Sun Storage 16 Gb Fibre Channel ExpressModule Universal Host Bus Adapter, Emulex Security Guide

For HBA Model 7101690

Part No: E39922-04
July 2015

Sun Storage 16 Gb Fibre Channel ExpressModule Universal Host Bus Adapter, Emulex Security Guide

Part No: E39922-04

Copyright © 2014, 2015, , Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS. Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Référence: E39922-04

Copyright © 2014, 2015, , Oracle et/ou ses affiliés. Tous droits réservés.

Ce logiciel et la documentation qui l'accompagne sont protégés par les lois sur la propriété intellectuelle. Ils sont concédés sous licence et soumis à des restrictions d'utilisation et de divulgation. Sauf stipulation expresse de votre contrat de licence ou de la loi, vous ne pouvez pas copier, reproduire, traduire, diffuser, modifier, breveter, transmettre, distribuer, exposer, exécuter, publier ou afficher le logiciel, même partiellement, sous quelque forme et par quelque procédé que ce soit. Par ailleurs, il est interdit de procéder à toute ingénierie inverse du logiciel, de le désassembler ou de le décompiler, excepté à des fins d'interopérabilité avec des logiciels tiers ou tel que prescrit par la loi.

Les informations fournies dans ce document sont susceptibles de modification sans préavis. Par ailleurs, Oracle Corporation ne garantit pas qu'elles soient exemptes d'erreurs et vous invite, le cas échéant, à lui en faire part par écrit.

Si ce logiciel, ou la documentation qui l'accompagne, est concédé sous licence au Gouvernement des Etats-Unis, ou à toute entité qui délivre la licence de ce logiciel ou l'utilise pour le compte du Gouvernement des Etats-Unis, la notice suivante s'applique:

U.S. GOVERNMENT END USERS. Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

Ce logiciel ou matériel a été développé pour un usage général dans le cadre d'applications de gestion des informations. Ce logiciel ou matériel n'est pas conçu ni n'est destiné à être utilisé dans des applications à risque, notamment dans des applications pouvant causer des dommages corporels. Si vous utilisez ce logiciel ou matériel dans le cadre d'applications dangereuses, il est de votre responsabilité de prendre toutes les mesures de secours, de sauvegarde, de redondance et autres mesures nécessaires à son utilisation dans des conditions optimales de sécurité. Oracle Corporation et ses affiliés déclinent toute responsabilité quant aux dommages causés par l'utilisation de ce logiciel ou matériel pour ce type d'applications.

Oracle et Java sont des marques déposées d'Oracle Corporation et/ou de ses affiliés. Tout autre nom mentionné peut correspondre à des marques appartenant à d'autres propriétaires qu'Oracle.

Intel et Intel Xeon sont des marques ou des marques déposées d'Intel Corporation. Toutes les marques SPARC sont utilisées sous licence et sont des marques ou des marques déposées de SPARC International, Inc. AMD, Opteron, le logo AMD et le logo AMD Opteron sont des marques ou des marques déposées d'Advanced Micro Devices. UNIX est une marque déposée d'The Open Group.

Ce logiciel ou matériel et la documentation qui l'accompagne peuvent fournir des informations ou des liens donnant accès à des contenus, des produits et des services émanant de tiers. Oracle Corporation et ses affiliés déclinent toute responsabilité ou garantie expresse quant aux contenus, produits ou services émanant de tiers, sauf mention contraire stipulée dans un contrat entre vous et Oracle. En aucun cas, Oracle Corporation et ses affiliés ne sauraient être tenus pour responsables des pertes subies, des coûts occasionnés ou des dommages causés par l'accès à des contenus, produits ou services tiers, ou à leur utilisation, sauf mention contraire stipulée dans un contrat entre vous et Oracle.

Accessibilité de la documentation

Pour plus d'informations sur l'engagement d'Oracle pour l'accessibilité à la documentation, visitez le site Web Oracle Accessibility Program, à l'adresse `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc`.

Accès au support électronique

Les clients Oracle qui ont souscrit un contrat de support ont accès au support électronique via My Oracle Support. Pour plus d'informations, visitez le site `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` ou le site `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` si vous êtes malentendant.

