Emulex® OneCommand® Manager for VMware vCenter

User Guide
Release 12.4

Table of Contents

Chapter 1: Introduction

Emulex® OneCommand® Manager for VMware vCenter is a comprehensive management utility for Emulex adapters that provides a powerful, centralized adapter management suite for the VMware vCenter management console. This comprehensive solution builds upon standard Emulex Common Information Model (CIM) management providers and advanced functionality delivered with the OneCommand Manager application to present native configuration management, status monitoring, and online maintenance of Emulex adapters in VMware ESXi environments, using a graphical interface (GUI) or a command line interface (CLI).

1.1 Compatibility

For supported versions of operating systems, platforms, and adapters, go to www.broadcom.com.

OneCommand Manager for VMware vCenter is supported on the following Windows operating systems:

- Windows 10
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019

See Table 1 to determine the support provided by the CIM Provider.

NOTE: Illustrations in this guide are for illustrative purposes only. Your system information can vary.

Table 1: Support Provided by Emulex CIM Provider Versions lists the Emulex OneCommand Manager application support provided by the Emulex CIM Provider package and the OneCommand Manager for VMware vCenter in each package. The Emulex CIM Provider packages can be downloaded from www.broadcom.com.

Table 1: Support Provided by Emulex CIM Provider Versions

Emulex OneCommand Manager Application Features	ELX CIM Provider Package v12.4	OneCommand Manager for VMware vCenter v 12.4
Discover virtual ports connected to a port	x	x
View virtual port information in a cluster (host-centric mode)	N/A	x
Discover hosts, adapters, targets, and logical unit numbers (LUNs) for selected ESXi hosts	x	x
Discover hosts and adapters for selected ESXi fabrics	x	x
View the firmware version	x	x
View the boot code version	x	x
Update firmware and boot code on a single adapter	x	x
Update firmware and boot code on a per-fabric basis	N/A	x
Change the World Wide Port Name (WWPN) or World Wide Name (WWN)	x	x
Locate adapters with beaconing	x	x
View PCI Express (PCIe) registers	x	x

Table 1: Support Provided by Emulex CIM Provider Versions (Continued)

Emulex OneCommand Manager Application Features	ELX CIM Provider Package v12.4	OneCommand Manager for VMware vCenter v 12.4
D_Port (also referred to as ClearLink®) test, for adapters connected to D_Port-enabled Brocade® switches only (Not supported on LPe12000-series adapters)	x	x
DHCHAP authentication	x	x
PCI loopback test	x	x
Internal and external loopback test	x	x
Echo test for LPe12000-series adapters	x	x
Power-on self-test (POST) for LPe12000-series adapters	N/A	x
Batch-update firmware and boot code to multiple adapters	N/A	x
Enable and disable ports	x	x
Get driver parameters (global and port)	x	x
Set global driver parameters to adapters	x	x
Set port driver parameters to adapters	x	x
Trunking (also called FC port aggregation)	x	x
Target and LUN information	x	x
Reset port	x	x
View vital product data (VPD)	x	x
Display flash contents (wakeup parameters and the flash load list) for ports	x	x
Export storage area network (SAN) configuration information at the cluster and host level	N/A	x
Perform the diagnostic dump at the adapter and port levels	x	x

1.2 Abbreviations

AL_PA	Arbitrated Loop Physical Address
BIOS	basic input/output system
BOFM	BladeCenter Open Firmware Manager
CA	certificate authority
CIM	Common Interface Model
CIN	Cisco, Intel, Nuova (Data Center Bridging Exchange)
CLI	command line interface
CLP	command line protocol
CRC	cyclic redundancy check
CSR	certificate signing request
CSV	comma-separated values
DHCHAP	Diffie-Hellman Challenge Handshake Authentication Protocol
DHCP	Dynamic Host Control Protocol
DNS	domain name system or domain name server
DOCSIS®	Data Over Cable Service Interface Specification
EC	engineering change
FA-PWWN	Fabric Assigned Port World Wide Name
FC	Fibre Channel
FCF	Fibre Channel over Ethernet Forwarder
FCP	Fibre Channel Protocol
FEC	forward error correction
FPMA	fabric-assigned MAC address
FW	firmware
Gb	gigabit
Gb/s	gigabits per second
GFO	Get Fabric Object
GUI	graphical user interface
HBA	host bus adapter
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IEEE	Institute of Electrical and Electronics Engineers
I/O	input/output
IP	Internet Protocol
IPL	initial program load
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
JEDEC ID	Joint Electron Device Engineering Council identification code
KB	Kilobyte (1024 bytes)
LAN	local area network
LIP	Loop Initialization Primitive
LUN	logical unit number

MAC	media access control
MB	megabyte
Mb	megabit
Mb/s	megabits per second
MN	manufacturer ID
MTU	maximum transmission unit
N/A	not applicable
NOS	network operating system
NVRAM	nonvolatile random access memory
OAS	Optimized Access Storage
OS	operating system
OUI	organizationally unique identifier
PCI	Peripheral Component Interconnect (interface)
PCIe	PCI Express
POST	power-on self-test
QoS	Quality of Service
RFC	Request for Comments
Rx	receive
SAN	storage area network
SCSI	Small Computer System Interface
SFCB	Small Footprint CIM Broker
SFP	small form-factor pluggable
SLI®	Service Level Interface
SR-IOV	Single Root input/output virtualization
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
Tx	transmit
ULP	Upper Layer Protocol
URL	Uniform Resource Locator
vCSA	VMware for vCenter Server Virtual Appliance
VF	virtual function
VLAN	virtual local area network
VLAN ID	VLAN identifier
VM	virtual machine
VMID	virtual machine ID
VM UUID	VM universal unique identifier
VPD	vital product data
vPort	virtual port
WLAN	wireless LAN
WWN	World Wide Name
WWNN	World Wide Node Name

WWPN	World Wide Port Name
XML	Extensible Markup Language

Chapter 2: Installing and Enabling OneCommand Manager for VMware vCenter

OneCommand Manager for VMware vCenter provides real-time management as a plug-in through VMware vCenter.

NOTE: System performance is directly influenced by the speed and efficiency of the underlying network infrastructure.

2.1 Hardware Requirements

- Physical or virtual (x86 or x86_64) servers with a minimum RAM of 2 GB and 250 GB of disk space.

2.2 Software Requirements

- Operating system – Windows 10, Windows Server 2012 (64 bit), and Windows Server 2012 R2, Windows Server 2016, and Windows Server 2019
- Adobe Flash Player 11.2 or later

NOTE: On the system where OneCommand Manager for VMware vCenter is installed, make sure that the port numbers configured during the installation are open and dedicated to the OneCommand Manager for VMware vCenter Server only. No other service should be listening on this port.

- Emulex CIM Provider Package version 12.x

NOTE: Version 12.x packages are not compatible with the 11.1 or earlier versions of Emulex software.

- Driver and firmware requirements

  Go to www.broadcom.com for the latest compatible driver and firmware versions.

2.3 Installing OneCommand Manager for VMware vCenter

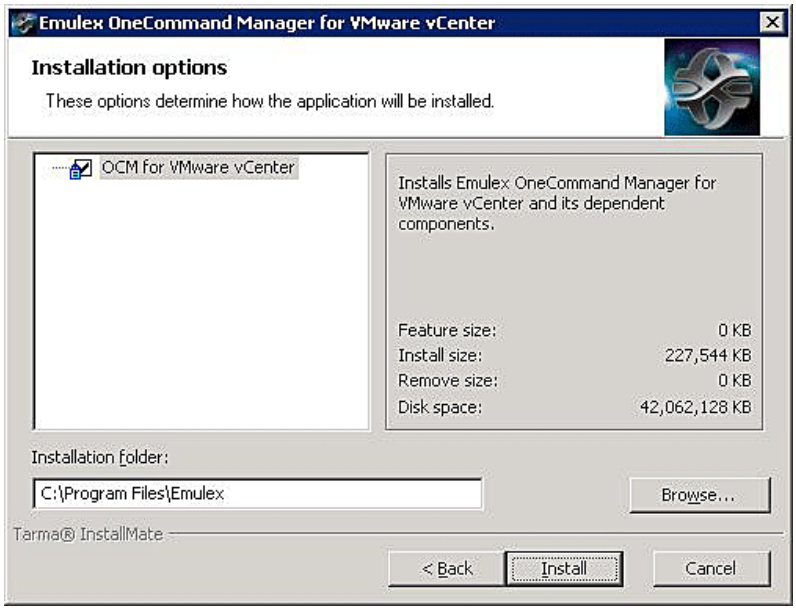
The Emulex CIM Provider must be installed on your ESXi host before installing OneCommand Manager for VMware vCenter. For more information on installing the CIM Provider, refer to the *CIM Provider Package Installation Guide* available on www.broadcom.com.

To install OneCommand Manager for VMware vCenter in Windows, perform these steps:

1. Go to www.broadcom.com to download the `ELXOCM-VMware-vCenter-<version>-Setup.exe` installation file to your system.
2. Navigate to the system directory to which you downloaded the file.
3. Double-click `ELXOCM-VMware-vCenter-<version>-Setup.exe`.

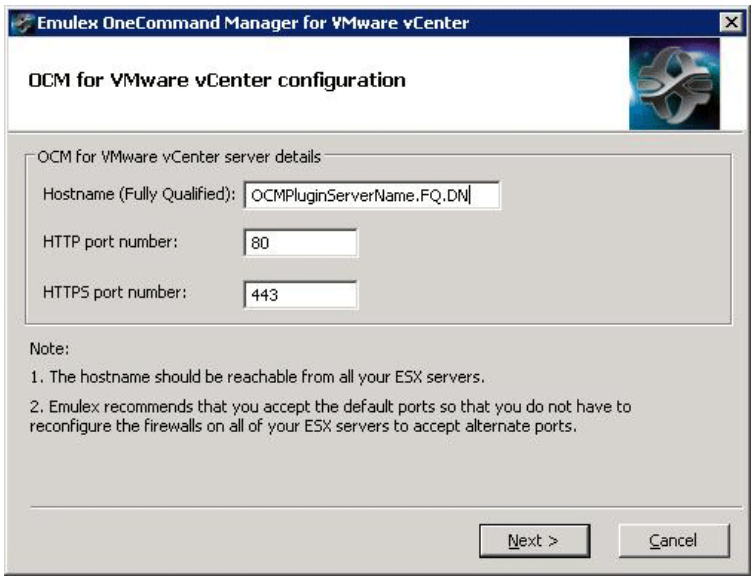
   The **OneCommand Manager for VMware vCenter** window appears.
4. Click **Next**. The **Installation options** window with the default Installation folder appears (Figure 1).

Figure 1: Installation options Window



5. Ensure that **OCM for VMware vCenter** is selected.
6. Program files install by default to `C:\Program Files\Emulex`. To change this location, click **Browse** and navigate to where you want the program files to reside.
7. Click **Install**. The **Operation in progress** window appears. When the process is complete, the **OCM for VMware vCenter configuration** window appears (Figure 2).

Figure 2: OCM for VMware vCenter configuration Window

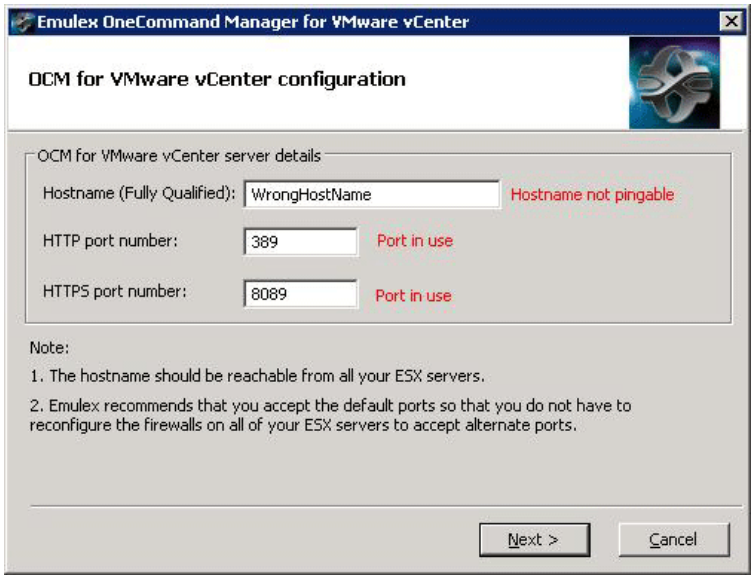


Default port numbers for OneCommand Manager for VMware vCenter Server are displayed.

NOTE: The Windows firewall setting must allow incoming connections on the HTTP and HTTPS ports that you configure here.

If the port numbers are already in use, a popup appears next to the port number (Figure 3).

Figure 3: OCM for VMware vCenter configuration Window with Port in use Popup



8. Click **Next**. The **Operation in progress** window appears. When the installation process is complete, a message prompts you to launch the registration utility.
9. Click **Yes**. The **Register/Unregister** dialog appears in a new browser window (Figure 4).

Figure 4: Register/Unregister Dialog

10. Enter the following details of the vCenter Server:
    - **vCenter Server Name** – The IP address of the vCenter Server.
    - **vCenter Server HTTPS Port** – The HTTPS port number of the vCenter Server.

NOTE: The vCenter Server HTTPS port is 443 by default. You can change this value if you have configured a different HTTPS port while installing the vCenter.

- **Username** – The user name with required privileges.
- **Password** – The user password.

11. Click **Register** to register OneCommand Manager for VMware vCenter with a new vCenter Server.

NOTE:

- You can unregister an existing OneCommand Manager for VMware vCenter by clicking **Unregister**.
- If you change the host name of the machine that hosts the vCenter Server, you must re-install the vCenter Server and re-register.

12. When the operation is successful, a message is displayed. Click **OK**.
13. Close the browser window. The **Installation completed** window appears.
14. Click **Finish**. The **OneCommand Manager for VMware vCenter Registration** icon is created on the desktop. You do not need to reboot the system.

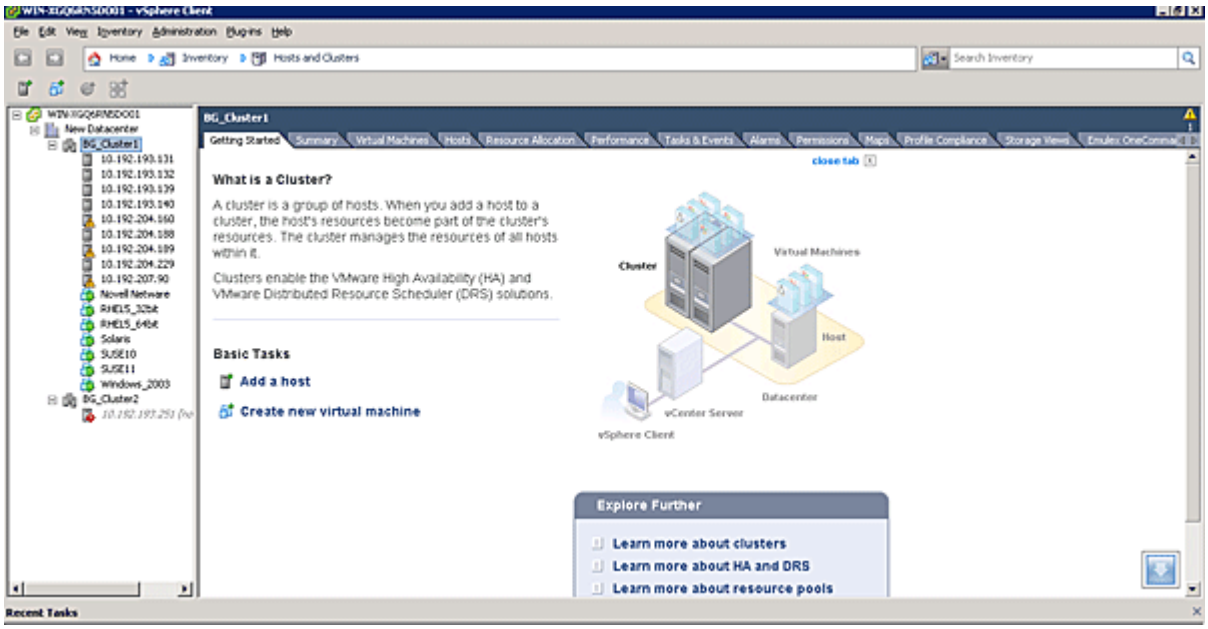
2.3.1 Verifying the OneCommand Manager for VMware vCenter Installation

To verify the OneCommand Manager for VMware vCenter installation, perform these steps:

1. Log on to the vCenter Server.
2. Enter the IP address and credentials of the vCenter Server where OneCommand Manager for VMware vCenter is registered.

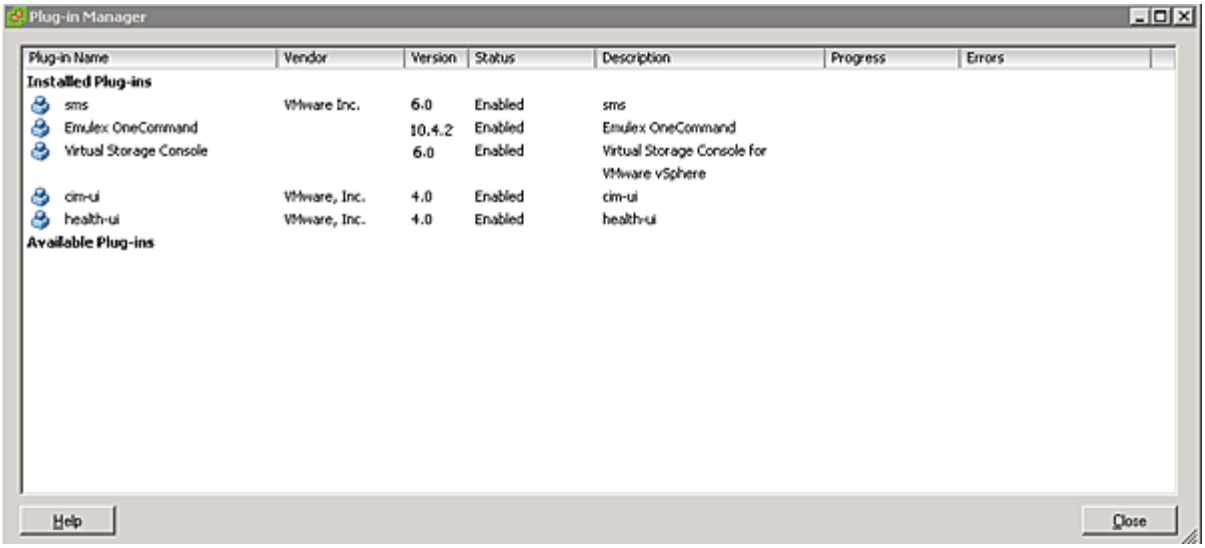
   The vCenter Server appears. (Figure 5).

Figure 5: VMware vCenter Server–Getting Started Tab



3. In the VMware vCenter Server, select **Plug-ins** from the menu bar and select **Manage Plug-ins**. The **Plug-in Manager** window appears (Figure 6).

Figure 6: Plug-in Manager Window



4. In the **Plug-in Manager** window, note the status of OneCommand Manager for VMware vCenter (Emulex OneCommand). If the OneCommand Manager for VMware vCenter installation is complete, the status of Emulex OneCommand is enabled by default.

2.4 Enabling ESXi Management

This section describes enabling OneCommand Manager for VMware vCenter.

NOTE: Refer to the VMware vCenter guide on the VMware website for information on creating a user with required privileges and changing access permissions for a user in the Active Directory.

2.4.1 Requirements

Only a user with these specific privileges can read and perform active management in OneCommand Manager for VMware vCenter:

- **Extension.Register extension** to register OneCommand Manager for VMware vCenter using the registration utility.
- **Extension.Unregister extension** to unregister OneCommand Manager for VMware vCenter using the registration utility.
- **Host.CIM.CIM Interaction** to read and manage data through the OneCommand Manager for VMware vCenter.

All other users, including the root user, of the ESXi host cannot perform any actions including reading data. If a user without the required privileges attempts to perform an action in OneCommand Manager for VMware vCenter, an error message is displayed.

NOTE: To configure user roles and assign privileges, refer to the *VMware vCenter Server Guide* on the VMware website.

2.4.2 Lockdown Mode Feature

Refer to the vSphere guide on the VMware website for information on enabling and disabling lockdown mode.

If lockdown mode is enabled for an ESXi host, only a user with the required privileges can access the ESXi host and manage adapters using OneCommand Manager for VMware vCenter. All other users, including the root user, do not have access to the ESXi host.

2.4.3 Enabling OneCommand Manager for VMware vCenter

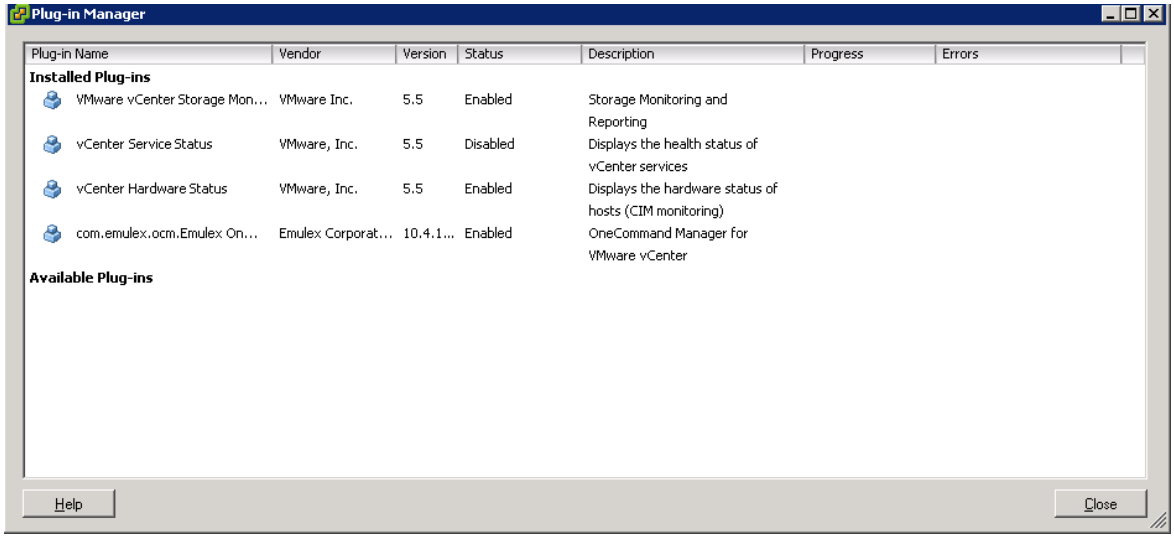
OneCommand Manager for VMware vCenter can be enabled or disabled from the Plug-In Management section.

NOTE: You must have sufficient privileges to access the Plug-In Management section. Refer to the VMware documentation for information on configuring users and privileges.

To enable OneCommand Manager for VMware vCenter, perform these steps:

1. From the **Navigation** panel on the left-side of the VMware vCenter, Home page, click **Plugins > Manage Plug-ins**. The **Plug-in Manager** page is displayed (Figure 7).

Figure 7: VMware vCenter, Management Page



2. In the Plug-In Manager page, select **com.emulex.ocm.Emulex OneCommand** and right-click under the **Status** column. A context menu opens.
3. Either select **Enable** to enable OneCommand Manager for VMware vCenter or select **Disable** to disable OneCommand Manager for VMware vCenter.

2.5 Enabling and Disabling OneCommand Manager for VMware vCenter with the Plug-in Manager

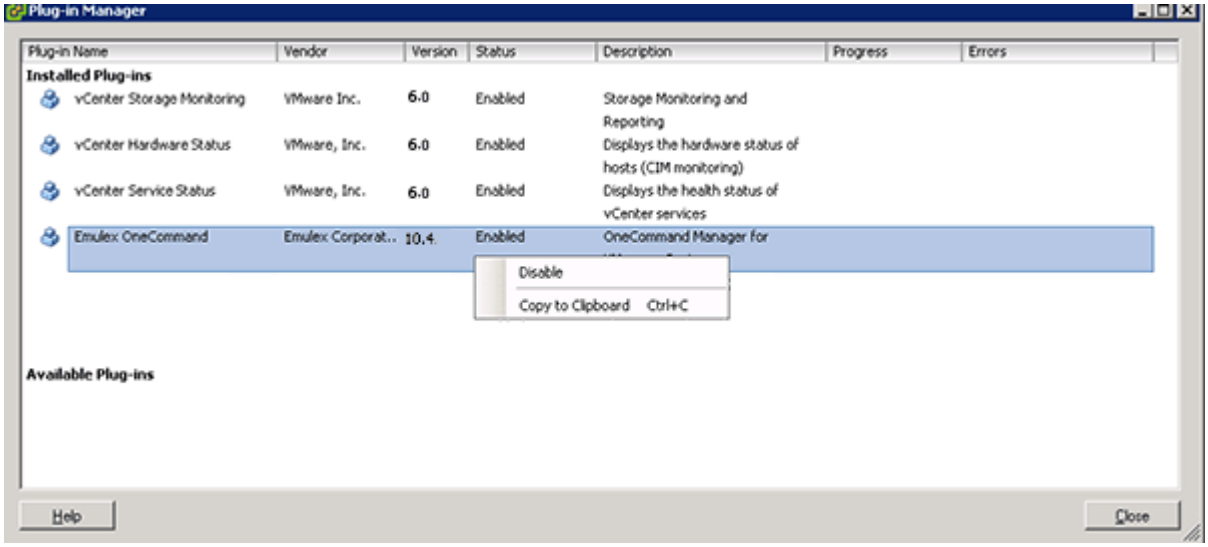
If you enable OneCommand Manager for VMware vCenter, the OneCommand Manager for VMware vCenter functionality immediately appears. If two or more plug-ins are registered, the **Emulex OneCommand** subtab (under the **Classic Solutions** tab) immediately appears. If only one plug-in is registered, the OneCommand Manager for VMware vCenter functionality immediately appears on the **Classic Solutions** tab.

If you disable OneCommand Manager for VMware vCenter, the OneCommand Manager for VMware vCenter functionality immediately disappears. If two or more plug-ins are registered, the **Emulex OneCommand** subtab immediately disappears. If only one plug-in is registered, the OneCommand Manager for VMware vCenter functionality immediately disappears from the **Classic Solutions** tab.

To change the status of OneCommand Manager for VMware vCenter, perform these steps:

1. Log on to the vCenter Server.
2. Enter the IP address and credentials of the vCenter Server where OneCommand Manager for VMware vCenter is registered.
3. After logging into vCenter Server, select **Plug-ins** from the menu bar, and select **Manage Plug-ins**. The **Plug-in Manager** window appears.
4. Click the **Emulex OneCommand** row. A context menu appears (Figure 8).

Figure 8: Plug-in Manager with Selected Row



5. Select **Enable** or **Disable**.

2.6 Registering and Unregistering OneCommand Manager for VMware vCenter

OneCommand Manager for VMware vCenter can be registered with more than one vCenter server.

To register or unregister OneCommand Manager for VMware vCenter with a new vCenter server, perform these steps:

1. Double-click the **OCM for VMware vCenter Registration** icon on the desktop. This icon is created when OneCommand Manager for VMware vCenter is successfully installed. The **Register/Unregister** dialog is displayed (Figure 4).
2. Enter the following details of the vCenter server:
   – **vCenter Server Name** – The IP address of the vCenter server.
   – **vCenter Server HTTPS Port** – The HTTPS port number of the vCenter server. The vCenter Server HTTPS port is 443 by default. You can change this value if you have configured a different HTTPS port while installing the vCenter.
   – **Username** – The user name with required privileges.
   – **Password** – The user password.
3. Do one of the following:
   – Click **Register** to register OneCommand Manager for VMware vCenter with a new vCenter server.

   or

   – Click **Unregister** to unregister an existing OneCommand Manager for VMware vCenter with a vCenter server.

NOTE:

- If you change the host name of the machine hosting the vCenter server, you must reinstall the vCenter server and re-register.
- If the vCenter server is already registered with another instance of OneCommand Manager for VMware server, it is replaced with this server instance.

4. When the operation is successful, a message is displayed. Click **OK**.
5. Close the window.

2.7 Uninstalling OneCommand Manager for VMware vCenter

Before you uninstall OneCommand Manager for VMware vCenter, you must unregister it from the vCenter Server. For more information, see Section 3, Using OneCommand Manager for VMware vCenter.

CAUTION! When you uninstall OneCommand Manager for VMware vCenter, ensure that you do not delete the default configuration and log files that are stored in the `%TEMP%\Emulex\OCM for VMware` directory. If these files are deleted, all historical information of active management performed from the host is permanently lost.

To uninstall OneCommand Manager for VMware vCenter in a Windows system, perform these steps:

1. Navigate to the system directory to which you downloaded the `ELXOCM-VMware-vCenter-<version>-Setup.exe` file.
2. Double-click the `ELXOCM-VMware-vCenter-<version>-Setup.exe` file. The **OneCommand Manager for VMware vCenter** window prompts you to reinstall or uninstall the application. Select **Uninstall the application completely** and click **Next**. A progress window is displayed. The window that indicates the detection of OneCommand Manager for VMware vCenter appears.
3. Click **OK**.

When uninstallation is complete, the **Uninstallation Completed** window is displayed.

4. Click **Finish**. You do not need to reboot the system.

NOTE: You can also uninstall the OneCommand Manager application from the **Programs and Features** window.

2.8 Upgrading or Reinstalling OneCommand Manager for VMware vCenter

To upgrade or reinstall OneCommand Manager for VMware vCenter in a Windows system, perform these steps:

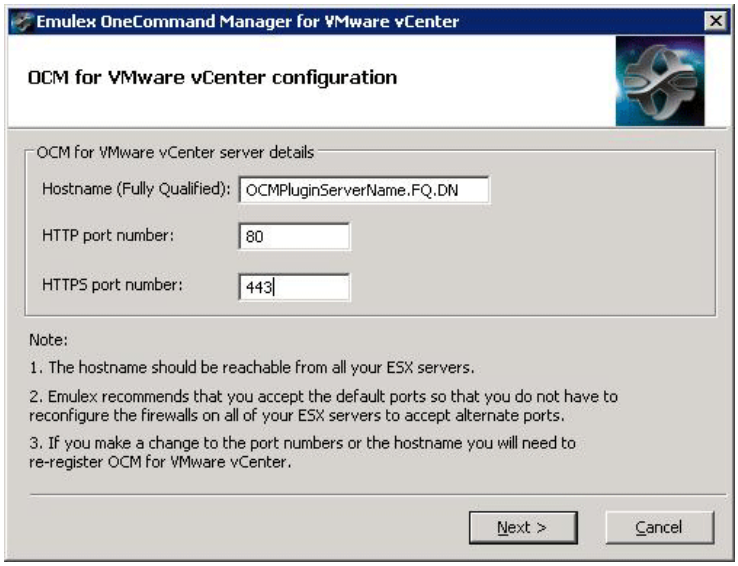
1. Navigate to the system directory to which you downloaded the `ELXOCM-VMware-vCenter-<version>-Setup.exe` file.
2. Double-click `ELXOCM-VMware-vCenter-<version>-Setup.exe`.

   The **OneCommand Manager for VMware vCenter** window prompts you to upgrade\reinstall or uninstall the application.
3. Select **Upgrade\Re-install the application** and click **Next**.

   The **Installation Options** window with the previous installation folder location appears (Figure 1).
4. Ensure that **OCM for VMware vCenter** is selected.
5. To change the installation folder location, click **Browse** and navigate to where you want the program files to reside.
6. Click **Install** on the Installation Options window.

   The **operation in progress** window appears. When the installation process is complete, the **OCM for VMware vCenter configuration** window appears (Figure 9).

Figure 9: OCM for VMware vCenter configuration Dialog



If OneCommand Manager for VMware vCenter was installed earlier with port numbers other than the defaults provided, those configured ports are displayed. If the port numbers are already in use, a warning appears next to the port number.

NOTE: The Windows firewall setting must allow incoming connections on the HTTP and HTTPS ports that you configure here.

7. Follow the instructions and complete the installation with steps 8 to 13 of Section 2.3, Installing OneCommand Manager for VMware vCenter.

Chapter 3: Using OneCommand Manager for VMware vCenter

OneCommand Manager for VMware vCenter is available at the host level and the cluster level in the inventory list.

NOTE: To increase the size of the OneCommand Manager for VMware window, the **Recent Tasks** panel on the right can be unpinned and collapsed.

3.1 Viewing OneCommand Manager for VMware vCenter

After you are logged on to the VMware vCenter server, the OneCommand Manager for VMware vCenter is under the **Manage** tab for a particular host or cluster that you select in the client.

To launch the OneCommand Manager for VMware vCenter, perform these steps:

1. Log on to the vCenter server. The home page is displayed.
2. Navigate to an ESXi host or cluster in the **Navigation** pane.
3. Perform one of the following actions:

   From the Host level view, select the host that you want to display.

   From the Cluster level view, select the cluster that you want to display.
4. Go to the **Manage** tab to access OneCommand Manager for VMware vCenter.

3.2 OneCommand Manager for VMware vCenter Window Elements

The OneCommand Manager for VMware vCenter window (Figure 10 and Figure 11) contains four basic components:

- The **Emulex Device Management** area
- The **Information** pane
- The **Console** buttons
- The **Filter** options menu (if applicable)

Figure 10: Cluster View with Callouts

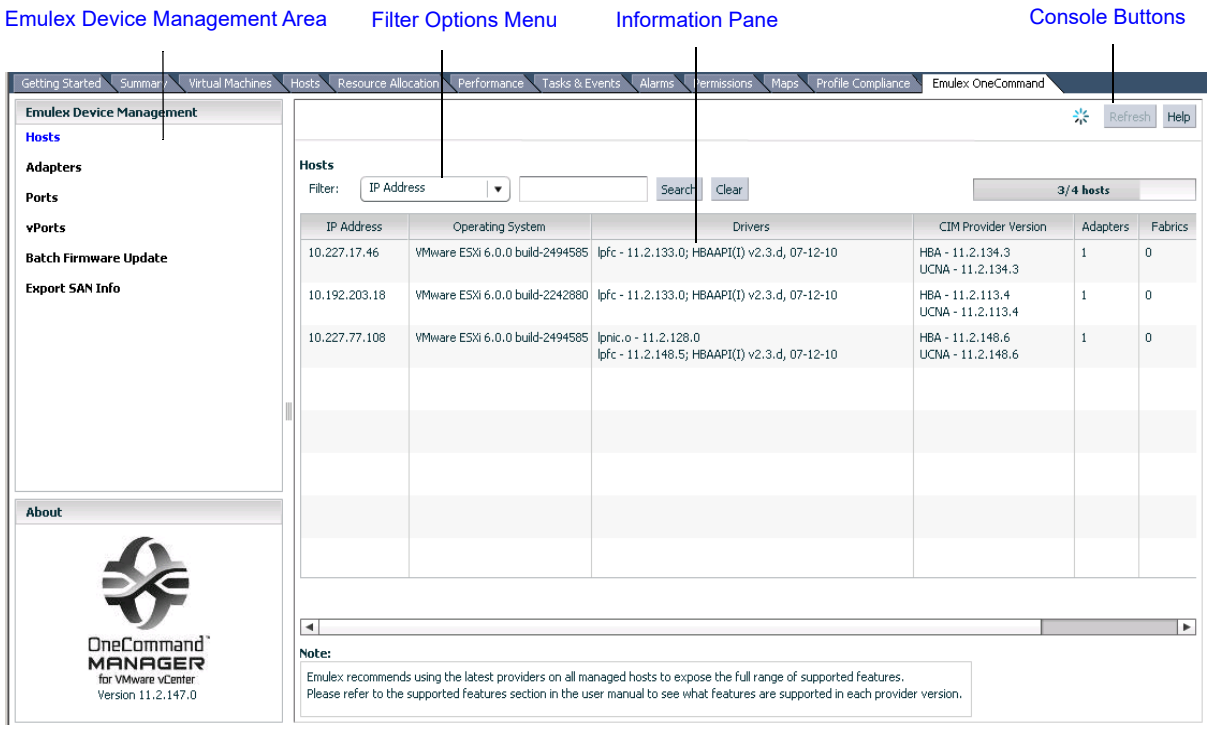
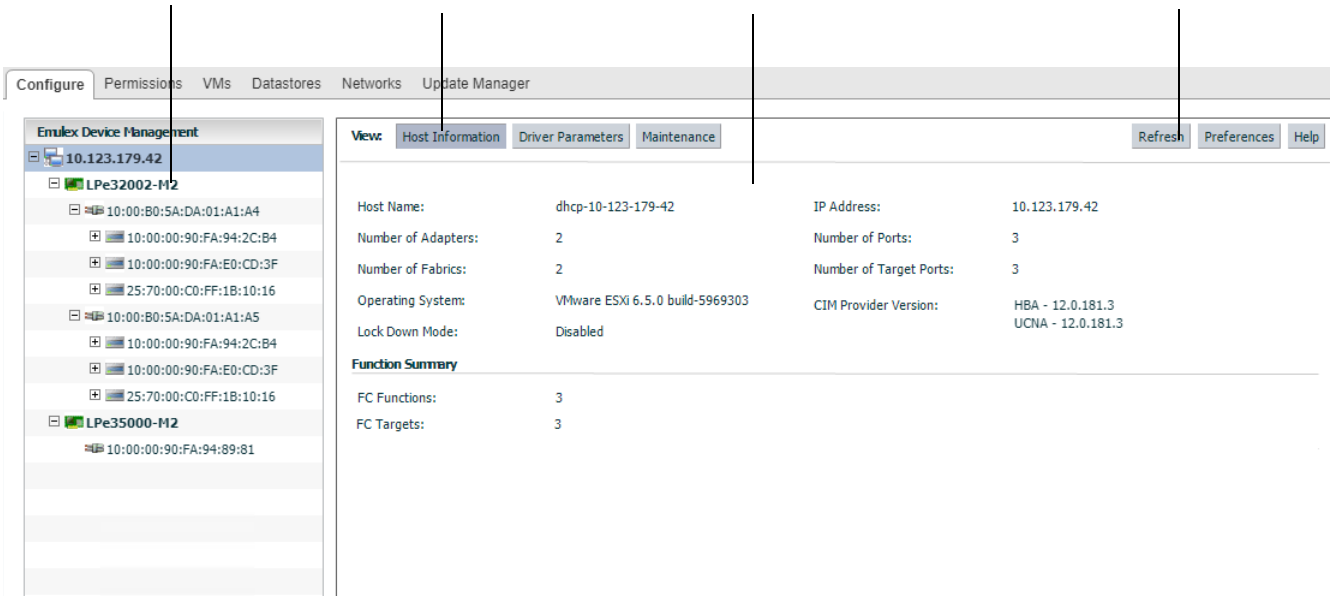


Figure 11: Host View with Callouts



3.2.1 Emulex Device Management Area

In a cluster view, the **Emulex Device Management** area contains links that determine what is displayed in the **Information** pane.

In a host view, the **Emulex Device Management** area is a discovery-tree with icons that represent discovered hosts, adapters, ports, virtual ports, fabrics, targets, and LUNs.

3.2.2 OneCommand Tabs

In a host view, the OneCommand tabs display configuration, statistical, and status information for network elements.

3.2.3 Information Pane

In a cluster view, the **Information** pane displays information based upon what is selected in the **Emulex Device Management** area.

In a host view, the **Information** pane displays information based upon the OneCommand tab that is selected.

3.2.4 Filter Options Menu

In a cluster view, selecting an item from the **Filter** options menu displays information that is sorted and displayed based upon by the item selected.

3.2.5 Console Tabs

- **Refresh** – Click to refresh CIM provider data and cluster or host information. The speed of the refresh operation depends on the number of adapters and the size of the SAN.
- **Preferences** – Click to access the **User Preferences** window. The **User Preferences** window is available in host view only. In the **User Preferences** window, select **Event Logging** to display up or down events for ports logged into the console. Port events are limited to the active vCenter client. If the same user logon is used from another vCenter client, the **User Preferences** window does not display these events.
- **Help** – Click to load the complete indexed online help for OneCommand Manager for VMware vCenter. You can search for information for all OneCommand Manager for VMware vCenter tabs and functions.

