NetApp HCI 1.6P1

Management Node User Guide for NetApp Element Software

October 2019 | 215-14554_2019-10_en-us
doccomments@netapp.com

NetApp®

Contents

About this guide

This guide introduces the management node for NetApp Element software-based systems. You can use this guide to better understand management node functionality and perform manual installations and upgrades.

Management node for Element software

The management node (mNode) is a virtual machine that runs in parallel with one or more Element software-based storage clusters. It is used to upgrade and provide system services including monitoring and telemetry, manage cluster assets and settings, run system tests and utilities, and enable NetApp Support access for troubleshooting.

As of the Element 11.3 release, the management node functions as a microservice host, allowing for quicker updates of select software services outside of major releases. These microservices or management services, such as the Active IQ collector, QoSSIOC for the vCenter Plug-in, and mNode service, are updated frequently as service bundles. Additional services including HealthTools for storage node software upgrades and support tools (remote support tunneling) are also available from the management node.

Management services for NetApp HCI

Management services provide central and extended management functionality for NetApp HCI. These services include system telemetry, logging, and update services, the QoSSIOC service for Element Plug-in for vCenter Server, as well as capabilities relevant to on-premises cloud solutions, such as NetApp Hybrid Cloud Control, provided by NetApp HCI.

Related tasks

Updating management services on page 35

Persistent volumes

Persistent volumes allow management node configuration data to be stored on a specified storage cluster, rather than locally with a VM, so that data can be preserved in the event of management node loss or removal. Persistent volumes are an optional but recommended management node configuration.

If you are deploying a management node for NetApp HCI using the NetApp Deployment Engine, persistent volumes are enabled and configured automatically.

An option to enable persistent volumes is included in the installation and upgrade scripts when deploying a new management node. Persistent volumes are volumes on an Element software-based storage cluster that contain management node configuration information for the host management node VM that persists beyond the life of the VM. If the management node is lost, a replacement management node VM can reconnect to and recover configuration data for the lost VM.

Persistent volumes functionality, if enabled during installation or upgrade, automatically creates multiple volumes with `NetApp-HCI-` pre-pended to the name on the assigned cluster. These volumes, like any Element software-based volume, can be viewed using the Element software web UI, NetApp Element Plug-in for vCenter Server, or API, depending on your preference and installation. Persistent volumes must be up and running with an iSCSI connection to the management node to maintain current configuration data that can be used for recovery.

Attention: Persistent volumes are assigned to a new account that is also created during installation or upgrade. After you created persistent volumes, you must not modify or delete the volumes and their associated account.

Network port requirements

You might need to allow the following TCP ports through your datacenter's edge firewall so that you can manage the system remotely and allow clients outside of your datacenter to connect to resources. Some of these ports might not be required, depending on how you use the system.

All ports are TCP unless stated otherwise, and should permit bi-directional communications between the NetApp Support Server, management node, and nodes running Element software.

Tip: Enable ICMP between the management node, nodes running Element software, and cluster MVIP.

The following abbreviations are used in the table:

- MIP: Management IP address, a per-node address
- SIP: Storage IP address, a per-node address
- MVIP: Management virtual IP address
- SVIP: Storage virtual IP address

Source	Destination	Port	Description
iSCSI clients	Storage cluster MVIP	443	(Optional) UI and API access
iSCSI clients	Storage cluster SVIP	3260	Client iSCSI communications
iSCSI clients	Storage node SIP	3260	Client iSCSI communications
Management node	sfsupport.solidfire.com	22	Reverse SSH tunnel for support access
Management node	Storage node MIP	22	SSH access for support
Management node	DNS servers	53 TCP/UDP	DNS lookup
Management node	Storage node MIP	442	UI and API access to storage node and Element software upgrades
Management node	Online software repository: • `https://repo.netapp.com/bintray/api/package` • `https://netapp-downloads.bintray.com`	443	Management node service upgrades
Management node	monitoring.solidfire.com	443	Storage cluster reporting to Active IQ
Management node	Storage cluster MVIP	443	UI and API access to storage node and Element software upgrades
SNMP server	Storage cluster MVIP	161 UDP	SNMP polling

Source	Destination	Port	Description
SNMP server	Storage node MIP	161 UDP	SNMP polling
Storage node MIP	DNS servers	53 TCP/UDP	DNS lookup
Storage node MIP	Management node	80	Element software upgrades
Storage node MIP	S3/Swift endpoint	80	(Optional) HTTP communication to S3/Swift endpoint for backup and recovery
Storage node MIP	NTP server	123 UDP	NTP
Storage node MIP	Management node	162 UDP	(Optional) SNMP traps
Storage node MIP	SNMP server	162 UDP	(Optional) SNMP traps
Storage node MIP	LDAP server	389 TCP/UDP	(Optional) LDAP lookup
Storage node MIP	Remote storage cluster MVIP	443	Remote replication cluster pairing communication
Storage node MIP	Remote storage node MIP	443	Remote replication cluster pairing communication
Storage node MIP	S3/Swift endpoint	443	(Optional) HTTPS communication to S3/Swift endpoint for backup and recovery
Storage node MIP	Management node	10514 TCP/UDP 514 TCP/UDP	Syslog forwarding
Storage node MIP	Syslog server	10514 TCP/UDP 514 TCP/UDP	Syslog forwarding
Storage node MIP	LDAPS server	636 TCP/UDP	LDAPS lookup
Storage node MIP	Remote storage node MIP	2181	Intercluster communication for remote replication
Storage node SIP	S3/Swift endpoint	80	(Optional) HTTP communication to S3/Swift endpoint for backup and recovery
Storage node SIP	S3/Swift endpoint	443	(Optional) HTTPS communication to S3/Swift endpoint for backup and recovery
Storage node SIP	Remote storage node SIP	2181	Intercluster communication for remote replication
Storage node SIP	Storage node SIP	3260	Internode iSCSI

