Post-deployment tasks

HCI

NetApp
December 05, 2020

Table of Contents

Post-deployment tasks

Post-deployment tasks

Depending on your choices during the deployment process, you need to complete some final tasks before your NetApp HCI system is ready for production use, such as updating firmware and drivers and making any needed final configuration changes.

Find more information

- NetApp HCI Documentation Center
- SolidFire and Element Software Documentation Center

Supported networking changes

After you deploy NetApp HCI, you can make limited changes to the default networking configuration. However, certain settings are required for smooth operation and proper network detection. Changing these settings will cause unexpected behavior, and might prevent you from expanding compute and storage resources.

After you deploy your system, you can make the following changes to the default network configuration in VMware vSphere as dictated by your network requirements:

- Change vSwitch names
- Change port group names
- Add and remove additional port groups
- Change the vmnic interface failover order for any additional port groups you have added

H300E, H500E, H700E and H410C compute nodes

NetApp HCI expects the following network configuration for H300E, H500E, H700E and H410C nodes.

The following is a six-interface configuration with VMware vSphere Distributed Switching (VDS). This configuration is only supported when used with VMware vSphere Distributed Switches, and requires VMware vSphere Enterprise Plus licensing.

Network function	vmkernel	vmnic (physical interface)
Management	vmk0	vmnic2 (Port A), vmnic3 (Port B)

Network function	vmkernel	vmnic (physical interface)
iSCSI-A	vmk1	vmnic5 (Port E)
iSCSI-B	vmk2	vmnic1 (Port D)
vMotion	vmk3	vmnic4 (Port C), vmnic0 (Port F)

The following is a six-interface configuration with VMware vSphere Standard Switching (VSS). This configuration uses VMware vSphere Standard Switches (VSS).

Network function	vmkernel	vmnic (physical interface)
Management	vmk0	vmnic2 (Port A), vmnic3 (Port B)
iSCSI-A	vmk2	vmnic1 (Port E)
iSCSI-B	vmk3	vmnic5 (Port D)
vMotion	vmk1	vmnic4 (Port C), vmnic0 (Port F)

The following is a two-interface configuration. This configuration is only supported when used with VMware vSphere Distributed Switches (VDS), and requires VMware vSphere Enterprise Plus licensing.

Network function	vmkernel	vmnic (physical interface)
Management	vmk0	vmnic1 (Port D), vmnic5 (Port E)
iSCSI-A	vmk1	vmnic1 (Port E)
iSCSI-B	vmk2	vmnic5 (Port D)
vMotion	vmk3	vmnic1 (Port C), vmnic5 (Port F)

H610C compute nodes

NetApp HCI expects the following network configuration for H610C nodes.

This configuration is only supported when used with VMware vSphere Distributed Switches (VDS), and requires VMware vSphere Enterprise Plus licensing.

Ports A and B are unused on the H610C.

Network function	vmkernel	vmnic (physical interface)
Management	vmk0	vmnic2 (Port C), vmnic3 (Port D)
iSCSI-A	vmk1	vmnic3 (Port D)
iSCSI-B	vmk2	vmnic2 (Port C)
vMotion	vmk3	vmnic2 (Port C), vmnic3 (Port D)

H615C compute nodes

NetApp HCI expects the following network configuration for H615C nodes.

This configuration is only supported when used with VMware vSphere Distributed Switches (VDS), and requires VMware vSphere Enterprise Plus licensing.

Network function	vmkernel	vmnic (physical interface)
Management	vmk0	vmnic0 (Port A), vmnic1 (Port B)
iSCSI-A	vmk1	vmnic0 (Port B)
iSCSI-B	vmk2	vmnic1 (Port A)
vMotion	vmk3	vmnic0 (Port A), vmnic1 (Port B)

Find more information

- NetApp HCI Documentation Center
- SolidFire and Element Software Documentation Center

Disable the `smartd` service on NetApp HCI compute nodes

By default, the `smartd` service periodically polls the drives in your compute nodes. You should disable this service on all compute nodes after you deploy NetApp HCI.

Steps

1. Using SSH or a local console session, log in to VMware ESXi on the compute node using root credentials.
2. Stop the running `smartd` service:

   ```
   /etc/init.d/smartd stop
   ```

3. Prevent the `smartd` service from starting at boot:

   ```
   chkconfig smartd off
   ```

4. Repeat these steps on the rest of the compute nodes in your installation.

Find more information

- Turn off the smartd service in VMware ESXi
- VMware KB article 2133286

Keep VMware vSphere up to date

After deploying NetApp HCI, you should use VMware vSphere Lifecycle Manager to apply the latest security patches for the version of VMware vSphere used with NetApp HCI.

Use the Interoperability Matrix Tool to ensure that all versions of software are compatible. See the VMware vSphere Lifecycle Manager documentation for more information.

Find more information

- NetApp HCI Documentation Center
- SolidFire and Element Software Documentation Center

Install GPU drivers for GPU-enabled compute nodes

Compute nodes with NVIDIA graphics processing units (GPUs), like the H610C, need NVIDIA software drivers installed in VMware ESXi so that they can take advantage of the increased processing power. After deploying compute nodes with GPUs, you need to perform these steps on each GPU-enabled compute node to install the GPU drivers in ESXi.

Steps

1. Open a browser and browse to the NVIDIA licensing portal at the following URL:

   ```
   https://nvid.nvidia.com/dashboard/
   ```

2. Download one of the following driver packages to your computer, depending on your environment:

vSphere version	Driver package
vSphere 6.5	`NVIDIA-GRID-vSphere-6.5-410.92-410.91-412.16.zip`
vSphere 6.7	`NVIDIA-GRID-vSphere-6.7-410.92-410.91-412.16.zip`

3. Extract the driver package on your computer.

   The resulting .VIB file is the uncompressed driver file.