NOTE: The **User Preferences** window logs only up and down events for the port. Other events, such as temperature, are not posted.

Chapter 4: Managing Clusters and Hosts

This chapter pertains to viewing cluster and host information.

4.1 Managing Clusters

From within a cluster, you can view information about:

- Hosts in a cluster
- Adapters that belong to hosts in a cluster
- Physical ports in host-centric mode
- Virtual ports in host-centric mode
- Physical ports in fabric-centric mode

Figure 10 displays the main elements of the cluster view.

4.1.1 Viewing Hosts in a Cluster

NOTE: Hosts in a cluster with different provider versions support features as listed in Table 1: Support Provided by Emulex CIM Provider Versions.

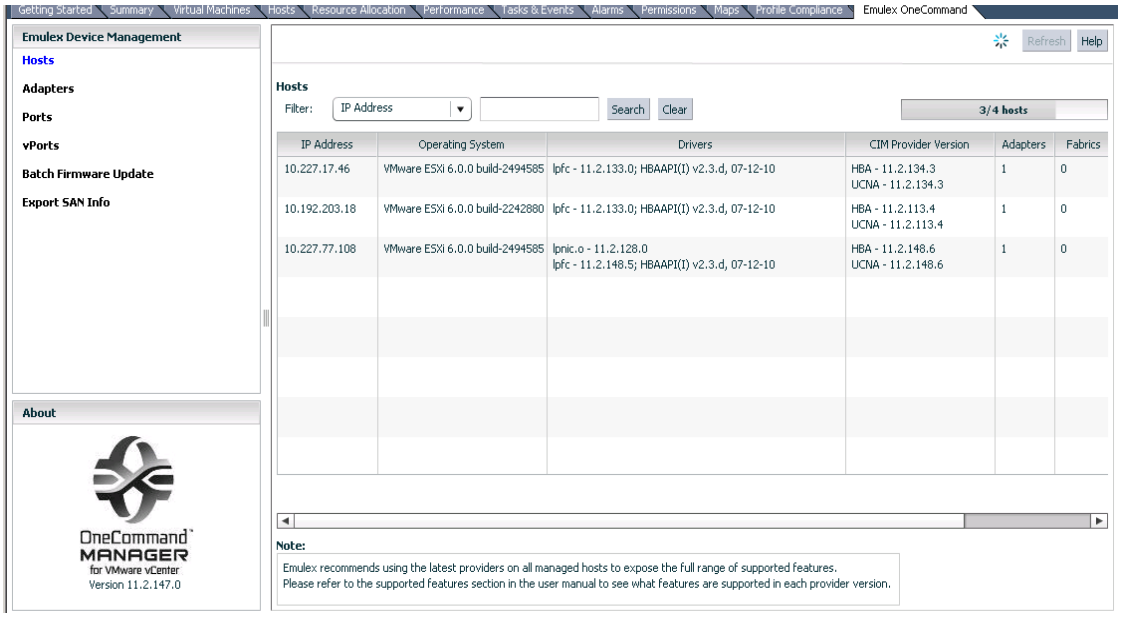
To view information about hosts in a cluster:

1. Select a cluster in the console tree-view. The **Getting Started** tab is selected by default.
2. If applicable, select the **Emulex OneCommand** tab. The **Hosts information** pane is displayed (Figure 12).

To filter information for a host within a cluster field:

1. Use the **Filter** options list to filter information.
   a. Search by any column title by selecting the title from the **Filter** options list.
   b. To further narrow the search, enter a value in the field to the right of the **Filter** options list. You can also enter a wildcard for this field.
   c. Click **Search**.
2. Click **Clear** to clear the search criteria.
3. Click **Refresh** to refresh the information. If a host is added to the currently selected cluster, the host information is refreshed.

Figure 12: Hosts within a Cluster



The following Hosts within a Cluster fields are displayed:

- **IP Address** – The IP address of the host in the cluster.
- **Operating System** – The operating system and version installed on the host.
- **Drivers** – The drivers and their versions installed on the host.
- **CIM Provider Version** – The version of the Emulex CIM Provider that is running on the ESXi host.
- **Adapters** – The number of adapters installed in the host.
- **Fabrics** – The number of fabrics to which the host is connected.
- **Ports** – The number of discovered physical ports that can be managed by the host.
- **Lock Down Mode** – Whether lockdown mode is enabled or disabled.

4.1.2 Viewing Adapters in a Cluster

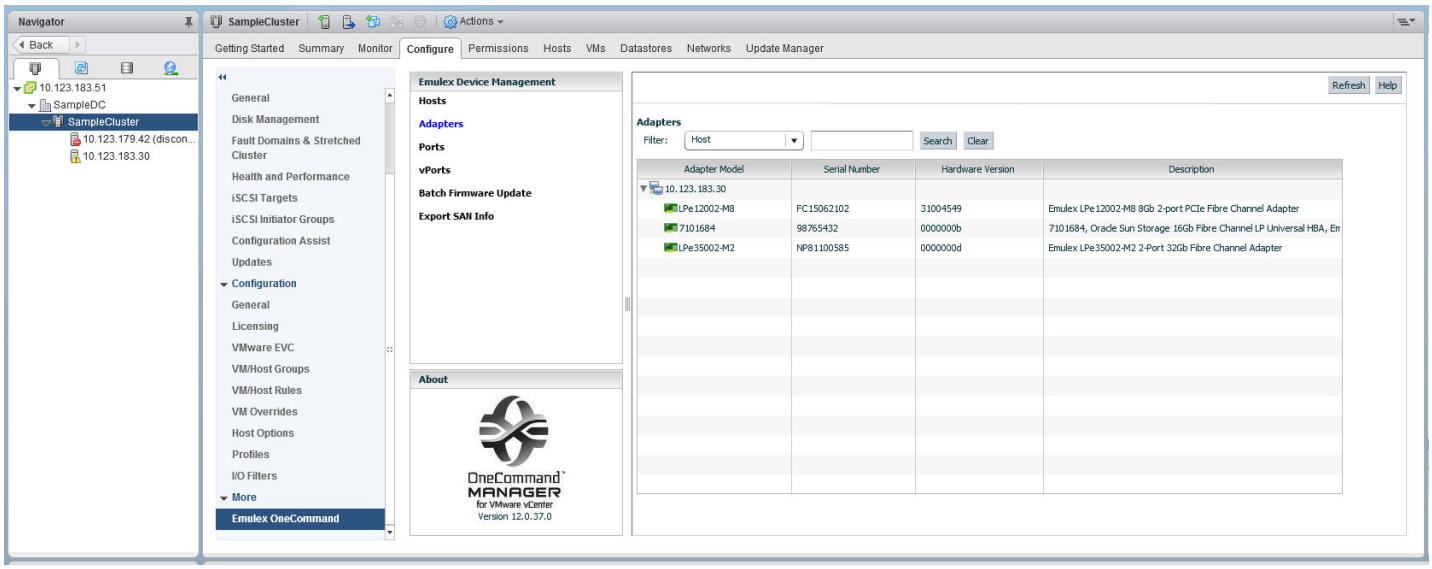
To view information about adapters belonging to a host in a cluster, perform these steps:

1. Select a cluster in the console tree-view, and if applicable, select the **Emulex OneCommand** tab.
2. From the **Emulex Device Management** options, select **Adapters**. Adapters information is displayed (Figure 13).

To filter adapter information within a cluster, perform these steps:

1. Use the **Filter** options list to filter the adapter information. Choose any of the available adapter information fields from the list, enter a wildcard for the field, and click **Search**.
2. Click **Clear** to clear the search criteria and the corresponding adapter information.
3. Click **Refresh** to refresh the information. If an adapter is added to any of the hosts, the adapter information is refreshed.

Figure 13: Adapters within a Cluster



The following Adapters within a Cluster fields are displayed:

- **Adapter Model** – The model of the adapter.
- **Serial Number** – The serial number of the adapter.
- **Hardware Version** – This field displays the JEDEC ID.
- **Description** – The type of adapter.

4.1.3 Viewing Physical Ports in a Cluster (Host-Centric Mode)

To view information about a physical port that is in a cluster, in host-centric mode, perform these steps:

1. Select a cluster in the console tree-view.
2. Select the **Emulex OneCommand** tab. Host information is displayed.
3. From the **Emulex Device Management** options, select **Ports**. The host-centric **Information** pane is displayed (Figure 14 and Figure 15).

NOTE: Make sure that **Group by Fabric** is not selected.

Figure 14: Physical Ports within a Cluster–Host-Centric View

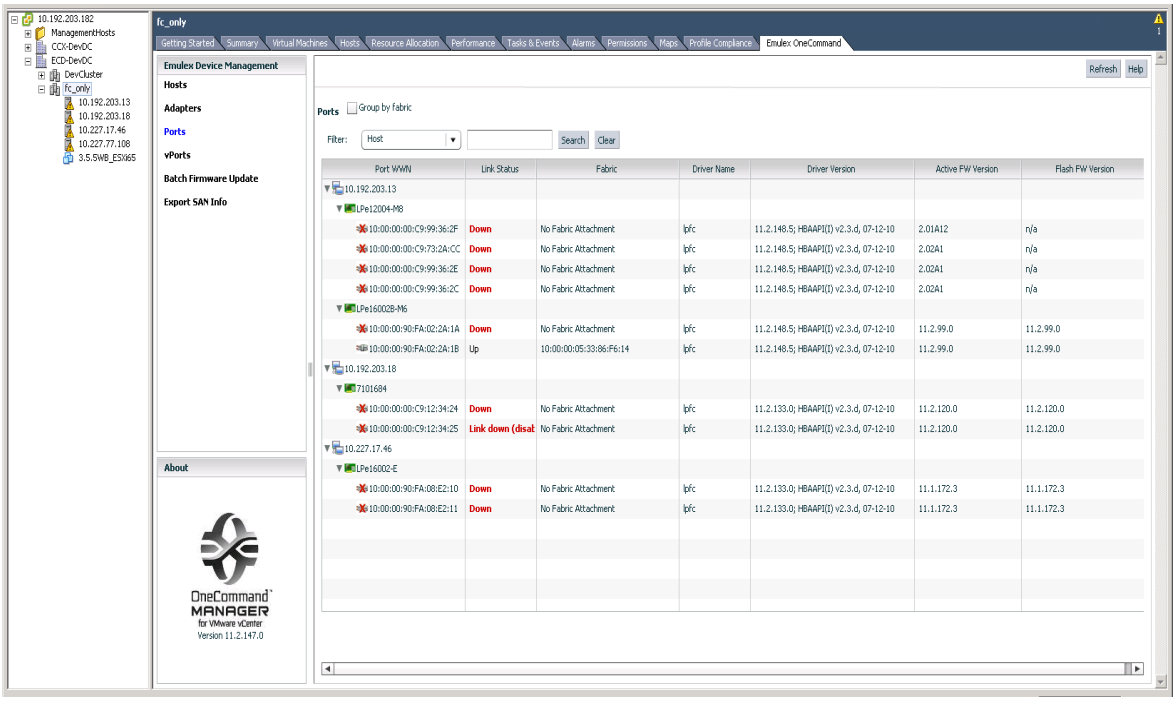
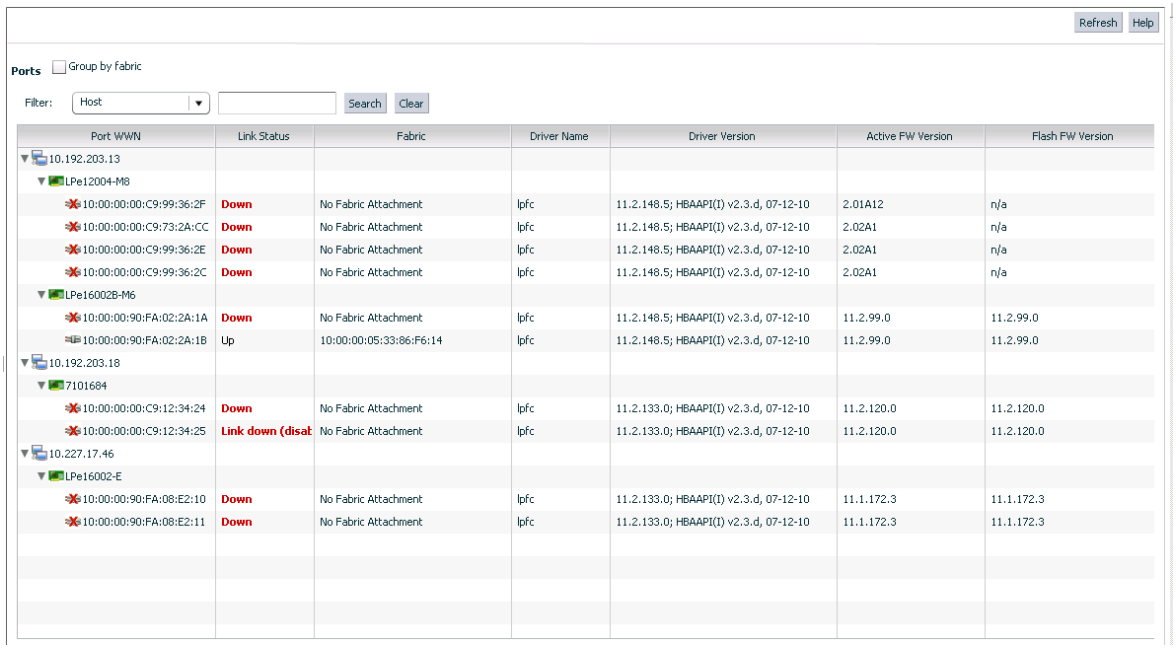


Figure 15: Close-Up of Physical Ports within a Cluster–Host-Centric View



The following fields are displayed:

- **Port WWN** – The port World Wide Name.
- **Link Status** – The status of the link on the selected port.
- **Fabric** – The 64-bit worldwide unique identifier assigned to the fabric.

- **Driver Name** – The executable file image name for the driver as it appears in the Emulex driver download package.
- **Driver Version** – The version of the installed driver.
- **Active FW Version** – The active FW version.
- **Flash FW Version** – The FW version that becomes active after the system is rebooted.

4.1.4 Viewing Virtual Ports in a Cluster (Host-Centric Mode)

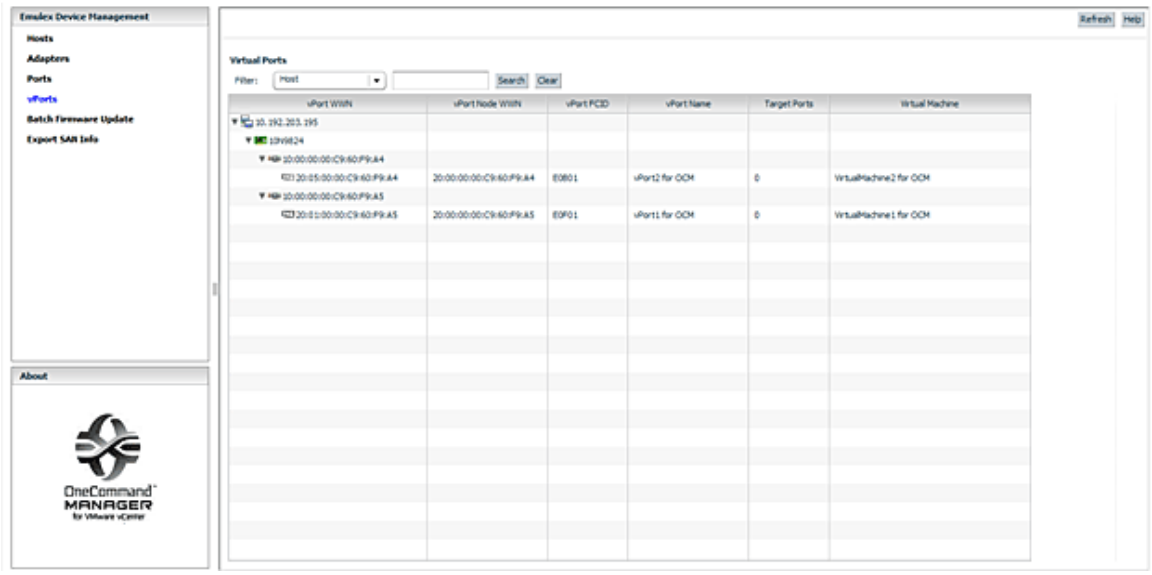
To view information about a virtual port that is in a cluster, in host-centric mode, perform these steps:

1. Select a cluster in the console tree-view.
2. If applicable, select the **Emulex OneCommand** tab. Port host information is displayed.
3. From the **Emulex Device Management** options, select **vPorts**. The virtual port information is displayed (Figure 16).

To filter virtual port information in a cluster, perform these steps:

1. Use the **Filter** options list to filter the port information.
2. Choose any of the available host information fields from the list, enter a wildcard for the field, and click **Search**.
3. Click **Clear** to clear the search criteria.

Figure 16: Virtual Ports in a Cluster–Host-Centric View



The following virtual ports in a cluster, host-centric fields are displayed:

- **vPort WWN** – The virtual port World Wide Name.
- **vPort Node WWN** – The virtual port node World Wide Name.
- **vPort FCID** – The virtual port FC ID.
- **vPort Name** – The virtual port name.
- **Target Ports** – The number of target ports.
- **Virtual Machine** – Virtual machine information.

4.1.5 Viewing Physical Port Information in a Cluster (Fabric-Centric Mode)

To view physical port information in a cluster, in fabric-centric mode, perform these steps:

1. Select a cluster in the console tree-view.
2. Select the **Emulex OneCommand** tab, host information is displayed.
3. From the **Emulex Device Management** options, select **Ports**. The host-centric **Information** pane is displayed.
4. Select **Group by Fabric**. Fabric information is displayed (Figure 17 and Figure 18).

Figure 17: Information for a Physical Port in a Cluster–Fabric-Centric View

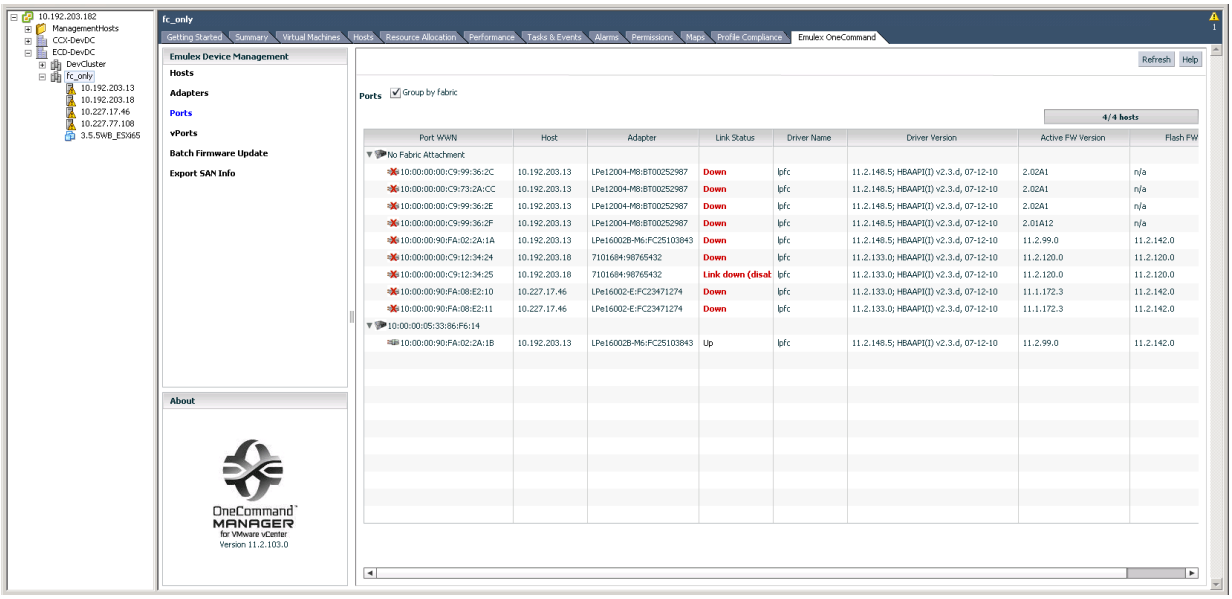


Figure 18: Close-up of Information for a Physical Port in a Cluster–Fabric-Centric View

Refresh Help

Ports ☑ Group by fabric

4/4 hosts

Port WWN	Host	Adapter	Link Status	Driver Name	Driver Version	Active FW Version	Flash FW
No Fabric Attachment							
10:00:00:00:C9:99:36:2C	10.192.203.13	LPe12004-M8:BT00252987	Down	lpfc	11.2.148.5; HBAAPI(I) v2.3.d, 07-12-10	2.02A1	n/a
10:00:00:00:C9:73:2A:CC	10.192.203.13	LPe12004-M8:BT00252987	Down	lpfc	11.2.148.5; HBAAPI(I) v2.3.d, 07-12-10	2.02A1	n/a
10:00:00:00:C9:99:36:2E	10.192.203.13	LPe12004-M8:BT00252987	Down	lpfc	11.2.148.5; HBAAPI(I) v2.3.d, 07-12-10	2.02A1	n/a
10:00:00:00:C9:99:36:2F	10.192.203.13	LPe12004-M8:BT00252987	Down	lpfc	11.2.148.5; HBAAPI(I) v2.3.d, 07-12-10	2.01A12	n/a
10:00:00:90:FA:02:2A:1A	10.192.203.13	LPe16002B-M6:FC25103843	Down	lpfc	11.2.148.5; HBAAPI(I) v2.3.d, 07-12-10	11.2.99.0	11.2.142.0
10:00:00:00:C9:12:34:24	10.192.203.18	7101684:98765432	Down	lpfc	11.2.133.0; HBAAPI(I) v2.3.d, 07-12-10	11.2.120.0	11.2.120.0
10:00:00:00:C9:12:34:25	10.192.203.18	7101684:98765432	Link down (disat	lpfc	11.2.133.0; HBAAPI(I) v2.3.d, 07-12-10	11.2.120.0	11.2.120.0
10:00:00:90:FA:08:E2:10	10.227.17.46	LPe16002-E:FC23471274	Down	lpfc	11.2.133.0; HBAAPI(I) v2.3.d, 07-12-10	11.1.172.3	11.2.142.0
10:00:00:90:FA:08:E2:11	10.227.17.46	LPe16002-E:FC23471274	Down	lpfc	11.2.133.0; HBAAPI(I) v2.3.d, 07-12-10	11.1.172.3	11.2.142.0
10:00:00:05:33:86:F6:14							
10:00:00:90:FA:02:2A:1B	10.192.203.13	LPe16002B-M6:FC25103843	Up	lpfc	11.2.148.5; HBAAPI(I) v2.3.d, 07-12-10	11.2.99.0	11.2.142.0

The following fabric-centric information fields are displayed:

- **Port WWN** – The port World Wide Name.
- **Host** – The host IP address.
- **Adapter** – The adapter model.
- **Link Status** – The status of the link on the selected port.
- **Driver Name** – The executable file image name for the driver as it appears in the Emulex driver download package.
- **Driver Version** – The version of the installed driver.
- **Active FW Version** – The active firmware version.
- **Flash FW Version** – The firmware version that becomes active after the system is rebooted.

4.2 Managing Hosts

Host information includes:

- Information for a single host
- Driver parameters for all adapters in a host
- Firmware information for all adapters in a host

Figure 11 displays the main elements of the host view.

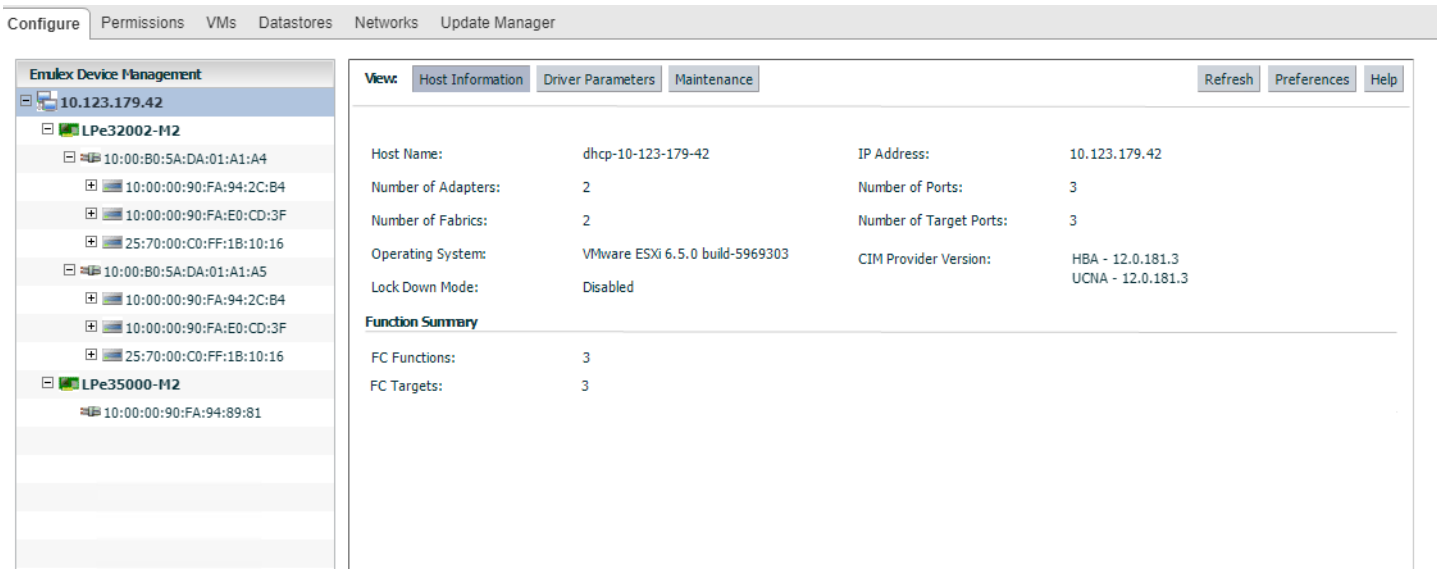
4.2.1 Viewing Host Information for a Single Host

To view host information for a single host, select a host in the console tree-view, and if applicable, select the **Emulex OneCommand** tab. The **Host Information** tab is selected by default and the information of the selected host appears (Figure 19).

To filter the host information, perform these steps:

1. Use the **Filter** options list to filter the fabric information.
2. Choose any of the available fabric information fields from the list, enter a wildcard for the field, and click **Search**.
3. Click **Clear** to clear the search criteria.

Figure 19: Information for a Single Host



The following host information fields are displayed:

- **Host Name** – The host identifier.
- **Number of Adapters** – The number of adapters installed in the host.
- **Number of Fabrics** – The number of fabrics to which the host is connected.
- **Operating System** – The operating system and version installed on the selected host.
- **Lock Down Mode** – Indicates whether lockdown mode is enabled or disabled.
- **IP Address** – The IP address of the host.
- **Number of Ports** – The number of discovered physical ports that can be managed by this host.
- **Number of Target Ports** – The number of targets discovered across the ports.
- **CIM Provider Version** – The versions of the Emulex CIM Providers that are running on the ESXi host.
- **Function Summary** area:
  - **FC Functions** – The number of FC functions running on the discovered adapters on this host.
  - **FC Targets** – The number of FC targets discovered on the FC functions on this host.

4.2.2 Viewing Driver Parameters of All Adapters in a Host

The host **Driver Parameters** tab enables you to view and edit the adapter driver parameter settings for a specific host. The host driver parameters are global values and apply to all adapters in that host unless they are overridden by parameters assigned to a specific adapter using the port **Driver Parameters** tab. When an adapter port parameter is specified, it overrides every host parameter for the adapter.

For each parameter, the **Information** pane displays the current value, the range of acceptable values, the default value, and whether the parameter is dynamic. A dynamic parameter allows the change to take effect without resetting the adapter or rebooting the system. For information on changing parameters for the host, see Section 6.6, Configuring Port Driver Parameters.

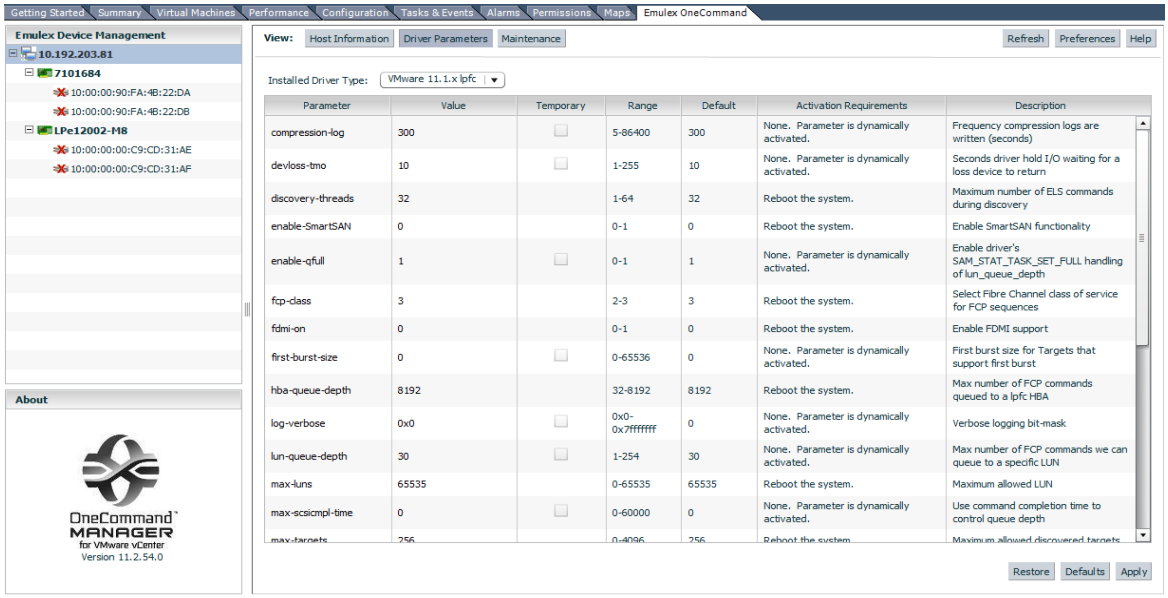
NOTE: If there are no discovered adapters, the driver parameters table is empty. This event occurs because there are no adapters to which the host driver parameters apply.

NOTE: Setting any port parameter will override all the host parameters on that port.

To view driver parameters for all adapters in a host, perform these steps:

1. Select a host in the console tree-view, and if applicable, select the **Emulex OneCommand** tab.
2. Select the **Driver Parameters** tab (Figure 20).

Figure 20: Host Driver Parameters



The following host **Driver Parameters** tab fields are displayed:

- **Installed Driver Type** – The current driver installed on this host.
- **Driver Parameter table** – A list of adapter driver parameters and their current values.

  Driver-parameter-specific information is displayed in this area. This information includes value, range, default, activation requirements, and description.
  - **Parameter** – The name of the driver parameter.
  - **Value** – The value of the driver parameter.
  - **Temporary** – Indicates if the value can be set temporarily at port level.

- **Range** – The range of acceptable values for the driver parameter.
- **Default** – The default value of the parameter.
- **Activation Requirements** – The steps required to activate the changed value of the driver parameter.
- **Description** – The description of the driver parameter.

To change the driver parameters for all adapters in a host, perform these steps:

1. From the console tree-view, select the host whose adapter driver parameters you want to change. If applicable, select the **Emulex OneCommand** tab.
2. Select the host **Driver Parameters** tab (Figure 20). If there are adapters with different driver types installed, the **Installed Driver Types** menu displays a list of all driver types and driver versions that are installed. Select the driver whose parameters you want to change. This menu does not appear if all the adapters are using the same driver.
3. In the driver parameter table, click the **Value** field of a parameter that you want to change. The range for the value is displayed. Enter a value in decimal or hexadecimal format, depending on how the current value is presented. If the value is in hexadecimal format, it is prefixed by 0x (for example, -0x2d).
4. Parameters that can be changed temporarily can only be changed from the corresponding port. Such parameters are represented with a check box next to them.
5. Click **Apply**.

If you changed some parameters and did not click **Apply**, you can restore the parameters back to the value they had before you made the changes. To restore the parameters, click **Restore**.

To reset all parameters back to their default values, click **Defaults**.

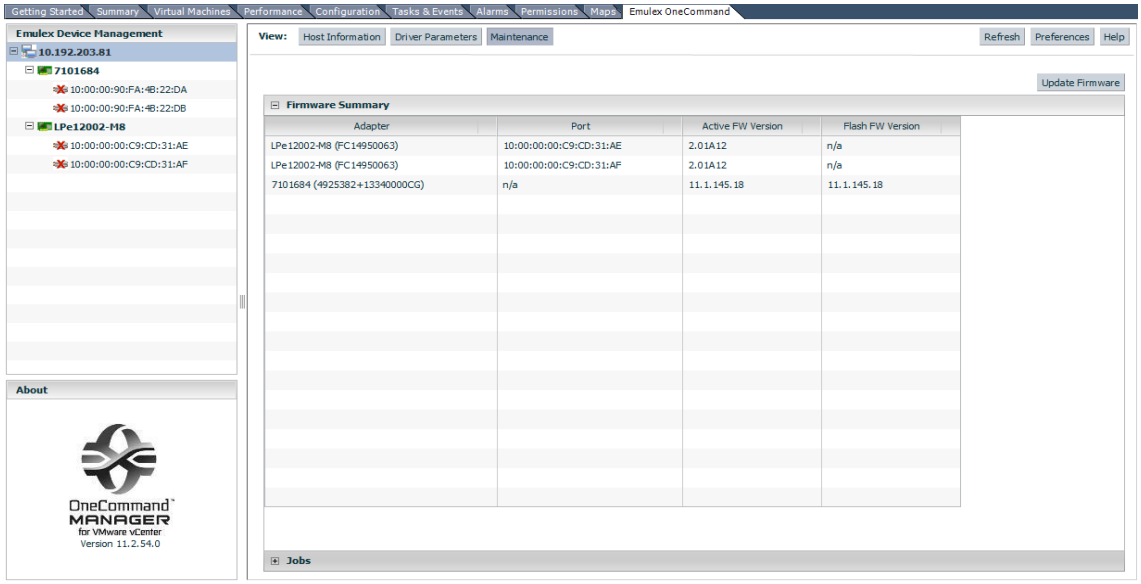
4.2.3 Viewing Firmware Information for All Adapters in a Host

The host **Maintenance** tab enables you to view and update firmware on multiple adapters in a specific host. To update firmware on FC adapters in a host, see Section 7.1.1, Updating Firmware on an LPe12000-Series Adapter in a Host.

To view firmware for all adapters in a host, perform these steps:

1. Select a host in the console tree-view, and if applicable, select the **Emulex OneCommand** tab.
2. Select the **Maintenance** tab (Figure 21).

Figure 21: Host Maintenance Tab



The following host **Maintenance** tab fields are displayed:

- **Adapter** – The model of the adapter.
- **Port** – The port WWN.
- **Active FW Version** – The current firmware on the adapter.
- **Flash FW Version** – The flashed firmware on the adapter. Displays **n/a** for ports that are not available.

Chapter 5: Managing Adapters and Ports

This chapter describes the various adapter and port management functions that you can perform using OneCommand Manager for VMware vCenter.

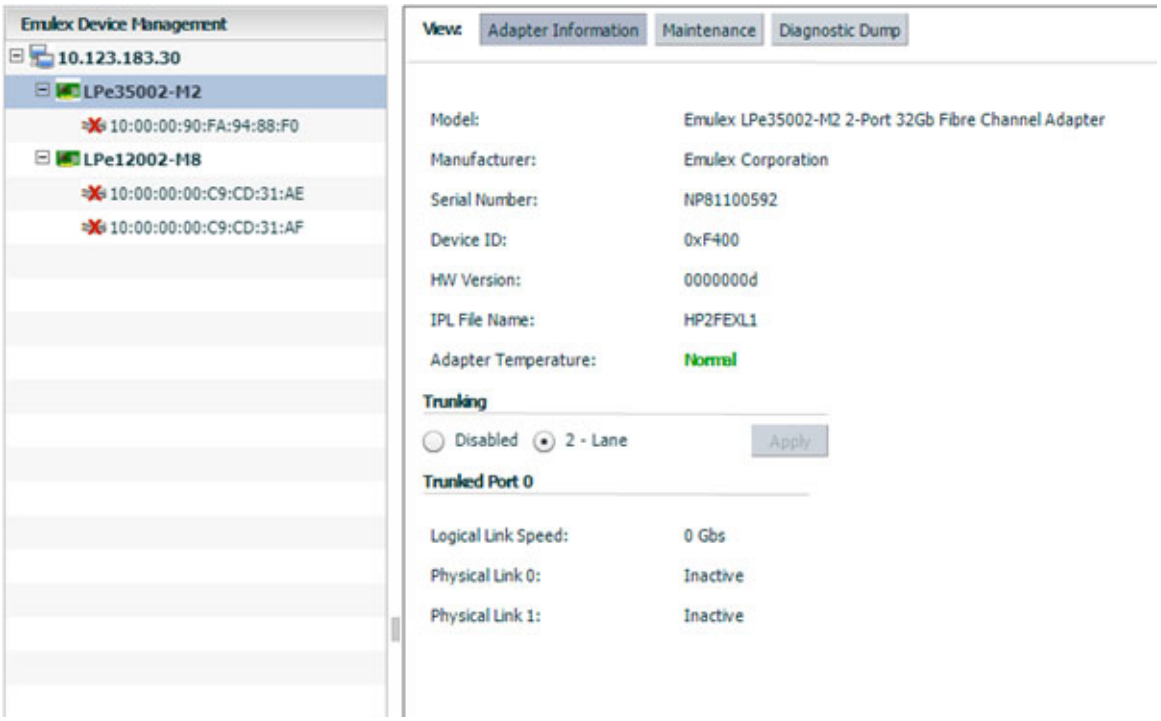
5.1 Viewing Adapter Information

When you select an adapter from the **Emulex Device Management** tree-view, the **Adapter Information** pane displays general attributes associated with the selected adapter.

To view information for an adapter, perform these steps:

1. Select a host in the console tree-view, and if applicable, select the **Emulex OneCommand** tab.
2. In the **Emulex Device Management** tree-view, select an FC adapter. The **Adapter Information** tab is displayed (Figure 22).

Figure 22: Adapter Information Tab



The following **Adapter Information** tab fields are displayed:

- **Model** – The complete model name of the adapter.
- **Manufacturer** – The manufacturer of the adapter.
- **Serial Number** – The manufacturer's serial number for the selected adapter.
- **Device ID** – The manufacturer's device identification number for the selected adapter.
- **HW Version** – This field displays the JEDEC ID.
- **IPL File Name** – This field displays the initial program load file name.

- **Adapter Temperature**:
  - **Normal**: The adapter's temperature is within normal operational range.
  - **Exceeded operational range – Critical:** The adapter's temperature is beyond normal operational range. If the temperature continues to increase, the adapter will shut down. You must determine the cause of the temperature issue and fix it immediately. Check for system cooling issues. Common causes of system cooling issues include clogged air filters, inoperative fans, and air conditioning issues that cause high ambient air temperatures.
  - **Exceeded operational range – Adapter stopped:** The temperature has reached the critical limit, forcing the adapter to shut down. You must determine the cause of the temperature issue and fix it before resuming operation. Check for system cooling issues. Common causes of system cooling issues include clogged air filters, inoperative fans, and air conditioning issues that cause high ambient air temperatures.
  - **Not Supported** - The adapter temperature is not available.

  After the system overheating issue is resolved and the adapter has cooled down, reboot the system or, if the system supports hot swapping, cycle the power of the adapter slot.
- **Trunking** area – When supported by the adapter, you can combine multiple physical FC links to form a single logical link. Once created, you can view an aggregated port's logical link speed and physical link status. See Section 5.3, Configuring Trunking, for additional information.