Source	Destination	Port	Description
Storage node SIP	Remote storage node SIP	4000 through 4020	Remote replication node-to-node data transfer
Storage node SIP	Compute node SIP	442	Compute node API, configuration and validation, and access to software inventory
System administrator PC	Storage node MIP	80	(NetApp HCI only) Landing page of NetApp Deployment Engine
System administrator PC	Management node	442	HTTPS UI access to management node
System administrator PC	Storage node MIP	442	HTTPS UI and API access to storage node
			(NetApp HCI only) Configuration and deployment monitoring in NetApp Deployment Engine
System administrator PC	Management node	443	HTTPS UI and API access to management node
System administrator PC	Storage cluster MVIP	443	HTTPS UI and API access to storage cluster
System administrator PC	Storage node MIP	443	HTTPS storage cluster creation, post-deployment UI access to storage cluster
vCenter Server	Storage cluster MVIP	443	vCenter Plug-in API access
vCenter Server	Management node	8443	(Optional) vCenter Plug-in QoSSIOC service.
vCenter Server	Storage cluster MVIP	8444	vCenter VASA provider access (VVols only)
vCenter Server	Management node	9443	vCenter Plug-in registration. The port can be closed after registration is complete.

Installing a management node

You can manually install the management node for your cluster running NetApp Element software using the appropriate image for your configuration. This manual process is intended for SolidFire all-flash storage administrators and NetApp HCI administrators who are not using the NetApp Deployment Engine for management node installation.

Before you begin

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

  Note: You can use the management node 11.1 if you need IPv6 support.
- You have permissions to download software from the NetApp Support Site.
- You have identified the management node image type that is correct for your platform. See the following table for guidance:

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

About this task

Prior to completing this procedure, you should have an understanding of persistent volumes and whether or not you want to use them. Persistent volumes allow management node data to be stored on a specified storage cluster so that data can be preserved in the event of management node loss or removal.

Steps

1. Download the OVA or ISO for your installation from the NetApp Support Site:
   - Element software: *https://mysupport.netapp.com/products/p/element_software.html*
   - NetApp HCI: *https://mysupport.netapp.com/products/p/hci.html*

   a. Select the version number of the software to download.

   b. Click **Go**.

   c. Read and click through the required prompts, accept the EULA, and 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 (eth1) or ensure that the management network can route to the storage network..

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

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

      - Six virtual CPUs
      - 12GB RAM
      - 400GB virtual disk, thin provisioned
      - One virtual network interface with internet access and access to the storage MVIP.
      - (Optional for SolidFire all-flash storage) One virtual network interface with management network access to the storage cluster. If your storage cluster is on a separate subnet from your management node (eth0) and you want to use persistent volumes, add a second network interface controller (NIC) to the VM on the storage subnet (eth1) or ensure that the management network can route to the storage network.

        Attention: 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.

      Note: 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.
5. Using the terminal user interface (TUI), create a management node admin user.

   Tip: To enter text, press **Enter** three times on the keyboard to open edit mode. After you enter text, press **Enter** again to close the edit mode. To navigate between fields, use the arrow keys.

6. Configure the management node network (eth0).

   Note: If you have a second NIC on eth1, see instructions on configuring a second NIC.

   Configuring a storage NIC (eth1)

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

   ```
   sudo su
   ```

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

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

10. Configure the management node setup command:

Note: You might be prompted to enter passwords or other information if you do not include them in the command. If your cluster is behind a proxy server, you must configure the proxy settings so you can reach a public network.

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

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

Note: 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 MVIP (management virtual IP address) of the storage cluster running Element software.

--storage_username (-su) [username]

The storage cluster administrator username for the cluster specified by the `--storage_mvip` parameter.

--telemetry_active (-t) [true]

Retain the value `true` that enables data collection for analytics by Active IQ.

b. (Optional): Add password or Active IQ endpoint parameters to the command. You will be prompted to enter these passwords in a secure prompt if you do not include them in the command:

--mnode_admin_password (-mp) [password]

The password of the management node administrator account. This is likely to be the password for the user account you used to log into the management node.

--storage_password (-sp) [password]

The password of the storage cluster administrator specified by the `--storage_username` parameter.

--remote_host (-rh) [AIQ_endpoint]

The endpoint where Active IQ telemetry data is sent to be processed. If the parameter is not included, the default endpoint is used.

c. (Optional): Add the following persistent volume parameters:

Attention: 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.

Note: 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 MVIP (management virtual IP address) 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.

11. (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.