4. Copy the `.VIB` driver file from your computer to ESXi running on the compute node. The following example commands for each version assume that the driver is located in the `$HOME/NVIDIA/ESX6.x/`

directory on the management host. The SCP utility is readily available in most Linux distributions, or available as a downloadable utility for all versions of Windows:

ESXi version	Description
ESXi 6.5	`scp $HOME/NVIDIA/ESX6.5/NVIDIA**.vib root@<ESXi_IP_ADDR>:/.`
ESXi 6.7	`scp $HOME/NVIDIA/ESX6.7/NVIDIA**.vib root@<ESXi_IP_ADDR>:/.`

5. Use the following steps to log in as root to the ESXi host and install the NVIDIA vGPU Manager in ESXi.

   a. Run the following command to log in to the ESXi host as the root user:

   ```
   ssh root@<ESXi_IP_ADDRESS>
   ```

   b. Run the following command to verify that no NVIDIA GPU drivers are currently installed:

   ```
   nvidia-smi
   ```

   This command should return the message `nvidia-smi: not found`.

   c. Run the following commands to enable maintenance mode on the host and install the NVIDIA vGPU Manager from the VIB file:

   ```
   esxcli system maintenanceMode set --enable true
   esxcli software vib install -v /NVIDIA**.vib
   ```

   You should see the message `Operation finished successfully`.

   d. Run the following command and verify that all eight GPU drivers are listed in the command output:

   ```
   nvidia-smi
   ```

   e. Run the following command to verify that the NVIDIA vGPU package was installed and loaded correctly:

   ```
   vmkload_mod -l | grep nvidia
   ```

   The command should return output similar to the following: `nvidia 816 13808`

f. Run the following command to reboot the host:

```
reboot -f
```

g. Run the following command to exit maintenance mode:

```
esxcli system maintenanceMode set --enable false
```

6. Repeat steps 4-6 for any other newly deployed compute nodes with NVIDIA GPUs.
7. Perform the following tasks using the instructions in the NVIDIA documentation site:
   a. Install the NVIDIA license server.
   b. Configure the virtual machine guests for NVIDIA vGPU software.
   c. If you are using vGPU-enabled desktops in a virtual desktop infrastructure (VDI) context, configure VMware Horizon View for NVIDIA vGPU software.

Find more information

- NetApp HCI Documentation Center
- SolidFire and Element Software Documentation Center

Configure Fully Qualified Domain Name web UI access

NetApp HCI with Element 12.2 or later enables you to access storage cluster web interfaces using the Fully Qualified Domain Name (FQDN). If you want to use the FQDN to access web user interfaces such as the Element web UI, per-node UI, or management node UI, you must first add a storage cluster setting to identify the FQDN used by the cluster. This enables the cluster to properly redirect a login session and improves integration with external services such as key managers and identity providers for multi-factor authentication.

What you'll need

- This feature requires Element 12.2 or later and management services version 2.15 or later.
- To use REST APIs, you must have deployed a management node running version 11.5 or later.

Steps

1. Ensure that the Element storage nodes and the management node have DNS configured correctly for the network environment so that FQDNs in the environment can be resolved. To set DNS, go to the per-node UI for storage nodes and to the management node, then select **Network Settings** > **Management Network**.

a. Per-node UI for storage nodes: `https://<storage_node_management_IP>:442`

b. Per-node UI for the management node: `https://<management_node_IP>:442`

2. Access the Element API and create the following cluster interface preference using the `CreateClusterInterfacePreference` API method, inserting the cluster MVIP FQDN for the preference value:

   - Name: `mvip_fqdn`
   - Value: <Fully Qualified Domain Name for the Cluster MVIP>

   For example, where the FQDN is `storagecluster.my.org`:

   ```
   https://<Cluster_MVIP>/json-rpc/12.2?method=CreateClusterInterfacePreference&name=mvip_fqdn&value=storagecluster.my.org
   ```

3. Change the management node settings using the REST API on the management node:

   a. Access the REST API UI for the management node by entering the management node IP address followed by `/mnode/2/`. For example:

   ```
   https://[management node IP]/mnode/2/
   ```

   b. Click **Authorize** or any lock icon and enter the cluster user name and password.

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

   d. Click **Authorize** to begin a session and then close the window.

   e. From the server list, select `mnode2`.

   f. Click **GET /settings**.

   g. Click **Try it out**.

   h. Click **Execute**.

   i. Record any proxy settings reported in the response body.

   j. Click **PUT /settings**.

   k. Click **Try it out**.

   l. In the request body area, enter the management node FQDN as the value for the `mnode_fqdn` parameter.

   m. Enter any proxy setting values you recorded earlier in the remaining parameters in the request body. If you leave the proxy parameters empty or do not include them in the request body, existing proxy settings will be removed.

   n. Click **Execute**.

Find more information

- CreateClusterInterfacePreference API information in the SolidFire and Element Documentation Center

Access NetApp Hybrid Cloud Control

NetApp Hybrid Cloud Control enables you to manage NetApp HCI. You can upgrade management services and other components of NetApp HCI and expand and monitor your installation. You log in to NetApp Hybrid Cloud Control by browsing to the IP address of the management node.

What you'll need

You have upgraded your management services to at least version 2.1.326. NetApp Hybrid Cloud Control is not available in earlier service bundle versions. For information about the current service bundle version, see the Management Services Release Notes.

Steps

1. Open a web browser and browse to the IP address of the management node. For example:

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

2. Log in to NetApp Hybrid Cloud Control by providing the NetApp HCI storage cluster administrator credentials.

   The NetApp Hybrid Cloud Control interface appears.

Find more information

- NetApp HCI Documentation Center
- SolidFire and Element Software Documentation Center