



Emulex[®] OneCommand[®] Manager for VMware vCenter for LightPulse[®] Adapters

**User Guide
Release 12.0**

Broadcom, the pulse logo, Connecting everything, Avago Technologies, Avago, and the A logo are among the trademarks of Broadcom and/or its affiliates in the United States, certain other countries, and/or the EU.

Copyright © 2011–2018 Broadcom. All Rights Reserved.

The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries. For more information, please visit www.broadcom.com.

Broadcom reserves the right to make changes without further notice to any products or data herein to improve reliability, function, or design. Information furnished by Broadcom is believed to be accurate and reliable. However, Broadcom does not assume any liability arising out of the application or use of this information, nor the application or use of any product or circuit described herein, neither does it convey any license under its patent rights nor the rights of others.

Table of Contents

Chapter 1: Introduction	6
1.1 Compatibility	6
1.2 Abbreviations	7
Chapter 2: Installing and Enabling OneCommand Manager for VMware vCenter	10
2.1 Hardware Requirements	10
2.2 Software Requirements	10
2.3 Installing OneCommand Manager for VMware vCenter	10
2.3.1 Verifying the OneCommand Manager for VMware vCenter Installation	13
2.4 Enabling ESXi Management	14
2.4.1 Requirements	14
2.4.2 Lockdown Mode Feature	15
2.4.3 Enabling OneCommand Manager for VMware vCenter	15
2.5 Enabling and Disabling OneCommand Manager for VMware vCenter with the Plug-in Manager	16
2.6 Registering and Unregistering OneCommand Manager for VMware vCenter	17
2.7 Uninstalling OneCommand Manager for VMware vCenter	17
2.8 Reinstalling OneCommand Manager for VMware vCenter	18
Chapter 3: Using OneCommand Manager for VMware vCenter	20
3.1 Viewing the OneCommand Manager for VMware vCenter	20
3.2 OneCommand Manager for VMware vCenter Window Elements	20
3.2.1 Emulex Device Management Area	22
3.2.2 OneCommand Tabs	22
3.2.3 Information Pane	22
3.2.4 Filter Options Menu	22
3.2.5 Console Tabs	22
Chapter 4: Managing Clusters and Hosts	23
4.1 Managing Clusters	23
4.1.1 Viewing Hosts in a Cluster	23
4.1.2 Viewing Adapters in a Cluster	24
4.1.3 Viewing Physical Ports in a Cluster (Host-Centric Mode)	25
4.1.4 Viewing Virtual Ports in a Cluster (Host-Centric Mode)	27
4.1.5 Viewing Physical Port Information in a Cluster (Fabric-Centric Mode)	28
4.2 Managing Hosts	29
4.2.1 Viewing Host Information for a Single Host	30
4.2.2 Viewing Driver Parameters of All Adapters in a Host	31
4.2.3 Viewing Firmware Information for All Adapters in a Host	32

Chapter 5: Managing Adapters and Ports	34
5.1 Viewing Adapter Information	34
5.1.1 Viewing FC Port Details	35
5.1.2 Viewing Firmware Parameters	37
Chapter 6: Managing Ports	41
6.1 Viewing Port Statistics	41
6.1.1 Viewing PCI Registers	42
6.1.2 Viewing Port Maintenance and Firmware Information	43
6.1.3 Configuring Port Driver Parameters	48
6.1.4 Viewing Port Vital Product Data (VPD)	49
6.1.5 Viewing Port Transceiver Information	50
6.1.6 Viewing Flash Contents for an FC Port	51
6.1.7 Viewing Target Information	52
6.1.8 Viewing LUN Information	52
Chapter 7: Updating Firmware	57
7.1 Updating Firmware for an LPe12000-Series Adapter	57
7.1.1 Updating Firmware on an LPe12000-Series Adapter in a Host	60
7.2 Updating Firmware for LPe16000-Series, LPe31000-Series, and LPe32000-Series Adapters	62
7.2.1 Performing a Batch Firmware Update in Cluster View	63
7.2.2 Updating Firmware on Multiple Adapters in a Host	64
7.2.3 Jobs Window	66
Chapter 8: Exporting SAN Information in Cluster View	68
8.1 Capturing SAN Information in XML or CSV Format	70
8.2 Considerations When Exporting SAN Information in a Cluster View	70
Chapter 9: Diagnostics	71
9.1 Emulex LightPulse Diagnostics	71
9.1.1 Running Loopback Tests	71
9.1.2 Running End to End (ECHO) Tests	72
9.1.3 Running D_Port Tests	73
9.1.4 Using FC Trace Route	76
9.1.5 Running a POST	78
9.1.6 Using Beacons	79
9.1.7 Setting Up Diagnostic Test Options	79
9.1.8 Saving the Log File	79
9.1.9 Creating Diagnostic Dumps	80
9.1.10 Viewing Diagnostic Dump Files	81

Chapter 10: Generating and Installing Secured Certificates	84
10.1 SSL Certificate.....	84
10.1.1 Generating an SSL Certificate	84
10.1.2 Generating a Self-Signed Certificate	84
10.2 Generating a CSR.....	85
10.2.1 Generating a CSR for a Server Using the Java Tool	86
10.2.2 Generating and Validating a CSR.....	86
10.2.3 Getting an SSL Certificate	86
10.2.4 Installing the SSL into the Web Server	87
Chapter 11: Troubleshooting	89
11.1 Security	89
11.1.1 Accepting the Blocked Content.....	89
11.1.2 Installing a Security Certificate.....	90
11.1.3 Issues and Resolutions	91
Chapter 12: Using OneCommand Manager for VMware vCenter Command Line Interface	93
12.1 elxvpcmd Syntax Usage	93
12.2 Help Commands	94
12.2.1 help (Single Command)	94
12.2.2 help (Group).....	94
12.3 CLI Command Reference Tables	94
12.4 Group Commands and CLI Command Descriptions	98
12.4.1 General Group Commands.....	98
12.4.2 Attribute Commands	100
12.4.3 Boot Command	104
12.4.4 Cluster Commands	104
12.4.5 Diagnostic Commands.....	106
12.4.6 Driver Parameter Commands	111
12.4.7 Dump Commands	114
12.4.8 Firmware Commands.....	117
12.4.9 Target and LUN Commands	118
12.4.10 Virtual Machines Commands	122
12.4.11 WWWN Management Commands.....	123
12.5 Viewing Audit Logs Using the CLI Command	124
Appendix A: License Notices	126
A.1 VI Java SDK	126

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 can be hosted and registered on the following servers:

- vCenter Server 6.0
- vCenter Server 6.5
- vCenter Server 6.7

NOTE: The OneCommand Manager application for VMware vCenter GUI is not supported on ESXi 6.7 systems. Use the OneCommand Manager application for VMware vCenter CLI, or the Windows OneCommand Manager application GUI or CLI, or the `esxcli` utility on ESXi 6.7 systems.

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

- Windows 8 x64
- Windows 8.1 x64
- Windows 10
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016

See [Table 1: Support Provided by Emulex CIM Provider Versions](#) to determine the support provided by the CIM Provider.

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

This product supports the following Emulex LightPulse® host bus adapters (HBAs):

- LPe12000-series adapters
- LPe15000-series adapters
- LPe16000-series adapters
- LPe31000-series adapters
- LPe32000-series adapters

[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 Common Information Model (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 v12.0	OneCommand Manager for VMware vCenter v 12.0
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 firmware version	x	x
View 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 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
D_Port (also referred to as ClearLink) test, for LPe16000, LPe31000, and LPe32000-series adapters connected to D_Port-enabled Brocade® switches only	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) test 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
Target and LUN information	x	x
ExpressLane™ priority queuing	x	x
ExpressLane LUN Level Frame Priority	x	x
Reset Port	x	x
View vital product data (VPD)	x	x
Display flash contents (wakeup parameters and flash load list) for ports	x	x
Export storage area network (SAN) configuration information at cluster level and at host level	N/A	x
Perform 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	Blade Open Firmware Management Protocol
CA	certificate authority
CIM	Common Information 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
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
FCoE	Fibre Channel over Ethernet
FPMA	fabric-provided 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	Institution 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	non-volatile 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
PXE	Preboot Execution Environment
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 I/O virtualization
SSL	secure sockets layer
TCP	Transmission Control Protocol
TCP/IP	TCP over Internet Protocol
Tx	Transmit
ULP	Upper Layer Protocol
URL	Uniform Resource Locator
vCSA	VMware for vCenter Server Appliance
VF	virtual function
VLAN	virtual local area network
VLAN ID	VLAN identifier
VM	virtual machine
VMID	virtual machine ID
VPD	vital product data
vPort	virtual port
VM UUID	VM universal unique identifier
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

- VMware ESXi 6.0, 6.5, and 6.7 environments
- Operating system – Windows 8 (64 bit), Windows 10, Windows Server 2012 (64 bit), and Windows Server 2012 R2, and Windows Server 2016
- Adobe Flash Player 11.2 or later
- vCenter Server 6.0, 6.5, and 6.7

NOTE: 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.

- 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.

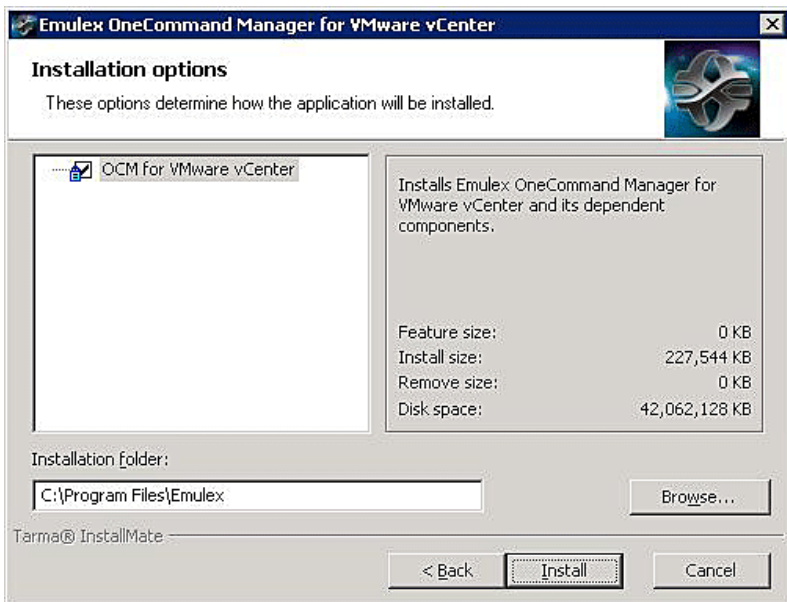
2.3 Installing OneCommand Manager for VMware vCenter

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 for LightPulse Adapters* available on www.broadcom.com.

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

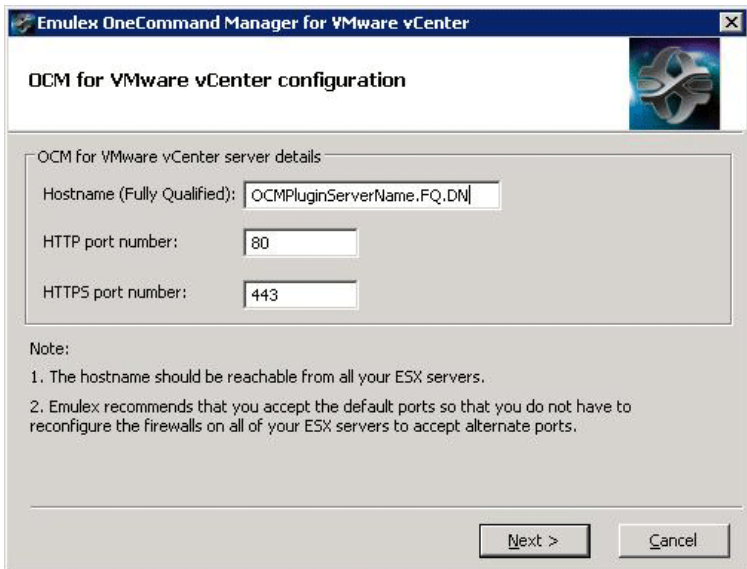
1. Go to www.broadcom.com to download the `ELXOCM-VMware-vCenter-<version>-Setup.exe` installation file to your system.
2. Navigate to the system directory to which you downloaded the file.
3. Double-click **ELXOCM-VMware-vCenter-<version>-Setup.exe**.
The **OneCommand Manager for VMware vCenter** window appears.
4. Click **Next**. The **Installation options** window with the default Installation folder appears ([Figure 1](#)).

Figure 1: Installation Options Window



5. Ensure that the **OCM for VMware vCenter** check box 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** screen appears. When the process is complete, the **OCM for VMware vCenter configuration** window appears (Figure 2).

Figure 2: OCM for VMware vCenter configuration Window

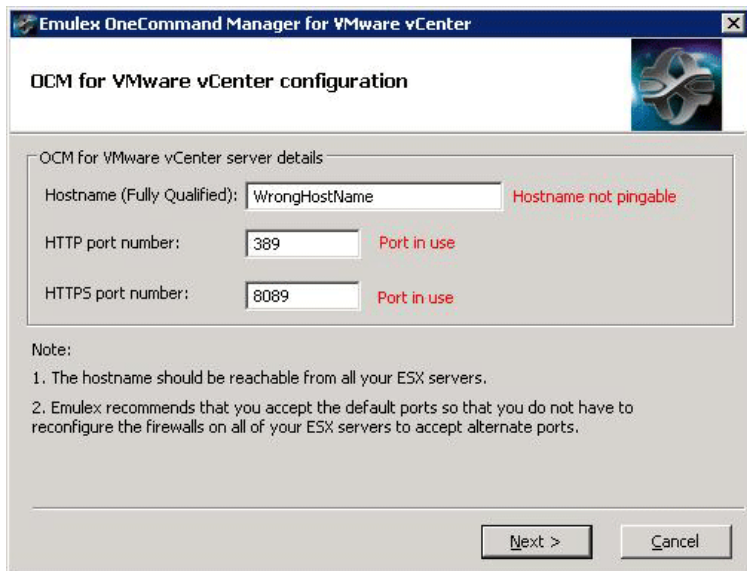


Default port numbers for OneCommand Manager for VMware vCenter Server are displayed.

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 warning appears next to the port number (Figure 3).

Figure 3: OCM for VMware vCenter Configuration Window with Port in use Warning



8. Click **Next**. The **Operation in progress** screen 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 hosting 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.

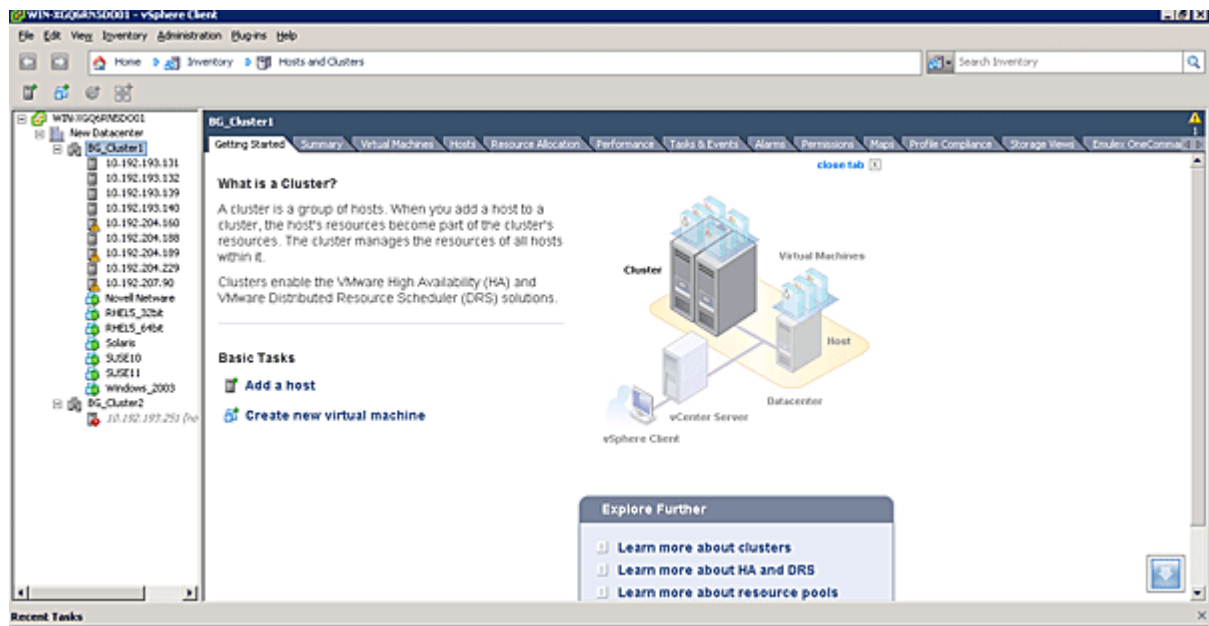
2.3.1 Verifying the OneCommand Manager for VMware vCenter Installation

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.

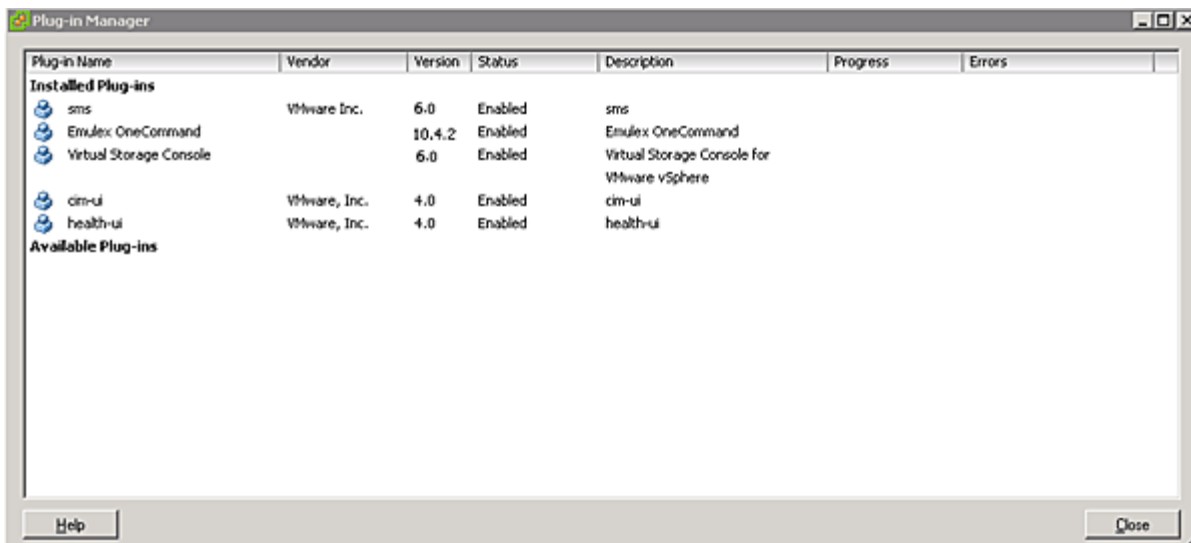
The vCenter Server appears. (Figure 5).

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

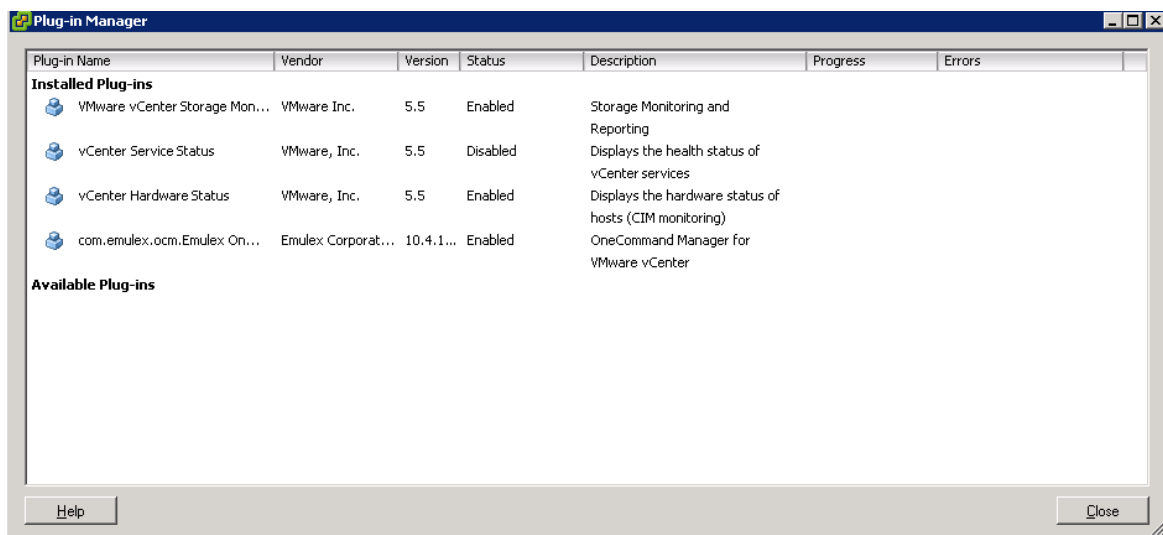
OneCommand Manager for VMware vCenter can be enabled or disabled from the Plug-In Management section.

