password.
  - ii. Enter the client ID as `mnode-client`.
  - iii. Select **Authorize** to begin a session.
  - iv. Close the window.
- c. From the REST API UI, select **GET /installations**.
- d. Select **Try it out**.
- e. Select **Execute**.
- f. From the code 200 response body, copy the `id` for the installation.

```
{
  "installations": [
    {
      "_links": {
        "collection":
"https://10.111.211.111/inventory/1/installations",
        "self":
"https://10.111.217.111/inventory/1/installations/abcd01e2-ab00-1xxx-91ee-12f111xxc7x0x"
      },
      "id": "abcd01e2-ab00-1xxx-91ee-12f111xxc7x0x",
    }
  ]
}
```



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

## 2. Activate telemetry:

- a. Access the mnode service API UI on the management node by entering the management node IP address followed by `/mnode`:

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

- b. Select **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. Select **Authorize** to begin a session.
- iv. Close the window.

- c. Configure the base asset:

- i. Select **PUT /assets/{asset\_id}**.
- ii. Select **Try it out**.
- iii. Enter the following in the JSON payload:

```
{
  "telemetry_active": true
  "config": {}
}
```

- iv. Enter the base ID from the previous step in **asset\_ID**.
- v. Select **Execute**.

The Active IQ service is automatically restarted whenever assets are changed. Modifying assets results in a short delay before settings are applied.

3. If you have not already done so, add a vCenter controller asset for NetApp Hybrid Cloud Control to the management node known assets:



A controller asset is required for NetApp monitoring services.

- a. Select **POST /assets/{asset\_id}/controllers** to add a controller sub-asset.
- b. Select **Try it out**.
- c. Enter the parent base asset ID you copied to your clipboard in the **asset\_id** field.
- d. Enter the required payload values with `type` as `vCenter` and vCenter credentials.



```
{
  "username": "string",
  "password": "string",
  "ip": "string",
  "type": "vCenter",
  "host_name": "string",
  "config": {}
}
```



ip is the vCenter IP address.

e. Select **Execute**.

### Find more information

- [NetApp Element Plug-in for vCenter Server](#)
- [SolidFire and Element Software Documentation](#)

## Configure NetApp Hybrid Cloud Control for multiple vCenters

You can configure NetApp Hybrid Cloud Control to manage assets from two or more vCenters that are not using Linked Mode.

You should use this process after your initial installation when you need to add assets for a recently scaled installation or when new assets were not added automatically to your configuration. Use these APIs to add assets that are recent additions to your installation.

### 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. [Add new vCenters as controller assets](#) to the management node configuration.
2. Refresh the inventory service API on the management node:

```
https://<ManagementNodeIP>/inventory/1/
```



As an alternative, you can wait 2 minutes for the inventory to update in NetApp Hybrid Cloud Control UI.

- a. Select **Authorize** and complete the following:
  - i. Enter the cluster user name and password.
  - ii. Enter the client ID as `mnode-client`.
  - iii. Select **Authorize** to begin a session.

- iv. Close the window.
  - b. From the REST API UI, select **GET /installations**.
  - c. Select **Try it out**.
  - d. Select **Execute**.
  - e. From the response, copy the installation asset ID ("id").
  - f. From the REST API UI, select **GET /installations/{id}**.
  - g. Select **Try it out**.
  - h. Set refresh to `True`.
  - i. Paste the installation asset ID into the `id` field.
  - j. Select **Execute**.
3. Refresh the NetApp Hybrid Cloud Control browser to see the changes.

### Find more information

- [NetApp Element Plug-in for vCenter Server](#)
- [SolidFire and Element Software Documentation](#)

## Add a controller asset to the management node

You can add a controller asset to the management node configuration using the REST API UI.

You might need to add an asset if you recently scaled your installation and new assets were not added automatically to your configuration. Use these APIs to add assets that are recent additions to your installation.

### 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.
- You have created a new NetApp HCC role in vCenter to limit the management node services view to NetApp-only assets. See [Create a NetApp HCC role in vCenter](#)

### Steps

1. Get the base asset ID for the installation:
  - a. Open the inventory service REST API UI on the management node:

```
https://<ManagementNodeIP>/inventory/1/
```

- b. Select **Authorize** and complete the following:
    - i. Enter the cluster user name and password.
    - ii. Enter the client ID as `mnode-client`.
    - iii. Select **Authorize** to begin a session.
    - iv. Close the window.

