Oracle® Solaris 10 Security Guidelines

Part No: E37990–11
June 2013

ORACLE

Copyright © 2011, 2013, 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, 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.

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.

130613@25097

Contents

Preface 5

1 Oracle Solaris 10 Security Guidelines 7

Oracle Solaris 10 System Hardening References 7

Additional Security References for Oracle Solaris 10 8

Preface

This guide provides pointers to and descriptions of security guidelines for the Oracle Solaris operating system (Oracle Solaris OS). The system hardening references describe how to harden Oracle Solaris 10 systems and how to use Oracle Solaris security features to protect your data and applications. You can tailor the recommendations in these references to your site security policy.

Additionally, this guide provides pointers to background information about Oracle Solaris security, and white papers that guide you through common implementations.

Audience

The *Oracle Solaris 10 Security Guidelines* is intended for security administrators and other administrators who perform the following tasks:

- Analyze security requirements
- Implement security policy in software
- Install and configure the Oracle Solaris OS
- Maintain system and network security

To use this guide, you must have general knowledge of UNIX administration, a good foundation in software security, and knowledge of your site security policy.

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.

Typographic Conventions

The following table describes the typographic conventions that are used in this book.

TABLE P–1 Typographic Conventions

Typeface	Description	Example
`AaBbCc123`	The names of commands, files, and directories, and onscreen computer output	Edit your `.login` file. Use `ls -a` to list all files. `machine_name% you have mail.`
`AaBbCc123`	What you type, contrasted with onscreen computer output	`machine_name%` **`su`** `Password:`
aabbcc123	Placeholder: replace with a real name or value	The command to remove a file is `rm` *filename*.
AaBbCc123	Book titles, new terms, and terms to be emphasized	Read Chapter 6 in the *User's Guide*. A *cache* is a copy that is stored locally. Do *not* save the file. **Note:** Some emphasized items appear bold online.

Shell Prompts in Command Examples

The following table shows UNIX system prompts and superuser prompts for shells that are included in the Oracle Solaris OS. In command examples, the shell prompt indicates whether the command should be executed by a regular user or a user with privileges.

TABLE P–2 Shell Prompts

Shell	Prompt
Bash shell, Korn shell, and Bourne shell	`$`
Bash shell, Korn shell, and Bourne shell for superuser	`#`
C shell	`machine_name%`
C shell for superuser	`machine_name#`

◆ ◆ ◆ CHAPTER 1

Oracle Solaris 10 Security Guidelines

Oracle Solaris 10 is a robust, premier enterprise operating system that offers proven security features. With a sophisticated network-wide security system that controls the way users access files, protect system databases, and use system resources, Oracle Solaris 10 addresses security needs at every layer. While traditional operating systems can contain inherent security weaknesses, the flexibility of Oracle Solaris 10 enables it to satisfy a variety of security objectives from enterprise servers to desktop clients.

Oracle Solaris 10 System Hardening References

The following two documents describe how to harden Oracle Solaris, how to use its security features to configure your systems to operate securely when you add applications and users to the systems, and how to use particular security features to protect network-based applications. A short description accompanies each document title.

- *CIS Solaris 10 Benchmark v5.0.0 (*`http://benchmarks.cisecurity.org/en-us/?route=downloads.show.single.solaris10.500`*)*, 9 July 2010.

  Another name for this document is *Security Configuration Benchmark for Solaris 10 11/06 through 10/09*. This benchmark is the result of over seven years of work by many contributors, including Sun Microsystems, the Defense Information Systems Agency (DISA), the Center for Internet Security (CIS), the National Institute of Standards and Technology (NIST), the National Security Agency (NSA), and many individual enterprises, academic institutions, and individuals. This benchmark establishes a set of baseline hardening guidance that Sun, CIS, NSA, and DISA agreed to.

- *An Overview of Oracle Solaris 10 Security Controls (*`http://www.oracle.com/technetwork/server-storage/solaris/documentation/o11-076-s10-cis-appendix-487450.pdf`*)*, Glenn Brunette, September 2011

This appendix to the *Security Configuration Benchmark for Solaris 10 11/06 through 10/09* focuses on the security controls in Oracle Solaris 10 that fall outside of the area of system hardening and security configurati on validation. This appendix provides a complete overview of the security features and capabilities of Oracle Solaris 10 and offers specific recommendations, where possible.

Additional Security References for Oracle Solaris 10

The following guides and articles supplement the system hardening guidelines in the preceding section:

- *System Administration Guide: Security Services*

  This security guide is published by Oracle for Oracle Solaris 10 administrators. This guide describes the security features of the Oracle Solaris 10 OS and how to use them when configuring your systems. Unlike *Security Configuration Benchmark for Solaris 10 11/06 through 10/09*, this guide is not designed as a system hardening or best practices document.

- *Solaris 10 Security Essentials*, Sun engineers, 2009. ISBN 978-0137012336

  Solaris engineers and technical writers describe 12 Solaris security technologies with examples in this trade book. Unlike *Security Configuration Benchmark for Solaris 10 11/06 through 10/09*, this guide is not designed as a system hardening or best practices document.

- *Using Oracle® Solaris 10 to Overcome Security Challenges (*`http://www.oracle.com/technetwork/server-storage/solaris/solaris-10-security-167783.pdf`*)*, August 2010.

  This Oracle white paper targets organizations that require comprehensive system security features. IT departments that need an effective and efficient solution to computer security can use the unique and powerful security features of Oracle Solaris 10 to protect the enterprise from potential threats, comply with corporate and regulatory requirements, and stay ahead of security challenges. This white paper provides a high-level description of Oracle Solaris security capabilities. It is not designed as a hardening or best practices document.