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.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

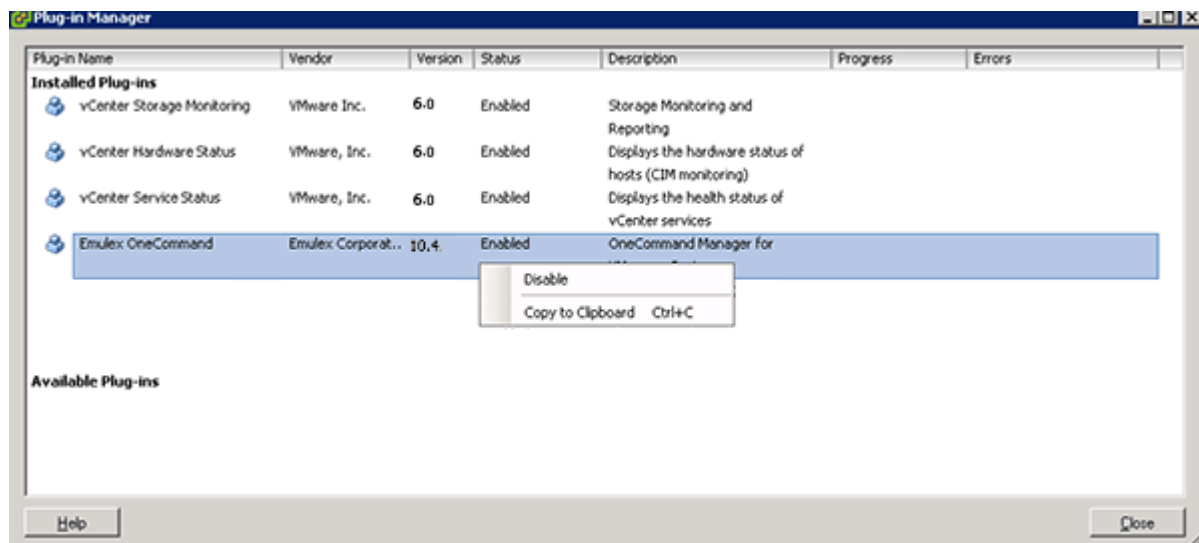
If you enable OneCommand Manager for VMware vCenter, the OneCommand Manager for VMware vCenter functionality immediately appears. If two or more plug-ins are registered, the **Emulex OneCommand** sub-tab (under the **Classic Solutions** tab) immediately appears. If only one plug-in is registered, the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

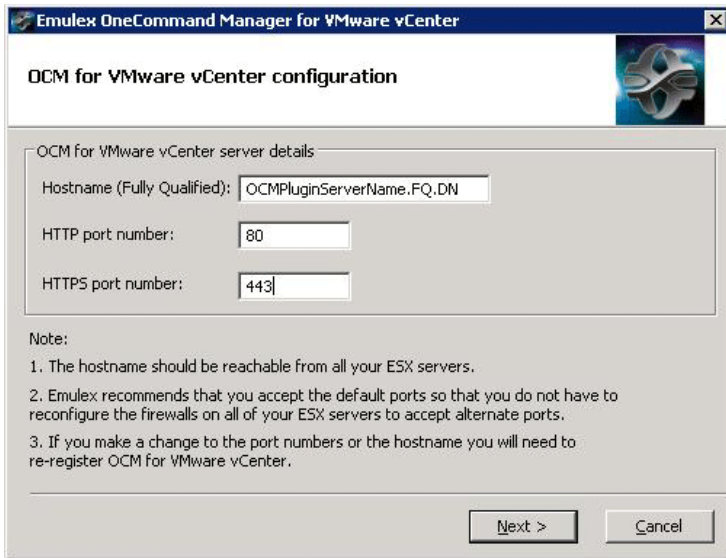
NOTE: You can also uninstall the OneCommand Manager application from the **Programs and Features** window.

2.8 Reinstalling OneCommand Manager for VMware vCenter

To 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 reinstall or uninstall the application.
3. Select **Re-install the application** and click **Next**.
A progress window is displayed. The **OCM for VMware vCenter** window appears.
4. Click **Next**.
The **License agreement** screen appears.
5. Read the agreement and select the **I agree to these terms and conditions** check box.
6. Click **Next**.
The **Installation Options** window with the previous installation folder location appears ([Figure 1](#)).
7. Ensure that the **OCM for VMware vCenter** check box is selected.
8. To change the installation folder location, click **Browse** and navigate to where you want the program files to reside.
9. Click **Install** on the Installation Options window.
The **operation in progress** window appears. When the installation process is complete, the **OneCommand Manager for VMware vCenter configuration** window appears ([Figure 9](#)).

Figure 9: Reinstallation Configuration Dialog



If OneCommand Manager for VMware vCenter was installed earlier with port numbers other than the defaults provided, those configured ports are shown. 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.

10. Follow the on-screen 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 screen, the Recent Tasks panel on the right can be unpinned and collapsed.

3.1 Viewing the OneCommand Manager for VMware vCenter

After you are logged into 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 you want to display.
 - From the Cluster level view, select the cluster you want to display.
4. Go to the **Manage** tab to access the 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

Emulex Device Management Area Filter Options Menu Information Pane Console Buttons

IP Address	Operating System	Drivers	CIM Provider Version	Adapters	Fabrics
10.227.17.46	VMware ESXi 6.0.0 build-2494585	lpfc - 11.2.133.0; HBAAPI(I) v2.3.d, 07-12-10	HBA - 11.2.134.3 UCNA - 11.2.134.3	1	0
10.192.203.18	VMware ESXi 6.0.0 build-2242880	lpfc - 11.2.133.0; HBAAPI(I) v2.3.d, 07-12-10	HBA - 11.2.113.4 UCNA - 11.2.113.4	1	0
10.227.77.108	VMware ESXi 6.0.0 build-2494585	lpnic.o - 11.2.128.0 lpfc - 11.2.148.5; HBAAPI(I) v2.3.d, 07-12-10	HBA - 11.2.148.6 UCNA - 11.2.148.6	1	0

Note:
 Emulex recommends using the latest providers on all managed hosts to expose the full range of supported features.
 Please refer to the supported features section in the user manual to see what features are supported in each provider version.

Figure 11: Host View with Callouts

Emulex Device Information Area OneCommand Tabs Information Panel Console Tabs

Host Name:	dhcp-10-123-179-42	IP Address:	10.123.179.42
Number of Adapters:	2	Number of Ports:	3
Number of Fabrics:	2	Number of Target Ports:	3
Operating System:	VMware ESXi 6.5.0 build-5969303	CIM Provider Version:	HBA - 12.0.181.3 UCNA - 12.0.181.3
Lock Down Mode:	Disabled		

Function Summary

NIC Functions:	0
----------------	---

FC/CoE

FC Functions:	3
FCoE Functions:	0
FC Targets:	3

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 shows information based upon what is selected in the Emulex Device Management area.

In a host view, the information pane shows 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 shows information that is sorted and displayed based upon by the item selected.

3.2.5 Console Tabs

- **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.
- **Preferences** – Click to access the **User Preferences** window. The **User Preferences** window is available in host view only. In the **User Preferences** window, select the **Event Logging** check box to show 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 show these events.
- **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.

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 section 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 belonging 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 shows 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](#).

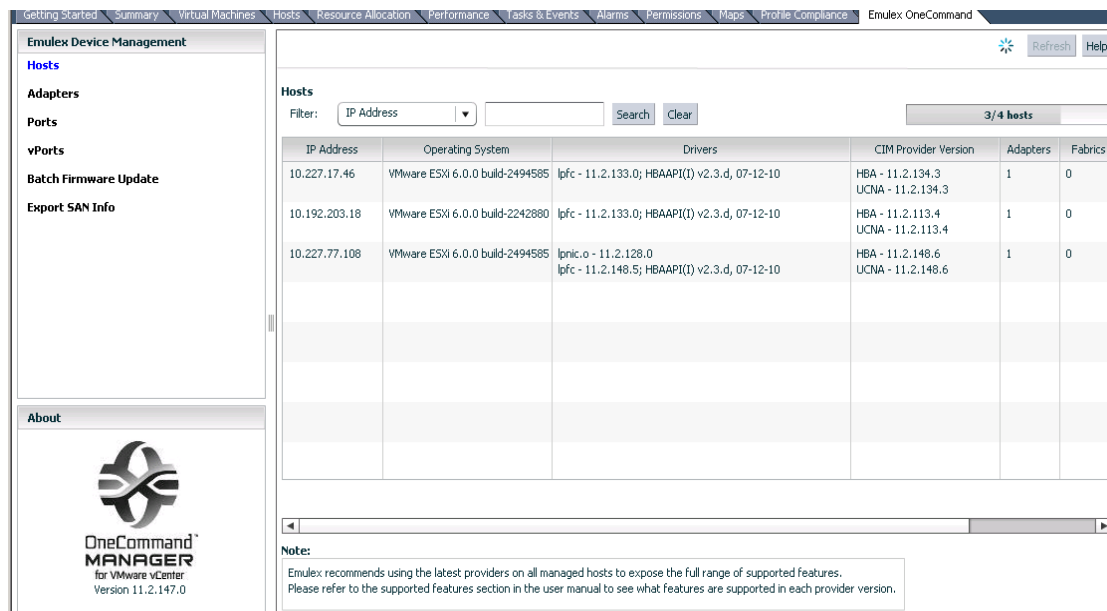
To view information about hosts in a cluster:

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** – Specifies if lockdown mode is enabled or disabled.

4.1.2 Viewing Adapters in a Cluster

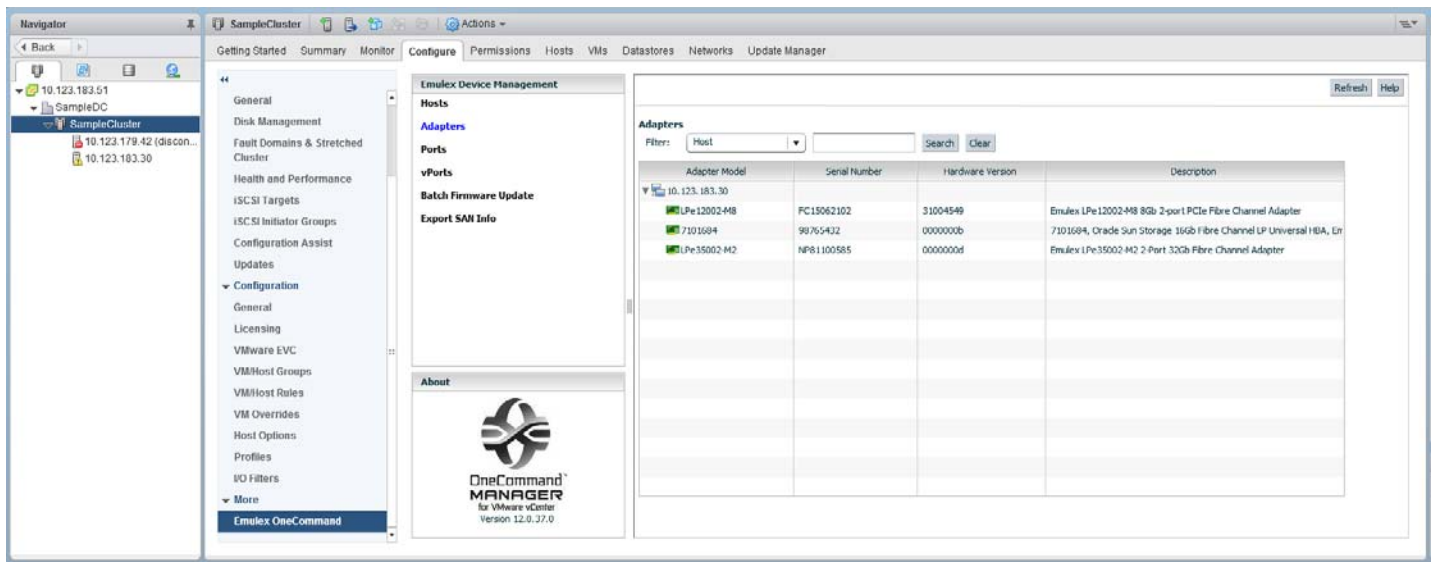
To view information about adapters belonging to a host in a cluster, perform these steps:

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 field are displayed:

- **Adapter Model** – The model of the adapter.
- **Serial Number** – The serial number of the adapter.
- **Hardware Version** – This field shows 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. Hosts 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 the **Group by Fabric** check box is not selected.

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

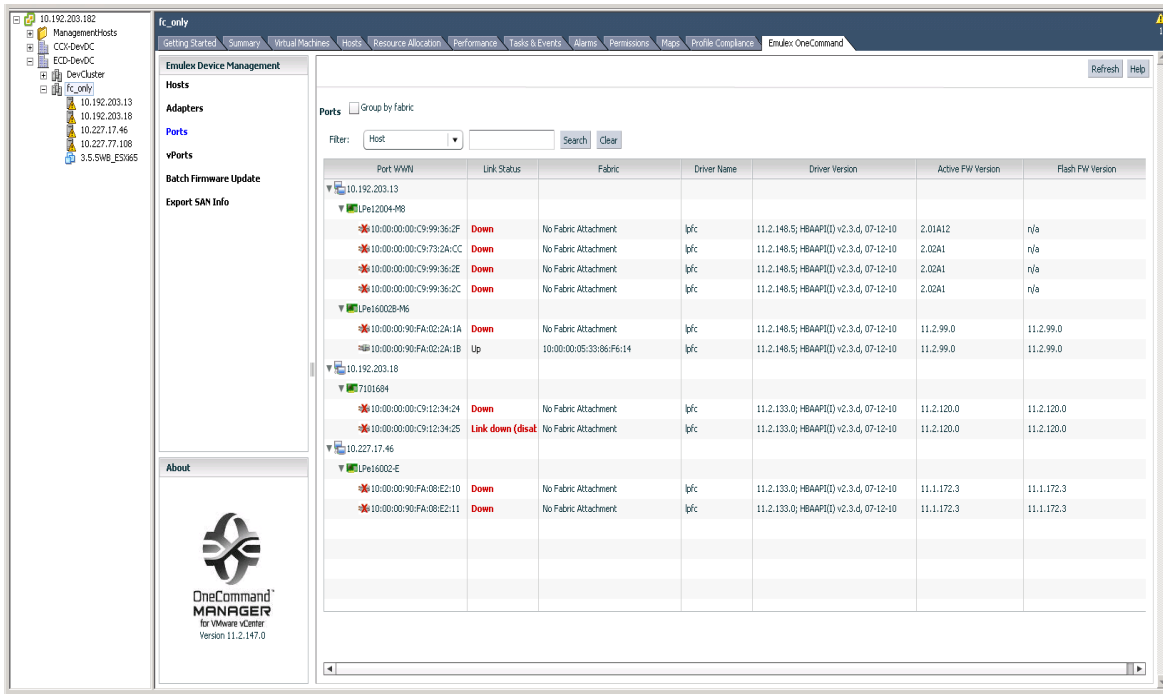
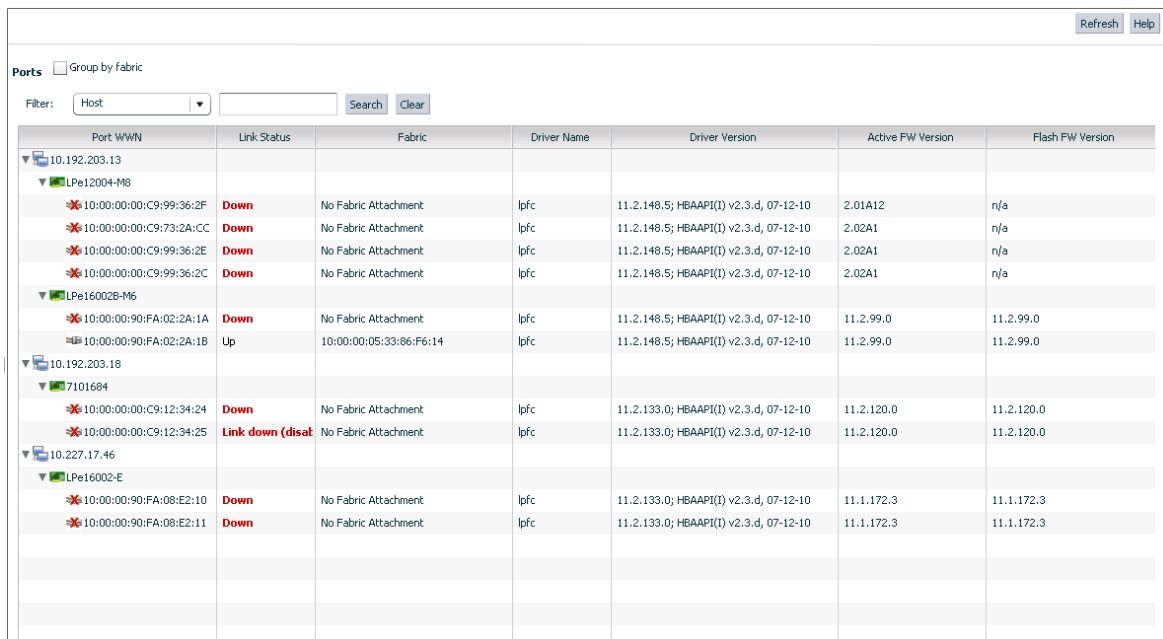


Figure 15: Close-Up of Physical Ports within a Cluster, Host-Centric View



The following physical ports within a cluster, host-centric 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

vPort WWN	vPort Node WWN	vPort FCID	vPort Name	Target Ports	Virtual Machine
20:00:00:00:C9:60:F9:A4	20:00:00:00:C9:60:F9:A4	E001	vPort2 for OCM	0	VirtualMachine2 for OCM
20:00:00:00:C9:60:F9:A5	20:00:00:00:C9:60:F9:A5	E0F1	vPort1 for OCM	0	VirtualMachine1 for OCM

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 the **Group by Fabric** check box. Fabric information is displayed ([Figure 17](#) and [Figure 18](#)).

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

The screenshot displays the Emulex OneCommand Manager interface. On the left, a navigation tree shows the hierarchy: 10.192.203.182 > ManagementHosts > ECD-DevIOC > DevCluster > fc_only. The main content area is titled 'Ports' and has a 'Group by fabric' checkbox checked. Below this, a table lists physical ports with columns for Port WWN, Host, Adapter, Link Status, Driver Name, Driver Version, Active FW Version, and Flash FW. The table shows several ports with 'Down' link status and one port with 'Up' status.

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() 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() 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() 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() v2.3-d, 07-12-10	2.01A12	n/a
10:00:00:90:FA:02:2A:1A	10.192.203.13	Lpe16002B-M6-FC25103043	Down	lpfc	11.2.148.5; HBAAPI() 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() 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 (discal)	lpfc	11.2.133.0; HBAAPI() 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() 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() v2.3-d, 07-12-10	11.1.172.3	11.2.142.0
10:00:00:05:33:96:F6:14							
10:00:00:90:FA:02:2A:1B	10.192.203.13	Lpe16002B-M6-FC25103043	Up	lpfc	11.2.148.5; HBAAPI() v2.3-d, 07-12-10	11.2.99.0	11.2.142.0

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

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 (disal)	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 shows the main elements of the host view.

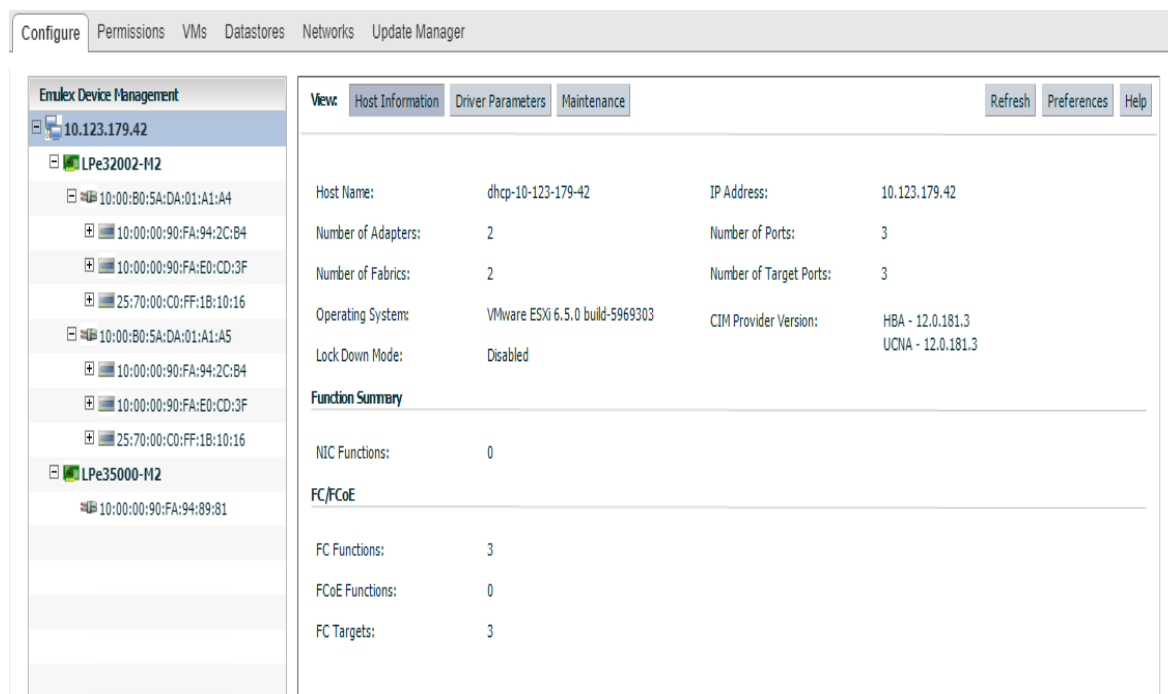
4.2.1 Viewing Host Information for a Single Host

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:
 - **NIC Functions** – N/A
- **FC/FCoE**:

- **FC Functions** – The number of FC functions running on the discovered adapters on this host.
- **FCoE Functions** – N/A
- **FC Targets** – The number of FC targets discovered on the FC or FCoE 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 shows 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 6.1.3, 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

Parameter	Value	Temporary	Range	Default	Activation Requirements	Description
compression-log	300	<input type="checkbox"/>	5-86400	300	None. Parameter is dynamically activated.	Frequency compression logs are written (seconds)
devloss-tmo	10	<input type="checkbox"/>	1-255	10	None. Parameter is dynamically activated.	Seconds driver hold I/O waiting for a loss device to return
discovery-threads	32	<input type="checkbox"/>	1-64	32	Reboot the system.	Maximum number of ELS commands during discovery
enable-SmartSAN	0	<input type="checkbox"/>	0-1	0	Reboot the system.	Enable SmartSAN functionality
enable-qfull	1	<input type="checkbox"/>	0-1	1	None. Parameter is dynamically activated.	Enable driver's SAM_STAT_TASK_SET_FULL handling of lun_queue_depth
fcp-class	3	<input type="checkbox"/>	2-3	3	Reboot the system.	Select Fibre Channel class of service for FCP sequences
fdmi-on	0	<input type="checkbox"/>	0-1	0	Reboot the system.	Enable FDMI support
first-burst-size	0	<input type="checkbox"/>	0-65536	0	None. Parameter is dynamically activated.	First burst size for Targets that support first burst
hba-queue-depth	8192	<input type="checkbox"/>	32-8192	8192	Reboot the system.	Max number of FCP commands queued to a lpfc HBA
log-verbose	0x0	<input type="checkbox"/>	0x0-0x7ffffff	0	None. Parameter is dynamically activated.	Verbose logging bit-mask
lun-queue-depth	30	<input type="checkbox"/>	1-254	30	None. Parameter is dynamically activated.	Max number of FCP commands we can queue to a specific LUN
max-luns	65535	<input type="checkbox"/>	0-65535	65535	Reboot the system.	Maximum allowed LUN
max-scsiopl-time	0	<input type="checkbox"/>	0-60000	0	None. Parameter is dynamically activated.	Use command completion time to control queue depth
max-targets	256	<input type="checkbox"/>	0-4096	256	Reboot the system.	Maximum allowed discovered targets

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 shows 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**.

