

SPARC and Netra SPARC S7-2 Series Servers Security Guide



Part No: E73203-01
June 2016

Part No: E73203-01

Copyright © 2016, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

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: E73203-01

Copyright © 2016, Oracle et/ou ses affiliés. Tous droits réservés.

Ce logiciel et la documentation qui l'accompagne sont protégés par les lois sur la propriété intellectuelle. Ils sont concédés sous licence et soumis à des restrictions d'utilisation et de divulgation. Sauf stipulation expresse de votre contrat de licence ou de la loi, vous ne pouvez pas copier, reproduire, traduire, diffuser, modifier, accorder de licence, transmettre, distribuer, exposer, exécuter, publier ou afficher le logiciel, même partiellement, sous quelque forme et par quelque procédé que ce soit. Par ailleurs, il est interdit de procéder à toute ingénierie inverse du logiciel, de le désassembler ou de le décompiler, excepté à des fins d'interopérabilité avec des logiciels tiers ou tel que prescrit par la loi.

Les informations fournies dans ce document sont susceptibles de modification sans préavis. Par ailleurs, Oracle Corporation ne garantit pas qu'elles soient exemptes d'erreurs et vous invite, le cas échéant, à lui en faire part par écrit.

Si ce logiciel, ou la documentation qui l'accompagne, est livré sous licence au Gouvernement des Etats-Unis, ou à quiconque qui aurait souscrit la licence de ce logiciel pour le compte du Gouvernement des Etats-Unis, la notice suivante s'applique :

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

Ce logiciel ou matériel a été développé pour un usage général dans le cadre d'applications de gestion des informations. Ce logiciel ou matériel n'est pas conçu ni n'est destiné à être utilisé dans des applications à risque, notamment dans des applications pouvant causer un risque de dommages corporels. Si vous utilisez ce logiciel ou ce matériel dans le cadre d'applications dangereuses, il est de votre responsabilité de prendre toutes les mesures de secours, de sauvegarde, de redondance et autres mesures nécessaires à son utilisation dans des conditions optimales de sécurité. Oracle Corporation et ses affiliés déclinent toute responsabilité quant aux dommages causés par l'utilisation de ce logiciel ou matériel pour des applications dangereuses.

Oracle et Java sont des marques déposées d'Oracle Corporation et/ou de ses affiliés. Tout autre nom mentionné peut correspondre à des marques appartenant à d'autres propriétaires qu'Oracle.

Intel et Intel Xeon sont des marques ou des marques déposées d'Intel Corporation. Toutes les marques SPARC sont utilisées sous licence et sont des marques ou des marques déposées de SPARC International, Inc. AMD, Opteron, le logo AMD et le logo AMD Opteron sont des marques ou des marques déposées d'Advanced Micro Devices. UNIX est une marque déposée de The Open Group.

Ce logiciel ou matériel et la documentation qui l'accompagne peuvent fournir des informations ou des liens donnant accès à des contenus, des produits et des services émanant de tiers. Oracle Corporation et ses affiliés déclinent toute responsabilité ou garantie expresse quant aux contenus, produits ou services émanant de tiers, sauf mention contraire stipulée dans un contrat entre vous et Oracle. En aucun cas, Oracle Corporation et ses affiliés ne sauraient être tenus pour responsables des pertes subies, des coûts occasionnés ou des dommages causés par l'accès à des contenus, produits ou services tiers, ou à leur utilisation, sauf mention contraire stipulée dans un contrat entre vous et Oracle.

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 7**
 - Access Restrictions 7
 - Serial Numbers 8
 - Hard Drives 8
- Understanding Software Security 9**
 - ▼ Prevent Unauthorized Access (Oracle Solaris OS) 9
 - ▼ Prevent Unauthorized Access (Oracle ILOM) 9
 - ▼ Prevent Unauthorized Access (Oracle VM Server for SPARC) 10
 - Restricting Access (OpenBoot) 10
 - ▼ Implement Password Protection 10
 - ▼ Enable the Security Mode 11
 - ▼ Disable the Security Mode 11
 - ▼ Check for Failed Log-Ins 12
 - ▼ Provide a Power-On Banner 12
 - Oracle System Firmware 12
 - Secure WAN Boot 13
 - Verified Boot 13

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 and Netra SPARC S7-2 series servers.

- [“Access Restrictions” on page 7](#)
- [“Serial Numbers” on page 8](#)
- [“Hard Drives” on page 8](#)

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 and Netra SPARC S7-2 series servers.

- “Prevent Unauthorized Access (Oracle Solaris OS)” on page 9
- “Prevent Unauthorized Access (Oracle ILOM)” on page 9
- “Prevent Unauthorized Access (Oracle VM Server for SPARC)” on page 10
- “Restricting Access (OpenBoot)” on page 10
- “Oracle System Firmware” on page 12
- “Secure WAN Boot” on page 13
- “Verified Boot” on page 13

▼ 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 11
- “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.

■ 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 0, 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 *Oracle Solaris Installation Guide: Network-Based Installations*.
- For the Oracle Solaris 11 OS, refer to *Securing the Network in Oracle Solaris 11.3*.

Verified Boot

Verified Boot can be used to verify system boot blocks and Oracle Solaris kernel modules before they are loaded on the system. Use Oracle ILOM to enable Verified Boot and to specify how the system should respond when a verification check fails. Enabling Verified Boot can prevent harmful changes to the system boot blocks or Oracle Solaris kernel modules from taking effect.

Refer to the information about configuring SPARC Verified Boot properties in *Oracle ILOM Administrator's Guide for Configuration and Maintenance*.

