Sun Server X2-4

Security Guide

Part No.: E50751-01
May 2014

Please
Recycle

Adobe PostScript

Contents

Sun Server X2-4 Security Guide

This document provides general security guidelines to help you protect your Oracle server, server network interfaces, and connected network switches.

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

The following sections are in this chapter:

Basic Security

There are basic security principles that you should adhere to when using all hardware and software. This section covers the four basic security principles:

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.

- Change all default passwords when installing a new system. Most types of equipment use default passwords, such as `changeme`, that are widely known and could allow unauthorized access to hardware or software.
- 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 physical access to USB ports, network ports, and system consoles. Servers and network switches have ports and console connections, which provide direct access to the system.
- Restrict the capability to restart the system over the network.
- 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

Authentication is how a user is identified, typically through confidential information such as user name and password. Authentication ensures that users of hardware and 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

Authorization allows administrators to control what tasks or privileges a user may perform or use. Personnel can only perform the tasks and use the privileges that have been assigned to them. Authorization refers to restrictions placed on personnel to 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

Accounting and auditing refer to maintaining a record of a user's activity on the system. Oracle servers have hardware and software features that allow administrators to monitor login activity and to 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 system or incur data loss. Access and commands should be carefully monitored through system logs.
- Record 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 motherboards, and can be used for inventory purposes.
- To detect and track components, provide a security mark on all significant items of computer hardware such as FRUs and CRUs. Use special ultraviolet pens or embossed labels.

Using Server Configuration and Management Tools Securely

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

- "Oracle Hardware Installation Assistant Security" on page 3
- "Oracle ILOM Security" on page 4
- "Oracle Hardware Management Pack Security" on page 5

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

Oracle Hardware Installation Assistant Security

Oracle Hardware Installation Assistant is an application that you can use for initial server configuration. This application helps you update firmware (Oracle ILOM firmware, BIOS, and RAID controller software) and to automate installation of a Linux or Microsoft Windows operating system. For more details, refer to the *Oracle Hardware Installation Assistant 2.5 User's Guide for x86 Servers* at:

`http://www.oracle.com/pls/topic/lookup?ctx=hia`

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, and mount remote storage devices.

- **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, or the standard data network port, it is essential that this physical port on the server 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. You should 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 (`changeme`) 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.

- **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. 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:

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

Oracle Hardware Management Pack Security

Oracle Hardware Management Pack is available for your server, and for many other 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 server.

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

SNMP is a standard protocol used to monitor or manage a system. With the 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 MIB capabilities. Oracle Hardware Management Pack itself does not contain an SNMP agent. For Linux, a module is added to the net-snmp agent. For Oracle Solaris, a module is added to the Solaris Management Agent. For Microsoft Windows, the Plugin extends the native SNMP service. 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.**

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

Security guidelines should be in place before the arrival of the system. After arrival, security guidelines should be periodically reviewed and adjusted to stay current with the security requirements of your organization.

Use the information in this section before and during the installation and configuration of a server and related equipment.

Contact your IT Security Officer for additional security requirements that pertain to your system and 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 should define:

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

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 old 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 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:

- **Oracle Solaris 10 1/13** - http://www.oracle.com/goto/Solaris10/docs
- **Oracle Solaris 11.x** - http://www.oracle.com/goto/Solaris11/docs
- **Oracle Linux 6** - http://www.oracle.com/technetwork/documentation/ol-1-1861776.html
- **Oracle VM 3.x** - http://www.oracle.com/technetwork/documentation/vm-096300.html

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

Network Switches and Port Security

Network 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.

- Separate sensitive clusters of systems from the rest of the network when using VLANs. 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.

- Use static VLAN configuration, when possible.
- Disable unused switch ports and assign them an unused VLAN number.

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.

Maintaining a Secure Environment

After the initial installation and setup, use Oracle hardware and software security features to continue controlling hardware and software assets.

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

Power Control

You can use software to turn power on and off 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 (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. For best security practices, update your system with the most recent software release, and all necessary security patches.

- Check regularly for software updates and security patches.
- 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 Security

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

Follow these guidelines to secure 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 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.

- 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 the system controller uses 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.
- 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 authentication, authorization, and accounting 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.
- Follow LDAP security measures when using LDAP to access the system.
- 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.

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 documentaiton at:

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

Data Protection and Security

Follow these guidelines to maximize data protection and security:

- Back up important data using devices such as external hard drives or USB storage devices. 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 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.