Oracle® Solaris 11.2 Security Compliance Guide

Part No: E39067
July 2014

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 or 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.

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.

Contents

Using This Documentation

- **Overview** – Describes how to assess and report the compliance of an Oracle Solaris system to specified security benchmarks.
- **Audience** – Security administrators and auditors who assess security on Oracle Solaris 11 systems.
- **Required knowledge** – Site security requirements.

Product Documentation Library

Late-breaking information and known issues for this product are included in the documentation library at http://www.oracle.com/pls/topic/lookup?ctx=E36784.

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.

Feedback

Provide feedback about this documentation at http://www.oracle.com/goto/docfeedback.

♦ ♦ ♦ CHAPTER 1

Reporting Compliance to Security Standards

This chapter describes how to assess and report the compliance of an Oracle Solaris system to security standards, also called *security benchmarks* and *security policies*. This chapter covers the following topics:

- "About Compliance" on page 7
- "Oracle Solaris Security Benchmarks" on page 8
- "Compliance Measurement" on page 8
- "Assessing Oracle Solaris Compliance" on page 10
- "Compliance Reference" on page 13

About Compliance

Systems that comply with security standards provide more secure computing environments, and in addition are easier to test, maintain, and protect. In this release, Oracle Solaris provides scripts that assess and report the compliance of your Oracle Solaris system to two security benchmarks, Solaris Security Benchmark and Payment Card Industry-Data Security Standard (PCI DSS).

Configuration validation to support system compliance to external and internal security policies is critical. The handling of security compliance and auditing requirements accounts for a large percent of IT security spending, including documentation, reports, and the validation itself. Organizations such as banks, hospitals, and governments have specialized compliance requirements. Auditors who are unfamiliar with an operating system can struggle to match security controls with requirements. Therefore, tools that map security controls to requirements can reduce time and costs by assisting auditors.

The compliance scripts are based on the Security Content Automation Protocol (SCAP) written in Open Vulnerability and Assessment Language (OVAL). The SCAP implementation in Oracle Solaris also supports scripts that conform to the Script Check Engine (SCE). These scripts add security checks that the current OVAL schemas and probes do not provide. Additional scripts can be used to meet other regulatory environment standards, such as the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA), Sarbanes Oxley (SOX), and the Federal Information Security Management Act (FISMA). For links to these standards, see "Compliance Reference" on page 13.

Oracle Solaris Security Benchmarks

Oracle Solaris 11 supplies compliance scripts for two standards, Solaris and PCI DSS.

Solaris Security Policy Benchmark

The Solaris security policy benchmark is a standard based on the “secure by default” (SBD) default installation of Oracle Solaris. The benchmark provides two profiles, Baseline and Recommended. The profiles are described in “Compliance Measurement” on page 8.

The features which comprise SBD are described in “Using the Secure by Default Configuration” in “Securing Systems and Attached Devices in Oracle Solaris 11.2 ” and “Oracle Solaris Configurable Security” in “Oracle Solaris 11 Security Guidelines ”.

This benchmark does not satisfy the requirements of the PCI DSS, the Center for Internet Security (CIS), or the Defense Information Systems Agency-Security Technical Information Guides (DISA-STIG) benchmarks for Oracle Solaris.

PCI DSS Security Policy Benchmark

The PCI DSS security policy benchmark is a proprietary information security standard for organizations that handle cardholder information for major debit and credit cards. The standard is defined by the Payment Card Industry Security Standards Council. The intent is to reduce credit card fraud.

An Oracle Solaris system requires configuration to comply with the PCI DSS standard. The compliance report indicates which tests failed and which tests passed, and provides remediation steps.

Compliance Measurement

To measure security compliance, hereafter called *compliance*, requires a security benchmark or profile, a measurement of compliance to that benchmark, called an *assessment*, and then a report of the findings. The report can also be printed in guide form for training or archiving purposes.

Oracle Solaris provides scripts that measure two security profiles in the Solaris benchmark.