Contents

Using This Documentation 7
Product Documentation Library 7
Feedback 7

Sun Storage 16 Gb FC ExpressModule Universal HBA, Emulex Security 9
Universal HBA Overview 9
Security Principles 10
Planning a Secure Environment 11
Hardware Security 11
Software Security 12
Firmware Security 12
Oracle ILOM Firmware 13
System Logs 13
Maintaining a Secure Environment 13
Asset Tracking 13
Firmware Updates 14
Software Updates 14
Log Security 14
Module Security 14

Using This Documentation

- **Overview** – Describes how securely use the universal host bus adapter
- **Audience** – Technicians, system administrators, and authorized service providers
- **Required knowledge** – Advanced experience troubleshooting and replacing hardware

Product Documentation Library

Documentation and resources for this product and related products are available at http://docs.oracle.com/cd/E24649_01/index.html.

Feedback

Provide feedback about this documentation at http://www.oracle.com/goto/docfeedback.

Sun Storage 16 Gb FC ExpressModule Universal HBA, Emulex Security

This document provides general security principles and guidelines to consider when using the Sun Storage 16 Gb FC ExpressModule Universal HBA, Emulex.

This documentation does *not* cover the following security information:

- Specific platform firmware security that relates to BIOS, Open Boot Prom (OBP), and Hypervisor
- Issues with operating system security
- Physical security of the hardware system
- Network security of external networking infrastructure
- Trusted Platform Module information

For security information about any of these security areas, see the security documentation provided with the specific product.

The document contains the following topics:

- "Universal HBA Overview" on page 9
- "Security Principles" on page 10
- "Planning a Secure Environment" on page 11
- "Maintaining a Secure Environment" on page 13

Universal HBA Overview

The Sun Storage 16 Gb FC ExpressModule Universal HBA, Emulex (marketing part number 7101690) is a standalone PCI Express ExpressModule host bus adapter (HBA). This HBA is a reconfigurable board that changes its operating protocol mode from a two-port 16 Gb FC HBA to a two-port 10 GbE CNA, based on the optical transcievers and optical cables that you insert and attach to the board at boot time.

The board interfaces an eight-lane PCI Express bus, with eight lanes supporting two Fibre Channel (FC) or two Fibre Channel over Ethernet (FCoE) optical media ports. Each independent FC port operates at 16 Gb/sec and features 16/8/4 autonegotiation. Each FCoE port operates at 10 Gb/sec. You can configure the following three options:

- **10 GbE FCoE option** - The version of the card that provides twin-ax (or copper) 10 GbE FCoE ExpressModule Converged Network Adapter functionality. No optic modules are installed in this Converged Network Adapter.
- **16 Gb FC optics option** - The version of the card that has 16 Gb FC optics installed (optics marketing part number 7101686) in the SFP+ connecter of the card, providing short-wave 16 Gb Fibre Channel ExpressModule Host Bus Adapter functionality.
- **10 GbE FCoE optics option** - The version of the card that has 10 GbE optics installed (optics marketing part number 7101688) in the SFP+ connector of the card, providing short-range 10 GbE FCoE ExpressModule Converged Network Adapter functionality.

The following image shows the Sun Storage 16 Gb FC ExpressModule Universal HBA, Emulex:

Security Principles

There are four basic security principles: access, authentication, authorization, and accounting.

- **Access**

  Physical and software controls protect your hardware or data from intrusion.

  - For hardware, access limits usually mean *physical* access limits.
  - For software, access is limited through both physical and virtual means.
  - Firmware cannot be changed except through the Oracle update process.

- **Authentication**

  Set up the authentication features such as a password system in your platform operating systems to ensure that users are who they say they are.

  Ensure that your personnel use employee badges properly to enter the computer room.
- **Authorization**

  Allow personnel to work only with hardware and software that they are trained and qualified to use. Set up a system of Read/Write/Execute permissions to control user access to commands, disk space, devices, and applications.
- **Accounting**

  Use Oracle software and hardware features to monitor login activity and maintain hardware inventories.

  - Use system logs to monitor user logins. Monitor system administrator and service accounts in particular because these accounts can access powerful commands.
  - Use component serial numbers to track system assets. Oracle part numbers are electronically recorded on all cards, modules, and motherboards.

Planning a Secure Environment

Review the information in this section before and during the installation and configuration of a server and Sun Storage 16 Gb Fibre Channel ExpressModule Universal HBA, Emulex.

This section contains the following topics:

- “Hardware Security ” on page 11
- “Software Security ” on page 12
- “Firmware Security” on page 12
- “Oracle ILOM Firmware” on page 13
- “System Logs” on page 13

Hardware Security

Physical hardware can be secured fairly simply: limit access to the hardware and record serial numbers.

