Updating the c7000 enclosure

Updating the Onboard Administrators

Prerequisites

You have access to the Customer Intent Document (CID) for your solution.

Procedure

1. On the installation system, open a web browser to the HPE OneView appliance address referenced in the CID tab:

   16_OneView_VMw > **OneView VM Solution Management Network IP Address**.
2. Log in using the credentials referenced in the CID.

   Username: Administrator

   Password: See the CID tab **16_OneView_VMw** > **OneView** > **Administrator**
3. In the top left corner, click **HPE OneView** > **Logical Enclosures**.
4. In the right pane, click **Actions** > **Update firmware**.
5. Select the custom SPP as the Firmware Baseline.
6. In the **Update firmware for** field, select **Onboard Administrators only**.
7. Click **OK**.

Updating the Virtual Connect modules

About this task

NOTE:

During the update, the enclosure may not be accessible on the network.

Procedure

1. On the installation system, open a web browser to the HPE OneView appliance address referenced in the CID tab:

   16_OneView_VMw > **OneView VM Solution Management Network IP Address**.
2. Log in using the credentials referenced in the CID.

   Username: **Administrator**

   Password: See the CID tab **16_OneView_VMw** > **OneView** > **Administrator**
3. In the top left corner, click **HPE OneView** > **Logical Interconnects**.
4. Click **Actions** > **Update Firmware**.
5. In the Update Action menu, select **Update firmware (Stage + Active)**.
6. Select the custom SPP as the firmware baseline.
7. For both the Ethernet and Fiber Channel activation, select **Serial**.

   Keep the delay time to the default, 5 minutes.
8. Click **OK**.

Updating the Fibre Channel Switch

Prerequisites

You have access to the Customer Intent Document (CID) for your product.

NOTE:

Link loss may occur during the update.

Procedure

1. Open an SSH connection to the SAN switch being configured.

   The IP address can be found in the CID tab labeled **20_SANSwitches** > **Management IP Address**.
2. Log in using the administrator credentials:

   Username: See the CID tab labeled **20_SANSwitches** > **admin Username.**.

   Password: See the CID tab labeled **20_SANSwitches** > **admin Password.**
3. To verify the current switch version, enter **`firmwareshow`**.

   To upload the firmware, use either the FTP or the USB method.

Uploading Firmware using FTP Method

Procedure

1. For FTP Server configuration information, see "**Configuring the FTP Server** on page 70".
2. Download and copy the firmware folder v8.0.2a to the FTP server.
   For example, v8.0.2a
3. Enter the following commands to download the firmware to the switch.

   Provide the IP address of the FTP server, FTP user account, and the location of the firmware in the FTP server.

   Replace **`<version>`** with the appropriate version. For example: **`v7.4.1c`**.

```
# firmwaredownload
Server Name or IP Address: 172.28.11.254
User Name: Administrator
File Name: <Ftp_Repo>/v8.0.2a
Network Protocol(1-auto-select, 2-FTP, 3-SCP, 4-SFTP) [1]: 2
Password: ***
Server IP: 172.28.11.254, Protocol IPv4
Checking system settings for firmwaredownload... System settings check passed.

You can run firmwaredownloadstatus to get the status of this command.

This command will cause a warm/non-disruptive boot but will require that
existing telnet, secure telnet or SSH sessions be restarted.

Do you want to continue (Y/N) [Y]: Y
Firmware is being downloaded to the switch. This step may take up to 30
minutes.
Preparing for firmwaredownload... Start to install packages...
```

4. Reconnect to the SSH session.

5. Enter **firmwaredownloadstatus** to check the status of the upgrade.
6. Enter **firmwareshow** to verify the version of the firmware on the switch after the update is complete.

Uploading Firmware using USB Method

NOTE:

Only a Brocade-supplied USB device is supported for the firmware upgrade. If a Brocade-supplied USB device is unavailable, use the FTP method.