- The Baseline profile of the Solaris benchmark closely matches the default SBD installation of Oracle Solaris.
- The Solaris Recommended profile satisfies organizations with stricter security requirements than the Baseline profile.

These profiles nest. Systems that comply with the Recommended profile comply with the Baseline profile.

The PCI DSS benchmark measures your system's compliance to the PCI DSS standard. Because PCI DSS requirements do not have direct code links, you must examine the report for compliance. For more information, see Meeting PCI DSS Compliance with Oracle Solaris 11.

`compliance` Package

Compliance functionality is available from the `pkg:/security/compliance` package, which is installed with the `solaris-small-server` and `solaris-large-server` package groups.

- For information about package groups, see "Installing the Oracle Solaris OS" in "Oracle Solaris 11 Security Guidelines ".
- For information about packages, see "Oracle Solaris 11.2 Package List ".
- To display a description of the compliance packages, issue the `pkg info compliance` command.

Oracle Solaris Compliance Assessment

The `compliance` command is used to assess and report the compliance of a system to a known benchmark. The Oracle Solaris compliance command maps the requirements of a benchmark to the code, file, or command output that verifies compliance to a specific requirement. For information about this command, see the `compliance`(1M) man page.

For information about the SCAP set of tools that support the `compliance` command, see the `oscap`(8) man page. To display the version of the SCAP set of tools, issue the `oscap -V` command.

Note - The SCAP set of tools cannot localize the reports that the `oscap` command produces, nor can it localize the test descriptions. (Localization involves translating the software into the local language.)

Third-Party Compliance Assessment

The CIS third-party standards organization provides automated compliance checking tools for its benchmark. You can contact CIS to determine the cost of using those tools to assess compliance to the CIS benchmark. CIS tools can be used on a Microsoft Windows system for checking Oracle Solaris compliance.

Assessing Oracle Solaris Compliance

The compliance command automates compliance assessment, not remediation. The command is used to list, generate, and delete assessments and reports. Any user can access compliance reports. To manage assessments and generate reports requires rights. For more information, see the compliance(1M) man page.

The compliance command checks local files only. If your system mounts file systems, you must separately test the compliance of the clients and the servers. For example, if you mount user home directories from central servers, run the compliance command on the user systems and on every server that exports the home directories.

Rights to Run the compliance Command

Oracle Solaris provides two rights profiles to handle compliance assessment and report generation.

- The Compliance Assessor rights profile enables users to perform assessments, place them in the assessment store, generate reports, and delete assessments from the store.
- The Compliance Reporter rights profile enables users to generate new reports from existing assessments.

Compliance subcommands require the following rights:

- compliance assess command – Requires all privileges and the solaris.compliance.assess authorization. The Compliance Assessor rights profile provides these rights.
- compliance delete command – Requires write access to the assessment store and the solaris.compliance.assess authorization. The Compliance Assessor rights profile provides these rights.
- compliance list command – Can be run by anyone who has basic rights. This command provides full visibility to both benchmarks and assessments.
- compliance report command – Can be run by anyone, but the range of functionality varies according the user's rights. Users who are assigned either the Compliance Assessor or Compliance Reporter profile can generate new reports in the assessment store. All users can view existing reports, but users with only basic rights cannot generate reports.

Creating Compliance Assessments and Reports

Compliance assessments are complete. Reports can include every item in the assessment or can include a subset of the information in the assessment. Run assessments regularly, for example, as a cron job, to monitor the compliance of your system.

How to Run Compliance Reports

By default, the `solaris-small-server` and `solaris-large-server` packages include the `compliance` package. The `solaris-desktop` and `solaris-minimal` packages do not include the `compliance` package.

Before You Begin You must be assigned the Software Installation rights profile to add packages to the system. You must be assigned administrative rights for most compliance commands, as described in "Rights to Run the `compliance` Command" on page 10. For more information, see "Using Your Assigned Administrative Rights" in "Securing Users and Processes in Oracle Solaris 11.2 ".