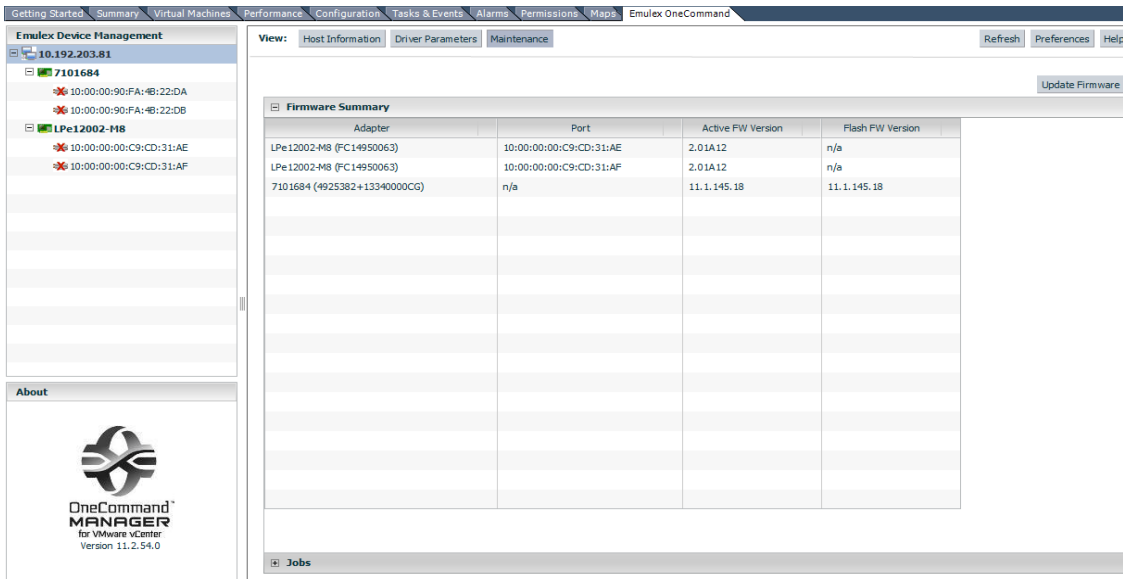
4.2.3 Viewing Firmware Information for All Adapters in a Host

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. Shows **n/a** for ports that are not available.

Chapter 5: Managing Adapters and Ports

This section describes the various adapter and port management functions 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 shows 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** – For Emulex LightPulse adapters, this field shows the JEDEC ID.
- **IPL File Name** – For Emulex LightPulse adapters, this field shows 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.

5.1.1 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.

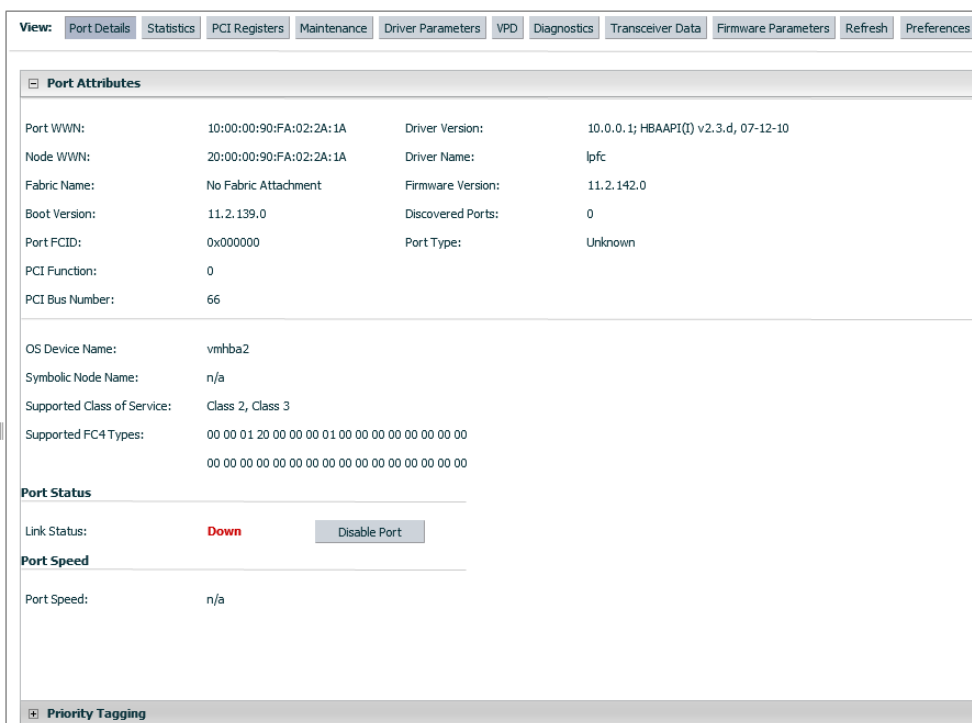
You can also configure virtual machine ID (VMID) when it is supported by the switch.

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 shows **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 5.1.1.1, Enabling and Disabling a Port](#) for more information.
- Port Speed area:
 - **Port Speed** – This field indicates the current port speed of the selected adapter port.

5.1.1.1 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.

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. Select the **Port Details** tab ([Figure 23](#)).
4. Click either **Enable Port** or **Disable Port**.

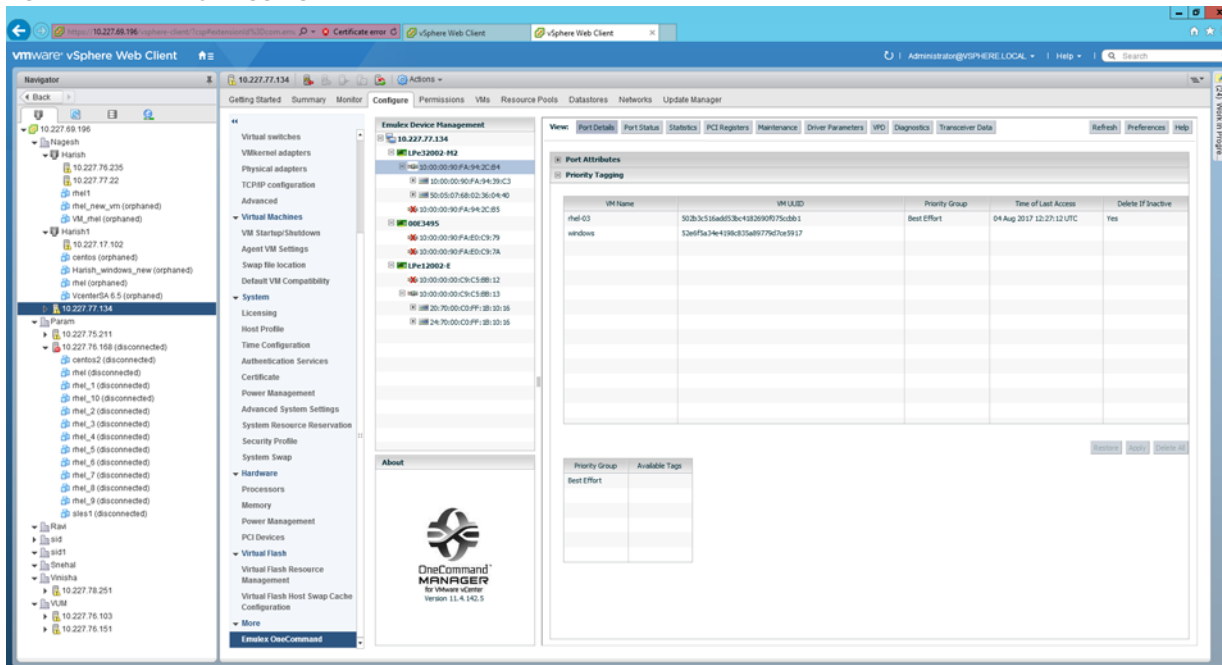
5.1.1.2 Configuring Priority Tagging

The **Priority Tagging** 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** tab, 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 6.1.3, Configuring Port Driver Parameters](#), for additional information.

Figure 24: Priority Tagging Tab



5.1.2 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 only available 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 25).

Figure 25: 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 shown.

- **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.
 - The switch must support FA-PWWN. Refer to the documentation that accompanied the switch for instructions on configuring FA-PWWN on the switch.
 - When a new WWPN is assigned using FA-PWWN, persistently stored configuration information associated with the original WWPN, such as driver parameters and LUN frame priority settings, 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. Enabling Dynamic D-Port allows D-Port tests to be initiated on the switch side. **Disabled** is the default setting.

5.1.2.1 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 that you want to enable or disable.
3. Select the FC **Firmware Parameters** tab (Figure 25).
4. Select a link speed from the **Configured Link Speed** drop-down list.
5. Click **Apply** to set the new link speed. The **Apply** button is only enabled 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 26: Change Link Speed Dialog



