Upgrade a management node

HCI

dbag-personal, Ann-Marie Grissino, Dave Bagwell
June 16, 2020

NetApp®

Table of Contents

Upgrade a management node 1
- Upgrade a management node to version 12.0 from 11.3 or later 1
- Upgrade a management node to version 12.0 from 11.1 or 11.0 3
- Migrating from management node version 10.x to 11.x 7
- Reconfigure authentication using the management node REST API 10

Upgrade a management node

You can upgrade your management node to management node version 12.0 from version 11.0 or later.

What you'll need

- The vCenter Plug-in 4.4 or later requires a management node 11.3 or later that is created with modular architecture and provides individual services.

Upgrade options

Choose one of the following management node upgrade options:

- If you are upgrading from management node 11.3 or later:
  Upgrade a management node to version 12.0 from 11.3 or later
- If you are upgrading from management node 11.0 or 11.1:
  Upgrade a management node to version 12.0 from 11.1 or 11.0
- If you are upgrading from a management node version 10.x:
  Migrating from management node version 10.x to 11.x

Choose this option if you have **sequentially** updated (1) your management services version and (2) your Element storage version and you want to **keep** your existing management node:

- If you are keeping existing management node:
  Reconfigure authentication using the management node REST API

If you do not sequentially update your management services followed by Element storage, you cannot reconfigure reauthentication using this procedure. Follow the appropriate upgrade procedure instead.

Upgrade a management node to version 12.0 from 11.3 or later

You can perform an in-place upgrade of the management node from 11.3 or later to version 12.0 without needing to provision a new management node virtual machine. You can use this procedure if you are upgrading from any of the following management node versions: 11.3, 11.5, 11.7, or 11.8.

Before you begin

- The management node you are intending to upgrade is version 11.3 or later and uses IPv4 networking. The management node version 12.0 does not support IPv6.

To check the version of your management node, log in to your management node and view the Element version number in the login banner.

- You have updated your management services bundle to the latest version using Hybrid Cloud Control (HCC). You can access HCC from the following IP: <code><a href="https://<ManagementNodeIP>" class="bare">https://<ManagementNodeIP>;</code>
- 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.

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.

- Storage nodes are running Element 11.3 or later. Use the latest HealthTools to upgrade Element software.

Steps

1. Log in to the management node virtual machine using SSH or console access.
2. Download the management node ISO for NetApp HCI or Element software from the NetApp Support Site to the management node virtual machine.

The name of the ISO is similar to `solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso`

3. Check the integrity of the download by running md5sum on the downloaded file and compare 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-<Element release>-patchX-XX.X.X.XXXX.iso`

4. 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-<Element release>-patchX-XX.X.X.XXXX.iso> /mnt
   ```

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

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

   ```
   sudo umount /mnt
   ```

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

```
sudo rm <path to iso>/solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso
```

7. On an 11.3 or later management node, run the following command to upgrade your management node OS version. The script retains all necessary configuration files after the upgrade, such as Active IQ collector and proxy settings.

```
sudo /sf/rtfi/bin/sfrtfi_inplace file:///upgrade/casper/filesystem.squashfs
sf_upgrade=1
```

   The management node reboots with a new OS after the upgrade process completes.

8. On the 11.3 or later management node, run the `redeploy-mnode` script to retain previous management services configuration settings:

   The script retains previous management services configuration, including configuration from the Active IQ collector service, controllers (vCenters), or proxy, depending on your settings.

```
sudo /sf/packages/mnode/redeploy-mnode -mu <mnode user>
```

Upgrade a management node to version 12.0 from 11.1 or 11.0

You can perform an in-place upgrade of the management node from 11.0 or 11.1 to version 12.0 without needing to provision a new management node virtual machine.

Before you begin

- Storage nodes are running Element 11.3 or later.

  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 version 12.0 does not support IPv6.

  To check the version of your management node, log in to your management node and view the Element version number in the login banner. 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.

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.

Steps

1. Log in to the management node virtual machine using SSH or console access.
2. Download the management node ISO for NetApp HCI or Element software from the NetApp Support Site to the management node virtual machine.

The name of the ISO is similar to `solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso`

3. Check the integrity of the download by running md5sum on the downloaded file and compare 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-<Element release>-patchX-XX.X.X.XXXX.iso
```

4. 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-<Element release>-patchX-XX.X.X.XXXX.iso /mnt
```

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

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

```
sudo umount /mnt
```

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

```
sudo rm <path to iso>/solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso
```

7. Run one of the following scripts with options to upgrade your management node OS version. Only run the script that is appropriate for your version. Each script retains all necessary configuration files after the upgrade, such as Active IQ collector and proxy settings.

   a. 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"
   ```

   b. 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"
   ```

   c. 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"
   ```

   The management node reboots with a new OS after the upgrade process completes.

