BROADCOM®

Emulex® OneCommand® Manager Application for Linux
Release 12.4.243.24 and 12.4.243.20

Purpose and Contact Information

These release notes describe the new features, resolved issues, known issues, and technical tips associated with this release of the Emulex® OneCommand® Manager application for Linux.

For the latest product documentation, and for supported driver versions, go to www.broadcom.com. If you have questions or require additional information, contact an authorized Broadcom® Technical Support representative at ecd-tech.support@broadcom.com.

New Features

Release 12.4.243.24

This release adds support for Oracle Linux 8.0.

Release 12.4.243.20

1. This release adds support for RHEL 8.1.

2. This release adds support for SLES 12 SP5.

3. This release adds support for AMD Epyc 7002-series processors (PCIe 4.0).

Resolved Issues

There are no resolved issues in this release.

Known Issues

1. Revision A of the FOIT AFCT-57F3TMZ-ELX (16GFC longwave optic transceiver) does not support D_Port (also called ClearLink®) for Brocade® switches and MDS for Cisco switches.

2. Neither Revision A nor Revision B of the FOIT AFCT-57F3TMZ-ELX (16GFC longwave optic transceiver) or AFCT-57G5MZ-ELX (32GFC longwave optic transceiver) supports D_Port for Brocade switches.

3. To perform a firmware dump on an LPe35000-series adapter with one of the following inbox Linux drivers installed, you cannot use the OneCommand Manager application. You must use the LPe35000-Series HBA Firmware Dump Tool instead. Refer to the *Emulex Drivers for Linux Release Notes* for instructions on using the tool.

    – SLES 15
    – RHEL 7.6 (except the RHEL7.6 errata kernel-3.10.0-990.el7)
    – Ubuntu 18.04 (except the Ubuntu 18.04.3 HWE release)

4. Beginning with software release 11.2, FC HBAs and OneConnect® converged network adapters (CNAs) have independent software kits. Before updating earlier drivers and applications to the software in release 12.4.*x*, refer to the *Emulex Software Kit Migration User Guide* for special instructions and considerations for using the 11.2 and later software kits for FC HBAs and OneConnect CNAs.

5. Do not use version 12.4.*x* applications to manage LPe16202 adapters on remote hosts running version 11.4.*x* software. Management of LPe16202 adapters must be performed using the legacy version 11.4.*x* applications available on those hosts. If version 12.4.*x* management is used to manage LPe16202 adapters on remote hosts running version 11.4.*x*, the following limitations apply:

    – The GUI will discover LPe16202 adapters installed on the remote hosts being managed; however, LPe16202 adapter-specific (FCoE or NIC) counters are not displayed on the various function summary tabs.
    – The CLI will discover LPe16202 adapters using the `ListHBAs` command, and will generally be manageable. However, the FCoE-specific commands `GetFIPParams`, `SetFIPParam,` and `GetFCFInfo` are no longer supported.

6. On Linux passthrough-only systems, the HBACMD `listhba` command might be slow to respond when adapters are attached to VMs.

    Workaround

    None.

7. The OneCommand Manager application does not display updated driver parameters after a batch update.

    Workaround

    None.

8. Enabling and disabling a Fabric Assigned Port World Wide Name (FA-PWWN) might cause an adapter port's WWPN to change. The OneCommand Manager application discovery-tree might not display the port's newly assigned WWPN.

    Workaround

    Stop and restart the OneCommand Manager application services and daemons when prompted by the OneCommand Manager application.

9. Except on LPe12000-series HBAs, resetting or disabling HBA ports turns off beaconing.

    Workaround

    Enable beaconing after resetting or disabling HBA ports.

10. On LPe35000-series adapters, loopback tests are not functional on the following Linux inbox drivers:

    – SLES 15
    – RHEL 7.6
    – Ubuntu 18.04 (except the Ubuntu 18.04.3 HWE release)

11. On LPe 35000-series adapters, a host reboot is required after a firmware update on the following Linux inbox drivers:
    – SLES 15
    – RHEL 7.6
    – Ubuntu 18.04 (except the Ubuntu 18.04.3 HWE release)

12. Brocade switches using Fabric Operating System (FOS) version 8.2.1B and earlier might encounter the following issues with DHCHAP authentication:
    – You might not be able to configure the secret pair between the switch and the HBA.
    – When authentication is enabled on the switch, and authentication is disabled on the HBA, the switch disables the port, but it does not issue the expected status messages.
    – The Brocade switch authenticates the HBA port when authentication is disabled on the switch, or when a frame is dropped.

13. On Linux hosts running with kernel version 4.15 or earlier, an incorrect port speed can be reported by the OneCommand Manager GUI and HBACMD if trunking is enabled on the adapter.

    Workaround

    None.

