

Emulex OneCommand Manager Application for Linux

Release Notes

Version: 10.3.135.0

Systems: SLES 10 SP3-SP4
SLES 11 SP2-SP3
SLES 12
RHEL 5.8-RHEL 5.11
RHEL 6.4-6.6
RHEL 7.1

Date: April 2015

Purpose and Contact Information

These release notes describe the new features, resolved issues, known issues, and technical tips associated with this Emulex OneCommand® Manager application version for the Emulex® drivers for Linux release. For the latest product documentation, go to www.Emulex.com. If you have questions or require additional information, contact an authorized Emulex technical support representative at tech.support@emulex.com, 800-854-7112 (US/Canada toll free), +1 714-885-3402 (US/International), or +44 1189-772929 (Europe, Middle East, and Africa).

New Features

1. Adds support for Linux Red Hat Enterprise (RHEL) 5.1, 6.6, and 7.1.
2. Adds support for SUSE Linux Enterprise Server (SLES) 12.

Resolved Issues

1. On IBM systems that are Unified Extensible Firmware Interface (UEFI) 2.1 compliant, changes to any settings configured using the Emulex OneCommand Manager application on LPe12000-series adapters, OCe11102 adapters, OCe14000-series adapters, and LPe16000-series adapters persist correctly across reboots.

Known Issues

1. **Known Issues regarding updating firmware.**

The following notes apply to updating firmware on OCe14000-series adapters for this release.

- Once an adapter has been flashed to firmware version 10.2.261.36 or later, do not attempt to flash down to an older version without first contacting IBM support. IBM support will provide a special required downgrade flash procedure. If this procedure is not followed, there is risk in making the adapter permanently unusable.
- If the adapter in use is currently running firmware 10.0.803.2202 or earlier and iSCSI boot firmware table (iBFT) functionality is required, special steps must be followed when

upgrading to this release. The recommended flash method is to use the Emulex OneConnect Offline Flash ISO, which will allow flashing in a single step.

- To upgrade and enable iBFT functionality with online tools, the most recent version of the network interface card (NIC) driver, the OneCommand Manager application, and the Emulex CIM Provider must first be installed. Additionally, the firmware must be flashed twice with a reboot after each flash.

Some online flash utilities, such as the OneCommand Manager application, may instruct you to reboot and flash the firmware a second time. If iBFT functionality is not required, this message can be safely ignored. No additional procedures are necessary when iBFT functionality is not required.

2. **The *OneCommand Manager Application User Manual* and the *OneCommand Manager Command Line Interface User Manual* include information about concurrent mode or concurrent storage. This feature is not supported in this release.**
3. **For OCe14000-series adapters with single root I/O virtualization (SR-IOV) enabled, changing a NIC configuration to a NIC + RDMA over Converged Ethernet (RoCE) configuration results in an error 114 and the configuration is not changed.**

Workaround

Before changing to the NIC + RoCE configuration, disable SR-IOV on all NIC functions.

- To disable SR-IOV in the OneCommand Manager application:
 - a) Select **Host** view.
 - b) Select a NIC port in the discovery-tree.
 - c) Select the **Port Information** tab.
 - d) Uncheck the **Enable SR-IOV** checkbox.
- To disable SR-IOV using the OneCommand Manager CLI:

Use the SRIOVEnable command to disable SR-IOV. As an example, the following command disables SR-IOV on NIC physical function with MAC address 00-00-c9-12-34-56:

```
hbacmd SRIOVEnable 00-00-c9-12-34-56 0
```

4. **On the Channel Management tab, the OneCommand Manager GUI application always shows the permanent Media Access Control (MAC) address for each channel.**

Workaround

View the Port Information tab. The Port Information tab always shows the current (user-settable) MAC address and the permanent MAC address.

5. **The OneCommand Manager GUI application does not show the operating system (OS) Device Name for logical unit numbers (LUNs) attached to vPorts.**

The LUN Information tab, Mapping Information area, OS Device Name field shows: "N/A" instead of the device name. All other information on the LUN Information tab is displayed correctly.

Workaround

None.

6. Creating OneCommand Manager Secure Management users and groups after the OneCommand Manager application is installed in Secure Management mode causes the GUI to fail.

