OneCommand Manager Application for Linux Release Notes

Version: 6.3.14.1

System: SLES 10 SP3–SP4
SLES 11 SP1–SP2
RHEL 5.7–5.9
RHEL 6.1–6.4
CentOS 5.7–5.9
CentOS 6.1–6.4
Oracle Linux 5.5–5.8
Oracle Linux 6.0–6.3
Oracle Linux UEK R1, R2 with OL 6
Oracle Linux UEK R1, R2 with OL 5

Date: June 2013

Purpose and Contact Information

These release notes describe the resolved issues and known issues associated with this OneCommand™ Manager (OCM) 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).

Resolved Issues

1. **You no longer need to unplug the port on the OneConnect™ OCe10102 Universal Converged Network Adapter (UCNA) before running a diagnostic test. Starting a diagnostic test takes the UCNA offline as indicated in the message that is displayed.**

Known Issues

1. **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 bandwidth to 0.

2. **Creating OCM Secure Management users and groups after the OCM application is installed in Secure Management mode causes the GUI to fail.**

   If the OCM Secure Management users and groups are created after the OCM application has been installed in Secure Management mode, when you attempt to start the OCM 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 OCM application in Secure Management mode.
- Uninstall and reinstall the OCM application.

3. **When running OCM Secure Management mode, in-band ports appear in the discovery-tree but cannot be managed.**

   Emulex is beginning the process of phasing out support for in-band discovery in the OCM application. Therefore, this issue will not be fixed.

4. **OCM Secure Management mode on Linux systems require PAM authentication configuration on the host machine.**

   In OCM Secure Management mode, a user is authenticated on the machine at OCM 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.

5. **Installing the OCM application on a guest operating system prompts for a management mode.**

   When installing the OCM 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 OCM 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.

6. **The OCe11101-E UCNA cannot run loopback diagnostic tests (PHY, MAC, External).**

   Any attempt to run a loopback test on the OCe11101-E UCNA fails.

   Workaround

   None.

7. **In-band (FC-CT) remote management operations do not work properly on SLES11 SP1, RHEL 6.0, and Oracle UEK 5.x/6.x systems.**

   In-band (FC-CT) remote management operations that involve transmitting large amounts of data across the wire do not work properly. This includes firmware download and retrieving targets and logical unit numbers (LUNs).

   Workaround

   Emulex recommends that you use out-of-band remote management on the affected Linux distributions.

8. **Changing a driver parameter in permanent mode fails on Linux SLES11 SP1 and SP2 releases.**

   This issue applies to Linux SLES11 SP1 and SLES11 SP2 only. No other Linux releases are affected. When setting a new driver (LPFC) parameter value via the OCM application GUI or OneCommand CLI using the permanent scope (change persists reboots), a failure occurs during the initial RAM disk regeneration of the Linux OS kernel - this is the final part of the OCM application driver parameter setting process.

The permanent driver parameter update via the OCM application involves updating a Linux system level file (/etc/modprobe.conf file) which is part of the initial RAM disk.

Because the initial RAM disk fails to regenerate with the updated contents of the Linux system level file, upon a system reboot (when the Linux LPFC driver is loaded) the older pre-modification driver parameters are in effect.

Workaround

To allow for a successful regeneration of the Linux OS initial RAM disk, set the following symbolic link before updating a driver module parameter with the OCM application:

```
#ln -s /sbin/mkinitrd /sbin/mk_initrd
```

This allows for any desired driver parameter changes to be permanent (persist system reboots).

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

10. **OCM application target LUN reporting can be interrupted during heavy target loading.**

    When reporting FC/FCoE targets, the OCM application discovery process periodically sends “SCSI Inquiry” and “Read Capacity” commands directly to the target LUNs. On some non-enterprise level targets when data I/O loading is heavy, the control plane response (for example, “SCSI Inquiry” and “Read Capacity” requests) can become sluggish. This can cause a temporary interruption in OCM application GUI client reporting of these target LUNs.

    Workaround

    None.

11. **On an OCe11102 series UCNA with a RHEL 6.3 host operating system, the multi-channel LogicalLinkState cannot be enabled or disabled using the OneCommand CLI.**

    Workaround

    None.

12. **SR-IOV: Running the OCM 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 OCM application in the virtual machine’s guest operating system, the NIC functions appear under a single adapter node in the OCM application discovery–tree. In this situation, the guest operating system in a virtual machine reports the same PCI bus number for all virtual functions and the OCM application incorrectly determines that each of the discovered NICs are from the same adapter.

