Oracle® Storage 12 Gb/s SAS PCIe RAID HBA, Internal Security Guide

For HBA Models 7110116 and 7110117

Part No: E52900
December 2014

Contents

Oracle Storage 12 Gb/s SAS PCIe RAID HBA, Internal Security

This document provides general security principles and guidelines to consider when using the Oracle Storage 12 Gb/s SAS PCIe RAID HBA, Internal.

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.

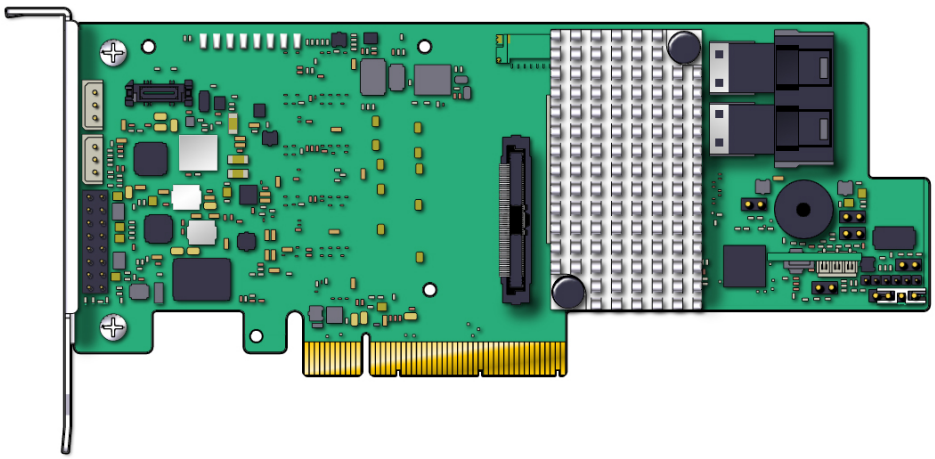
The document contains the following topics:

HBA Overview

The Oracle Storage 12 Gb/s SAS PCIe RAID HBA, Internal (marketing part numbers 7110116 and 7110117) is a PCIe 3.0, low-profile RAID controller that supports eight internal 12 Gb/s SAS/SATA ports through two SFF-8643 x4 internal Mini SAS HD connectors.

Note - SATA II is the only type of SATA supported by this HBA.

The following image shows the Oracle Storage 12 Gb/s SAS PCIe RAID HBA, Internal:



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 the Oracle Storage 12 Gb/s SAS PCIe RAID HBA, Internal.

This section contains the following topics:

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 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 HBA drivers.
- Most hardware security is implemented through software measures.
- The software components that support the HBA rely on system security features to provide secure access.

Firmware Security

The 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 LSI website: http://www.lsi.com/sep/Pages/oracle/index.aspx

  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 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 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 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 HBA, use Oracle hardware and software security features to continue controlling hardware and tracking system assets.

The following sections are included:

- "Module Security" on page 12

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.lsi.com/sep/Pages/oracle/index.aspx`.
- Refer to the HBA documentation, located at 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 HBA is managed by the LSI StorCLI command-line interface (CLI) or MegaRAID SAS graphical user interface (GUI) software. This software enables you to do the following:

- Monitor HBA operation.
- Update HBA firmware.

The StorCLI and MegaRAID SAS GUI software 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 StorCLI CLI and MegaRAID SAS GUI, see the LSI documentation at the following website: `http://www.lsi.com/sep/Pages/oracle/index.aspx`