5.2 Viewing FC Port Details

When you select an FC port from the **Emulex Device Management** tree-view, the **Port Details** tab contains general attributes associated with the selected FC port.

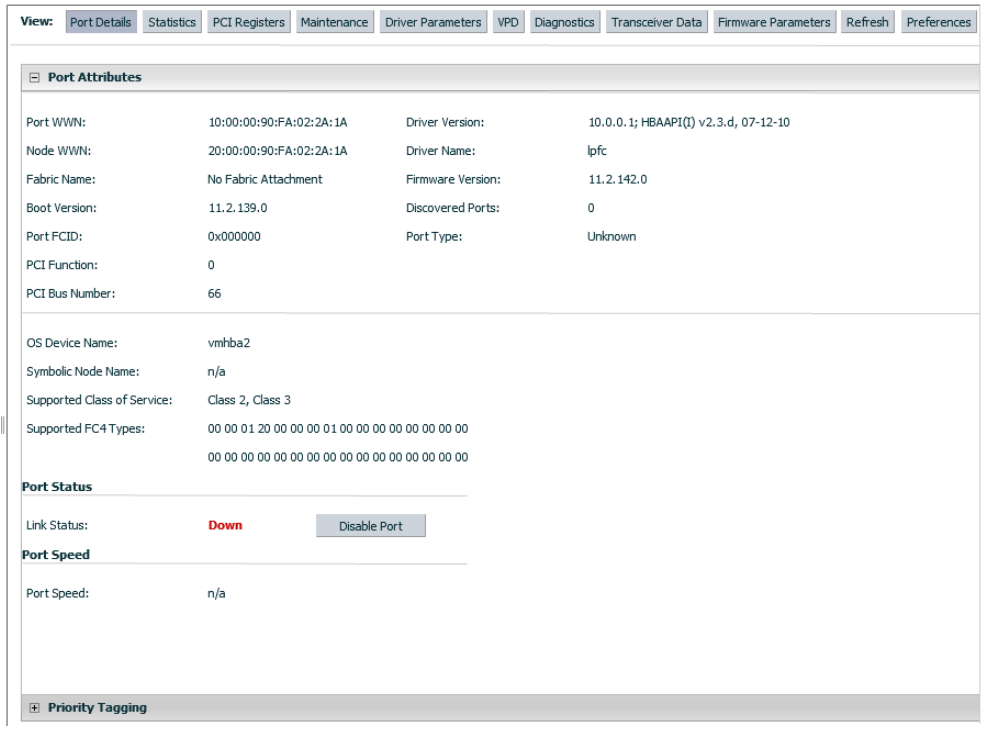
You can also configure the virtual machine ID (VMID) when it is supported by the switch.

To view details for an FC port, perform these steps:

1. Select a host in the console tree-view, and if applicable, select the **Emulex OneCommand** tab.
2. In the **Emulex Device Management** tree-view, select the FC port whose information you want to view.

   The **Port Details** tab is displayed (Figure 23).

Figure 23: FC Port Details Tab (Priority Tagging Supported)



The following FC **Port Details** tab fields are displayed:

- **Port Attributes** area:
  - **Port WWN** – The port World Wide Name of the selected adapter.
  - **Node WWN** – The node World Wide Name of the selected adapter.
  - **Fabric Name** – The 64-bit worldwide unique identifier assigned to the fabric.
  - **Boot Version** – The version of boot code installed on the selected adapter port. If the boot code is disabled, the field displays **Disabled**.
  - **Port FCID** – The FC ID of the selected adapter port.
  - **PCI Function** – The PCI function number of the selected port.
  - **PCI Bus Number** – The PCI bus number.
  - **Driver Version** – The version of the driver installed for the adapter.
  - **Driver Name** – The executable file image name for the driver as it appears in the Emulex driver download package.
  - **Firmware Version** – The version of Emulex firmware currently active on the adapter port.
  - **OS Device Name** – The platform-specific name by which the selected adapter is known to the operating system.
  - **Symbolic Node Name** – The FC name used to register the driver with the name server.
  - **Supported Class of Service** – A frame delivery scheme exhibiting a set of delivery characteristics and attributes. There are three classes of service.
    - **Class 1** – Provides a dedicated connection between a pair of ports with confirmed delivery or notification of non-delivery.
    - **Class 2** – Provides a frame switched service with confirmed delivery or notification of non-delivery.
    - **Class 3** – Provides a frame switched service similar to Class 2, but without notification of frame delivery or non-delivery.
- **Supported FC4 Types** – A 256-bit (8-word) map of the FC-4 protocol types supported by the port containing the selected adapter.

- **Port Status** area:
  - **Link Status** – This field indicates the status of the link on the selected adapter port.
  - **Enable or Disable Port** – Click this button to enable or disable the selected port. See Section 5.4, Enabling and Disabling a Port, for more information.
- **Port Speed** area:
  - **Port Speed** – The current port speed of the selected adapter port. For trunked ports, the maximum speed that the trunked port is capable of (if all ports in the trunk are up) is displayed.

5.3 Configuring Trunking

NOTE:

- Trunking is supported only on LPe35002 and LPe35004 adapters.
- Neither FA-PWWN nor Dynamic D_Port can coexist with the trunking feature on LPe35000-series adapters. If trunking is enabled, the firmware automatically disables FA-PWWN and Dynamic D_Port.
- Trunking is not supported at 8 Gb/s, and the link will not come up at this speed.
- Before you configure trunking on the Emulex adapter, follow the instructions from Brocade for configuring trunking on the switch.

Using the **Adapter Information** tab, trunking enables you to combine multiple physical FC links to form a single logical link (aggregated port). The aggregated port's maximum link speed is the sum of the maximum link speeds of the individual physical links comprising the aggregated port. For example, an aggregated port comprised of two physical links running at 64 Gb/s each will have a potential logical (aggregate) link speed of 128 Gb/s. The actual link speed of the aggregated port depends on the states (active/non-active) of the individual physical links comprising the aggregated port.

The physical links comprising an aggregated port are referred to as lanes. Both 2-lane and 4-lane aggregated ports are supported. For dual-port adapters, only 2-lane port aggregation is possible. If 2-lane port aggregation is configured on a dual-port adapter, the two physical links are combined to form a single 2-lane aggregated port whose aggregate speed is potentially 128 Gb/s, assuming both physical links are active.

LPe35004 adapters support both 2-lane port aggregation and 4-lane port aggregation. If 2-lane port aggregation is configured on an LPe35004 adapter, the four physical links on the adapter will be divided among two separate aggregated ports. The two lowest numbered physical links will form the first aggregated port, and the two highest number physical links will form the second aggregated port. If 4-lane port aggregation is configured on an LPe35004 adapter, all four physical links will be combined to form a single 4-lane trunk whose aggregate speed is potentially 256 Gb/s, assuming all 4 links are active.

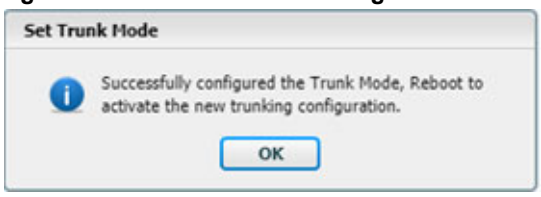
To set trunking, perform these steps:

1. Select a host in the console tree-view, and if applicable, select the **Emulex OneCommand** tab.
2. In the **Emulex Device Management** tree-view, select an FC adapter. The **Adapter Information** tab is displayed (Figure 22).
3. Select **Disabled**, or **2-lane**, or **4-lane**.

NOTE: On an LPe35004 adapter, if 2-lane port aggregation is selected, the four physical links on the adapter are divided among two separate aggregated ports (Port 0 and Port 1). The two lowest numbered physical links form the first aggregated port (Port 0), and the two highest number physical links form the second aggregated port (Port 1).

4. Click **Apply**. The **Set Trunk Mode** dialog appears notifying you that your changes require a system reboot.

Figure 24: Set Trunk Mode Dialog



5. Click **OK** and reboot the system.

5.4 Enabling and Disabling a Port

When you disable a port, you disable all functions for the port. Disabled ports appear in the **Emulex Device Management** tree-view with an x over the port icon.

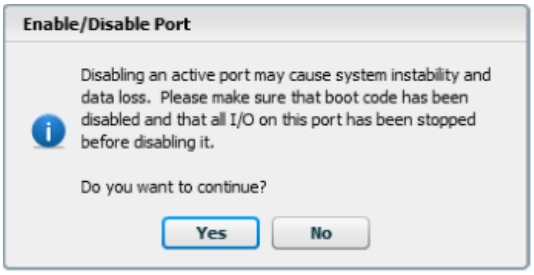
CAUTION! Do not disable a boot port; doing so could result in data loss or corruption.

NOTE:

- Ensure that there is no I/O traffic on the port before disabling it.
- You must reset the adapter to activate the new value.

To enable or disable a port, perform these steps:

1. Select a host in the console tree-view. If applicable, select the **Emulex OneCommand** tab.
2. In the **Emulex Device Management** tree-view, select the FC port that you want to enable or disable.
3. From the **Port Details** tab (Figure 23), click **Enable Port** or **Disable Port**. The following dialog appears.



4. Click **Yes** to enable or disable the port.

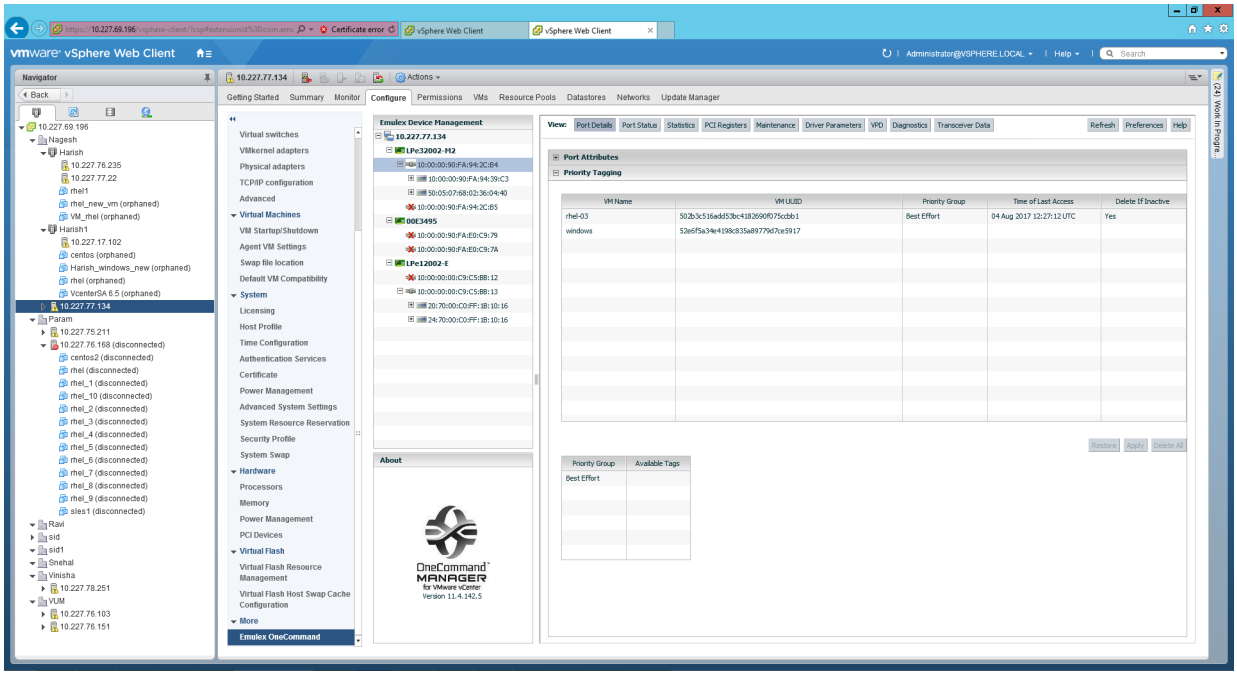
5.5 Configuring Priority Tagging

The **Priority Tagging** area of the **Port Details** tab displays all the VMs on an ESXi host and the corresponding priority mapping for each VM. Each entry contains the VM name, the VM universal unique identifier (VM UUID), the assigned priority group, the time the VM was last accessed, and *Delete If Inactive* indicating whether the mapping will be deleted when there is no I/O from a VM.

Using the **Priority Tagging** area, you can view the priority group assigned to a VM.

NOTE: Priority tagging configuration is supported only when the `vmid-priority-tagging` driver parameter is enabled. See Section 6.6, Configuring Port Driver Parameters, for additional information.

Figure 25: Port Details Tab–Priority Tagging Area



5.6 Viewing Firmware Parameters

The **Firmware Parameters** tab displays information about, and allows you to change, the configured link speed, the FA-PWWN status, and the Dynamic D_Port status of the selected port.

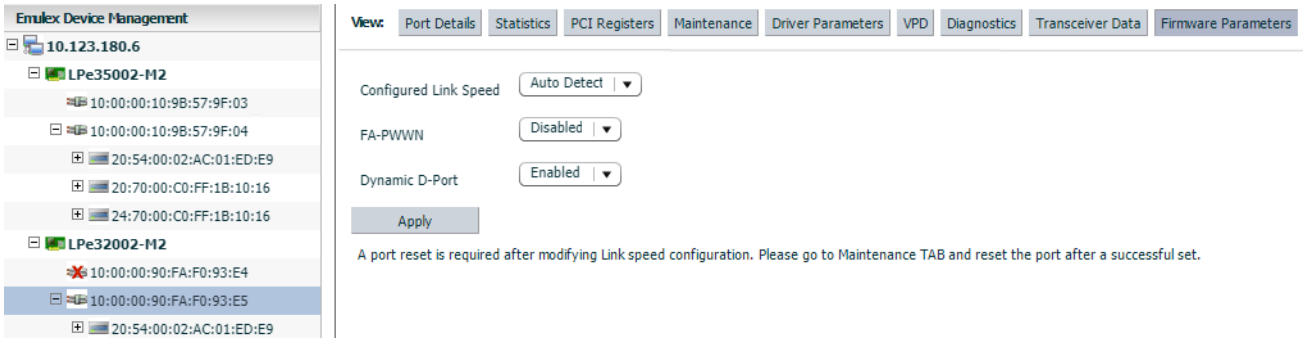
NOTE:

- The **Firmware Parameters** tab is available only for supported adapters and CIM providers.
- Unsupported features do not appear on the **Firmware Parameters** tab.

To view firmware parameters for a port, perform these steps:

1. Select a host in the console tree-view, and if applicable, select the **Emulex OneCommand** tab.
2. In the **Emulex Device Management** tree-view, select the port whose firmware information you want to view.
3. Select the **Firmware Parameters** tab (Figure 26).

Figure 26: Firmware Parameters Tab



The following FC **Firmware Parameters** tab fields are displayed:

- **Configured Link Speed** – This field displays the link speeds that are supported on the port. The list varies depending on the adapter type. The list also includes an Auto Detect option, which indicates that the link speed should be auto-negotiated.

NOTE: If an installed adapter does not support forced link speeds, the **Configured Link Speed** settings and the **Apply** button are not displayed.

- **FA-PWWN** – This field displays the FA-PWWN status. FA-PWWN allows a switch to assign a virtual WWPN to the initiator. **Disabled** is the default setting.

NOTE:

  - Dynamic D_Port and FA-PWWN cannot be enabled simultaneously. If Dynamic D_Port is enabled and you want to enable FA-PWWN, you must first disable Dynamic D_Port. If FA-PWWN is enabled and you want to enable Dynamic D_Port, you must first disable FA-PWWN.
  - FA-PWWN is not available when trunking is enabled.
  - If DHCHAP is enabled, Dynamic D_Port and FA-PWWN are disabled.

  – The switch must support FA-PWWN. Refer to the documentation that accompanied the switch for instructions on configuring FA-PWWN on the switch.
  – The link is toggled if FA-PWWN is enabled, but the switch does not support FA-PWWN.
  – When a new WWPN is assigned using FA-PWWN, persistently stored configuration information associated with the original WWPN, such as driver parameters, is not applied to the newly assigned WWPN. The configuration information associated with the original WWPN must be reconfigured for the new WWPN.

- **Dynamic D_Port** – This field indicates displays the Dynamic D_Port status. Dynamic D_Port allows D_Port tests to be initiated on the switch side. **Enabled** is the default setting.

NOTE:

  - Dynamic D_Port testing is not available when trunking is enabled.
  - Dynamic D_Port and FA-PWWN cannot be enabled simultaneously. If Dynamic D_Port is enabled and you want to enable FA-PWWN, you must first disable Dynamic D_Port. If FA-PWWN is enabled and you want to enable Dynamic D_Port, you must first disable FA-PWWN.
  - Dynamic D_Port cannot be enabled when DHCHAP is enabled.
  - If Dynamic D_Port is enabled on an adapter, it is not supported in a direct-connect point-to-point environment. The adapter must be connected to a switch.

5.7 Configuring the Link Speed on a Port

To configure link speed on an FC port, perform these steps:

1. Select a host in the console tree-view. If applicable, select the **Emulex OneCommand** tab.
2. In the **Emulex Device Management** tree-view, select the FC port whose link speed you want to configure.
3. Select the FC **Firmware Parameters** tab (Figure 26).
4. Select a link speed from the **Configured Link Speed** list.
5. Click **Apply** to set the new link speed. The **Apply** button is enabled only if the currently selected link speed does not match the currently configured speed.

   If the speed has been set successfully, the following message is displayed.

Figure 27: Firmware Parameters Dialog

6. Click **OK**.
7. Reset the port to activate the new link speed setting. See Section 6.5, Resetting a Port, for instructions.

In some situations, the currently configured link speed is not in the supported speed list for the port. This situation can occur if a new SFP is installed that supports a different set of link speeds than the previously installed SFP. If the currently configured link speed is not in the supported speed list, the following message is displayed:

```
Warning: The currently configured port speed is not a valid supported speed.
Please select a link speed and click Apply.
```

The **Apply** button remains enabled until you select a valid port speed.

If the installed SFP is not supported by the adapter, you cannot configure a link speed. If this is attempted, the following message is displayed:

```
Unsupported optics installed.
```

5.8 Enabling and Disabling FA-PWWN

FA-PWWN allows a switch to assign a virtual WWPN to the initiator.

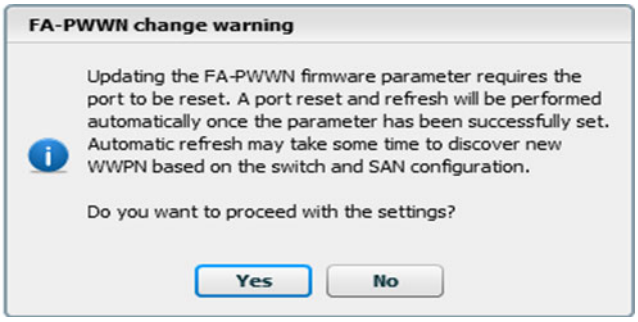
NOTE:

- The switch must support FA-PWWN. Refer to the documentation that accompanied the switch for instructions on configuring FA-PWWN on the switch.
- The link is toggled if FA-PWWN is enabled, but the switch does not support FA-PWWN.
- When a new WWPN is assigned using FA-PWWN, persistently stored configuration information associated with the original WWPN, such as driver parameters, is not applied to the newly assigned WWPN. The configuration information associated with the original WWPN must be reconfigured for the new WWPN.
- The FA-PWWN firmware parameter must be disabled to change the WWN. See Section 6.4, Changing the WWN Configuration, for information about changing WWN configuration.
- FA-PWWN is not available when trunking is enabled.

To enable or disable FA-PWWN, perform these steps:

1. Select a host in the console tree-view. If applicable, select the **Emulex OneCommand** tab.
2. In the **Emulex Device Management** tree-view, select the FC port on which you want enable or disable FA-PWWN.
3. Select the FC **Firmware Parameters** tab (Figure 26).
4. Select **Enable** or **Disable** from the **FA-PWWN** list.
5. Click **Apply**. The **FA-PWWN change warning** popup appears (Figure 28).
6. Click **Yes**.

Figure 28: FA-PWWN change warning Popup



7. A dialog appears notifying you that the parameter was successfully updated. Click **OK**.

OneCommand Manager displays the new WWNs.

NOTE: The speed of this operation depends on the size and infrastructure of the SAN.

5.9 Enabling and Disabling Dynamic D_Port

Dynamic D_Port allows D_Port tests to be initiated on the switch side. **Enabled** is the default setting.

NOTE:

- Dynamic D_Port does not appear on the **Firmware Parameters** tab if it is not supported.
- Dynamic D_Port must be disabled to use D_Port from the adapter. See Section 9.3, Running D_Port Tests, for information about running D_Port tests from the adapter.
- Dynamic D_Port testing is not available when trunking is enabled.
- Dynamic D_Port and FA-PWWN cannot be enabled simultaneously. If Dynamic D_Port is enabled and you want to enable FA-PWWN, you must first disable Dynamic D_Port. If FA-PWWN is enabled and you want to enable Dynamic D_Port, you must first disable FA-PWWN.
- If Dynamic D_Port is enabled on an adapter, it is not supported in a direct-connect point-to-point environment. The adapter must be connected to a switch.

To enable or disable Dynamic D_Port, perform these steps:

1. Select a host in the console tree-view. If applicable, select the **Emulex OneCommand** tab.
2. In the **Emulex Device Management** tree-view, select the FC port on which you want to enable or disable Dynamic D_Port.
3. Select the FC **Firmware Parameters** tab (Figure 26).
4. Select **Enable** or **Disable** from the **Dynamic D_Port** list.
5. Click **Apply**.

   A dialog appears notifying you that the parameter was successfully updated.
6. Click **OK**.

5.10 Using FC-SP DHCHAP Authentication

Use the **DHCHAP** tab to view and configure Fibre Channel Security Protocol (FC-SP) DHCHAP authentication between an adapter and a switch.

FC-SP-2 authentication is disabled by default. To enable it, the `enable_auth` parameter must be passed to the driver by typing the following command:

```
elxvcpcmd.exe enable_auth=1
```

After DHCHAP has been activated and configured, manually initiate authentication per adapter by clicking **Initiate Authentication** or by inducing a fabric login (FLOGI) time in accordance with the FC-SP standard to the switch. A FLOGI can also be caused by bringing the link between the switch and adapter down and then up (not available in read-only mode).

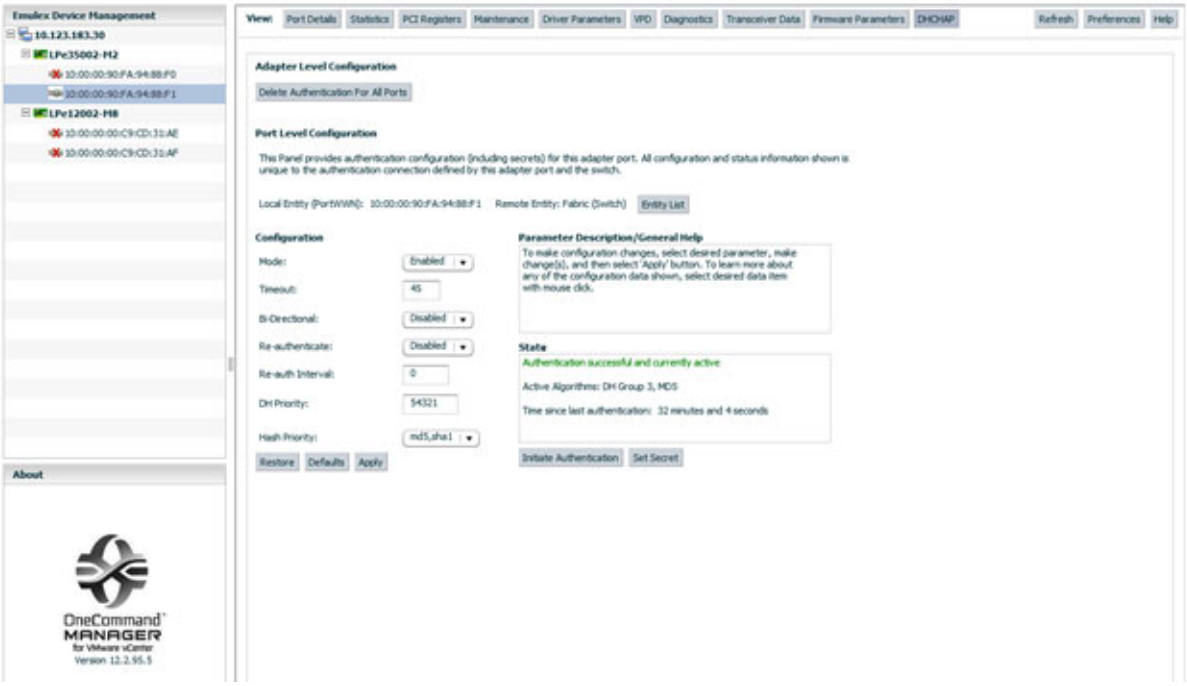
NOTE:

- Boot from SAN is not supported when DHCHAP authentication is enabled.
- DHCHAP is supported only on Windows and Linux operating systems.
- DHCHAP is available only for physical ports, not for virtual ports.
- The authentication driver parameters are available only on local hosts. The OneCommand Manager application GUI does not display this driver parameter for any remote hosts.
- DHCHAP is not supported on FA-PWWN ports.
- DHCHAP is not supported on LPe12000-series adapters.
- DHCHAP cannot be enabled when Dynamic D_Port is enabled.

NOTE: Authentication must be enabled at the driver level. Enable the `enable_auth` parameter before attempting to configure DHCHAP. See Section 6.6, Configuring Port Driver Parameters, for instructions on changing driver parameters. Authentication is disabled by default.

The **DHCHAP** tab (Figure 29) enables you to configure authentication.

Figure 29: DHCHAP Tab (LPe35000-Series Adapter Depicted)



The following **DHCHAP** tab fields and buttons are displayed:

- **Adapter-Level Configuration** area (Not supported on LPe12000-series adapters):
  - Click **Delete Authentication For All Ports** to permanently delete the entire authentication configuration for all the ports on the adapter.
- **Port-Level Configuration** area (Not supported on LPe12000-series adapters):
  - Click **Entity List** to see the list of entity pairs with a saved authentication configuration.
- **Configuration** area:
  - **Mode** – The mode of operation. Three modes are available:
    - **Enabled** – The FC function initiates authentication after issuing an FLOGI to the switch. If the connecting device does not support DHCHAP authentication, the software still continues with the rest of the initialization sequence.
    - **Passive** – The FC function does not initiate authentication, but participates in the authentication process if the connecting device initiates an authentication request.
    - **Disabled** – The FC function does not initiate authentication or participate in the authentication process when initiated by a connecting device. This mode is the default mode.
  - **Timeout** – During the DHCHAP protocol exchange, if the switch does not receive the expected DHCHAP message within a specified time interval, authentication failure is assumed (no authentication is performed). The time value ranges from 20 to 999 seconds and the default is 45 seconds.
  - **Bi-directional** – If enabled, the FC driver supports authentication initiated by either the switch or the FC function. If disabled, the driver supports only FC function-initiated authentication. The remote password must be configured to enable this setting. See Section 5.10.3, Setting or Changing Secrets, for instructions.
  - **Re-authenticate** – If enabled, the FC driver can periodically initiate authentication.
  - **Re-auth Interval** – The value in minutes that the FC driver uses to periodically initiate authentication. Valid interval ranges are 10 to 3600 minutes. The default is 300 minutes.
  - **DH Priority** – The priority of the five supported DH groups (Null group and groups 1, 2, 3, and 4) that the FC driver presents during the DHCHAP authentication negotiation with the switch.

  - **Hash Priority** – The priority of the two supported hash algorithms (MD5 and SHA1) that the FC driver presents during the DHCHAP authentication negotiation with the switch (default is MD5 first, then SHA1, 2, 3...).
  - Click **Restore**, **Defaults**, or **Apply** to restore parameters to their previous settings, to return parameters to their default settings, or to apply new parameter settings.

NOTE: Clicking **Restore** removes all current configuration settings, including port secrets and this switch/target connection.

- **Parameter Description/General Help** area:
  - This section of the dialog contains a brief description of the selected parameter and the options available for the parameter.
- **State** area:
  - This section of the dialog displays the authentication state. Possible states are Not Authenticated, Authentication In Progress, Authentication Success, and Authentication Failed.
- **Initiate Authentication** – After DHCHAP has been activated and configured, click this button to perform immediate authentication.
- **Set Secret** – Click this button to set a new local or remote secret in ASCII or hexadecimal (binary). See Section 5.10.3, Setting or Changing Secrets, for instructions.

5.10.1 Deleting Authentication for All Ports

NOTE:

- The driver authentication parameter `enable_auth` must be disabled before deleting authentication for all ports. See Section 6.6, Configuring Port Driver Parameters, for instructions on changing driver parameters.
- This command deletes the authentication configuration, including secrets, from the adapter flash memory. To activate the new driver settings, you must reload the driver.

To delete authentication for all ports, perform these steps:

1. Select a host in the console tree-view. If applicable, select the **Emulex OneCommand** tab.
2. In the **Emulex Device Management** tree-view, select the FC adapter on whose ports you want to delete authentication.
3. Select the **DHCHAP** tab (Figure 29).
4. Click **Delete Authentication For All Ports**.

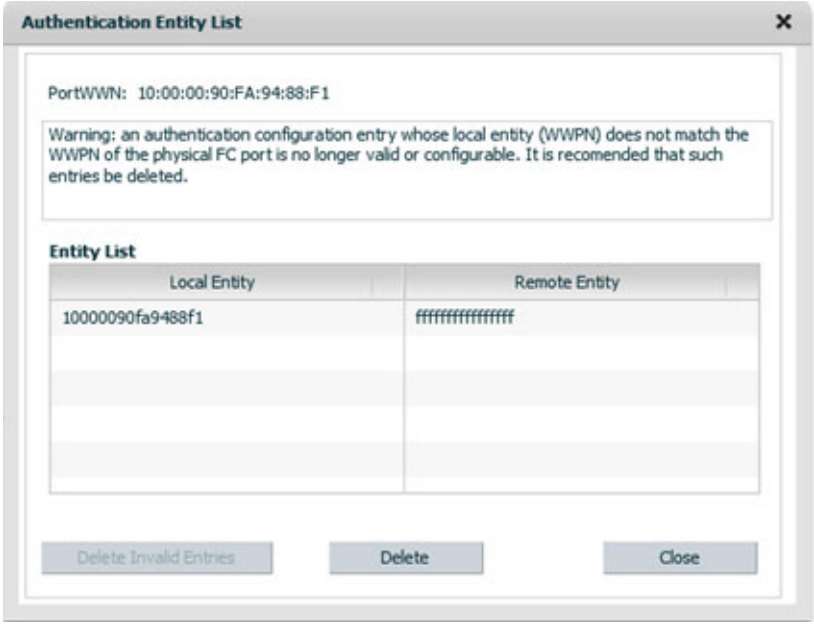
5.10.2 Viewing Saved Authentication Configuration Entities

The Entity List displays a list of entity pairs that have a saved authentication configuration. The list might include entity pairs for authentication configurations that are no longer valid or configurable. For example, the list would contain an entity pair whose configuration become obsolete and invalid after a port WWN change.

To view saved authentication configuration entities, perform these steps:

1. Select a host in the console tree-view. If applicable, select the **Emulex OneCommand** tab.
2. In the **Emulex Device Management** tree-view, select the adapter port whose authentication configuration entities you want to view.
3. Select the **DHCHAP** tab (Figure 29).
4. Click **Entity List**. The **Authentication Entity List** dialog appears (Figure 30).

Figure 30: Authentication Entity List Dialog



5.10.2.1 Deleting Authentication Entities

You can delete all invalid entities or particular entities.

To delete saved authentication configuration entities, perform these steps:

1. Select a host in the console tree-view. If applicable, select the **Emulex OneCommand** tab.
2. In the **Emulex Device Management** tree-view, select the adapter port whose authentication configuration entities you want to delete.
3. Select the **DHCHAP** tab (Figure 29).
4. Click **Entity List**. The **Entity List** dialog appears (Figure 30).
5. Click **Delete Invalid Entries** to remove all invalid entities (red), or select single or multiple entities and click **Delete**.

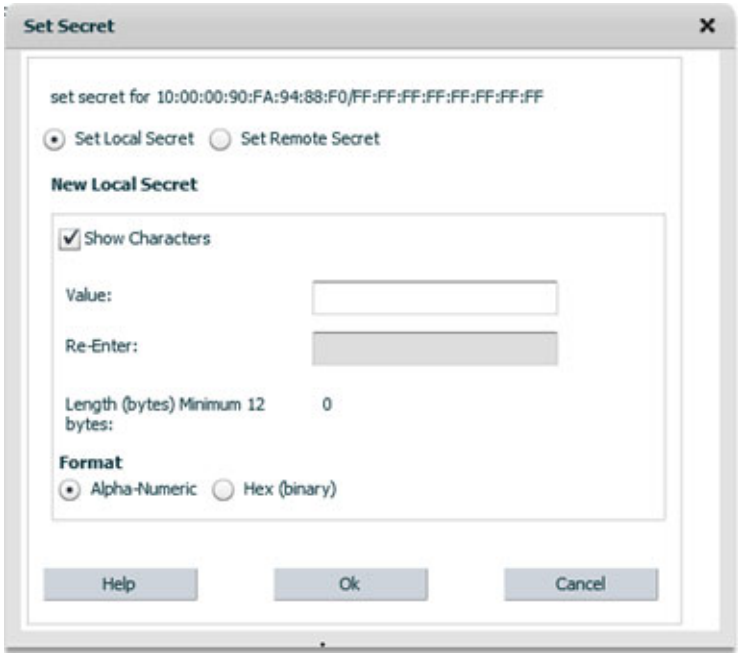
5.10.3 Setting or Changing Secrets

You can change or set the local or remote secret. The local secret is typically used by the driver when the adapter initiates authentication to the switch. The remote secret is used by the driver if the switch attempts to authenticate with the adapter. Bi-directional authentication requires the remote secret.

To set or change secrets, perform these steps:

1. Select a host in the console tree-view. If applicable, select the **Emulex OneCommand** tab.
2. In the **Emulex Device Management** tree-view, select the adapter port whose secrets you want to set or change.
3. Select the **DHCHAP** tab (Figure 29).
4. Click **Set Secret**. The **Set Secret** dialog appears (Figure 31).

Figure 31: Set Secret Dialog



5. Choose **Set Local Secret** or **Set Remote Secret**.
   - The FC driver uses the local password when the adapter initiates authentication to the switch (typical use).
   - The FC driver uses the remote password if the switch authenticates with the adapter. This situation is only possible when bi-directional is selected on the **DHCHAP** tab (Figure 29).
6. To see the password characters entered in the dialog, select **Show Characters**.
7. Enter the new value. Values must contain at least 12 bytes, and local and remote values must be different.
8. Re-enter the new value.
9. Select alphanumeric or hexadecimal format.
10. Click **OK**.

    A dialog notifies you that the secret was set.
11. Click **OK**.

CAUTION! Do not forget the password after one has been assigned. After a password is assigned to an adapter, subsequent DHCHAP configuration settings for that adapter, including the default configuration or new passwords, require you to enter the existing password to validate your request. No further changes can be made without the password.

NOTE: Click **Help** on the **Set Secret** dialog for assistance with secrets.

5.10.4 Changing the Authentication Configuration

NOTE: You can configure DHCHAP only on the local host.

To view or change authentication configuration, perform these steps:

1. Select a host in the console tree-view. If applicable, select the **Emulex OneCommand** tab.
2. In the **Emulex Device Management** tree-view, select the adapter port whose authentication configuration you want to change.
3. Select the **DHCHAP** tab (Figure 29).

NOTE: If the fields on this tab are dimmed, either authentication has not been enabled at the driver level or the local secret has not been set.

- For instructions on enabling the driver authentication parameter `enable_auth`, see Section 6.6, Configuring Port Driver Parameters.
- For instructions on setting the local secret, see Section 5.10.3, Setting or Changing Secrets.

4. Change the configuration values that you want.
5. Click **Apply.**

NOTE: If you click **Apply**, changes cannot be canceled.

To return settings to the status before you started this procedure, click **Restore** before you click **Apply**.

To return all settings to the default configuration, click **Defaults**.

CAUTION! This action also resets any passwords to NULL for this configuration.

Chapter 6: Managing Ports

This chapter pertains to managing ports.

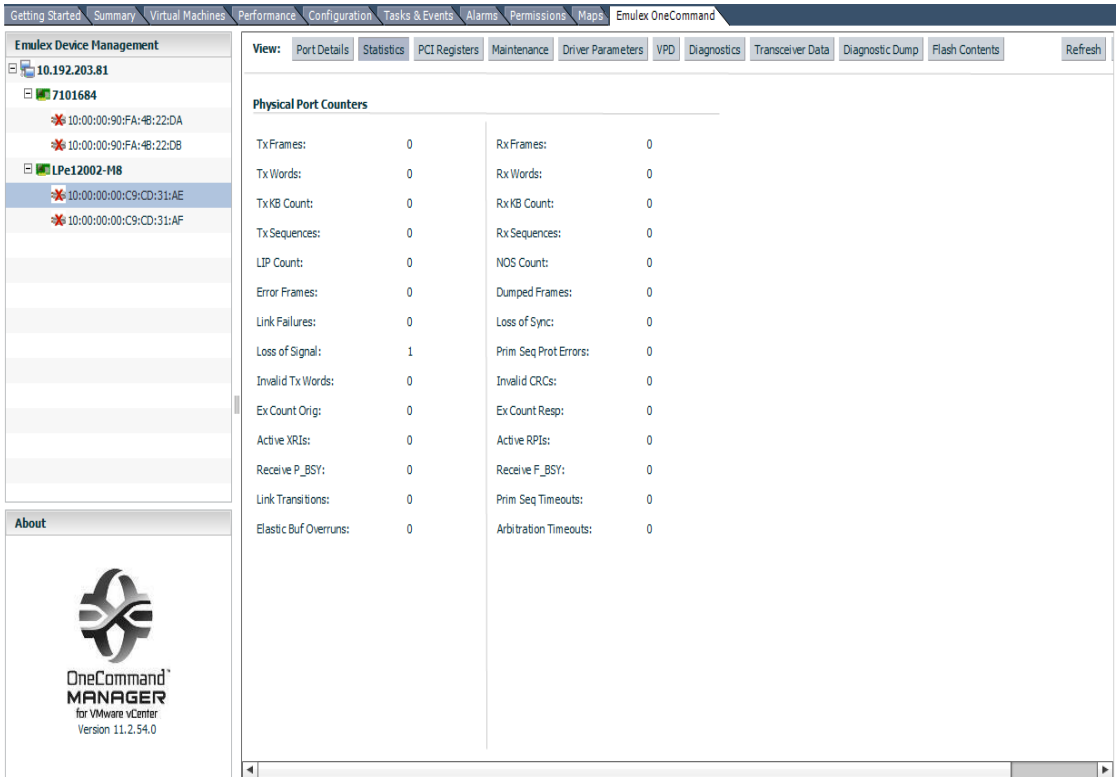
6.1 Viewing Port Statistics

When you select a port from the discovery-tree, the **Statistics** tab displays cumulative totals for error events and statistics on the port. Some statistics are cleared when the adapter is reset.

To view statistics for a port, perform these steps:

1. Select a host in the console tree-view, and if applicable, select the **Emulex OneCommand** tab.
2. In the **Emulex Device Management** tree-view, select the port whose statistics you want to view.
3. Select the **Statistics** tab (Figure 32).

Figure 32: Statistics Tab



The following **Port Statistics** tab fields are displayed:

- **Tx Frames** – The FC frames transmitted by this adapter port.
- **Tx Words** – The FC words transmitted by this adapter port.
- **Tx KB Count** – The FC kilobytes transmitted by this adapter port.
- **Tx Sequences** – The FC sequences transmitted by this adapter port.