6. Click **OK**.
7. Reset the port to activate the new link speed setting. See [6.1.2.2 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..
```

5.1.2.2 Enabling and Disabling FA-PWWN

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

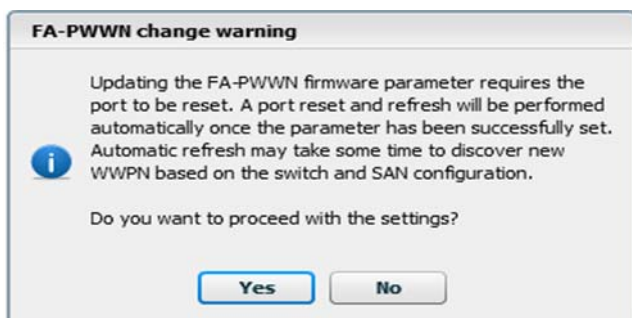
NOTE:

- The switch must support FA-PWWN. Refer to the documentation that accompanied the switch for instructions on configuring FA-PWWN on the switch.
- When a new WWPN is assigned using FA-PWWN, persistently stored configuration information associated with the original WWPN, such as driver parameters and LUN frame priority settings, 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 WWPN. See [Section 6.1.2.1, Changing WWN Configuration](#), for information about changing WWN configuration.

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

1. Select the **FC Firmware Parameters** tab ([Figure 25](#)).
2. Select **Enable** or **Disable** from the **FA-PWWN** drop-down list.
3. Click **Apply**. The **FA-PWWN change warning** dialog appears ([Figure 27](#)).
4. Click **Yes**.

Figure 27: FA-PWWN change warning Dialog



5. 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.

5.1.2.3 Enabling and Disabling Dynamic D_Port

When enabled, Dynamic D_Port allows D_Port tests to be initiated on the switch side.

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 9.1.3, Running D_Port Tests](#), for information about running D_Port tests from the adapter.

To enable or disable Dynamic D_Port, perform these steps:

1. Select the FC **Firmware Parameters** tab ([Figure 25](#)).
2. Select **Enable** or **Disable** from the **Dynamic D-Port** drop-down list.
3. Click **Apply**.
4. A dialog appears notifying you that the parameter was successfully updated. Click **OK**.

Chapter 6: Managing Ports

This section pertains to managing ports.

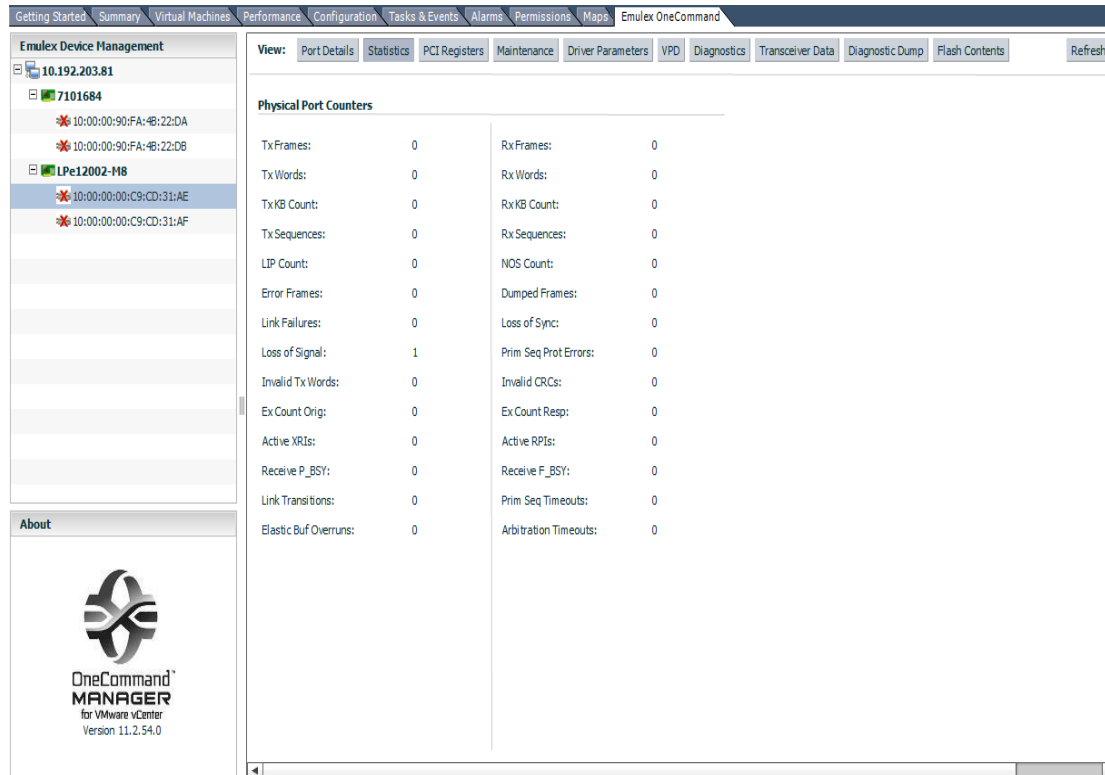
6.1 Viewing Port Statistics

When you select a port from the discovery-tree, the **Port Statistics** tab shows 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 28).

Figure 28: Port Statistics Tab



The screenshot displays the Emulex OneCommand Manager interface. The left sidebar shows a tree view with the host '10.192.203.81' expanded, and the device 'LPe12002-M8' selected. The main content area shows the 'Statistics' tab for the selected port. The 'Physical Port Counters' section displays the following data:

Counter	Value	Counter	Value
Tx Frames:	0	Rx Frames:	0
Tx Words:	0	Rx Words:	0
Tx KB Count:	0	Rx KB Count:	0
Tx Sequences:	0	Rx Sequences:	0
LIP Count:	0	NOS Count:	0
Error Frames:	0	Dumped Frames:	0
Link Failures:	0	Loss of Sync:	0
Loss of Signal:	1	Prim Seq Prot Errors:	0
Invalid Tx Words:	0	Invalid CRCs:	0
Ex Count Orig:	0	Ex Count Resp:	0
Active XRLs:	0	Active RPLs:	0
Receive P_BSY:	0	Receive F_BSY:	0
Link Transitions:	0	Prim Seq Timeouts:	0
Elastic Buf Overruns:	0	Arbitration Timeouts:	0

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.
- **Primitive Seq Timeouts** – The number of times a primitive sequence event timed out.
- **Arbitration Timeouts** – The number of times the arbitration loop has timed out. Large counts could indicate a malfunction somewhere in the loop or heavy usage of the loop.

6.1.1 Viewing PCI Registers

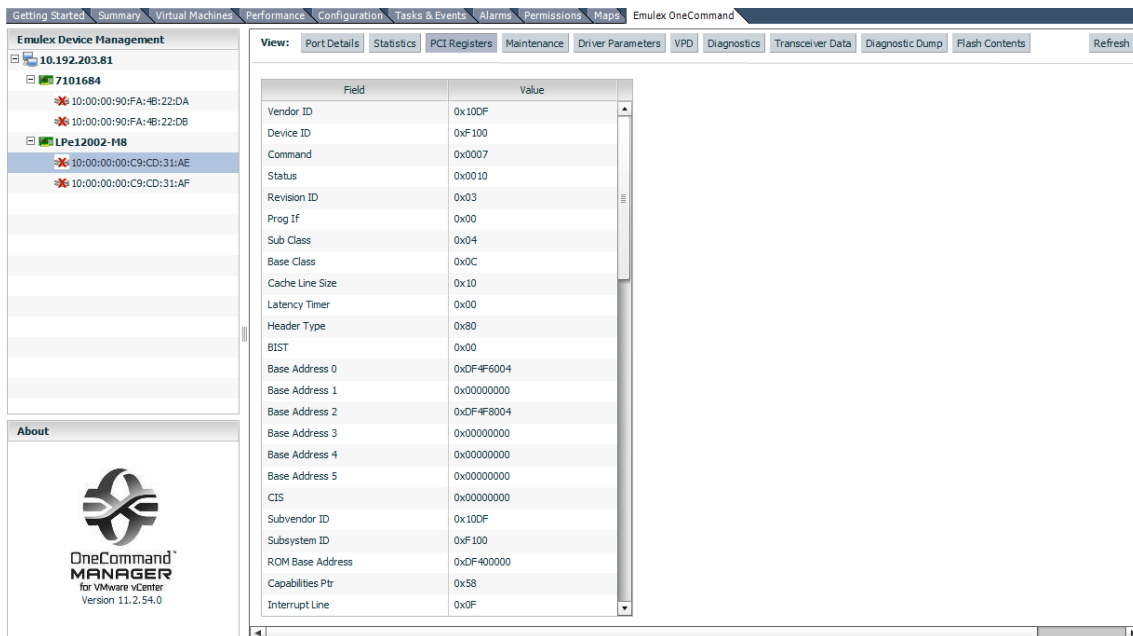
The **PCI Registers** tab shows PCI information, including PCIe details, about the selected port.

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 29](#)).

Figure 29: Port PCI Registers Tab



6.1.2 Viewing Port Maintenance and Firmware Information

The **Maintenance** tab shows 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 30](#)) or a port on any other LightPulse adapter port ([Figure 31](#)).

Figure 30: Maintenance Tab for a Port on an LPe12000-Series Adapter

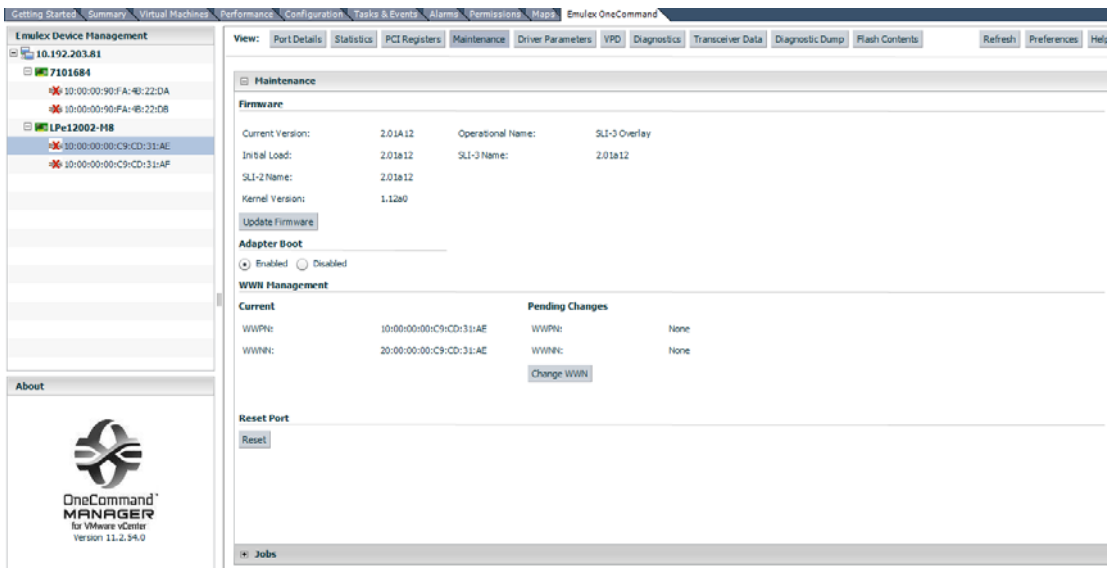
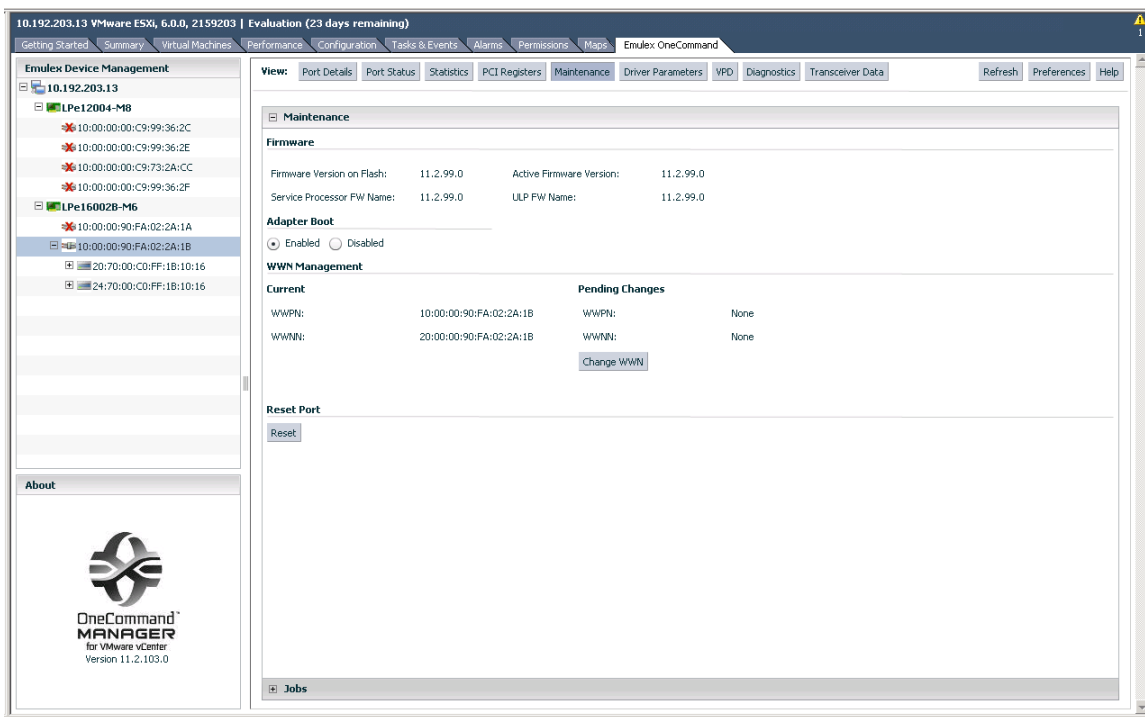


Figure 31: Port Maintenance Tab for a Port on Other LightPulse Adapters



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 6.1.2.1, Changing WWN Configuration](#), for more information about changing the WWN configuration.

For instructions on resetting a port, see [Section 6.1.2.2, Resetting a Port](#), for more information.

6.1.2.1 Changing 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.

6.1.2.1.1 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 show **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 5.1.2.2, 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 30](#)).
4. Click **Change WWN**. The **Change WWN Configuration** dialog is displayed ([Figure 32](#)).

Figure 32: Change WWN Configuration Dialog

Change WWN Configuration

Update the world wide port name (WWPN) and the world wide node name (WWNN) below and click OK to save changes.

To use the factory default WWNs or to use non-volatile WWNs, click the appropriate "Get" button.

NOTE:

- 1) If the current WWNs are of type volatile, a successful non-volatile change will destroy the volatile settings.
- 2) Depending on the adapter type and the firmware version, volatile change option may not be available.
- 3) Depending on the type of the WWN change and the current state of the firmware, applying more changes without activating the pending changes may result in errors.
- 4) Volatile WWNs are preserved across reboots until system power-down or adapter power-cycle.

New WWPN: 10 00 00 00 C9 99 0A 3B

New WWNN: 20 00 00 00 C9 99 0A 3B

Write changes to volatile memory for temporary use

Get Factory Default WWNs Get Non-Volatile WWNs

Clear Ok Cancel

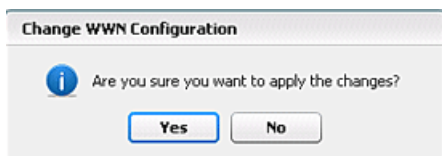
5. Do one of the following:
 - Enter a new WWPN or WWNN.
 - Click **Get Factory Default WWNs** to load the settings that were assigned when the adapter was manufactured. These values can then be modified and saved as volatile or non-volatile WWNs.

- 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, the **Write changes to volatile memory for temporary use** check box is not selected. This type of change is supported locally and using TCP/IP connections. This check box is not available for remote in-band adapters, regardless of adapter models and firmware version.

7. Click **OK**. The following warning is displayed ([Figure 33](#)).

Figure 33: Change WWN Configuration Warning



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.

6.1.2.2 Resetting a Port

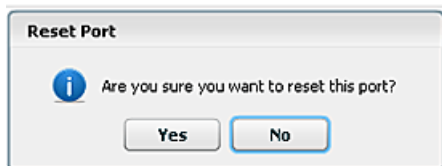
CAUTION! Do not reset an adapter port while copying or writing files. This action could result in data loss or corruption.

NOTE: When you reset a port or change 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 ([Figure 30](#)) for LPe12000-series adapter ports or [Figure 31](#) for other LightPulse adapter ports.
4. Click **Reset**. The following warning is displayed ([Figure 34](#)).

Figure 34: Reset Port Warning



- 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.

6.1.3 Configuring Port Driver Parameters

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

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

- Select a host in the console tree-view, and if applicable, select the **Emulex OneCommand** tab.
- In the Emulex Device Management tree-view, select the port whose driver parameters you want to view.
- Select the **Driver Parameters** tab (Figure 35).

Figure 35: Port Driver Parameters Tab

Parameter	Value	Temporary	Range	Default	Activation Requirements	Description
ad5	Disabled	<input type="checkbox"/>	-	Disabled	Reboot the system.	Enable ACIO support
device-time	10	<input type="checkbox"/>	1-255	10	The parameter is currently not settable on a per adapter basis.	Seconds driver hold [0] waiting for a loss device to return
discovery-threads	32	<input type="checkbox"/>	1-64	32	Reboot the system.	Maximum number of ELS commands during discovery
enable-npiv	Enabled	<input type="checkbox"/>	-	Enabled	Reboot the system.	Enable NPiv functionality.
enable-npiv	0	<input type="checkbox"/>	0-1	0	Reboot the system.	Enable NPiv functionality.
fcf-falover-policy	1	<input type="checkbox"/>	1-2	1	Reboot the system.	FCF Fast falover=1 Priority falover=2
fcq-class	3	<input type="checkbox"/>	2-3	3	Reboot the system.	Select Fibre Channel class of service for FCF sequences
fdm-on	0	<input type="checkbox"/>	0-2	0	Reboot the system.	Enable FDM support
hba-queue-depth	2048	<input type="checkbox"/>	32-8192	8192	Reboot the system.	Max number of FCF commands we can queue to a lport HBA
link-speed	Auto Detect	<input type="checkbox"/>	0-8	Auto Detect	Reboot the system.	Select link speed: [2 4 8] or 0 for auto negotiate
log-verbose	0x5	<input type="checkbox"/>	0x0-0xffffffff	0	The parameter is currently not settable on a per adapter basis.	Verbose logging bit-mask
lun-queue-depth	30	<input type="checkbox"/>	1-128	30	None. Parameter is dynamically activated.	Max number of FCF commands we can queue to a specific LUN
max-ioctl-time	0	<input type="checkbox"/>	0-60000	0	The parameter is currently not settable on a per adapter basis.	Use command completion time to control queue depth
scan-down	Enabled	<input type="checkbox"/>	-	Enabled	Reboot the system.	Start scanning for devices from highest ALPA to lowest
scg-seg-cnt	64	<input type="checkbox"/>	64-256	64	Reboot the system.	Max Scatter Gather Segment Count
tgt-queue-depth	8192	<input type="checkbox"/>	10-8192	8192	Reboot the system.	Max number of FCF commands we can queue to a specific target port
topology	Auto (loop first)	<input type="checkbox"/>	0-6	Auto (loop first)	Reboot the system.	Select Fibre Channel topology: valid values are 0,1,2,4,6. See driver manual
use-adisc	Disabled	<input type="checkbox"/>	-	Disabled	The parameter is currently not settable on a per adapter basis.	Use ADISC on rediscovery to authenticate FCF devices

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 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:

- Select a host in the console tree-view. If applicable, select the **Emulex OneCommand** tab.
- 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 35).
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 the **Temporary** check box. 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 the **Make all changes temporary** check box. This setting overrides the setting of the **Make change temporary** check box. 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 35).
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.

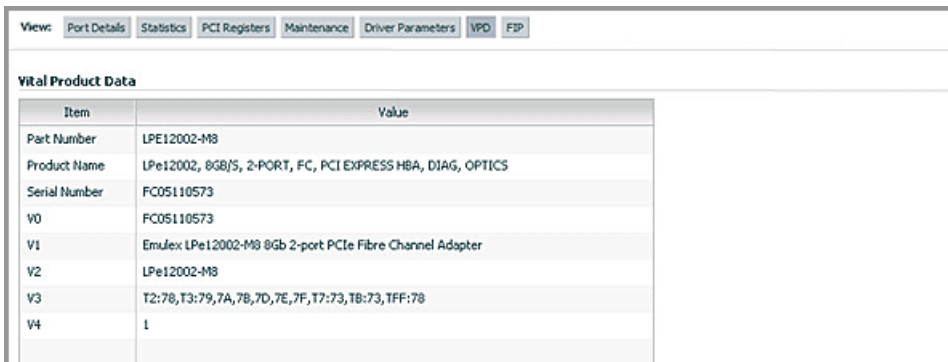
6.1.4 Viewing Port Vital Product Data (VPD)

The **VPD** tab shows 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 36).

Figure 36: Port 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	T2:76,T3:79,7A,7B,7D,7E,7F,T7:73,TB:73,TF: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 Vx (where x is a number).

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

6.1.5 Viewing Port Transceiver Information

The **Transceiver Data** tab shows 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 37).

Figure 37: Port Transceiver Data Tab

View: Physical Port Info Diagnostics DCB Transceiver Data			
Module Attributes			
Vendor:	FINISAR CORP.	OUI:	00-90-65
Identifier/Type:	3h	Date:	01/01/1970
Ext. Identifier:	4h	Serial Number:	AM70PDV
Connector:	7h	Part Number:	FTLX8571D3BCL-EM
Wavelength:	850nm	Revision:	A
Diagnostic Data			
Temperature:	39.56 °C		
Supply Voltage:	3.32 V		
Tx Bias Current:	8.21 mA		
Tx Output Power:	0.58 mW		
Rx Input Power:	0.57 mW		

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.

6.1.6 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 38](#)).

Figure 38: FC Port Flash Contents

Program Type	Revision	Description	Program ID	Start Address	Length	Next Entry	Previous Entry	Wake-Up Image
Test Program	1.00#4	NPort0 Loopback	Not Available	00094004	00002C70	00015774	00015774	No
Functional Firmware	2.01a7	USC-01A7	Not Available	0009797C	00001720	00015794	00015794	Yes
SLI-2 Overlay	2.01a7	U002.01A7	Not Available	0009909C	00002320	00015700	00015774	Yes
SLI-3 Overlay	2.01a7	U002.01A7	Not Available	0008C208	00031A04	00015790	00015794	Yes

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

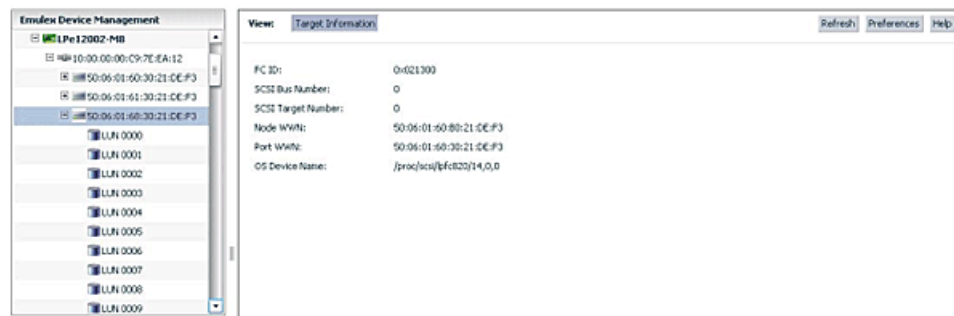
6.1.7 Viewing Target Information

When you select a port target associated with an adapter from the Emulex Device Management tree-view, the **Target Information** tab shows 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 39).

Figure 39: 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.

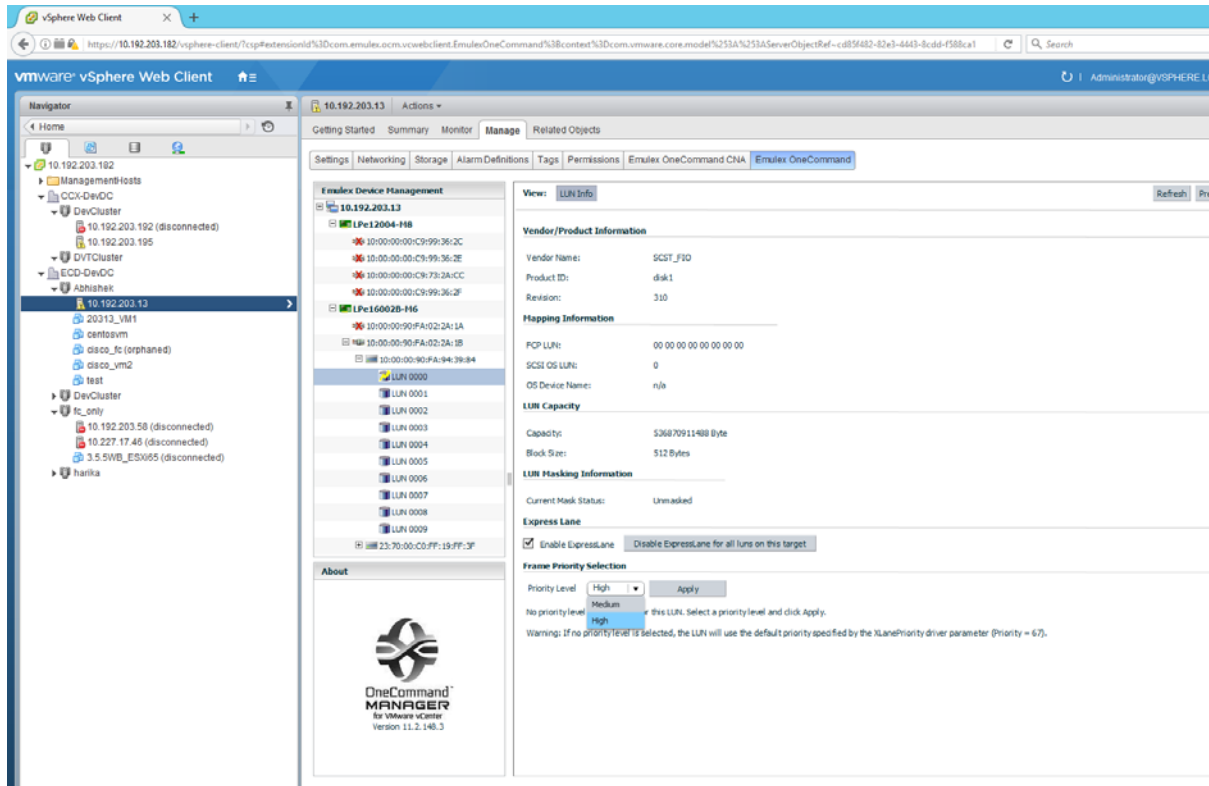
6.1.8 Viewing LUN Information

When you select a LUN associated with an adapter from the Emulex Device Management tree-view, the LUN Info pane shows 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 40**).

Figure 40: LUN Info Tab (ExpressLane LUN with Frame Priority Selection Supported)



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 only provided 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.
- ExpressLane area (Only appears if supported by the adapter):
 - **Enable ExpressLane** – Select this check box to create an ExpressLane LUN.
 - **Priority Level** – When ExpressLane is enabled, you can assign the frame priority to the ExpressLane LUN.

- **Disable ExpressLane on all LUNs** button – Clicking this button disables ExpressLane on all ExpressLane LUNs.
- **Apply** button - Clicking this button saves your ExpressLane changes.


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

6.1.8.1 Enabling an Optimized Access Storage (ExpressLane) LUN

Enabling an ExpressLane LUN is supported only for the LPe16000-series, LPe31000-series, and LPe32000-series adapters.

NOTE:

- An ExpressLane LUN must be enabled in the driver before it can be used by the OneCommand Manager for VMware vCenter. Additionally, the priority value to mark each of the ExpressLane frames must be specified to the FC driver through new driver parameters.
- ExpressLane is not supported for LUNs attached to virtual ports.
- Masked LUNs cannot be ExpressLane enabled because they are not presented to the host. Conversely, ExpressLane LUNs cannot be masked.

In host view, the **ExpressLane LUN** icon  is displayed in the Emulex Device Management area and represents a LUN with ExpressLane priority queuing enabled.

If your system contains flash and rotational storage I/O on the same initiator port, the improved performance of the flash storage can be hindered by the slower rotational storage I/O performance. Because both are sharing the same queue, rotational storage I/O requests queued up in front of flash storage I/O requests can prevent the performance gains of flash storage I/O (that is, head of line blocking).

To prevent this situation, you can create a separate priority queue in the driver to process the requests ahead of the normal queue. Additionally, the I/O frames placed on this queue can be marked with a priority so that the switch and target also prioritizes the flash I/O requests. By indicating to the FC driver which LUNs receive this special priority queuing (for example, ExpressLane LUNs), performance on these LUNs can be greatly improved. Even if only FC flash storage is available on your system, there can be LUNs that you want to run I/O with a higher priority than other LUNs.

To enable an ExpressLane LUN, perform these steps:

1. Select a host in the console tree-view. If applicable, select the **Emulex OneCommand** tab.
2. From the discovery-tree, select a LUN under the adapter on which you want to enable ExpressLane. The **LUN Information** tab appears ([Figure 40](#)).
3. Select the **Enable ExpressLane** check box.

The LUN icon in the discovery-tree changes to the **ExpressLane LUN** icon .

NOTE: The ExpressLane state of a LUN is enabled at the driver (active) level and the configured level (persists across reboots).

To disable an ExpressLane LUN, perform these steps:

1. Select a host in the console tree-view. If applicable, select the **Emulex OneCommand** tab.
2. From the discovery-tree, select a LUN under the adapter on which you want to disable ExpressLane. The **LUN Information** tab appears ([Figure 40](#)).
3. Clear the **Enable ExpressLane** check box to disable the selected LUN.

To disable all ExpressLane LUNs, perform these steps:

1. Select a host in the console tree-view. If applicable, select the **Emulex OneCommand** tab.
2. From the discovery-tree, select a LUN under the adapter on which you want to disable ExpressLane. The **LUN Information** tab appears (Figure 40).
3. Click **Disable ExpressLane for all LUNs on this target**.
4. A dialog appears warning you that you are about to delete all ExpressLane LUNs on this target. Click **OK**. All **ExpressLane LUN** icons in the discovery-tree (for the selected adapter port) will change to the regular **LUN** icon and any assigned frame priority is removed.

6.1.8.2 Selecting a Frame Priority

If the adapter and switch support it, you can assign a frame priority to the ExpressLane LUN. Switches can provide up to three priority levels, **Low**, **Medium**, and **High**, but they might provide fewer options.

To select a frame priority, perform these steps:

NOTE: The `EnableXLane` driver parameter must be enabled on the **Driver Parameters** tab to set frame priorities.

1. Select a host in the console tree-view. If applicable, select the **Emulex OneCommand** tab.
2. From the discovery-tree, select a LUN under the adapter on which you want to enable ExpressLane. The **LUN Information** tab appears (Figure 40).
3. Select the **Enable ExpressLane** check box if it is not already checked. The **LUN** icon in the discovery-tree changes to the **ExpressLane LUN** icon.
4. Select a frame priority from the **Priority Level** pull-down menu.

NOTE: If the switch connected to the initiator does not support LUN specific frame priority levels using the Get Fabric Object (GFO), you must manually enter the frame priority values in the range of 0–127 for all ExpressLane enabled LUNs as depicted in Figure 41.

Figure 41: LUN Information Tab

The screenshot displays the Emulex OneCommand Manager interface. The top navigation bar includes 'Getting Started', 'Summary', 'Monitor', 'Configure', 'Permissions', 'VMs', 'Datastores', 'Networks', and 'Update Manager'. The left sidebar shows a tree view with categories like Storage, Networking, Virtual Machines, and System. The main content area is divided into three sections: 'Emulex Device Management', 'About', and 'LUN Info'. The 'Emulex Device Management' section shows a list of devices, with 'LUN 0000' selected. The 'About' section displays the OneCommand Manager logo and version information (Version 12.0.37.0). The 'LUN Info' section provides detailed information about the selected LUN, including Vendor/Product Information, Mapping Information, LUN Capacity, LUN Masking Information, Express Lane settings, and Frame Priority Selection.

Emulex Device Management

- 10.123.183.30
 - LPe12002-M8
 - 10:00:00:00:C9:CD:AB:06
 - 10:00:00:00:C9:CD:AB:07
 - 7101684
 - 10:00:00:00:C9:00:34:56
 - 10:00:00:00:C9:00:34:57
 - LPe35002-M2
 - 10:00:00:90:FA:94:89:05
 - 50:05:07:68:02:26:04:40
 - LUN 0000**
 - 10:00:00:90:FA:94:89:01

View: LUN Info Refresh Preferences Help

Vendor/Product Information

Vendor Name:	IBM
Product ID:	2145
Revision:	0000

Mapping Information

FCP LUN:	00 00 00 00 00 00 00 00
SCSI OS LUN:	0
OS Device Name:	n/a

LUN Capacity

Capacity:	32212254208 Byte
Block Size:	512 Bytes

LUN Masking Information

Current Mask Status:	Unmasked
----------------------	----------

Express Lane

Enable ExpressLane Disable ExpressLane for all luns on this target

Frame Priority Selection

Priority Level: High Apply

No priority level has been set for this LUN. Select a priority level and click Apply.