14. The OCM GUI cannot be used to set a hash priority to a single value on an HBA port.

    Workaround

    Use HBACMD to set a hash priority to a single value on the HBA port. Ensure that the same hash priority value is set on the switch or authentication will fail.

15. Boot from SAN is not supported if FC-SP-2 authentication (DHCHAP) is enabled.

16. After deleting authentication, you must reload the driver or reboot the system to view the new settings in the OneCommand Manager GUI.

17. A link speed that was configured using the OneCommand Manager application is not reflected in the x86 Boot BIOS utility.

    Workaround

    In the x86 Boot BIOS utility, to view a non-default link speed that was configured in the OneCommand Manager application, ensure that the link is up in the x86 Boot BIOS utility by performing a `scan for target devices` or `configure the boot devices`.

18. Dual-port LPe35002 HBAs display quad-port LPe35004 HBA trunking attributes.

    Workaround

    None.

19. On RHEL 8 inbox systems, the GUI displays incorrect trunking information.

    Workaround

    Use the RHEL 8 out-of-box driver.

20. You must first update the OneCommand Manager application to version 12.4.*x* before using it to update the firmware to version 12.4.*x*.

    Workaround

    None.

21. On some inbox Linux distributions, the `lpfc_enable_mds_diags` driver parameter cannot be enabled dynamically.

    Workaround

    This parameter should be enabled only to run the Cisco diagnostics. Enable the `lpfc_enable_mds_diags` parameter temporarily by issuing the following commands:

    ```
    rmmod lpfc
    modprobe lpfc lpfc_enable_mds_diags=1
    ```

    After the diagnostics are complete, reload the driver without the `lpfc_enable_mds_diags` parameter.

22. If an adapter is installed in a server running version 12.4 of the OneCommand Manager application, do not attempt to manage, view or set the FABL (Fabric Assigned Boot LUN) EFI boot parameter from a remote OneCommand Manager application client. Doing so might result in incorrect settings being read or written.

    Workaround

    When running version 12.4 of the OneCommand Manager application, do not manage the FABL EFI parameter from a remote version of the OneCommand Manager application client. Manage the FABL EFI boot parameter using the local version 12.4 of the OneCommand Manager application.

23. When running version 12.4 of the OneCommand Manager application, do not attempt to manage, view or set the EFI boot parameters for a remote adapter installed in a server that is running version 12.2, or earlier, of the OneCommand Manager application. Doing so will yield unpredictable results.

    Workaround

    Use version 12.2, or earlier, of the OneCommand Manager application to manage the EFI settings on the version 12.2 server.

Technical Tips

1. If you change the volatile World Wide Name (WWN) on an LPe16000-series adapter, a reboot is required.

2. The OneCommand Manager application does not display the OS Device Name for LUNs attached to vPorts.

   In the **LUN Information** tab, under **Mapping Information**, the **OS Device Name** field displays **N/A** instead of the device name. All other information on the **LUN Information** tab is displayed correctly.

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

   If the 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 application does not run. The operating system displays the following error message:

   ```
   -Bash: /usr/sbin/OneCommand Manager/OneCommand Manager: 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.

4. The OneCommand Manager Secure Management mode on Linux systems requires Pluggable Authentication Module (PAM) authentication configuration on the host machine.

   In Secure Management mode, a user is authenticated on the machine at OneCommand Manager application GUI startup. The PAM interface manages this authentication.

   Workaround

   Configure the `/etc/pam.d/passwd` file authentication section or its earlier equivalent.

NOTE: Refer to the *Emulex OneCommand Manager Application for LightPulse® Adapters User Guide* for additional information about Secure Management mode.

5. When you install the OneCommand Manager application on a guest operating system, answers to the installer prompts are ignored.

   When you install the OneCommand Manager application on a guest operating system, you are presented with management mode options (for example, local only, full-management, read-only, and so on). Answers to these questions are ignored; all installations on guest operating systems are set to local only, read-only, and remote management.

6. Interference can occur with the OneCommand Manager application's ability to permanently change WWNs.

   Some newer adapters on some newer systems use techniques in the BIOS code at boot time to configure the adapter, such as the adapter WWN. In such cases, this might interfere with the OneCommand Manager application's ability to make permanent (nonvolatile) changes to the adapter's WWN.

7. 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 the OneCommand Manager `hbaapi` layer.

   Workaround

   Reinstall the OneCommand Manager application.

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

   When you make permanent driver parameter changes using the OneCommand Manager application, the application automatically makes the required entry in the `/etc/modprobe.conf` or equivalent file. Because the driver loads so early in the Linux machine boot sequence, the new contents of the `/etc/modprobe.conf` file must be reinserted into the Linux system `initrd` file (using the `mkinitrd` utility) for the driver to pick up the new driver parameter value on the next boot. Failure to generate a new `initrd` file prevents the driver from retrieving the new driver parameter value on subsequent driver loads (machine boots). The OneCommand Manager application automatically does this for you (re-creates `initrd` using the `mkinit` function); however, it can take as long as 45 to 60 seconds after the driver parameter is changed for a complete `initrd` rebuild. If you reboot the machine immediately after the driver parameter change is made, the automatic re-creation of the `initrd` file by the OneCommand Manager application might 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 to 60 seconds after making the driver parameter change before rebooting the machine.

9. Newly added LUNs on a storage array might 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.

10. A set link speed issue occurs after an SFP hot swap.

    LPe16000-series adapters do not support an SFP hot swap if the replacement SFP is not the same model as the original SFP. Two consequences occur in the OneCommand Manager application:

    – The **Port Attributes** tab in the OneCommand Manager application or the OneCommand Manager CLI `PortAttributes` command might display incorrect data for the **Supported Link Speeds** attribute. This issue is cosmetic.

    – Boot from SAN Management might 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.

11. A dump command on a boot from SAN adapter might cause a system panic.

    When the OneCommand Manager application performs a dump of an adapter that is booting from a 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.

12. The `elxhbmgrd` daemon can take up to 30 seconds to stop.

    The behavior of the `elxhbmgrd` daemon is linked with the MAX timeout that the Linux kernel associates with the block BSG driver interface commands, and with the OneCommand Manager application register for events function.

13. When using an Internet Explorer 11 browser, navigating to the **Index** or **Search** pages in the online help results in those pages being blank.

    Workaround

    Click **Contents** and refresh the browser, or load the help URL in a different browser.

14. When using Secure Management, if you belong to the ocmadmin group, you might be unable to change settings for remote adapters.

    Workaround

    Switch to Full Management when changing the settings on a remote adapter.

15. If the CLI (HBACMD) is used to perform a firmware download to a local adapter, and the OneCommand Manager GUI is running while that firmware download is occurring, the OneCommand Manager GUI might experience problems displaying information on various display tabs after the download completes. The value displayed for most of the fields on the affected tabs or dialogs is N/A.

    Workaround

    Do one of the following:

    – Perform the firmware download using the OneCommand Manager GUI instead of HBACMD.

    – When a firmware download has been performed by using HBACMD, if N/A is shown for most of the OneCommand Manager GUI display fields, exit the GUI, and then restart it. The fields are displayed correctly after doing this action.

    – Ensure that the OneCommand Manager GUI is stopped or is not running prior to performing a firmware download using HBACMD.

16. 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 the new **Chrome** icon and select **Properties**.

    c. Add the `--allow-file-access-from-files` text to the end of the path appearing in the target. You must leave a space between the original string and the tag you are adding.

    d. Click **OK** to save your settings. Close any open instances of Chrome.

    e. To open a local copy of the online help, either use the new shortcut to open Chrome, and then press **Ctrl** + **Open** and browse to the start page; or open Chrome with the new shortcut, and then right-click the start page and click **Open With > Google Chrome**.

17. The OneCommand Manager GUI might not appear to display the adapter's next boot configuration for all available ports when a remote management console is being used; for example, integrated Lights Out (iLO), integrated Dell Remote Access Controller (iDRAC), and Interactive Media Manager (IMM).

    The size of the screen provided by these management modules might not be big enough for the OneCommand Manager window to fully display all the GUI components and information under the **Adapter Configuration** tab. Readjust the size of the OneCommand Manager GUI window for all the GUI scroll bars under the **Adapter Configuration** tab to become visible. You can also decrease the width of the **Discovery-Tree** panel.

18. LPe31000-series and LPe32000-series adapters might experience a link-down condition after running a cable link diagnostics test when they are connected to Brocade switches running FOS versions prior to v8.1.2.

    Workaround

    Manually reset the switch port using the `portdporttest --exit` command.

19. D_Port and FA-PWWN cannot be enabled simultaneously.

    Workaround

    If D_Port is enabled and you want to enable FA-PWWN, you must first disable D_Port. If FA-PWWN is enabled and you want to enable D_Port, you must first disable FA-PWWN.

20. Neither FA-PWWN nor D_Port can coexist with the trunking feature on LPe35000-series adapters. If trunking is enabled, the firmware automatically disables FA-PWWN and D_Port.

21. D_Port and DHCHAP cannot be enabled simultaneously.

    Workaround

    If D_Port is enabled and you want to enable DHCHAP, you must first disable D_Port. If DHCHAP is enabled and you want to enable D_Port, you must first disable DHCHAP.

22. D_Port is enabled by default.

23. After Dynamic D_Port is transitioned from enabled to disabled, OneCommand Manager might fail D_Port diagnostics.

    Workaround

    Perform a port reset.

24. Loopback tests attempt to run without a loopback connector on trunked ports if the loopback connector was removed after running a previous loopback test.

    Workaround

    Ensure a loopback connector is installed on the trunked port before running loopback tests.

BROADCOM®