Oracle® Storage 12 Gb SAS PCIe HBA, External Security Guide

Part No: E52902-02
October 2021

Oracle Storage 12 Gb SAS PCIe HBA, External Security Guide

Part No: E52902-02

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: E52902-02

Accès aux services de support Oracle

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

- **Overview** – Describes how to securely use the Oracle Storage 12 Gb SAS PCIe HBA, External
- **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 https://docs.oracle.com/cd/E52365_01/index.html.

Feedback

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

Oracle Storage 12 Gb SAS PCIe HBA, External Security

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

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.

When using hardware and software in your environment, follow the four basic security principles detailed in this section:

- "Access" on page 9
- "Authentication" on page 10
- "Authorization" on page 10
- "Accounting and Auditing" on page 10

Access

Access refers to physical access to hardware, or physical or virtual access to software.

- Use physical and software controls to protect your hardware and data from intrusion.
- Firmware cannot be changed except through the Oracle update process.
- Refer to the documentation that came with your software to enable the software security features.

- Install HBAs and related equipment in a locked, restricted access room.
- 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.

Authentication

Authentication is how a user is identified, typically through confidential information such as user name and password. Authentication ensures that users of hardware or software are who they say they are.

- Set up authentication features, such as a password system, in your platform operating systems to ensure that users are who they say they are.
- For user accounts: use access control lists where appropriate; set time-outs for extended sessions; set privilege levels for users.
- Ensure that your personnel use employee badges properly to enter the computer room.

Authorization

Authorization allows administrators to control what tasks or privileges a user can perform or use. Personnel can only perform the tasks and use the privileges that have been assigned to them. Authorization places restrictions on personnel who work with hardware or software.

- 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 and Auditing

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 those accounts have access to commands that if used incorrectly could cause harm to the hardware and software or incur data loss. Carefully monitor access and commands through system logs.

- Record the serial numbers of all your hardware. Use component serial numbers to track system assets. Oracle serial numbers are electronically recorded on cards, modules, and motherboards, and can be used for inventory purposes.
- To detect and track components, provide a security mark on all significant computer hardware components. Use special ultraviolet pens or embossed labels.
- Keep physical copies of hardware activation keys and licenses in a secure location that is easily accessible to the system administrator, especially during system emergencies. Printed documents might be your only proof of ownership.

Using Configuration and Management Tools Securely

Follow the security guidelines in these sections when using software and firmware tools to configure and manage your host bus adapter (HBA):

- "Oracle ILOM Security" on page 13
- "Oracle Hardware Management Pack Security" on page 14

Contact your IT Security Officer for additional security requirements that pertain to your system and specific environment.

Oracle ILOM Security

You can actively secure, manage, and monitor system components using Oracle Integrated Lights Out Manager (ILOM) management firmware, which is embedded on Oracle x86-based servers and Oracle SPARC-based servers. Depending on the authorization level granted to system administrators, functions might include the ability to power off the server, create user accounts, mount remote storage devices, and so on.

- **Use a secure, internal trusted network.**

  Whether you establish a physical management connection to Oracle ILOM through the local serial port, dedicated network management port, sideband management port, or the standard data network port, it is essential that this physical port on the server where your HBA is installed is always connected to an internal trusted network, or a dedicated secure management or private network.

  Never connect the Oracle ILOM service processor (SP) to a public network, such as the Internet. Keep the Oracle ILOM SP management traffic on a separate management network and grant access only to system administrators.

- **Limit the use of the default Administrator account.**

  Limit the use of the default Administrator account (`root`) to the initial Oracle ILOM login. This default Administrator account is provided only to aid with the initial server installation. Therefore, to ensure the most secure environment, you must change the

default Administrator password as part of the initial setup of the system. Gaining access to the default Administrator account gives a user unrestricted access to all features of Oracle ILOM. In addition, establish new user accounts with unique passwords and assign authorization levels (user roles) for each new Oracle ILOM user account. For more details, see securing Oracle ILOM user access in the *Oracle ILOM Security Guide*.

- **Carefully consider risks when connecting the serial port to a terminal server.**

  Terminal devices do not always provide the appropriate levels of user authentication or authorization that are required to secure the network from malicious intrusions. To protect your system from unwanted network intrusions, do not establish a serial connection (serial port) to Oracle ILOM through any type of network redirection device, such as a terminal server, unless the server has sufficient access controls.

  In addition, certain Oracle ILOM functions, such as password reset and the Preboot menu, are only made available using the physical serial port. Connecting the serial port to a network using an unauthenticated terminal server removes the need for physical access, and lowers the security associated with these functions.