- c. From the REST API UI, select **GET /installations**.
- d. Select **Try it out**.
- e. Select **Execute**.
- f. From the code 200 response body, copy the `id` for the installation.

```
{
  "installations": [
    {
      "_links": {
        "collection":
"https://10.111.211.111/inventory/1/installations",
        "self":
"https://10.111.217.111/inventory/1/installations/abcd01e2-ab00-1xxx-
91ee-12f111xxc7x0x"
      },
      "id": "abcd01e2-ab00-1xxx-91ee-12f111xxc7x0x",
    }
  ]
}
```



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

- g. From the REST API UI, select **GET /installations/{id}**.
  - h. Select **Try it out**.
  - i. Paste the installation asset ID into the `id` field.
  - j. Select **Execute**.
  - k. From the response, copy and save the cluster controller ID (`"controllerId"`) for use in a later step.
2. To add a controller sub-asset to an existing base asset, select:

```
POST /assets/{asset_id}/controllers
```

- a. Open the mNode service REST API UI on the management node:

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

- b. Select **Authorize** and complete the following:
  - i. Enter the cluster user name and password.
  - ii. Enter the client ID as `mnode-client`.
  - iii. Select **Authorize** to begin a session.
  - iv. Close the window.
- c. Select **POST /assets/{asset\_id}/controllers**.
- d. Select **Try it out**.

- e. Enter the parent base asset ID in the **asset\_id** field.
- f. Add the required values to the payload.
- g. Select **Execute**.

### Find more information

- [NetApp Element Plug-in for vCenter Server](#)
- [SolidFire and Element Software Documentation](#)

## 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://<ManagementNodeIP>/inventory/1/
```

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`.
  - c. Select **Authorize** to begin a session.
  - d. Close the window.
3. Select **GET /installations**.
4. Select **Try it out**.

5. Select **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-sf-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://<ManagementNodeIP>/storage/1/
```

8. Select **Authorize** or any lock icon and complete the following:

- Enter the cluster user name and password.
- Enter the client ID as `mnode-client`.
- Select **Authorize** to begin a session.
- Close the window.

9. Select **GET /clusters**.

10. Select **Try it out**.

11. Enter the installation ID you saved earlier into the `installationId` parameter.

12. Select **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 NetApp 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://<ManagementNodeIP>/storage/1/
```

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`.
  - c. Select **Authorize** to begin a session.
  - d. Close the window.
3. Select **POST /clusters**.
4. Select **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.
password	string	The password used to communicate with the storage cluster.

Parameter	Type	Description
userId	string	The user ID used to communicate with the storage cluster (the user must have administrator privileges).

6. Select **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://<ManagementNodeIP>/storage/1/
```

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`.
  - c. Select **Authorize** to begin a session.
  - d. Close the window.
3. Select **PUT /clusters/{storageId}**.
4. Select **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. Select **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://<ManagementNodeIP>/storage/1/
```

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`.
  - c. Select **Authorize** to begin a session.
  - d. Close the window.
3. Select **DELETE /clusters/{storageId}**.
4. Select **Try it out**.
5. Enter the storage cluster ID you copied earlier in the `storageId` parameter.
6. Select **Execute**.

Upon success, the API returns an empty response.

### Find more information

- [Authoritative cluster](#)
- [NetApp Element Plug-in for vCenter Server](#)
- [SolidFire and Element Software Documentation](#)



## View or edit existing controller assets

You can view information about and edit existing VMware vCenter controllers in the management node configuration using the REST API. Controllers are VMware vCenter instances registered to the management node for your NetApp SolidFire installation.

### Before you begin

- 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.

## Access the management services REST API

### Steps

1. Access the REST API UI for management services by entering the management node IP address followed by `/vcenter/1/`:

