Emulex® OneCommand® CNA Manager Application for OneConnect® Adapters for Linux Release Notes

Version: 11.2.1153.25

Systems: RHEL 6.6 and later
RHEL 7.0 and 7.3 (out-of-box)
SLES 11 SP3 and SP4
SLES 12 and 12 SP1 and SP2
Oracle Linux 6.6 and later
Oracle Linux UEK R1, R2 with OL 6
Oracle Linux UEK R1, R2 with OL 5
Ubuntu 16.04 (inbox only)
Xen Server 6 and 7

Note: This version of the OneCommand CNA Manager application for Linux provides full inbox management support for the OCe11100- and OCe14000-series CNAs. This OneCommand CNA Manager application version also provides iSCSI support for SLES 12, SLES 11 SP2–SP3, RHEL 6.5, and Oracle Linux UEK R1, R2 with OL 6.

Date: January 30, 2017

Purpose and Contact Information

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

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 ccx-tech.support@broadcom.com or request assistance online at https://oemsupportportal.emulex.com/web2tech/ccx.html.

New Features

- 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 11.2, refer to the *Emulex Software Kit Migration User Guide* for special instructions and considerations for using the 11.2 software kits for LightPulse and OneConnect adapters.
- Adds support for SuSE Linux Enterprise Server (SLES) 12 SP2
- iSCSI qualified Name (IQN) is assigned on a per-port basis instead of globally

Resolved Issues

There are no resolved issues for this release.

Known Issues

Known Issues for the Inbox Linux NIC Driver

1. **A 10 to 30 second delay exists in response time when using the OneCommand CNA Manager application with an inbox driver.**

   Workaround

   None.

General Known Issues

1. **Known issues related to updating firmware.**

   For OCe14000-series adapters, firmware version 11.x includes new features that require new flash regions to support them. Firmware versions earlier than 10.0.803.37 did not have the ability to configure the flash regions to support these new features.

   If you are updating from a firmware version earlier than 10.0.803.37, use one of these methods to update the firmware to 11.x:

   - Use the Offline Flash International Standards Organization (ISO) flash tool.
   - Use the released 11.x version of the OneCommand CNA Manager application graphical user interface (GUI) or OneCommand CNA Manager command line interface (CLI) application. You must perform the firmware update procedure twice to ensure that the flash regions are properly configured, and you must reboot the system after each firmware update.

   After you have updated the firmware, you must not downgrade the firmware to a version earlier than 10.0.803.37.

   Note: Do not use Linux inbox drivers when performing the firmware update.

2. **For OCe14000–series adapters, on the Physical Port Info tab, the Set Speed button might be disabled.**

   Workaround

   None.

3. **The Port Information and Maintenance tabs show Unknown as the current firmware version.**

   Workaround

   None.

4. **The network interface card (NIC) driver must be installed and enabled to run the OneCommand CNA Manager application on the OneConnect adapter.**

   If the OneConnect adapter is running without the NIC driver installed and enabled, many of the management functions are unavailable, or the OneCommand CNA Manager application displays erroneous information.

   Unavailable management functions include:

   - Downloading
   - All diagnostics, including beaconing and diagnostic dumps
   - Disabling or enabling a port

- Changing data center bridging (DCB) settings

Erroneous information includes:

- Fibre Channel over Ethernet (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
- Basic input/output system (BIOS) version
- Boot code version
- Transceiver data display
- Physical port link status
- All DCB settings
- Event log display (CLI only)
- Adapter temperature

Workaround

Install and enable the NIC driver before running the OneCommand CNA Manager application or the OneCommand CNA Manager CLI.

5. **The OneCommand CNA Manager application does not display the 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.

   Workaround

   None.

6. **Enabling channel management at less than 10 Gb/s might cause the link to go down, and channel management settings might not take effect.**

   Channel management can be enabled and configured for 10 Gb/s ports running at slower speeds. Channel management is only supported for OneConnect converged network adapter (CNA) ports running at speeds of at least 10 Gb/s.