Warning: If no priority level is selected, the LUN will use the default priority specified by the xLanePriority driver parameter (Priority = 67).

5. Click **Apply**.

If there were problems assigning the frame priority, the **LUN Information** tab displays a message with a suggested solution.

Chapter 7: Updating Firmware

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

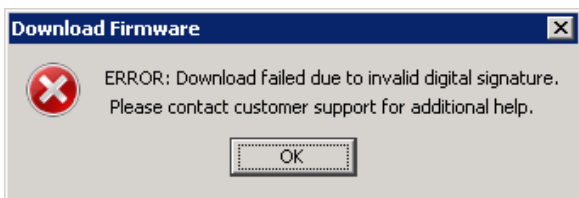
The submitted firmware update job can be tracked in the VMware tasks window.

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.

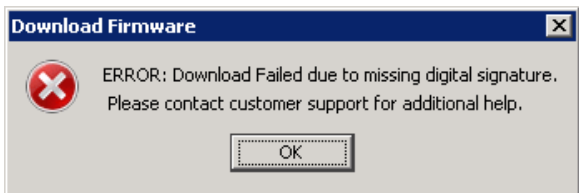
The firmware update progresses in the background until all the jobs are completed. During this period, you can still browse through the other tabs. However, if you start a firmware update and log out from the console before the firmware update is completed, all pending jobs fail.

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 LPe16000-series, LPe31000-series, or LPe32000-series adapter, the following error message will be displayed.



If you attempt to update unsecured firmware for a secure LPe16000-series, LPe31000-series, or LPe32000-series adapter, the following error message will be displayed.



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.

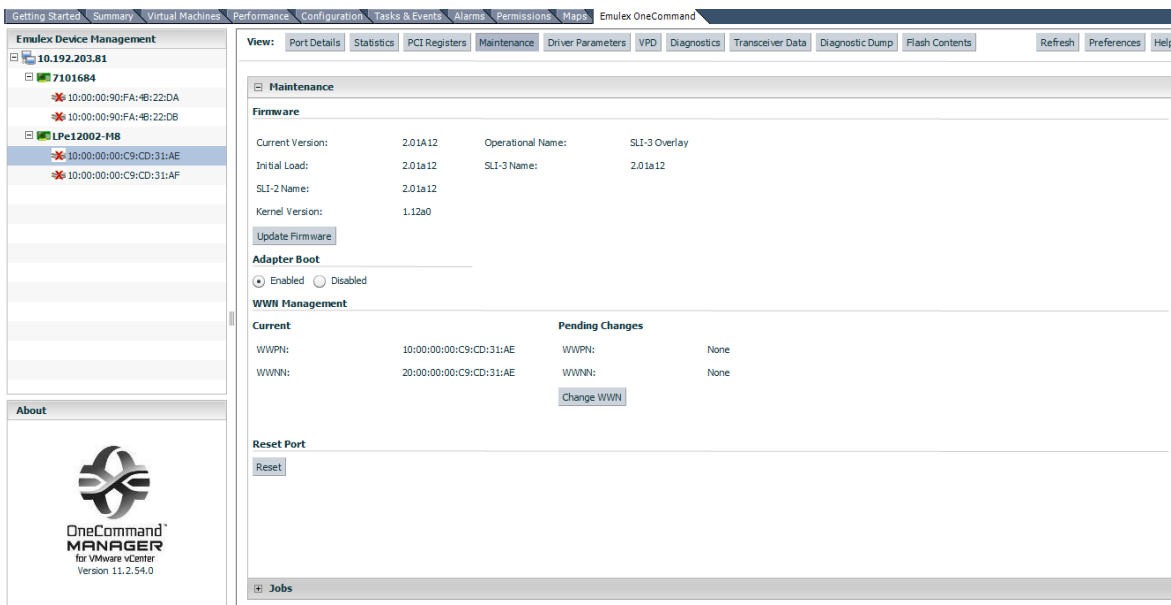
Do one of the following:

- 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:

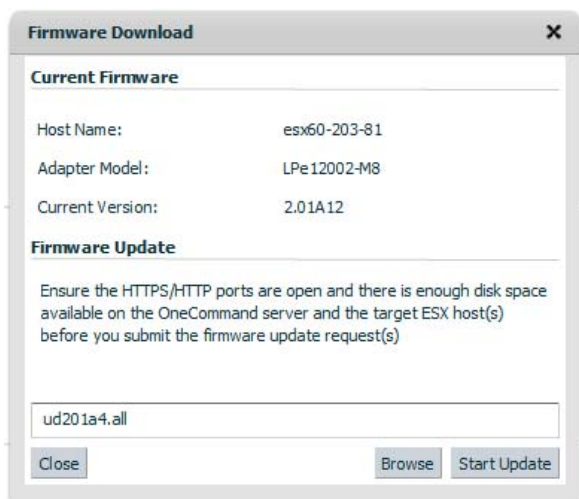
1. Select a host in the console tree-view; and, if applicable, select the **Emulex OneCommand** tab (Figure 5).
2. In the Emulex Device Management tree-view, select LPe12000-series adapter port for which you want to update firmware.
3. Select the **Maintenance** tab (Figure 42).

Figure 42: Maintenance Tab



4. Click **Update Firmware**. If a warning screen appears, click **Yes**. The **Firmware Download** dialog is displayed (Figure 43).

Figure 43: Firmware Download Dialog



5. Click **Browse** and navigate to the unzipped, extracted image file 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 44](#))

Figure 44: Jobs Window

Active Jobs							
User	Host	Adapter	Port	StartTime	Status Message	Cancel	

Completed Jobs							
User	Host	Adapter	Port	StartTime	EndTime	Status Message	
VSPHERE.LOCAL\Admini:	10.227.17.46	LPe16002-E	10:00:00:90:FA:08:E2:11	08 Nov 2016 19:21	08 Nov 2016 19:24	Successfully completed. Reboot required for changes to take effect.	
VSPHERE.LOCAL\Admini:	10.192.203.13	LPe16002B-M6	10:00:00:90:FA:02:2A:1B	08 Nov 2016 19:21	08 Nov 2016 19:25	Successfully completed.	

A status message in the Active Job list shows 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** field in the Completed Jobs list shows 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 logout 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

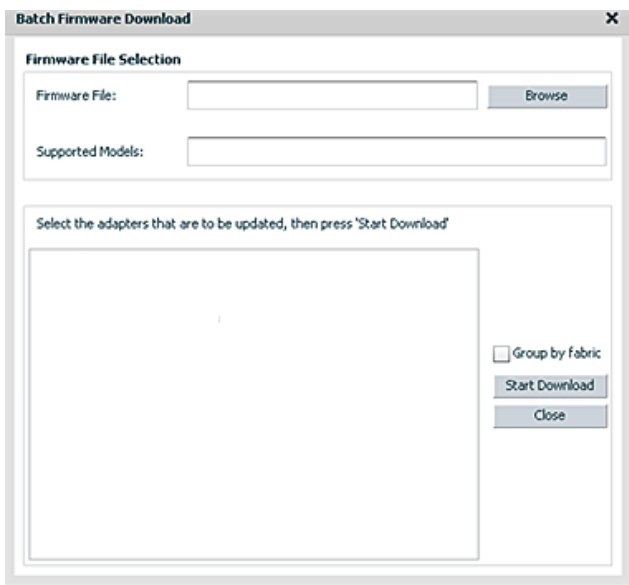
On the system where OneCommand Manager for VMware vCenter is installed, make sure the port numbers configured during the installation are open and dedicated to the OneCommand Manager for VMware vCenter server only. No other service should be listening on this port.

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:

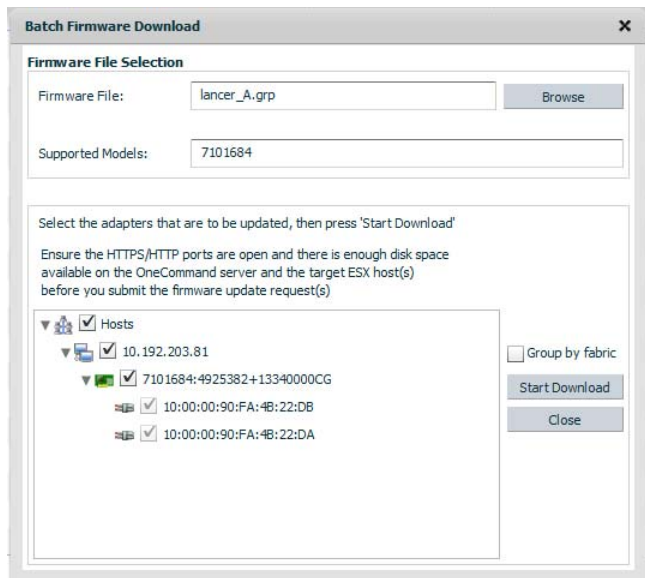
1. Select a host in the console tree-view, and, if applicable, select the **Emulex OneCommand** tab.
2. Select the **Maintenance** tab and click **Update Firmware**. The **Batch Firmware Download** dialog appears (Figure 45).

Figure 45: Batch Firmware Download Dialog



3. Click **Browse** to find the firmware file and click **Open**.
4. Click **Start Download** (Figure 46).

Figure 46: Populated Batch Firmware Download Dialog



The tree-view shows 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 the **Group by Fabric** check box. 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 shows 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** field in the Completed Jobs list shows 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.

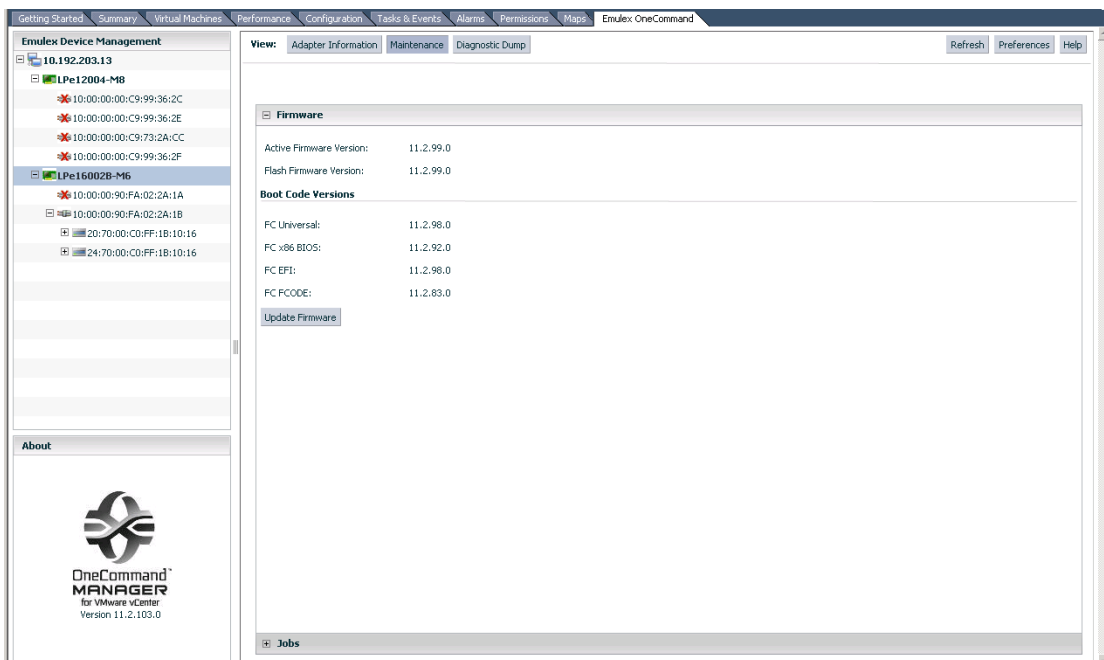
7.2 Updating Firmware for LPe16000-Series, LPe31000-Series, and LPe32000-Series Adapters

For all LightPulse 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:

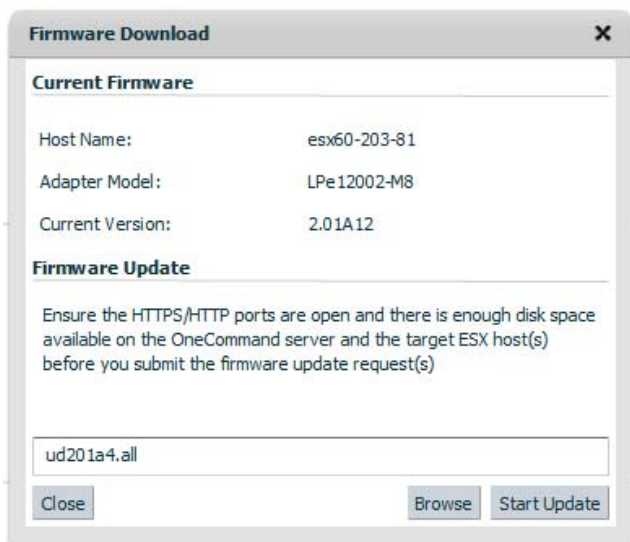
1. Select a host in the console tree-view, and if applicable, select the **Emulex OneCommand** tab.
2. In the Emulex Device Management tree-view, select the adapter for which you want to update firmware information.
3. Select the **Maintenance** tab (Figure 47).

Figure 47: Maintenance Tab



4. Click **Update Firmware**. If a warning message appears, click **Yes**. The **Firmware Download dialog** is displayed (Figure 48).

Figure 48: Firmware Download Dialog



5. Click **Browse** and navigate to the unzipped, extracted image file 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 53). A status message in the Active Job list shows 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** field in the Completed Jobs list shows 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.

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.

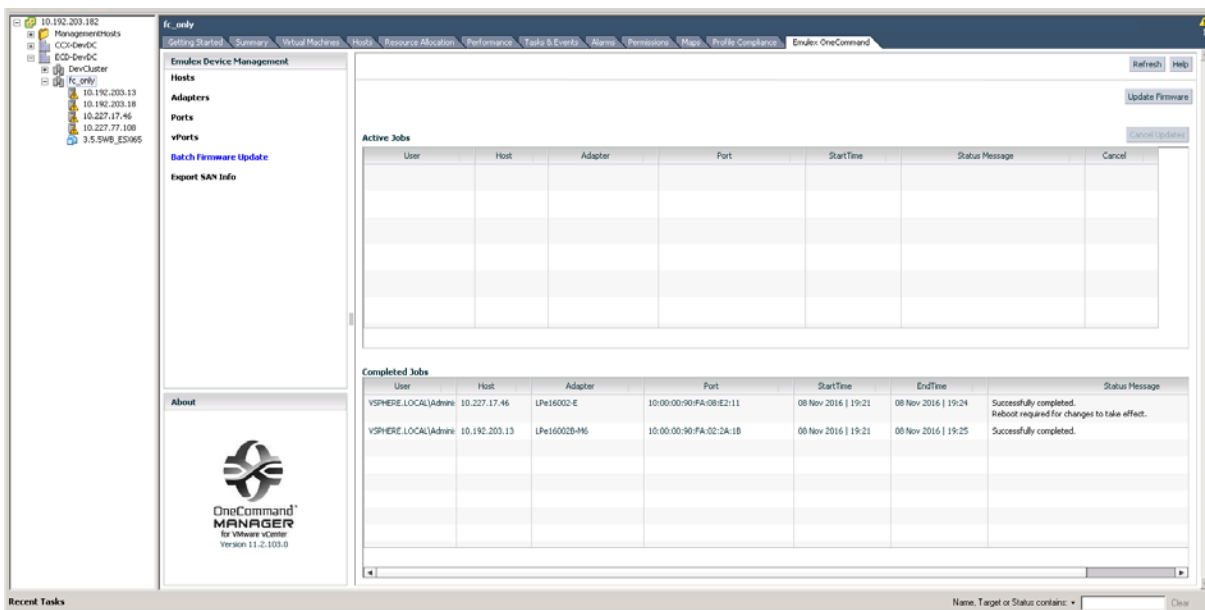
NOTE: On the system where OneCommand Manager for VMware vCenter is installed, make sure the port numbers configured during the installation are open and dedicated to the OneCommand Manager for VMware vCenter server only. No other service should be listening on this port.

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 49). The **Batch Firmware Download** dialog appears (Figure 45).

Figure 49: Batch Firmware Update Information



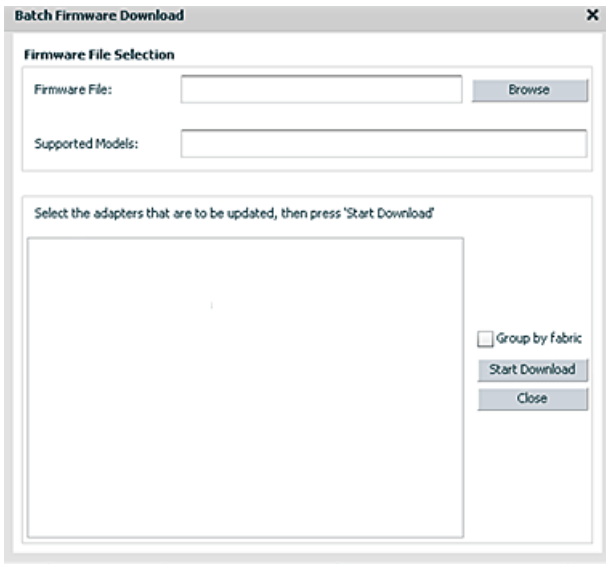
3. Click **Start Download** to install firmware on multiple adapters in a single step. Batch firmware loading is restricted to a single firmware file and to all accessible adapters for which that file is compatible.

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 warning message appears, click **Yes**. The **Batch Firmware Download** dialog is displayed (Figure 50).

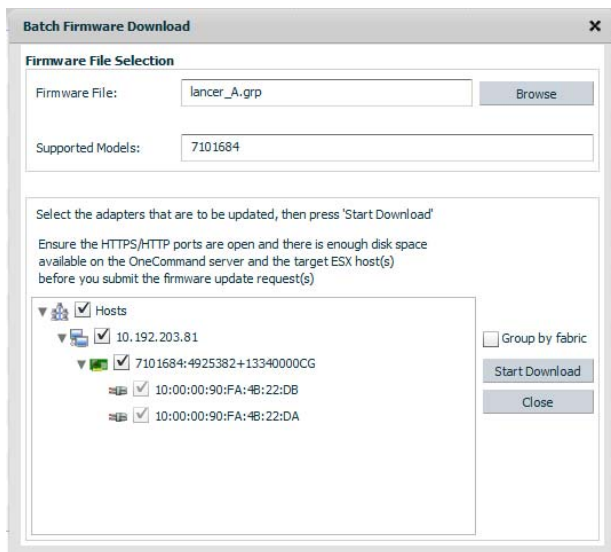
Figure 50: Batch Firmware Update Dialog



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

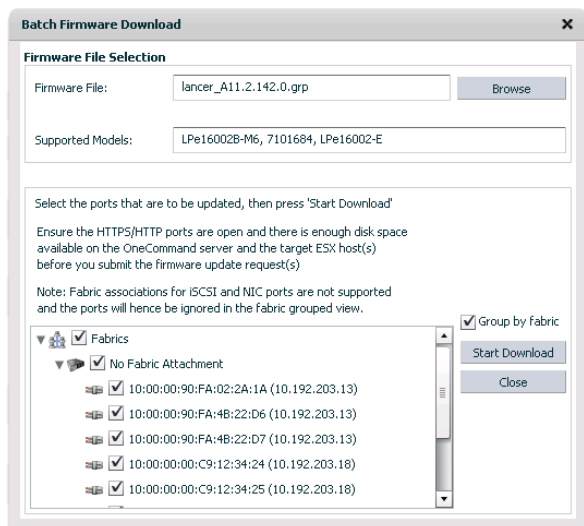
3. Click **Browse**, and a search dialog appears. On the search dialog, select the file you want to use and click **OK**. A status message appears indicating that OneCommand Manager for VMware vCenter is searching for compatible adapters. After compatible adapters are found, the following is displayed in the **Batch Firmware Download** dialog (Figure 51):
 - **Firmware File** – This field shows the selected image file name.
 - **Supported Models** – This field shows 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 the **Group by Fabric** check box is not selected.

Figure 51: Batch Firmware Download Dialog, Host-Centric View



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

Figure 52: Batch Firmware Download Dialog, Fabric-Centric View



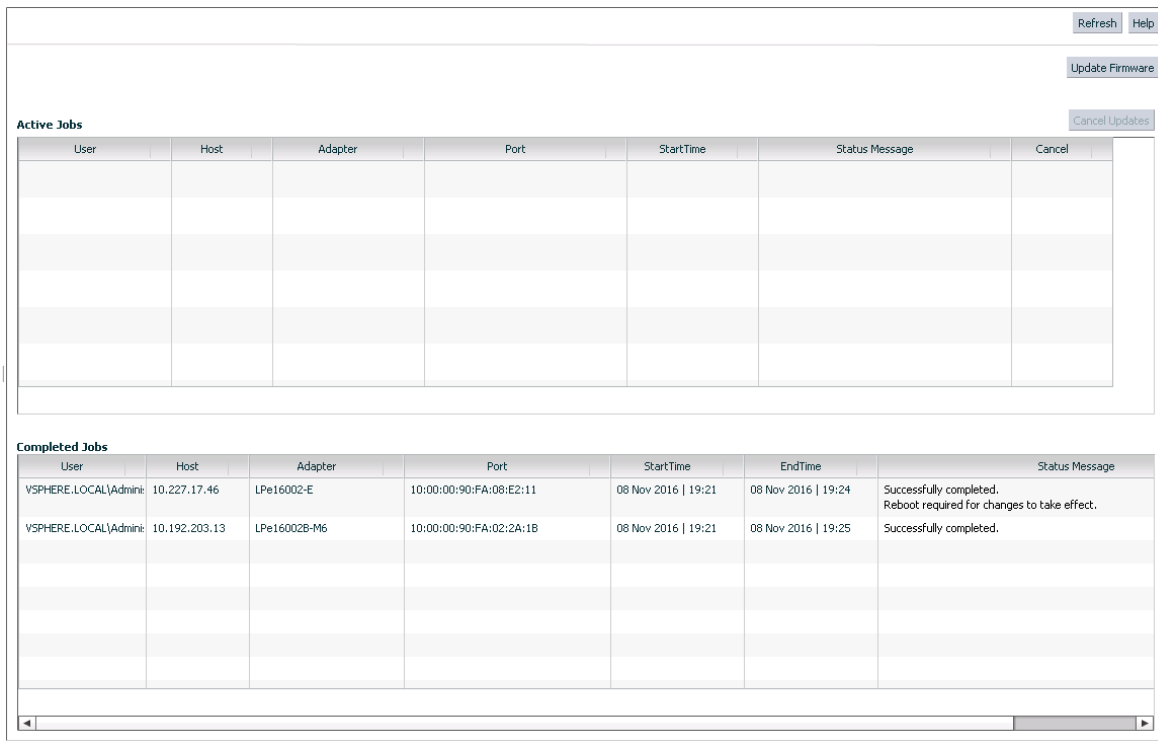
The tree-view shows all adapters and their corresponding hosts or fabrics for which the selected firmware file is compatible. Use the check boxes next to the entries to select or deselect a host, fabric, adapter, or port (if the adapters where the individual port can have new firmware downloaded).

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 shows 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** field in the Completed Jobs list shows the status of the completed job (Figure 53).

Figure 53: Completed Jobs Window



The screenshot displays the 'Completed Jobs' window with the following data:

User	Host	Adapter	Port	StartTime	EndTime	Status Message
VSPHERE.LOCAL\Admini	10.227.17.46	LPe16002-E	10:00:00:90:FA:08:E2:11	08 Nov 2016 19:21	08 Nov 2016 19:24	Successfully completed. Reboot required for changes to take effect.
VSPHERE.LOCAL\Admini	10.192.203.13	LPe16002B-M6	10:00:00:90:FA:02:2A:1B	08 Nov 2016 19:21	08 Nov 2016 19:25	Successfully completed.

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

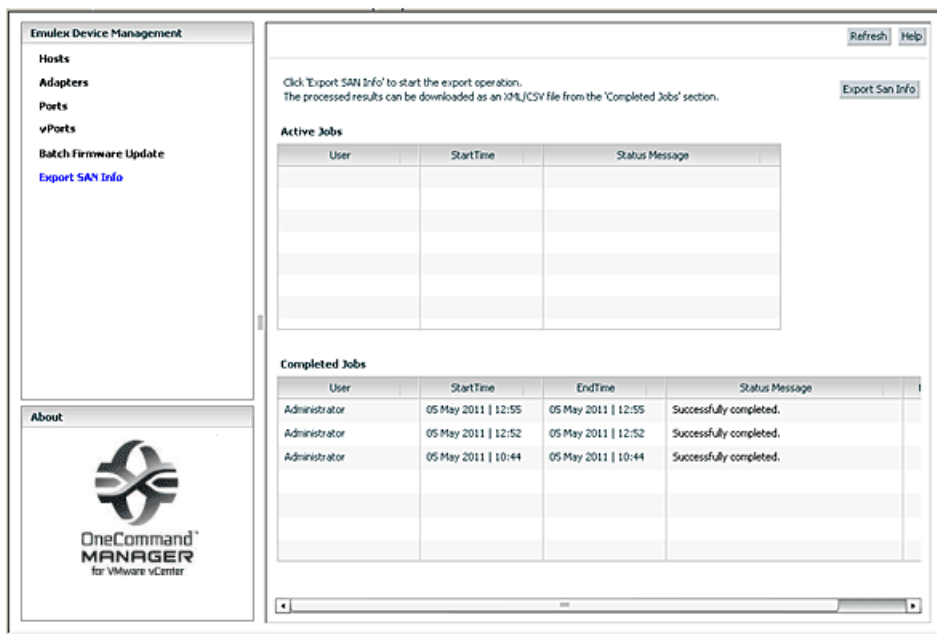
Exporting SAN information (creating a SAN report) processes in the background until all the jobs are completed. During this period, you can still browse through the other tabs.

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 54).

Figure 54: Export SAN Info Option in the Emulex Device Management Tree-View

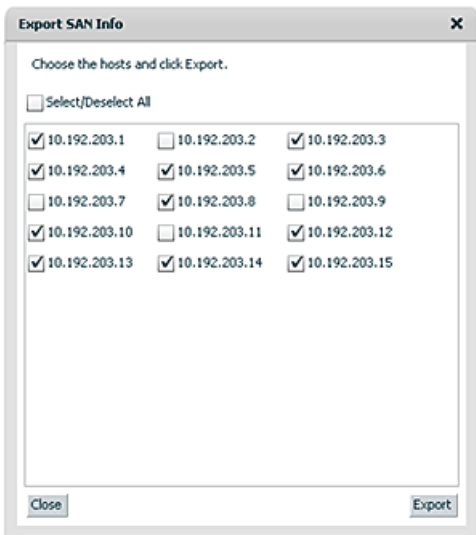


The following **Export SAN Info** window fields are displayed:

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

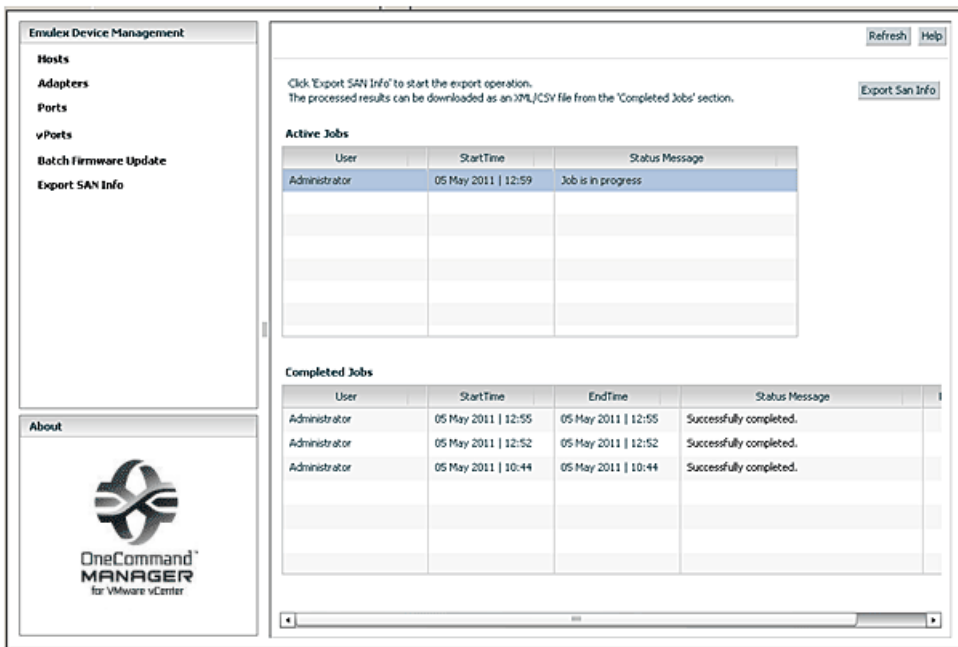
3. Click **Export San Info**. The **Export SAN Info** dialog is displayed (Figure 55).

Figure 55: Export SAN Info Dialog



4. Select host or hosts to export. Optionally, select the **Select/Deselect All** check box to select all hosts. Clear the **Select/Deselect All** check box 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 56).

Figure 56: 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 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: Diagnostics

This section describes diagnostics for Emulex LightPulse adapters.

9.1 Emulex LightPulse Diagnostics

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.

9.1.1 Running Loopback Tests

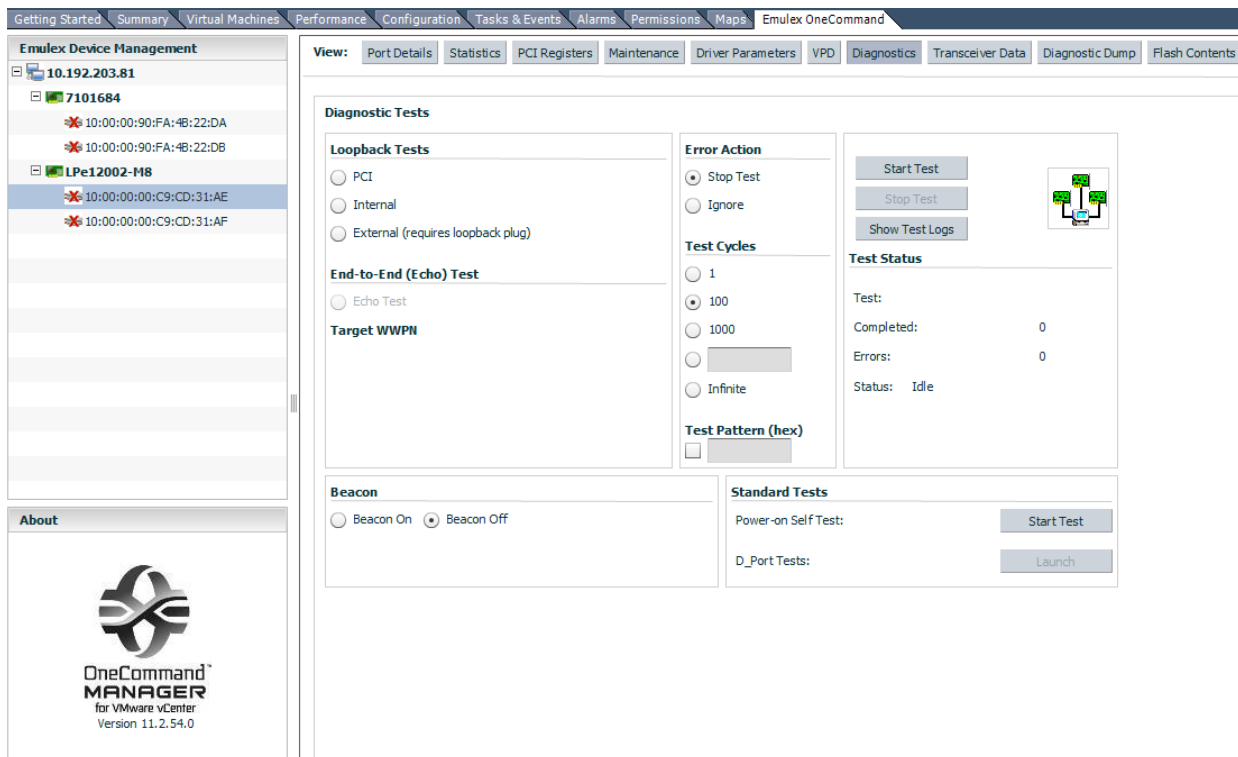
You can run three loopback tests for the FC adapter port:

- 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.

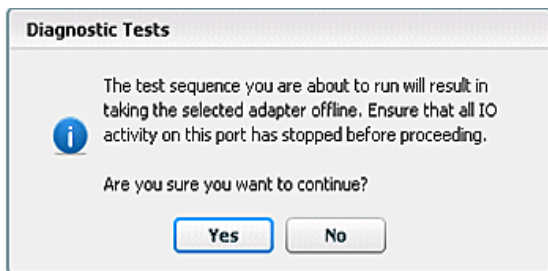
To run loopback tests, perform these steps:

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 57). In the Loopback Test area of the dialog, choose the type of loopback test you want to run, and define the loopback test parameters.

Figure 57: Diagnostics Tab



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



4. Click **Yes**. A progress bar shows that the test is running.

5. Periodic test feedback, consisting of the current loopback test/cycle plus 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.

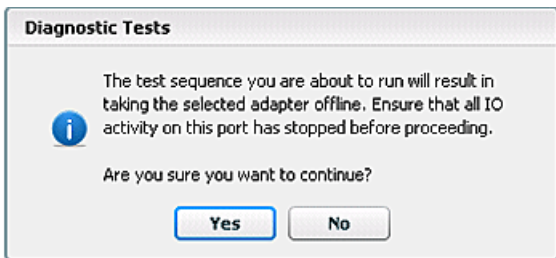
9.1.2 Running End to End (ECHO) Tests

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 57). In the End-to-End (Echo) Test area, select **Echo Test**.

3. Enter the WWPN for the target. The following warning appears:



4. Click **Yes**. A result screen 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.

9.1.3 Running D_Port Tests

D_Port is a diagnostic mode supported by Brocade switches for LPe16000-series, LPe31000-series, and LPe32000-series 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 5.1.2.3, Enabling and Disabling Dynamic D_Port](#), for information about disabling Dynamic D_Port.

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

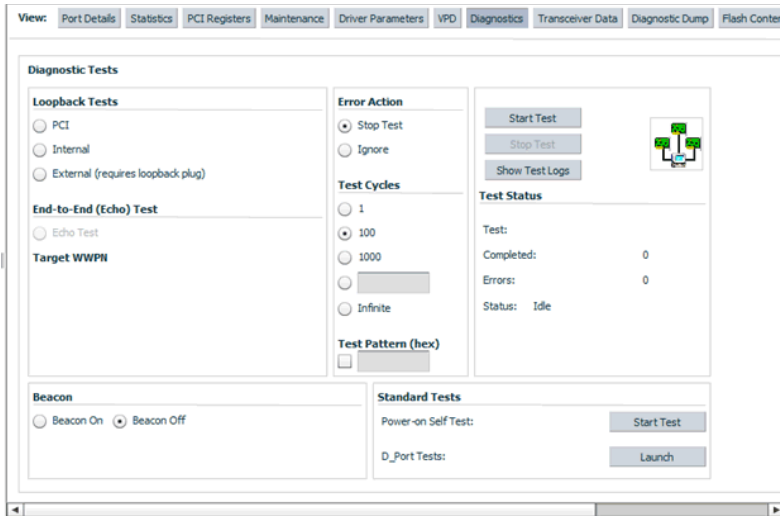
- Local electrical loopback
- Loopback to the remote optics
- Loopback from the remote port to the local optics
- A full device loopback test with data integrity checks
- An estimate of cable length (to validate that a proper buffering scheme is in place)

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

To run D_Port tests, perform these steps:

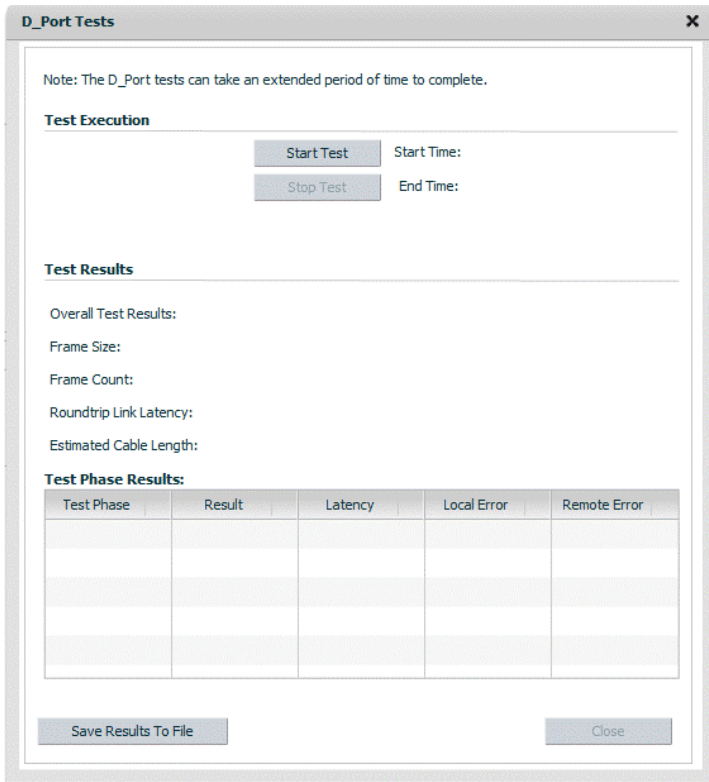
1. From the Emulex Device Management tree-view, select the FC adapter physical port for which you want to run the D_Port tests.
2. Select the **Diagnostics** tab, and in the Standard Tests area, click **Launch** ([Figure 58](#)).

Figure 58: FC Adapter Diagnostics Tab with D_Port Tests Option



3. The D_Port Tests dialog is displayed (Figure 59). Click **Start Test**.

Figure 59: D_Port Tests Dialog



The D_Port tests are launched. If all tests pass, a dialog similar to Figure 60 is displayed. If all tests do not pass, the Failed result is shown in the Test Phase Results (Figure 61).

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 may not be reported in the results. However, the failed phase will be reported.

If the Overall Test Result 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 60: D_Port Tests Dialog – Passed Result

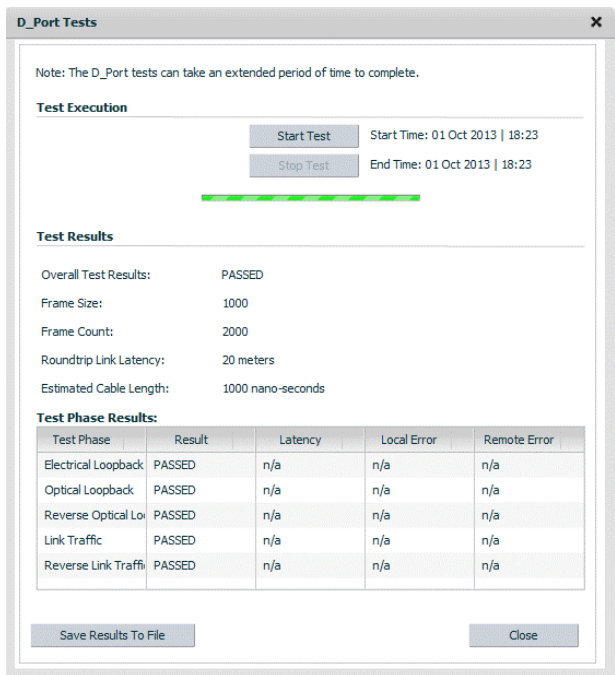
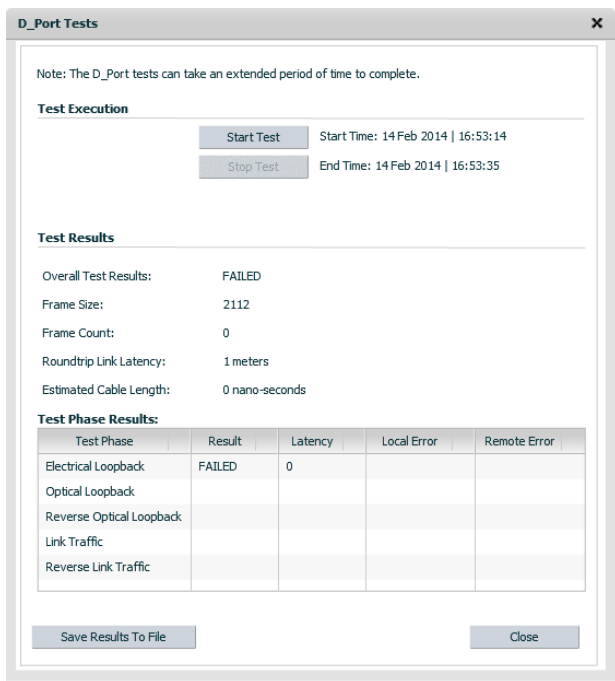


Figure 61: D_Port Tests Dialog – Failed Results



9.1.4 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.

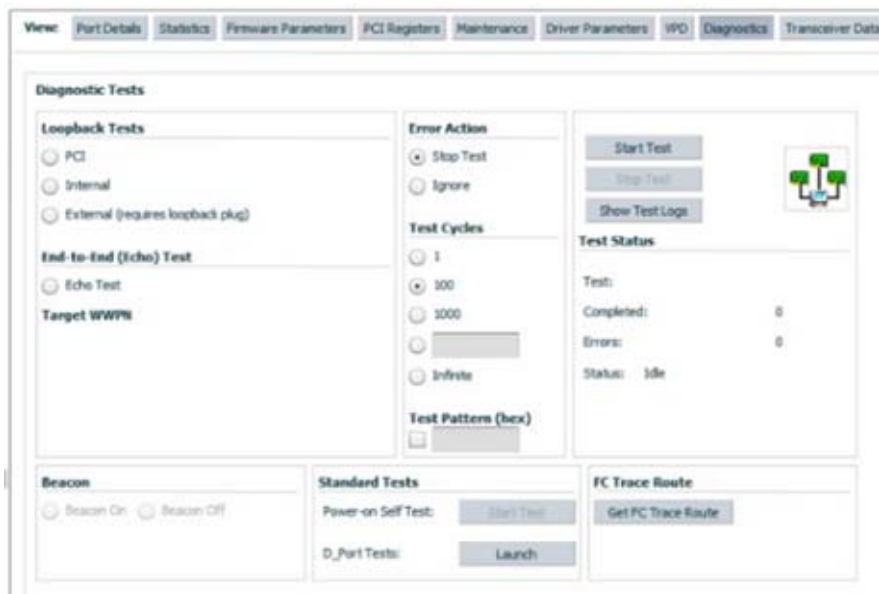
Communication route information such as the switch name, domain ID, ingress and egress port name, and ingress and egress physical port number, is accumulated for all switch ports through which packets are routed. Data for both the outward bound route from the initiator to the target, and the inbound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

The **FC Trace Route** button on the **Diagnostics** tab enables you to collect FC Trace Route information on LPe15000-series, LPe16000, LPe31000, and LPe32000-series adapters. (Figure 62)

9.1.4.1 FC Trace Route Considerations

- FC Trace Route is only supported on LPe15000-series, LPe16000-series, LPe31000-series, and LPe32000-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.

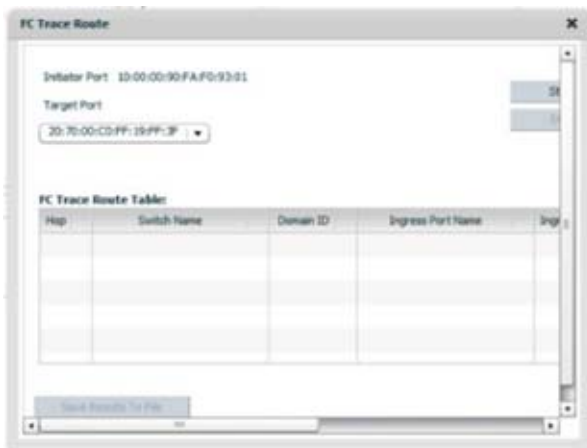
Figure 62: Diagnostics Tab (FC Trace Route Button Depicted)



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 62) and click **Get FC Trace Route**. The **FC Trace Route** dialog appears (Figure 63).

Figure 63: FC Trace Route Dialog



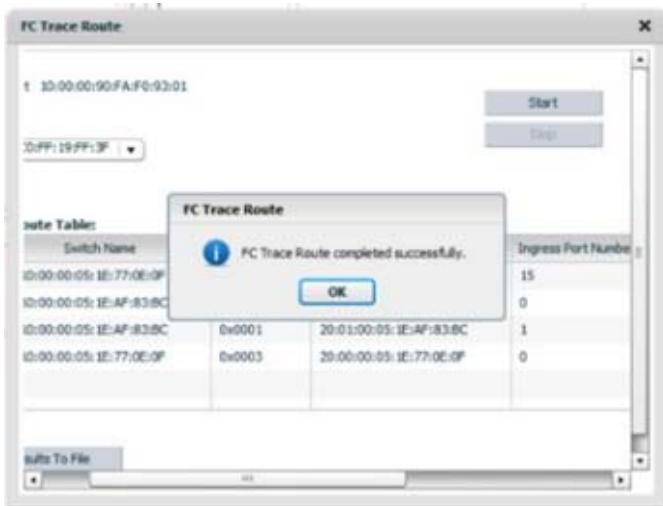
3. The **Target Port** drop-down list displays the WWPNs of all targets that are seen by the initiator port. Select a target port and Click **Start**.

The **FC Trace Route** dialog displays trace route information for selected initiator and target ports (Figure 64).

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 64: 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 0–255.
- Ingress Port Name – The port WWN of the physical port through which an FC packet enters a specific switch.
- Ingress Physical 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.

9.1.5 Running a POST

The power-on self-test (POST) is a firmware test 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 57) 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.

9.1.6 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.

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

To enable or disable 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 57) and click either **Beacon On** or **Beacon Off**.

9.1.7 Setting Up Diagnostic Test Options

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

9.1.7.1 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.

9.1.7.2 Setting Up Test Cycles

Specify one of the following test cycles:

- Select an established cycle count by clicking on 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**.

9.1.7.3 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.

9.1.7.4 Test Status

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

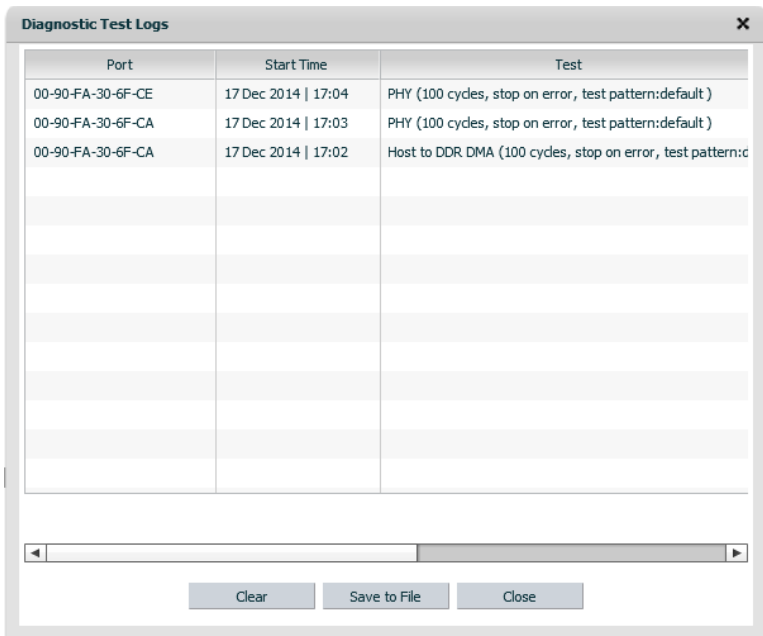
9.1.8 Saving the Log File

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 65 shows the Diagnostic Test log entries that will be saved to the log file.

Figure 65: Diagnostic Test Log Entries



Port	Start Time	Test
00-90-FA-30-6F-CE	17 Dec 2014 17:04	PHY (100 cycles, stop on error, test pattern:default)
00-90-FA-30-6F-CA	17 Dec 2014 17:03	PHY (100 cycles, stop on error, test pattern:default)
00-90-FA-30-6F-CA	17 Dec 2014 17:02	Host to DDR DMA (100 cycles, stop on error, test pattern:d

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. Browse to the desired directory, change the log file name if you want, and click **Save to File**.

9.1.9 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.

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 66). Diagnostic dump information is displayed.

Figure 66: Diagnostic Dump Tab

Dump Details

Serial Number: VTH6280012

Dump File Directory:

Modify Dump Directory

Dump File Retention

Currently, up to 10 dump files per adapter may be retained on this host. You may change the number of retained dump files, but be aware that the individual dump files can be as large as 6 megabytes. Take this into account when selecting a retention count.

10 |

Generate Dump

Delete Existing Dump Files Start Dump Show Dump Files

4. Enter a name in the **Dump File Directory** field in the Dump Details area to set the dump file directory. A prefix of `/vmfs/volumes` is added to the location, if it is not specified.
5. To specify up to 20 files to retain using the **Dump Files 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.

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

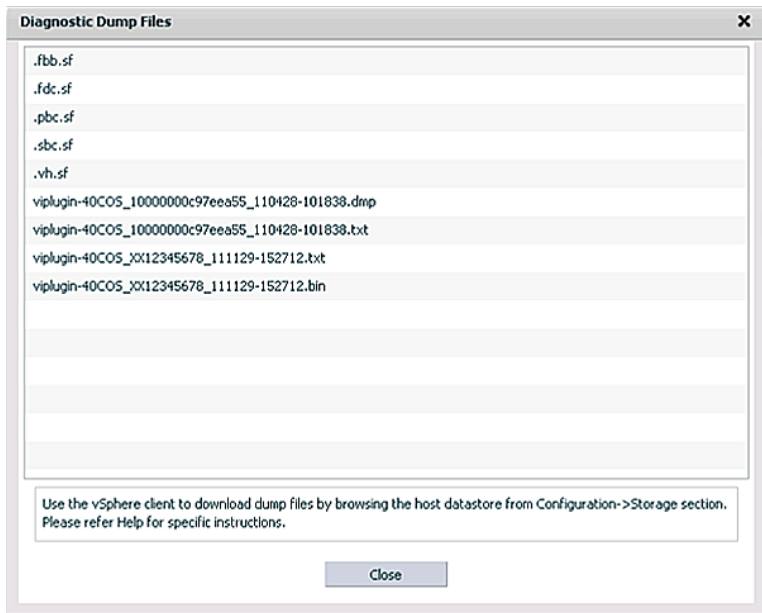
9.1.10 Viewing Diagnostic Dump Files

You can view diagnostic dump file names using the 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:

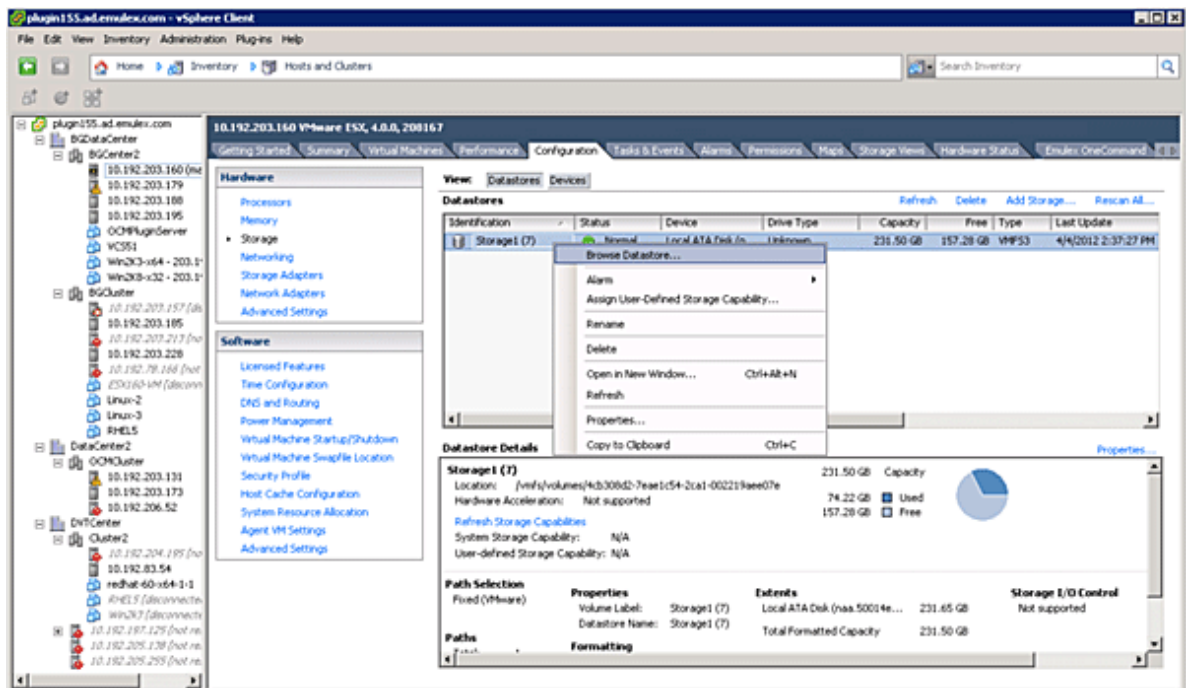
1. On the **Diagnostic Dump** tab, click **Show Dump Files**. The **Diagnostic Dump Files** window opens showing the diagnostic dump files currently on your system (Figure 67). These files are available in the dump directory configured from the **Diagnostic Dumps** tab. You can extract these files using the client.

Figure 67: Diagnostic Dump Files Window



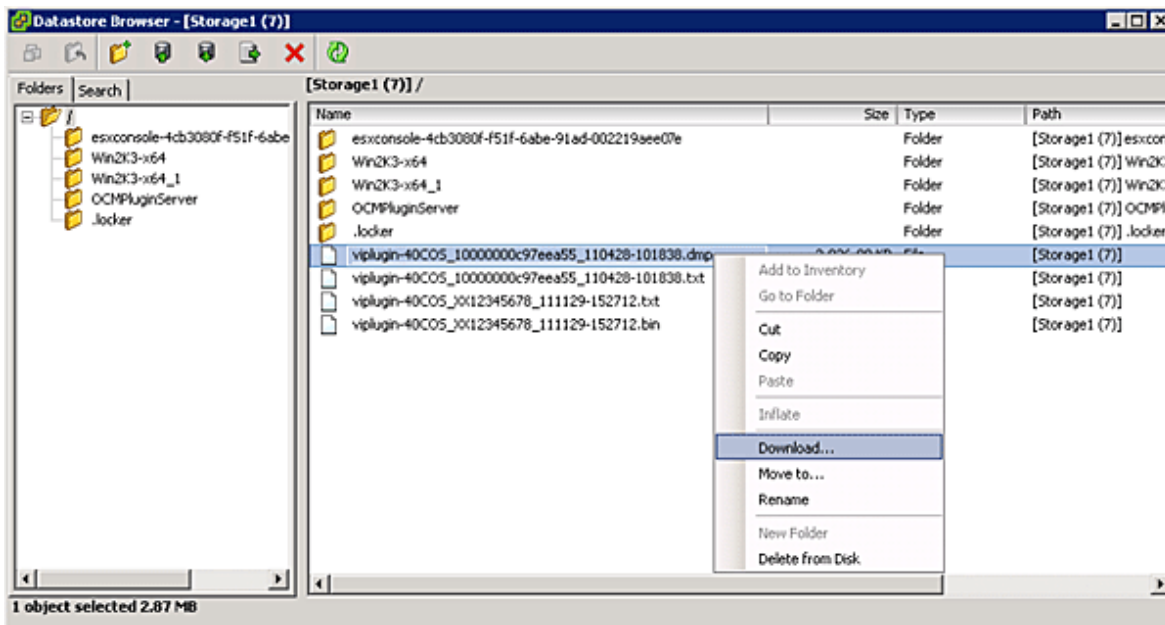
2. Extract the dump files by using the client to download the dump files by browsing the data store.
 - a. Click the **Configuration** tab in the client. The Datastores view is displayed (Figure 68).

Figure 68: Datastores View of Client



- b. Right-click the datastore where the dump file is located, and select **Browse Datastore** from the context menu. A Datastore Browser window opens (Figure 69).

Figure 69: Datastore Browser



- c. In the Datastore Browser, right-click the dump file that you want to review and select **Download...** from the context menu. A **Browse for Folder** window opens.
 - d. 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.
3. Click **Yes**. A progress bar shows that the test is running.
- Periodic test feedback, consisting of the current loopback test/cycle plus 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.

Chapter 10: Generating and Installing Secured Certificates

OCMNG is a web application, based on a client-server model, running 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 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 warning is shown 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  
A1UEChMDZWx4MQRwwCgYDVQQLEwNvY20xHzAdBgNVBAMTFmJnc3N5ZWQxLmFkLmVtdWxleC5jb20w  
ggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCdhovljXhfjNPM/5eBsX4280AIl3YARn0p  
R6Z7eOqslr5Qh07kT58M6T8fER+NpIN7WhOOF/TbsFsS0gmfYwJQqtvtvtqldtxUGpvFe9lywbP+l  
kY+w6GOyPTG2qnXgILtX5ArZbC2UBbz+J8WJ3SjPHXiSY35EZWnyZZmIN8v1vOe9e21f8vwRkn/4  
fdFfrpoQa3H+GcAJMRSBRTd5H6mXQv6HaA5Z0BbsABisFx4scqSum/HJKLP6GcSHR61bzHfio/NH  
4qU/s6I2LC5DvGs1hIW3PPbmlrxBiEFpjPtWhfzPXPmKSU8uey+lE0UIPMS0FMTxo63oYnMeiSX  
X5mxAgMBAAGgMDAuBgkqhkiG9w0BCQ4xITAfMBOGA1UdDgQWBBSvpKLBf31Y03Jin9kI4ym94bji  
zjANBgkqhkiG9w0BAQsFAAOCAQEafs94wzEU1DAMq0jITi6fid7YxK2KFWJgMBfjxZIGex2zx1HL  
mOS14BGSWk5dvSMwqDBC1414C79rU01TUwwWs9zFqMHynndQ2Ze2vuJNTWulnFyFb37/rEvbFufB  
QVvFXgycakRgUpWo2x5sekRJRAPxXI/vLWOFRLlrzcVykGZ/sg3QrO4ezlKFc49put0vKpvIldY9  
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 only works 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 the `keystorePass` matches the password for the keystore, and 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 section includes information about certificate or insecure-content warnings that might be displayed on the console. This section 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

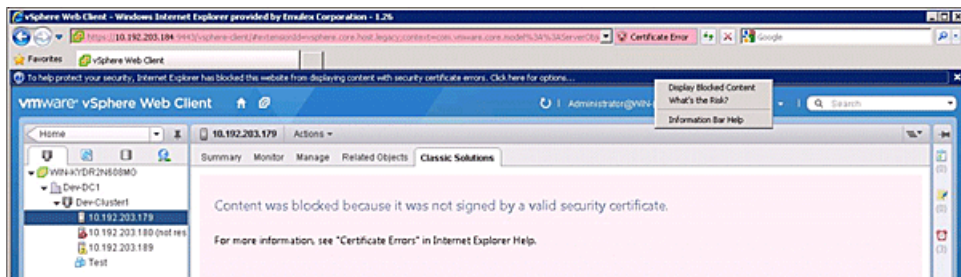
11.1.1 Accepting the Blocked Content

The procedure for accepting blocked content depends on the type of browser 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

Accept the blocked content ([Figure 70](#)).

Figure 70: Blocked Content in Internet Explorer



11.1.1.2 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
```