12. Run the `setup-mnode` command.

Important: If you have an NetApp HCI installation, in addition to running the setup script you also need to add a controller asset for vCenter using the REST API UI for the management node (`https:// [mNode IP]/mnode`). A controller asset is necessary for NetApp HCI monitoring and cloud control functionality to operate properly and is not installed as part of manual upgrade. To create a controller asset, use the following REST API: `POST /assets/{asset_id}/controller`. You can acquire the `asset_ID` necessary to complete the command from the base asset using `GET /assets`.

Related concepts

Persistent volumes on page 5

Related tasks

Upgrading the management node to version 11.3 on page 13

Upgrading the management node to version 11.3

You can perform an in-place upgrade of the management node from 11.0 or 11.1 to version 11.3 without needing to provision a new management node virtual machine.

Before you begin

- Storage nodes are running Element 11.3.

  Note: Use the latest HealthTools to upgrade Element software.

- The management node you are intending to upgrade is version 11.0 or 11.1 and uses IPv4 networking. The management node 11.3 does not support IPv6.

  Note: For management node 11.0, the VM memory needs to be manually increased to 12GB.

- You have configured an additional network adapter (if required) using the instructions for configuring a storage NIC (eth1) in the management node user guide your product.

  Note: Persistent volumes might require an additional network adapter if eth0 is not able to be routed to the SVIP. Configure a new network adapter on the iSCSI storage network to allow the configuration of persistent volumes.

- You have logged in to the management node virtual machine using SSH or console access.

- You have downloaded the management node ISO for *NetApp HCI* or *Element software* from the NetApp Support Site to the management node virtual machine.

  Note: The name of the ISO is similar to `solidfire-fdva-sodium-patch3-11.3.0.xxxx.iso`

- You have checked the integrity of the download by running md5sum on the downloaded file and compared the output to what is available on NetApp Support Site for *NetApp HCI* or *Element software*, as in the following example:

```
sudo md5sum -b <path to iso>/solidfire-fdva-sodium-
patch3-11.3.0.xxxx.iso
```

Steps

1. Mount the management node ISO image and copy the contents to the file system using the following commands:

```
sudo mkdir -p /upgrade
```

```
sudo mount solidfire-fdva-sodium-patch3-11.3.0.xxxx.iso /mnt
```

```
cd /mnt
```

```
sudo cp -r * /upgrade
```

2. Change to the home directory, and unmount the ISO file from `/mnt`:

```
cd ~
```

```
sudo umount /mnt
```

3. Delete the ISO to conserve space on the management node:

```
sudo rm <path to iso>/solidfire-fdva-sodium-patch3-11.3.0.xxxx.iso
```

4. Run one of the following scripts with options to upgrade the management node OS version for either management node 11.1 or management node 11.0. Each script retains all necessary configuration files after the upgrade, such as Active IQ collector and proxy settings.

   - On an 11.1 (11.1.0.73) management node, run the following command:

```
sudo /sf/rtfi/bin/sfrtfi_inplace file:///upgrade/casper/
filesystem.squashfs sf_upgrade=1 sf_keep_paths="/sf/packages/
solidfire-sioc-4.2.3.2288 /sf/packages/solidfire-nma-1.4.10/
conf /sf/packages/sioc /sf/packages/nma"
```

   - On an 11.1 (11.1.0.72) management node, run the following command:

```
sudo /sf/rtfi/bin/sfrtfi_inplace file:///upgrade/casper/
filesystem.squashfs sf_upgrade=1 sf_keep_paths="/sf/packages/
solidfire-sioc-4.2.1.2281 /sf/packages/solidfire-nma-1.4.10/
conf /sf/packages/sioc /sf/packages/nma"
```

   - On an 11.0 (11.0.0.781) management node, run the following command:

```
sudo /sf/rtfi/bin/sfrtfi_inplace file:///upgrade/casper/
filesystem.squashfs sf_upgrade=1 sf_keep_paths="/sf/packages/
solidfire-sioc-4.2.0.2253  /sf/packages/solidfire-nma-1.4.8/
conf /sf/packages/sioc /sf/packages/nma"
```

5. After the process completes, access the management node CLI using SSH or console access, and link to the upgraded `<management node ip>:442`:

```
sudo unlink /etc/nginx.legacy.conf.d/node.conf
```

```
sudo ln -s /sf/etc/webmgmt/11.3/nginx_conf/node.conf /etc/
nginx.legacy.conf.d/node.conf
```

```
sudo systemctl restart nginx
```

6. Ensure there are no escape characters (for example: '\') in the `"password="` field of the `/sf/packages/sioc/app.properties` file. These characters might cause the upgrade process to fail.

7. On the 11.3 management node, run the `upgrade-mnode` script to copy the Active IQ collector to the new configuration format.

   Note: Because this is an in-place upgrade, the -mu, -pmi, -pmu commands point to the upgraded 11.3 management IP and user name, not a newly installed 11.3 management node. You need to enter the same password twice.