If the OneCommand Manager Secure Management users and groups are created after the OneCommand Manager application has been installed in Secure Management mode, when you attempt to start the OneCommand Manager application GUI as a member of this group, the GUI does not run. The following error message is displayed by the operating system:

```
-Bash: /usr/sbin/ocmanager/ocmanager: Permission denied
```

Workaround

Do one of the following:

- Create the users and groups before you install the OneCommand Manager application in Secure Management mode.
- Uninstall and reinstall the OneCommand Manager application.

7. OneCommand Manager Secure Management mode on Linux systems require Pluggable Authentication Modules (PAM) authentication configuration on the host machine.

In OneCommand Manager Secure Management mode, a user is authenticated on the machine at OneCommand Manager application GUI startup. This is handled via the PAM interface. The /etc/pam.d/passwd file "auth" section or its earlier equivalent must be configured.

Note: Refer to the *OneCommand Manager Application User Manual* for more information about Secure Management mode.

8. Installing the OneCommand Manager application on a guest operating system prompts for a management mode.

When installing the OneCommand Manager application on a guest operating system running on a virtual machine, the installer prompts you for a management mode (e.g. local-only, full-remote, Secure Management, etc.) and read-only mode. However, when the OneCommand Manager application runs on a guest operating system it runs in local-only and read-only modes, so it does not matter how these modes are specified during installation.

Workaround

None.

9. Some RHEL 6.x versions are not configured by default to return LDAP group user membership.

By default, some versions of RH6.x do not return the Lightweight Directory Access Protocol (LDAP) group user membership along with the LDAP group info for LDAP client machines, as can be evidenced by inspecting the output of the "getent group" Linux command.

Workaround

To work with OneCommand Manager Secure Management, these machines must be configured such that the "getent group" command returns not only the groups configured on the machine or domain but also each group's users. Otherwise, OneCommand Manager Secure Management requires the OneCommand Manager group to be the user's primary group to provide the OneCommand Manager Secure Management function.

10. SR-IOV: Running the OneCommand Manager application on a guest operating system with more than one virtual function causes all NIC ports to appear under a single adapter.

If you assign NIC virtual functions from adapters to a virtual machine and run the OneCommand Manager application in the virtual machine's guest operating system, the NIC functions appear under a single adapter node in the OneCommand Manager application discovery-tree. In this situation, the guest operating system in a virtual machine reports the same Peripheral Component Interconnect (PCI) bus number for all virtual functions and the OneCommand Manager application incorrectly determines that each of the discovered NICs are from the same adapter.

Workaround

None.

11. Performing a core dump command may fail if a world wide port name (WWPN) is specified.

When performing a core dump operation in the OneCommand Manager command line interface (CLI) and specifying a Fibre Channel WWPN to indicate which adapter to dump, the command fails if the adapter is in a "down" state.

Workaround

Always use the MAC address for one of the NIC ports on the adapter in the core dump command.

12. On OCe11100-series adapters, if the Mode is set to Force and the Speed is set to 1Gb, do not perform a MAC loopback test in the OneCommand Manager application.

If you perform a MAC loopback test, the link does not come back up after the test is performed.

Workaround

None.

13. If you enable Dynamic Host Configuration Protocol (DHCP) for iSCSI ports from the Modify TCP/IP Configuration dialog box (under the Port Information tab) and if virtual local area networking (VLAN) is already enabled, a TCP over Internet Protocol (TCP/IP) address may not be obtained from the DHCP server (remaining 0.0.0.0): IP address, subnet mask and gateway address.

You may encounter this known issue if your DHCP Server is not VLAN-aware or is not configured for VLAN.

Workaround

Use one of the following workarounds:

- Use a DHCP Server that is VLAN-aware and properly configured.
- Follow these steps to disable and enable DHCP and VLAN:
 - a) On the Port Information tab, click **Modify**. The Modify TCP/IP Configuration dialog box is displayed.
 - b) Clear the **VLAN Enabled** and **DHCP Enabled** check boxes.
 - c) Click **OK**. The Port Information tab is displayed.
 - d) On the Port Information tab, click **Modify**. The Modify TCP/IP Configuration dialog box is displayed.

- e) On the Modify TCP/IP Configuration dialog box, check the **VLAN Enabled** and **DHCP Enabled** check boxes and click **OK**.

14. OneConnect installation path order recommendation.

When installing new OCe11102 adapter driver and firmware versions, it is best to install both the driver and the firmware without rebooting between installations to minimize the possibility of operating with mismatched versions of driver and firmware.