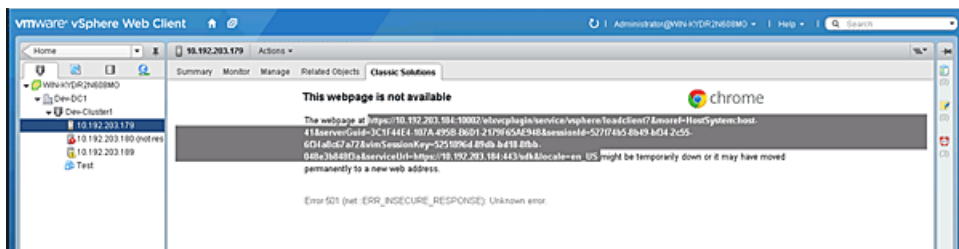
For example:

```
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 or accept the certificate warning ([Figure 71](#)).
3. Refresh the window.

Figure 71: Blocked Content in the Firefox or Chrome Browser



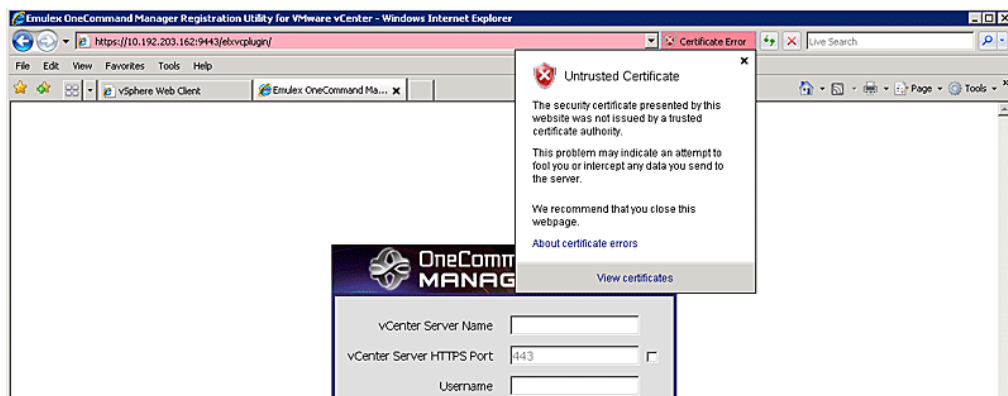
11.1.2 Installing a Security Certificate

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 showing the untrusted certificate (Figure 72).

Figure 72: Untrusted Certificate



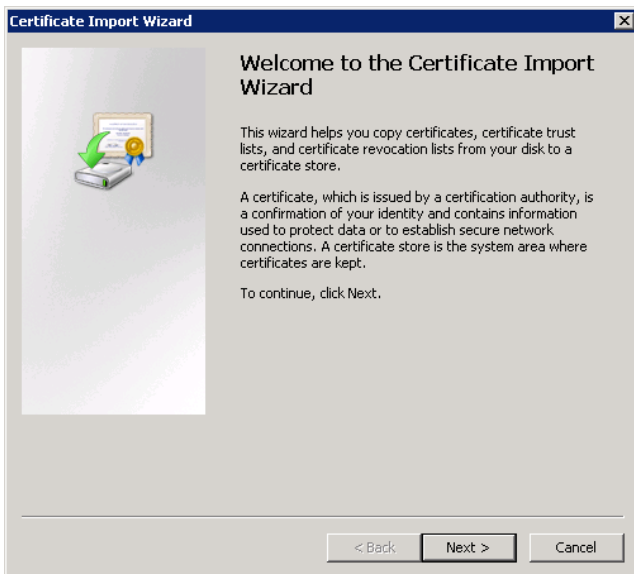
4. Click **View certificates** in the Certificate Error list. The **Certificate** dialog is displayed (Figure 73).

Figure 73: Certificate Dialog



5. Click **Install Certificate...** The **Certificate Import Wizard** is displayed (Figure 74).

Figure 74: Certificate Import Wizard



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

11.1.3 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 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 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: <ul style="list-style-type: none"> ■ 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: <code>esxcli network firewall unload</code>
Firmware update fails with the error message <code>Error reading resource</code> .	Check the following: NOTE: Make sure that you can run the <code>ping</code> command the host name, on which the OneCommand Manager for VMware vCenter is installed, from the ESXi host. If you cannot run the <code>ping</code> command on the host name, either reinstall providing the reachable IP or host name (with domain) or add the host name to the DNS. <ul style="list-style-type: none"> ■ 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 <code>sfcdb</code> on the ESXi host using the command: <code>/etc/init.d/sfcdb-watchdog restart</code> 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 <code>C:\Program Files\</code> have no write and full control privileges. To remedy the problem: <ul style="list-style-type: none"> ■ Assign your account write and full control privileges to <code>C:\Program Files \.</code> or ■ Install OneCommand Manager for VMware vCenter on another disk, for example, D.
When OneCommand Manager for VMware vCenter loads within the console, it shows a Security warning.	See Section 11.1, Security .
Registration of a new host from a non-English system results in a <i>Host not Pingable</i> 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 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.

12.1 elxvcpcmd Syntax Usage

- OneCommand Manager for VMware vCenter CLI runs only in TCP/IP mode.
- OneCommand Manager for VMware vCenter CLI can manage Emulex adapters in systems with VMware ESXi 6.0, 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.

12.2 Help Commands

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

12.2.1 help (Single Command)

Syntax

