Sun Server X2-8

Security Guide

Part No: E49450–01
September 2013

130919@25097

Contents

Overview

This document provides general security guidelines to help you protect the Sun Server X2-8, its network interfaces, and the network switches to which it is connected.

System Overview

The Sun Server X2-8 is a rack-mounted server containing two or four CPU modules with two cores each. It supports eight 2.5 inch small form-factor SAS-2 hot-pluggable, dual-port, enterprise-class hard drives, slots for eight PCIe cards, and two network express modules,.

The Sun Server X2-8 includes an onboard service processor (SP) that supports Oracle Integrated Lights Out Manager (ILOM). Oracle ILOM provides secure local and remote management.

Security Principles

Basic security consists of four principles: access, authentication, authorization, and accounting.

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.
- Refer to the documentation that came with your software to enable any security features available for the software.
- 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 connectors or ports, which can provide more powerful access than SSH connections. Devices such as system controllers, power distribution units (PDUs), and network switches provide connectors and ports.
- 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.

Authentication consists of ensuring 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.
- Ensure that your personnel use employee badges properly to enter the computer room.
- For user accounts: use access control lists where appropriate; set time-outs for extended sessions; set privilege levels for users.

Authorization refers to restrictions that limit access to hardware and software.

- Allow personnel to work only with hardware and software *that is relevant to their job description, and* 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 refers to software and hardware features used to monitor login activity and maintenance of hardware inventories.

- Use system logs to monitor user logins. Monitor system administrator and service accounts in particular because those accounts can access powerful commands.
- Keep a record of the serial numbers of all your hardware. Use component serial numbers to track system assets. Oracle part numbers are electronically recorded on cards, modules, and components.
- To detect and track components, provide a security mark on all significant items of computer hardware such as FRUs. Use special ultraviolet pens or embossed labels.

Using Server Configuration and Management Tools

Follow these security guidelines when using software and firmware tools to configure and manage your server.

Oracle ILOM Security

Oracle ILOM provides server control and monitoring functions to system administrators on Oracle x86-based servers and on some Oracle SPARC-based servers.

Use a dedicated internal network for the service processor (SP) to separate it from the general network. Depending on the authorization level granted to the administrators, these functions might include the ability to power off the server, create user accounts, mount remote storage devices, and so on. Therefore, to maintain the most reliable and secure environment for Oracle ILOM, the dedicated network management port or the sideband management port on the server must always be connected to an internal trusted network or a dedicated secure management/private network.

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 sever installation. To ensure the most secure environment, change the default Administrator password (`changeme`) during the initial setup of the system. In addition to changing the password for the default Administrator account, new user accounts with unique passwords and assigned authorization levels should be established for each new Oracle ILOM user.

The *Oracle Integrated Lights Out Manager (ILOM) 3.1 Security Guide* provides security information specific to Oracle ILOM.

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. For security guidelines specific to Oracle ILOM, refer to the *Oracle Integrated Lights Out Manager (ILOM) 3.1 Security Guide*, which is part of the Oracle ILOM 3.1 documentation library. You can find the Oracle ILOM 3.1 documentation at `http://www.oracle.com/goto/ILOM/docs`.

The Sun Server X2-8 uses Oracle ILOM 3.0, not Oracle ILOM 3.1. However, most of the information in the *Oracle Integrated Lights Out Manager (ILOM) 3.1 Security Guide* is relevant to Oracle ILOM 3.0, with the following exceptions:

- *Web Interface Timeout*: In Oracle ILOM 3.1, the administrator can set the timeout for all sessions and it can not be overridden in individual sessions. In Oracle ILOM 3.0, the timeout can be set for each session. The default is 15 minutes.
- *Event Log and Audit Log*: Oracle ILOM 3.1 has both an event log and an audit log. Oracle ILOM 3.0 has only an event log, however the Oracle ILOM 3.0 event log contains the same entries as the Oracle ILOM 3.1 event log and audit log.
- *Ethernet-over-USB*: Oracle ILOM 3.0 does not support a high-speed Ethernet-over-USB connection.