Workaround

None.

15. The NIC driver must be installed to run the OneCommand Manager application on OneConnect adapters.

If the OneConnect adapter is run without the NIC driver installed and enabled, many of the management functions are unavailable and erroneous/corrupted information is displayed by the OneCommand Manager application.

The management functions that are unavailable are:

- Firmware
 - Core dump
 - Download
 - All diagnostics, including beaconing and diagnostic dumps
 - Disabling or enabling a port
- Erroneous display information includes:
 - FCoE storage ports are incorrectly grouped under the physical port
 - NIC, FCoE, and iSCSI ports do not appear under the correct adapter
 - Active and flash firmware versions
 - Firmware status
 - BIOS version
 - Boot code version
 - Transceiver data display
 - Physical port link status
 - All Converged enhanced Ethernet (CEE) settings
 - Event log display (OneCommand Manager CLI only)
 - Adapter temperature

Workaround

The NIC driver must always be installed on OneConnect adapters.

16. Requirement for unloading or loading Emulex device drivers (FC/FCoE, NIC and iSCSI).

If you load or unload an Emulex device driver for Linux (FC/FCoE, NIC and iSCSI) after the machine is rebooted, you must perform the following steps in the following order:

- a) Close any open OneCommand Manager applications.
- b) Restart OneCommand Manager application daemons. To restart OneCommand Manager application daemons, the daemons must be stopped and started.
 - i) Run the `/usr/sbin/ocmanager/stop_ocmanager` script.
 - ii) Run the `/usr/sbin/ocmanager/start_ocmanager` script.

- c) Run the Emulex OneCommand Manager application GUI and/or the OneCommand Manager CLI client applications.

17. If both VLAN and Data Center Bridging Capabilities Exchange (DCBX) are disabled, the iSCSI priority configured in the DCB tab is not set in the iSCSI packets sent out by the port.

Workaround

Enable or disable VLAN from the iSCSI Port Info tab in the OneCommand Manager application.

18. Possible interference with the OneCommand Manager applications ability to permanently change WWNs.

Some newer adapters (for example, CNAs) on some newer systems employ techniques in the BIOS code at boot time to configure the adapter, such as the adapter WWN. In such cases, this may interfere with the OneCommand Manager application's ability to make permanent (non-volatile) changes to the adapter's WWN.

Workaround

None.

19. iSCSI InitialR2T is not supported for iSCSI OneConnect adapters.

Although both the OneCommand Manager application GUI and the OneCommand Manager CLI (hbacmd) clients allow the configuring of the "iSCSI InitialR2T" parameter to "yes" or "no", the adapter does not recognize the setting. The adapter always operates with "iSCSI InitialR2T" set to "yes".

Workaround

None.

20. Messages appear on the terminal during Web-Launch install or uninstall.

On Linux SLES11 SP2 systems, when the OneCommand Manager Web-launch component is installed or uninstalled using wsinstall and wsuninstall scripts respectively, the following messages are displayed to the terminal.

```
insserv: Script jexec is broken: incomplete LSB comment.  
insserv: missing `Required-Stop:' entry: please add even if empty.
```

These are warning messages that do not affect the operation or installation of the Web-launch component. They appear on SLES 11 SP1 specific versions of the relevant software (insserv and jexec). The scripts invoke this software via invocation of the standard Linux chkconfig utility typically used for daemon installations.

Workaround

None.

21. On SLES 11 systems, the Open-FCoE RPM Package Manager (RPM) package (open-fcoe-1.0.4-10.2) is incompatible with the OneCommand Manager application package and must be removed from the target host machine.

The HBA API library that the open-fcoe package installs (libhbalinux.so.1) causes all OneCommand Manager application processes to crash with a segmentation violation.

Workaround

To recover you must reinstall OneCommand Manager application without loading the Open-FCoE package.

- 22. On SLES 11 systems, installing or uninstalling the Open-FCoE RPM package after the OneCommand Manager application is installed, removes OneCommand Manager application entries in the system file in the /etc/hba.conf file.**

This breaks the Linux system HBA API functionality and as a result, the OneCommand Manager application client applications no longer run.

Workaround

Re-install the OneCommand Manager application.