```
https://<ManagementNodeIP>/vcenter/1/
```

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`.
  - c. Select **Authorize** to begin a session.
  - d. Close the window.

## View stored information about existing controllers

You can list existing vCenter controllers that are registered with the management node and view stored information about them using the REST API.

### Steps

1. Select **GET /compute/controllers**.
2. Select **Try it out**.
3. Select **Execute**.

The API returns a list of all known vCenter controllers, along with the IP address, controller ID, hostname, and user ID used to communicate with each controller.

4. If you want the connection status of a particular controller, copy the controller ID from the `id` field of that controller to your clipboard and see [View the status of an existing controller](#).

## View the status of an existing controller

You can view the status of any of the existing vCenter controllers registered with the management node. The API returns a status indicating whether NetApp Hybrid Cloud Control can connect with the vCenter controller as well as the reason for that status.

### Steps

1. Select **GET** `/compute/controllers/{controller_id}/status`.
2. Select **Try it out**.
3. Enter the controller ID you copied earlier in the `controller_id` parameter.
4. Select **Execute**.

The API returns a status of this particular vCenter controller, along with a reason for that status.

### Edit the stored properties of a controller

You can edit the stored user name or password for any of the existing vCenter controllers registered with the management node. You cannot edit the stored IP address of an existing vCenter controller.

#### Steps

1. Select **PUT** `/compute/controllers/{controller_id}`.
2. Enter the controller ID of a vCenter controller in the `controller_id` parameter.
3. Select **Try it out**.
4. Change either of the following parameters in the **Request body** field:

Parameter	Type	Description
<code>userId</code>	string	Change the user ID used to communicate with the vCenter controller (the user must have administrator privileges).
<code>password</code>	string	Change the password used to communicate with the vCenter controller.

5. Select **Execute**.

The API returns updated controller information.

### Find more information

- [Add a controller asset to the management node](#)
- [NetApp Element Plug-in for vCenter Server](#)
- [SolidFire and Element Software Documentation](#)

### 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 monitoring service, 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://<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`.
  - c. Select **Authorize** to begin a session.
  - d. Close the window.
3. Select **PUT /settings**.
4. Select **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. Select **Execute**.



You might need to reboot your management node depending on your environment.

### Find more information

- [NetApp Element Plug-in for vCenter Server](#)
- [SolidFire and Element Software Documentation](#)

## 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: ${TOKEN}"
```



You can find the bearer `${TOKEN}` used by the API command when you [authorize](#). The bearer `${TOKEN}` is in 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](#)
- [SolidFire and Element Software Documentation](#)

## 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.
  - Beginning with management services 2.21.61:


```
https://<ManagementNodeIP>/mnode/4/
```

- For management services 2.20.69 or earlier:


```
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**.
7. From the response body, select **Download** to save the log output.

### Find more Information

- [NetApp Element Plug-in for vCenter Server](#)
- [SolidFire and Element Software Documentation](#)

## Manage support connections

### Accessing storage nodes using SSH for basic troubleshooting

Beginning with Element 12.5, you can use the `sfireadonly` system account on the storage nodes for basic troubleshooting. You can also enable and open remote support tunnel access for NetApp Support for advanced troubleshooting.

The `sfireadonly` system account enables access to run basic Linux system and network troubleshooting commands, including `ping`.



Unless advised by NetApp Support, any alterations to this system are unsupported, voiding your support contract, and might result in instability or inaccessibility of data.

### Before you begin

- **Write permissions**: Verify that you have write permissions to the current working directory.
- **(Optional) Generate your own key pair**: Run `ssh-keygen` from Windows 10, MacOS, or Linux distribution. This is a one-time action to create a user key pair and can be reused for future troubleshooting

sessions. You might want to use certificates associated with employee accounts, which would also work in this model.

- **Enable SSH capability on the management node:** To enable remote access functionality on the management node, see [this topic](#). For management services 2.18 and later, the capability for remote access is disabled on the management node by default.
- **Enable SSH capability on the storage cluster:** To enable remote access functionality on the storage cluster nodes, see [this topic](#).
- **Firewall configuration:** 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

## Troubleshooting options

- [Troubleshoot a cluster node](#)
- [Troubleshoot a cluster node with NetApp Support](#)
- [Troubleshoot a node that is not part of cluster](#)

## Troubleshoot a cluster node

You can perform basic troubleshooting using the `sfireadonly` system account:

### Steps

1. SSH to the management node using your account login credentials you selected when installing the management node VM.
2. On the management node, go to `/sf/bin`.
3. Find the appropriate script for your system:
  - `SignSshKeys.ps1`
  - `SignSshKeys.py`
  - `SignSshKeys.sh`



`SignSshKeys.ps1` is dependent on PowerShell 7 or later and `SignSshKeys.py` is dependent on Python 3.6.0 or later and the [requests module](#).

The `SignSshKeys` script writes `user`, `user.pub`, and `user-cert.pub` files into the current working directory, which are later used by the `ssh` command. However, when a public key file is provided to the script, only a `<public_key>` file (with `<public_key>` replaced with the prefix of the public key file passed into the script) is written out to the directory.

4. Run the script on the management node to generate the SSH keychain. The script enables SSH access using the `sfireadonly` system account across all nodes in the cluster.