- **LIP Count** – The number of LIP events that have occurred for the port. This field is supported only if the topology is arbitrated loop.

  Loop initialization consists of the following:
  - Temporarily suspending loop operations.
  - Determining whether loop-capable ports are connected to the loop.
  - Assigning AL_PA IDs.
  - Providing notification of configuration changes and loop failures.
  - Placing loop ports in the monitoring state.
- **Error Frames** – The number of frames received with CRC errors.
- **Link Failures** – The number of times the link has failed. A link failure can cause a timeout.
- **Loss of Signal** – The number of times the signal was lost.
- **Invalid Tx Words** – The total number of invalid words transmitted by this adapter port.
- **Ex Count Orig** – The number of FC exchanges originating on this port.
- **Active XRIs** – The number of active exchange resource indicators.
- **Received P_BSY** – The number of FC port-busy link response frames received.
- **Link Transitions** – The number of times the SLI port sent a link attention condition.
- **Elastic Buf Overruns** – The number of times the link interface has had its elastic buffer overrun.
- **Rx Frames** – The number of FC frames received by this adapter port.
- **Rx Words** – The number of FC words received by this adapter port.
- **Rx KB Count** – The received kilobyte count by this adapter port.
- **Rx Sequences** – The number of FC sequences received by this adapter port.
- **NOS Count** – The number of NOS events that have occurred on the switched fabric (not supported for an arbitrated loop).
- **Dumped Frames** – The number of frames that were lost due to a lack of host buffers available.
- **Loss of Sync** – The number of times loss of synchronization has occurred.
- **Prim Seq Prot Errs** – The primitive sequence protocol error count. This counter is incremented whenever there is any type of protocol error.
- **Invalid CRCs** – The number of frames received that contain CRC failures.
- **Ex Count Resp** – The number of FC exchange responses made by this port.
- **Active RPIs** – The number of remote port indicators.
- **Receive F_BSY** – The number of FC port-busy link response frames received.
- **Prim Seq Timeouts** – The number of times a primitive sequence event timed out.
- **Arbitration Timeouts** – The number of times that the arbitration loop has timed out. Large counts could indicate a malfunction somewhere in the loop or heavy usage of the loop.

6.2 Viewing PCI Registers

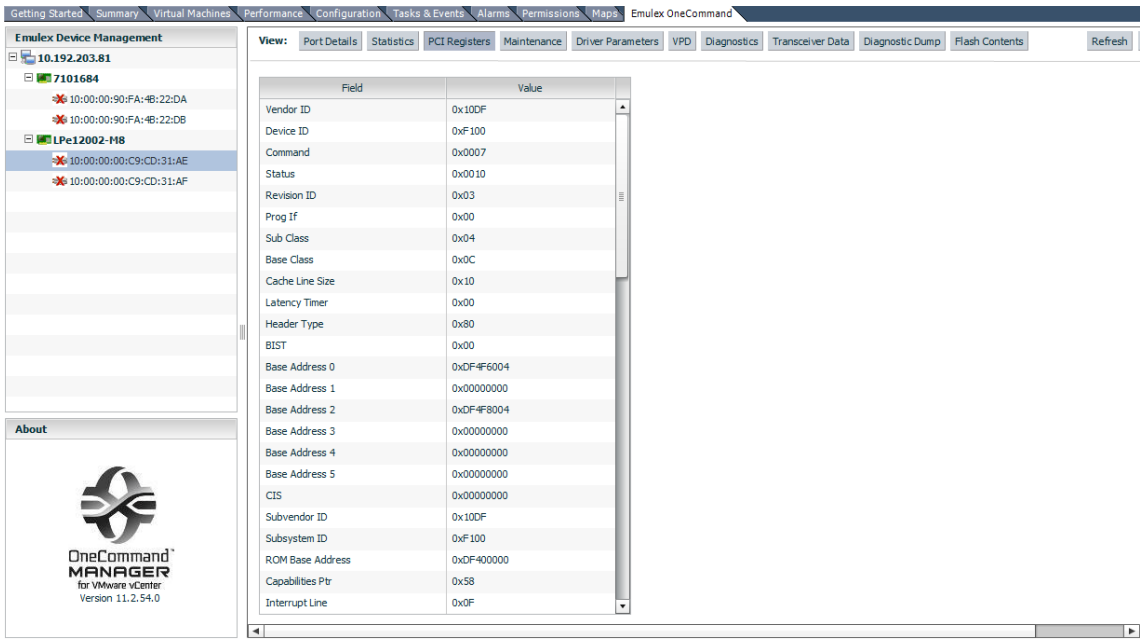
The **PCI Registers** tab displays PCI information, including PCIe details, about the selected port.

NOTE: The PCI fields can vary with the type of adapter installed.

To view PCI registers for a port, perform these steps:

1. Select a host in the console tree-view, and if applicable, select the **Emulex OneCommand** tab.
2. In the **Emulex Device Management** tree-view, select the port whose PCI information you want to view.
3. Select the **PCI Registers** tab (Figure 33).

Figure 33: PCI Registers Tab



6.3 Viewing Port Maintenance and Firmware Information

The **Maintenance** tab displays firmware information for a port.

To view firmware information for a port, perform these steps:

1. Select a host in the console tree-view, and if applicable, select the **Emulex OneCommand** tab.
2. In the **Emulex Device Management** tree-view, select the port whose firmware information you want to view.
3. Select the **Maintenance** tab for a port on an LPe12000-series adapter (Figure 34) or a port on any other adapter (Figure 35).

Figure 34: Maintenance Tab for a Port on an LPe12000-Series Adapter

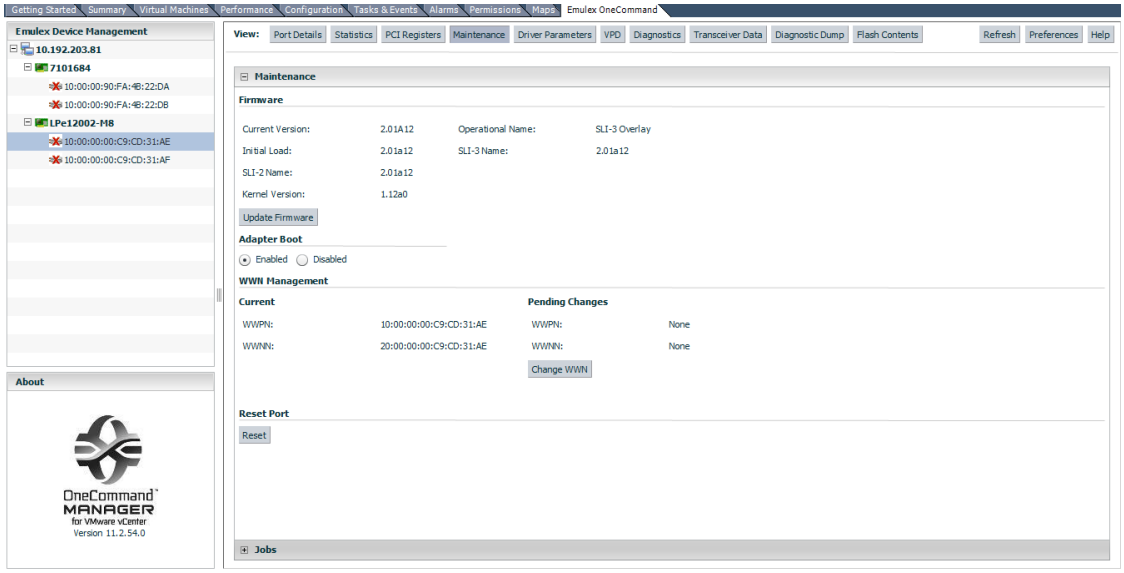
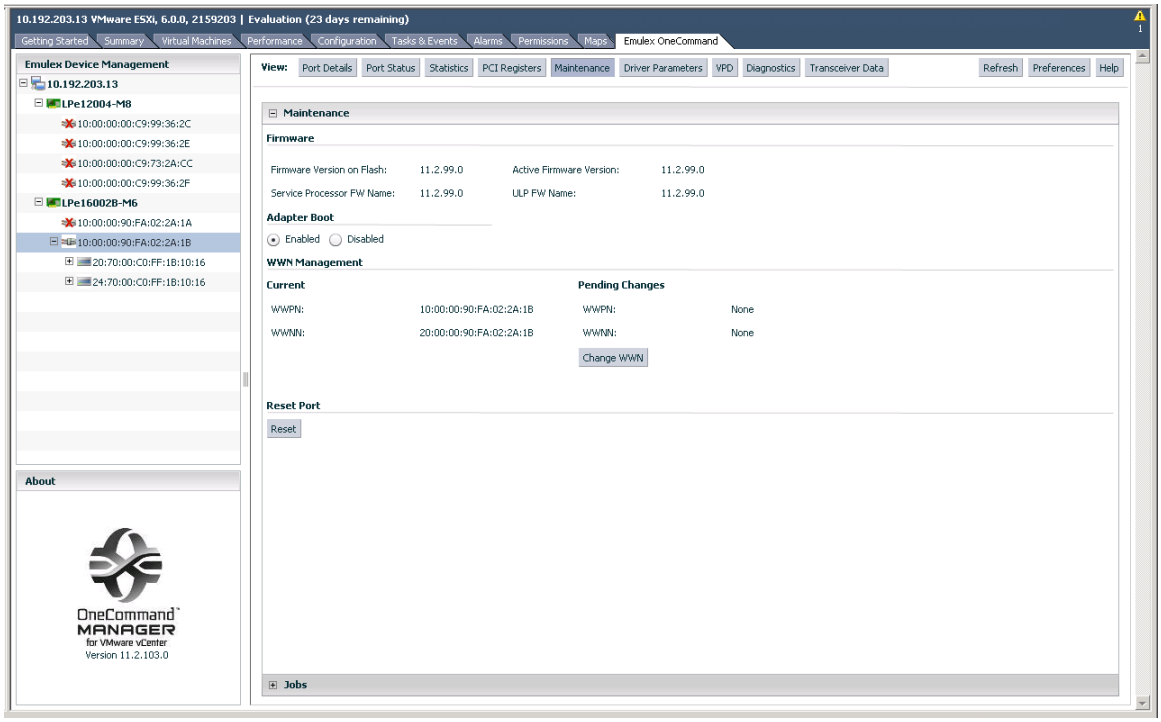


Figure 35: Maintenance Tab for a Port on Other Adapters



The **Maintenance** tab fields displayed depend on the adapter selected.

- **FC Port Firmware** area:
  - **Current Version** – The Emulex firmware version number for this adapter.
  - **Initial Load** – The firmware version stub responsible for installing SLI code into its proper slot.
  - **SLI-2 Name** – The name of the SLI-2 firmware overlay.
  - **Kernel Version** – The version of the firmware responsible for starting the driver.

  - **Operational Name** – The name of the operational firmware for the adapter.
  - **SLI-1 Name** – The name of the SLI-1 firmware overlay.
  - **SLI-3 Name** – The name of the SLI-3 firmware overlay.

  For information on updating firmware on an FC port, see Section 7.1, Updating Firmware for an LPe12000-Series Adapter.
- **WWN Management** area:
  - **Current**
    - **WWPN** – The WWPN for the selected adapter port.
    - **WWNN** – The WWNN for the selected adapter port.
  - **Pending Changes**
    - **WWPN** – If the WWPN has been changed, the new WWPN is displayed in this list. After rebooting, the new WWPN is displayed in the Current list.
    - **WWNN** – If the WWNN has been changed, the new WWNN is displayed in this list. After rebooting, the new WWNN is displayed in the Current list.

  See Section 6.4, Changing the WWN Configuration, for more information about changing the WWN configuration.

  For instructions on resetting a port, see Section 6.5, Resetting a Port.

6.4 Changing the WWN Configuration

The **Maintenance** tab enables you to change the WWPN and the WWNN of a selected adapter port. For example, you might want to use an installed adapter as a standby if another installed adapter fails. By changing the standby adapter's WWPN or WWNN, the adapter can assume the identity and configuration (such as driver parameters and persistent binding settings) of the failed adapter.

There are three options for referencing WWNs:

- Factory default WWN – The WWN as shipped from the factory.
- Non-volatile WWN – The values that are saved in the non-volatile adapter’s flash memory that survive a reboot or a power outage.
- Volatile WWN – A temporary value that is saved in the volatile memory on the flash. If volatile WWNs are set, they are used instead of the non-volatile WWNs. Volatile WWN changes require a warm system reboot to take effect. Volatile WWN changes are lost on systems that power cycle the adapters during the reboot.

CAUTION! Changing volatile WWNs results in taking the selected adapter offline. Ensure that this adapter is not controlling a boot device and that all I/O activity on this adapter has stopped before proceeding. This change could result in data loss or corruption.

Considerations When Changing WWN Configuration

- To avoid address conflicts, do not assign a WWNN or WWPN with OneCommand Manager for VMware vCenter if you also use another address management tool.
- The WWPN and WWNN in the Pending Changes list can display **n/a** instead of **None**. This display occurs when the remote host is busy processing some critical task and WWN Management cannot obtain the current state of WWN management.
- In an environment where preboot management exists, a WWPN or WWNN modified by OneCommand Manager for VMware vCenter can be overridden by preboot management, such as Lenovo System X BOFM and industry-standard CLP.

For example:

In an environment with CLP/BOFM, OneCommand Manager for VMware vCenter modifies the WWNN or WWPN. OneCommand Manager for VMware vCenter requires a reboot to complete the change. After a reboot, the CLP string is sent during the system boot and rewrites the WWNN or WWPN, or EFIBoot finds the BOFM protocol and uses the default WWNN or WWPN per the BOFM's command.

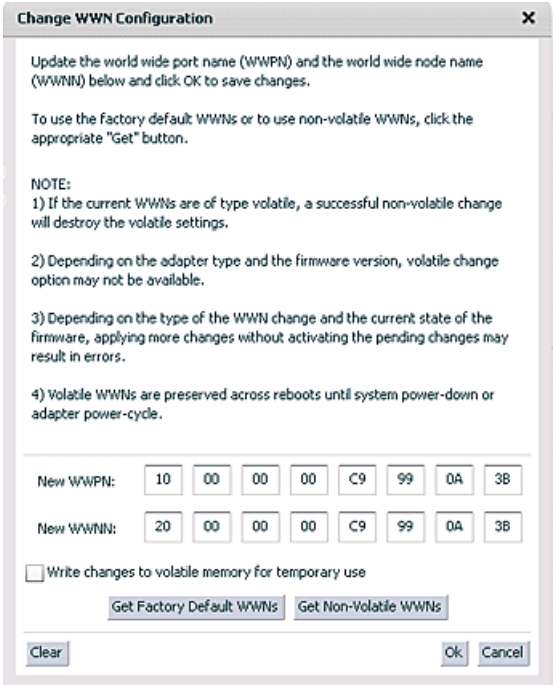
In an environment without CLP/BOFM, OneCommand Manager for VMware vCenter modifies the WWNN or WWPN. OneCommand Manager for VMware vCenter requires a reboot to complete the change. The system boots, and the OneCommand Manager for VMware vCenter-modified WWNN or WWPN is used.

- On a system where OneCommand Manager for VMware vCenter is installed, make sure the port numbers configured during the installation are open and dedicated to the OneCommand Manager for VMware vCenter server only. No other service should be listening on this port.
- The FA-PWWN firmware parameter must be disabled to change the WWN. See Section 5.8, Enabling and Disabling FA-PWWN, for information about disabling FA-PWWN.

To change a port's WWPN or WWNN, perform these steps:

1. Select a host in the console tree-view. If applicable, select the **Emulex OneCommand** tab.
2. In the **Emulex Device Management** tree-view, select the port for which you want to change the WWN information.
3. Select the **Maintenance** tab (Figure 34).
4. Click **Change WWN**. The **Change WWN Configuration** dialog is displayed (Figure 36).

Figure 36: Change WWN Configuration Dialog



5. Do one of the following:
   - Enter a new WWPN or WWNN.
   - Click **Get Factory Default WWNs** to load the settings that were assigned when the adapter was manufactured. These values can then be modified and saved as volatile or non-volatile WWNs.

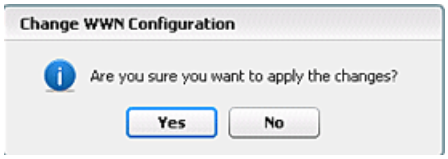
– Click **Get Non-Volatile WWNs** to load the current non-volatile WWN. These values can be modified and saved to volatile or non-volatile memory. You can edit the data returned from the button.

6. Check **Write changes to volatile memory for temporary use** to save the **New WWPN** and **New WWNN** settings as volatile WWNs. If cleared, the **New WWPN** and **New WWNN** settings are saved as non-volatile WWNs.

NOTE: If the adapter or firmware does not support volatile WWNs, **Write changes to volatile memory for temporary use** is not selected. This type of change is supported locally and using TCP/IP connections. This option is not available for remote in-band adapters, regardless of adapter models and firmware version.

7. Click **OK**. The following popup is displayed (Figure 37).

Figure 37: Change WWN Configuration Popup



8. Click **Yes**. The new WWPN and new WWNN values are saved. The new WWPN and WWNN appear in the Pending Changes list in the **WWN Management** area of the **Maintenance** tab.
9. Reboot the system for the changes to take effect (the new WWPN and WWNN appear in the Pending Changes list of the **Maintenance** tab until the system is rebooted). After rebooting, the changes are applied and appear in the Current section of the **Maintenance** tab.

NOTE: After changing the WWN of an adapter, you must reboot the system before trying to access the adapter on that system.

6.5 Resetting a Port

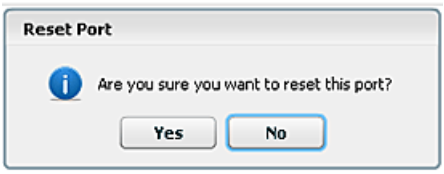
CAUTION! Do not reset an adapter port while copying or writing files. This action could result in data loss or corruption.

NOTE: When you reset a port or change the WWN configuration on OneCommand Manager for VMware vCenter, do not perform any active management operations on the ESXi host.

To reset a port, perform these steps:

1. Select a host in the console tree-view. If applicable, select the **Emulex OneCommand** tab.
2. In the **Emulex Device Management** tree-view, select the FC port you want to reset.
3. Select the **Maintenance** tab for LPe12000-series adapter ports (Figure 34) or for other adapter ports Figure 35.
4. Click **Reset**. The following popup is displayed (Figure 38).

Figure 38: Reset Port Popup



5. Click **Yes**. The adapter port resets. The reset can require several seconds to complete. While the adapter port is resetting, the message `Operation is in progress` is displayed. When the reset is finished, the message `Reset Port Completed` is displayed.

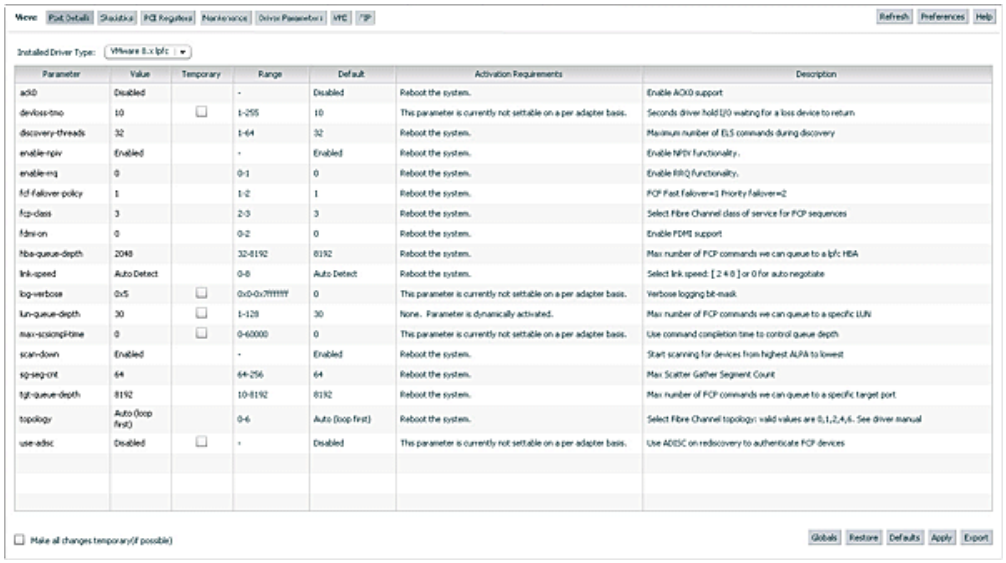
6.6 Configuring Port Driver Parameters

The **Driver Parameters** tab displays driver parameters for a port.

To view driver parameters for a port, perform these steps:

1. Select a host in the console tree-view, and if applicable, select the **Emulex OneCommand** tab.
2. In the **Emulex Device Management** tree-view, select the port whose driver parameters you want to view.
3. Select the **Driver Parameters** tab (Figure 39).

Figure 39: Driver Parameters Tab



The following **Driver Parameters** tab fields are displayed:

- **Installed Driver Type** – The current driver installed on this host.
- **Port Parameter table** – A list of port driver parameters and their current values.
  - **Parameter** – The driver parameter's name.
  - **Value** – The driver parameter's value.
  - **Temporary** – An indication that the value is temporary.
  - **Range** – The range of acceptable values for the driver parameter.
  - **Default** – The driver parameter's default value.
  - **Activation Requirements** – The steps required to activate the changed value of the driver parameter.
  - **Description** – The driver parameter's description.

To change the driver parameters for a port using the **Value** field, perform these steps:

1. Select a host in the console tree-view. If applicable, select the **Emulex OneCommand** tab.
2. In the **Emulex Device Management** tree-view, select the port for which you want to change the driver parameters.

3. Select the **Driver Parameters** tab (Figure 39).
4. In the driver parameter table, click the **Value** field of a parameter that you want to change. The range for the value is displayed. Enter a value in decimal or hexadecimal format, depending on how the current value is presented. If the value is in hexadecimal format, it is prefaced by 0x (for example, 0x2d). You can enter a hexadecimal value without the 0x. For example, if you enter `ff10`, this value is interpreted and displayed as 0xff10.
5. If you want the change to be temporary (causing the parameter to revert to its last permanent setting when the system is rebooted), select **Temporary**. This option is available only for dynamic parameters.
6. If you are making changes to multiple parameters, and you want all the changes to be temporary, select **Make all changes temporary**. This setting overrides the setting of **Make change temporary**. Only dynamic parameters can be made temporary.
7. Click **Apply**.

To set a port parameter value to the corresponding host parameter value, click **Globals**. All parameter values are set the same as the global, or host, values.

To apply the global values, click **Apply**.

If you changed parameters but did not click **Apply,** and you want to restore the parameters to their last saved values, click **Restore**.

To reset all parameter values to their default (factory) values, click **Defaults**.

To save driver parameters to a file, perform these steps:

1. Select a host in the console tree-view. If applicable, select the **Emulex OneCommand** tab.
2. In the **Emulex Device Management** tree-view, select the FC port for which you want to change the driver parameters.
3. Select the **Driver Parameters** tab (Figure 39).
4. Click **Export** to create and save a desired port parameter configuration. Each definition is saved in a comma-delimited file with the following format:
   `<parameter-name>=<parameter-value>`
5. Click **Apply** to apply your configuration changes.

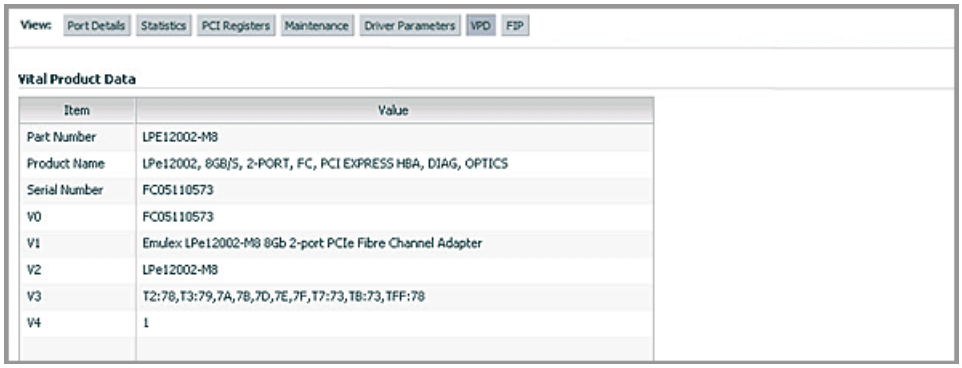
6.7 Viewing Port Vital Product Data (VPD)

The **VPD** tab displays vital product data (if available) for the selected port, such as the product name, part number, serial number, and so on.

To view VPD information for a port, perform these steps:

1. Select a host in the console tree-view, and if applicable, select the **Emulex OneCommand** tab.
2. In the **Emulex Device Management** tree-view, select the port whose VPD information you want to view.
3. Select the **VPD** tab (Figure 40).

Figure 40: VPD Tab



Item	Value
Part Number	LPE12002-M8
Product Name	LPe12002, 8GB/S, 2-PORT, FC, PCI EXPRESS HBA, DIAG, OPTICS
Serial Number	FC05110573
V0	FC05110573
V1	Emulex LPe12002-M8 8Gb 2-port PCIe Fibre Channel Adapter
V2	LPe12002-M8
V3	T2:78,T3:79,7A,7B,7D,7E,7F,T7:73,T8:73,TFF:78
V4	1

The following **VPD** tab fields are displayed:

- **Part Number** – The adapter's part number.
- **Product Name** – The product information about the selected adapter port.
- **Serial Number** – The adapter's serial number.
- **VO** – Vendor-unique data. V indicates a vendor-specific field. An adapter can have none, one, or more of these fields defined. Valid values for this field are VO (the letter O, not the number zero) and V*x* (where *x* is a number).

NOTE: Some adapters display additional VPD information such as EC and MN.

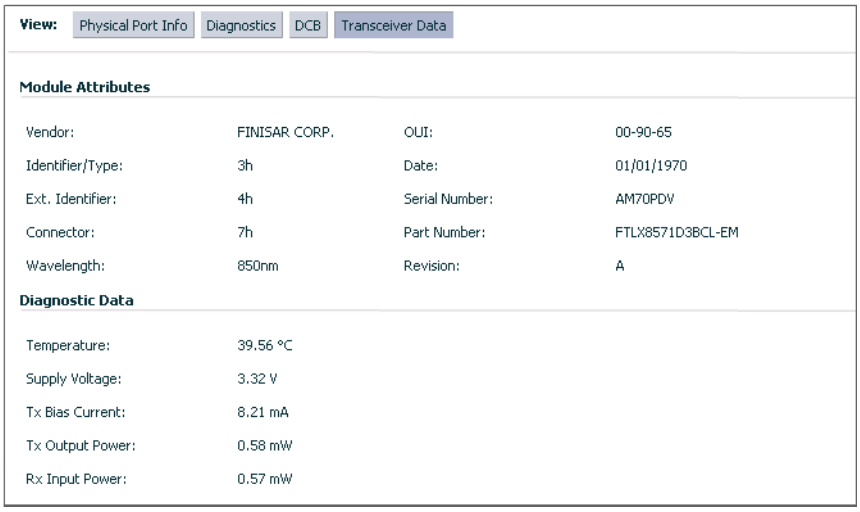
6.8 Viewing Port Transceiver Information

The **Transceiver Data** tab displays transceiver information such as vendor name, serial number, and part number. If the adapter or transceiver does not support some or all of the transceiver data, the fields display **N/A**.

To view transceiver information for a port, perform these steps:

1. Select a host in the console tree-view, and if applicable, select the **Emulex OneCommand** tab.
2. In the **Emulex Device Management** tree-view, select the port whose transceiver information you want to view.
3. Select the **Transceiver Data** tab (Figure 41).

Figure 41: Port Transceiver Data Tab



The following **Transceiver Data** tab fields are displayed:

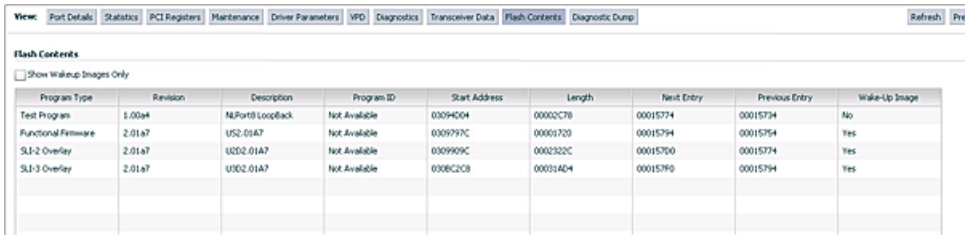
- **Module Attributes** area:
  - **Vendor** – The name of the vendor.
  - **Identifier/Type** – A value that specifies the physical device described by the serial information.
  - **Ext. Identifier** – Additional information about the transceiver.
  - **Connector** – The external optical or electrical cable connector provided as the media interface.
  - **Wavelength** – The nominal transmitter output wavelength at room temperature.
  - **OUI** – The vendor's Organizationally Unique Identifier. It is also known as the IEEE Company Identifier for the vendor.
  - **Date** – The vendor's date code in the MM/DD/YY format.
  - **Serial Number** – The serial number provided by the vendor.
  - **Part Number** – The part number provided by the SFP vendor.
  - **Revision** – The vendor revision level.
- **Diagnostic Data** area:
  - **Temperature** – The internally measured module temperature.
  - **Supply Voltage** – The internally measured supply voltage in the transceiver.
  - **Tx Bias Current** – The internally measured Tx bias current.
  - **Tx Output Power** – The measured Tx output power.
  - **Rx Input Power** – The measured Rx input power.

6.9 Viewing Flash Contents for an FC Port

To view the flash contents for an FC port, perform these steps:

1. Select a host in the console tree-view, and if applicable, select the **Emulex OneCommand** tab.
2. In the **Emulex Device Management** tree-view, select the FC port whose Flash contents you want to view.
3. Select the **Flash Contents** tab. The Flash Contents information is displayed (Figure 42).

Figure 42: FC Port Flash Contents



4. Select **Show Wakeup Images Only** if you want to see only the flash contents with the wake-up images.

6.10 Viewing Target Information

When you select a port target associated with an adapter from the **Emulex Device Management** tree-view, the **Target Information** tab displays information associated with that target.

To view target information, perform these steps:

1. Select a host in the console tree-view, and select the **Emulex OneCommand** tab.
2. In the **Emulex Device Management** tree-view, select the target port whose information you want to view. The **Target Information** tab appears (Figure 43).

Figure 43: Target Information Tab

The following **Target Information** tab fields are displayed:

- **FC ID** – The FC ID for the target; assigned automatically in the firmware.
- **SCSI Bus Number** – The SCSI bus number to which the target is mapped.
- **SCSI Target Number** – The target's identifier on the SCSI bus.
- **Node WWN** – A unique 64-bit number, in hexadecimal, for the target (N_PORT or NL_PORT).
- **Port WWN** – A unique 64-bit number, in hexadecimal, for the fabric (F_PORT or Switched Fabric Loop Port [FL_PORT]).
- **OS Device Name** – The operating system device name.

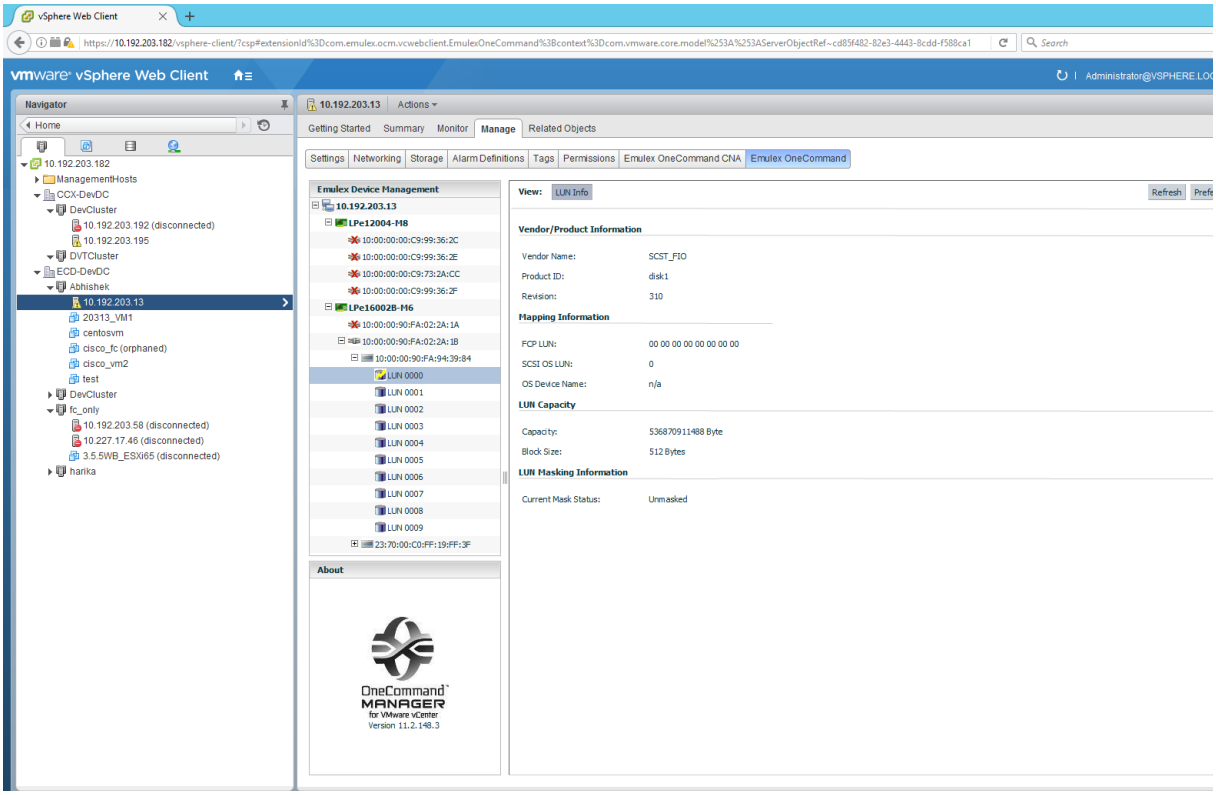
6.11 Viewing LUN Information

When you select a LUN associated with an adapter from the **Emulex Device Management** tree-view, the **LUN Info** pane displays information associated with that LUN.

To view LUN information, perform these steps:

1. Select a host in the console tree-view, and if applicable, select the **Emulex OneCommand** tab.
2. In the **Emulex Device Management** tree-view, select the LUN whose information you want to view. The corresponding **LUN Info** pane is displayed (Figure 44).

Figure 44: LUN Info Tab



The following **LUN Information** tab fields are displayed:

- **Vendor Product Information** area:
  - **Vendor Name** – The name of the vendor of the LUN.
  - **Product ID** – The vendor-specific ID for the LUN.
  - **Revision** – The vendor-specific revision number for the LUN.
- **Mapping Information** area:
  - **FCP LUN** – The FC identifier used by the adapter to map to the operating system LUN.
  - **SCSI OS LUN** – The SCSI identifier used by the operating system to map to the specific LUN.
  - **OS Device Name** – The name assigned by the operating system to the LUN.

- **LUN Capacity** area: LUN capacity information is provided only when the LUN is a mass-storage (disk) device. Other devices, such as tapes and scanners, do not display capacity.
  - **Capacity** – The capacity of the LUN, in megabytes.
  - **Block Size** – The length of a logical unit block, in bytes.
- **LUN Masking Information** area:
  - **Current Mask Status** – The current status is masked or unmasked.

The adapter information that is displayed depends upon the type of adapter that you select.

Chapter 7: Updating Firmware

OneCommand Manager for VMware vCenter enables you to update firmware for a single adapter or simultaneously for multiple adapters.

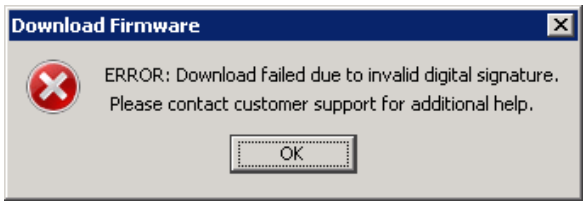
The submitted firmware update job can be tracked in the VMware tasks window.

Multiple firmware update jobs can be submitted for different adapters and ports on the same or different ESXi hosts simultaneously to OneCommand Manager for VMware. However, only a single job is processed on a given ESXi host. The remaining jobs on that host will be queued and processed sequentially.

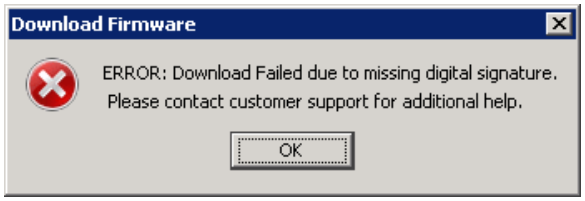
The firmware update progresses in the background until all the jobs are completed. During this period, you can still browse through the other tabs. However, if you start a firmware update and log out from the console before the firmware update is completed, all pending jobs fail.

NOTE: If a secure version of firmware (version 11.0 or later) is installed on an LPe16000-series adapter and you want to update to an earlier unsecured version of firmware, you must remove the secure firmware jumper block before performing the update. Refer to the installation guide for the adapter for more information.

If you attempt to update unauthenticated firmware for a secure adapter, the following error message will be displayed. (Not supported on LPe12000-series adapters.)



If you attempt to update unsecured firmware for a secure adapter, the following error message will be displayed. (Not supported on LPe12000-series adapters.)



Contact customer support for more information.

7.1 Updating Firmware for an LPe12000-Series Adapter

CAUTION! Updating firmware or boot code on an LPe12000-series adapter that is being used to boot from SAN is not advisable. After the update has completed, an adapter reset is issued that can cause a loss of connectivity to the SAN and possible loss of data. To update firmware on an LPe12000-series adapter, you must make sure that the adapter is not currently being used to boot from SAN.

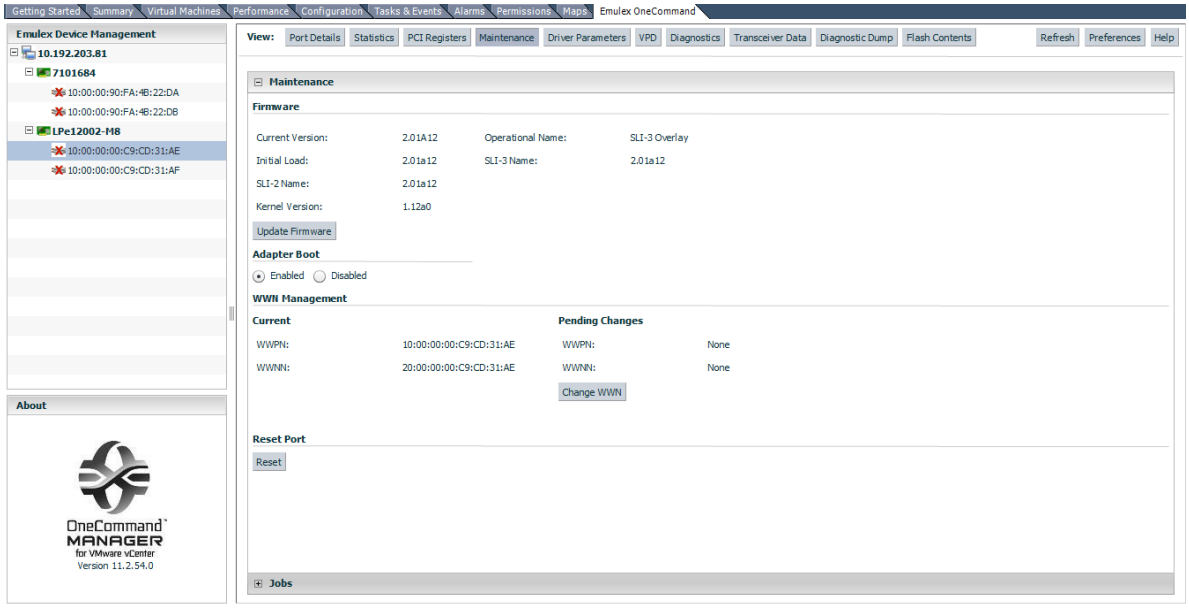
Do one of the following:

- Move the adapter to be updated to a non-boot from SAN host, and perform the update from that location.
- If the host with the target adapter is also hosting other boot from SAN adapters, perform a boot from SAN using one of the other boot from SAN adapters. The target adapter can now be updated.

