Emulex® OneCommand® Manager Application for Linux Release Notes

Version: 11.4.329.44

Systems: SLES 11 SP3 and SP4, SLES 12 SP2, SP3, and SP4, and SLES 15
RHEL 6.8, 6.9, 6.10, 7.3, 7.4, 7.5, and 7.6

Date: April 17, 2019

Purpose and Contact Information

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

For the latest product documentation, 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

Adds support for the following operating systems:

- RHEL 7.6
- SLES 12 SP4

Resolved Issues

There are no resolved issues in this release.

Known Issues

1. **Beginning with software release 11.2, LightPulse® adapters and OneConnect® adapters have independent software kits.**

   Before updating earlier drivers and applications to the software in release 11.4, refer to the *Emulex Software Kit Migration User Guide* for special instructions and considerations for using the 11.2 and later software kits for LightPulse and OneConnect adapters.

2. **Some Red Hat Enterprise Linux (RHEL) 6.x versions are not configured by default to return LDAP group user membership.**

   By default, some versions of RHEL 6.x do not return the LDAP group user membership along with the LDAP group information 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.

3. **The following is a requirement for unloading or loading Emulex FC device drivers.**

   If you load or unload the Emulex FC device driver for Linux after the machine is rebooted, you must perform the following steps:

   a) Close any open OneCommand Manager applications.
   b) Restart the 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 OneCommand Manager application GUI or the OneCommand Manager CLI client application.

4. **On some RHEL x86_64 and Power PC (PPC64) 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.

5. **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.

6. **The 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 halts when the adapter is taken offline to perform the boot and writes 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, make sure that the 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.

7. **The OneCommand Manager application elxhbamgrd daemon can take up to 30 seconds to stop.**

   The OneCommand Manager application elxhbamgrd daemon process might take up to 30 seconds to stop when attempting to terminate it.

   Workaround

   None. The behavior of the elxhbmgrd daemon is linked with the MAX timeout that the Linux kernel associates with the SCSI block SCSI generic driver (BSG) interface commands and the OneCommand Manager application register for events function.

8. **The Linux operating system with Security Enhanced Linux (SELinux) enabled receives numerous benign warning messages in `/var/log/messages` when starting the OneCommand Manager application.**

   When the OneCommand Manager application is installed and SELinux is enabled, numerous messages similar to the one that follows will appear in the `/var/log/messages`:

   ```
   SELinux is preventing /usr/sbin/ethtool from write access on the file.
   For complete SELinux messages. run sealert -l
   a5c4abd9-5279-4621-8976-52ed71bd8c13 Oct 16 19:12:07 localhost python:
   SELinux is preventing /usr/sbin/ethtool from write access on the file.
   ```

   Workaround

   To suppress these messages, run the following two commands:

   ```
   grep ethtool /var/log/audit/audit.log | audit2allow -M mypol

   semodule -i mypol.pp
   ```

9. **LUNs are not displayed when the target connection is refreshed after a port flap.**

   Workaround

   Restart the OneCommand Manager application.

Technical Tips

1. **FC in-band management is no longer supported.**
2. **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 bandwidths to 0.
3. **On 8-Gb/s FC adapters, the OneCommand Manager application Firmware tab is in a different location than with 16-Gb/s FC adapters.**
4. **An end-to-end (ECHO) diagnostic test fails if the corresponding targets are not supported.**

   Make sure that 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 the new **Chrome** icon and select **Properties**.
   c) Add the `--allow-file-access-from-files` text to the end of the path that appears 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 right-click the start page and select **Open With > Google Chrome**.

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

7. **Creating OneCommand Manager Secure Management users and groups after the OneCommand Manager application is installed in Secure Management mode causes the graphical user interface (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 operating system displays the following error message:

   ```
   -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.

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

   In OneCommand Manager Secure Management mode, a user is authenticated on the machine at OneCommand Manager application GUI startup. The PAM interface handles this authentication. The `/etc/pam.d/passwd` file authorization section or its earlier equivalent must be configured.

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

9. **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 of the GUI scroll bars under the **Adapter Configuration** tab to become visible. You can also decrease the width of the discovery-tree panel.

10. **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 mode, read-only, and remote management.

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

    When you make permanent driver parameter changes with the OneCommand Manager application, the application automatically makes the required entry in the `/etc/modprobe.conf` or equivalent file. Because the FC 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 include the new driver parameter value on the next boot. Failure to generate the new `initrd` file causes the driver to fail to include the new driver parameter value on subsequent driver loads (machine boots). The OneCommand Manager application automatically does this function for you (re-creates initrd with 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 auto-recreation 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.

12. **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 to the target array.

13. **A set link speed issue exists after a small form-factor pluggable (SFP) hot swap.**

    The LPe16000-series adapters do not support SFP hot swap if the replacement SFP is not the same model as the original SFP. The OneCommand Manager application experiences two ramifications:

    - 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 Storage Area Network (SAN) Management might be unable to set the `Boot Code Link Speed` parameter to 16 Gb/s.

    Workaround

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

14. **If the CLI is used to perform a firmware download to a local adapter, and the OneCommand Manager GUI is running while the firmware download is taking place, the OneCommand Manager GUI might not display information on various tabs after the download completes. The value displayed for most of the fields on the affected tabs and dialogs will be N/A.**

    Workaround

    There are three possible workarounds:

- After having performed a firmware download using the CLI, if **N/A** is displayed for most of the OneCommand Manager GUI display fields, exit the GUI and restart it. The fields should be displayed correctly.
- Make sure that the OneCommand Manager GUI is stopped and not running prior to performing a firmware download using the CLI.
- Perform the firmware download using the OneCommand Manager GUI instead of the CLI.