Oracle Dual Port QDR InfiniBand Adapter M3

Security Guide

Part No.: E48585-01
September 2013

Please
Recycle

Adobe PostScript

Contents

Oracle Dual Port QDR InfiniBand Adapter M3 Security Guide

This document provides general security guidelines to help you protect Oracle hardware products such as servers, network switches, network interface cards, adapters, and so on.

The following sections are in this chapter:

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 authorization 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 cards, modules, and motherboards.

Planning a Secure Environment

Use the following notes for the installation and configuration of a server and related equipment.

Hardware Security

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

- **Restrict access**
  - Install servers 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.
  - Restrict access to USB consoles, which can provide more powerful access than SSH connections. Devices such as system controllers, power distribution units (PDUs), and network switches can have USB connections.
  - Restrict access to hot-plug or hot-swap devices in particular because they can be easily removed.
  - Store spare field-replaceable units (FRUs) and customer-replaceable units (CRUs) in a locked cabinet. Restrict access to the locked cabinet to authorized personnel.

- **Record serial numbers**
  - Security-mark all significant items of computer hardware such as FRUs. Use special ultraviolet pens or embossed labels.
  - Keep a record of the serial numbers of all your hardware.
  - Keep hardware activation keys and licenses in a secure location that is easily accessible to the system manager in system emergencies. The printed documents might be your only proof of ownership.

Software Security

Most hardware and software security is implemented through software measures.

- Refer to the documentation that came with your software to enable any security features available for the software.
- Implement port security to limit access based upon MAC addresses. Disable auto-trunking on all ports.
- Use a dedicated network for service processors to separate them from the general network.
- You can boot a system securely over a wide area network (WAN) or a storage area network (SAN). For information about using WAN Boot or iSCSI Boot for secure booting, refer to the Oracle Solaris Installation Guide: Network-Based Installations book for your Oracle Solaris operating system release.
- Change all default passwords when installing a new system. Most types of equipment use default passwords, such as changeme, that are widely known and would allow unauthorized access to the equipment.
- Change every password on network switches which might have multiple user accounts and passwords by default.

Oracle Solaris OS Guidelines

Refer to Oracle Solaris Security Guidelines documents for information on:

- How to harden Oracle Solaris
- How to use Oracle Solaris security features when configuring your systems
- How to operate securely when you add applications and users to a system
- How to protect network-based applications

Oracle Solaris Security Guidelines documents can be found at:

- http://www.oracle.com/technetwork/indexes/documentation/index.html#sys_sw

Network Switches

Different switches offer different levels of port security features. Refer to the switch documentation to learn how to do the following:

- Use authentication, authorization, and accounting features for local and remote access to the switch.
- Manage switches out-of-band (separated from data traffic). If out-of-band management is not feasible, then dedicate a separate VLAN number for in-band management.
- Use the port mirroring capability of the network switch for intrusion detection system (IDS) access.
- Maintain a switch configuration file off-line and limit access only to authorized administrators. The configuration file should contain descriptive comments for each setting.
- Use these port security features if they are available on your switch:
  - **MAC Locking** involves tying a Media Access Control (MAC) address of one or more connected devices to a physical port on a switch. If you lock a switch port to a particular MAC address, superusers cannot create backdoors into your network with rogue access points.
  - **MAC Lockout** disables a specified MAC address from connecting to a switch.
  - **MAC Learning** uses the knowledge about each switch port's direct connections so the network switch can set security based on current connections.

Oracle Firmware Security

Use the superuser account to set up and update the OpenBoot PROM (OBP) or other Oracle firmware. Ordinary user accounts allow users to view but not edit firmware. The Oracle Solaris OS firmware update process prevents unauthorized firmware modifications.

For information for setting OBP security variables, refer to the *OpenBoot 4.x Command Reference Manual* at:

- http://download.oracle.com/docs/cd/E19455-01/816-1177-10/cfg-var.html#pgfId-17069

Oracle ILOM Firmware

You can actively secure, manage, and monitor system components through Oracle Integrated Lights Out Manager (Oracle ILOM) management firmware which is preinstalled on some SPARC servers.