- For a single storage cluster managed by the existing management node, with persistent volumes:

```
/sf/packages/mnode/upgrade-mnode -mu <mnode user> -pmi <current
mnode ip> -pmu <current mnode user> -pv <true - persistent volume>
-pva <persistent volume account name - storage volume account>
```

- For a single storage cluster managed by the existing management node, with no persistent volumes:

```
/sf/packages/mnode/upgrade-mnode -mu <mnode user> -pmi <current ip
address> -pmu <current mnode user>
```

- For multiple storage clusters managed by the existing management node, with persistent volumes:

```
/sf/packages/mnode/upgrade-mnode -mu <mnode user> -pmi <current
mnode ip> -pmu <current mnode user> -pv <true - persistent volume>
-pva <persistent volume account name - storage volume account> -
pvm <persistent volumes mvip>
```

- For multiple storage clusters managed by the existing management node, with no persistent volumes (-pvm flag is just to provide one of the cluster's MVIP addresses):

```
/sf/packages/mnode/upgrade-mnode -mu <mnode user> -pmi <current ip
address> -pmu <current mnode user> -pvm <mvip for persistent
volumes>
```

8. (For installations with the NetApp Element Plugin for vCenter Server) Upgrade the vCenter Plug-in on the 11.3 management node:

   a. Log out of the vSphere Web Client.

   b. Browse to the registration utility (`<management node ip>:9443`).

   c. Click the **vCenter Plug-in Registration** tab.

   d. Under **Manage vCenter Plug-in**, select **Update Plug-in**.

   e. Update the vCenter address, vCenter administrator user name, and vCenter administrator password.

   f. Click **Update**.

   g. Log in to the vSphere Web Client and verify that the plug-in information has been updated by browsing to **Home > NetApp Element Configuration > About**.

9. (For NetApp HCI only) Add a vCenter controller asset.

   a. Open a browser to the storage MVIP and log in, which will accept the certificate for the next step.

   b. Open a browser to `https://<mnodeip>/mnode`.

   c. Click **Authorize** and enter your MVIP username and password credentials. Close the pop-up window.

   d. Execute **GET /assets** to pull the base asset ID needed to add the vcenter/controller asset.

   e. Execute **POST /assets/{ASSET_ID}/controllers** to add a controller asset with vCenter credentials.

Related concepts

Persistent volumes on page 5

Related tasks

Installing a management node on page 9

Configuring a storage NIC (eth1)

If you are using a second NIC for storage, you can SSH in to the management node or use the vCenter console and run a curl command to set up the network for eth1.

Before you begin

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

Steps

1. Open an SSH or vCenter console.
2. Replace the values in the following command template (represented by `$`) for each of the required parameters for eth0 and eth1:

   Note: The `cluster` object in the following template is optional and can be used for management node host name renaming. The `- -insecure` and the `-k` options should not be used in production environments.

```
curl -u $mnode-username:$mnode-password --insecure -X POST \
  https://$mnode_management_IP:442/json-rpc/10.0 \
  -H 'Content-Type: application/json' \
  -H 'cache-control: no-cache' \
  -d '  {
        "params": {
                "network": {
                        "eth0": {
                                "address": "$eth0_ip_mnode_management_IP",
                                "dns-nameservers": "$dns_ip_or_hostname",
                                "netmask": "$eth0_net_mask",
                                "gateway": "$gateway_IP",
                                "gatewayV6": ""
                        },
                        "eth1": {
                                "address": "$eth1_ip",
                                "netmask": "$eth1_netmask",
                                "status": "Up",
                                "method": "static",
                                "mtu": "9000"
                        }
      },
                "cluster": {
                        "name": "$desired_mNode_vm_hostname"
                }
        },
        "method": "SetConfig"
}
'
```

3. Run the command.

Recovering a management node

You can manually recover and redeploy the management node for your cluster running NetApp Element software if your previous management node used persistent volumes. You can deploy a new OVA and run a redeploy script to pull configuration data from a previously installed management node running version 11.3 and later.

Before you begin

- Your previous management node was running NetApp Element software version 11.3 or later with persistent volumes functionality engaged.
- You know the MVIP and SVIP of the cluster containing the persistent volumes.
- Your cluster version must be running NetApp Element software 11.3 or later.
- Your installation uses IPv4. The management node does not support IPv6.
- You have permissions to download software from the NetApp Support Site.
- You have identified the management node image type that is correct for your platform. See the following table for guidance:

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

Steps

1. Download the OVA or ISO for your installation from the NetApp Support Site:
   - Element software: *https://mysupport.netapp.com/products/p/element_software.html*
   - NetApp HCI: *https://mysupport.netapp.com/products/p/hci.html*
   a. Select the version number of the software to download.
   b. Click **Go**.
   c. Read and click through the required prompts, accept the EULA, and 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 (eth1).
3. If you downloaded the ISO, follow these steps:
   a. Create a new 64-bit virtual machine from your hypervisor with the following configuration:

- Six virtual CPUs
- 12GB RAM
- 400GB virtual disk, thin provisioned
- One virtual network interface with internet access and access to the storage MVIP.
- (Optional for SolidFire all-flash storage) One virtual network interface with management network access to the storage cluster. If your storage cluster is on a separate subnet from your management node (eth0) and you want to use persistent volumes, add a second network interface controller (NIC) to the VM on the storage subnet (eth1) or ensure that the management network can route to the storage network.

  Attention: 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.

   Note: 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.
5. Using the terminal user interface (TUI), create a management node admin user.

   Tip: To enter text, press **Enter** three times on the keyboard to open edit mode. After you enter text, press **Enter** again to close the edit mode. To navigate between fields, use the arrow keys.

