Sun Network QDR InfiniBand Gateway Switch

Hardware Security Guide

Part No.: E26703-02
March 2013

Please
Recycle

Adobe PostScript

Contents

Sun Network QDR InfiniBand Gateway Switch Security Guide

This document provides general security guidelines to help you protect the Sun Network QDR InfiniBand Gateway Switch.

Topics discussed include:

Understanding Security Principles

The the four As (AAAA) of basic security principles are: 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 gateway to ensure that users are who they say they are.

  Ensure that your personnel use employee badges properly to enter the data center.

- **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 and Oracle ILOM logs to monitor user logins. Monitor the `root`, `ilom-admin`, and root-privileged accounts in particular because these accounts can access powerful commands.
  - Use component serial numbers to track system assets. Oracle serial numbers are physically marked on chassis and electronically recorded on all management controllers and main boards.

Planning a Secure Environment

Review these topic before and during the installation and configuration of the gateway.

Hardware Security

Physical hardware can be secured simply by limiting access to the hardware and recording serial numbers.

- **Restrict access**
  - Install the gateway in a locked, restricted access room.
  - If equipment is installed in a rack with a locking door, keep the door secured at all times.
  - Restrict access to USB consoles at the gateway itself. USB consoles permit greater privileges to user management, and error and debug messaging. USB consoles are also less secure than SSH connections.
  - Restrict access to power supplies, fan modules, and transceivers in particular because they can be easily removed.

- Store spare replaceable components in a locked cabinet. Allow access to the locked cabinet by authorized personnel only.

- **Record serial numbers**
  - Security-mark all significant items including replaceable components. Use special ultraviolet pens or embossed labels.
  - Keep a serial number record of all your hardware.
  - Keep copies of invoices, purchasing records, and licenses in a secure location that is easily accessible to the system manager during system emergencies. These printed documents might be the only proof of ownership.

Software Security

Most hardware security is implemented through software measures.

- Refer to the gateway documentation for additional guidelines to implement security features within the firmware.
- Refer to the documentation with the BXOFED software to enable any security features available for the software suite.
- Implement port security to limit access based upon MAC addresses. Disable auto-trunking on all ports.
- Manage the gateway out-of-band on a separate dedicated network. This management network is separate from data traffic and the general network.
- If out-of-band management is not feasible, then dedicate a unique VLAN number solely for in-band management.
- Change all default passwords when installing a new gateway. The gateway has four default user accounts and respective passwords:
  - **`ilom-admin`** – The `ilom-admin` user has administrator privileges for the CLI, web, and IPMI interfaces. The default password is `ilom-admin`. Change the password with the Oracle ILOM `set /SP/users/ilom-admin password` command.
  - **`ilom-operator`** – The `ilom-operator` user has read-only privileges for the CLI and web interfaces. The default password is `ilom-operator`. Change the password with the Oracle ILOM `set /SP/users/ilom-operator password` command.
  - **`root`** – The `root` user has superuser privileges. The default password is `changeme`. Change the password with the `passwd` command.
  - **`nm2user`** – The `nm2user` has read-only privileges for the CLI interface. The default password is `changeme`. Change the password with the `passwd` command.
- Schedule and regularly change every password on the gateway, especially when configured with additional user accounts.

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 the gateway.

To understand more about using this firmware when setting up passwords, managing users, and applying security-related features, refer to Oracle ILOM documentation:

- http://www.oracle.com/pls/topic/lookup?ctx=E19860-01

VLAN Security

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

- Define VLANs so as 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

Keep Infiniband hosts and switches secure. An Infiniband fabric is only as secure as its least secure Infiniband switch.

- Configure the Subnet Managers and switches to use *secret* M_Keys.
  - If you configure only readable M_Keys, you prevent *inccidental* misconfiguration and elevate the threshold for Subnet Manager attacks.
  - If you configure secret M_Keys, you prevent *intentional* misconfiguration of the InfiniBand fabric by effectively excluding unauthorized Subnet Manager.
- Partitioning and implementing P_Keys do not protect an Infiniband fabric. Partitioning only offers Infiniband traffic isolation between partitions.
- Use static VLAN configurations when possible.
- Disable unused gateway ports and assign them an unused VLAN number.

User Accounts

- The gateway firmware does not support RADIUS authentication. It is important to administer local user management on the gateway.
- 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.

Asset Tracking

Use serial numbers to track inventory. Oracle embeds serial numbers in firmware on management controllers. Refer to the gateway documentation for instructions how to read these serial numbers.

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 BXOFED software and firmware versions current on your gateway.

- Check regularly for updates.
- Always install the latest released version of the software or firmware.
- Install any necessary security patches for the BXOFED software.

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.
- Configure and use version 3 (v3) of SNMP to provide secure transmissions. Versions v1 and v2c of SNMP are not secure and transmit authentication data in unencripted text.
- Change the default SNMP community string (PUBLIC) to a strong community string if SNMP is necessary. Attackers can query a community to draw a very complete network map and possibly modify management information base (MIB) values.
- Do not enable SNMP `set` requests unless absolutely necessary. If enabled, create separate SNMP v3 users with read-only and read-write permissions.
- Always log out after accessing the management controller through the web interface.
- Disable unused or unnecessary services, such as TCP small servers or HTTP. Only enable necessary services and configure these services securely.

Data Protection

Follow these guidelines to maximize data security:

- Backup gateway configuration files to remote, secure locations and limit their access to authorized administrators only. The configuration files should contain descriptive comments for each setting.
- Use data encryption software to keep confidential information on hard drives secure.
- The management controller's filesystem contains data equivalent to a system hard drive. When replacing an old management controller, physically destroy the controller or completely erase all the data in the controller's filesystem. Use disk wiping software to completely erase all data on the filesystem.

Log Security

Inspect and maintain your log files on a regular schedule.

- Review both system and Oracle ILOM logs for possible incidents and archive them in accordance with a security policy.
- Periodically archive and clear log files when they exceed a reasonable size. Maintain the archives in a secure location for possible future reference or statistical analysis.