8. On the 12.0 management node, run the `upgrade-mnode` script to retain previous configuration settings.

   If you are migrating from an 11.0 or 11.1 management node, the script copies the Active IQ collector to the new configuration format.

   a. For a single storage cluster managed by an existing management node 11.0 or 11.1 with persistent volumes:

   ```
   sudo /sf/packages/mnode/upgrade-mnode -mu <mnode user> -pv <true - persistent
   volume> -pva <persistent volume account name - storage volume account>
   ```

   b. For a single storage cluster managed by an existing management node 11.0 or 11.1 with no persistent volumes:

   ```
   sudo /sf/packages/mnode/upgrade-mnode -mu <mnode user>
   ```

c. For multiple storage clusters managed by an existing management node 11.0 or 11.1 with persistent volumes:

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

d. For multiple storage clusters managed by an existing management node 11.0 or 11.1 with no persistent volumes (the `-pvm` flag is just to provide one of the cluster's MVIP addresses):

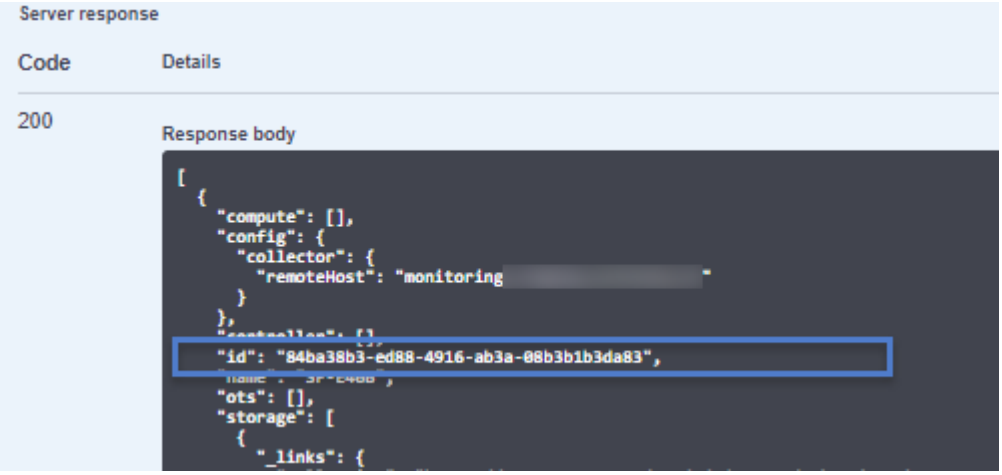
```
sudo /sf/packages/mnode/upgrade-mnode -mu <mnode user> -pvm <mvip for persistent
volumes>
```

9. (For all NetApp HCI installations and SolidFire stand-alone storage installations with NetApp Element Plug-in for vCenter Server) Update the vCenter Plug-in on the 12.0 management node by following the steps in the Upgrade the Element Plug-in for vCenter Server to version 4.4 topic.
10. Use the management node API to add assets:
    a. From a browser, log into the management node REST API UI:
        i. Go to the storage MVIP and log in.
        This action causes certificate to be accepted for the next step.
        ii. Open the REST API UI on the management node:

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

    b. From the management node REST API UI, click **Authorize** or any lock icon and complete the following:
        i. Enter the cluster user name and password.
        ii. Enter the client ID as `mnode-client` if the value is not already populated.
        iii. Copy the token URL string and paste it into another browser tab to initiate a token request.
        iv. Click **Authorize** to begin a session.
        v. Close the window.
    c. Run `GET /assets` to find the base asset ID that you will need for the next steps:
        i. Click **GET /assets**.
        ii. Click **Try it out**.
        iii. Click **Execute**.
        iv. Copy the value for **"id"** for the base asset to your clipboard:
        NOTE: You installation has a base asset configuration that was created during installation or

upgrade.



d. Add a vCenter controller asset for HCI monitoring (NetApp HCI installations only) and Hybrid Cloud Control (for all installations) to the management node known assets:

   i. Click **POST /assets/{asset_id}/controllers** to add a controller sub-asset.

   ii. Click **Try it out**.

   iii. Enter the required payload values as defined in the **Model** tab with type `vCenter` and vCenter credentials.

   iv. Enter the parent base asset ID you copied to your clipboard in the **asset_id** field.

   v. Click **Execute**.

e. (For NetApp HCI only) Add a compute node asset to the management node known assets:

   i. Click **POST/assets/{asset_id}/compute-nodes** to add a compute node sub-asset with credentials for the compute node asset.

   ii. Click **Try it out**.

   iii. In the payload, enter the required payload values as defined in the **Model** tab. Use type `ESXi Host` and remove the `hardware_tag` parameter.

   iv. Enter the parent base asset ID you copied to your clipboard in the **asset_id** field.

   v. Click **Execute**.

Migrating from management node version 10.x to 11.x

If you have a management node at version 10.x, you cannot upgrade from 10.x to 11.x. You can instead use this migration procedure to copy over the configuration from 10.x to a newly deployed 11.1 management node. If your management node is currently at 11.0 or higher, you should skip this procedure. You need management node 11.0 or 11.1 and the latest HealthTools to upgrade Element software from 10.3 + through 11.x.