6. Configure the management node network (eth0).

   Note: If you have a second NIC on eth1, see instructions on configuring a second NIC.

   Configuring a storage NIC (eth1)

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

   ```
   sudo su
   ```

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

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

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

    Note: You will be prompted to enter passwords if you do not include them in the command.

    ```
    /sf/packages/mnode/redeploy-mnode --mnode_admin_user [username] --
    storage_username [username] --storage_mvip [mvip] --storage_svip
    [svip] --persistent_volumes_account [account-name]
    ```

    a. Replace the values in `[ ]` brackets for each of the following required parameters:

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

--mnode_admin_user (-mu) [username]

The user name for the management node administrator account. This is likely to be the user name for the user account you used to log into the management node.

--storage_username (-su) [username]

The storage cluster administrator user name for the cluster specified by the `--storage_mvip` parameter.

--storage_mvip (-sm) [MVIP address]

The MVIP (management virtual IP address) of the storage cluster running Element software with the persistent volumes that contain management node data for recovery.

--storage_svip (-ss) [svip]

The SVIP (storage virtual IP address) of the storage cluster running Element software with the persistent volumes that contain management node data for recovery.

--persistent_volumes_account (-pva) [account_name]

Enter the storage account name from the cluster containing the persistent volumes. This is the exact name of the storage user account that owns the volumes in the cluster.

b. (Optional): Add administrator and storage credential parameters to the command. You will be prompted to enter these passwords in a secure prompt if you do not include them in the command:

--mnode_admin_password (-mp) [password]

The password of the management node administrator account. This is likely to be the password for the user account you used to log into the management node.

--storage_password (-sp) [password]

The password of the storage cluster administrator specified by the `--storage_username` parameter.

c. (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.

d. Run the `redeploy-mnode` command.

Related concepts

Persistent volumes on page 5

Working with the management node

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

For clusters running Element software version 11.3 or later, you can make changes to network and cluster settings, run system tests, or use system utilities using the management node UI (`https://[mNode IP}:442`). You can also use the built-in REST API UI (`https://[mNode IP}/mnode`) to run or understand APIs relating to the management node services, including proxy server configuration, service level updates, or managing assets known to the management node.

Related tasks

Accessing the management node per-node UI on page 21
Accessing the management node REST API UI on page 22
Enabling remote NetApp Support connections on page 29
Getting authorization to use REST APIs on page 23

Accessing 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.

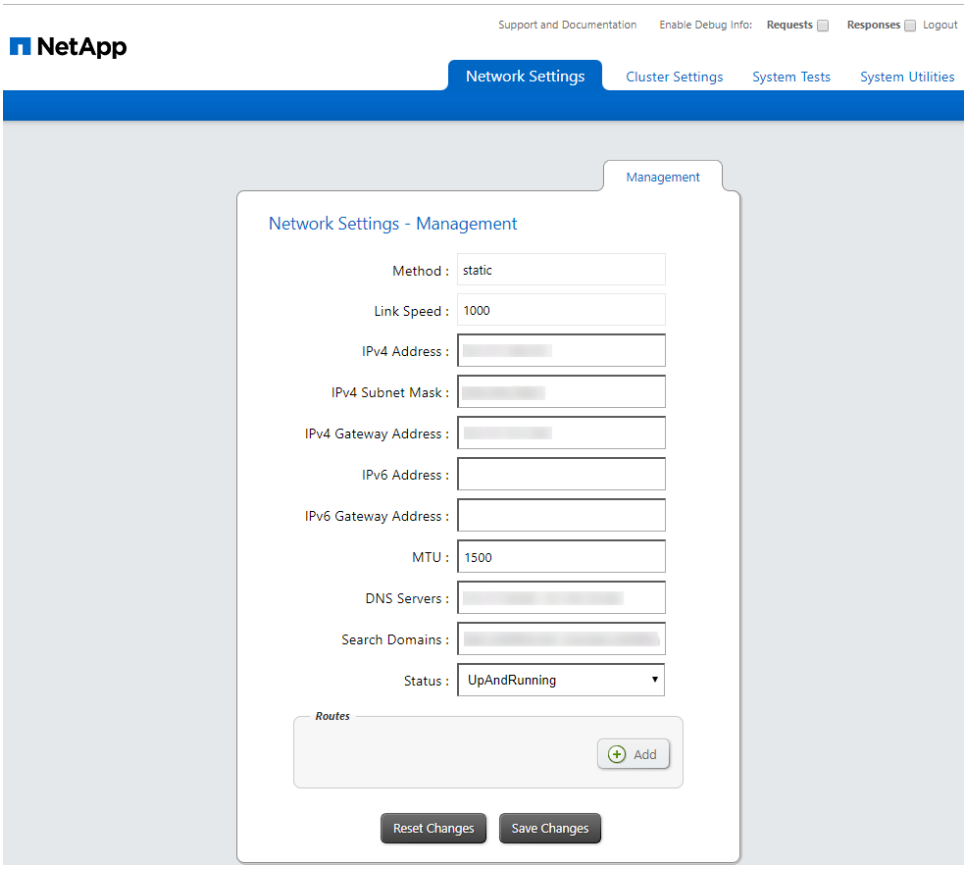
Accessing the management node per-node UI