- **Access to the Preboot menu requires physical access to the server.**

  The Oracle ILOM Preboot menu is a powerful utility that provides a way to reset Oracle ILOM to default values, and to flash firmware if Oracle ILOM were to become unresponsive. Once Oracle ILOM has been reset, a user is then required to either press a button on the server (the default) or type a password. The Oracle ILOM Physical Presence property controls this behavior (`check_physical_presence=true`). For maximum security when accessing the Preboot menu, do not change the default setting (`true`), so that access to the Preboot menu always requires physical access to the server.

- **Refer to the Oracle ILOM documentation.**

  Refer to Oracle ILOM documentation to learn more about setting up passwords, managing users, and applying security-related features, including Secure Shell (SSH), Secure Socket Layer (SSL), and RADIUS authentication. For security guidelines that are specific to Oracle ILOM, refer to the *Oracle ILOM Security Guide*, which is part of the Oracle ILOM documentation library. You can find the Oracle ILOM documentation at `https://www.oracle.com/goto/ilom/docs`.

Oracle Hardware Management Pack Security

Oracle Hardware Management Pack is available for Oracle x86-based servers and some Oracle SPARC-based servers. Oracle Hardware Management Pack features two components: an SNMP monitoring agent and a family of cross-operating system command-line interface tools (CLI Tools) for managing your hardware. The CLI Tools work with Oracle Solaris, Oracle Linux, Oracle VM, and other variants of Linux operating systems.

- **Use Hardware Management Agent SNMP Plugins.**

Simple Network Management Protocol (SNMP) is a standard protocol used to monitor or manage a system. With Hardware Management Agent SNMP Plugins, you can use SNMP to monitor Oracle servers in your data center with the advantage of not having to connect to two management points, the host and Oracle ILOM. This functionality enables you to use a single IP address (the host's IP address) to monitor multiple servers.

The SNMP Plugins run on the host operating system of Oracle servers. The SNMP Plugin module extends the native SNMP agent in the host operating system to provide additional Oracle management information base (MIB) capabilities. Oracle Hardware Management Pack itself does not contain an SNMP agent. For Linux, a module is added to the net-snmp agent. Any security settings related to SNMP for the Oracle Hardware Management Pack are determined by the settings of the native SNMP agent or service, and not by the Plugin.

For Oracle Solaris, a module is added to the Oracle Solaris Management Agent. Any security settings related to SNMP for the Oracle Hardware Management Pack are determined by the settings of the native SNMP agent or service, and not by the Plugin.

Note that SNMPv1 and SNMPv2c provide no encryption and use community strings as a form of authentication. SNMPv3 is more secure and is the recommended version to use because it employs encryption to provide a secure channel, as well as individual user names and passwords.

- **Refer to the Oracle Hardware Management Pack documentation.**

  System management products include powerful tools that require administrator or root privileges to run. With this level of access, it is possible to change hardware configuration and erase data. Refer to the Oracle Hardware Management Pack documentation for more information about these features. For security guidelines that are specific to Oracle Hardware Management Pack, refer to the *Oracle Hardware Management Pack Security Guide*, which is part of the Oracle Hardware Management Pack documentation library. You can find the Oracle Hardware Management Pack documentation at:

  `https://www.oracle.com/goto/ohmp/docs`

Planning a Secure Environment

Have security guidelines in place before the arrival of any hardware or software. After arrival, review security guidelines periodically. Adjust the guidelines to stay current with the security requirements of your organization.

Use the information in these sections before and during the installation and configuration of a server, host bus adapter (HBA), and related equipment:

- "Password Protection" on page 17
- "Operating System Security Guidelines" on page 18

Contact your IT Security Officer for additional security requirements that pertain to your specific environment.

Password Protection

Passwords are an important aspect of security since poorly chosen passwords could result in unauthorized access to company resources. Implementing password management best practices ensures that users adhere to a set of guidelines for creating and protecting their passwords. Typical components of a password policy define:

- Password length and strength
- Password duration
- Common password practice

For details about minimum password requirements, refer to the Oracle ILOM Administrator's Guide for Configuration and Maintenance *Firmware Release 5.0.x*.

Enforce the following standard practices for creating strong, complex passwords:

- Do not create a password that contains the user name, employee name, or family names.
- Do not select passwords that are easy to guess.
- Do not create passwords that contain a consecutive string of numbers such as 12345.

- Do not create passwords that contain a word or string that is easily discovered by a simple Internet search.
- Do not allow users to reuse the same password across multiple systems.
- Do not allow users to reuse previous passwords.

Change passwords on a regular basis. This helps to prevent malicious activity and ensures that passwords adhere to current password policies.

Operating System Security Guidelines

Refer to Oracle operating system (OS) documents for information about:

- How to use security features when configuring your systems.
- How to operate securely when you add applications and user access to a system.
- How to protect network-based applications.