Procedure

1. Copy the firmware to the default firmware directory in the USB file system.
2. Connect the drive to one of the USB ports on the switch.
3. To enable the USB drive in the switch, enter **usbstorage -e**.
4. To verify the contents of the USB drive, enter **usbstorage -l**.
5. Ensure the required firmware version is listed.
6. Download the firmware from the USB drive to the switch to install it.

   When providing a path to the firmware image on the USB drive, only the relative or absolute path can be specified.

   Replace **<version>** with the appropriate firmware version. For example: **v7.4.1c**.

   a. Downloading from the USB drive using the relative path:

   ```
   # firmwaredownload –U v8.0.2a
   ```

   b. Downloading from the USB drive using the absolute path:

   ```
   # firmwaredownload –U /usb/usbstorage/brocade/firmware/v8.0.2a
   ```

   c. Result

   ```
   Firmware filename: v8.0.2a
   Checking system settings for firmwaredownload... System checkings check
   passed.
   You can run firmwaredownloadstatus to get the status of the command.

   This command will cause a warm/non-disruptive boot but will require that
   existing telnet, secure telnet or SSH sessions be restarted.


   Do you want to continue (Y/N) [y]: y
   Firmware is being downloaded to the switch. This step may take up to 30
   minutes. Preparing for firmwaredownload...
   Start to install packages... dir-1.0.5-5
   ################################## [ 100% ]
   ldconfig-2.16.2-4
   ################################## [ 100% ]
   ...
   ```

   The firmware upload and installation takes approximately 20 minutes.
7. Restart the SSH session.
8. Check the status of the firmware installation.

```
# firmwaredownloadstatus
[1]: Thu Apr 21 07:48:25 2017
Firmware is being downloaded to the switch. This step may take up to 30
minutes.

[2]: Thu Apr 21 07:53:35 2017
Firmware has been downloaded to the secondary partition of the switch.

[3]: Thu Apr 21 07:55:36 2017
The firmware commit operation has started. This may take up to 10 minutes.

[4]: Thu Apr 21 07:59:35 2017
The commit operation has completed successfully.

[5]: Thu Apr 21 07:59:35 2017
Firmwaredownload command has completed successfully. Use firmwareshow to
verify the firmware versions.
```

9. Verify the version of the firmware on the switch after the update is complete.

```
# firmwareshow
Appl    Primary/Secondary Versions
------------------------------
FOS      v8.0.2a
      v8.0.2a
```

Updating 3PAR

About this task

NOTE:

The estimated time to update 3PAR depends on the size of the storage array, including the number of cages, physical disks, and so on. The update process must be performed for each storage array in the solution.

NOTE:

Back up the 3PAR StoreServ configuration details before performing the upgrade process. For more details on the procedure to back up the configuration files, refer to the respective document.

Hewlett Packard Enterprise recommends that you review the release notes of a given version and understand the implications before starting the upgrade process.

Procedure

1. On the Installation System menu, open the vSphere .NET Client.
2. Navigate to **Hosts and Clusters**.
3. In the left pane, select the management cluster.
4. In the right, navigate to **Configuration** > **Storage**.
5. Right-click a datastore to which the Solution Management and/or Troubleshooting VM has access. For example, sms01-localdatastore
6. Select **Browse Datastore**.
7. In the top navigation bar, click the green up arrow to upload a file.
8. Navigate to and select the 3PAR Management Console file:

   IMC 4.7.3 QR482-11188.iso
9. Repeat the steps for the 3PAR StoreServe Management Console file.

3PAR_StoreServ_Mgmt_Console_4.7.3_SW_QR482-11188.iso

10. Repeat the steps for the 3PAR Inform OS file.

    3PAR_Inform_OS_3.2.2_MU4_CLI_SNMP_SW_QR482-110192.iso

Updating InForm Management Console

About this task

NOTE:

During the update, there is no access to the InForm Management Console (IMC).