- 23. On RHEL host systems and on Citrix 5.6 and later host systems, the OneCommand iSCSI Simple Network Management Protocol (SNMP) daemon does not start if the libsensors shared object library is not found (for example, if libsensors RPM package is not installed).**

Workaround

Install the libsensors RPM package off the appropriate RHEL or Citrix distribution and restart the OneCommand iSCSI SNMP daemon.

- 24. On some RHEL x86_64 and ppc 64 systems, uninstalling the Red Hat 32-bit or 64-bit libhbaapi RPM deletes entries in the /etc/hba.conf hbaapi configuration file thereby disabling OneCommand Manager hbaapi layer.**

Workaround

Re-install the OneCommand Manager application.

- 25. Unloading the NIC driver from a Linux machine causes the OneCommand Manager application to lose connectivity.**

If you unload the NIC driver from a Linux machine, any OneCommand Manager application (GUI or OneCommand Manager CLI client) running on the machine loses connectivity with the NIC and related configuration data.

Workaround

To recover, you must perform the following steps in the following order:

- a) Stop the OneCommand Manager applications and daemons using the stop_ocmanager script.
 - b) Reload the NIC driver using modprobe.
 - c) Restart the OneCommand Manager application daemons using the start_ocmanager script.
 - d) Restart the OneCommand Manager application GUI or OneCommand Manager CLI client).
- 26. When Management Interface Library (MILI) and SNMP daemons start, they trigger warning messages within SELinux for certain operations.**

Workaround

To avoid SELinux warning messages, disable SELinux.

- a) To disable SELinux, open a terminal and enter the following command at the prompt:

```
echo 0 > /selinux/enforce
```

- b) To enable SELinux, open a terminal and enter the following command at the prompt:

```
echo 1 > /selinux/enforce
```

27. A permanent driver parameter change fails if the system is rebooted too soon.

When you make permanent driver parameter changes via the OneCommand Manager application, the application automatically makes the required entry in the `/etc/modprobe.conf` or equivalent file. Because the LPFC driver loads so early in the Linux machine boot sequence, the new contents of the `/etc/modprobe.conf` file must be re-inserted into the Linux system `initrd` file (via “`mkinitrd`” utility) for the driver to pick up the new driver parameter value on the next boot. Failure to generate the new `initrd` file causes the driver to fail to get the new driver parameter value on subsequent driver loads (machine boots). The OneCommand Manager application automatically does this for you (re-creates `initrd` via `mkinit` function); however, it can take as long as 45-60 seconds after the driver parameter is changed for a complete `initrd` re-build. If you reboot the machine immediately after the driver parameter change is made, the auto-recreation of the `initrd` file by the OneCommand Manager application may fail to complete. In these cases, this failure causes the driver to “not obtain” the new driver parameter value upon subsequent reboots.

Workaround

Wait a minimum of 45-60 seconds after making the driver parameter change before rebooting the machine.

28. Newly added LUNs on a storage array may not appear on the host machine Linux operating system or the OneCommand Manager application.

Workaround

Do one of the following:

- Run the following script from the command shell:

```
/usr/sbin/lpfc/lun_scan all
```
- Reboot the host machine after the LUN has been added at the target array.

29. When using IET software, target portals with more than 60 iSCSI targets may not be discovered.

When using the open source iSCSI Enterprise Target (IET) software package to present targets to the iSCSI initiator, adding target portals that contain greater than 60 targets fails the resulting target discovery operation. This is the result of an error in the IET target implementation.

Workaround

None.

30. Logged in iSCSI targets retain login options through reboots.

When an iSCSI target is discovered by adding a target portal, that target takes the target portal’s login options. The target portal’s login options are taken from the initiator login options. However, you can modify them when adding a target portal. If a target is discovered by iSNS, it gets its default login options from the initiator login options.

Once a target is discovered, its login properties are not changed when the initiator login options are changed. When you log into a target, the login properties used at the time of

login are remembered. If you reboot, the logged in targets are logged in again with the remembered login options (initiator login options are not used).

When you remove the targets (and the target portal if that is how they were discovered) and then cause the targets to be rediscovered, the targets login properties are defined once again by how they are discovered as described at the beginning of this known issue.

Workaround

None.

31. On RHEL 6.0, 6.1, and 6.2 systems, an issue exists with the Java Runtime that may result in the inability to run the OneCommand Manager application on a RHEL 6.x host.