```
elxvcpcmd.exe [CmdName] help
```

Description

This command shows the help for a specific command.

Parameters

CmdName Any CLI command.

12.2.2 help (Group)

Syntax

```
elxvcpcmd.exe help
```

Description

This command shows 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](#) shows 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 attributes help
```

Parameters

None.

12.3 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
changewwn	Section 12.4.11.1, changewwn
D_Port (Clearlink)	Section 12.4.5.1, D_Port
deletedumpfiles	Section 12.4.7.1, deletedumpfiles
driverconfig	Section 12.4.6.1, driverconfig
dump	Section 12.4.7.2, dump
echotest	Section 12.4.5.2, echotest

Table 3: CLI Commands (Continued)

Command	Section
enablebootcode	Section 12.4.3.1, enablebootcode
exportsaninfo	Section 12.4.4.1, exportsaninfo
fctraceroute	Section 12.4.5.3, fctraceroute
firmwareupdate	Section 12.4.4.2, firmwareupdate
getbeacon	Section 12.4.5.4, getbeacon
getdriverparams	Section 12.4.6.2, getdriverparams
getdriverparamsglobal	Section 12.4.6.3, getdriverparamsglobal
getdumpdirectory	Section 12.4.7.3, getdumpdirectory
getdumpfilenames	Section 12.4.7.4, getdumpfilenames
getexpresslanelunlist	Section 12.4.9.1, getexpresslanelunlist
getfwparams	Section 12.4.8.2, getfwparams
getlunlist	Section 12.4.9.2, getlunlist
getpcidata	Section 12.4.2.1, getpcidata
getportstatistics	Section 12.4.2.2, getportstatistics
getretentioncount	Section 12.4.7.5, getretentioncount
getvpd	Section 12.4.2.3, getvpd
getwwncap	Section 12.4.2.4, getwwncap
getxcvrdata	Section 12.4.5.5, getxcvrdata
hbaattributes	Section 12.4.2.5, hbaattributes
listhbas	Section 12.4.2.6, listhbas
listvms	Section 12.4.10.1, listvms
listvports	Section 12.4.10.2, listvports
loadlist	Section 12.4.5.6, loadlist
loopbacktest	Section 12.4.5.7, loopbacktest
pcidata	Section 12.4.2.7, pcidata
portattributes	Section 12.4.2.8, portattributes
posttest	Section 12.4.5.8, posttest
providerrefresh	Section 12.4.2.9, providerrefresh
readwwn	Section 12.4.11.3, readwwn
reset	Section 12.4.1.2, reset
restorewwn	Section 12.4.11.4, restorewwn
saveconfig	Section 12.4.6.4, saveconfig
serverattributes	Section 12.4.2.10, serverattributes
setbeacon	Section 12.4.5.9, setbeacon
setdriverparam	Section 12.4.6.5, setdriverparam
setdriverparamdefaults	Section 12.4.6.6, setdriverparamdefaults
setdumpdirectory	Section 12.4.7.6, setdumpdirectory
setexpresslanelunstate	Section 12.4.9.3, setexpresslanelunstate
setfwparam	Section 12.4.8.3, setfwparams
setportenabled	Section 12.4.2.11, setportenabled
setretentioncount	Section 12.4.7.7, setretentioncount
setvcred	Section 12.4.1.1, setvcred
targetmapping	Section 12.4.9.6, targetmapping

Table 3: CLI Commands (Continued)

Command	Section
version	Section 12.4.1.3, 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.	<ul style="list-style-type: none"> ■ setvccred ■ reset ■ version 	<p>setvccred – An optional command that saves vCenter credentials and executes subsequent commands without specifying vCenter credentials.</p> <p>reset – Resets the adapter.</p> <p>version – Shows the version of the installed CLI.</p>
Attributes group – Commands to read and manage information about an adapter.	<ul style="list-style-type: none"> ■ getpcidata ■ getportstatistics ■ getvpd ■ getwwncap ■ hbaattributes ■ listhbas ■ pcidata ■ portattributes ■ providerrefresh ■ serverattributes ■ setportenabled 	<p>getpcidata – Lists PCI register details for ports.</p> <p>getportstatistics – Lists statistics for a port. If the optional parameter, <code>clear</code>, is set, this command clears the 10GBASE-T counters.</p> <p>getvpd – Shows the VPD details for the specified port on the adapter.</p> <p>getwwncap – Shows the WWN capabilities of the specified port.</p> <p>hbaattributes – At the host level, shows adapter attributes for a port on the adapter.</p> <p>listhbas – For a cluster or a host, shows a list of manageable Emulex adapters.</p> <p>pcidata – Lists PCI attributes for a port on the adapter.</p> <p>portattributes – Shows a list of all port attributes for the port on the adapter.</p> <p>providerrefresh – Updates the displayed CIM provider data, and cluster or host information.</p> <p>serverattributes – Lists basic information about the host.</p> <p>setportenabled – Enables or disables the port status for a port on a host.</p>
Boot group – Commands to enable an ESXi host to manage the boot environment.	<ul style="list-style-type: none"> ■ enablebootcode 	<p>enablebootcode - Enables or disables the bootBIOS state on a given port.</p>
Cluster group – Commands that can be run on a cluster.	<ul style="list-style-type: none"> ■ exportsaninfo ■ firmwareupdate ■ listhbas 	<p>exportsaninfo – Exports SAN information related to Emulex adapters in all the hosts in a cluster.</p> <p>firmwareupdate – Updates the firmware on the Emulex adapters found in a VMware cluster or the ESXi host.</p> <p>listhbas – Lists manageable Emulex adapters.</p>