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

Steps

1. To access the per-node UI for the management node, enter the management node IP address followed by `:442`:

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



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

Related tasks

Accessing the management node REST API UI on page 22

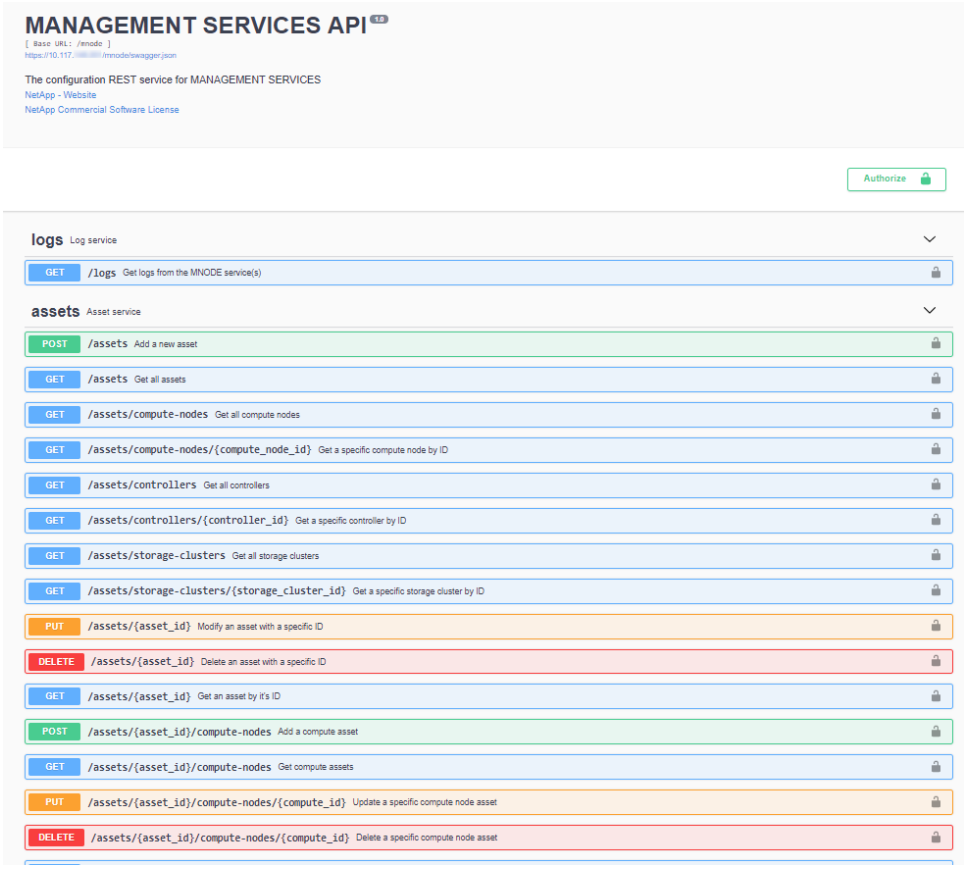
Accessing the management node REST API UI

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

Steps

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

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



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

Related tasks

Accessing the management node per-node UI on page 21
Configuring a proxy server on page 31
Enabling Active IQ and HCI monitoring services for NetApp HCI on page 29

Getting authorization to use REST APIs

You must authorize before you can use APIs for management services in the REST API UI. You must provide cluster admin credentials and a client ID to obtain an access token. Each token lasts approximately ten minutes. After a token expires, you can authorize again for a new access token.

Before you begin

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

About this task

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.

Steps

1. Open the REST API UI on the management node: `https://[management node IP]/mnode`
2. Click **Authorize** and complete the following:

Note: Alternately, you can click on a lock icon next to any service API and follow these same steps to authorize.

a. Enter the cluster user name and password.

b. Select **Request body** from the **type** drop-down list if the value is not already selected.

c. Enter the client ID as `mnode-client` if the value is not already populated.

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

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

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

The **Available authorizations** screen indicates **Authorized** and the button to authorize has changed to **Logout**.

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

Note: If you attempt to run a command after the token expires, a 401 `Error: UNAUTHORIZED` message is returned. If you receive this response, authorize again.

NetApp HCI system alerts

You can use the Alert Monitor tab in the web UI on a management node to run a system test and configure settings for a NetApp HCI monitor server.

You can access the Alert Monitor settings by browsing to the management node IP address using the following notation:

```
https://<IP address>:442
```

VMware vCenter Alert Monitor

The following table details the configuration options for the alert monitor functionality:

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

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

Management node network settings

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

Method

The method used to configure the interface. Possible methods are:

- `loopback`: Used to define the IPv4 loopback interface.
- `manual`: Used to define interfaces for which no configuration is done by default.

- `dhcp`: Used to obtain an IP address via DHCP.
- `static`: Used to define Ethernet interfaces with statically allocated IPv4 addresses.

Link Speed

The speed negotiated by the virtual NIC.

IPv4 Address

The IPv4 address for the eth0 network.

IPv4 Subnet Mask

Address subdivisions of the IPv4 network.

IPv4 Gateway Address

Router network address to send packets out of the local network.

IPv6 Address

The IPv6 address for the eth0 network.

Attention: This functionality is not supported for the Element software 11.3 version of the management node.

IPv6 Gateway Address

Router network address to send packets out of the local network.