Workaround

None.

13. **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 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.

14. **When RDAC (redundant disk array controller) multipath is installed, the OCM application does not display LUN information correctly. This is caused by issues with the RDAC device driver and the mapping of SCSI block device names to various operating system infrastructures.**

    Workaround

    None.

15. **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 OCM application.**

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

    Workaround

    None.

16. **On OCe11102 series 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.**

    Workaround

    None.

17. **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/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:
      1) On the Port Information tab, click **Modify**. The Modify TCP/IP Configuration dialog box is displayed.
      2) Clear the **VLAN Enabled** and **DHCP Enabled** check boxes.
      3) Click **OK**. The Port Information tab is displayed.

4) On the Port Information tab, click **Modify**. The Modify TCP/IP Configuration dialog box is displayed.
5) Check the **VLAN Enabled** and **DHCP Enabled** check boxes and click **OK**.

18. **OneConnect installation path order recommendation.**

    When installing new UCNA 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.

19. **The NIC driver must be installed to run the OCM application with an FCoE adapter. If the OneConnect FCoE adapter is run without the NIC driver installed, many of the management functions are unavailable.**

    FCoE ports are very closely coupled with their associated NIC ports (associated NIC ports are NIC ports that appear under the same physical port as an FCoE port). Critical information characterizing the FCoE port is retrieved via the associated NIC port. When a NIC port is disabled, Emulex software cannot access the NIC port, thus the information needed to accurately render the discovered FCoE ports cannot be retrieved.

    The management functions that are unavailable are:

    - Firmware
        - Download
        - Active and flash firmware versions
        - Firmware status
        - BIOS version
        - Boot code version
    - All diagnostics including beaconing
    - Transceiver data display
    - Port disable
    - Physical port link status
    - All CEE settings
    - Event log display (CLI only)
    - Diagnostic dumps

    Workaround

    None.

20. **Restriction when assigning DCB priorities to priority groups.**

    Although there are eight priority groups to which priorities can be assigned, you can assign priorities and bandwidths to only two of the priority groups. You must assign the FCoE or iSCSI priority to one priority group and assign the other seven (NIC) priorities to the other priority group.

    Note: If you are using a DCBX enabled switch to configure the priority groups, configure the switch for only two priority groups to work correctly with the OneConnect adapter.

Workaround

None.

21. **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:

    1. Close any open OCM applications.
    2. Restart OCM application daemons. To restart OCM application daemons, the daemons must be stopped and started.
        a) Run the /usr/sbin/ocmanager/stop_ocmanager script.
        b) Run the /usr/sbin/ocmanager/start_ocmanager script.
    3. Run the Emulex OCM application GUI and/or the OneCommand CLI client applications.

22. **If both VLAN and DCBX are disabled, the iSCSI priority configured in the CEE 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 OCM application.

23. **Transceiver data is unavailable for OneConnect OCe1110x UCNAs.**

    The transceiver data is not displayed in the OCM application or the OneCommand CLI for OneConnect OCe1110x UCNAs.

    Workaround

    None.

24. **Possible interference with the OCM 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 OCM application’s ability to make permanent (non-volatile) changes to the adapter’s WWN.

    Workaround

    None.

25. **iSCSI InitialR2T is not supported for iSCSI OneConnect adapters.**

    Although both the OCM application GUI and the OneCommand 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.

26. **In-band FC-CT remote management timeouts may cause the OCM application processes to hang on SLES11 SP1, RHEL 6.0, CentOS 6.0, Oracle UEK 5.x/6.x, or Citrix XS 6.0 systems.**

    Timeouts in the in-band (FC-CT) remote management commands can cause the OCM application processes to hang. These processes report as defunct, cannot be killed, and a reboot is required to recover them. Example causes of these timeouts include cable pulls, server machine reboots, and port disables. This issue has been isolated to the block SCSI generic (BSG) driver in the kernel. A kernel fix is in process.

Workaround

None. Emulex recommends that you avoid using in-band management on the affected Linux distributions.

27. **In-band FC-CT remote management operations may not work properly on SLES11 SP1, RHEL 6.0, CentOS 6.0, and Oracle UEK 5.x/6.x systems.**

    In-band (FC-CT) remote management operations that involve transmitting large amounts of data do not work properly. This includes firmware download and retrieving targets and LUNs.

    Workaround

    None. Emulex recommends that you avoid using in-band management on the affected Linux distributions.