To update firmware for a port on an LPe12000-series adapter, perform these steps:

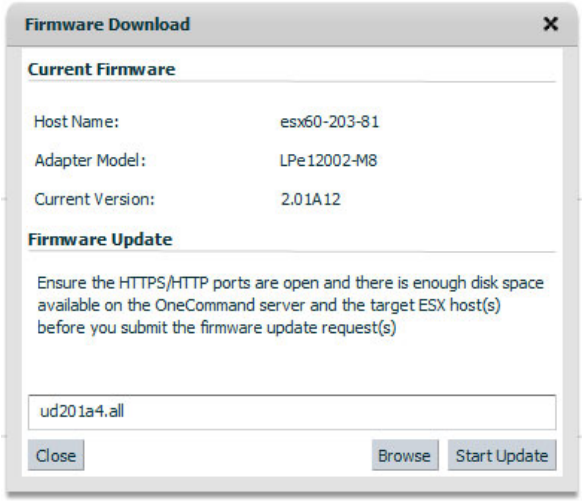
1. Select a host in the console tree-view; and, if applicable, select the **Emulex OneCommand** tab (Figure 5).
2. In the **Emulex Device Management** tree-view, select LPe12000-series adapter port for which you want to update firmware.
3. Select the **Maintenance** tab (Figure 45).

Figure 45: Maintenance Tab



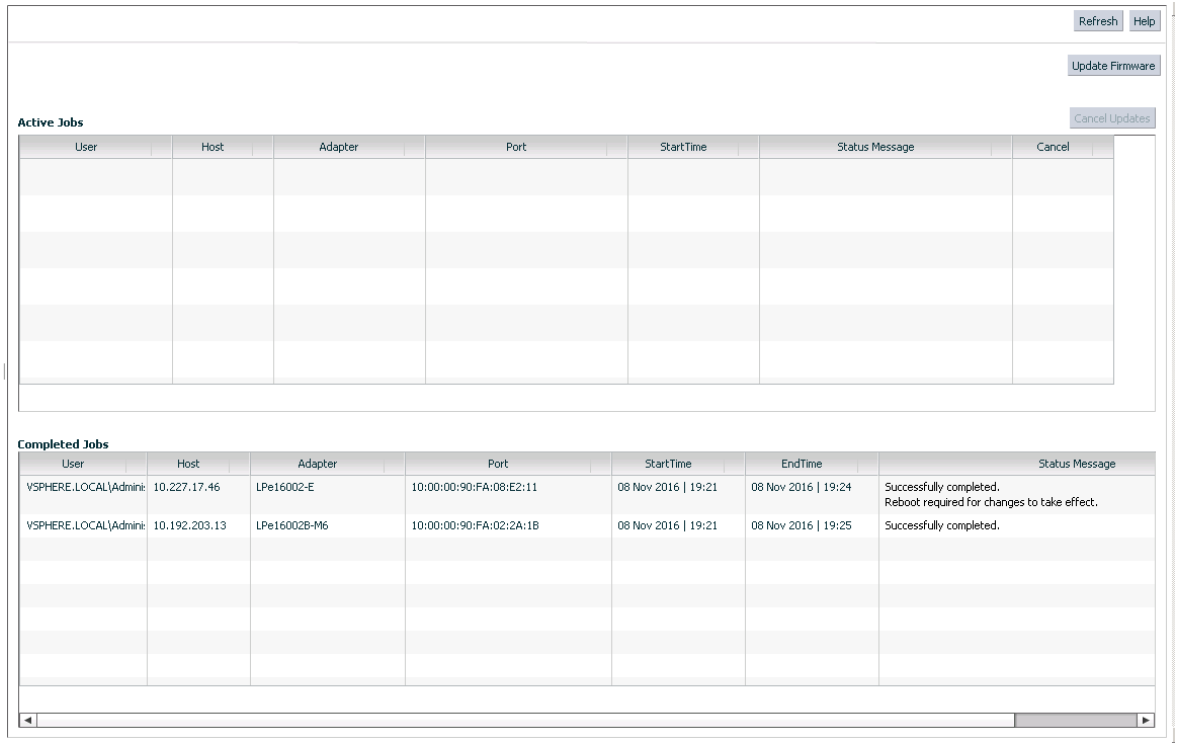
4. Click **Update Firmware**. If a popup appears, click **Yes**. The **Firmware Download** dialog is displayed (Figure 46).

Figure 46: Firmware Download Dialog



5. Click **Browse** and navigate to the unzipped, extracted image file that you want to download.
6. On the browse window, select the file and click **OK**. The **Firmware Download** dialog appears.
7. Click **Start Update**. A message prompting you to confirm the firmware update appears.
8. Click **Yes**. When the update begins, the **Jobs** window is displayed (Figure 47).

Figure 47: Jobs Window



A status message in the **Active Job** list displays the progress of the download. The ports on which the firmware is being downloaded have the status **Job is in progress**; the others have **Waiting in queue to start**. When the download is completed, the entry moves to the **Completed Jobs** list. The **Status Message** column in the **Completed Jobs** list displays the status of the completed job.

NOTE: The firmware update progresses in the background until all the jobs are completed. During this period, you can still browse through the other tabs.

If you start a firmware update and log out from the console before the firmware update is completed, all pending jobs fail.

7.1.1 Updating Firmware on an LPe12000-Series Adapter in a Host

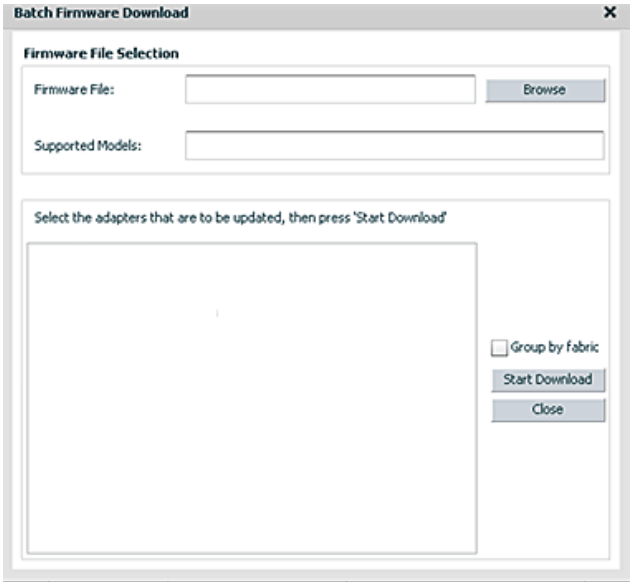
On the system where OneCommand Manager for VMware vCenter is installed, make sure the port numbers configured during the installation are open and dedicated to the OneCommand Manager for VMware vCenter server only. No other service should be listening on this port.

Before you can perform a batch update, the firmware file must be downloaded from www.broadcom.com and extracted to a directory on your local drive.

To update firmware for compatible adapters, perform these steps:

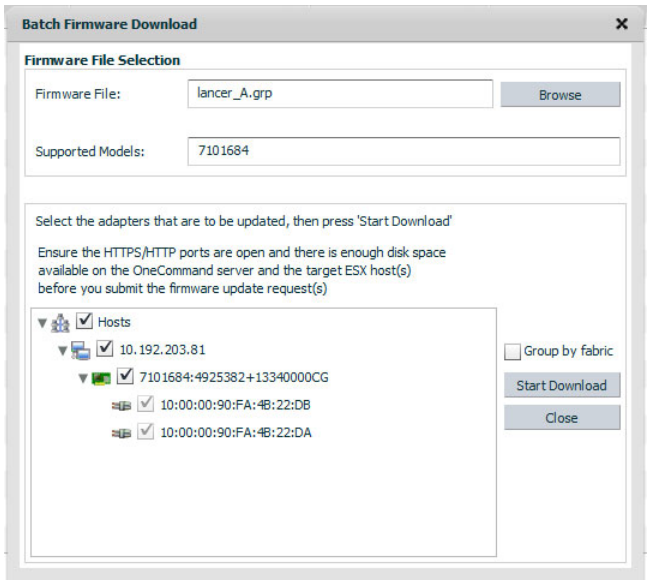
1. Select a host in the console tree-view, and if applicable, select the **Emulex OneCommand** tab.
2. Select the **Maintenance** tab and click **Update Firmware**. The **Batch Firmware Download** dialog appears (Figure 48).

Figure 48: Batch Firmware Download Dialog



3. Click **Browse** to find the firmware file and click **Open**.
4. Click **Start Download** (Figure 49).

Figure 49: Populated Batch Firmware Download Dialog



The tree-view displays all adapters and their corresponding hosts for which the selected firmware file is compatible. Use the check boxes next to the host and adapter entries to select or deselect an entry. Selecting or clearing an adapter selects or removes that adapter, respectively; selecting a host removes or selects all eligible adapters for that host.

To view the compatible adapters in a fabric-centric mode, select **Group by Fabric**.

For adapters where each individual port can have new firmware installed, you can select the ports on the adapter to which you want to download firmware.

5. Make your selections and click **Start Download**. When a message prompting you to confirm the firmware update appears, click **Yes**.

   When the update begins, a status message in the Active Job list displays the progress as either **Job is in progress** or **Waiting in queue to start**. The ports on which the firmware is being downloaded have the status **Job is in progress**; the others have **Waiting in queue to start**. You can select the check box to cancel the jobs with status **Waiting in queue to start**. When download is completed, the entry moves to the Completed Jobs list. The **Status Message** column in the **Completed Jobs** list displays the status of the completed job.

NOTE: If you start a firmware update and log out from the console before the firmware update is completed, all pending jobs fail.

The firmware update progresses in the background until all the jobs are completed. During this period, you can still browse through the other tabs.

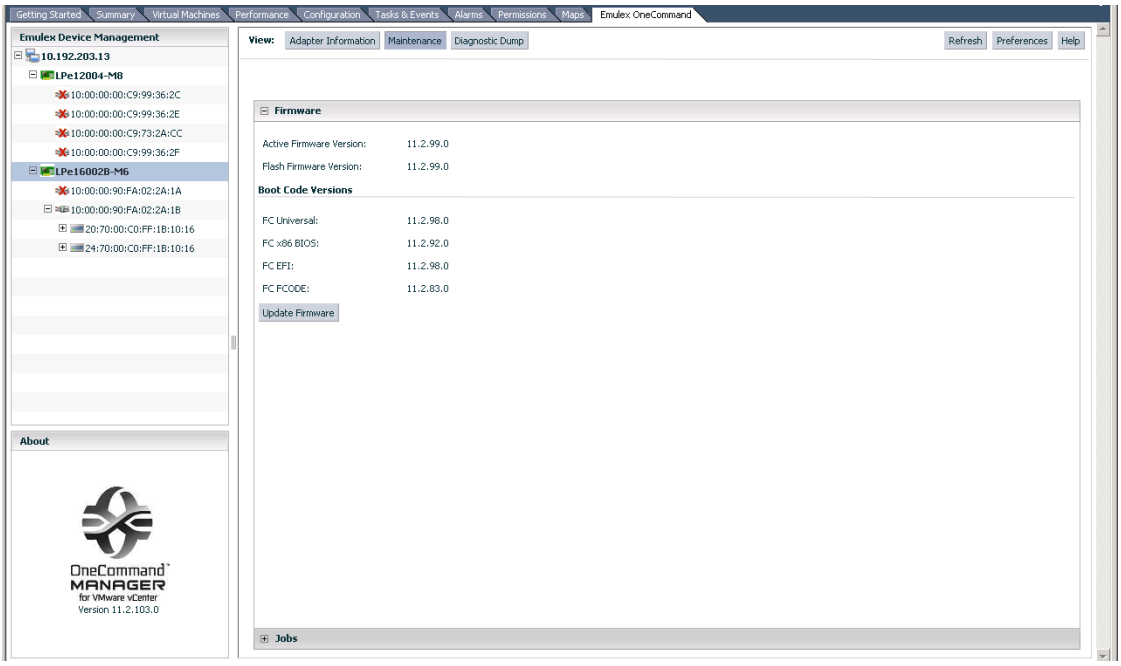
7.2 Updating Firmware for All Other Adapters

For all adapters except LPe12000-series adapters, you update the firmware for the entire adapter and not for individual ports.

To update firmware for an adapter, perform these steps:

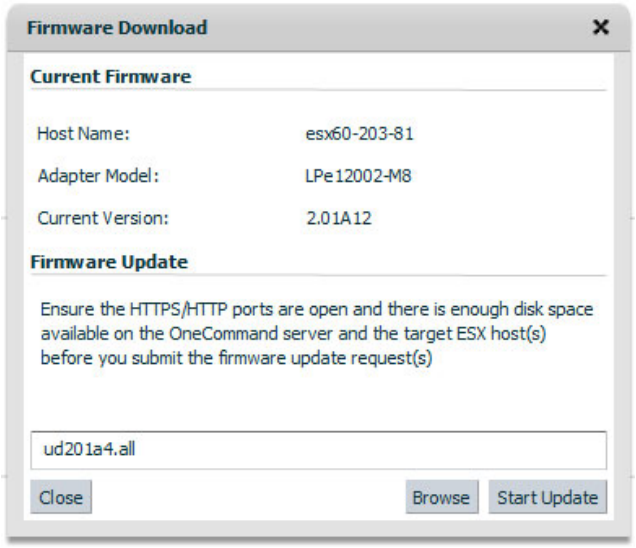
1. Select a host in the console tree-view, and if applicable, select the **Emulex OneCommand** tab.
2. In the **Emulex Device Management** tree-view, select the adapter for which you want to update firmware information.
3. Select the **Maintenance** tab (Figure 50).

Figure 50: Maintenance Tab



4. Click **Update Firmware**. If a popup appears, click **Yes**. The **Firmware Download** dialog is displayed (Figure 51).

Figure 51: Firmware Download Dialog



5. Click **Browse** and navigate to the unzipped, extracted image file that you want to download.
6. On the browse window, select the file and click **OK**.
7. Click **Start Update**.

   When the update begins, the **Jobs** window is displayed (Figure 56). A status message in the **Active Job** list displays the progress of the download. The ports on which the firmware is being downloaded have the status **Job is in progress**; the other ports display the **Waiting in queue to start** status.

   When the download has completed, the entry moves to the **Completed Jobs** list. The **Status Message** column in the **Completed Jobs** list displays the status of the completed job.

   You can monitor jobs submitted through the OneCommand Manager for VMware vCenter command line interface. If you start a firmware update and log out from the console before the firmware update is completed, all pending jobs fail. The firmware update progresses in the background until all the jobs are completed. During this period, you can still browse through the other tabs. The firmware update job submitted can also be tracked in the VMware tasks window.
8. Open **Firmware Summary**, and the updated firmware information for the selected adapter is displayed.

   For LPe35000-series adapters only:

   In some cases, a firmware update requires a firmware reset, depending on the features available in the new firmware. A firmware reset is performed automatically if it is needed.

   If a firmware reset occurs when the firmware is downloaded, a message similar to the following appears:

   ```
   Download successfully completed.
   ```

   In some cases, a full reboot is required to activate new firmware or to enable a new feature. In that case, a message similar to one of the following messages appears after the firmware download is complete:

   ```
   Download successfully completed. Please reboot the system to activate new firmware.
   Download completed. Some features require an optional reboot. Refer to the Adapter's Firmware and Boot Code Release Notes for details.
   ```

   For a list of features that require a reboot in order to be enabled, refer to the *Emulex LPe35000-Series HBA Firmware and Boot Code Release Notes*.

7.2.1 Performing a Batch Firmware Update in Cluster View

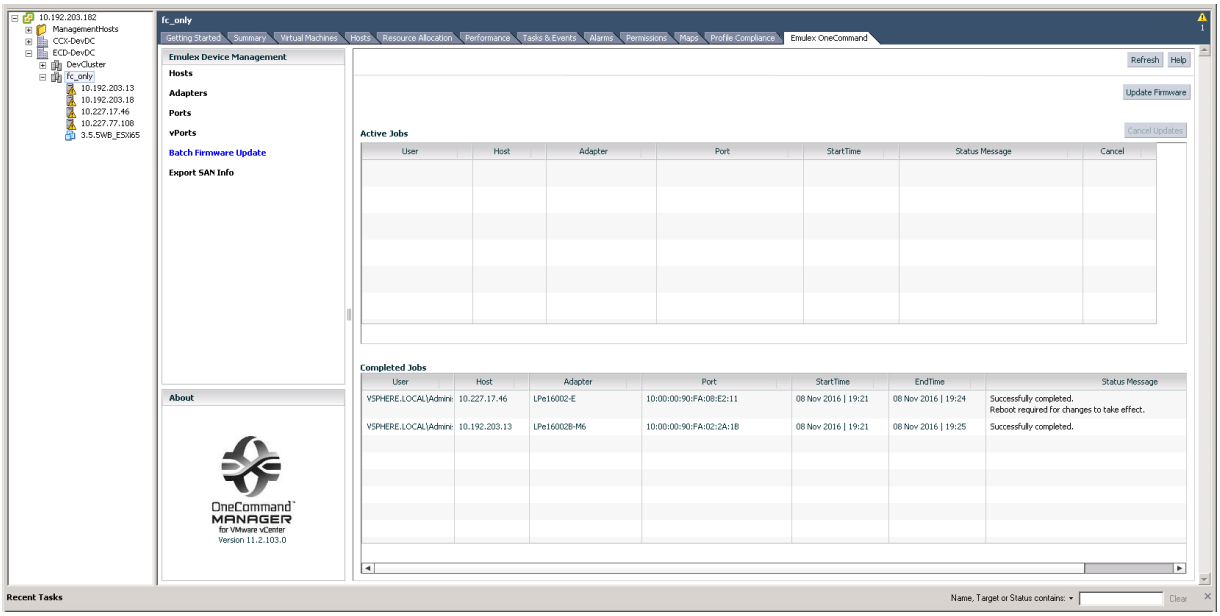
Before you can perform a batch update, you must download the firmware file from www.broadcom.com and extract it into a directory on your local drive.

NOTE: On the system where OneCommand Manager for VMware vCenter is installed, make sure that the port numbers configured during the installation are open and dedicated to the OneCommand Manager for VMware vCenter server only. No other service should be listening on this port.

To perform a batch firmware update on a host, perform these steps:

1. Select a cluster in the console tree-view, and if applicable, select the **Emulex OneCommand** tab.
2. From the **Emulex Device Management** options, select **Batch Firmware Update** (Figure 52)**.** The **Batch Firmware Download** dialog appears (Figure 48).

Figure 52: Batch Firmware Update Information



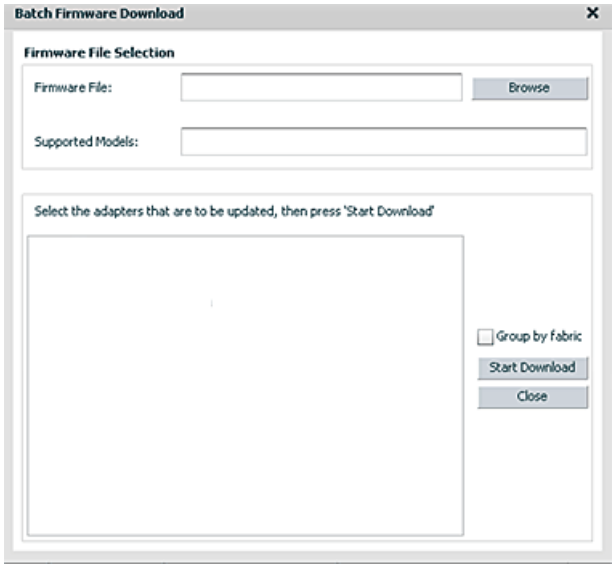
3. Click **Start Download** to install firmware on multiple adapters in a single step. Batch firmware loading is restricted to a single firmware file and to all accessible adapters for which that file is compatible.

7.2.2 Updating Firmware on Multiple Adapters in a Host

To update firmware for multiple adapters on a single host, perform these steps:

1. Select a host in the console tree-view, and if applicable, select the **Emulex OneCommand** tab.
2. Select the **Maintenance** tab and click **Update Firmware**. If a popup appears, click **Yes**. The **Batch Firmware Download** dialog is displayed (Figure 53).

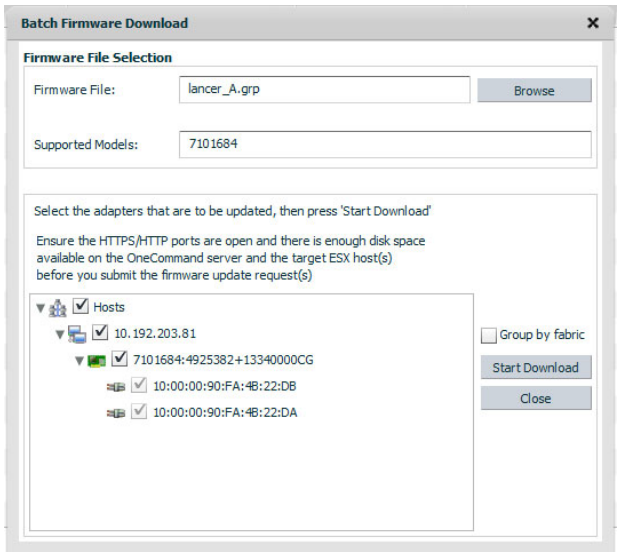
Figure 53: Batch Firmware Download Dialog



NOTE: Do not select a particular tree element for this operation.

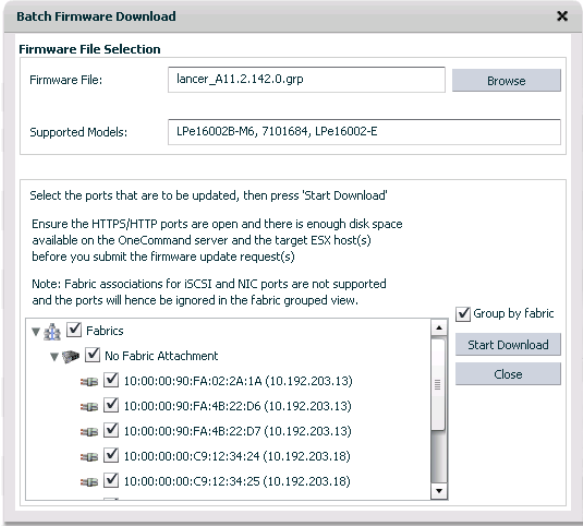
3. Click **Browse,** and a search dialog appears. On the search dialog, select the file that you want to use and click **OK**. A status message appears indicating that OneCommand Manager for VMware vCenter is searching for compatible adapters. After compatible adapters are found, the following is displayed in the **Batch Firmware Download** dialog (Figure 54):
   - **Firmware File** – This field displays the selected image file name.
   - **Supported Models** – This field displays a list of all adapter models that are compatible with the selected image file.
   - The set of compatible adapters appears in the dialog's tree-view.
4. To view the compatible adapters in host-centric mode, make sure that **Group by fabric** is not selected.

Figure 54: Batch Firmware Download Dialog–Host-Centric View



5. To view the compatible adapters in a fabric-centric mode, select **Group by fabric**.

Figure 55: Batch Firmware Download Dialog–Fabric-Centric View



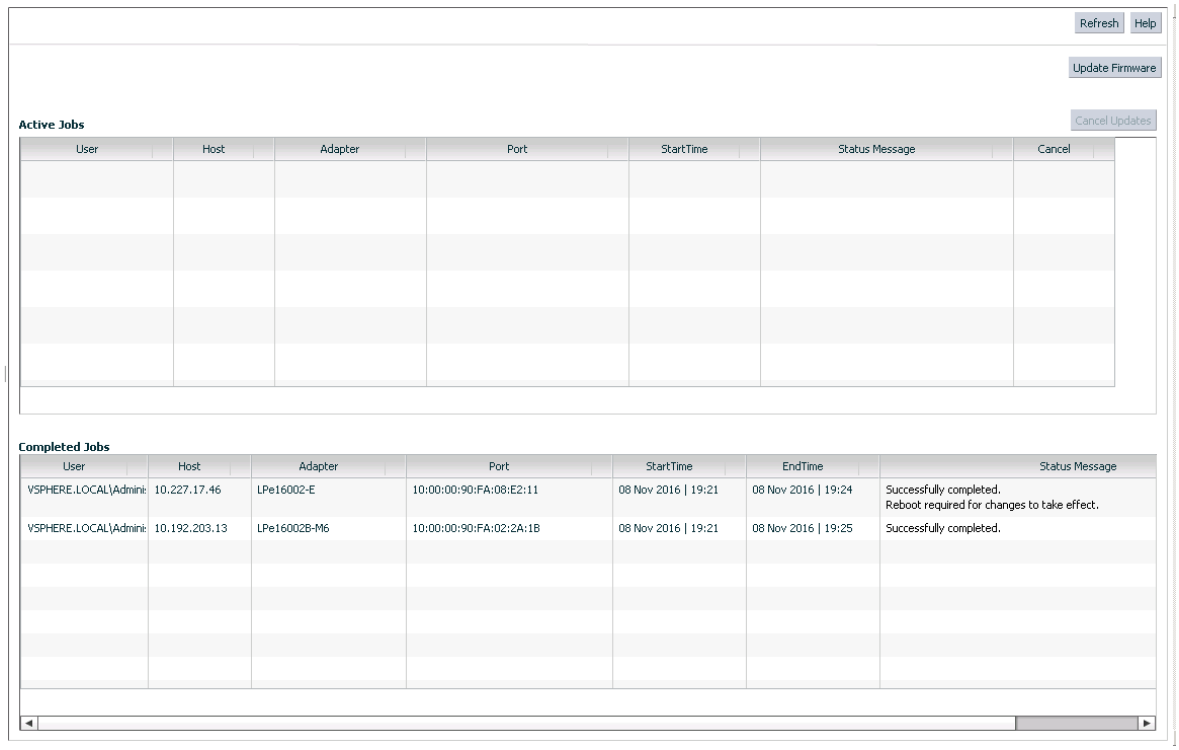
The tree-view displays all adapters and their corresponding hosts or fabrics for which the selected firmware file is compatible. Use the check boxes next to the entries to select or deselect a host, fabric, adapter, or port (if the adapters where the individual port can have new firmware downloaded).

6. Make your selections and click **Start Download**. A message prompting you to confirm the firmware update appears; click **Yes**.

7.2.3 Jobs Window

When the download begins, the **Jobs** window is displayed. A status message in the **Active Job** list displays the progress of the firmware download. The ports on which the firmware is being downloaded have the status **Job is in progress**, the other ports have **Waiting in queue to start**. When the download is completed, the entry moves to the **Completed Jobs** list. The **Status Message** column in the **Completed Jobs** list displays the status of the completed job (Figure 56).

Figure 56: Completed Jobs Window



The following **Jobs** window fields are displayed:

- **Active Jobs** list:
  - **User** – The user who updated the firmware.
  - **Host** – The IP address of the host to which the adapter or port belongs.
  - **Adapter** – The model of the adapter selected for the firmware update request.
  - **Port** – The port WWN for an FC adapter.
  - **Start Time** – The time the job is submitted.
  - **Status Message** – The status of the job. This field also indicates if a reboot is required to activate the firmware.
  - **Cancel** – An indication of a canceled job.
- **Completed Jobs** list:
  - **User** – The user who updated the firmware.
  - **Host** – The IP address of the host to which the adapter or port belongs.
  - **Adapter** – The model of the adapter.
  - **Port** – The port WWN for an FC adapter.
  - **Start Time** – The time the job is submitted.
  - **End Time** – The time the job is completed.
  - **Status Message** – The status of the job.

To cancel the jobs with the status *Waiting in queue to start*, click **Cancel Updates**.

Chapter 8: Exporting SAN Information in Cluster View

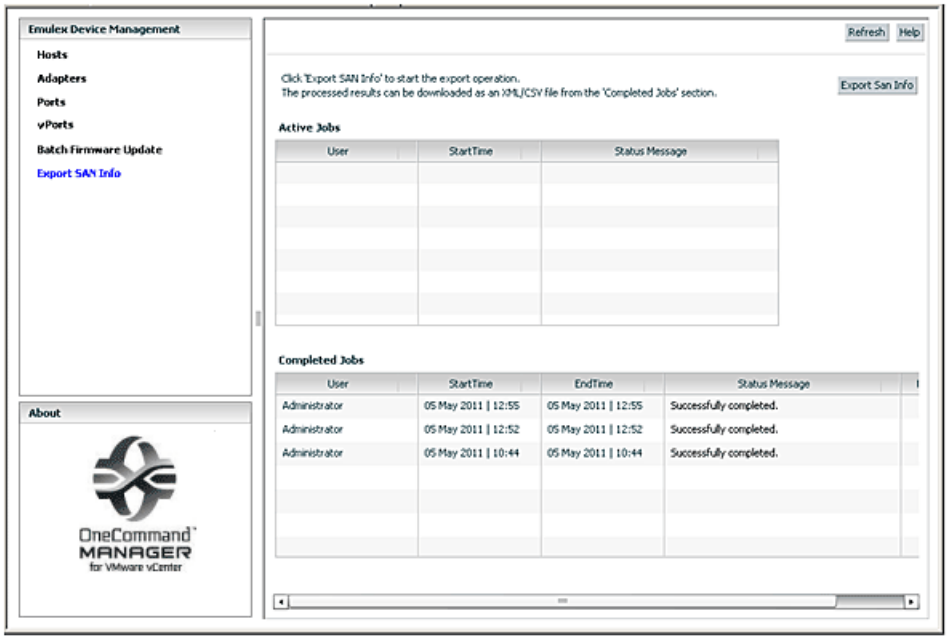
Exporting SAN information (creating a SAN report) processes in the background until all jobs are completed. During this period, you can still browse through the other tabs.

NOTE: Creating a SAN report can take several minutes for a large SAN.

To export SAN information, perform these steps:

1. Select a cluster in the console tree-view, and if applicable, select the **Emulex OneCommand** tab.
2. From the **Emulex Device Management** tree-view, select **Export SAN Info**. Export SAN information is displayed (Figure 57).

Figure 57: Export SAN Info Option in the Emulex Device Managment Tree-View



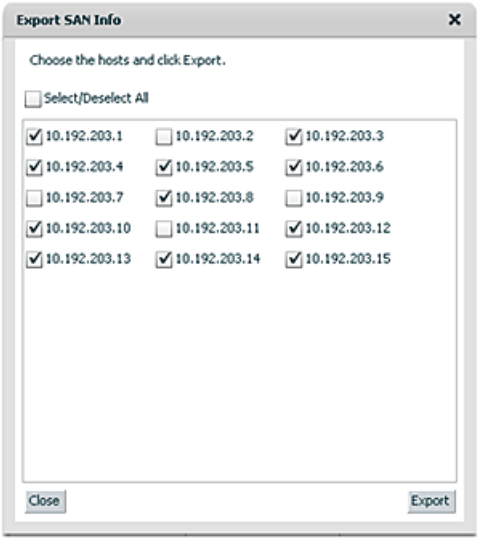
The following **Export SAN Info** window fields are displayed:

– **Active Jobs** area:
  - **User** – The user who updated the firmware.
  - **Start Time** – The time the job is submitted.
  - **Status Message** – The status of the job.

– **Completed Jobs** area:
  - **User** – The user who updated the firmware.
  - **Start Time** – The time the job is submitted.
  - **End Time** – The time the job is completed.
  - **Status Message** – The status of the job.
  - **Download** – Click **XML** or **CSV** to download the file with SAN information in the specified format.

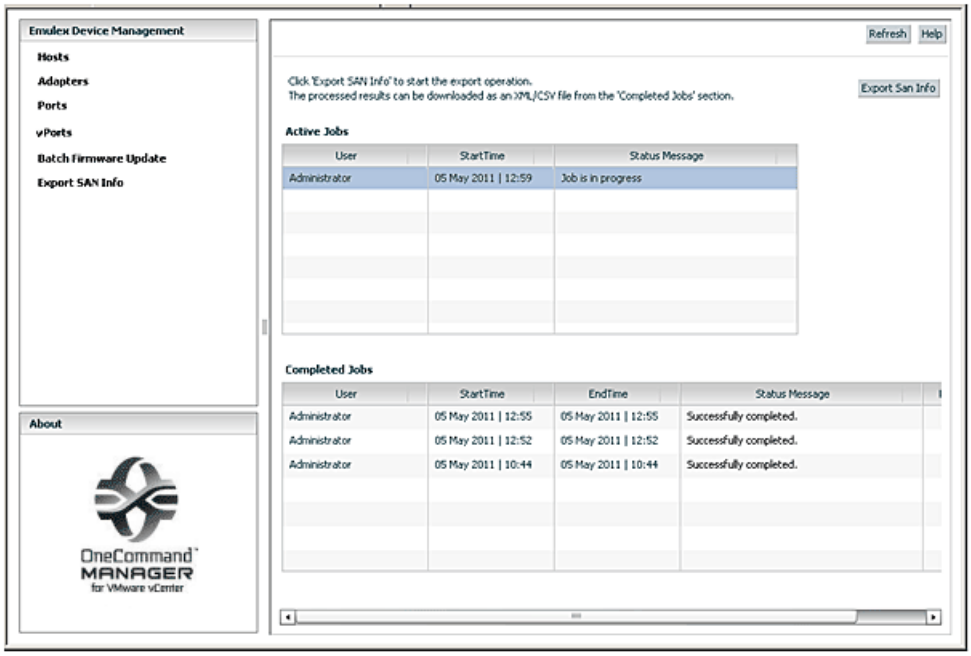
3. Click **Export SAN Info**. The **Export SAN Info** dialog is displayed (Figure 58).

Figure 58: Export SAN Info Dialog



4. Select host or hosts to export. Optionally, select **Select/Deselect All** to select all hosts. Clear **Select/Deselect All** to clear all host check boxes.
5. Click **Export**.The **Export SAN Info Jobs** window is displayed. The status is displayed in the **Active Jobs** list (Figure 59).

Figure 59: Export SAN Info Jobs Window–Active Jobs List



6. When the export job is completed, the entry is displayed in the **Completed Jobs** list with a **Successfully completed** status.

8.1 Capturing SAN Information in XML or CSV Format

1. Click the row that represents the information that you want to capture.
2. Scroll to the right until the **Download** column appears.
3. In the **Download** column, click either **XML** or **CSV** to capture the information.

8.2 Considerations When Exporting SAN Information in a Cluster View

- At any time, only 10 completed jobs are available to be exported. If more than 10 jobs are completed, the first completed jobs are not available for download.
- If you click **Export SAN Info** and log out from the console before the export is completed, all pending jobs fail.

Chapter 9: Emulex Diagnostics

This chapter describes diagnostics for Emulex adapters.

NOTE: When running port diagnostic tests using OneCommand Manager for VMware vCenter, do not perform any active management operations on the ESXi host.

CAUTION! Running a PCI Loopback, Internal Loopback, External Loopback, or POST test on an LPe12000-series adapter that is being used to boot from SAN is not advisable. After the tests have completed, the system performs an adapter reset, which can cause a loss of connectivity to the SAN and possible loss of data. To perform these tests, you must make sure that the adapter is not currently being used to boot from SAN.

Do one of the following:

- Move the target adapter to a non-boot-from-SAN host, and perform the tests from that location.
- If the host with the target adapter is also hosting other boot from SAN adapters, perform a boot from SAN using one of the other boot from SAN adapters. The target adapter can now be tested because it is no longer being used for boot from SAN.

9.1 Running Loopback Tests

You can run three loopback tests for the FC adapter port:

- PCI Loopback – A firmware-controlled diagnostic test in which a random data pattern is routed through the PCI bus without being sent to an adapter link port. The returned data is subsequently validated for integrity.
- Internal Loopback – A diagnostic test in which a random data pattern is sent down to an adapter link port, and then is immediately returned without actually going out on the port. The returned data is subsequently validated for integrity.
- External Loopback – A diagnostic test in which a random data pattern is sent down to an adapter link port. The data goes out of the port and immediately returns using a loopback connector. The returned data is subsequently validated for integrity.

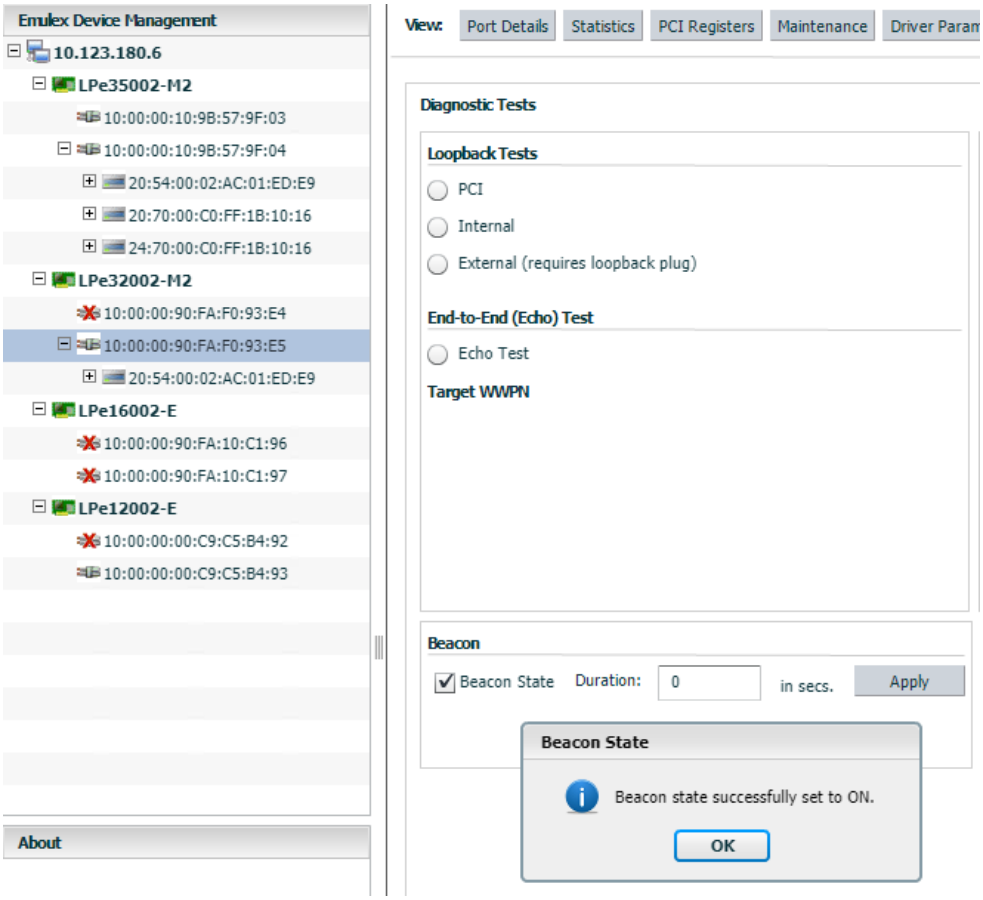
NOTE:

- Adapters and port information are not available during diagnostic loopback tests.
- Internal and External loopback tests on trunking enabled ports do not support Infinite test cycles.
- Internal and External loopback test results are displayed for each physical port.
- Each physical port must have a loopback connector when performing External loopback tests on trunking enabled ports.