Attention: This functionality is not supported for the Element software 11.3 version of the management node.

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.

DNS Servers

Network interface used for cluster communication.

Search Domains

Search for additional MAC addresses available to the system.

Status

Possible values:

- `UpAndRunning`
- `Down`
- `Up`

Routes

Static routes to specific hosts or networks via the associated interface the routes are configured to use.

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.

Role

Role the management node has in the cluster. Possible value: `Management`.

Hostname

Name of the management node.

Version

Element software version running on the cluster.

Default Interface

Default network interface used for management node communication with the cluster running Element software.

Testing 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.

Before you begin

You are logged in to the management node per-node UI (`https://[mNode IP address]:442`) using the management node admin credentials.

Steps

1. In the management node user interface, click **System Tests**.
2. Run any of the following:
   - To verify that the network settings you configured are valid for the system, click **Test Network Config**.
   - To test network connectivity to all nodes in the cluster on both 1G and 10G interfaces using ICMP packets, click **Test Ping**.

   The following additional options can also be defined:

   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.

Related references

Management node network settings on page 25

Running 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.

Before you begin

You are logged in to the management node per-node UI (`https://[mNode IP address]:442`) using the management node admin credentials.

Steps

1. In the per-node UI for the management node, click **System Utilities**.
2. Click the button for the utility that you want to run:
   - **Control Power**: Reboots, power cycles, or shuts down the node.

     Attention: This operation causes temporary loss of networking connectivity.

     Specify the following options:

     Action

     Options include `Restart` and `Halt` (power off).

     Wakeup Delay

     Any additional time before the node comes back online.
   - **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.
   - **Delete All Support Bundles**: Deletes any current support bundles on the management node.

- **Reset Node**: Resets the management node to a new install image. This changes all settings except the network configuration to the default state.

  Attention: This operation causes temporary loss of networking connectivity.

  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.

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

  Attention: This operation causes temporary loss of networking connectivity.

Enabling remote NetApp Support connections

If you require technical support for your NetApp Element software-based storage system, NetApp Support can connect remotely with your system. To gain remote access, NetApp Support can open a reverse Secure Shell (SSH) connection to your environment.

About this task

You can open a TCP port for an SSH reverse tunnel connection with NetApp Support. This connection allows NetApp Support to log in to your management node. If your management node is behind a proxy server, the following TCP ports are required in the `sshd.config` file:

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

Steps

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

   ```
   rst –r sfsupport.solidfire.com –u element –p <port number>
   ```

   NetApp Support can provide the port number needed to access your management node with an SSH connection.
3. To close a remote support tunnel, enter the following:

   ```
   rst --killall
   ```

Enabling Active IQ and HCI monitoring services for NetApp HCI

You can enable storage and compute telemetry (the Active IQ collector and NetApp HCI monitoring services) if you did not already do so during installation or upgrade. This process involves modifying

a base asset and adding a vCenter controller asset using the REST API. You might need to use this procedure if you disabled telemetry using the NetApp Deployment Engine.

Before you begin

- 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 internet access. The Active IQ collector service cannot be used from dark sites.

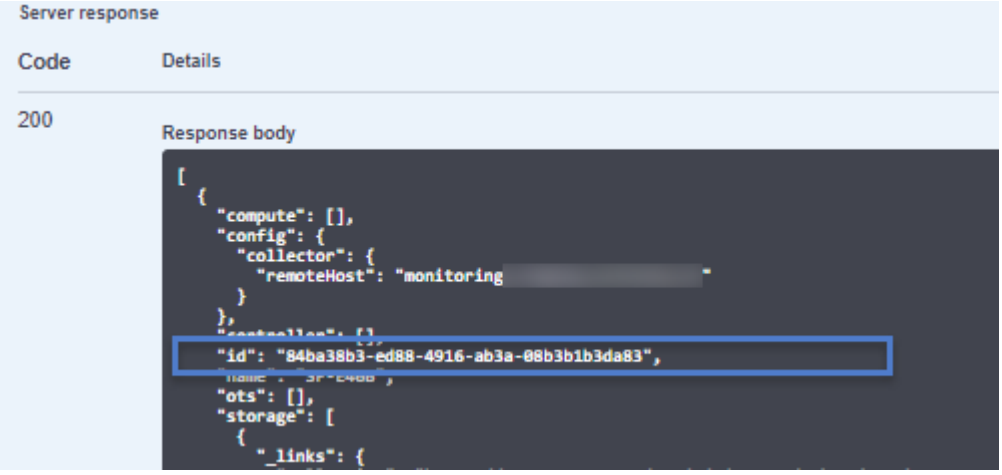
About this task

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

Steps

1. Open the REST API UI on the management node: `https://[management node IP]/mnode`
2. Click **Authorize** or any lock icon and complete the following:
   a. Enter the cluster user name and password.
   b. Enter the client ID as `mnode-client` if the value is not already populated.
   c. Copy the token URL string and paste it into another browser tab to initiate a token request.
   d. Click **Authorize** to begin a session.
3. Click **GET /assets**.
4. Copy the value for `"id"` for the base asset to your clipboard:

   Note: A base asset and sub-assets were created when you ran the upgrade or setup scripts during management node installation or upgrade or deployed your NetApp HCI using the NetApp Deployment Engine.