1. **Install the `compliance` package.**

   ```
   # pkg install compliance
   ```

   The following message indicates that the package is installed:

   ```
   No updates necessary for this image.
   ```

   For more information, see the `pkg`(1) man page.

   Note - Install the package in every zone where you plan to run compliance tests.

   ---

2. **Create an assessment.**

   ```
   # compliance list -p
   Benchmarks:
   pci-dss: Solaris_PCI-DSS
   solaris: Baseline, Recommended
   Assessments:
    No assessments available
   # compliance -p profile -a assessment-directory
   ```

   -p Indicates the name of the profile. The profile name is case sensitive.

   -a Indicates the directory name of the assessment. The default name includes a time stamp.

   For example, the following command creates an assessment using the Recommended profile.

   ```
   # compliance -p Recommended -a recommended
   ```

   The command creates a directory in `/var/share/compliance/assessments` named `recommended` that contains the assessment in three files: a log file, an XML file, and an HTML file.

   ```
   # cd /var/share/compliance/assessments/recommended
   # ls
   ```

```
recommended.html
recommended.txt
recommended.xml
```

If you run this command again, the files are not replaced. You must remove the files before reusing an assessment directory.

3. **(Optional) Create a customized report.**

```
# compliance report -s -pass,fail,notselected
/var/share/compliance/assessments/recommended/report.-pass,fail,notselected.html
```

This command creates a report that contains failed and not selected items in HTML format. The report is run against the most recent assessment.

You can run customized reports repeatedly. However, you can run the full reports, that is, the assessment, only once in the original directory.

4. **View the full report.**

You can view the log file in a text editor, view the HTML file in a browser, or view the XML file in an XML viewer.

For example, to view the customized HTML report from the preceding step, type the following browser entry:

```
file:///var/share/compliance/assessments/recommended/report.-pass,fail,notselected.html
```

5. **Fix any failures that your security policy requires to pass.**

   a. **Complete the fix for the entry that failed.**

   b. **If the fix includes rebooting the system, reboot the system before running the assessment again.**

6. **(Optional) Run the `compliance` command as a `cron` job.**

```
# cron -e
```

For daily compliance assessments at 2:30 a.m., `root` adds the following entry:

```
30 2 * * * /usr/bin/compliance assess -b solaris -p Baseline
```

For weekly compliance assessments at 1:15 a.m. Sundays, `root` adds the following entry:

```
15 1 * * 0 /usr/bin/compliance assess -b solaris -p Recommended
```

For monthly assessments on the first of the month at 4:00 a.m., `root` adds the following entry:

```
0 4 1 * * /usr/bin/compliance assess -b pci-dss
```

For assessments on the first Monday of the month at 3:45 a.m., `root` adds the following entry:

```
45 3 1,2,3,4,5,6,7 * 1 /usr/bin/compliance assess
```

7. **(Optional) Create a guide for some or all of the benchmarks that are installed on your system.**

```
# compliance guide -a
```

A guide contains the rationale for each security check and the steps to fix a failed check. Guides can be useful for training and as guidelines for future testing. By default, guides for each security profile are created at installation. If you add or change a benchmark, you might create a new guide.

Compliance Reference

The compliance area of computer security assumes familiarity with many standards, acronyms, and processes. The following lists of terms and references is provided for your convenience.

The following programs implement compliance assessment and reporting:

- Security Content Automation Protocol (SCAP)
- SCAP tools (OpenSCAP)
- Open Vulnerability and Assessment Language (OVAL)
- eXtensible Configuration Checklist Description Format (XCCDF)

The following bodies provide compliance standards or laws:

- Center for Internet Security (CIS)
- Federal Information Security Management Act (FISMA)
- Gramm-Leach-Bliley Act (GLBA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Payment Card Industry-Data Security Standard (PCI DSS)
- Sarbanes Oxley (SOX)