This problem usually occurs on Blade platforms. This issue causes the OneCommand Manager application to crash immediately upon invocation.

Workaround

Use one of the following management methods:

- Manage the problematic RHEL 6.x host from a remote host that is running the OneCommand Manager application.
- Install WebLaunch services on the RHEL6.x host, then point a browser on another host to that RHEL 6.x host.

32. Set Link Speed Issue exists after a small form-factor pluggable (SFP) Hot Swap.

The LPe16000 family of adapters does not support SFP hot swap if the replacement SFP is not the same model as the original SFP. There are two ramifications in the OneCommand Manager application:

- The Port Attributes tab in the OneCommand Manager application or the OneCommand Manager CLI “PortAttributes” command may display incorrect data for the Supported Link Speeds attribute. This issue is cosmetic.
- Boot From SAN Management may be unable to set the Boot Code Link Speed parameter to 16 Gb/s.

Workaround

After changing the SFP, reset the LPe16000 port or reboot the server.

33. Loopback diagnostics are not supported on LPe1600x FC HBAs.

The OneCommand Manager application internal and external loopback diagnostic tests are not supported for the LPe1600x FC HBA.

Workaround

Use the PCI loopback diagnostic test, which is an abbreviated form of the internal and external loopback diagnostic tests. This workaround is not available on earlier versions of Linux (RHEL 5.5, 5.6, and 5.7, and SLES 10.3 and 10.4).

34. The Web Launch browser client must be run with administrator or root privileges.

When running the OneCommand Manager Web Launch GUI, you must have administrator privileges when logged into the Web Launch client user. On a Linux browser client, you must be logged in as the 'root' user. Unusual behavior may occur if this requirement is not met.

Workaround

None.

35. Vital Product Data (VPD) is required on NIC-only and iSCSI adapters.

Once you license a FCoE personality on an existing NIC-only or iSCSI adapter, you must make sure that the adapter has VPD written on it. Otherwise, FCoE management does not work in the OneCommand Manager application. Only older adapters of these types do not have VPD.

Workaround

None.

36. Dump command on a boot-from-SAN adapter causes a system panic.

When the OneCommand Manager application performs a dump of an adapter that is booting from SAN and has no failover support, the operating system crashes when the adapter is taken offline to perform the boot and write the dump file to the host file system. The file system is unavailable because the adapter was taken offline.

Workaround

Before performing a dump of an adapter, ensure that the desired adapter is not a boot-from-SAN adapter. Alternatively, provide failover support so when the adapter is taken offline to perform the dump, the boot-from-SAN connection is maintained by the failover.

37. The OneCommand Manager application elxhbmgrd daemon can take up to 30 seconds to stop.

The OneCommand Manager application elxhbamgrd daemon process may take up to 30 seconds to stop when attempting to kill it. This applies to SLES 11 SP1 and RHEL 6.0 and all subsequent Linux distributions corresponding to the 8.3.x LPFC driver versions.

Workaround

None. The behavior of the elxhbmgrd daemon is linked with the MAX time out the Linux kernel associates with SCSI BSG interface commands and the OneCommand Manager application register for events function.

Technical Tips

1. **The OneCommand Manager application no longer installs OneCommand Vision components.**

2. **FC in-band management is no longer supported.**

3. **Diffie-Hellman Challenge Handshake Authentication Protocol (DH-CHAP) authentication is no longer supported.**

There is no support for DH-CHAP authentication for the RHEL 6.0 and RHEL 6.1 and subsequent Linux distributions. The kernel has removed this technology from the FC device driver module layer.

4. **You can open multiple instances of the OneCommand Manager GUI application on a single system. Although it causes no problems, this practice is not recommended.**

5. **Requirement if Data Center Bridging (DCB) settings are connected to a non-DCBX switch.**

If DCB settings are required when connected to a non-DCBX switch (or a switch with DCBX disabled), DCBX must be disabled on the OneConnect adapter to use the adapter's configured parameters. If DCBX is enabled, DCB PFC and Priority Groups are ignored (the adapter assumes the switch does not support these parameters) and for FCoE adapters, the FCoE priority (COS) is 3.

6. **The “HbaCmd UmcEnableChanLink” command has been removed.**

To enable the logical link status of a channel, use the “CMSetBW” command to set the minimum bandwidth to a value greater than 0. To disable the logical link status, set the minimum and maximum bandwidth to 0.