5. Configure the base asset:
   a. Click **PUT /assets/{asset_id}**.
   b. Click **Try it out**.

c. Enter the following in the JSON payload:

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

d. Enter the ID from the base asset step in **asset_ID**.

e. Click **Execute**.

6. Add a controller asset for vCenter.

   Note: A controller asset is required for NetApp HCI monitoring services.

a. Click **POST /assets/{asset_id}/controllers**.

b. Click **Try it out**.

c. Enter the configuration information for the controller asset. All fields are optional:

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

d. Enter the parent ID from the base asset in **asset_ID**.

e. Click **Execute**.

Configuring 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.

Before you begin

- You know host and credential information for the proxy server you are configuring.
- Your cluster version is running NetApp Element software 11.3 or later.
- You have deployed a management node running version 11.3 or later.

About this task

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

Steps

1. Open the REST API UI on the management node: `https://[management node IP]/mnode`

2. Click **Authorize** or any lock icon and complete the following:
   a. Enter the cluster user name and password.
   b. Enter the client ID as `mnode-client` if the value is not already populated.
   c. Copy the token URL string and paste it into another browser tab to initiate a token request.
   d. Click **Authorize** to begin a session.
3. Click **PUT /settings**.
4. Click **Try it out**.
5. To enable a proxy server, you must set `"use_proxy"` to `true`. Enter the IP or host name and proxy port destinations. The proxy user name, proxy password, and SSH port are optional and should be omitted if not used.

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

6. Click **Execute**.

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.

Before you begin

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

Steps

1. Open the REST API UI on the management node: `https://[management node IP]/mnode`
2. Click **Authorize** or any lock icon and complete the following:
   a. Enter the cluster user name and password.
   b. Enter the client ID as `mnode-client` if the value is not already populated.
   c. Copy the token URL string and paste it into another browser tab to initiate a token request.
   d. Click **Authorize** to begin a session.
3. Click **GET /logs**.
4. Click **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 100.
- `service-name`: Enter a service name.

  Tip: Use the `GET /services` command to list services on the management node.

- `type`: Select the specific log type to pull:

  a. `service`: Pulls regular public running services. This is the default and most common option.

  b. `syslog`: Pulls all syslog from the host machine.

  c. `all`: Pulls from all public services and syslogs.

- `since`: Adds a ISO-8601 timestamp for the service logs starting point.
- `archived`: Adds archived files to the log request.

6. Click **Execute**.

Verifying management services version

You can verify the version number of management services using the REST API UI in the management node.

Before you begin

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

Steps

1. Open the REST API UI on the management node: `https://[management node IP]/mnode`
2. Click **GET /about**.
3. Click **Try it out**.
4. Click **Execute**.

   The version number `mnode_bundle_version` is indicated in the response body.

Updating management services

You can manually update management services using the REST API UI from the management node. Management services updates are available as service bundles from an online software repository. NetApp HCI users should perform management services updates from the NetApp Deployment Engine monitoring page.

Before you begin

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

About this task

Management services include the SIOC service for the Element Plug-in for vCenter, the Active IQ collector service, the NetApp HCI monitoring service (for NetApp HCI installations only) and additional services. Updates to non-service-based components of the management node are provided as updated images (OVA or ISO) and cannot be updated using this procedure.

Steps

1. Open the REST API UI on the management node: `https://[management node IP]/mnode`
2. Click **Authorize** and complete the following:
   a. Enter the cluster user name and password.
   b. Enter the client ID as `mnode-client` if the value is not already populated.
   c. Copy the token URL string and paste it into another browser tab to initiate a token request.
   d. Click **Authorize** to begin a session.
3. (Optional) Confirm available versions of management node services: `GET /services/versions`
4. (Optional) Get detailed information about the latest version: `GET /services/versions/latest`
5. (Optional) Get detailed information about a specific version: `GET /services/versions/{version}/info`
6. Perform one of the following management services update options:

Option	Description
`PUT /services/update/latest`	Run this command to update to the most recent version of management node services.
`PUT /services/update/{version}`	Run this command to update to a specific version of management node services.

7. Use `GET/services/update/status` to monitor the status of the update.

   A successful update returns a result similar to the following example:

```
{
    "current_version": "2.0.442",
```

```
    "details": "Updated to version 2.0.442",
    "status": "success"
}
```

Related information

KB: Management Services Release Notes

Where to find product documentation and other information

You can learn more about using and managing NetApp HCI and SolidFire all-flash storage from the resources available in the Documentation Centers and Resources pages for both products.

In the Documentation Centers, you can also find information about hardware installation and maintenance, additional content resources available, links to known issues and resolved issues, and the latest release notes. On the Resources pages, you can find links to data sheets, technical reports, white papers, and videos.

- *NetApp HCI Documentation Center*
- *NetApp HCI Resources page*
- *SolidFire and Element 11.3 Documentation Center*
- *SolidFire Resources page*

Contacting NetApp Support

If you need help with or have questions or comments about NetApp products, contact NetApp Support.

- Web:
  mysupport.netapp.com
- Phone:
  - 888.4.NETAPP (888.463.8277) (US and Canada)
  - 00.800.44.638277 (EMEA/Europe)
  - +800.800.80.800 (Asia/Pacific)