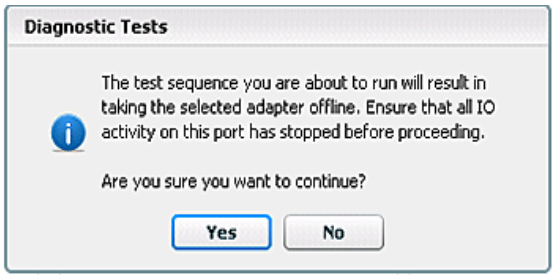
To run loopback tests, perform these steps:

1. From the **Emulex Device Management** tree-view, select the FC adapter physical port on which you want to run the loopback test.
2. Select the **Diagnostics** tab (Figure 60). In the **Loopback Tests** area of the dialog, choose the type of loopback test that you want to run, and define the loopback test parameters.

Figure 60: Diagnostics Tab (Beaconing Enabled)



3. Click **Start Test**. The following popup is displayed.



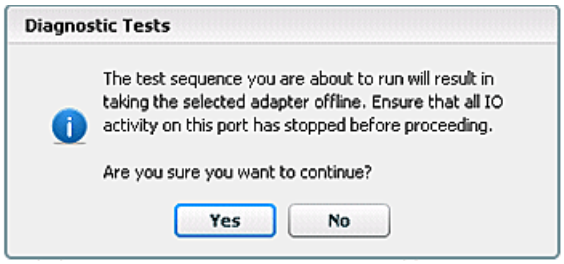
4. Click **Yes**. A progress bar displays that the test is running.
5. Periodic test feedback, consisting of the current loopback test/cycle and the completion status of each type of test, is displayed in the **Test Status** section of the dialog. Click **Show Test Logs** to view and save the log file.

9.2 Running End-to-End (ECHO) Tests

Run echo tests using the **End-to-End (ECHO) Test** section of the **Diagnostics** tab. The end-to-end test enables you to send an ECHO command/response sequence between an adapter port and a target port.

To run end-to-end echo tests, perform these steps:

1. From the **Emulex Device Management** tree-view, select the physical port on which you want to initiate the End-to-End (ECHO) test.
2. Select the **Diagnostics** tab (Figure 60). In the **End-to-End (Echo) Test** area, select **Echo Test**.
3. Enter the WWPN for the target. The following popup appears:



4. Click **Yes**. A result window appears, and the test results appear in the **Test Log**.
5. Either click **Clear** to erase the contents of the log display or click **Save to File** to save the log file.

NOTE: The **ECHO Test** button is enabled only if its port has targets connected.

9.3 Running D_Port Tests

D_Port is a diagnostic mode supported by Brocade switches for adapters with D_Port support. Bidirectional D_Port testing is supported. The switch or initiator can initiate D_Port testing.

NOTE:

- D_Port is also referred to as ClearLink.
- You must disable Dynamic D_Port on the switch to run D_Port tests from the adapter. See Section 5.9, Enabling and Disabling Dynamic D_Port, for information about disabling Dynamic D_Port.
- D_Port testing is not available when FC port aggregation is enabled.
- D_Port is not supported on LPe12000-series or LPe15000-series adapters.

D_Port tests detect physical cabling issues that can result in increased error rates and intermittent behavior. When activated, D_Port tests include:

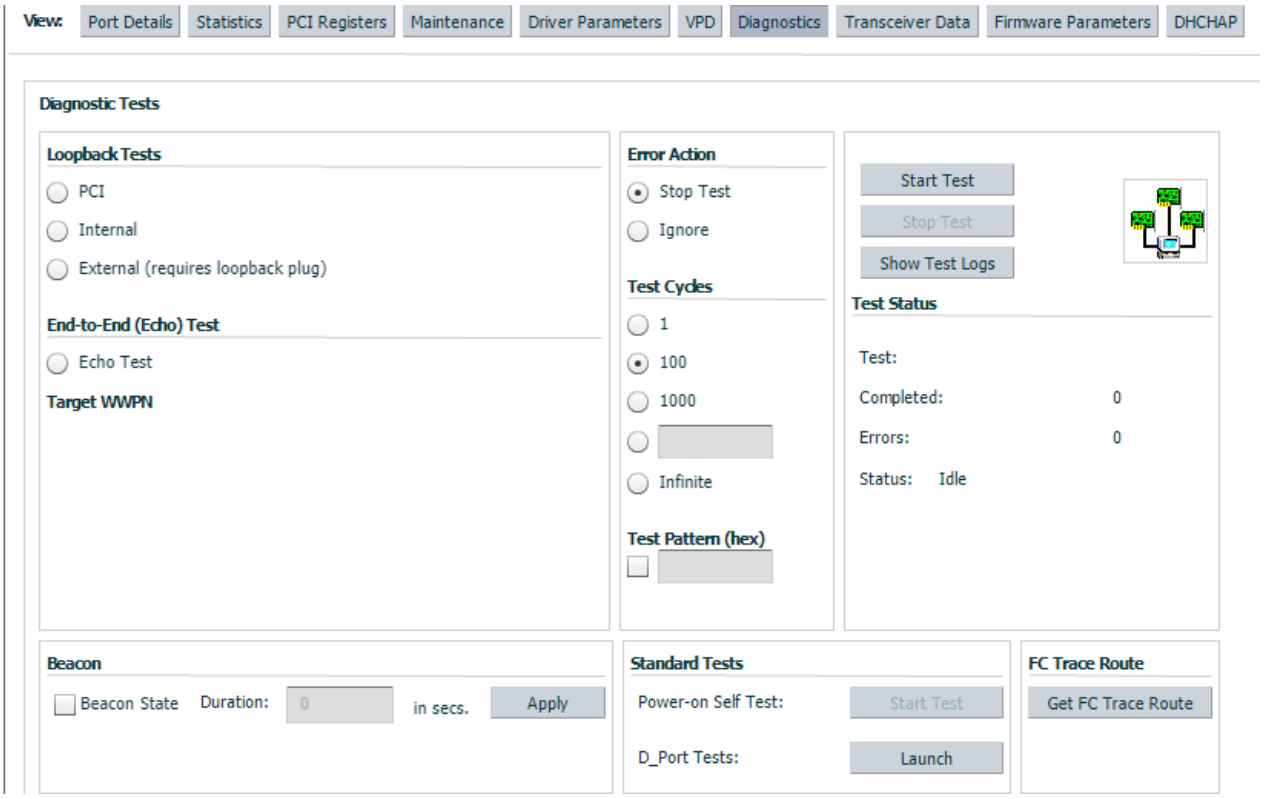
- Local electrical loopback
- Loopback to the remote optics
- Loopback from the remote port to the local optics
- A full device loopback test with data integrity checks
- An estimate of cable length (to validate that a proper buffering scheme is in place)

These tests allow a level of fault isolation to distinguish faults due to marginal cables, optics modules, and connector or optics seating.

To run D_Port tests, perform these steps:

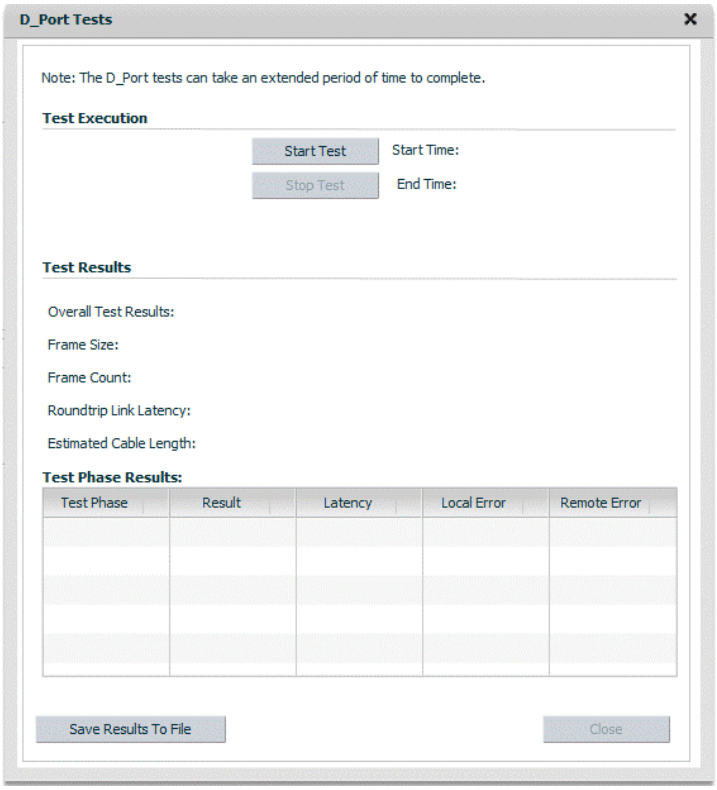
1. From the **Emulex Device Management** tree-view, select the FC adapter physical port for which you want to run the D_Port tests.
2. Select the **Diagnostics** tab, and in the **Standard Tests** area, click **Launch (**Figure 61).

Figure 61: FC Adapter Diagnostics Tab with D_Port Tests Option



3. The **D_Port Tests** dialog is displayed (Figure 62). Click **Start Test**.

Figure 62: D_Port Tests Dialog



The D_Port tests are launched. If all tests pass, a dialog similar to Figure 63 is displayed. If all tests do not pass, the failed result is shown in the **Test Phase Results** area (Figure 64).

Click **Save Results To File** to save the test results to a text file. You can view this text file in any text editor.

To stop tests, click **Stop Test**. If a test phase fails, the D_Port diagnostics are automatically stopped. In this case, some of the phases might not be reported in the results. However, the failed phase will be reported.

If the **Overall Test Results** is **FAILED**, you must either rerun the tests successfully, or reset the HBA port to bring the link back up.

NOTE:

- The D_Port tests can take an extended period of time to complete.
- If an older SFP version is detected by the OneCommand Manager for VMware vCenter, a message is displayed under the results box indicating that the SFP version does not fully support all D_Port tests.

Figure 63: D_Port Tests Dialog–Passed Result

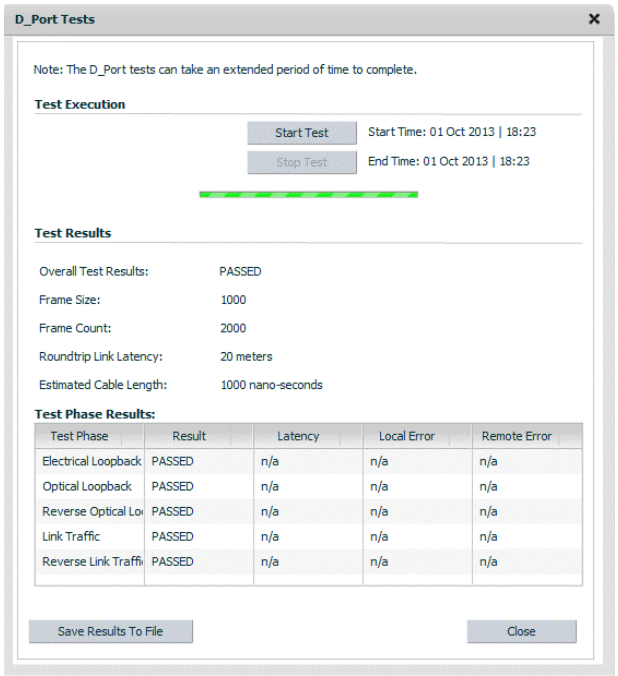
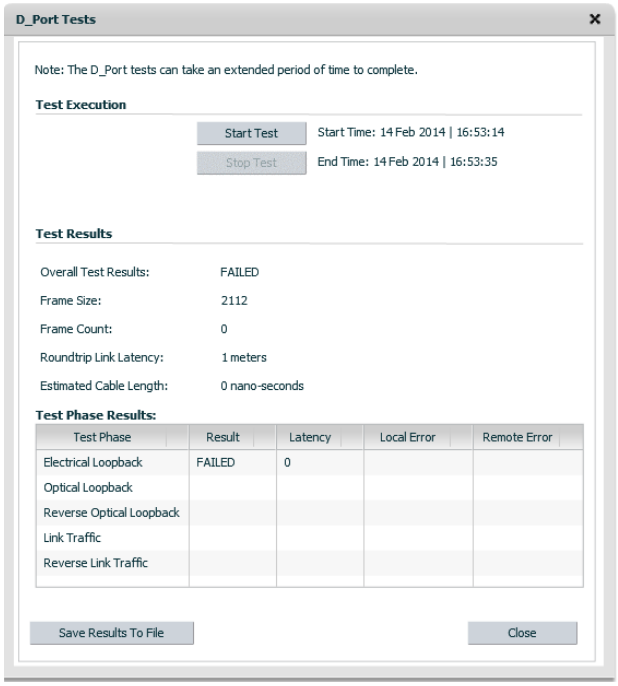


Figure 64: D_Port Tests Dialog–Failed Results



9.4 Using FC Trace Route

FC Trace Route allows you to trace the communication route for FC packets transmitted between an FC initiator port and an FC target port.

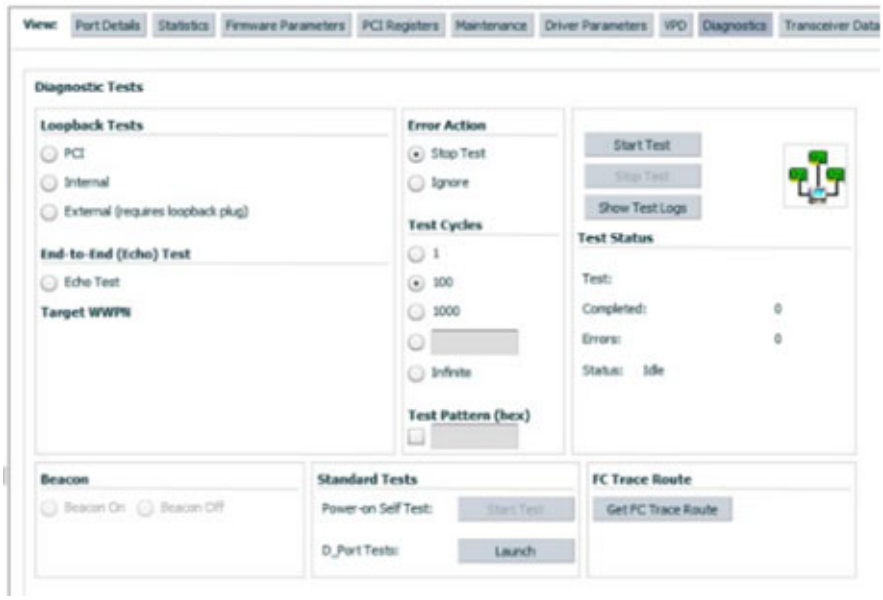
Communication route information, such as the switch name, domain ID, ingress and egress port name, and ingress and egress physical port number, is accumulated for all switch ports through which packets are routed. Data is collected for both the outward bound route from the initiator to the target, and the inbound route from the target to the initiator is collected.

The **FC Trace Route** button on the **Diagnostics** tab enables you to collect an adapter's FC Trace Route information. (Figure 65).

NOTE:

- FC Trace Route is not supported on LPe12000-series adapters.
- Both local and remote support for FC Trace Route must be provided.
- FC Trace Route support must be provided on Windows and ESXi operating system platforms.

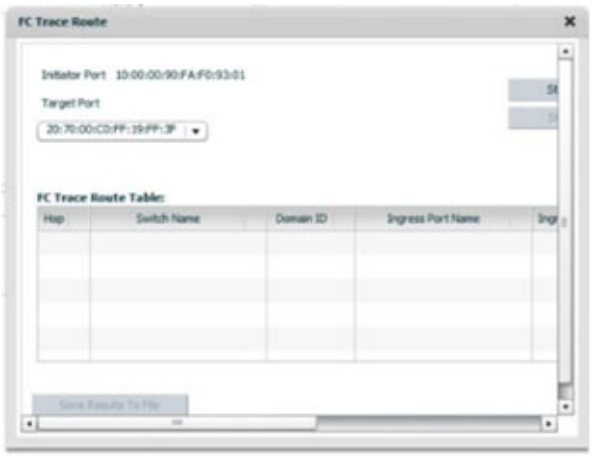
Figure 65: Diagnostics Tab (Get FC Trace Route Button Depicted)



To enable FC Trace Route, perform these steps:

1. From the discovery-tree, select the FC port on which you want to enable FC Trace Route.
2. Select the **Diagnostics** tab (Figure 65) and click **Get FC Trace Route**. The **FC Trace Route** dialog appears (Figure 66).

Figure 66: FC Trace Route Dialog



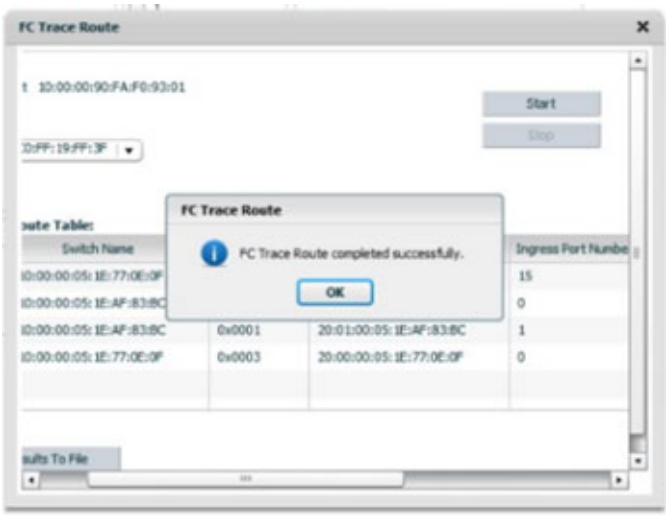
3. The **Target Port** list displays the WWPNs of all targets that are seen by the initiator port. Select a target port and click **Start**.

   The **FC Trace Route** dialog displays trace route information for the selected initiator and target ports (Figure 67).

NOTE: Error messages are displayed if there was a problem processing the FC trace route request.

Click **Save Results to File** to save the results of the most recent FC trace route operation to a log text file. The default file name for the log text file is `FCTrace-<ESXiHostIP>`. You can change the file name.

Figure 67: FC Trace Route Dialog with Route Information Displayed



The following information is collected for each trace route:

- **Switch Name** – The switch chassis WWN.
- **Domain ID** – A number used to uniquely identify a switch in a fabric. This number is assigned by a fabric administrator as part of fabric configuration. The domain IDs is an 8-bit field whose value ranges from 0 to 255.
- **Ingress Port Name** – The port WWN of the physical port through which an FC packet enters a specific switch.
- **Ingress Port Number** – The physical port number of the port through which an FC packet enters a specific switch.

- **Egress Port Name** – The port WWN of the physical port through which an FC packet exits a specific switch.
- **Egress Physical Port Number** – The physical port number of the port through which an FC packet exits a specific switch.

9.5 Running a POST

The power-on self-test (POST) is a firmware test that is normally performed on an adapter after a reset or restart. The POST does not require any configuration to run.

NOTE: The POST test is available only for LPe12000-series adapters.

To run the POST, perform these steps:

1. From the **Emulex Device Management** tree-view, select the FC adapter physical port on which you want to run the POST.
2. Select the **Diagnostics** tab (Figure 60) and, in the **Standard Tests** area, click **Start Test**. A progress window appears, showing the progress of the POST test.
3. After the test is completed, the **Test Completion Status** window appears. Click **OK**. A POST window is displayed with the POST information.

9.6 Using Beaconing

Beaconing enables you to force a specific adapter's LEDs to blink in a particular sequence. The blinking pattern acts as a beacon, making it easier to locate a specific adapter among racks of other adapters. On supported adapters, you can also specify a specific beaconing duration, in seconds.

NOTE: Beaconing is disabled if the selected adapter does not support beaconing.

To enable beaconing, perform these steps:

1. From the **Emulex Device Management** tree-view, select the adapter port whose LEDs you want to set.
2. Select the **Diagnostics** tab (Figure 60) and select **Beacon State**.

   On supported adapters, you can also enter an optional **Duration** time, in seconds, for the LEDs to blink. Enter the duration time.
3. Click **Apply**.

To disable beaconing, perform these steps:

1. From the **Emulex Device Management** tree-view, select the adapter port whose LEDs you want to disable.
2. Select the **Diagnostics** tab (Figure 60) and clear **Beacon State**.
3. Click **Apply**.

9.7 Setting Up Diagnostic Test Options

Setting up test options includes error actions, test cycle counts, and test patterns.

9.7.1 Setting Up a Test Failure Error Action

Two error action options are available in the event of a test failure:

- **Stop Test** – Does not log the error and aborts the test. No further tests are run.
- **Ignore** – Logs the error and proceeds with the next test cycle.

9.7.2 Setting Up Test Cycles

Specify one of the following test cycles:

- Select an established cycle count by clicking the corresponding radio button.
- Enter a custom cycle count in the blank field in the **Test Cycles** area.
- Select **Infinite** to set the test to run until you manually click **Stop Test**.

9.7.3 Setting Up a Test Pattern

Enter a custom test pattern to be used in tests that transfer data. The test pattern can be up to 8 hexadecimal bytes.

9.7.4 Test Status

The **Test Status** area displays how many completed cycles of each test ran, as well as the number of errors.

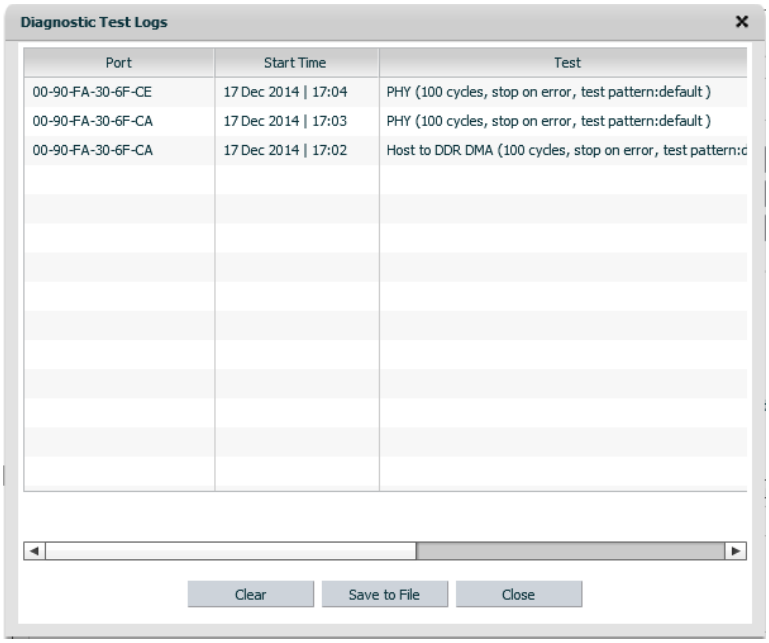
9.8 Saving the Log File

You can save the test log to a log file for later viewing or printing. When data is written to a saved file, the data is appended at the end of the file. Each entry has a two-line header with the adapter identifier and the date and time of the test. The data accumulates to form a chronological history of the diagnostics performed on the adapter.

- The default location is the OneCommand Manager for VMware vCenter install directory on your local drive.
- In the VMware Server, there is no default directory for ESXi.

After writing an entry into the log, you are prompted to clear the display. Figure 68 displays the **Diagnostic Test** log entries that will be saved to the log file.

Figure 68: Diagnostic Test Log Entries



To save the log file, perform these steps:

1. After running a test from the **Diagnostic** tab, click **Show Test Logs**. The **Diagnostic Test Logs** dialog appears. The default name of a saved file is `DiagTest.log`.
2. Click **Save to File** to save the file or click **Clear** to delete the log entries.

9.9 Creating Diagnostic Dumps

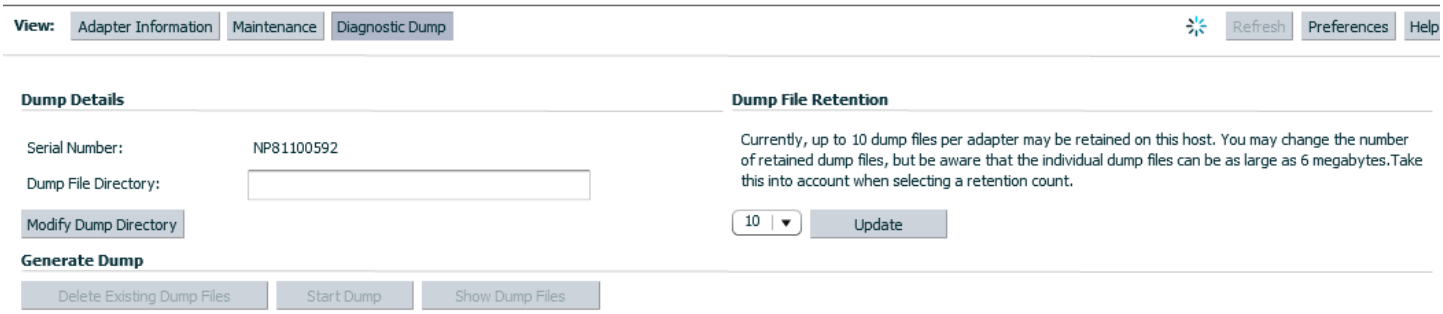
Diagnostic dump enables you to create and manage a diagnostic dump for a selected adapter. Dump files contain information, such as firmware version and driver version, that is particularly useful when troubleshooting an adapter.

You can retrieve user initiated and driver initiated driver dump files, delete the dump files, or repeat the process on all resident dump files. You can also retrieve or delete dump files from remote hosts.

To start a diagnostic dump, perform these steps:

1. Select a host in the console tree-view, and if applicable, select the **Emulex OneCommand** tab.
2. In the **Emulex Device Management** tree-view, select the adapter. (Select the port for LPe12000-series adapters.)
3. Select the **Diagnostic Dump** tab (Figure 69). Diagnostic dump information is displayed.

Figure 69: Diagnostic Dump Tab (No Dump File Directory Specified)



4. Enter a location in the **Dump File Directory** field in the **Dump Details** area to set the dump file directory. The **Delete Existing Dump Files**, **Start Dump**, and **Show Dump Files** buttons are enabled.

NOTE: If the location is not specified, a prefix of `/vmfs/volumes` is added to the location.

5. To specify up to 20 files to retain using the **Dump File Retention** counter, enter the number of files and click **Update**.
6. Click **Start Dump** to initiate a diagnostic dump on the selected port.

Click **Delete Existing Dump Files** to remove existing dump files for the selected port. Click **Show Dump Files** to display the retained dump files. Click **Modify Dump Directory** to change the dump directory location.

CAUTION! Disruption of service can occur if a diagnostic dump is run during I/O activity.

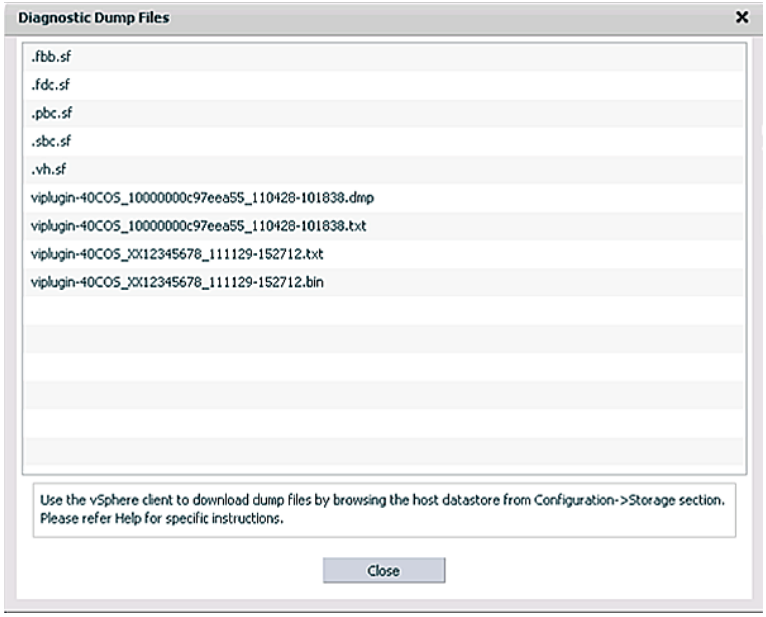
9.10 Viewing Diagnostic Dump Files

You can view diagnostic dump file names using OneCommand Manager for VMware vCenter. The dump files are stored on the host's data store, and the client can be used to download dump files by browsing the host data store.

To view the diagnostic dump, perform these steps:

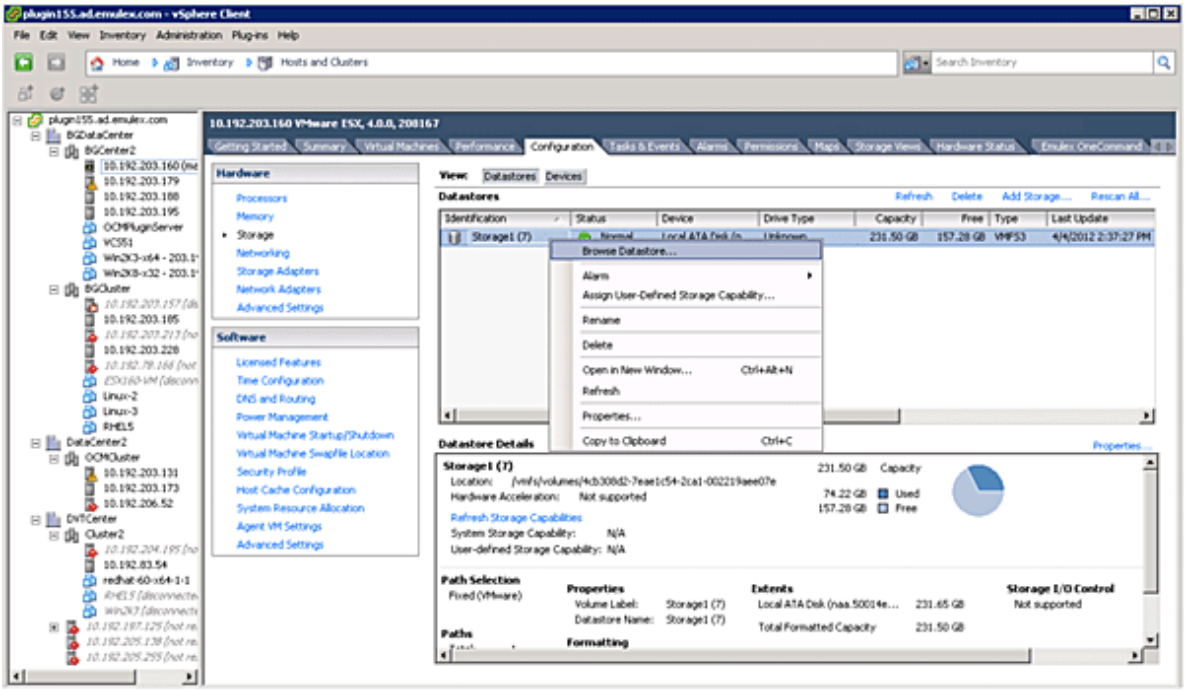
1. On the **Diagnostic Dump** tab, click **Show Dump Files**. The **Diagnostic Dump Files** window opens displaying the diagnostic dump files currently on your system (Figure 70). These files are available in the dump directory configured from the **Diagnostic Dump** tab. You can extract these files using the client.

Figure 70: Diagnostic Dump Files Window



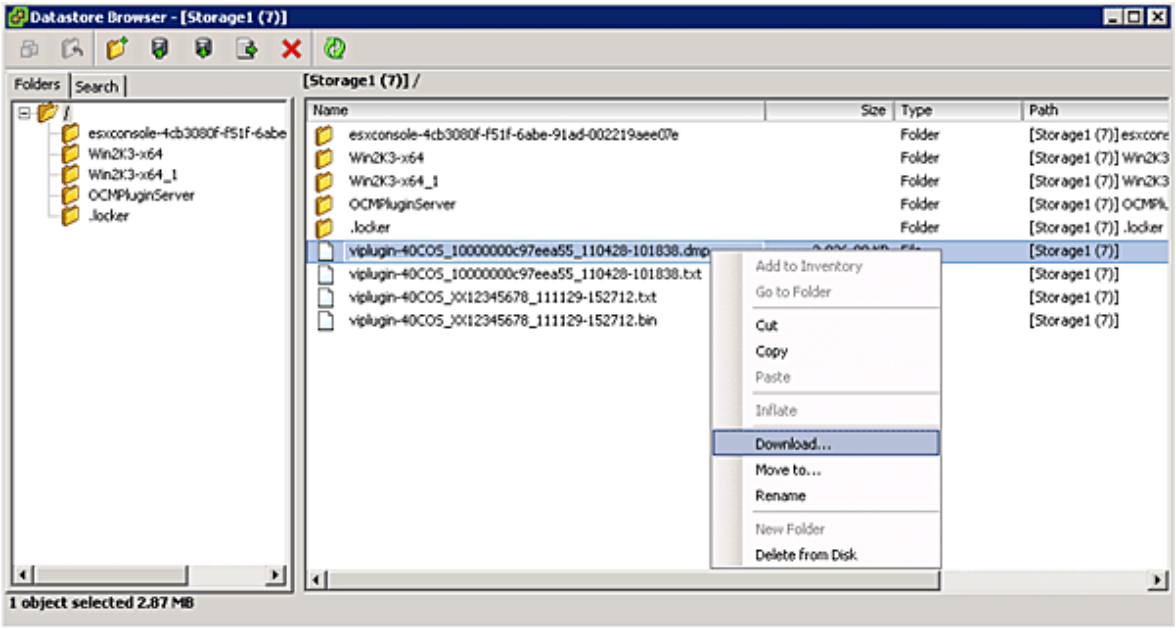
2. Extract the dump files by using the client to download the dump files by browsing the data store.
3. Click the **Configuration** tab in the client. The **Datastores** view is displayed (Figure 71).

Figure 71: Datastores View of Client



4. Right-click the datastore where the dump file is located, and select **Browse Datastore** from the context menu. The **Datastore Browser** window opens (Figure 72).

Figure 72: Datastore Browser



5. In the Datastore Browser window, right-click the dump file that you want to review and select **Download** from the context menu. A **Browse for Folder** window opens.
6. Select the desired location for the dump files in the **Browse for Folder** window and press **OK**. The file is downloaded to the location you select. You can view the dump file in any text editor.

Chapter 10: Generating and Installing Secured Certificates

OCMNG is a web application, based on a client-server model, that runs on the Apache Tomcat Web Server. Data is exchanged between the client (browser) and the server (on a remote machine), which requires a secure user logon to manage Emulex adapters on different and multiple hosts.

10.1 SSL Certificate

A Secure Sockets Layer (SSL) certificate establishes an encrypted connection between the web server and the web browser on a remote machine. This connection allows private information to be transmitted without eavesdropping, data tampering, or message forgery.

An SSL certificate provides security through encryption and authentication. Encryption is ensured by accessing the remote server using the HTTPS protocol and an SSL certificate.

NOTE: If OneCommand Manager for VMware vCenter is running, the server must be configured to support HTTPS protocol access and provide a self-signed certificate.

The OneCommand Manager for VMware vCenter server is authenticated to the browser by a public key in the self-signed certificate.

10.1.1 Generating an SSL Certificate

To allow secured communication between the client and the server, perform these steps:

1. Generate a self-signed certificate with a keystore file for each server providing the server's domain name and company details. See Section 10.1.2, Generating a Self-Signed Certificate, for instructions. For more information, refer to the X.509 attributes list on the International Telecommunications Union website.
2. Use this certificate to create a request to the customer's trusted certificate authority (CA). The request certificate is referred as a Certificate Signing Request (CSR). The CA issues a new SSL certificate. See Section 10.2.1, Generating a CSR for a Server Using the Java Tool, for instructions.
3. Import the new SSL certificate to the application server, and install the SSL certificate on the client's browser. See Section 10.2.4.1, Installing the Certificates to the Keystore of OneCommand Manager for VMware vCenter, for instructions.
4. Configure the server to use the keystore file. See Section 10.2.4.2, Configuring a Web Server, for instructions.
5. Access the server's content through the browser using the HTTPS protocol.

   The browsers understand the certificate, and the browsers allow access to and from the remote server.

10.1.2 Generating a Self-Signed Certificate

A self-signed certificate is a certificate that is signed by itself (the server hosting OneCommand Manager for VMware vCenter) rather than a trusted CA. This self-signed certificate includes a public or private key that is distributed by the SSL to verify the identity of the server.

A self-signed certificate can also be used as an alternative to SSL certificates if the server is not running in a public domain.

If a self-signed certificate is used in place of an SSL, a popup is displayed in the browser before accessing the server content.

For Java-based applications, a self-signed certificate can be generated using the tools provided by Java. This creates a keystore file that must be installed on the web server. This keystore includes a private key specific to the server used for generating a CSR and authenticating the server.

As the OneCommand Manager for VMware vCenter server is developed using Java, it leverages the keystore tool provided by Java to generate the self-signed certificates at no cost.

NOTE: The self-signed certificate for the OneCommand Manager for VMware vCenter server is generated and installed on its server as part of the OneCommand Manager for VMware server installation on a Windows machine. This self-signed certificate is generated with Broadcom® organization details using RSA algorithm and private key of size 2048 bits.

To generate a self-signed certificate, perform these steps:

1. In the OCM for VMware installation directory, go to `ApacheTomcat\conf`.
   ```
   >>cd /d  "C:\Program Files\Emulex\OCM for VMware\ApacheTomcat\conf"
   ```
2. Run the following command:
   ```
   >> ..\..\JRE\bin\keytool.exe -genkey -alias <new-alias> -keyalg RSA -keystore emulex.vcplugin.jks
   -keysize 2048
   ```

NOTE: You can change alias, keysize, and keystore name.

Example

```
Enter keystore password: (Enter "emulex" if using the same keystore name)
Re-enter new password:
What is your first and last name?
  [Unknown]:  pluginserver.ad.emulex.com  (Give the complete domain name of the server [FQDN])
What is the name of your organizational unit?
  [Unknown]:  ocm
What is the name of your organization?
  [Unknown]:  elx
What is the name of your City or Locality?
  [Unknown]:  bg
What is the name of your State or Province?
  [Unknown]:  ka
What is the two-letter country code for this unit?
  [Unknown]:  in
Is CN=pluginserver.ad.emulex.com, OU=ocm, O=elx, L=bg, ST=ka, C=in correct?
  [no]:  yes

Enter key password for <elxocm>:
        (RETURN if same as keystore password)
```

10.2 Generating a CSR

A Certificate Signing Request (CSR) is a block of encrypted text that is generated on the server on which the certificate is used. A CSR contains information to be included in the SSL certificate, such as the organization name, common name (domain name), locality, country, and other X.509 attributes. It also contains the public key that is included in the certificate. The CA uses the CSR to create a new SSL certificate.

