Netra Blade X3-2B (formerly Sun Netra X6270 M3 Server Module)

Security Guide

Part No.: E26849-04
November 2012

Please
Recycle

Adobe PostScript™

Contents

Overview

The following topics are covered in this overview:

- "Product Overview" on page 1
- "Basic Security Principles" on page 1

Product Overview

The Sun Blade X6270 M3 server module is an enterprise class server blade that supports 2P (two processor) configurations. The server module has a standard Sun Blade 6000 chassis blade form factor, layout, airflow, and compatibility with RAID expansion modules (REMs) and fabric expansion modules (FEMs). The Sun Blade X6270 M3 server module is based on two Intel (R) Xeon (R) processors in the E5-2600 family, and the Intel C600 series chipset. The Sun Blade X6270 M3 server module includes an on-board Oracle ILOM service processor (SP).

Basic Security Principles

There are four basic security principles: access, authentication, authorization, and accounting.

Access

Use physical and software controls to protect your hardware or data from intrusion.

- For hardware, access limits usually mean physical access limits.
- For software, access limits usually mean both physical and virtual means.
- Firmware cannot be changed except through the Oracle update process.

Authentication

Set up all authentication features such as a password system in your platform operating systems to verify that users are who they say they are.

Authentication provides varying degrees of security through measures such as badges and passwords. For example, ensure that personnel use employee badges properly to enter a computer room.

Authorization

Authorization allows company personnel to work only with hardware and software that they are trained and qualified to use.

For example, set up a system of Read/Write/Execute permissions to control user access to commands, disk space, devices, and applications.

Accounting

Customer IT personnel can use Oracle software and hardware features to monitor login activity and maintain hardware inventories.

- Use system logs to monitor user logins. In particular, track System Administrator and Service accounts through system logs because these accounts can access powerful commands.
- Periodically retire log files when they exceed a reasonable size, in accordance with the customer company policy. Logs are typically maintained for a long period, so it is essential to maintain them.
- Use component serial numbers to track system assets for inventory purposes. Oracle part numbers are electronically recorded on all cards, modules, and mother boards.

Planning a Secure Environment

This section provides guidelines for use before and during the installation and configuration of a server and related equipment.

The following topics are covered:

- "Hardware Physical Security" on page 3
- "Software Security" on page 4
- "Oracle ILOM Firmware" on page 5
- "Operating System Security Guidelines" on page 5
- "Oracle System Assistant Security Information" on page 5

Hardware Physical Security

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

The following topics are covered:

- "Restrict Access" on page 3
- "Record Serial Numbers" on page 4

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 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) 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 USB 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 upon MAC addresses. Disable autotrunking on all ports.

Oracle ILOM Firmware

You can actively secure, manage, and monitor system components through Oracle Integrated Lights Out Manager (Oracle ILOM). Oracle ILOM management firmware is preinstalled on the SP on the Sun Netra X6270 M3 server module.

To understand more about using this firmware when setting up passwords, managing users, and applying security-related features, including Secure Shell (SSH), Secure Socket Layer (SSL), and RADIUS authentication, refer to Oracle Integrated Lights Out Manager (Oracle ILOM) documentation:

http://www.oracle.com/pls/topic/lookup?ctx=ilom31

Operating System Security Guidelines

Operating System	Link
Oracle Solaris OS	http://docs.oracle.com/cd/E23824_01/html/819-3195/index.html
Oracle Linux OS	http://linux.oracle.com/documentation/
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
VMware OS	For information on non-Oracle operating systems, refer to the vendor's documentation.

Oracle System Assistant Security Information

The following post-installation topics are covered:

- "Understanding that OSA Contains a Bootable Root Environment" on page 6

Understanding that OSA Contains a Bootable Root Environment

Oracle System Assistant is an application running on a pre-installed, internal USB flash drive. It is built on top of a bootable linux root environment. OSA also provides the ability to access its underlying root shell. Users who have physical access to the system, or who have Remote KVMS access to the system through ILOM, will be able to access OSA and the root shell.

A root environment can be used to change ILOM configuration, system policies, as well as access data on other disks. It is recommended that physical access to the server be protected and the administrator and console privileges for ILOM users be assigned sparingly. Encrypting the operating system filesystem will also prevent root shell users of OSA from being able to read disk contents.

Understanding that OSA Mounts a USB Storage Device Accessible to the OS

In addition to being a bootable environment, Oracle System Assistant is also mounted as a USB storage device accessible to the host operating system after installation. This is useful in accessing tools and drivers for maintenance and reconfiguration. The OSA flash device is both readable and writable and could be a potential filesystem exploited by viruses.

It is recommended that the same methods for protecting disks be applied to the OSA storage device including regular virus scans and integrity checks.

Disabling OSA

Oracle System Assistant can be a useful tool in helping setup a server, update and configure firmware, and install the host operating system.However, if the security implications mentioned above are undesirable or if the tool is simply not needed, OSA itself can also be disabled. Disabling OSA means that the USB storage device will no longer be accessible to the host operating system. In addition, it will not be possible to boot to Oracle System Assistant.

It is possible to disable Oracle System Assistant from either OSA itself or from BIOS. Once disabled, it can only be re-enabled from BIOS Setup. It is recommended that BIOS Setup be password-protected such that only authorized users can re-enable OSA.

See the Oracle System Assistant documentation for instructions on how to disable OSA or refer to the Netra Blade X3-2B Administration Guide.

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.

The following topics are covered:

Oracle ILOM Security

Refer to the Oracle ILOMSecurity Guide for further information on Oracle Integrated Lights OutManager (Oracle ILOM).

For general Oracle ILOM information refer to:

`http://www.oracle.com/pls/topic/lookup?ctx=ilom31`

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.

See 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`

Maintaining 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.
- Devices such as network switches, and ExpressModules also contain firmware and might require patches and firmware updates.

Local and Remote Access

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

- 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 upon aMAC address. Disable autotrunking 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.
- Early versions of SNMP are not secure and transmit authentication data in unencrypted text. Only version 3 of SNMP can provide secure transmissions.
- Some products come out of the box with 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. If SNMP is necessary, change the default SNMP community string to a strong community string.
- Enable logging and send logs to a dedicated secure log host.
- Configure logging to include accurate time information, using NTP and timestamps.
- Review logs for possible incidents and archive them in accordance with the security policy.
- If your system controller uses a browser interface, be sure to log out after using it.

Data Security

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.
- Data destruction: 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 will remove only the address tables on the drive - information can still be recovered from a drive after deleting files or reformatting the drive. (Use disk wiping software to completely erase all data on a drive.)