SPARC M5-32 and SPARC M6-32 Servers Security Guide

Part No: E41219-03
March 2015

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc`.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit `https://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` or visit `https://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` if you are hearing impaired.

Accessibilité de la documentation

Pour plus d'informations sur l'engagement d'Oracle pour l'accessibilité à la documentation, visitez le site Web Oracle Accessibility Program, à l'adresse `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc`.

Accès au support électronique

Les clients Oracle qui ont souscrit un contrat de support ont accès au support électronique via My Oracle Support. Pour plus d'informations, visitez le site `https://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` ou le site `https://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` si vous êtes malentendant.

Contents

Understanding Hardware Security

Physical isolation and access control are the foundation on which you should build the security architecture. Ensuring that the physical server is installed in a secure environment protects it against unauthorized access. Likewise, recording all serial numbers helps to prevent theft, resale, or supply chain risk (that is, injection of counterfeit or compromised components into your organization's supply chain).

This chapter provides general hardware security guidelines for the SPARC M5-32 and M6-32 servers.

The following sections are in this chapter:

Access Restrictions

- Install servers and related equipment in a locked, restricted access room.
- If equipment is installed in a rack with a locking door, always lock the rack door until you have to service the components within the rack. Locking the doors also restricts access to hot-plug or hot-swap devices.
- Store spare field-replaceable units (FRUs) or customer-replaceable units (CRUs) in a locked cabinet.Restrict access to the locked cabinet to authorized personnel.
- Periodically, verify the status and integrity of the locks on the rack and the spares cabinet to guard against, or detect, tampering or doors being left unlocked.
- Store cabinet keys in a secure location with limited access.
- Restrict access to USB consoles. Devices such as system controllers, power distribution units (PDUs), and network switches can have USB connections. Physical access is a more secure method of accessing a component since it is not susceptible to network-based attacks.
- Connect the console to an external KVM to enable remote console access. KVM devices often support two-factor authentication, centralized access control, and auditing. For more information about the security guidelines and best practices for KVMs, refer to the documentation that came with the KVM device.

Serial Numbers

- Keep a record of the serial numbers of all your hardware.
- Security-mark all significant items of computer hardware such as replacement parts. Use special ultraviolet pens or embossed labels.
- 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.

Wireless RFID readers can further simplify asset tracking. For more information, read *How to Track Your Oracle Sun System Assets by Using RFID* at:

http://www.oracle.com/technetwork/articles/systems-hardware-architecture/o11-001-rfid-oracle-214567.pdf

Hard Drives

Hard drives are often used to store sensitive information. To protect this information from unauthorized disclosure, sanitize hard drives prior to reusing, decommissioning, or disposing of them.

- Use disk-wiping tools such as the Oracle Solaris format (1M) command to completely erase all data from the disk drive.
- Organizations should refer to their data protection policies to determine the most appropriate method to sanitize hard drives.
- If required, take advantage of Oracle's Customer Data and Device Retention Service http://www.oracle.com/us/support/library/data-retention-ds-405152.pdf

Understanding Software Security

Most hardware security is implemented through software measures. This chapter provides general software security guidelines for SPARC M5-32 and SPARC M6-32 servers.

The following sections are in this chapter:

▼ Prevent Unauthorized Access (Oracle Solaris OS)

- **Use Oracle Solaris OS commands to restrict access to the Oracle Solaris software, to harden the OS, to use security features, and to protect applications.**

  Obtain the Oracle Solaris security guidelines document for the OS version you are using at:

  `http://www.oracle.com/goto/Solaris11/docs`

  `http://www.oracle.com/goto/Solaris10/docs`

▼ Prevent Unauthorized Access (Oracle ILOM)

1. **Use the Oracle ILOM commands to restrict user access to the Oracle ILOM software, to change the factory-set password, to limit the use of the root superuser account, and to secure the private network to the service processor.**

   Obtain the *Oracle ILOM Security Guide* at:

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

2. **Use the platform-specific Oracle ILOM commands to secure individual domains by creating user accounts with roles that apply to a specific physical domain.**

When you assign user roles to a physical domain, the capabilities for that domain mirror those of the user roles assigned for the platform, but they are restricted to the commands executed on the given component.

Note - Only user roles of administrator (`a`), console (`c`), and reset (`r`) can be assigned for individual physical domains.

Obtain the *SPARC M5-32 and SPARC M6-32 Servers Administration Guide* at:

`http://www.oracle.com/goto/M6-32/docs`

▼ Prevent Unauthorized Access (Oracle VM Server for SPARC)

- **Use Oracle VM for SPARC commands to restrict access to the Oracle VM for SPARC software.**

  Obtain the *Oracle VM for SPARC Security Guide* at:

  `http://www.oracle.com/goto/VM-SPARC/docs`

Restricting Access (OpenBoot)

These topics explain how to restrict access at the OpenBoot prompt.

- "Implement Password Protection (OpenBoot)" on page 10
- "Check for Failed Logins (OpenBoot)" on page 11
- "Provide a Power-On Banner (OpenBoot)" on page 11

Related Information

- For information about setting OpenBoot 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`

▼ Implement Password Protection (OpenBoot)

- **Set the security-mode parameter to either `full` or `command`.**

When set to `full`, a password is required to perform any action including normal operations, such as booting. When set to `command`, a password is not required for the `boot` or `go` commands, but all other commands require a password. For business continuity reasons, set the security-mode parameter to command, as in the following example.

```
ok password
ok setenv security-mode command
ok password
```

▼ Check for Failed Logins (OpenBoot)

1. **Determine if someone has attempted and failed to access the OpenBoot environment by using the `security-#badlogins` parameter, as in the following example.**

```
ok printenv security-#badlogins
```

If this command returns any value greater than zero, a failed attempt to access the OpenBoot environment was recorded.

2. **Reset the `security-#badlogins` parameter by typing the following command.**

```
ok setenv security-#badlogins 0
```

▼ Provide a Power-On Banner (OpenBoot)

- **Use the following commands to enable a custom warning message.**

```
ok setenv oem-banner banner-message
ok setenv oem-banner? true
```

Oracle System Firmware

The Oracle system firmware uses a controlled update process to prevent unauthorized modifications. Only the superuser or an authenticated user with proper authorization can use the update process.

For information about obtaining the latest updates or patches, refer to the product notes for your server.

Secure WAN Boot

WAN boot supports varying levels of security. You can use a combination of the security features that are supported in WAN boot to meet the needs of your network. A more secure configuration requires additional administration, but also protects your system data to a greater extent.

- For the Oracle Solaris 10 OS, refer to “Secure WAN Boot Installation Configuration” in *Oracle Solaris Installation Guide: Network-Based Installations*.

  `http://www.oracle.com/goto/Solaris10/docs`
- For the Oracle Solaris 11 OS, refer to *Securing the Network in Oracle Solaris 11.1*.

  `http://www.oracle.com/goto/Solaris11/docs`