10.2.1 Generating a CSR for a Server Using the Java Tool

To generate a CSR for a server, use the Java tool available in the `jre/bin` folder. The syntax using the Java tool follows:

```
keytool -certreq -keyalg <algorithm>  -alias <alias-name>  -file <csr-name> -keystore <keystore-name>
```

Example

```
keytool -certreq -keyalg RSA -alias selfsigned -file elxocmreq.csr -keystore emulex.vcplugin.jks
```

10.2.2 Generating and Validating a CSR

To generate a CSR, perform these steps:

1. Generate a self-signed certificate (see Section 10.1.2, Generating a Self-Signed Certificate, for instructions).
2. Generate a CSR using the following syntax:

```
>>..\..\JRE\bin\keytool -certreq -v -alias <new-alias> -file elxocmreq.csr -keypass elxocm -keystore emulex.vcplugin.jks
Enter the keystore password: (Enter "emulex" if using the default keystore name)
Certification request stored in file <elxocmreq.csr>
```

To validate a CSR for its completeness, perform these steps:

You can validate the generated CSR for its completeness before submitting (with the help of the CA). Copy the CSR content from the following link for validation.

```
http://www.sslshopper.com/csr-decoder.html
```

NOTE: The CSR must begin and end with the following tags:

```
-----BEGIN NEW CERTIFICATE REQUEST-----
-----END NEW CERTIFICATE REQUEST-----
```

Example


```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIC2TCCAcECAQAwZDELMAkGA1UEBhMCaW4xCzAJBgNVBAgTAmthMQswCQYDVQQHEwJiZzEMMAoG
A1UEChMDZWx4MQwwCgYDVQQLEwNvY20xHzAdBgNVBAMTFmJnc3N5ZWQxLmFkLmVtdWxleC5jb20w
ggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCDhovljXhfjNPM/5eBsX4280AIl3YARn0p
R6Z7eOqs1r5Qh07kT58M6T8fER+NpIN7WhOOF/TbsFsS0gmfYwJQqttvtq1dtxUGpvFe9lywbP+l
kY+w6GOyPTG2qnXgILtX5ArZbC2UBbz+J8WJ3SjPHXiSY35EZWnyZZmIN8v1vOe9e21f8vwRkn/4
fdfFrpoQa3H+GcAJMRSBRTd5H6mXQv6HaA5Z0BbsABisFx4scqSuM/HJKLP6GcSHR61bzHfiO/NH
4qU/s6I2LC5DvGs1hIW3PPbmb1rxBiEFpjPtWhfzPxPMKSU8uey+lE0UIPMS0FMTxo63oYnMeiSX
X5mxAgMBAAGgMDAuBgkqhkiG9w0BCQ4xITAfMB0GA1UdDgQWBBSvpKLBF3lY03Jin9kI4ym94bJi
zjANBgkqhkiG9w0BAQsFAAOCAQEAfs94wzEUlDAMq0jITi6fiD7YxK2KFWJgMBfjxZIGex2zxlHL
mOS14BGSWk5dvSMwqDBC14l4C79rUOlTUwwWs9zFqMHynndQ2Ze2vuJNTWUlnFyFb37/rEvbFufB
QVvFXgycaKRgUpWo2x5sekRJRAPxXI/vLWOFRLLrzcVykgZ/sg3QrO4ezlKFc49put0vKpvI1dY9
l9BN2REuWrlmq5y3L8nx8mKX9dRmP6CKzHBaVrvY+nVju+Vf/ikfTtQIDEXAIW2Q7AObpcOaudnf
Nsaey+u27vGy77gAv7092xBHsDyOrD7COy/83b194igmVBVY4dt0496oXkOHCA0txA==
-----END NEW CERTIFICATE REQUEST----
```


10.2.3 Getting an SSL Certificate

The CSR can be submitted to the trusted CA (as chosen by you). The CA validates the CSR and issues a new SSL certificate.

10.2.4 Installing the SSL into the Web Server

When you receive the SSL certificate from the CA, you must install the SSL certificate on the server to accept the secure connections.

NOTE: The CSR must be generated on the same machine that the server is running on. The SSL certificate must also be installed on this same server.

10.2.4.1 Installing the Certificates to the Keystore of OneCommand Manager for VMware vCenter

The Root Certificate file, the Intermediate Certificate file, and the Primary Certificate file must all be installed in the keystore.

To install the certificates to the keystore of OneCommand Manager for VMware vCenter, perform these steps:

1. Download the SSL certificate file from the CA. Save the SSL certificate file to the same directory as the keystore (self-signed certificate) that was created for the CSR.

NOTE: The certificate works only with the same keystore that was initially created for the CSR. The certificates must be installed to your keystore in the correct order.

2. Install the Root Certificate file.

   Every time you install a certificate to the keystore, you must enter the keystore password that you chose when you generated it. Enter the following command to install the Root Certificate file:

   ```
   keytool -import -trustcacerts -alias root -file RootCertFileName.crt -keystore keystore.key
   ```

   If the following message is displayed, select `Yes`:

   ```
   Certificate already exists in system-wide CA keystore under alias <...> Do you still want to add
   it to your own keystore?
   ```

   If successful, the following message is displayed:

   ```
   Certificate was added to keystore.
   ```

3. Install the Intermediate Certificate file.

   If the CA provided an Intermediate Certificate file, you must install it here using the following command:

   ```
   keytool -import -trustcacerts -alias intermediate -file IntermediateCertFileName.crt -keystore
   keystore.key
   ```

   If successful, the following message is displayed:

   ```
   Certificate was added to keystore.
   ```

4. Install the Primary Certificate file.

   Use following command to install the Primary Certificate file (for your domain name):

   ```
   keytool -import -trustcacerts -alias tomcat -file PrimaryCertFileName.crt -keystore keystore.key
   ```

   If successful, the following message is displayed:

   ```
   Certificate reply was installed in keystore.
   ```

All the certificates are now installed to the keystore file. You must configure your server to use the keystore file.

10.2.4.2 Configuring a Web Server

NOTE: These configuration changes are not required if the default keystore name and password are used. If they are different, you must change the configuration as needed.

1. Copy the keystore file or SSC to a directory (preferably, the `conf` folder) of the web server.

2. Open the file `${CATALINA_HOME}/conf/server.xml` in a text editor.
3. Uncomment the SSL Connector Configuration.
4. Make sure that the keystorePass matches the password for the keystore and that the keystoreFile contains the path and file name of the keystore.

   Your connector should be displayed similar to the following:

```
<Connector className="org.apache.catalina.connector.http.HttpConnector" port="8443"
minProcessors="5" maxProcessors="75" enableLookups="true" acceptCount="10" debug="0"
scheme="https" secure="true">

<Factory className="org.apache.catalina.net.SSLServerSocketFactory" clientAuth="false"
protocol="TLS" keystoreFile="./conf/emulex.vcplugin.jks" keystorePass="emulex"/>
```

5. Save the changes to `server.xml`.
6. Restart the web server.

   If you launch the OneCommand Manager for VMware vCenter URL in the browser, the application should be launched without any security warnings.

NOTE: Use the host name with the domain name that you used to generate the CSR.

Chapter 11: Troubleshooting

This chapter includes information about certificate or insecure-content warnings that might be displayed on the console. This chapter also describes unexpected circumstances and some proposed solutions.

11.1 Security

OneCommand Manager for VMware vCenter can be installed on different machines. As a result, certificate or insecure-content warnings can occur. The two ways to remedy the issue are:

- Accept the blocked content – temporary solution
- Install a security certificate – permanent solution

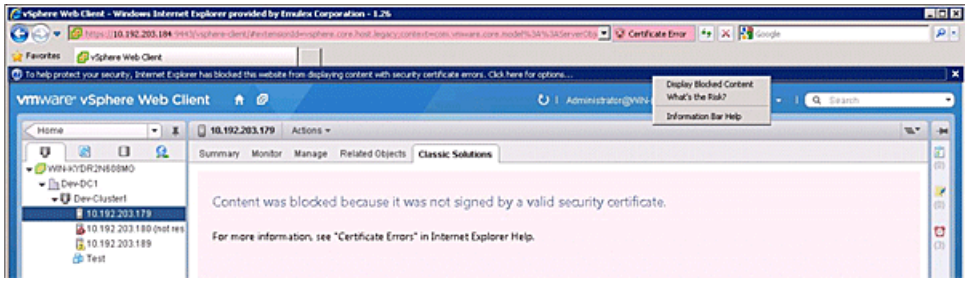
11.1.1 Accepting the Blocked Content

The procedure for accepting blocked content depends on the type of browser that you are using. This solution is not permanent, and you must repeat this procedure every time you use OneCommand Manager for VMware vCenter. If you want a permanent solution, you must install the correct security certificate. See Section 11.1.2, Installing a Security Certificate.

11.1.1.1 Internet Explorer 9 or Earlier Versions

Accept the blocked content (Figure 73).

Figure 73: Blocked Content in Internet Explorer



11.1.1.2 Internet Explorer 10 or Later, Chrome, and Firefox

1. Load the plug-in URL in a separate tab or window.

   The plug-in URL format is:

   `https://<plugin-server>:<https-port>/elxvcplugin`

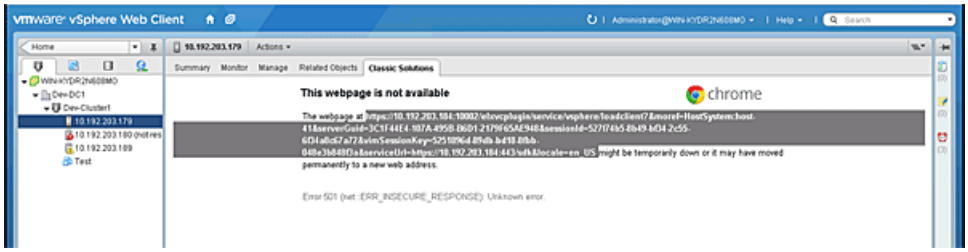
   For example:

   `https://pluginserverhostFQDN:443/elxvcplugin`

NOTE: You can extract the plug-in server, IP address, host name, and port number from the browser warning message.

2. Confirm the certificate warning (Figure 74).
3. Refresh the **vSphere Web Client** tab or window.

Figure 74: Blocked Content in the Firefox or Chrome Browser



11.1.2 Installing a Security Certificate

A permanent solution to the security warnings is to install the correct security certificate.

To install a security certificate, perform these steps:

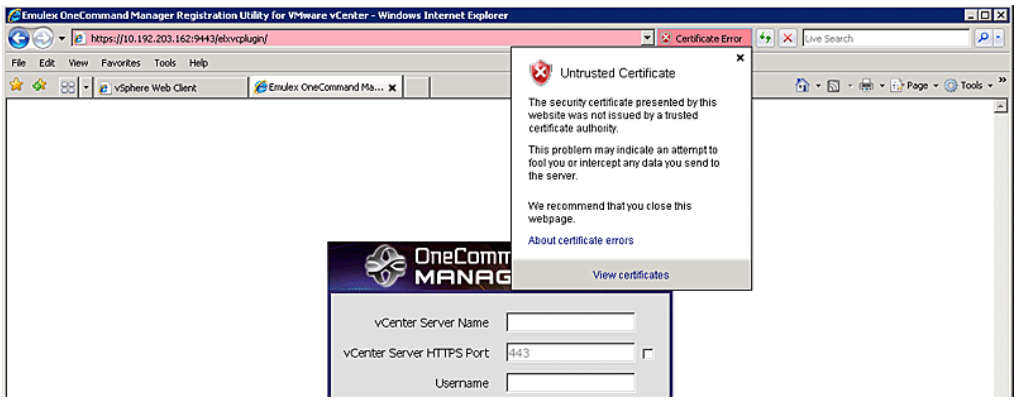
1. Open Internet Explorer in Administrative mode.
2. Load the plug-in URL, and accept the certificate warning.

   The plug-in URL must have the following format:

   `https://<plugin-server>:<https-port>/elxvcplugin`

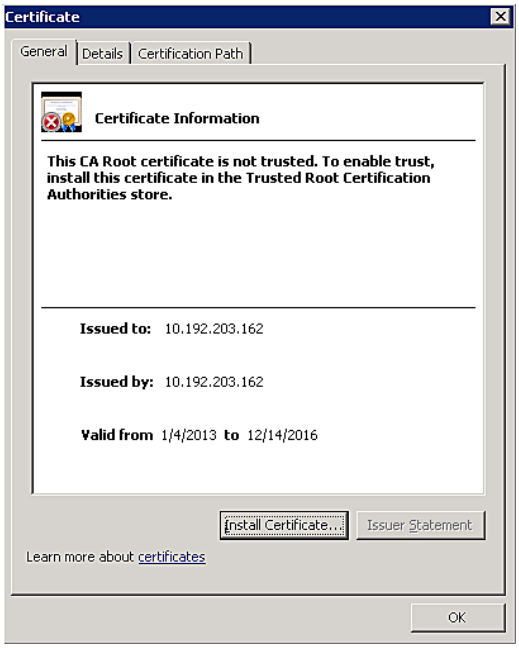
   The page loads with a certificate error.
3. Click the **Certificate Error**. A list appears displaying the untrusted certificate (Figure 75).

Figure 75: Untrusted Certificate



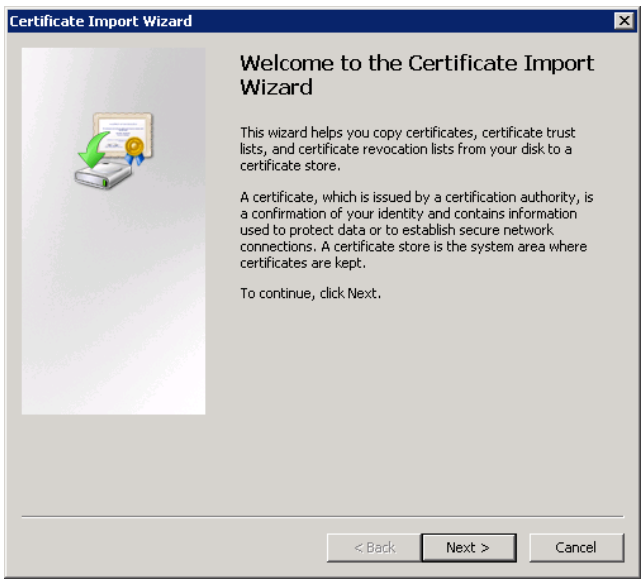
4. Click **View certificates** in the Certificate Error list. The **Certificate** dialog is displayed (Figure 76).

Figure 76: Certificate Dialog



5. Click **Install Certificate**. The **Certificate Import Wizard** is displayed (Figure 77).

Figure 77: Certificate Import Wizard



6. Follow the wizard instructions and install the certificate to the Trusted Root Certification Authorities location.

11.2 Issues and Resolutions

Your system might operate in an unexpected manner in several circumstances. Table 2: Troubleshooting Issues and Resolutions explains some of these circumstances and offers one or more solutions for each issue.

Table 2: Troubleshooting Issues and Resolutions

Issue	Resolution
The **Emulex OneCommand** tab is not visible in the console.	In the console, select the **Plug-in** menu and choose **Manage Plug-ins**. In the **Plug-in Manager** window, check the status of the Emulex OneCommand Manager for VMware vCenter (Emulex OneCommand). The status must be Enabled. If it is not, enable it. On the machine where OneCommand Manager for VMware vCenter is installed, make sure that the port numbers configured during the installation are open and dedicated to the plug-in server only. No other service should be listening on this port.
When you select the **Emulex OneCommand** tab in the console, a message appears indicating that the Adobe Flash player is required.	Ensure that the version of Adobe Flash player installed is 11.2 or later. If you have not installed the Adobe Flash player, you can download it from the Adobe website.
When you select the **Emulex OneCommand** tab in the console, the **Emulex Device Management** tree-view does not display any elements.	Ensure that you have the required privileges to view information in the console.
There is slow response from OneCommand Manager for VMware vCenter.	Ensure that the following are on the same network: ■ ESXi servers managed by the OneCommand Manager VMware for vCenter server ■ Systems hosting the OneCommand Manager for VMware vCenter server ■ OneCommand Manager for VMware vCenter
Firmware update fails.	On the ESXi host, check the firewall settings and ensure that the HTTP/HTTPS ports are open. Use the following command to disable the firewall: `esxcli network firewall unload`
Firmware update fails with the error message `Error reading resource`.	Check the following: **NOTE:** Make sure that you can run the `ping` command the host name, on which the OneCommand Manager for VMware vCenter is installed, from the ESXi host. If you cannot run the `ping` command on the host name, either reinstall providing the reachable IP or host name (with domain) or add the host name to the DNS. ■ Check the memory space in the ESXi host and clean up the old logs.
When you make any changes to the ESXi host, such as plugging cables, unplugging cables, or storage references, OneCommand Manager for VMware vCenter does not reflect the change immediately.	Click **Refresh** in the GUI. If the change is not reflected, restart `sfcb` on the ESXi host using the command: `/etc/init.d/sfcbd-watchdog restart` Click **Refresh** again in the GUI.
On a Windows 7 x64 operating system, executing the CLI commands using the executables results in unnecessary error traces.	The C disk is highly protected; even the administrator account has limited privileges. For example, the contents in the directory `C:\Program Files\` have no write and full control privileges. To remedy the problem: ■ Assign your account write and full control privileges to `C:\Program Files\`. or ■ Install OneCommand Manager for VMware vCenter on another disk, for example, `D:`.
When OneCommand Manager for VMware vCenter loads within the console, it displays a security warning.	See Section 11.1, Security.
Registration of a new host from a non-English system results in a *Host not Pingable* error.	When adding the host, change the locale of the system to English. Once the host is added, the locale can be changed.

Chapter 12: Using the OneCommand Manager for VMware vCenter Command Line Interface

The CLI client component of OneCommand Manager for VMware vCenter is installed as part of OneCommand Manager for VMware vCenter installation.

elxvcpcmd Syntax Usage

- The OneCommand Manager for VMware vCenter CLI runs only in TCP/IP mode.
- The OneCommand Manager for VMware vCenter CLI can manage Emulex adapters in systems with VMware ESXi 6.5 and 6.7 environments.
- CLI client commands are supported for Windows operating systems only.
- All commands must start with `elxvcpcmd.exe`. The `elxvcpcmd.exe` command is available in the OneCommand Manager for VMware vCenter installation directory (which is by default `C:\Program Files\Emulex`). This component is intended for use in scripted operations within batch files. Each time you run this script from the command line, a single operation is performed.
- Most operations retrieve information about an entity on the SAN and show that information on the console.
- Most of the CLI client commands require one or more additional parameters that specify the nature of the command.
- The requested operation must contain at least three characters, or as many as needed to distinguish it from any other operation.
- The parameters must be specified in the order indicated in the syntax.
- Parameters that are not required and can be omitted are in square brackets [ ].
- To run a command at the cluster level, use:
  ```
  elxvcpcmd.exe  v=<vcenter server> u=<vc_username> p=<vc_pwd> c=<clustername> <ocm_cmd>
  [<ocm_cmd_arg>...]
  ```
- To run a command at the host level, use:
  ```
  elxvcpcmd.exe  v=<vcenter server> u=<vc_username> p=<vc_pwd> h=<esx_host> <ocm_cmd>
  [<ocm_cmd_arg>...]
  ```
- The WWPN of the adapter must be specified.

NOTE: When a WWPN is specified, individual fields are separated by colons (`:`).

For example, run the following command to display the port attributes for the adapter with the specified WWPN:

```
elxvcpcmd.exe  v=10.120.121.122 u=Administrator p=password h=10.120.121.123 portattributes
10:00:00:00:C9:39:6C:9D
```

NOTE: When a MAC address is specified, the fields are separated by a dash (`-`).

For example, run the following command to show the port attributes for the adapter port with the specified MAC address:

```
elxvcpcmd.exe  v=10.120.121.122 u=Administrator p=password h=10.120.121.123 portattributes 00-11-
22-33-44-55
```

- For help purposes only, commands are grouped together.

12.1 Help Commands

Help commands include help for a single command or a group of commands.

12.1.1 help (Single Command)

Syntax

`elxvcpcmd.exe [CmdName] help`

Description

This command displays the help for a specific command.

Parameters

CmdName Any CLI command.

12.1.2 help (Group)

Syntax

`elxvcpcmd.exe help`

Description

This command displays the help for a group. These help groups are categorized based on the functionality of the commands. Table 4: Help Groups and Supported CLI Commands displays all supported groups, definitions, and supported commands. You can specify the group name in the `help` command to find the commands supported for a group.

Example Command

`elxvcpcmd.exe help`

Parameters

None.

12.2 CLI Command Reference Tables

Table 3 lists CLI commands in alphabetical order, with the corresponding section number for details.

Table 4 lists the CLI commands within a help group. These help groups are categorized based on the functionality of the commands..

Table 3: CLI Commands

Command	Section
`authconfiglist`	Section 12.3.3.5, authconfiglist
`changewwn`	Section 12.3.13.1, changewwn
`D-Port (ClearLink)`	Section 12.3.7.1, D_Port
`deletedumpfiles`	Section 12.3.6.1, deletedumpfiles
`driverconfig`	Section 12.3.8.1, driverconfig
`dump`	Section 12.3.6.2, dump
`echotest`	Section 12.3.7.2, echotest
`enablebootcode`	Section 12.3.4.1, enablebootcode

Table 3: CLI Commands (Continued)

Command	Section (Continued)
enablefecstate	Section 12.3.2.1, enablefecstate
exportsaninfo	Section 12.3.5.1, exportsaninfo
fctraceroute	Section 12.3.7.3, fctraceroute
firmwareupdate	Section 12.3.5.2, firmwareupdate
getauthconfig	Section 12.3.3.6, getauthconfig
getauthstatus	Section 12.3.3.7, getauthstatus
getbeacon	Section 12.3.7.4, getbeacon
getbootparams	Appendix 12.3.4.2, getbootparams
getdriverparams	Section 12.3.8.2, getdriverparams
getdriverparamsglobal	Section 12.3.8.3, getdriverparamsglobal
getdumpdirectory	Section 12.3.6.3, getdumpdirectory
getdumpfilenames	Section 12.3.6.4, getdumpfilenames
getfwparams	Section 12.3.9.2, getfwparams
getlunlist	Section 12.3.10.1, getlunlist
getportstatistics	Section 12.3.2.2, getportstatistics
getretentioncount	Section 12.3.6.5, getretentioncount
gettrunkinfo	Section 12.3.11.1, gettrunkinfo
getvpd	Section 12.3.2.3, getvpd
getwwncap	Section 12.3.2.4, getwwncap
getxcvrdata	Section 12.3.7.5, getxcvrdata
hbaattributes	Section 12.3.2.5, hbaattributes
initiateauth	Section 12.3.3.8, initiateauth
listhbas	Section 12.3.2.6, listhbas
listvms	Section 12.3.12.1, listvms
listvports	Section 12.3.12.2, listvports
loadlist	Section 12.3.7.6, loadlist
loopbacktest	Section 12.3.7.7, loopbacktest
pcidata	Section 12.3.2.7, pcidata
portattributes	Section 12.3.2.8, portattributes
posttest	Section 12.3.7.8, posttest
readwwn	Section 12.3.13.3, readwwn
removeadapterauthconfig	Section 12.3.3.4, removeadapterauthconfig
removeauthconfig	Section 12.3.3.3, removeauthconfig
reset	Section 12.3.1.2, reset
restorewwn	Section 12.3.13.4, restorewwn
saveconfig	Section 12.3.8.4, saveconfig
serverattributes	Section 12.3.2.9, serverattributes
setauthconfigparams	Section 12.3.3.2, setauthconfigparams
setauthconfigsecret	Section 12.3.3.1, setauthconfigsecret
setbeacon	Section 12.3.7.9, setbeacon
setbootparam	Section 12.3.4.3, setbootparam
setdriverparam	Section 12.3.8.5, setdriverparam
setdriverparamdefaults	Section 12.3.8.6, setdriverparamdefaults

Table 3: CLI Commands (Continued)

Command	Section (Continued)
`setdumpdirectory`	Section 12.3.6.6, setdumpdirectory
`setfwparam`	Section 12.3.9.3, setfwparams
`setportenabled`	Section 12.3.2.10, setportenabled
`setportspeed`	Section 12.3.2.11, setportspeed
`setretentioncount`	Section 12.3.6.7, setretentioncount
`settrunkmode`	Section 12.3.11.2, settrunkmode
`setvcred`	Section 12.3.1.1, setvccred
`targetmapping`	Section 12.3.10.2, targetmapping
`version`	Section 12.3.1.3, version

Table 4: Help Groups and Supported CLI Commands

Help Group	Supported CLI Commands	Command Descriptions
General group – General commands that can be run on the OneCommand manager application for VMware servers.	■ reset ■ setvccred ■ version	`reset` – Resets the adapter. `setvcred` – An optional command that saves vCenter credentials and executes subsequent commands without specifying vCenter credentials. `version` – Shows the version of the installed CLI.
Attributes group – Commands to read and manage information about an adapter.	■ enablefecstate ■ getportstatistics ■ getvpd ■ hbaattributes ■ listhbas ■ pcidata ■ portattributes ■ serverattributes ■ setportenabled ■ setportspeed	`enablefecstate` – Enables and disables FEC. `getportstatistics` – Lists statistics for a port. If the optional parameter, `clear`, is set, this command clears the 10GBASE-T counters. `getvpd` – Shows the VPD details for the specified port on the adapter. `hbaattributes` – At the host level, displays adapter attributes for a port on the adapter. `listhbas` – For a cluster or a host, displays a list of manageable Emulex adapters. `pcidata` – Lists PCI attributes for a port on the adapter. `portattributes` – Shows a list of all port attributes for the port on the adapter. `serverattributes` – Lists basic information about the host. `setportenabled` – Enables or disables the port status for a port on a host. `setportspeed` – Defines the link speed of the specified port.

Table 4: Help Groups and Supported CLI Commands (Continued)

Help Group	Supported CLI Commands	Command Descriptions (Continued)
Authentication group – Commands to configure DHCHAP authentication between the adapter and the switch.	■ setauthconfigsecret ■ setauthconfigparams ■ removeauthconfig ■ removeadapterauthconfig ■ authconfiglist ■ getauthconfig ■ getauthstatus ■ initiateauth	`setauthconfigsecret` – Sets the local or remote secret on the adapter for an authenticated connection to the switch. `setauthconfigparams` – Sets one or more authentication configuration parameters for the FC port `removeAuthConfig` – Removes or deletes one or more authentication configuration entries for an FC port. `removeadapterauthconfig` – Removes or deletes all authentication configuration entries for an adapter. `authconfiglist` – Retrieves the authentication configuration for the specified entity pair. `getauthconfig` – Retrieves the authentication configuration for the specified entity pair. `getauthstatus` – Returns the current status for the authentication connection specified by WWPN1 and WWPN2. `initiateauth` – Initiates the authentication configuration on the adapter.
Boot group – Commands to enable an ESXi host to manage the boot environment.	■ enablebootcode ■ getbootparams ■ setbootparam	`enablebootcode` – Enables or disables the bootBIOS state on a given port. `getbootparams` – Fetches the boot parameters for a given port and given boot type. `setbootparam` – Fetches the boot parameters for a given port and given boot type
Cluster group – Commands that can be run on a cluster.	■ exportsaninfo ■ firmwareupdate ■ listhbas	`exportsaninfo` – Exports SAN information related to Emulex adapters in all the hosts in a cluster. `firmwareupdate` – Updates the firmware on the Emulex adapters found in a VMware cluster or the ESXi host. `listhbas` – Lists manageable Emulex adapters.
Diagnostic group – Commands to run diagnostic tests for an Emulex adapter or port.	■ D_Port ■ echotest ■ fctraceroute ■ getbeacon ■ getxcvrdata ■ loadlist ■ loopbacktest ■ posttest ■ setbeacon	`D_Port` – Runs D_Port diagnostics. Also known as ClearLink. `echotest` – Runs an echo test on a port. `fctraceroute` – Issues an FC trace route request for the communication path between an FC initiator port and an FC target port. `getbeacon` – Shows the current beacon state for a port on an adapter. `getxcvrdata` – Shows the transceiver data, such as vendor name and serial number. `loadlist` – Lists the flash memory load list data for an FC port. `loopbacktest` – Runs a loopback test on a port. `posttest` – Runs a POST on a specified FC port. `setbeacon` – Turns the beacon state on or off for an adapter port and sets the beacon's duration.

Table 4: Help Groups and Supported CLI Commands (Continued)

Help Group	Supported CLI Commands	Command Descriptions (Continued)
Driver Parameters group – Commands to enable an ESXi host to read and manage driver parameters for the host and an Emulex adapter.	■ driverconfig ■ getdriverparamsglobal ■ saveconfig ■ setdriverparam ■ setdriverparamdefaults	`driverconfig` – Sets all driver parameters to the values in the `.dpv` file on an ESXi host. `getdriverparamsglobal` – Lists global driver parameters for a port. `saveconfig` – Saves an adapter's driver parameters to a file. `setdriverparam` – Sets a driver parameter for a port and designates the scope of the change. `setdriverparamdefaults` – Restores all driver parameters to the default value, at the port or global level (temporarily or permanently).
Collect Dump group – Commands to manage dump files for a selected adapter. Dump files are useful when troubleshooting.	■ deletedumpfiles ■ dump ■ getdumpdirectory ■ getdumpfilenames ■ getretentioncount ■ setdumpdirectory ■ setretentioncount	`deletedumpfiles` – Deletes all diagnostic dump files for a port. `dump` - Performs a dump of a local port. `getdumpdirectory` – Shows a dump file directory for a port in the host. `getdumpfilenames` – Lists all dump file names for a port. `getretentioncount` – Shows the maximum number of diagnostic dump files to keep for a port. `setdumpdirectory` – Sets the dump directory for all adapters in the server. `setretentioncount` – Specifies the maximum number of diagnostic dump files for the adapter.
Firmware group – Commands to update the firmware, view the firmware parameters, and change the firmware parameters on an Emulex adapter or port.	■ firmwareupdate ■ getfwparams ■ setfwparams	`firmwareupdate` – Updates the firmware on Emulex adapters in a VMware cluster or ESXi host. `getfwparams` – Displays the available firmware parameters, and their ranges, for the specified port. `setfwparams` – Assigns new firmware parameter values to the specified port.
Target and LUNs group – Commands to enable an ESXi host to read targets and LUNs attached to the port on an Emulex adapter.	■ getlunlist ■ targetmapping	`getlunlist` – Lists the LUNs attached to the target of the specified port. `targetmapping` – Lists the targets attached to the specified port.
Trunking group – Commands to view and configure trunking.	■ gettrunkinfo ■ settrunkmode	`gettrunkinfo` – Shows the trunking configuration for the specified port. `settrunkmode` – Configures trunking for the specified port.
Virtual Machines group – Commands to enable an ESXi host to find virtual machines and their attached ports.	■ listvms ■ listvports	`listvms` – Lists all virtual machines and their information for all manageable ports. `listvports` – Lists all virtual ports on the specified physical port.
WWWN Management group – Commands to enable an ESXi host to read and manage the WWN details for the port on an Emulex adapter.	■ changewwn ■ getwwncap ■ readwwn ■ restorewwn	`changewwn` – Changes the WWN of the port. `getwwncap` – Lists the WWN capabilities of the port. `readwwn` – Lists the WWN details of the port and category. `restorewwn` – Restores the WWN value of the port.

12.3 Group Commands and CLI Command Descriptions

This section provides syntax and descriptions for group and CLI commands.

12.3.1 General Group Commands

The General group commands save vCenter credentials, reset the adapter, and show the version of the installed CLI.

12.3.1.1 setvccred

Syntax

`elxvcpcmd.exe setvccred v=<vCenter IP/Name> u=<username> p=<password>`

Description

While executing a set of CLI commands, you must enter vCenter credentials repeatedly. By executing the `setvccred` command first, you can save these credentials including vCenter server name/IP, user name, and password to a file in an encrypted format and execute subsequent commands without the use of vCenter credentials.

Using this command is optional. You can continue to execute the commands providing all credentials.

NOTE: This command does not apply to ports or adapters.

Parameters

`v` The vCenter server IP address.

`u` The user name for the vCenter server.

`p` The user password for the vCenter server.

Examples

Execute `setvccred` first:

```
elxvcpcmd.exe setvccred v=12.345.678.xxx u=username p=password
```

Subsequent commands can be:

New format:

```
elxvcpcmd.exe h=12.345.678.xxx listhbas
```

or

Old format:

```
elxvcpcmd.exe v=12.345.678.901 u=username p=password h=12.345.678.xxx listhbas
```

12.3.1.2 reset

This command resets the adapter. An adapter reset can require several seconds to complete, especially for remote devices. When the reset is completed, the system command prompt is displayed.

Syntax

```
elxvcpcmd.exe v=<vcenter_server> u=<vc_username> p=<vc_password>  h=<esx_host> reset <WWPN>
```

Parameters

`v`	The vCenter server IP address.
`u`	The user name for the vCenter server.
`p`	The user password for the vCenter server.
`h`	The IP address of the ESXi host.
`WWPN`	The WWPN of the port.

12.3.1.3 version

This command displays the version of the CLI installed.

Syntax

```
elxvcpcmd.exe version
```

Parameters

None.

12.3.2 Attribute Commands

The Attribute commands show and update CIM information, port information, adapter attributes, PCI data, and server attributes. These commands also enable a port on a host and set the physical port speed.

12.3.2.1 enablefecstate

This command enables or disables FEC on the specified adapter.

NOTE: Not supported on LPe12000-series adapters.

Syntax

```
elxvcpcmd.exe v=<vcenter_server> u=<vc_username> p=<vc_password> h=<esx_host> enablefecstate <WWPN>
[Flag]
```

Parameters

`v`	The vCenter server IP address.
`u`	The user name for the vCenter server.
`p`	The user password for the vCenter server.
`h`	The IP address of the ESXi host.
`WWPN`	The WWPN of the HBA.
`Flag`	`0` = Disable FEC state. `1` = Enable FEC state.

12.3.2.2 getportstatistics

This command extracts the statistics for a designated port.

Syntax

```
elxvcpcmd.exe v=<vcenter_server> u=<vc_username> p=<vc_password> h=<esx_host> getportstatistics
<WWPN>
```

Parameters

v	The vCenter server IP address.
u	The user name for the vCenter server.
p	The user password for the vCenter server.
h	The IP address of the ESXi host.
WWPN	The WWPN of a port.

12.3.2.3 getvpd

This command displays the VPD details for the specified port on the adapter.

Syntax

```
elxvcpcmd.exe  v=<vcenter server> u=<vc_username> p=<vc_pwd> h=<ESXhostIP> getvpd <WWPN>
```

Parameters

v	The vCenter server IP address.
u	The user name for the vCenter server.
p	The user password for the vCenter server.
h	The IP address of the ESXi host
WWPN	The WWPN of a port.

12.3.2.4 getwwncap

This command displays the WWN capabilities of the specified port.

Syntax

```
elxvcpcmd.exe  v=<vcenter server> u=<vc_username> p=<vc_pwd> h=<ESXhostIP> getwwncap <WWPN>
```

Parameters

v	The vCenter server IP address.
u	The user name for the vCenter server.
p	The user password for the vCenter server.
h	The IP address of the ESXi host.
WWPN	The WWPN of a port.

12.3.2.5 hbaattributes

This command displays a list of all adapter attributes for the specified port on the adapter. This command is supported only at the host level.

Syntax

```
elxvcpcmd.exe  v=<vcenter server> u=<vc_username> p=<vc_pwd> h=<ESXhostIP> hbaattributes  <WWPN>
```

Parameters

v	The vCenter server IP address.
u	The user name for the vCenter server.
p	The user password for the vCenter server.
h	The IP address of the ESXi host.
WWPN	The WWPN of a port.

12.3.2.6 listhbas

This command displays a list of the manageable Emulex adapters found by remote discovery.

Syntax

For a cluster:

```
elxvcpcmd.exe  v=<vcenter server> u=<vc_username> p=<vc_pwd> c=<clustername> listhbas
```

For a host:

```
elxvcpcmd.exe  v=<vcenter server> u=<vc_username> p=<vc_pwd> h=<ESXhostIP> listhbas
```

Parameters

v	The vCenter server IP address.
u	The user name for the vCenter server.
p	The user password for the vCenter server.
c	The cluster name in the console.
h	The IP address of the ESXi host.

12.3.2.7 pcidata

This command displays the PCI attributes for the port specified on the adapter.

Syntax

```
elxvcpcmd.exe  v=<vcenter server> u=<vc_username> p=<vc_pwd> h=<ESXhostIP> pcidata <WWPN>
```

Parameters

v	The vCenter server IP address.
u	The user name for the vCenter server.
p	The user password for the vCenter server.
h	The IP address of the ESXi host.
WWPN	The WWPN of a port.

12.3.2.8 portattributes

This command displays a list of all port attributes for the port on the adapter.

Syntax

```
elxvcpcmd.exe  v=<vcenter server> u=<vc_username> p=<vc_pwd> h=<ESXhostIP> portattributes <WWPN>
```

Parameters

`v`	The vCenter server IP address.
`u`	The user name for the vCenter server.
`p`	The user password for the vCenter server.
`h`	The IP address of the ESXi host.
`WWPN`	The WWPN of a port.

12.3.2.9 serverattributes

This command retrieves basic information about the host such as the operating system version and CIM Provider version.

Syntax

```
elxvcpcmd.exe v=<vcenter_server> u=<vc_username> p=<vc_password>  h=<esx_host> serverattributes
```

Parameters

`v`	The vCenter server IP address.
`u`	The user name for the vCenter server.
`p`	The user password for the vCenter server.
`h`	The IP address of the ESXi host.

12.3.2.10 setportenabled

This command enables or disables a port on a host.

NOTE:

- Ensure that all I/O traffic on the port is stopped before disabling the port.
- When the `setportenabled` command disables a port, the adapter must be reset to activate the new value.

Syntax

```
elxvcpcmd.exe v=<vcenter_server> u=<vc_username> p=<vc_password>  h=<esx_host> setportenabled <WWPN>
<Flag>
```

Parameters

`v`	The vCenter server IP address.
`u`	The user name for the vCenter server.
`p`	The user password for the vCenter server.
`h`	The IP address of the ESXi host.
`WWPN`	The WWPN of a port.
`Flag`	`0` = Disabled. `1` = Enabled.

12.3.2.11 setportspeed

This command defines the link speed for a port.

Syntax

```
elxvcpcmd.exe v=<vcenter_server> u=<vc_username> p=<vc_password>  h=<esx_host> setportspeed <WWPN>
<linkspeed>
```

Parameters

`v`	The vCenter server IP address.
`u`	The user name for the vCenter server.
`p`	The user password for the vCenter server.
`h`	The IP address of the ESXi host.
`WWPN`	The WWPN of a port.
`linkspeed`	A numeric value representing a supported link speed. For a list of port speeds supported by the adapter, use the `PortAttributes` command. Specify a value of `0` to configure Auto Detect mode.

12.3.3 Authentication Commands

These commands configure a DHCHAP connection between an FC function and a switch port. (These commands are not supported on LPe12000-series adapters.)

12.3.3.1 setauthconfigsecret

This command sets the local or remote secret on the adapter for an authenticated connection to the switch.

Syntax

```
elxvcpcmd.exe  v=<vcenter server> u=<vc_username> p=<vc_pwd> h=<ESXhostIP> setauthconfigsecret <WWPN1>
<WWPN2> <Flag> <Nst> <Nsv>
```

Parameters

`v`	The vCenter server IP address.
`u`	The user name for the vCenter server.
`p`	The user password for the vCenter server.
`h`	The IP address of the ESXi host.
`WWPN1`	The WWPN of an FC function.
`WWPN2`	Use either `ff:ff:ff:ff:ff:ff:ff:ff` for a switch, or use the actual WWPN for a target.
`Flag`	`1` = Local (secret used by the adapter when the adapter authenticates to the switch, and when using bidirectional authentication). `2` = Remote (secret used when the switch initiates authentication to the HBA and when using bidirectional authentication).
`Nst`	Current secret type. `1` = ASCII `2` = Hexadecimal (binary)
`Nsv`	New secret value. `1` = ASCII `2` = Hexadecimal (binary)

12.3.3.2 setauthconfigparams

This command sets one or more authentication configuration parameters for the FC port.

Syntax

`elxvcpcmd.exe v=<vcenter server> u=<vc_username> p=<vc_pwd> h=<ESXhostIP> setauthconfigparams <WWPN1> <WWPN2> <mode value> <dh-priority value> <hash-priority value> <timeout value> <bidirectional value> <re-authentication value> <re-authentication-interval value>`

NOTE: Where multiple parameters and values are used, separate them using commas.