Steps

1. From the VMware vSphere interface, deploy the management node 11.1 OVA and power it on.
2. Open the management node VM console, which brings up the terminal user interface (TUI).
3. Use the TUI to create a new administrator ID and assign a password.
4. In the management node TUI, log in to the management node with the new ID and password and validate that it works.
5. From the vCenter or management node TUI, get the management node 11.1 IP address and browse to the IP address on port 9443 to open the management node UI.

   ```
   https://<mNode 11.1 IP address>:9443
   ```

6. In vSphere, select **NetApp Element Configuration** > **mNode Settings**. (In older versions, the top-level menu is **NetApp SolidFire Configuration**.)
7. Click **Actions** > **Clear**.
8. To confirm, click **Yes**. The mNode Status field should report Not Configured.

   When you go to the **mNode Settings** tab for the first time, the mNode Status field might display as **Not Configured** instead of the expected **UP**; you might not be able to choose **Actions** > **Clear**. Refresh the browser. The mNode Status field will eventually display **UP**.

9. Log out of vSphere.
10. In a web browser, open the management node registration utility and select **QoSSIOC Service Management**:

    ```
    https://<mNode 11.1 IP address>:9443
    ```

11. Set the new QoSSIOC password.

    The default password is `solidfire`. This password is required to set the new password.

12. Click the **vCenter Plug-in Registration** tab.
13. Select **Update Plug-in**.
14. Enter required values. When you are finished, click **UPDATE**.
15. Log in to vSphere and select **NetApp Element Configuration** > **mNode Settings**.
16. Click **Actions** > **Configure**.
17. Provide the management node IP address, management node user ID (the user name is `admin`), password that you set on the **QoSSIOC Service Management** tab of the registration utility, and

vCenter user ID and password.

In vSphere, the **mNode Settings** tab should display the mNode status as **UP**, which indicates management node 11.1 is registered to vCenter.

18. From the management node registration utility (`https://<mNode 11.1 IP address>:9443`), restart the SIOC service from **QoSSIOC Service Management**.
19. Wait for one minute and check the **NetApp Element Configuration** > **mNode Settings** tab. This should display the mNode status as **UP**.

    If the status is **DOWN**, check the permissions for `/sf/packages/sioc/app.properties`. The file should have read, write, and execute permissions for the file owner. The correct permissions should appear as follows:

    ```
    -rwx------
    ```

20. After the SIOC process starts and vCenter displays mNode status as **UP**, check the logs for the `sf-hci-nma` service on the management node. There should be no error messages.
21. (For management node 11.1 only) SSH into the management node version 11.1 with root privileges and start the NMA service with the following commands:

    ```
    # systemctl enable /sf/packages/nma/systemd/sf-hci-nma.service
    ```

    ```
    # systemctl start sf-hci-nma21
    ```

22. Perform actions from vCenter to remove a drive, add a drive or reboot nodes. This triggers storage alerts, which should be reported in vCenter. If this is working, NMA system alerts are functioning as expected.
23. If ONTAP Select is configured in vCenter, configure ONTAP Select alerts in NMA by copying the `.ots.properties` file from the previous management node to the management node version 11.1 `/sf/packages/nma/conf/.ots.properties` file, and restart the NMA service using the following command:

    ```
    systemctl restart sf-hci-nma
    ```

24. Verify that ONTAP Select is working by viewing the logs with the following command:

    ```
    journalctl -f | grep -i ots
    ```

25. Configure Active IQ by doing the following:

a. SSH in to the management node version 11.1 and go to the `/sf/packages/collector` directory.

b. Run the following command:

```
sudo ./manage-collector.py --set-username netapp --set-password --set-mvip <MVIP>
```

c. Enter the management node UI password when prompted.

d. Run the following commands:

```
./manage-collector.py --get-all
```

```
sudo systemctl restart sfcollector
```

e. Verify `sfcollector` logs to confirm it is working.

26. In vSphere, the **NetApp Element Configuration** > **mNode Settings** tab should display the mNode status as **UP**.
27. Verify NMA is reporting system alerts and ONTAP Select alerts.
28. If everything is working as expected, shut down and delete management node 10.x VM.

Reconfigure authentication using the management node REST API

You can keep your existing management node if you have sequentially upgraded (1) management services and (2) Element storage. If you have followed a different upgrade order, see the procedures for in-place management node upgrades.

Before you begin

- You have updated your management services to 2.10.29 or later.
- Your storage cluster is running Element 12.0 or later.
- Your management node is 11.3 or later.
- You have sequentially updated your management services followed by upgrading your Element storage. You cannot reconfigure authentication using this procedure unless you have completed upgrades in the sequence described.

Steps

1. Open the management node 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. Click **Authorize** to begin a session.
3. From the REST API UI, click **POST /services/reconfigure-auth**.
4. Click **Try it out**.
5. For the **load_images** parameter, select `true`.
6. Click **Execute**.

    The response body indicates that reconfiguration was successful.

Find more information

- NetApp HCI Documentation Center
- NetApp HCI Resources Page