   If a port's native speed is 10 Gb/s or higher, but the port is currently operating at a speed lower than 10 Gb/s, the OneCommand CNA Manager application allows channel management to be enabled and configured. However, enabling channel management in this case might cause the link to go down and channel management settings might not take effect.

   Workaround

   Before enabling channel management, make sure the OneConnect CNA port's physical link is operating at 10 Gb/s or higher. If a 10 Gb/s link is not possible, do not enable channel management on that port.

7. **The OneCommand CNA Manager application reports virtual ports under one adapter on a Linux guest operating system.**

   When running the OneCommand CNA Manager application client on a Linux guest operating system (virtual machine), Emulex virtual NIC functions (ports) are displayed

under one Emulex adapter. This situation is caused by the virtual (Bus:Device:Function) information returned on the guest operating system.

Workaround

None.

8. **Creating Secure Management users and groups after the OneCommand CNA 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 CNA Manager application has been installed in Secure Management mode, when you attempt to start the OneCommand CNA 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 CNA Manager application in Secure Management mode.
   - Uninstall and reinstall the OneCommand CNA Manager application.

9. **The OneCommand CNA 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 CNA Manager application GUI startup. The PAM interface manages this authentication.

   Workaround

   Configure the `/etc/pam.d/passwd` file auth section or its earlier equivalent must be configured.

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

10. **When you install the OneCommand CNA Manager application on a guest operating system, the installer prompts for the management mode.**

    When installing the OneCommand CNA Manager application, you are presented with management mode options (for example, local-only, full-management, read-only, and so on.) to specify how the OneCommand CNA Manager application will run on the host. When the OneCommand CNA Manager application runs on a virtual machine (VM) with an Emulex NIC virtual function (VF), it automatically runs in local-only and read-only management mode. This situation means you can view the VF and only the VF in the OneCommand CNA Manager application, but you cannot manage the adapter or the VF from the OneCommand CNA Manager application. Any selections for the management mode options made during installation outside of this mode are ignored.

    For example, if you select full management mode during installation, the VF can be viewed from remote OneCommand CNA Manager hosts, and the OneCommand CNA Manager application running on the VM cannot view or manage any remote host adapters, or manage the adapter on which the VF is running.

Workaround

None.

11. **The OCe11101-E CNA cannot run loopback diagnostic tests (physical layer [PHY], media access control [MAC], External).**

    Attempts to run a loopback test on the OCe11101-E CNA fail.

    Workaround

    None.

12. **Some RHEL 6.x versions are not configured by default to return Lightweight Directory Access Protocol (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 systems, as can be seen by inspecting the output of the `getent group` Linux command.

    Workaround

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

13. **Single Root I/O virtualization (SR-IOV): Running the OneCommand CNA 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 CNA Manager application in the virtual machine's guest operating system, the NIC functions appear under a single adapter node in the OneCommand CNA 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 CNA Manager application incorrectly determines that each of the discovered NICs are from the same adapter.

    Workaround

    None.

14. **Performing a core dump command might fail if a World Wide Port Name (WWPN) is specified.**

    When performing a core dump operation in OneCommand CNA Manager 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.

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

The Mode and Speed can be set either from the Physical Port info tab in the OneCommand CNA Manager application or with the `SetPhyPortSpeed` OneCommand CNA CLI command.

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

Workaround

None.

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

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

    Workaround

    Do one of the following:

    - 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 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 is displayed.
        e) Check the **VLAN Enabled** and **DHCP Enabled** check boxes and click **OK**.

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

    Some newer adapters (for example, CNAs) 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 CNA Manager application's ability to make permanent (nonvolatile) changes to the adapter's WWN.

    Workaround

    None.

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

    Although the OneCommand CNA Manager application and OneCommand CNA Manager CLI clients allow a **yes** or **no** iSCSI InitialR2T parameter, the adapter does not recognize the setting. The adapter always operates with InitialR2T set to **yes**.

    Workaround

    None.

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

    On Linux SLES 11 SP1 systems, when the OneCommand CNA Manager Web Launch component is installed or uninstalled using `wsinstall` and `wsuninstall` scripts respectively, the following messages are displayed:

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

    These warning messages do not affect the operation or installation of the Web Launch component. They appear on SLES 11 SP2-specific versions of the relevant software (`insserv` and `jexec`). The scripts invoke this software using the invocation of the standard Linux `chkconfig` utility that is typically used for daemon installations.