Refer to Oracle ILOM documentation to understand more about setting up passwords, managing users, and applying security-related features, including Secure Shell (SSH), Secure Socket Layer (SSL), and RADIUS authentication:

- http://docs.oracle.com/cd/E37444_01/index.html

VLAN Security

If you set up a virtual local area network (VLAN), remember that VLANs share bandwidth on a network and require additional security measures.

- Define virtual local area networks (VLANs) to separate sensitive clusters of systems from the rest of the network. This decreases the likelihood that users will gain access to information on these clients and servers.
- Assign a unique native VLAN number to trunk ports.
- Limit the VLANs that can be transported over a trunk to only those that are strictly required.
- Disable VLAN Trunking Protocol (VTP), if possible. Otherwise, set the following for VTP: management domain, password and pruning. Then set VTP into transparent mode.

Infiniband Security

Infiniband security is a function of the Infiniband Fabric and the Subnet Manager (SM) running in the IB fabric. For more information about securing InfiniBand and supported switches, which also run the SM, see the InfiniBand Switch Security Guide for the applicable switch:

- For Sun Datacenter InfiniBand Switch 36, see the *Sun Datacenter InfiniBand Switch 36 Hardware Security Guide* at:

  http://docs.oracle.com/cd/E36265_01/

- For Sun Network QDR InfiniBand Gateway Switch, see the *Sun Network QDR InfiniBand Gateway Switch Hardware Security Guide* at:

  http://docs.oracle.com/cd/E36256_01/

- For the IB switch and SM on an Oracle Virtual Network InfiniBand switch, see:

  http://docs.oracle.com/cd/E38500_01/

User Accounts

- Set up RADIUS and TACACS+ access protocols if possible:

  RADIUS (Remote Authentication Dial In User Service) is a client/server protocol that secures networks against unauthorized access.

  TACACS+ (Terminal Access Controller Access-Control System) is a protocol that permits a remote access server to communicate with an authentication server to determine if a user has access to the network.

- Limit the use of the root superuser account. Instead, assign Oracle Integrated Lights Out Manager (Oracle ILOM) accounts such as `ilom-operator` and `ilom-admin` whenever possible.
- Use access control lists where appropriate.
- Set time-outs for extended sessions.
- Set privilege levels.
- Create a system banner to remind the user that unauthorized access is prohibited.

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

Hardware Power Control

You can use software to turn on and off power to some Oracle systems. The power distribution units (PDUs) for some system cabinets can be enabled and disabled remotely. Authorization for these commands is typically set up during system configuration and is usually limited to system administrators and service personnel. Refer to your system or cabinet documentation for further information.

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. 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

Keep your software and firmware versions current on your server equipment.

- Check regularly for updates.
- Always install the latest released version of the software or firmware.
- Install any necessary security patches for your software.
- Remember that devices such as network switches also contain firmware and might require patches and firmware updates.

Network Access

Follow these guidelines to secure local and remote access to your systems:

- Implement port security to limit access based upon a MAC address. Disable auto-trunking on all ports.
- 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 LAN segment to see login credentials. Set a strong password for SSH.
- Use version 3 of SNMP to provide secure transmissions. Earlier versions of SNMP are not secure and transmit authentication data in unencrypted text.
- Change the default SNMP community string to a strong community string if SNMP 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 it uses a browser interface.
- Disable unnecessary network services, such as TCP small servers or HTTP. Enable necessary network services and configure these services securely.

Data Protection

Follow these guidelines to maximize data security:

- Back up important data using devices such as external hard drives, pen drives, or memory sticks. Store the backed up data in a second, off-site, secure location.
- Use data encryption software to keep confidential information on hard drives secure.
- When disposing of an old hard drive, physically destroy the drive or completely erase all the data on the drive. Information can still be recovered from a drive after files are deleted or the drive has been reformatted. Deleting the files or reformatting the drive removes only the address tables on the drive. Use disk wiping software to completely erase all data on a drive.

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.