28. **FC-CT commands to the switch that time out can cause the OCM application processes to hang on SLES11 SP1, RHEL 6.0, CentOS 6.0, Oracle UEK 5.x/6.x, or Citrix XS 6.0 systems.**

    The OCM application uses FC-CT commands to the switch name server to obtain local HBA symbolic name information. FC-CT commands to the switch originating from the listed Linux distributions that time out may cause the OCM application process sending the FC-CT command to hang. This issue has been isolated to the block SCSI generic (BSG) driver in the kernel. A kernel fix is in process.

    Scenarios that might result in this behavior include disabling a switch port and modifying VLAN configuration, either on the switch or on the host machine via the OCM application.

    Workaround

    None. This issue has been addressed in the RHEL 6.1 kernel. Inclusion is also expected in SLES11 SP2.

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

    On Linux SLES11 SP1 systems, when the OCM 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.

30. **On SLES 11 SP1 and later systems, the Open-FCoE RPM package (open-fcoe-1.0.4-10.2) is incompatible with the OCM 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 OCM application processes to crash with a segmentation violation. To recover you must reinstall OCM application without loading the Open-FCoE package.

Workaround

None.

31. **On SLES 11 SP1 and later systems, installing or uninstalling the Open-FCoE RPM package after the OCM application is installed, removes OCM 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 OCM application client applications no longer runs.

    Workaround

    Re-install the OCM application.

32. **On RHEL 5.5 and later host systems and on Citrix 5.6 and later host systems, the OneCommand iSCSI 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.

33. **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 OCM hbaapi layer.**

    Workaround

    Re-install the OCM application.

34. **Unloading the NIC driver from a Linux machine causes the OCM application to lose connectivity.**

    If you unload the NIC driver from a Linux machine, any OCM application (GUI or 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:

    1. Stop the OCM applications and daemons using the stop_ocmanager script.
    2. Reload the NIC driver using modprobe.
    3. Restart the OCM application daemons using the start_ocmanager script.
    4. Restart the desired OCM application (GUI or CLI client).

35. **When MILI and SNMP daemons start, they trigger warning messages within SELinux for certain operations.**

    Workaround

    To avoid SElinux warning messages, disable SELinux.

    1. To disable SElinux, open a terminal and enter the following command at the prompt:

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

    2. To enable SElinux, open a terminal and enter the following command at the prompt:

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

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

    When you make permanent driver parameter changes via the OCM 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 OCM 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 OCM 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.

37. **An unaligned access message can appear on the Linux command shell for IA64 systems.**

    When running the OneCommand CLI client on IA64 systems, the following unaligned access message can appear on the Linux command shell:

    ```
    elxdiscoveryd(24489): unaligned access to 0x200...008005f1c,
    ip=0x20...8fa680
    ```

    Workaround

    These messages are informational only and do not cause any inaccuracies in the OCM application configuration or status reporting. These messages are indications that the OCM application code execution is sometimes referencing data aligned to four bytes instead of eight and the IA64 architecture issues a page fault to accomplish it (causing a slight performance hit). These messages can be turned off with the "prtcl" or "dmesg" Linux commands.

38. **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.

    Workaround

    None.

39. **Newly added LUNs on a storage array may not appear on the host machine Linux operating system or the OCM 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.

40. **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.

41. **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.

42. **A physical loopback diagnostic test fails if no transceiver is present on a OneConnect OCe1010x UCNA port.**

    Workaround

    Insert a transceiver into the port before you run a physical loopback diagnostic test.

43. **A MAC loopback diagnostic test may fail on OneConnect OCe10102 UCNA adapters if the Etherlink is up.**

    The MAC loopback diagnostic test may fail if there is heavy TCP/IP traffic on the port.

    Workaround

    Unplug the port on the OneConnect OCe10102 UCNA before running the MAC loopback diagnostic test.

44. **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 OCManager on a RHEL 6.x host.**

    This problem usually occurs on Blade platforms. This issue causes the OCM 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 OCM application.
- Install WebLaunch services on the RHEL6.x host, then point a browser on another host to that RHEL 6.x host.

45. **Set Link Speed Issue exists after a 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 OCM application:

    1. The Port Attributes tab in the OCM application or the OneCommand CLI "PortAttributes" command may display incorrect data for the Supported Link Speeds attribute. This issue is cosmetic.
    2. 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.

46. **Board temperature is unavailable for the LPe16000 family of adapters.**

    The OCM application does not support the board temperature display for the LPe16000 family of adapters on Linux distributions running the version 8.3.x Emulex FC (LPFC) device driver. This includes RHEL 6.x and SLES 11 SPx distributions.