    Workaround

    None.

20. **On SLES 11 SP1 systems, installing or uninstalling the Open-FCoE RPM package manager (RPM) package after the OneCommand CNA Manager application is installed results in the removal of the OneCommand CNA Manager application entries in the system file in the `/etc/hba.conf` file.**

    This situation breaks the Linux system host bus adapter (HBA) application programing interface (API) functionality, and the OneCommand CNA Manager application client application no longer runs.

    Workaround

    Reinstall the OneCommand CNA Manager application.

21. **On RHEL 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 the 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.

22. **On some RHEL x86_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 CNA Manager hbaapi layer.**

    Workaround

    Re-install the OneCommand CNA Manager application.

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

    If you unload the NIC driver from a Linux machine, OneCommand CNA Manager applications or OneCommand CNA Manager CLI commands running on the machine lose connectivity with the NIC and related configuration data.

Workaround

To recover connectivity, perform the following steps:

a) Stop the OneCommand CNA Manager application and daemons using the `stop_ocmanager` script.

b) Reload the NIC driver using `modprobe`.

c) Restart the OneCommand CNA Manager application daemons using the `start_ocmanager` script.

d) Restart the desired OneCommand CNA Manager application or OneCommand Manager CLI client.

24. When the SNMP daemon starts, it triggers warning messages within Security Enhanced Linux (SELinux) for certain operations.

Workaround

To avoid SELinux warning messages, disable SELinux.

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

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

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

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

25. Newly added LUNs on a storage array might not appear on the host machine Linux operating system or the OneCommand CNA 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.

26. 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 Internet Storage Name Service (iSNS), it gets its default login options from the initiator login options.

After 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 (the 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 target's login properties are defined again by how they are discovered as described at the beginning of this known issue.

Workaround

None.

27. **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 might occur if this requirement is not met.

    Workaround

    None.

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

    When the OneCommand CNA 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.

29. **Logical port VLAN ID(LPVID) update causes an `ifdown-ifup` error message to be displayed.**

    When attempting to update LPVID values through either Hbacmd commands or the GUI, the following warning messages might be displayed in standard output (stdout):

    ```
    usage: ifdown <device name>
    /sbin/ifup: configuration for ethx not found.
    Usage: ifup <device name>
    ```

    The `ifdown` and `ifup` commands are executed by the OneCommand CNA Manager application when the LPVID is changed for an enabled Universal Multi-Channel (UMC) Channel for the NIC driver to automatically reload for that channel and possibly acquire a new DHCP address (based on the switch configuration). The warning messages are seen only when the necessary interface configuration file (`ifcfg-ethx`) does not exist.

    Hbacmd commands:

    ```
    CMSetLPVID
    UmcSetLPVID
    ```

    Workaround

    Because the `ifdown` and `ifup` commands use the interface configuration file to determine which interface to bring down or up and how to configure it, you must manually create this file if it was not previously generated by the network manager utility. Refer to the appropriate reference guide for the Linux distribution you are running to get instructions for the values required in the interface configuration file.

    For example, the `ifcfg-eth0` file for an interface using DHCP on RHEL distributions might look like the following:

    ```
    DEVICE=eth0
    BOOTPROTO=dhcp
    ```

```
ONBOOT=yes
```

30. **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.

31. **When running the `Hbacmd Dump` command, after setting the Retention Count to 2, the `Hbacmd Dump` command might return an `Unable to produce dump file` error, and a dump file is not created.**

    Workaround

    If you set the retention count to 1, the `Hbacmd Dump` command successfully creates a dump file.

32. **When using the Linux SLES 12 operating system, all the iSCSI functions present might not be displayed when opening the OneCommand Manager.**

    The management interface library (MILI) is not showing the iSCSI functions after reboot because the Linux Open-iSCSI driver is taking more time to load and loads before the MILI service is started during boot time.

    Workaround

    Exit and restart the OneCommand CNA Manager application.

