

Sun Rack II Power Distribution Units

Security Guide

Copyright © 2014, 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 software documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, 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 on 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. 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.

Copyright © 2014, 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 disposition de votre contrat de licence ou de la loi, vous ne pouvez pas copier, reproduire, traduire, diffuser, modifier, breveter, 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 concédé sous licence au Gouvernement des Etats-Unis, ou à toute entité qui délivre la licence de ce logiciel ou l'utilise 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 des dommages corporels. Si vous utilisez ce logiciel ou 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 ce type d'applications.

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 d'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. 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.



Adobe PostScript

Contents

Using This Documentation v

Understanding Hardware Security 1

Access Restrictions 1

Serial Numbers 2

Hard Drives 2

Understanding Software Security 3

General Software Security Guidelines 3

▼ Prevent Unauthorized Access (Oracle ILOM) 4

Restricting Access (OpenBoot) 5

▼ Implement Password Protection (OpenBoot) 5

▼ Check for Failed Logins (OpenBoot) 5

Oracle Sun Rack II PDU Firmware 6

Using This Documentation

This document provides security guidelines for the Sun Rack II PDU from Oracle.

This document is written for professional installers, authorized service providers (ASPs), and users who have experience installing and cabling equipment into rack cabinets.

- “Product Notes” on page v
- “Related Documentation” on page vi
- “Feedback” on page vi
- “Access to Oracle Support” on page vi

Product Notes

For late-breaking information and known issues about this product, refer to the product notes at:

<http://www.oracle.com/goto/SUNRACKII/docs>

Related Documentation

Documentation	Links
All Oracle products	http://docs.oracle.com
Sun Rack II	http://www.oracle.com/goto/SUNRACKII/docs
Oracle Integrated Lights Out Manager (ILOM)	http://www.oracle.com/goto/ILOM/docs
Oracle Solaris OS and system software library	http://www.oracle.com/technetwork/indexes/documentation/index.html#sys_sw

Feedback

Provide feedback about this documentation at:

<http://www.oracle.com/goto/docfeedback>

Access to Oracle Support

Oracle customers 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.

Understanding Hardware Security

This chapter provides general hardware security guidelines for Oracle's Sun Rack II PDUs.

Physical isolation and access control are the foundation on which you should build the security architecture. Ensuring that the physical rack is installed in a secure environment protects it and the Sun Rack II PDU 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).

The following sections are in this chapter:

- ["Access Restrictions" on page 1](#)
- ["Serial Numbers" on page 2](#)

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, 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

This chapter provides software security guidelines for Oracle's Sun Rack II PDUs.

The following sections are in this chapter:

- ["General Software Security Guidelines"](#) on page 3
- ["Prevent Unauthorized Access \(Oracle ILOM\)"](#) on page 4
- ["Restricting Access \(OpenBoot\)"](#) on page 5
- ["Oracle Sun Rack II PDU Firmware"](#) on page 6

General Software Security Guidelines

For the Sun Rack II PDU, most hardware security is implemented through software measures.

- 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 auto-trunking on all ports.
- Use a dedicated network for the Sun Rack II PDU interface to separate it from the general network.
- Change all default passwords when installing a new Sun Rack II PDU. Most types of equipment use default passwords that are widely known and would allow unauthorized access to the equipment.

For user accounts:

- If possible, set up RADIUS and TACACS+ access 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.

- Limit the use of the root superuser account. Instead, assign Oracle Integrated Lights Out Manager (Oracle ILOM) accounts whenever possible.
- Use access control lists where appropriate.
- Set time-outs for extended sessions.
- Set privilege levels.
- Create a system banner to remind the user that unauthorized access is prohibited.

▼ Prevent Unauthorized Access (Oracle ILOM)

You can actively secure, manage, and monitor system components through the Oracle Sun Rack II PDU interface management firmware.

1. **Use 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.

Refer to the Oracle Sun Rack II PDU interface documentation to understand more about setting up passwords, managing users, and applying security-related features, including Secure Shell (SSH) and Secure Socket Layer (SSL).

Restricting Access (OpenBoot)

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

- “Implement Password Protection (OpenBoot)” on page 5
- “Check for Failed Logins (OpenBoot)” on page 5

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`. For 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.

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

Oracle Sun Rack II PDU Firmware

Keep your Oracle Sun Rack II PDU firmware updated to receive the latest security enhancements and bug fixes.

The 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 the Sun Rack II at:

<http://www.oracle.com/goto/SUNRACKII/docs>