Procedure

1. On the Installation System, open the vSphere Web Client to CID tab **12_vSphereSettings** > **vCenter Server Solution Management IP Address**.
2. Log in using the username CID tab **12_vSphereSettings** > **vCenter Single Sign On Administrator** and password CID tab **12_vSphereSettings** > **vCenter Single Sign On Password**.
3. In the left pane, right-click the Solution Management VM (smgmt01) or the VM being configured (Troubleshooting VMs as well) and select **Edit Settings**.
   a. Expand the **CD/DVD drive 1** menu and click **Browse**.
   b. Navigate to and select the IMC .ISO file. Click **OK**.
   c. Ensure the **Connected** checkbox is checked.
   d. Click **OK**.
4. Open a RDP session and log into the Solution Management VM (smgmt01).
5. Once logged in, open File Explorer and navigate to the **D:/windows** directory.
6. Double-click **setup.exe.** A pre-installation dialog displays.
7. On the Introduction screen, click **Next**.
8. On the Choose Install Folder screen, leave the default and click **Next**.
9. On the Pre-Installation Summary screen, verify the details and click **Install**. The installation takes a few minutes.
10. Once the installation is complete, click **Done**.
11. Repeat this process for the Troubleshooting VMs. Ensure this process is completed for all applicable VMs.

Installing StoreServ Management Console

Procedure

1. Return to the vSphere Web Client.
2. In the left pane, right-click the Solution Management VM (smgmt01) and select **Edit Settings**.
   a. Expand the CD/DVD drive 1 menu and click **Browse**.
   b. Navigate to and select the SSMC ISO file.
   c. Click **OK**
   d. Ensure that the **Connected** check box is checked.
   e. Click **OK**.
3. Open an RDP session.
4. Log in to the Solution Management VM (smgmt01).
5. Open File Explorer and navigate to the **D:/**.
6. Double-click the StoreServ Management Console file.

   HPSSMC-3.0.0.22054-win64.exe

   A preinstallation dialog displays.

7. Select the appropriate language and click **OK**.
8. On the Introduction screen, click **Next**.
9. Read and accept the License Agreement to continue.

   Click **OK**.
10. Click **Next**.
11. On the previous SSMC Data Option screen, select **Yes** and click **Next**.
12. On the Choose Installation Folder screen, leave the default value, and click **Next**.
13. On the Configure SSMC Server Secure Port screen, click **Next**.
14. On the Pre-Installation Summary screen, verify the details and click **Install**.

    The installation takes a few minutes.
15. Review the Important Firewall Information and click **Next** to continue.
16. Once the installation is complete, click **Done**.
17. Repeat this procedure for the Troubleshooting VMs.

    Ensure that this process is completed for all applicable VMs.

Updating 3PAR Command Line Interface (CLI)

NOTE:

During the update, network access to the 3PAR CLI will be lost.

The update may not completely remove the previous version of 3PAR CLI from the system.

The entry "3PAR CLI" may remain in Programs and Features, but can be safely ignored.

Procedure

1. Log in to the vSphere Web Client.
2. In the left pane, right-click the Solution Management VM (smgmt01) and select **Edit Settings**.

   This includes VMs being configured and Troubleshooting VMs.
3. Select **Edit Settings**.
   a. Expand the **CD/DVD drive 1** menu and click **Browse**.
   b. Navigate to and select the 3PAR CLI ISO file and click **OK**.
   c. Ensure that the **Connected** check box is checked and click **OK**.
4. Open an RDP session and log in to the Solution Management VM (smgmt01).
5. Open File Explorer and navigate to the directory:

   D:/cli/windows
6. Double-click **setup.exe**.

   A preinstallation dialog displays.
7. On the Introduction screen, click **Next**.
8. On the Choose Install Folder screen, click **Next**.

   Leave the default value automatically assigned.
9. Read and verify the details on the Pre-Installation Summary screen.
10. Click **Install**.

    The installation takes a few minutes.
11. Once the installation is complete, click **Done**.

    Repeat this procedure for the Troubleshooting VMs and all applicable VMs.