Security Guide documents for supported Oracle operating systems are part of the documentation library for the operating system. To find the Security Guide document for an Oracle operating system, go to the Oracle operating system documentation library.

Operating System	Link to Documentation Library
Oracle Solaris OS	http://www.oracle.com/technetwork/documentation/solaris-11-192991.html
Oracle Linux OS	http://www.oracle.com/technetwork/documentation/ol-1-1861776.html

For information on operating systems from other vendors, such as Red Hat Enterprise Linux, Microsoft Windows Server, and VMware ESXi, refer to the vendor's documentation.

Maintaining a Secure Environment

After the initial installation and setup of the host bus adapter (HBA), use Oracle hardware and software security features to continue controlling hardware and tracking system assets.

Use the information in these sections to maintain a secure environment:

Contact your IT Security Officer for additional security requirements that pertain to your specific environment.

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 (LAN) connections.

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

`http://www.oracle.com/technetwork/articles/systems-hardware-architecture/o11-001-rfid-oracle-214567.pdf`

Updates for Software and Firmware

Security enhancements are introduced through new software releases and patches. Effective, proactive patch management is a critical part of system security. To maintain or increase your

system security, update your system with the more recent software release, and all necessary security patches.

- Check regularly for software or firmware updates, and security patches.
- Always install the latest released version of the software or firmware on your equipment.
- Install any necessary security patches for your software.
- 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: https://www.broadcom.com/support/oem/oracle-fc/
- Refer to the host bus adapter (HBA) documentation, located at the Oracle website, for late-breaking news, information about software update requirements, or other security information.
- Devices also contain firmware and might require firmware updates.

You can find software updates and security patches on the My Oracle Support web site at:

https://support.oracle.com

Network Security

After the networks are configured based on security principles, regular review and maintenance are needed.

To secure local and remote access to your systems, follow these guidelines:

- Limit remote configuration to specific IP addresses using SSH instead of Telnet. Telnet passes user names and passwords in clear text, potentially allowing everyone on the local area network (LAN) segment to see login credentials. Set a strong password for SSH.
- Use version 3 of Simple Network Management Protocol (SNMP) to provide secure transmissions. Earlier versions of SNMP are not secure and transmit authentication data in unencrypted text. SNMPv3 uses encryption to provide a secure channel as well as individual user names and passwords.
- Change the default SNMP community string to a strong community string if SNMPv1 or SNMPv2 is necessary. Some products have PUBLIC set as the default SNMP community string. Attackers can query a community to draw a very complete network map and possibly modify management information base (MIB) values.
- Always log out after using the system controller if the system controller uses a browser interface.

- Enable necessary network services and configure these services securely. Disable unnecessary network services, such as Transmission Control Protocol (TCP) or Hypertext Transfer Protocol (HTTP).
- Use LDAP security measures when using LDAP to access the system.
- Create a banner message that appears at login to state that unauthorized access is prohibited. You can inform users of any important policies or rules. The banner can be used to warn users of special access restrictions for a given system, or to remind users of password policies and appropriate use.
- Use access control lists to apply restrictions, where appropriate.
- Set time-outs for extended sessions and set privilege levels.
- Use these network services in very secure environments as they are secured by certificates and other forms of strong encryption to protect the channel:
  - Active Directory
  - LDAP/SSL (Lightweight Directory Access Protocol/Secure Socket Layer)
- Use these network services on private, secure networks where there are no suspected malicious users:
  - RADIUS (Remote Authentication Dial In User Service)
  - TACACS+ (Terminal Access Controller Access-Control System)
- Implement port security to limit access based upon a MAC address. Disable auto-trunking on all ports.

For more information about network security, refer to the *Oracle ILOM Security Guide*, which is part of the Oracle ILOM documentation library. You can find the Oracle ILOM documentation at:

`https://www.oracle.com/goto/ilom/docs`

Module Security

The HBA is managed by the OneCommand Manager command-line interface (CLI) and graphical user interface (GUI) or MegaRAID SAS graphical user interface (GUI) software. This software enables you to do the following. These utilities enable you to do the following:

- Monitor HBA operation.
- Change the operating protocol mode configuration of the HBA.
- Update 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 Broadcom OneCommand Manager documentation at the following website: https://www.broadcom.com/support/oem/oracle-fc/

Log Maintenance

Inspect and maintain your log files on a regular schedule. Use these methods to secure log files:

- Enable logging and send system logs to a dedicated secure log host.
- Configure logging to include accurate time information, using Network Time Protocol (NTP) and timestamps.
- Perform regularly scheduled scans of network device logs for unusual network activity or access.
- 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.