- **Restrict access**
  - If equipment is installed in a rack with a locking door, keep the door locked except when you have to service components in the rack.

  - Store spare field-replaceable units (FRUs) or customer-replaceable units (CRUs) in a locked cabinet. Restrict access to the locked cabinet to authorized personnel.
- **Record serial numbers**

  Keep a record of the serial numbers of all universal HBA cards.

Software Security

The security considerations for software components are:

- Refer to the documentation that came with your software to enable any security features available for the software.
- Use the superuser account to set up and update the universal HBA drivers.
- Most hardware security is implemented through software measures.
- The software components that support the universal HBA rely on system security features to provide secure access.

Firmware Security

The universal HBA ships with all of the firmware installed. Firmware installation is not required in the field, except for updates.

- If firmware updates are ever needed, obtain the firmware updates from the Oracle support area of the Emulex website: `http://www.emulex.com/downloads/oem-qualified/oracle/`

  You can also contact Oracle support to arrange for support or check Oracle support for the latest updates and procedures for the product.

  `https://support.oracle.com`
- Use the superuser account to set up and update the universal HBA firmware management utility. Ordinary user accounts allow users to view but not edit firmware. The Oracle Solaris OS firmware update process prevents unauthorized firmware modifications.
- Refer to the universal HBA installation guide, located on the Oracle web site, for late-breaking news, information about firmware update requirements, or other security information.
- For information about setting SPARC OpenBootPROM (OBP) security variables, refer to the *OpenBoot 4.x Command Reference Manual*.

Oracle ILOM Firmware

You can actively secure, manage, and monitor system components, such as the universal HBA, through Oracle Integrated Lights Out Manager (Oracle ILOM) firmware, which is preinstalled on some x86 servers. To understand more about using this firmware when setting up passwords, managing users, and applying security-related features, including Secure Shell (SSH), Secure Socket Layer (SSL), and RADIUS authentication, refer to Oracle ILOM documentation:

`http://www.oracle.com/pls/topic/lookup?ctx=ilom31`

System Logs

- Enable logging and send logs to a dedicated secure log host.
- Configure logging to include accurate time information, using NTP and timestamps.

Maintaining a Secure Environment

After the initial installation and setup of the universal HBA, use Oracle hardware and software security features to continue controlling hardware and tracking system assets.

The following sections are included:

- "Asset Tracking" on page 13
- "Firmware Updates" on page 14
- "Software Updates " on page 14
- "Log Security" on page 14
- "Module Security" on page 14

Asset Tracking

Use serial numbers to track inventory. Oracle embeds serial numbers in firmware on option cards and system motherboards. You can read these serial numbers through local area network connections.

You can also use wireless radio frequency identification (RFID) readers to further simplify asset tracking. Refer to an Oracle white paper, *How to Track Your Oracle Sun System Assets by Using RFID*.

Firmware Updates

Keep firmware versions current on your equipment.

- Check regularly for updates.
- All operating systems in general, and Oracle Solaris in particular, require you to log in with `root` credentials to administer the cards and to upgrade the drivers or firmware.
- Always install the latest released version of the firmware.

Software Updates

Keep your software versions current on your equipment.

- Software updates for Oracle Solaris drivers are available through Oracle Solaris patches and updates.
- Software updates for drivers for other operating systems might be available from `http://www.emulex.com/downloads/oem-qualified/oracle/`.
- Refer to the universal HBA documentation, located in the Documenation area of the Oracle website, for late-breaking news, information about software update requirements, or other security information.
- Always install the latest released version of the software.
- Install any necessary security patches for your software.
- Devices also contain firmware and might require firmware updates.

Log Security

Inspect and maintain your log files on a regular schedule.

- Review logs for possible incidents and archive them in accordance with a security policy.
- Periodically retire log files when they exceed a reasonable size. Maintain copies of the retired files for possible future reference or statistical analysis.

Module Security

The universal HBA is managed by the Emulex OneCommand Manager command-line interface (CLI) or graphical user interface (GUI) utilities. These utilities enable you to do the following:

- Monitor universal HBA operation.
- Change the operating protocol mode configuration of the universal HBA.
- Update universal HBA firmware.

The OneCommand Manager utilities provide access only to users with `root` credentials. Therefore, unprivileged users cannot make changes to the SAN environment through the use of these utilities.

For information about the OneCommand Manager CLI and GUI, see the Emulex OneCommand Manager documentation at the following website: `http://www.emulex.com`