33. **When using the OneCommand CNA Manager application on a virtual machine and attaching the NIC function or NIC+FCoE function to the virtual machine, the NIC ports might not be displayed in the OneCommand CNA Manager application.**

    Workaround

    None.

34. **If you are using the OneCommand CNA Manager application to update firmware from a previous version to version 11.x, you must first update the OneCommand CNA Manager application to version 11.x.**

35. **Enabling SR-IOV and then rebooting does not enable SR-IOV.**

    Workaround

    Refer to the most recent *Emulex Drivers for Linux for OneConnect Adapters User Guide* (available on the Broadcom website) for instructions on enabling SR-IOV.

36. **The iPv6 Automatic Assignment on iSCSI functions cannot be enabled or disabled by the OneCommand CNA Manager application GUI or the CLI.**

    Workaround

    Use either Option ROM (OROM) or Human Interface Infrastructure (HII) to set the Automatic Assignment.

37. **In the OneCommand CNA Manager application GUI, if you are logged into an iSCSI target, the Source IP Address on the Sessions screen (from the iSCSI Target Information tab), might be reported as either 0.0.0.0 or another invalid IP address when multiple iSCSI adapters are installed.**

Workaround

The source IP address is equivalent to the iSCSI initiator IP address, which can be found on the **Network Information** tab under TCP/IP Information.

38. **The OneCommand CNA Manager application does not display adapter-specific information (such as model, serial number, and firmware state) for OCe10100-series adapters on Oracle Linux operating systems.**

    Workaround

    None.

39. **When an adapter is configured with iSCSI in pNIC mode and you log into an iSCSI target, if boot flag has been enabled for the target LUN, target logout is successful with Unified Extensible Firmware Interface (UEFI) but not with the OneCommand CNA Manager application.**

    Workaround

    None.

40. **NIC traffic bandwidth uses 0 Mb/s for most of the iperf connections (parallel threads) on OCe14000-series 1Gb/s adapters.**

    On a 1Gb/s port, traffic flows only on single connections when traffic is run using the `iperf` utility with multiple connections.

    Workaround

    Create a 1TX queue using the `ethtool -L` command. Traffic will then flow on all TCP connections.

41. **For OCe14000-series adapters, on the Adapter Configuration tab, the third function does not allow the selection of any storage protocol.**

    For example:

    On the **Adapter Configuration** tab with the **Custom** button selected, if you select **FCoE** from the list of the second function, the third function does not display other protocols (such as **iSCSI**) in the list.

    Workaround

    a) Switch the protocols from **FCoE** to **iSCSI** for the second function. The third function now displays **FCoE**.

    b) Switch back to the original option for the second function (**FCoE**). This action now displays **iSCSI** for the third function.

    This workaround can be repeated for the remaining ports if needed.

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

    Workaround

    Restart the OneCommand CNA Manager application.

43. **The Echo test is not supported on OCe14000-series and OCe11100-series FCoE adapters.**

    Workaround

    None.

44. **In SELinux, if iSCSI is enabled on one or more of the installed CNAs, numerous messages similar to the following might be logged to the `/var/log/messages` file when the OneCommand CNA Manager application is running:**

```
Apr 19 04:57:46 dhcp-10-192-232-209 python: SELinux is preventing
/usr/sbin/iscsiadm from write access on the file
/var/opt/emulex/ocmanager/logs/cnaboardmgmt.log.
If you want to ignore iscsiadm trying to write access the
cnaboardmgmt.log file, because you believe it should not need this
access, then you should report this as a bug.
```

These messages can be safely ignored, and they have no effect on the functionality of the OneCommand CNA Manager application.

Workaround

To suppress these warnings, run the following two commands:

```
> grep iscsiadm /var/log/audit/audit.log | audit2allow -M mypol
> semodule -i mypol.pp
```

45. **If the CLI (HBACMD) is used to perform a firmware download to a local adapter, and the OneCommand Manager GUI is up and running while that firmware download is taking place, 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:

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

46. **A timeout occurs when the OneCommand CNA Manager application issues dump commands while it is connected to a remote host that is using inbox drivers.**

Workaround

Use a local host to collect dumps.