    Workaround

    None.

47. **The OCM application's diagnostic "echo test" is not supported on SLES 11 SP1/SP2, RHEL 6.0/6.1, CentOS 6.0, Oracle UEK 5.x/6.x, and Citrix XS 6.0 systems.**

    Because of an issue that has been isolated to the block BSG driver in the kernel that surfaces when in-band (FC-CT) commands time out, the OCM application's diagnostic echo test is not supported on the affected Linux distributions. The echo test is based on FC-CT remote communications.

    Workaround

    None. Emulex recommends that you avoid using in-band management on the affected distributions.

48. **OneCommand Vision dependency on kernel 'net-snmp' package.**

    OneCommand Vision rpm packages are included with the OCM application installation packages starting with OCM application version 6.0. The OneCommand Vision package has a dependency on the Linux kernel 'net-snmp' rpm package.

    Workaround

    If you want to include OneCommand Vision in the OCM installation, you must first install the 'net-snmp' rpm package from the Linux kernel installation source repository. Otherwise, the OneCommand Vision portion of the installation process causes an error and indicates this dependency. OCM installation remains unaffected.

49. **Loopback diagnostics are not supported on LPe1600x FC HBAs.**

    The OCM 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).

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

    When running the OCM 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.

51. **DH-CHAP authentication is not supported on OneConnect FCoE adapters.**

    There is no support for FCoE Diffie-Hellman Challenge Handshake Authentication Protocol (DH-CHAP) on OneConnect FCoE adapters. In the OCM application, the DH-CHAP tab is not displayed when the FCoE node of a OneConnect port is selected in the discovery tree. In the OneCommand CLI, the authentication commands return an error indicating that the command is not supported when a OneConnect FCoE port is specified.

    Workaround

    None.

52. **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 OCM application. Only older adapters of these types do not have VPD.

    Workaround

    None.

53. **OCM application installation output messages may be misleading for OneCommand Vision installation failures.**

    Newer Linux distributions (for example, RHEL 5.8) may have trouble with OneCommand Vision installations. If you choose to install OneCommand Vision as part of the OCM application installation and there are any installation problems with OneCommand Vision, no installation failure messages are displayed. The message “OneCommand Manager Installation Successful” is displayed regardless of OneCommand Vision installation problems because the OCM application has no dependency on the OneCommand Vision package. However, a OneCommand Vision issue could still exist.

    Workaround

    None.

54. **OCM JRE issue exists on RHEL 6.0, 6.1 and 6.2.**

    OCM application installation and execution on the RHEL 6.0, 6.1 and 6.2 distributions may fail if the standard C++ library file (libstdc++.so.5) is not installed on the machine.

    Workaround

    Install the 64-bit version of the compat-libstdc++ RPM included in the RHEL 6.x distribution. This includes the libstdc++.so.5 shared object library file.

55. **DH-CHAP authentication is not supported for RHEL 6.0, RHEL 6.1, and SLES 11 SP1.**

    There is no support for DH-CHAP authentication for the RHEL 6.0, RHEL 6.1, and SLES 11 SP1 and subsequent Linux distributions. The kernel has removed this technology from the FC device driver module layer.

    Workaround

    None.

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

    When the OCM 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.

57. **The NIC driver that comes in-box with the Linux distribution does not support OCM application management functions.**

    Workaround

    Emulex recommends that you replace the in-box NIC driver on the Linux machine twith a version compatible with the OCM application version associated with the target Linux distribution.

58. **The OCM application elxhbmgrd daemon takes up to 30 seconds to stop.**

    The OCM 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 OCM application register for events function.

Technical Tips

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

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

2. **New roles based Secure Management mode is available.**

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

   - A non-root or non-administrator user can now run the OCM application.

- The OCM application host uses a user's credentials for authentication.
- A user has OCM application configuration privileges according to the OCM 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.

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

   OCM Secure Management must be able to get the OCM 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 OCM application user groups:

   Table 1 Secure Management User Privileges

User Group	OCM 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 OCM application groups must be created and configured on the host machine or network domain. OCM Secure Management uses the C-library API calls 'getgrnam' and 'getgrid' to retrieve the OCM 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 OCM application groups are listed, along with their member users, this is an indication that the host machine is sufficiently configured to work with OCM Secure Management.

   The OCM application Firmware tab is at a different location for 8 Gb/s and lower Fibre Channel adapters, and 16 Gb/s and 10 Gb/s Fibre Channel 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.

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

   Check to be sure the connected targets are supported.

5. **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**.