Oracle Hardware Management Pack Security

Oracle Hardware Management Pack is available for your server, and for many other x86-based servers and some SPARC servers. Oracle Hardware Management Pack features two components:

- *SNMP monitoring agent*: With the Hardware Management Agent SNMP Plugins, you can use SNMP to monitor Oracle servers and server modules 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 and server modules. The SNMP Plugins run on the host operating system of Oracle servers.
- *Cross-operating system command line interface tools (CLI)*: You can use the Oracle Server CLI Tools to configure Oracle servers. The CLI Tools work with Oracle Solaris, Oracle Linux, Oracle VM, other variants of Linux, and Microsoft Windows operating systems.

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 (HMP) Security Guide, which is part of the Oracle Hardware Management Pack documentation library. You can find the Oracle Hardware Management Pack documentation at:

`http://www.oracle.com/goto/OHMP/docs`

Planning a Secure Environment

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

The following topics are included:

Operating System Security Guidelines

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

- How to use 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

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
Oracle Solaris OS	`http://docs.oracle.com/cd/E23824_01/html/819-3195/index.html`
Linux OS	`http://linux.oracle.com`
Windows OS	For information on non-Oracle operating systems, refer to the vendor's documentation.
Oracle VM OS	`http://www.oracle.com/technetwork/documentation/vm-096300.html`

Operating System	Link
VMware OS	For information on non-Oracle operating systems, refer to the vendor's documentation.

Network Ports and 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.
- Change every password on network switches that might have multiple user accounts and passwords by default.
- Manage switches out-of-band (separated from data traffic). If out-of-band management is not feasible, then dedicate a separate virtual local area network (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.
- Implement port security to limit access based upon MAC addresses. Disable auto-trunking on all ports.
- Use these port security features if they are available on your switch:
  - **MAC Locking** involves associating 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 that the network switch can set security based on current connections.

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 VLANs to separate sensitive clusters of systems from the rest of the network. This decreases the likelihood of users gaining 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 secure. An Infiniband fabric is only as secure as its least secure Infiniband host.

- Note that partitioning does not protect an Infiniband fabric. Partitioning only offers Infiniband traffic isolation between virtual machines on a host.
- Use static VLAN configuration when possible.
- Disable unused switch ports and assign them an unused VLAN number.

Hardware Physical Security

Physical hardware can be secured by simply limiting access to the hardware and by recording 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. Lock the door after servicing the equipment.
  - Restrict access to 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) or 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 security is implemented through software measures.

- 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.
- Limit use of the root superuser account. Oracle Integrated Lights Out Manager (Oracle ILOM) accounts such as ilom-operator and ilom-admin should be used instead whenever possible.
- Use a dedicated network for service processors to separate them from the general network.
- Protect access to consoles. Devices such as system controllers, power distribution units (PDUs), and network switches can have USB connections, which can provide more powerful access than SSH connections.
- 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 on MAC addresses. Disable autotrunking on all ports.

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 your server. 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 mother boards. 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 on your equipment.
- Install any necessary security patches for your software.
- Remember that devices such as network switches and Express Modules also contain firmware and might require patches and firmware updates.

Network Access

Follow these guidelines to ensure the security of local and remote access to your systems:

- 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 Simple Network Management Protocol (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 especially if using a browser interface.
- Disable unnecessary network services, such as Transmission Control Protocol (TCP) or Hypertext Transfer Protocol (HTTP). Enable necessary network services and configure these services securely.
- Follow LDAP security measures when using LDAP to access the system. Refer to the Oracle ILOM Security Guide.
- Create a banner to state that unauthorized access is prohibited.
- Use access control lists where appropriate.
- Set time-outs for extended sessions and set privilege levels.
- Use authentication, authorization, and accounting (AAA) features for local and remote access to a switch.
- If possible, use the RADIUS and TACACS+ security protocols:
  - 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.
- Use the port mirroring capability of the switch for intrusion detection system (IDS) access.
- Implement port security to limit access based on 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.

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. Deleting all 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 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.
- 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.