47. **If CNAs are installed on a machine running SELinux, numerous messages similar to the following may be logged to the `/var/log/messages` file when the OneCommand CNA Manager application is running:**

```
Aug 21 23:14:52 localhost setroubleshoot: SELinux is preventing
/usr/sbin/ethtool from "read, write" accesses on the chr_file
/dev/be2iscsi_1.
For complete SELinux messages, run sealert -l
5dbbc40c-10aa-44ad-ad11-0fe6f5253653
```

Workaround

To suppress these warnings, run the following two commands:

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

48. **If the OneCommand CNA Manager application for LightPulse adapters is running, the OneConnect FCoE driver cannot be unloaded.**

    Workaround

    Stop the OneCommand CNA Manager application for LightPulse adapters by typing the following command:

    ```
    /usr/sbin/ocmanager/stop_ocmanager
    ```

Technical Tips

1. **If DCB settings are required when connected to a non-Data Center Bridging Exchange Protocol (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 priority flow control (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.**

2. **On OneConnect adapters, if you change the port speed by using the Change Port Speed dialog 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.**

3. **The OneCommand CNA Manager application no longer installs OneCommand Vision components.**

4. **OneCommand CNA Manager application differences exist when running the Open-iSCSI driver.**

   When running the Open-iSCSI version of the Linux iSCSI driver (which is used on RHEL 6.3 and later and SLES 11 SP2 and later), the OneCommand CNA Manager application functionality differs from the proprietary device driver (which is used on RHEL 5.x and SLES 10 SPx).

   Extended time out (ETO) and link down time out (LDTO) are not available in the Open-iSCSI implementation. Therefore, you cannot set ETO on a per-target basis. Only the boot target should be made persistent for each port.

5. **Roles-based Secure Management mode is available.**

   Secure Management mode is a roles-based security implementation. During the OneCommand CNA Manager application installation, you are asked if you want to run in Secure Management mode. When the OneCommand CNA Manager application is installed in this mode, the following operational changes occur:

   - A non-root or non-administrator user can run the OneCommand CNA Manager application.
   - The OneCommand CNA Manager application host uses a user's credentials for authentication.
   - A user has OneCommand CNA Manager application configuration privileges according to the OneCommand CNA 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 (OneCommand CNA CLI does not require credentials) but no remote privileges.

Note: Refer to the *Emulex OneCommand CNA Manager application for OneConnect Adapters User Guide* for more information on Secure Management mode.

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

   OneCommand CNA Manager Secure Management must be able to get the OneCommand CNA Manager application group to which the user belongs from the host's domain (Active Directory or 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 CNA Manager application user groups.

   Table 1 Secure Management User Privileges

User Group	OneCommand CNA Manager 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 groups must be created and configured on the host machine or network domain. OneCommand CNA Manager Secure Management uses the C-library API calls `getgrnam` and `getgrid` to retrieve the OneCommand CNA 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 CNA 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 CNA Manager Secure Management.

7. **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, 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**.

8. **The OneCommand CNA Manager application supports a maximum of 16 ASICs for OneConnect adapters. Most OneConnect adapters have a single ASIC, so the OneCommand CNA Manager application can see and manage a maximum of 16 adapters. Some OneConnect adapter models have two ASICs. When all the adapters have two ASICS, the OneCommand CNA Manager application can see and manage a maximum of eight adapters.**

9. **The OneCommand CNA 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 CNA Manager window to fully display all the GUI components and information under the Adapter Configuration tab. Re-adjust the size of the OneCommand CNA 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.**

10. **If you load or unload an Emulex device driver for Linux (FCoE, NIC, and iSCSI) after the machine is rebooted, you must perform the following steps:**
    a) Close any open OneCommand CNA Manager applications.
    b) Stop and then restart the OneCommand CNA Manager application daemons:
       - Run the `/usr/sbin/ocmanager/stop_ocmanager` script.
       - Run the `/usr/sbin/ocmanager/start_ocmanager` script.
    c) Run the OneCommand CNA Manager application or the OneCommand Manager CLI client applications.