```
SignSshKeys --ip [ip address] --user [username] --duration [hours]
--publickey [public key path]
```

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



You can use either the abbreviated or full form parameter.

- **--ip | -i [ip address]**: IP address of the target node for the API to run against.
- **--user | -u [username]**: Cluster user used to run the API call.
- **(Optional) --duration | -d [hours]**: The duration a signed key should remain valid as an integer in hours. The default is 24 hours.
- **(Optional) --publickey | -k [public key path]**: The path to a public key, if the user chooses to provide one.

b. Compare your input against the following sample command. In this example, 10.116.139.195 is the IP of the storage node, admin is the cluster username, and the duration of key validity is two hours:

```
sh /sf/bin/SignSshKeys.sh --ip 10.116.139.195 --user admin --duration
2
```

c. Run the command.

5. SSH to the node IPs:

```
ssh -i user sfreadonly@[node_ip]
```

You will be able to run basic Linux system and network troubleshooting commands, such as ping, and other read-only commands.

6. (Optional) Disable [remote access functionality](#) again after troubleshooting is complete.



SSH remains enabled on the management node if you do not disable it. SSH enabled configuration persists on the management node through updates and upgrades until it is manually disabled.

## Troubleshoot a cluster node with NetApp Support

NetApp Support can perform advanced troubleshooting with a system account that allows a technician to run deeper Element diagnostics.

### Steps

1. SSH to the management node using your account login credentials you selected when installing the management node VM.
2. Run the rst command with the port number sent by NetApp Support to open the support tunnel:

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



NetApp Support will log in to your management node using the support tunnel.

3. On the management node, go to `/sf/bin`.
4. Find the appropriate script for your system:
  - `SignSshKeys.ps1`
  - `SignSshKeys.py`
  - `SignSshKeys.sh`



`SignSshKeys.ps1` is dependent on PowerShell 7 or later and `SignSshKeys.py` is dependent on Python 3.6.0 or later and the [requests module](#).

The `SignSshKeys` script writes `user`, `user.pub`, and `user-cert.pub` files into the current working directory, which are later used by the `ssh` command. However, when a public key file is provided to the script, only a `<public_key>` file (with `<public_key>` replaced with the prefix of the public key file passed into the script) is written out to the directory.

5. Run the script to generate the SSH keychain with the `--sfadmin` flag. The script enables SSH across all nodes.

```
SignSshKeys --ip [ip address] --user [username] --duration [hours]
--sfadmin
```

To SSH as `--sfadmin` to a clustered node, you must generate the SSH keychain using a `--user` with `supportAdmin` access on the cluster.

To configure `supportAdmin` access for cluster administrator accounts, you can use the Element UI or APIs:



- [Configure "supportAdmin" access using the Element UI](#)
- Configure `supportAdmin` access by using APIs and adding "supportAdmin" as the "access" type in the API request:
  - [Configure "supportAdmin" access for a new account](#)
  - [Configure "supportAdmin" access for an existing account](#)

To get the `clusterAdminID`, you can use the [ListClusterAdmins](#) API.

To add `supportAdmin` access, you must have cluster administrator or administrator privileges.

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



You can use either the abbreviated or full form parameter.

- `--ip` | `-i [ip address]`: IP address of the target node for the API to run against.
- `--user` | `-u [username]`: Cluster user used to run the API call.

- **(Optional) --duration | -d [hours]:** The duration a signed key should remain valid as an integer in hours. The default is 24 hours.

- Compare your input against the following sample command. In this example, 192.168.0.1 is the IP of the storage node, admin is the cluster username, duration of key validity is two hours, and --sfadmin allows NetApp Support node access for troubleshooting:

```
sh /sf/bin/SignSshKeys.sh --ip 192.168.0.1 --user admin --duration 2 --sfadmin
```

- Run the command.

- SSH to the node IPs:

```
ssh -i user sfadmin@[node_ip]
```

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

```
rst --killall
```

- (Optional) Disable [remote access functionality](#) again after troubleshooting is complete.



SSH remains enabled on the management node if you do not disable it. SSH enabled configuration persists on the management node through updates and upgrades until it is manually disabled.

## Troubleshoot a node that is not part of cluster

You can perform basic troubleshooting of a node that has not yet been added to a cluster. You can use the sfreadonly system account for this purpose with or without the help of NetApp Support. If you have a management node set up, you can use it for SSH and run the script provided for this task.

- From a Windows, Linux, or Mac machine that has an SSH client installed, run the appropriate script for your system provided by NetApp Support.
- SSH to the node IP:

