SPARC T8 Series Servers Security Guide

Part No: E80503-01
September 2017

SPARC T8 Series Servers Security Guide

Part No: E80503-01

Access to Oracle Support

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

Référence: E80503-01

Accès aux services de support Oracle

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 `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` ou le site `http://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).

These sections provide general hardware security guidelines for the SPARC T8-1, T8-2, and T8-4 servers.

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 accidentally 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 radio frequency identification (RFID) readers can 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

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. These sections provide general software security guidelines for the SPARC T8-1, T8-2 and SPARC T8-4 servers.

▼ 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 version you are using at:

  - `http://www.oracle.com/goto/solaris11/docs`
  - `http://www.oracle.com/goto/solaris10/docs`

▼ Prevent Unauthorized Access (Oracle ILOM)

- **Use Oracle ILOM commands to restrict 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`

▼ 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 describe how to restrict access at the OpenBoot prompt.

- "Implement Password Protection" on page 10
- "Enable the Security Mode" on page 11
- "Disable the Security Mode" on page 12
- "Check for Failed Log-Ins" on page 12
- "Provide a Power-On Banner" on page 12

For information about setting OpenBoot security variables, refer to the OpenBoot documentation at:

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

▼ Implement Password Protection

- **If you have not already set a password, perform this step.**

```
{0} ok password
New password (8 characters max):
Retype new password: password
```

The password can be one to eight characters. If you enter more than eight characters, only the first eight characters will be used. All printable characters are accepted. Control characters are not accepted.

Note - Setting the password to zero characters turns off security and treats the `security-mode` parameter as if it were set to `none`. However, it does not change the setting.

▼ Enable the Security Mode

1. **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 `boot`. 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.

   ```
   {0} ok setenv security-mode command
   {0} ok
   ```

2. **Obtain the security mode prompt.**

   After setting the security mode as described above, there are two ways to obtain the security mode prompt.

   Note - When the HOST console starts, HUP is sent to the console. If `security-mode` is set in OpenBoot, then HUP will result in logout action. Thus when the HOST console is restarted user will be required to login to access the OpenBoot OK prompt.

   - **Use the `logout` and `login` words.**

     ```
     {0} ok logout
     Type boot , go (continue), or login (command mode)
     >
     > login
     Firmware Password: password
     Type help for more information
     {0} ok
     ```

     To exit the security mode, use the `logout` and `login` names, as shown in the example.

   - **Use the `reset-all` word.**

     ```
     {0} ok reset-all
     ```

     This word resets the system. When the system comes back up, OpenBoot goes to the security mode prompt. To log back in to the command prompt (or log out of the security mode), use the `logout` and `login` names, and then enter the password, as described above.

Disable the Security Mode

1. **Set the `security-mode` parameter to `none`.**

   ```
   {0} ok setenv security-mode none
   ```

2. **Set the password to zero length by typing Return after both password prompts.**

Check for Failed Log-Ins

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

   ```
   {0} ok printenv security-#badlogins
   ```

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

2. **Reset the parameter by typing this command.**

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

Provide a Power-On Banner

Although it is not a direct preventative or detective control, a banner can be used for these reasons:

- Convey ownership.
- Warn users of the acceptable use of the server.
- Indicate that access or modifications to OpenBoot parameters is restricted to authorized personnel.

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

  ```
  {0} ok setenv oem-banner banner-message
  {0} ok setenv oem-banner? true
  ```

  The banner message can be up to 68 characters. All printable characters are accepted.

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 on how to obtain 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 more administration, but also protects your system data to a greater extent.

- For the Oracle Solaris 10 OS, refer to the information on securing WAN boot installation configuration in the *Oracle Solaris Installation Guide: Network-Based Installations* book.
- For the Oracle Solaris 11 OS, refer to Installing Oracle Solaris 11.3 Systems.