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

Help Group	Supported CLI Commands	Command Descriptions
Diagnostic group – Commands to run diagnostic tests for an Emulex adapter or port.	<ul style="list-style-type: none"> ■ D_Port ■ echotest ■ fctraceroute ■ getbeacon ■ loadlist ■ loopbacktest ■ posttest ■ setbeacon 	<p>D_Port – Runs D_Port diagnostics. Also known as ClearLink.</p> <p>echotest – Runs an echo test on a port.</p> <p>fctraceroute – Issues an FC trace route request for the communication path between an FC initiator port and an FC target port.</p> <p>getbeacon – Shows the current beacon state for a port on an adapter.</p> <p>loadlist – Lists the flash memory load list data for an FC port.</p> <p>loopbacktest – Runs a loopback test on a port.</p> <p>posttest – Runs a POST on a specified FC port.</p> <p>setbeacon – Turns the beacon state on or off for a port on an adapter.</p>
Driver Parameters group – Commands to enable an ESXi host to read and manage driver parameters for the host and an Emulex adapter.	<ul style="list-style-type: none"> ■ driverconfig ■ getdumpdirectory ■ getdriverparamsglobal ■ saveconfig ■ setdriverparam ■ setdriverparamdefaults 	<p>driverconfig – Sets all driver parameters to the values in the <code>.dpv</code> file on an ESXi host.</p> <p>getdumpdirectory – Lists driver parameters for a port.</p> <p>getdriverparamsglobal – Lists global driver parameters for a port.</p> <p>saveconfig – Saves an adapter’s driver parameters to a file.</p> <p>setdriverparam – Sets a driver parameter for a port and designates the scope of the change.</p> <p>setdriverparamdefaults – Restores all driver parameters to the default value, at the port or global level (temporarily or permanently).</p>
Dump group – Commands to manage dump files for a selected adapter. Dump files are useful when troubleshooting.	<ul style="list-style-type: none"> ■ deletedumpfiles ■ dump ■ getdumpdirectory ■ getdumpfilenames ■ getretentioncount ■ setdumpdirectory ■ setretentioncount 	<p>deletedumpfiles – Deletes all diagnostic dump files for a port.</p> <p>dump - Performs a core dump of a local port.</p> <p>getdumpdirectory – Shows a dump file directory for a port in the host.</p> <p>getdumpfilenames – Lists all dump file names for a port.</p> <p>getretentioncount – Shows the maximum number of diagnostic dump files to keep for a port.</p> <p>setdumpdirectory – Sets the dump directory for all adapters in the server.</p> <p>setretentioncount – Specifies the maximum number of diagnostic dump files for the adapter.</p>
Firmware group – Commands to update the firmware, view the firmware parameters, and change the firmware parameters on an Emulex adapter or port.	<ul style="list-style-type: none"> ■ firmwareupdate ■ getfwparams ■ setfwparams 	<p>firmwareupdate – Updates the firmware on Emulex adapters in a VMware cluster or ESXi host.</p> <p>getfwparams – Displays the available firmware parameters, and their ranges, for the specified port.</p> <p>setfwparams – Assigns new firmware parameter values to the specified port.</p>

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

Help Group	Supported CLI Commands	Command Descriptions
Target And LUNs group – Commands to enable an ESXi host to read targets and LUNs attached to the port on an Emulex adapter, enable ExpressLane LUNs, and set frame priority levels for ExpressLane LUNs.	<ul style="list-style-type: none"> ■ getexpresslanelunlist ■ getlunlist ■ setexpresslanelunstate ■ GetLunXLaneConfig ■ SetLunXLaneConfig ■ targetmapping 	<p>getexpresslanelunlist – On LPe16000-series, LPe31000-series, and LPe32000-series adapters, lists the LUNs that support ExpressLane and their respective ExpressLane status.</p> <p>getlunlist – Lists the LUNs attached to the target of the specified port.</p> <p>setexpresslanelunstate – Enables or disables ExpressLane on a LUN.</p> <p>GetLunXLaneConfig – Displays the frame priority value for ExpressLane LUNs on the specified target.</p> <p>SetLunXLaneConfig – Configures the ExpressLane state and the frame priority levels, or values, for ExpressLane LUNs.</p> <p>targetmapping – Lists the targets attached to the specified port.</p>
Virtual Machines group – Commands to enable an ESXi host to find Virtual Machines and their attached ports.	<ul style="list-style-type: none"> ■ listvms ■ listvports 	<p>listvms – Lists all virtual machines and their information for all manageable ports.</p> <p>listvports – Lists all virtual ports on the specified physical port.</p>
WWWN Management group – Commands to enable an ESXi host to read and manage the WWN details for the port on an Emulex adapter.	<ul style="list-style-type: none"> ■ changewwn ■ getwwncap ■ readwwn ■ restorewwn 	<p>changewwn – Changes the WWN of the port.</p> <p>getwwncap – Lists the WWN capabilities of the port.</p> <p>readwwn – Lists the WWN details of the port and category.</p> <p>restorewwn – Restores the WWN value of the port.</p>

12.4 Group Commands and CLI Command Descriptions

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

12.4.1 General Group Commands

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

12.4.1.1 setvccred

12.4.1.1.1 Syntax

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

12.4.1.1.2 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 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.

12.4.1.1.3 Parameters

- v The vCenter server IP address.
- u The user name for the vCenter server.
- p The user password for the vCenter server.

12.4.1.1.4 Examples

Execute `setvccred` first:

```
elxvpcmd.exe setvccred v=12.345.678.901 u=username p=password
```

Subsequent commands can be:

New format:

```
elxvpcmd.exe h=12.345.678.123 listhbas
```

or

Old format:

```
elxvpcmd.exe v=12.345.678.901 u=username p=password h=12.345.678.123 listhbas
```

12.4.1.2 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.

12.4.1.2.1 Syntax

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

12.4.1.2.2 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.

12.4.1.3 version

This command shows the version of the CLI installed.

12.4.1.3.1 Syntax

```
elxvpcmd.exe version
```

12.4.1.3.2 Parameters

None.

12.4.2 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 physical port speed.

12.4.2.1 getpcidata

This command shows PCI register details for ports.

12.4.2.1.1 Syntax

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

12.4.2.1.2 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.

12.4.2.2 getportstatistics

This command extracts the statistics for a designated port.

12.4.2.2.1 Syntax

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

12.4.2.2.1.1 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.

12.4.2.3 getvpd

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

12.4.2.3.1 Syntax

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

12.4.2.3.2 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.

12.4.2.4 getwwncap

This command shows the WWN capabilities of the specified port.

12.4.2.4.1 Syntax

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

12.4.2.4.2 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.

12.4.2.5 hbaattributes

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

12.4.2.5.1 Syntax

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

12.4.2.5.2 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.

12.4.2.6 listhbas

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

12.4.2.6.1 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
```

12.4.2.6.2 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.

12.4.2.7 pcidata

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

12.4.2.7.1 Syntax

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

12.4.2.7.2 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.

12.4.2.8 portattributes

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

12.4.2.8.1 Syntax

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

12.4.2.8.2 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.

12.4.2.9 providerrefresh

This command refreshes the displayed CIM provider data, and cluster or host information.

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

12.4.2.9.1 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.

12.4.2.10 serverattributes

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

12.4.2.10.1 Syntax

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

12.4.2.10.2 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.

12.4.2.11 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 an FC port, the adapter must be reset to activate the new setting.

12.4.2.11.1 Syntax

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

12.4.2.11.2 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

12.4.3 Boot Command

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.

12.4.3.1 enablebootcode

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

12.4.3.1.1 Syntax

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

12.4.3.1.2 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 BootBIOS state. 1 = enable BootBIOS state.

12.4.4 Cluster Commands

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

12.4.4.1 exportsaninfo

This command exports all SAN information related to Emulex adapters in all the 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.

12.4.4.1.1 Syntax

```
elxvpcmd.exe v=<vcenter_server> u=<vc_username> p=<vc_pwd> c=<clustername> exportsaninfo [format]
```


NOTE: [*format*] 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 shows the data in XML format.

12.4.4.1.2 Parameters

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

12.4.4.2 firmwareupdate

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

12.4.4.2.1 Procedure

1. Run the `firmwareupdate` command. A list of adapter serial numbers (for LPe16000-series, LPe31000-series, and LPe32000-series adapters) or port WWNs (for LPe12000-series adapters) are displayed, applicable to the firmware file specified.
2. Select the adapter or port option to use for the update. `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.

12.4.4.2.2 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>
```

12.4.4.2.3 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.
a11 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.

12.4.4.3 listhbas

See [Section 12.4.2.6, listhbas](#).

12.4.5 Diagnostic Commands

The Diagnostic commands run diagnostics, including POST and loopback. Diagnostic commands also show and set beacon, and run the D_Port diagnostic (LPe16000-series, LPe31000-series, and LPe32000-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.

12.4.5.1 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 LPe16000-series, LPe31000-series, and LPe32000-series adapters with D_Port support.

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 cable, optics modules, and connector or optics seating.

Considerations for running D_Port

- 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 re-run 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.

12.4.5.1.1 Example

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

12.4.5.1.2 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.

12.4.5.2 echotest

This command runs a loopback test on a given port.

12.4.5.2.1 Syntax

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

12.4.5.2.2 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).

12.4.5.2.3 Example

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

12.4.5.3 fctraceroute

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

12.4.5.3.1 Syntax

```
fctraceroute <WWPN> <Target WWPN>
```

12.4.5.3.2 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.

12.4.5.3.3 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
```

12.4.5.4 getbeacon

This command shows the current beacon state, on or off.

12.4.5.4.1 Syntax

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

12.4.5.4.2 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.

12.4.5.5 getxcvrdata

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

12.4.5.5.1 Syntax

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

12.4.5.5.2 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.

12.4.5.6 loadlist

This command shows the flash parameters for a given port.

12.4.5.6.1 Syntax

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

12.4.5.6.2 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.

12.4.5.7 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.

12.4.5.7.1 Syntax

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

12.4.5.7.2 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
<i>Pattern</i> (optional)	1 to 8 hexadecimal bytes to use for loopback data (for example: 1a2b3c4d)

12.4.5.7.3 Example Command

```
elxvcpcmd.exe v=<vcenter_server> u=<vc_username> p=<vc_password> h=<esx_host> loopbacktest 00-00-c9-93-2f-9f 4 120 0
```

12.4.5.8 posttest

This command runs the POST on a specified FC port.

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

12.4.5.8.1 Syntax

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

12.4.5.8.2 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.

12.4.5.9 setbeacon

This command turns the beacon on or off.

12.4.5.9.1 Syntax

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

12.4.5.9.2 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

12.4.6 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.

12.4.6.1 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.

12.4.6.1.1 Syntax

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

12.4.6.1.2 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 <code>.dpv</code> file (stored in the Emulex Repository directory)
Flag	G = Makes change global (all adapters on this host) N = Makes change non-global (adapter-specific)

12.4.6.2 getdriverparams

This command shows the driver parameters of the specified port.

12.4.6.2.1 Syntax

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

12.4.6.2.2 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.

12.4.6.3 getdriverparamsglobal

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

12.4.6.3.1 Syntax

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

12.4.6.3.2 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.

12.4.6.4 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 those 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.

12.4.6.4.1 Syntax

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


12.4.6.4.2 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)

12.4.6.5 setdriverparam

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

12.4.6.5.1 Syntax

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

12.4.6.5.2 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 re-boot) T = Temporary.
Param	The name of the driver parameter.
Value	The value of the driver parameter.

12.4.6.6 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.

12.4.6.6.1 Syntax

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

12.4.6.6.2 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 re-boot)
T = Temporary.

12.4.7 Dump Commands

The Dump commands initiate a core 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.

12.4.7.1 deletedumpfiles

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

12.4.7.1.1 Syntax

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

12.4.7.1.2 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.

12.4.7.2 dump

This command performs a core 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>.core
```

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

```
Dump Successful.
```

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

12.4.7.2.1 Syntax

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

12.4.7.2.2 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.

12.4.7.3 getdumpdirectory

This command shows 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.

12.4.7.3.1 Syntax

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

12.4.7.3.2 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.

12.4.7.4 getdumpfilenames

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

12.4.7.4.1 Syntax

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

12.4.7.4.2 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.

12.4.7.5 getretentioncount

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

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

12.4.7.5.1 Syntax

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

12.4.7.5.2 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.

12.4.7.6 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.

12.4.7.6.1 Syntax

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

12.4.7.6.2 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.

12.4.7.6.3 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
```

This example shows the dump directory set to `/vmfs/volumes/vcenter-datastore`.

12.4.7.7 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.

12.4.7.7.1 Syntax

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

12.4.7.7.2 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.

12.4.8 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.

12.4.8.1 firmwareupdate

The `firmwareupdate` command updates firmware on the Emulex adapters found in the specified VMware cluster or the ESXi host. See [Section 12.4.4.2, firmwareupdate](#).

12.4.8.2 getfwparams

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

12.4.8.2.1 Syntax

```
elxvcpcmd.exe v=<vcenter_server> u=<vc_username> p=<vc_password> h=<esxi_host> getfwparams <WWPN of the FC function on the adapter>
```

12.4.8.2.2 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 with Emulex adapters.
WWPN	The WWPN of the FC function on the adapter.

12.4.8.2.3 Example

```
elxvcpcmd.exe 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		0	1	0	1	5
2		0	1	1	1	1
3		0	1	0	0	1

12.4.8.3 setfwparams

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

12.4.8.3.1 Syntax

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

12.4.8.3.2 Parameters

- WWPN** The World Wide Port Name of FC function on the adapter.
- Param Name** The name of the parameter 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 12.4.8.2, getfwparams](#) for more information about the `getfwparams` command.

12.4.8.3.3 Example

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

12.4.9 Target and LUN Commands

The Target and LUN commands show the LUNs that support ExpressLane and their status, and also show LUNs attached to the target of the port.

12.4.9.1 getexpresslanelunlist

This command shows the LUNs that support ExpressLane and their respective ExpressLane status, and is supported on LPe16000-series, LPe31000-series, and LPe32000-series adapters only.

NOTE: Only LUNs that support ExpressLane are shown by this command. LUNS without ExpressLane support are not shown.

12.4.9.1.1 Syntax

```
elxvcpcmd.exe v=<vcenter_server> u=<vc_username> p=<vc_pwd> h=<ESXhostIP> getexpresslanelunlist  
<WWPN> <Target_WWPN> <Option>
```

12.4.9.1.2 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 connected to the target.
Target WWPN	The WWPN of the target.
Option	Valid options: 0 = Get information from the driver. 1 = Get information from configuration.

12.4.9.1.3 Example

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

12.4.9.2 getlunlist

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

12.4.9.2.1 Syntax

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

12.4.9.2.2 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.

12.4.9.2.3 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
```

12.4.9.3 setexpresslanelunstate

NOTE: This command has been deprecated. Use the `SetLunXLaneConfig` command to configure ExpressLane. The setting has been saved to both the driver and configuration to match the behavior of the `SetLunXLaneConfig` command.

This command enables and disables ExpressLane on a particular LUN, and is supported on LPe16000-series, LPe31000-series, and LPe32000-series adapters only.

NOTE: A masked LUN cannot be enabled for ExpressLane.

12.4.9.3.1 Syntax

```
setexpresslanelunstate <WWPN> <Target_WWPN> <Lun> <State> <Option>
```

12.4.9.3.2 Parameters

WWPN	The WWPN of the port connected to the target.
Target WWPN	The WWPN of the target.
Lun	LUN number to enable/disable ExpressLane.
State	0 = Disable ExpressLane. 1 = Enable ExpressLane.
Option	Valid ExpressLane options: 0 = Set ExpressLane LUN state in driver (active). 1 = Set ExpressLaneLUN state in configuration (persist across reboots). 2 = Set ExpressLane LUN state in both (driver and configuration).

12.4.9.3.3 Example Commands

The following command enables ExpressLane for LUN 2 on specified target, in the driver and configuration.

```
elxvpcmd.exe v=10.192.000.000 u=user p=password h=10.192.87.198 setexpresslanelunstate  
10:00:00:00:00:87:01:98 20:22:d4:ae:52:6e:6f:08 2 1 2
```

The following command enables ExpressLane for LUN 2 on a specified target, in the driver only. After a reboot, a LUN is not an ExpressLane LUN.

```
elxvpcmd.exe v=10.192.000.000 u=user p=password h=10.192.87.198 setoaslanstate  
10:00:00:00:00:87:01:98 20:22:d4:ae:52:6e:6f:08 2 1 0
```

The following command disables ExpressLane for LUN 2 on a specified target, in the driver and configuration.

```
elxvpcmd.exe v=10.192.000.000 u=user p=password h=10.192.87.198 setoaslanstate  
10:00:00:00:00:87:01:98 20:22:d4:ae:52:6e:6f:08 2 0 2
```

The following command disables ExpressLane for LUN 2 on a specified target, in the driver only. Assuming this is configured to be an ExpressLane LUN, after a reboot LUN 2 is an ExpressLane LUN again.

```
elxvpcmd.exe v=10.192.000.000 u=user p=password h=10.192.87.198 setoaslanstate  
10:00:00:00:00:87:01:98 20:22:d4:ae:52:6e:6f:08 2 0 0
```

12.4.9.4 GetLunXLaneConfig

This command displays the frame priority value for ExpressLane LUNs on the specified target.

Syntax

```
GetLunXLaneConfig <WWPN> [vport=<vPort_WWPN>] <Target_WWPN> <Option>
```


Parameters

WWPN	World-wide port name of any function on the adapter.
vPort WWPN	The WWPN of an optional vPort.
Target WWPN	The WWPN of the target connected to the LUNs.
Option	0 = Get the information from the driver. 1 = Get the information from the configuration.

12.4.9.4.1 Example Command

```
GetLunXLaneConfig 10:00:00:00:c9:55:55:56 50:06:01:60:10:20:5C:38 0
```

Supported Priority Levels: High, Medium, Low

FCP_LUN	OS_LUN	Priority Level	Priority Value
0000 0000 0000 0000	0	High	113
0001 0000 0000 0000	1	High	113
0002 0000 0000 0000	2	Medium	92
0009 0000 0000 0000	9	Low	53

12.4.9.5 SetLunXLaneConfig

If the adapter and switch support it, the `SetLunXLaneConfig` command enables you to configure the ExpressLane Optimized Access Storage (OAS) state and the frame priority levels, or values, for ExpressLane LUNs. Switches can provide up to three priority levels, Low, Medium, and High, but they might provide fewer options.

NOTE: If the switch connected to the initiator does not support LUN-specific frame priority levels using the Get Fabric Object (GFO), you must manually enter the frame priority values in the range of 0–127 for all ExpressLane-enabled LUNs.

You can also use the `SetLunXLaneConfig` command to disable ExpressLane on all LUNs in a single operation.

Use the `GetLunXLaneConfig` command to determine if frame priority levels are supported.

The following rules apply when using the `SetLunXLaneConfig` command:

- The ExpressLane (OAS) state and priority levels, or values, will be automatically saved to both the driver and configuration settings. You cannot specify where to save the configuration.
- The priority parameter is only required if the ExpressLane state parameter is set to 1 (enable).
 - You cannot disable the ExpressLane OAS state with the priority level, or value, parameter set.
 - You cannot disable all LUNs with the priority level, or value, parameter set.
- The `EnableXLane` driver parameter must be enabled.

Syntax

```
SetLunXLaneConfig <WWPN> [vport=<vPort_WWPN>] <Target_WWPN> <LUN> <State>  
<PriorityLevel|PriorityValue>
```

Parameters

WWPN	The World-wide port name of any function on the adapter.
vPort WWPN	The WWPN of an optional vPort.
Target WWPN	The WWPN of the target connected to the LUNs.

LUN	The LUN number. (The OS_LUN from the <code>GetExpressLaneLunList</code> command to set.) Use ALL to disable ExpressLane for all LUNs.
State	0=disable ExpressLane, 1=enable ExpressLane.
PriorityLevel	The levels are high, medium, or low. (Use the <code>GetSmartSanPriorities</code> command to get an accurate list of the supported priority levels.) This value must be omitted if the State = 0.
PriorityValue	A value within the range of 0–127. This value is only allowed if priority levels are not supported by the switch. This value must be omitted if the State =0.

12.4.9.5.1 Example Command

```
SetLunXLaneConfig 10:00:00:00:c9:55:55:56 50:06:01:60:10:20:5C:38 0 1 low
```

ExpressLane configuration successfully changed on the specified LUN(s)

12.4.9.6 targetmapping

See [Section 12.4.9.6, targetmapping](#).

12.4.10 Virtual Machines Commands

12.4.10.1 listvms

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

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 only displayed 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.

12.4.10.1.1 Syntax

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

12.4.10.1.2 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.

12.4.10.2 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.

12.4.10.2.1 Syntax

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

12.4.10.2.2 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.

12.4.11 WWN 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.

12.4.11.1 changewwn

This command changes the WWN of the specified port.

12.4.11.1.1 Syntax

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

12.4.11.1.2 Parameters

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.
v	The vCenter server IP address.
u	The user name for the vCenter server.
p	The user password for the vCenter server.

12.4.11.2 getwwncap

See [Section 12.4.2.4, getwwncap](#).

12.4.11.3 readwwn

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

12.4.11.3.1 Syntax

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

12.4.11.3.2 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.

12.4.11.4 restorewwn

This command restores the WWN value of the specified port.

12.4.11.4.1 Syntax

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

12.4.11.4.2 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.

12.5 Viewing Audit Logs Using the CLI Command

You can use the `elxvcpaudit.exe` script to log all the historical active management performed through the console on the 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.

12.5.0.0.1 Syntax

```
elxvcpaudit.exe <event_name>
```

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

12.5.0.0.2 Parameter

event name The command name describing the appropriate active management action performed.

12.5.0.0.3 List of Supported Event Names

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

12.5.0.0.4 Example

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

Copyright (c) 2012 Steve Jin. All Rights Reserved.

Copyright (c) 2008 VMware, Inc. All Rights Reserved.

Copyright (c) 2009 Altor Networks. All Rights Reserved.

Copyright (c) 2009 NetApp. All Rights Reserved.

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.