```
ssh -i user sfreadonly@[node_ip]
```

- (Optional) Disable [remote access functionality](#) again after troubleshooting is complete.



SSH remains enabled on the management node if you do not disable it. SSH enabled configuration persists on the management node through updates and upgrades until it is manually disabled.

## Find more information

- [NetApp Element Plug-in for vCenter Server](#)

## Start a remote NetApp Support session

If you require technical support for your 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.

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.

### Before you begin

- For management services 2.18 and later, the capability for remote access is disabled on the management node by default. To enable remote access functionality, see [Manage SSH functionality on the 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
```

- (Optional) Disable [remote access functionality](#) again.



SSH remains enabled on the management node if you do not disable it. SSH enabled configuration persists on the management node through updates and upgrades until it is manually disabled.

### Find more information

- [NetApp Element Plug-in for vCenter Server](#)
- [SolidFire and Element Software Documentation](#)

## 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 disabled by default on management nodes running management services 2.18 or later.

Beginning with Management Services 2.20.69, you can enable and disable SSH capability on the management node using the NetApp Hybrid Cloud Control UI.

### What you'll need

- **NetApp Hybrid Cloud Control permissions:** You have permissions as administrator.
- **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:**
  - To use the NetApp Hybrid Cloud Control UI, you have updated your [management services bundle](#) to version 2.20.69 or later.
  - To use the REST API UI, you have updated your [management services bundle](#) to version 2.17.

### Options

- [Disable or enable the SSH capability on the management node using NetApp Hybrid Cloud Control UI](#)

You can do any of the following tasks after you [authenticate](#):

- [Disable or enable the SSH capability on the management node using APIs](#)
- [Determine status of the SSH capability on the management node using APIs](#)

## Disable or enable the SSH capability on the management node using NetApp Hybrid Cloud Control UI

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 disabled by default on management nodes running management services 2.18 or later. 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 NetApp Hybrid Cloud Control UI.



To enable or disable support access using SSH for a storage cluster, you must use the [Element UI cluster settings page](#).

### Steps

1. From the Dashboard, select the options menu on the top right and select **Configure**.
2. In the **Support Access for Management Node** screen, toggle the switch to enable management node SSH.
3. After you complete troubleshooting, in the **Support Access for Management Node** screen, toggle the switch to disable management node SSH.

## Disable or enable the SSH capability on the management node using APIs

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 disabled by default on management nodes running management services 2.18 or later. 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

For management services 2.18 or later:

```
curl -k -X PUT
"https://<ManagementNodeIP>/mnode/2/settings/ssh?enabled=<false/true>" -H
"accept: application/json" -H "Authorization: Bearer ${TOKEN}"
```

For management services 2.17 or earlier:

```
curl -X PUT
"https://<ManagementNodeIP>/mnode/settings/ssh?enabled=<false/true>" -H
"accept: application/json" -H "Authorization: Bearer ${TOKEN}"
```



You can find the bearer `${TOKEN}` used by the API command when you [authorize](#). The bearer `${TOKEN}` is in 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. Select **Try it out**.
  - b. Set the **enabled** parameter to `false` to disable SSH or `true` to re-enable SSH capability that was previously disabled.
  - c. Select **Execute**.

## Determine status of the SSH capability on the management node using APIs

You can determine whether or not SSH capability is enabled on the management node using a management node service API. SSH is disabled by default on management nodes running management services 2.18 or later.

### API command

For management services 2.18 or later:

```
curl -k -X PUT
"https://<ManagementNodeIP>/mnode/2/settings/ssh?enabled=<false/true>" -H
"accept: application/json" -H "Authorization: Bearer ${TOKEN}"
```

For management services 2.17 or earlier:

```
curl -X PUT
"https://<ManagementNodeIP>/mnode/settings/ssh?enabled=<false/true>" -H
"accept: application/json" -H "Authorization: Bearer ${TOKEN}"
```



You can find the bearer `${TOKEN}` used by the API command when you [authorize](#). The bearer `${TOKEN}` is in 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. Select **Try it out**.
  - b. Select **Execute**.

### Find more information

- [NetApp Element Plug-in for vCenter Server](#)
- [SolidFire and Element Software Documentation](#)

## Copyright information

Copyright © 2024 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.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

## 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.