7. **Emulex SR-IOV features are available on SLES11 distributions beginning with the SP2 release.**

The OneCommand Manager application support for displaying the SR-IOV virtual functions on the base operating system are provided on SLES11 distributions beginning with the SP3 release.

8. **Roles based Secure Management mode is available.**

Secure Management mode is a management mode available with this release. It is a roles based security implementation. During the OneCommand Manager application installation, a user is prompted as to whether or not to run in Secure Management mode. When the OneCommand Manager application is installed in this mode, the following changes occur:

- A non-root or non-administrator user can now run the OneCommand Manager application.
- The OneCommand Manager application host uses a user's credentials for authentication.
- A user has OneCommand Manager application configuration privileges according to the OneCommand Manager application group to which the user is assigned.
- In Secure Management mode, a root or administrator user is provided full privileges on the local machine (CLI does not require credentials) but no remote privileges.

Note: Refer to the *OneCommand Manager Application User Manual* for more information on Secure Management mode.

9. **OneCommand Manager Secure Management mode requires OneCommand Manager user groups be configured on the domain or if the host is not running in a domain, the host machine.**

OneCommand Manager Secure Management must be able to get the OneCommand Manager application group to which the user belongs from the host's domain (Active Directory or Lightweight Directory Access Protocol [LDAP]) or if the host is not part of a domain, the host's local user accounts. This access is associated with user groups, not with specific users. Administrators set up user accounts such that a user belongs to one of these four OneCommand Manager application user groups:

Table 1 Secure Management User Privileges

User Group	OneCommand Manager Application Capability
ocmadmin	Allows full active management of local and remote adapters.
ocmlocaladmin	Permits full active management of local adapters only.
ocmuser	Permits read-only access of local and remote adapters.
ocmlocaluser	Permits read-only access of local adapters.

These four OneCommand Manager application groups must be created and configured on the host machine or network domain. OneCommand Manager Secure Management uses the C-library API calls 'getgrnam' and 'getgrid' to retrieve the OneCommand Manager Secure Management group information. The equivalent to these can be obtained on the shell command line by typing the "getent group" command. If the four OneCommand Manager application groups are listed, along with their member users, this is an indication that the host machine is sufficiently configured to work with OneCommand Manager Secure Management.

10. **On 8Gb/s and lower FC adapters, the OneCommand Manager application Firmware tab is in a different location than with 16 Gb/s FC adapters and 10 Gb/s CNA adapters.**

Because the 16 Gb/s and 10 Gb/s adapters share a single firmware image for all ports on the adapter, the Firmware tab for 16 Gb/s and 10 Gb/s adapters is at the adapter level. Because 8 Gb/s and lower adapters have a separate firmware image for each individual port, the Firmware tab for 8 Gb/s and lower adapters is at the port level.

11. **An end-to-end (ECHO) diagnostic test fails if the corresponding targets are not supported.**

Check to be sure the connected targets are supported.

12. **To view online help using the Google Chrome browser, you must disable Chrome's security check using the "--allow-file-access-from-files" option.**

- a) Create a copy of the Chrome shortcut on the desktop and rename it to RH Chrome L.
- b) Right-click on the new Chrome icon and choose **Properties**.
- c) Add the "--allow-file-access-from-files" text to the end of the path appearing in Target. You must leave a space between the original string and the tag you are adding to the end of it.
- d) Click **OK** to save your settings.
- e) Close any open instances of Chrome.

- f) To open a local copy of the online help, use the new shortcut to open Chrome, then press **Ctrl + Open** and browse to the start page; or open Chrome with the new shortcut, then right-click the start page and click **Open With > Google Chrome**.
- 13. On OneConnect adapters, if you change the port speed via the Change Port Speed dialog box, and the selected speed is supported by the adapter's port but is not supported by the connected hardware, the link does not come up.**

Copyright © 2012–2015 Emulex. All rights reserved worldwide. This document refers to various companies and products by their trade names. In most, if not all cases, their respective companies claim these designations as trademarks or registered trademarks. This information is provided for reference only. Although this information is believed to be accurate and reliable at the time of publication, Emulex assumes no responsibility for errors or omissions. Emulex reserves the right to make changes or corrections without notice. This report is the property of Emulex and may not be duplicated without permission from the Company.