Parameters

`v`	The vCenter server IP address.
`u`	The user name for the vCenter server.
`p`	The user password for the vCenter server.
`h`	The IP address of the ESXi host.
`WWPN1`	The WWPN of an FC function.
`WWPN2`	Either use `ff:ff:ff:ff:ff:ff:ff:ff` for a switch, or use the WWPN for a target.
`PasswordType`	`1` = ASCII `2` = Hexadecimal (binary) `3` = Password not yet defined
`Password`	The current password value.
`Param`	The parameter names: ■ `Mode` ■ `DH-priority` ■ `Hash-priority` ■ `Timeout` ■ `Bidirectional` ■ `Re-authentication` ■ `Re-authentication-interval`
`Value`	The value is based on the type of <*Param*>: ■ `Mode`: `disabled`, `enabled`, or `passive` ■ `Timeout`: time in seconds ■ `Bidirectional`: `disabled` or `enabled` ■ `Hash-priority`: `md5` or `sha1` (`md5` = first md5, then sha1; `sha1` = first sha1, then md5) ■ `DH-priority`: `1`, `2`, `3`, `4`, `5`; any combination up to 5 digits ■ `Re-authentication`: `disabled` or `enabled` ■ `Re-authentication-interval`: `0`, `10` to `3600`, in seconds

12.3.3.3 removeauthconfig

This command removes or deletes one or more authentication configuration entries for an FC port.

Syntax

```
elxvcpcmd.exe  v=<vcenter server> u=<vc_username> p=<vc_pwd> h=<ESXhostIP> removeauthconfig <WWPN>
<entity pair 1> <entity pair 2> <entity pair N>
```

Parameters

`v`	The vCenter server IP address.
`u`	The user name for the vCenter server.
`p`	The user password for the vCenter server.
`h`	The IP address of the ESXi host.
`WWPN`	The WWPN of the FC port whose configuration you want to delete.
`Entity pair`	LocalEntity, RemoteEntity `LocalEntity` = Source WWPN `RemoteEntity` = Destination WWPN Use `all` to delete the entire authentication configuration.

12.3.3.4 removeadapterauthconfig

This command removes or deletes all authentication configuration entries for an adapter.

NOTE: This command deletes the authentication configuration, including secrets, from the adapter flash memory. To activate the new driver settings, you must reload the driver.

Syntax

```
elxvcpcmd.exe  v=<vcenter server> u=<vc_username> p=<vc_pwd> h=<ESXhostIP> removeadapterauthconfig
<WWPN>
```

Parameters

`v`	The vCenter server IP address.
`u`	The user name for the vCenter server.
`p`	The user password for the vCenter server.
`h`	The IP address of the ESXi host.
`WWPN`	The WWPN of the port whose configurations you want to delete.

12.3.3.5 authconfiglist

This command returns the list of entity pairs (source WWPN and destination WWPN) that have a stored authentication configuration.

Syntax

```
elxvcpcmd.exe  v=<vcenter server> u=<vc_username> p=<vc_pwd> h=<ESXhostIP> authconfiglist <WWPN>
```

Parameters

`v`	The vCenter server IP address.
`u`	The user name for the vCenter server.
`p`	The user password for the vCenter server.
`h`	The IP address of the ESXi host.
`WWPN`	The WWPN of an FC function.

12.3.3.6 getauthconfig

This command retrieves the authentication configuration for the specified entity pair (source port and destination port).

Syntax

```
elxvcpcmd.exe  v=<vcenter server> u=<vc_username> p=<vc_pwd> h=<ESXhostIP> getauthconfig <WWPN1>
<WWPN2>
```

Parameters

`v`	The vCenter server IP address.
`u`	The user name for the vCenter server.
`p`	The user password for the vCenter server.
`h`	The IP address of the ESXi host.
`WWPN1`	The WWPN of an FC function.
`WWPN2`	Use either `ff:ff:ff:ff:ff:ff:ff:ff` for a switch or the WWPN for a target.

12.3.3.7 getauthstatus

This command returns the current status for the authentication connection specified by WWPN1 and WWPN2 (adapter and switch).

Syntax

```
elxvcpcmd.exe  v=<vcenter server> u=<vc_username> p=<vc_pwd> h=<ESXhostIP> getauthstatus <WWPN1>
<WWPN2>
```

Parameters

`v`	The vCenter server IP address.
`u`	The user name for the vCenter server.
`p`	The user password for the vCenter server.
`h`	The IP address of the ESXi host.
`WWPN1`	The WWPN of an FC function.
`WWPN2`	Use either `ff:ff:ff:ff:ff:ff:ff:ff` for a switch or the WWPN for a target.

12.3.3.8 initiateauth

This command initiates the authentication configuration on the adapter.

Syntax

```
elxvcpcmd.exe  v=<vcenter server> u=<vc_username> p=<vc_pwd> h=<ESXhostIP> > initiateauth <WWPN1>
<WWPN2>
```

Parameters

`v`	The vCenter server IP address.
`u`	The user name for the vCenter server.
`p`	The user password for the vCenter server.
`h`	The IP address of the ESXi host.
`WWPN1`	The WWPN of an FC function.
`WWPN2`	Use either `ff:ff:ff:ff:ff:ff:ff:ff` for a switch or the WWPN for a target.

12.3.4 Boot Commands

The `enablebootcode` command enables or disables the bootBIOS state on a port.

CAUTION! Using the `enablebootcode` command on an LPe12000-series adapter that is being used to boot from SAN is not advisable. After the command has completed, the system performs an adapter reset, which might cause a loss of connectivity to the SAN and possible loss of data. To perform this command, you must make sure that the adapter is not currently being used to boot from SAN.

Do one of the following:

- Move the target adapter to a non-boot from SAN host.
- If the host with the target adapter is also hosting other boot from SAN adapters, perform a boot from SAN using one of the other boot from SAN adapters. The target adapter can now be used.

12.3.4.1 enablebootcode

This command enables or disables the bootBIOS state on a given port by enabling or disabling the boot code on the adapter.

Syntax

```
elxvcpcmd.exe v=<vcenter_server> u=<vc_username> p=<vc_password>  h=<esx_host> enablebootcode <WWPN>
[Flag]
```

Parameters

`v`	The vCenter server IP address.
`u`	The user name for the vCenter server.
`p`	The user password for the vCenter server.
`h`	The IP address of the ESXi host.
`WWPN`	The WWPN of a port.
`Flag`	`0` = Disable the BootBIOS state. `1` = Enable the BootBIOS state.

12.3.4.2 getbootparams

This command fetches the boot parameters for a given port and given boot type.

Syntax

```
elxvcpcmd.exe v=<vcenter_server> u=<vc_username> p=<vc_password> h=<esx_host> getbootparams <wwpn>
<boot type>
```

Parameters

`v`	The vCenter server IP address.
`u`	The user name for the vCenter server.
`p`	The user password for the vCenter server.
`h`	The IP address of the ESXi host.
`WWPN`	The WWPN of the HBA.
`boot type`	`X86` = X86 `EFI` = EFI Boot `OB` = OpenBoot

12.3.4.3 setbootparam

This command sets the boot parameter for a specified port and a specified boot type.

Syntax

```
elxvcpcmd.exe v=<vcenter_server> u=<vc_username> p=<vc_password> h=<esx_host> setbootparam <WWPN>
<Type> <Param> <Value1> [BootDev <Value2>]
```

Parameters

`v`	The vCenter server IP address.
`u`	The user name for the vCenter server.
`p`	The user password for the vCenter server.
`h`	The IP address of the ESXi host.
`WWPN`	The WWPN of the HBA.
`boot type`	`X86` = X86 `EFI` = EFI Boot `OB` = OpenBoot

`adapter parameters`	`DefaultAlpa` <*value*> `EnableAdapterBoot` (`0` = disable, `1` = enable) `EnableBootFromSan` (`0` = disable, `1` = enable) `LinkSpeed` (`2`, `4`, `8`, `16`, `32`) `PlogiRetryTimer` (`0`, `1`, `2`, `3`) `Topology` (`0`, `1`, `2`, `3`) `AutoScan` (`0`, `1`, `2`, `3`) X86 only `AutoBootSectorEnable` (`0` = disable, `1` = enable) X86 only `EDD30Enable` (`0` = disable, `1` = enable) X86 only `EnvVarEnable` (`0` = disable, `1` = enable) X86 only `SpinupDelayEnable` (`0` = disable, `1` = enable) X86 only `StartUnitCommandEnable` (`0` = disable, `1` = enable) X86 only `BootTargetScan` (`0`, `1`, `2`) EFI only `DevicePathSelection` (`0`, `1`) EFI only `MaxLunsPerTarget` <*value*> EFI only `ResetDelayTimer` <*value*> EFI only `SfsFlag` (`0` = disable, `1` = enable) OB only
`boot device parameters`	`D_ID` (<*value*>[`BootDev` <*value2*>]) `LUN` (<*value*>[`BootDev` <*value2*>]) `TargetWwpn` (<*value*>[`BootDev` <*value2*>]) `TargetID` <*value*> OB only

12.3.5 Cluster Commands

The Cluster commands export SAN information, update firmware, and list adapters.

12.3.5.1 exportsaninfo

This command exports all SAN information related to Emulex adapters in all hosts in a cluster. This command is supported only at the cluster level.

NOTE: Due to the amount of information that must be obtained and reported, this command can take a long time to run on large SAN configurations. You can redirect this output to a file with a proper extension, `.xml` for XML-formatted files and `.csv` for CSV-formatted files.

Syntax

`elxvcpcmd.exe v=<vcenter server> u=<vc_username> p=<vc_pwd> c=<clustername> exportsaninfo [format]`

NOTE: The `[format]` parameter is optional. If the `format` parameter is specified as `csv`, the adapter information is shown in CSV format. If the `format` parameter is specified as `xml`, the adapter information is shown in XML format. Leaving the `format` parameter blank displays the data in XML format.

Parameters

`v`	The vCenter server IP address.
`u`	The user name for the vCenter server.
`p`	The user password for the vCenter server.
`c`	The cluster name.
`format`	`csv` – The output information in CSV format. `xml` – The output information in XML format (default).

12.3.5.2 firmwareupdate

This command updates the firmware on the Emulex adapters found in the specified VMware cluster or the ESXi host.

Procedure

1. Run the `firmwareupdate` command. A list of adapter serial numbers or port WWNs (for LPe12000-series adapters) is displayed, applicable to the firmware file specified.
2. Select the adapter or port option to use for the update. The `List`, `Range`, `All`, or `Choice` options are displayed.
3. The firmware update process begins and returns the result for each adapter or port.
4. If you press **Ctrl + C** and the firmware update process has started on any adapter or port, the update continues. But if the firmware update process is queued, the update is canceled.

NOTE: The optional argument [`all`|`WWNs`|`MACs`] updates the firmware without any user prompt. Either `all` or a combination of `WWNs` and `MACs` can be given as an option.

You can view the status of submitted firmware jobs on the OneCommand Manager VMware for vCenter, **Maintenance** tab of the cluster or host.

Syntax

For a cluster:

```
elxvcpcmd.exe v=<vcenter server> u=<vc_username> p=<vc_pwd> c=<clustername> firmwareupdate
[all|WWNs|MACs] <filelocation>
```

For a host:

```
elxvcpcmd.exe v=<vcenter server> u=<vc_username> p=<vc_pwd> h=<ESXhostIP> firmwareupdate
[all|WWNs|MACs] <file location>
```

Parameters

`v`	The vCenter server IP address.
`u`	The user name for the vCenter server.
`p`	The user password for the vCenter server.
`c`	The cluster name in the console.
`h`	The IP address of the ESXi host.
`all|WWNs|MACs` (optional)	The `all` optional argument updates all compatible adapters or ports without any user prompt. The `WWNs` or `MACs` optional argument updates the port WWNs or MACs belonging to a specified cluster or host without any user prompt.
`file location`	The firmware file path on the local disk.

12.3.5.3 listhbas

See Section 12.3.2.6, listhbas.

12.3.6 Collect Dump Commands

The Collect Dump commands initiate a dump on a local port, show the dump file for the port on the host, show the diagnostic dump file retention count set on a port, and specify the maximum number of diagnostic dump files for the adapter.

12.3.6.1 deletedumpfiles

This command deletes all diagnostic dump files for a given port.

Syntax

```
elxvcpcmd.exe v=<vcenter_server> u=<vc_username> p=<vc_password>  h=<esx_host> deletedumpfiles <WWPN>
```

Parameters

`v`	The vCenter server IP address.
`u`	The user name for the vCenter server.
`p`	The user password for the vCenter server.
`h`	The IP address of the ESXi host.
`WWPN`	The WWPN of the port.

12.3.6.2 dump

This command performs a dump on a local port. The dump file is placed in the dump directory with the following file name format:

```
<Hostname>_<Adapter_serial_number>_<datetimestamp>
```

If the command is successful, the following message is displayed:

```
Dump Successful.
```

NOTE: Because this command dumps memory, it can take time while generating large files.

Syntax

```
elxvcpcmd.exe v=<vcenter_server> u=<vc_username> p=<vc_password>  h=<esx_host> dump <WWPN>
```

Parameters

`v`	The vCenter server IP address.
`u`	The user name for the vCenter server.
`p`	The user password for the vCenter server.
`h`	The IP address of the ESXi host.
`WWPN`	The WWPN of the port.
Options	Additional options are available under the direction of Broadcom Technical Support.

12.3.6.3 getdumpdirectory

This command displays the dump file directory.

NOTE: The dump directory applies to all adapters in the server. There is not a separate dump directory for each adapter.

Syntax

```
elxvcpcmd.exe v=<vcenter_server> u=<vc_username> p=<vc_password>  h=<esx_host> getdumpdirectory
<WWPN>
```

Parameters

v	The vCenter server IP address.
u	The user name for the vCenter server.
p	The user password for the vCenter server.
h	The IP address of the ESXi host.
WWPN	The WWPN of a port.

12.3.6.4 getdumpfilenames

This command displays a list of all the dump file names for a given port.

Syntax

```
elxvcpcmd.exe v=<vcenter_server> u=<vc_username> p=<vc_password>  h=<esx_host> getdumpfilenames
<WWPN>
```

Parameters

v	The vCenter server IP address.
u	The user name for the vCenter server.
p	The user password for the vCenter server.
h	The IP address of the ESXi host.
WWPN	The WWPN of a port.

12.3.6.5 getretentioncount

This command displays the diagnostic dump file retention count set on a port.

NOTE: The retention count applies to all adapters in the server.

Syntax

```
elxvcpcmd.exe v=<vcenter_server> u=<vc_username> p=<vc_password>  h=<esx_host> getretentioncount
<WWPN>
```

Parameters

v	The vCenter server IP address.
u	The user name for the vCenter server.
p	The user password for the vCenter server.
h	The IP address of the ESXi host.
WWPN	The WWPN of a port.

12.3.6.6 setdumpdirectory

Use the `setdumpdirectory` command to set the dump directory for a given port. To use the `setdumpdirectory` command, you must have a directory mapped under `/vmfs/volumes/` where the files will be placed.

NOTE: The dump directory applies to all adapters in the server. There is no separate dump directory for each adapter.

Syntax

```
elxvcpcmd.exe v=<vcenter_server> u=<vc_username> p=<vc_password>  h=<esx_host> setdumpdirectory
<WWPN> <DumpDirectory>
```

Parameters

`v`	The vCenter server IP address.
`u`	The user name for the vCenter server.
`p`	The user password for the vCenter server.
`h`	The IP address of the ESXi host.
`WWPN`	The WWPN of a port.
`DumpDirectory`	The directory under `/vmfs/volumes` that you created to store the dump files.

Example Command

```
elxvcpcmd v=12.345.678.901 u=username p=password h=12.345.678.123 setdumpdirectory
10:00:00:00:c9:61:f2:64 vcenter-datastore
```

In this example, the dump directory is set to `/vmfs/volumes/vcenter-datastore`.

12.3.6.7 setretentioncount

This command specifies the maximum number of diagnostic dump files for the adapter. When the count reaches the limit, the next dump operation deletes the oldest file.

The retention count applies to all adapters in the server.

Syntax

```
elxvcpcmd.exe v=<vcenter_server> u=<vc_username> p=<vc_password>  h=<esx_host> setretentioncount
<WWPN> <RetentionCount>
```

Parameters

`v`	The vCenter server IP address.
`u`	The user name for the vCenter server.
`p`	The user password for the vCenter server.
`h`	The IP address of the ESXi host.
`WWPN`	The WWPN of port.
`RetentionCount`	The number of dump files to retain.

12.3.7 Diagnostic Commands

The Diagnostic commands run diagnostics, including POST and loopback. Diagnostic commands also show and set beaconing and run the D_Port diagnostic. (Not supported on LPe12000-series and LPe15000-series adapters.)

CAUTION! Using the loopback or POST test commands on an LPe12000-series adapter that is being used to boot from SAN is not advisable. After the command has completed, the system performs an adapter reset, which can cause a loss of connectivity to the SAN and possible loss of data. To perform these commands, you must make sure that the adapter is not currently being used to boot from SAN.

Do one of the following:

- Move the target adapter to a non-boot from SAN host.
- If the host with the target adapter is also hosting other boot from SAN adapters, perform a boot from SAN using one of the other boot from SAN adapters. The target adapter can now be used.

12.3.7.1 D_Port

The D_Port diagnostic is also known as ClearLink. The D_Port diagnostic tests are run from the OneCommand Manager for VMware vCenter CLI by specifying the D_Port command. D_Port is a diagnostic mode supported by Brocade switches for adapters with D_Port support. D_Port is enabled by default. (D_Port is not supported on LPe12000-series adapters.)

D_Port tests detect physical cabling issues that can result in increased error rates and intermittent behavior. When activated, D_Port tests include:

- Local electrical loopback
- Loopback to the remote optics
- Loopback from the remote port to the local optics
- A full device loopback test with data integrity checks
- An estimate of cable length (to validate that a proper buffering scheme is in place)

These tests allow a level of fault isolation to distinguish faults due to marginal cables, optics modules, and connector or optics seating.

NOTE:

- Dynamic D_Port and FA-PWWN cannot be enabled simultaneously. If D_Port is enabled and you want to enable FA-PWWN, you must first disable Dynamic D_Port. If FA-PWWN is enabled and you want to enable Dynamic D_Port, you must first disable FA-PWWN.
- It is not possible to detect if the switch can run D_Port tests before running the tests. Therefore, a test failure occurs if the D_Port command is run with a switch that does not support D_Port.
- To terminate tests while they are running, type **<CTL> + <C>**. In this case, no results are given.
- If the overall test result is FAILED, you must rerun the tests successfully or reset the HBA port to bring the link back up. A message is displayed instructing you to perform one of these actions if the overall test result is FAILED.
- If a test phase fails, the D_Port tests are automatically stopped. In this case, some of the phases might not be reported in the results. However, the failed phase is reported.
- More than one error can be reported. In this case, multiple lines are displayed for the test phase showing each error.

Example

```
elxvcpcmd.exe v=10.192.000.000 u=root p=password d_Port WWPN
```

Parameters

`v`	The vCenter server IP address.
`u`	The user name for the vCenter server.
`p`	The user password for the vCenter server.
`WWPN`	The WWPN of the port on which to run tests.

12.3.7.2 echotest

This command runs a loopback test on a given port.

Syntax

```
elxvcpcmd.exe  v=<vcenter_server> u=<vc_username> p=<vc_password>  h=<esx_host> echotest <WWPN>
<Destination WWPN> <Count> <StopOnError> [Pattern]
```

Parameters

`v`	The vCenter server IP address.
`u`	The user name for the vCenter server.
`p`	The user password for the vCenter server.
`h`	The IP address of the ESXi host.
`WWPN`	The WWPN of a port.
`Destination WWPN`	The WWPN of the destination (echoing) adapter.
`Count`	The number of times to run the test (`0` = run test infinitely; Range = `1` to `99,999`).
`StopOnError`	Checks if the test must be halted on error. `0` = No halt `1` = Halt
`Pattern` (optional)	1 to 8 hexadecimal bytes to use for loopback data (for example: `1a2b3c4d`).

Example

```
elxvcpcmd.exe  v=10.20.30.40 u=user p=password  h=1.2.3.4 echotest 10:00:00:c9:12:34:56
10:00:00:c9:ab:cd:ee 100 1 1a2b3c4d5e
```

12.3.7.3 fctraceroute

This command issues an FC trace route request for the communication path between an FC initiator port and an FC target port.

Syntax

`fctraceroute <WWPN> <Target WWPN>`

Parameters

`WWPN`	The WWPN of the FC port to use as the FC trace route source.
`Target WWPN`	The WWPN of the FC target to use as the FC trace route endpoint.

Example

```
> elxvcpcmd [credentials] fctraceroute 10:00:00:90:fa:5d:05:a9 50:06:01:60:90:20:5C:38


Starting the diagnostic test: FC Trace Route Test

FC Trace Route test status:
Test pending. Polling for results

Test running....

FC Trace Route test succeeded - Results:

 Initiator Port: 10:00:00:90:FA:C7:6E:33
 Target Port   : 20:00:00:11:0D:13:DF:01

 Hop 0
  Switch Name         : 10:00:00:27:F8:F1:15:C0
  Domain ID           : 0x0001
  Ingress Port Name   : 20:0C:00:27:F8:F1:15:C0
  Ingress Port Number : 12
  Egress Port Name    : 20:00:00:27:F8:F1:15:C0
  Egress Port Number  : 0

 Hop 1
  Switch Name         : 10:00:00:27:F8:F1:15:C0
  Domain ID           : 0x0001
  Ingress Port Name   : 20:00:00:27:F8:F1:15:C0
  Ingress Port Number : 0
```

12.3.7.4 getbeacon

This command displays the current beacon state; on or off.

Syntax

```
elxvcpcmd.exe v=<vcenter_server> u=<vc_username> p=<vc_password>  h=<esx_host> getbeacon <WWPN>
```

Parameters

v	The vCenter server IP address.
u	The user name for the vCenter server.
p	The user password for the vCenter server.
h	The IP address of the ESXi host.
WWPN	The WWPN of the port.

12.3.7.5 getxcvrdata

This command displays transceiver data, such as the vendor name and serial number.

Syntax

```
elxvcpcmd.exe v=<vcenter_server> u=<vc_username> p=<vc_password>  h=<esx_host> getxcvrdata <WWPN>
```

Parameters

v	The vCenter server IP address.
u	The user name for the vCenter server.
p	The user password for the vCenter server.
h	The IP address of the ESXi host.
WWPN	The WWPN of the port.

12.3.7.6 loadlist

This command displays the flash parameters for a given port.

Syntax

```
elxvcpcmd.exe v=<vcenter_server> u=<vc_username> p=<vc_password>  h=<esx_host> loadlist <WWPN>
```

Parameters

v	The vCenter server IP address.
u	The user name for the vCenter server.
p	The user password for the vCenter server.
h	The IP address of the ESXi host.
WWPN	The WWPN of the port.

12.3.7.7 loopbacktest

This command runs a loopback test on a given port.

NOTE:

- ESXi 6.7 systems, specifying a non-default value for the number of loopback cycles does not work.
- Adapters and port information are not available during diagnostic loopback tests.
- Internal and External loopback tests are supported on trunking enabled ports.

Syntax

```
elxvcpcmd.exe v=<vcenter_server> u=<vc_username> p=<vc_password>  h=<esx_host> loopbacktest <WWPN>
<Type> <Count> <StopOnError> [Pattern]
```

Parameters

`v`	The vCenter server IP address.
`u`	The user name for the vCenter server.
`p`	The user password for the vCenter server.
`h`	The IP address of the ESXi host.
`WWPN`	The WWPN of a port.
`Type`	The type of loopback test to run: `0` = PCI Loopback Test `1` = Internal Loopback Test `2` = External Loopback Test (requires loopback plug)
`Count`	The number of times to run the test (0 = run test infinitely; Range = 1 to 99,999)
`StopOnError`	Checks if the test must be halted on error. `0` = No halt `1` = Halt
`Pattern` (optional)	1 to 8 hexadecimal bytes to use for loopback data (for example: 1a2b3c4d)

12.3.7.8 posttest

This command runs the POST on a specified FC port.

NOTE: The `posttest` command is available only for LPe12000-series adapters.

Syntax

```
elxvcpcmd.exe v=<vcenter_server> u=<vc_username> p=<vc_password>  h=<esx_host> posttest <WWPN>
```

Parameters

`v`	The vCenter server IP address.
`u`	The user name for the vCenter server.
`p`	The user password for the vCenter server.
`h`	The IP address of the ESXi host.
`WWPN`	The WWPN of the port.

12.3.7.9 setbeacon

This command turns the beacon on or off and sets the beacon's duration.

Syntax

```
elxvcpcmd.exe v=<vcenter_server> u=<vc_username> p=<vc_password>  h=<esx_host> setbeacon <WWPN>
<BeaconState>[BeaconDuration]
```

Parameters

`v`	The vCenter server IP address.
`u`	The user name for the vCenter server.
`p`	The user password for the vCenter server.
`h`	The IP address of the ESXi host.
`WWPN`	The WWPN of a port.
`BeaconState`	New state of the beacon: `0` = Off `1` = On
`BeaconDuration`	(Optional) On supported adapters, specifies the amount of time, in seconds, beaconing is enabled. `0` - `65535` (seconds) `0` = Infinite (default)

12.3.8 Driver Parameter Commands

The Driver Parameter commands show, set, and save driver parameter values. You can also change the parameters back to factory default values.

12.3.8.1 driverconfig

This command sets all driver parameters to the values in the `.dpv` file on a particular ESXi host. The `.dpv` file's driver type must match the driver type of the host platform adapter.

Syntax

```
elxvcpcmd.exe v=<vcenter_server> u=<vc_username> p=<vc_password>  h=<esx_host> driverconfig <WWPN>
<FileName> <Flag>
```

Parameters

`v`	The vCenter server IP address.
`u`	The user name for the vCenter server.
`p`	The user password for the vCenter server.
`h`	The IP address of the ESXi host.
`WWPN`	The WWPN of the port.
`FileName`	The name of the `.dpv` file (stored in the Emulex Repository directory)
`Flag`	`G` = Makes change global (all adapters on this host) `N` = Makes change non-global (adapter-specific)

12.3.8.2 getdriverparams

This command displays the driver parameters of the specified port.

Syntax

```
elxvcpcmd.exe  v=<vcenter server> u=<vc_username> p=<vc_pwd> h=<ESXhostIP> getdriverparams <WWPN>
```

Parameters

v	The vCenter server IP address.
u	The user name for the vCenter server.
p	The user password for the vCenter server.
h	The IP address of the ESXi host.
WWPN	The WWPN of the port.

12.3.8.3 getdriverparamsglobal

This command displays the global driver parameters of the specified port.

Syntax

```
elxvcpcmd.exe  v=<vcenter server> u=<vc_username> p=<vc_pwd> h=<ESXhostIP> getdriverparamsglobal
<WWPN>
```

Parameters

v	The vCenter server IP address.
u	The user name for the vCenter server.
p	The user password for the vCenter server.
h	The IP address of the ESXi host.
WWPN	The WWPN of the port.

12.3.8.4 saveconfig

This command saves the specified adapter's driver parameters to a file on an ESXi host. The resulting file contains a list of driver parameter definitions in ASCII file format with definitions delimited by a comma. Each definition is of the form:

```
<parameter-name>=<parameter-value>
```

The command saves either the values of the global set or the values specific to the adapter in the Emulex Repository directory.

NOTE: Driver parameters that are set temporarily and globally (using the `G` and `T` flags) must be read using the `getdriverparamsel xvcpcmd` command to view the current value of the parameter. The `getdriverparamsglobal elxvcpcmd` command returns only permanently set driver parameter values. Additionally, if temporary, global values have been set for one or more driver parameters, the `saveconfig elxvcpcmd` command must be run with the `N` flag (using the `N` flag is analogous to the `elxvcpcmd` command `getdriverparams`) to force the driver parameter values for the specified adapter to be saved. Inaccurate values can be saved if the `G` flag is used for this command.

Syntax

```
elxvcpcmd.exe v=<vcenter_server> u=<vc_username> p=<vc_password>  h=<esx_host> saveconfig <WWPN>
<FileName> <Flag>
```

Parameters

`v`	The vCenter server IP address.
`u`	The user name for the vCenter server.
`p`	The user password for the vCenter server.
`h`	The IP address of the ESXi host.
`WWPN`	The WWPN of the port.
`FileName`	The name of the local `.dpv` file.
`Flag`	Valid types are: `G` = Make change global (all adapters on this host). `N` = Make change non-global (adapter-specific).

12.3.8.5 setdriverparam

This command sets the driver parameter at the port or global level, either permanently or temporarily, for the specified port.

Syntax

```
elxvcpcmd.exe  v=<vcenter server> u=<vc_username> p=<vc_pwd> h=<ESXhostIP> setdriverparam <WWPN>
<Flag1> <Flag2> <Param> <Value>
```

Parameters

`v`	The vCenter server IP address.
`u`	The user name for the vCenter server.
`p`	The user password for the vCenter server.
`h`	The IP address of the ESXi host.
`WWPN`	The WWPN of a port.
`Flag1`	`L` = Local (all adapters on this host). `G` = Global (all adapters on this host).
`Flag2`	`P` = Permanent (persists across reboot). `T` = Temporary.
`Param`	The name of the driver parameter.
`Value`	The value of the driver parameter.

12.3.8.6 setdriverparamdefaults

This command restores the driver parameter to the default value at the port or global level, either permanently or temporarily, for the specified port.

Syntax

```
elxvcpcmd.exe  v=<vcenter server> u=<vc_username> p=<vc_pwd> h=<ESXhostIP> setdriverparamdefaults
<WWPN> <Flag1> <Flag2>
```

Parameters

`v`	The vCenter server IP address.
`u`	The user name for the vCenter server.
`p`	The user password for the vCenter server.
`h`	The IP address of the ESXi host.
`WWPN`	The WWPN of a port.

`Flag1` `L` = Local (all adapters on this host).
`G` = Global (all adapters on this host).

`Flag2` `P` = Permanent (persists across reboot).
`T` = Temporary.

12.3.9 Firmware Commands

The Firmware commands allow you to update the firmware, view the firmware parameters, and change the firmware parameters on an Emulex adapter or port.

12.3.9.1 firmwareupdate

The `firmwareupdate` command updates firmware on the Emulex adapters found in the specified VMware cluster or the ESXi host. See Section 12.3.5.2, firmwareupdate.

12.3.9.2 getfwparams

The `getfwparams` command displays the available firmware parameters and their ranges for the specified port.

Syntax

```
elxvcpcmd.exe v=<vcenter_server> u=<vc_username> p=<vc_password> h=<esxi_host> getfwparams <WWPN>
```

Parameters

`v`	The vCenter server IP address.
`u`	The user name for the vCenter server.
`p`	The user password for the vCenter server.
`h`	The IP address of the ESXi host.
`WWPN`	The WWPN of the port.

Example

```
elxvcpcmd.exe v=10.192.000.000 u=user p=password h=10.192.87.198
getfwparams 10:00:00:90:fa:f0:93:d6


FW params for 10:00:00:90:fa:f0:93:d6


DX        Param              Low     High     Def       Cur       Dyn
--        ----------------   -----   ------   -------   -------   -------
1         FA-PWWN            0       1        0         1         5
2         FEC                0       1        1         1         1
3         DYNAMIC D-PORT     0       1        0         0         1
```

12.3.9.3 setfwparams

The `setfwparams` command assigns new firmware parameter values to the specified port.

Syntax

```
elxvcpcmd.exe setfwparam <WWPN> <Param Name> <Value>
```

Parameters

`WWPN`	The Word Wide Port Name of FC function on the adapter.
`Param Name`	The name of the parameter that you want to set.
`Value`	The new value of the parameter to be set. Use the `getfwparams` command to see the parameter's range of values. See Section 12.3.9.2, getfwparams, for more information about the `getfwparams` command.

Example

The command `elxvcpcmd.exe  setfwparam 10:00:00:90:FA:F0:93:D6 dynamic-dport 1` would enable the `dynamic-dport` parameter.

12.3.10 Target and LUN Commands

The Target and LUN commands show LUNs attached to the target of the port.

12.3.10.1 getlunlist

This command displays the LUNs attached to a target for the specified port.

Syntax

```
elxvcpcmd.exe  v=<vcenter server> u=<vc_username> p=<vc_password> h=<ESXihostIP> getlunlist <WWPN>
<TargetWWN>
```

Parameters

`v`	The IP address of the vCenter server managing the ESXi host.
`u`	The administrative user name for the vCenter server.
`p`	The user password.
`h`	The IP address of the ESXi host.
`WWPN`	The WWPN of the port connected to the target.
`Target WWPN`	The WWPN of the target.

Example

```
elxvcpcmd.exe v=10.192.000.000 u=user p=password h=10.192.87.198 getlunlist 10:00:00:00:00:87:01:98
20:22:d4:ae:52:6e:6f:08 0
```

12.3.10.2 targetmapping

This command displays the targets attached to the specified port.

Syntax

```
elxvcpcmd.exe  v=<vcenter server> u=<vc_username> p=<vc_pwd> h=<ESXhostIP> targetmapping <WWPN>
```

Parameters

`v`	The vCenter server IP address.
`u`	The user name for the vCenter server.
`p`	The user password for the vCenter server.
`h`	The IP address of the ESXi host.
`WWPN`	The WWPN of the port.

12.3.11 Trunking Commands

The Trunking commands enable you to view and configure trunking.

NOTE:

- Trunking is supported only on LPe35002 and LPe35004 adapters.
- D_Port testing is not available when trunking is enabled.
- FA-PWWN is not available when trunking is enabled.
- Trunking is not supported at 8 Gb/s, and the link will not come up at this speed.
- Before you configure trunking on the Emulex adapter, follow the instructions from Brocade for configuring trunking on the switch.

12.3.11.1 gettrunkinfo

This command displays the trunking configuration for the specified port.

Syntax

```
elxvcpcmd.exe  v=<vcenter server> u=<vc_username> p=<vc_pwd> h=<ESXhostIP> gettrunkinfo <WWPN>
```

Parameters

`v`	The vCenter server IP address.
`u`	The user name for the vCenter server.
`p`	The user password for the vCenter server.
`h`	The IP address of the ESXi host.
`WWPN`	The WWPN of a port.

12.3.11.2 settrunkmode

This command configures trunking for the specified port.

Syntax

```
elxvcpcmd.exe  v=<vcenter server> u=<vc_username> p=<vc_pwd> h=<ESXhostIP> settrunkmode <WWPN>
<trunk mode>
```

Parameters

`v`	The vCenter server IP address.
`u`	The user name for the vCenter server.
`p`	The user password for the vCenter server.
`h`	The IP address of the ESXi host.
`WWPN`	The WWPN of a physical or trunked port.
`trunk mode`	`0` = Disable trunking. `1` = Two-lane trunking. `2` = Four-lane trunking.

12.3.12 Virtual Machine Commands

The Virtual Machines commands list all virtual machines and their information for all manageable ports.

12.3.12.1 listvms

If you specify the host with the `h=<esx_host>` option or just give the physical WWPN, only the virtual machines for that host are shown. If you specify the physical port and the virtual port, only the virtual machine for the specified virtual port returns.

The virtual machine name is displayed only if the virtual port is associated with a virtual machine on VMware ESXi and 5.1. If you are running this command on any other server that has virtual ports, you will not see the virtual machine name.

Syntax

```
elxvcpcmd.exe v=<vcenter_server> u=<vc_username> p=<vc_password>  h=<esx_host> listvms <WWPN>
```

Parameters

`v`	The vCenter server IP address.
`u`	The user name for the vCenter server.
`p`	The user password for the vCenter server.
`h`	The IP address of the ESXi host.
`WWPN`	The WWPN of the port.

12.3.12.2 listvports

This command lists virtual ports on the specified physical port. Leaving the physical WWPN parameter blank lists all virtual ports on all manageable hosts that support virtual ports.

Syntax

```
elxvcpcmd.exe v=<vcenter_server> u=<vc_username> p=<vc_password>  h=<esx_host> listvports [WWPN]
```

Parameters

`v`	The vCenter server IP address.
`u`	The user name for the vCenter server.
`p`	The user password for the vCenter server.
`h`	The IP address of the ESXi host.
`WWPN` (optional)	The WWPN of the port.

12.3.13 WWWN Management Commands

CAUTION! Using the `changewwn` or `restorewwn` commands on an LPe12000-series adapter that is being used to boot from SAN is not advisable. After the command has completed, the system performs an adapter reset, which can cause a loss of connectivity to the SAN and possible loss of data. To perform these commands, you must make sure that the adapter is not currently being used to boot from SAN.

Do one of the following:

- Move the target adapter to a non-boot from SAN host.
- If the host with the target adapter is also hosting other boot from SAN adapters, perform a boot from SAN using one of the other boot from SAN adapters. The target adapter can now be used.

12.3.13.1 changewwn

This command changes the WWN of the specified port.

Syntax

```
elxvcpcmd.exe  v=<vcenter_server> u=<vc_username> p=<vc_pwd> h=<ESXhostIP> changewwn <WWPN> <New_WWPN>
<New_WWNN> <ReadType>
```

Parameters

`v`	The vCenter server IP address.
`u`	The user name for the vCenter server.
`p`	The user password for the vCenter server.
`h`	The IP address of the ESXi host.
`WWPN`	The WWPN of the port.
`New WWPN`	The new WWPN of the port.
`New WWNN`	The new WWNN of the port.
`ReadType`	`0` = Volatile, `1` = Non-volatile.

12.3.13.2 getwwncap

See Section 12.3.2.4, getwwncap.

12.3.13.3 readwwn

This command displays the WWN details of the specified port and category.

Syntax

```
elxvcpcmd.exe v=<vcenter_server> u=<vc_username> p=<vc_pwd> h=<ESXhostIP>
getwwncap <WWPN> [ReadType]
```

Parameters

`v`	The vCenter server IP address.
`u`	The user name for the vCenter server.
`p`	The user password for the vCenter server.
`h`	The IP address of the ESXi host.
`WWPN`	The WWPN of a port.
`ReadType`	Valid types are: `0` = Volatile. `1` = Non-volatile. `2` = Factory default. `3` = Current. `4`= Configured.

12.3.13.4 restorewwn

This command restores the WWN value of the specified port.

Syntax

```
elxvcpcmd.exe  v=<vcenter_server> u=<vc_username> p=<vc_pwd> h=<ESXhostIP> restorewwn <WWPN>
<RestoreType>
```

Parameters

`v`	The vCenter server IP address.
`u`	The user name for the vCenter server.
`p`	The user password for the vCenter server.
`h`	The IP address of the ESXi host.
`WWPN`	The WWPN of a port.
`RestoreType`	Valid types are: `0` = Restore default WWNs. `1` = Restore NVRAM WWNs.

12.4 Viewing Audit Logs Using the CLI Command

You can use the `elxvcpaudit.exe` script to log all historical active management performed through the console on Emulex adapters. To see the usage information, run the script with no parameters specified. All supported events are displayed.

NOTE: All active management actions performed are saved to a log file specific to the action. The maximum size of a log file is 2 MB. If the size of the log file exceeds this limit, old log entries are deleted for the particular event.

Syntax

`elxvcpaudit.exe [event name]`

NOTE: If an event name is not specified, all events are displayed.

Parameter

`event name`	The command name that describes the appropriate active management action performed.

List of Supported Event Names

`changewwn`	WWN change activities.
`download`	Firmware download activities.
`loopbacktest`	Diagnostic tests.
`reset`	Port reset activities.
`setbeacon`	Beacon setting changes.
`setdriverparam`	Driver parameters changes, at both port and global levels.

Example

```
elxvcpaudit.exe changewwn


Audit log  for       : changewwn
--------------------

User Name            : Administrator
Date and Time        : 2011-06-16T19:25:12Z
Operation            : ChangeWWNJobInfo
Host Name            : 10.192.203.179
Adapter Id           : BT11161224
Port Id              : 10:00:00:00:C9:BB:1E:77
Message              : Successfully changed WWN

New State
                     New WWPN = 10:00:00:00:C9:BB:1E:78
                     New WWNN = 20:00:00:00:C9:BB:1E:78
                     Volatile = false

Old State
                     Old WWPN = 10:00:00:00:C9:BB:1E:77
                     Old WWNN = 20:00:00:00:C9:BB:1E:77
```

Appendix A: License Notices

A.1 VI Java SDK

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
* Neither the name of VMware, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.
THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.
IN NO EVENT SHALL VMWARE, INC. OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

BROADCOM®