

Using the Oracle Solaris Compliance Tool for SAP Installation

ORACLE WHITE PAPER | OCTOBER 2015





Table of Contents

Introduction	1
Compliance Package	1
Compliance Report Framework	1
Compliance Report Benchmark	1
Oracle Solaris Benchmark	2
PCI-DSS Benchmark	2
Compliance Commands	3
List	3
Guide	3
Assess	4
Report	5
Delete	6
Creating Tailorings from Compliance Benchmarks	6
Compliance Tailor	6
Export a Tailoring	8
Compliance Report with SAP Applications	9
Compliance Report with the New Benchmark for SAP applications	10
About the Author	12
References	12

Introduction

This paper provides instructions and best practices for a new Oracle Solaris 11 feature, the compliance report. 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 simple-to-use Oracle Solaris tool provides users with not only reporting but also simple instructions on how to mitigate any compliance test failure, and also provides compliance report templates. Available since release 11.2, Oracle Solaris provides scripts that assess and report the compliance of Oracle Solaris to two security benchmarks:

- » Oracle Solaris Security Benchmark and
- » Payment Card Industry-Data Security Standard (PCI-DSS).

The new command, `compliance (1M)`, is used to run system assessments against security/compliance benchmarks and to generate HTML reports from those assessments. The reports indicate which system tests failed and which passed, and they provide any corresponding remediation steps. The goal of this document is to introduce the compliance report on Oracle Solaris and to provide information on how to assess and report the compliance of an Oracle Solaris system to security standards. The procedure in this whitepaper was tested on an Oracle Solaris global zone, non-global zone, kernel zone, Oracle SuperCluster, Oracle Solaris Cluster, as well as various SAP Advanced Business Application Programming (ABAP) and Java releases with Oracle Database 11g and 12g. This document concludes with information on an additional new SAP benchmark for SAP applications with special security requirements.

Compliance Package

The compliance functionality is available from the `pkg:/security/compliance` package.

Compliance Report Framework

The compliance scripts are based on the Security Content Automation Protocol (SCAP) and written in Open Vulnerability and Assessment Language (OVAL) and the Extensible Configuration Checklist Description Format (XCCDF). OVAL enables a checkable security policy to be written and then verified against the running systems. The current compliance report repository, located at `/usr/lib/compliance/tests`, has over 200 checks.

Compliance Report Benchmark

Oracle Solaris delivers scripts for the PCI-DSS compliance standard as well as two policies called “Solaris Baseline” and “Solaris Recommended”. The following directories are relevant to the benchmarks and compliance reports:

- » `/usr/lib/compliance`: Directory of test benchmarks, compliance programs, and data
- » `/usr/lib/compliance/benchmarks`: Directory of packaged compliance benchmarks
- » `/var/share/compliance/assessments`: Directory of compliance assessments and reports

Oracle Solaris Benchmark

The Oracle Solaris security policy benchmark is a standard based on the “secure by default” (SBD) installation of Oracle Solaris and provides two profiles, Baseline and Recommended. The Oracle Solaris Baseline profile is meant to test a default plain install of Oracle Solaris. The Oracle Solaris Recommended profile satisfies organizations with stricter security requirements than the Baseline profile. Figure 1 shows an example report for the Oracle Solaris benchmark and Baseline profile.

Compliance and Scoring



Rule Overview

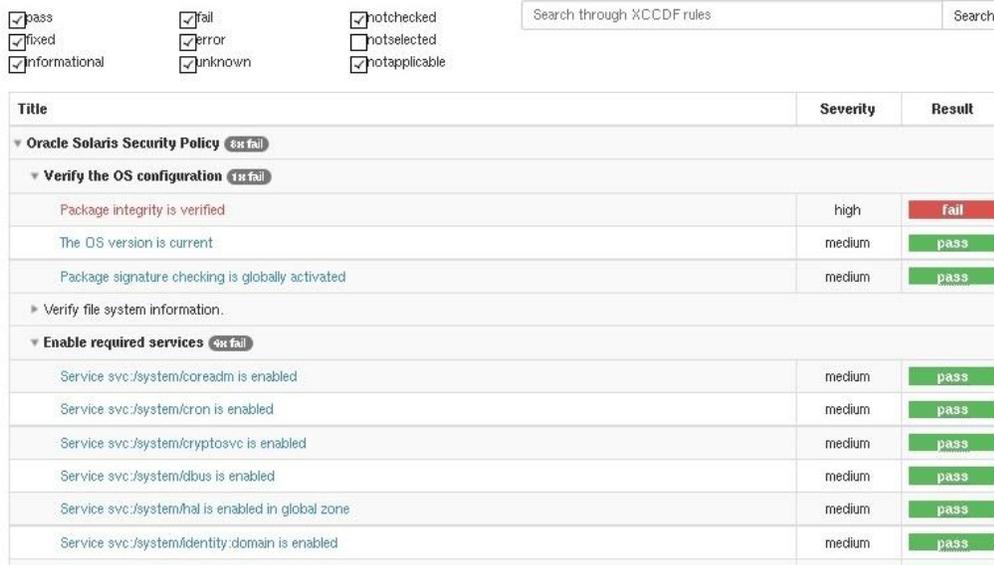


Figure 1. Compliance reporting and checking screen for the Oracle Solaris benchmark and Baseline profile.

PCI-DSS Benchmark

The PCI-DSS benchmark measures the system’s compliance to the PCI-DSS standard. 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 of this standard is to reduce credit card fraud.

Compliance Commands

The `compliance` command is used to list, generate, and delete assessments and reports of the compliance of a system to a known benchmark. 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.

The following sections provide an overview of the `compliance` command. For more detailed information, refer to the `compliance(1M)` man page.

List

The `list` command can be run by anyone who has basic rights. This command provides full visibility to both benchmarks and assessments. The command lists information about the installed named benchmarks and the conducted assessments.

The syntax for the `compliance list` command is:

```
compliance list -b [-v] [-p] [benchmark]
compliance list -a [-v] [assessment]
```

The following example shows the result of using the `compliance list` command to list information about the Oracle Solaris and PCI-DSS benchmarks:

```
root@blade9:~# compliance list -b -v -p solaris
solaris:      Baseline, Recommended
              Oracle Solaris Security Policy
root@blade9:~# compliance list -b -v -p pci-dss
pci-dss:     Solaris_PCI-DSS
              Payment Card Industry Data Security Standard
```

Guide

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.

The syntax for the `compliance guide` command is:

```
compliance guide [-p profile] [-b benchmark] [-o file]
compliance guide -a
```

The following example shows how to run the `compliance guide` command to see all existing guides in the system:

```
root@blade9:~# compliance guide -a
/var/share/compliance/guides/pci-dss.html
/var/share/compliance/guides/pci-dss.Solaris_PCI-DSS.html
/var/share/compliance/guides/solaris.html
/var/share/compliance/guides/solaris.Baseline.html
/var/share/compliance/guides/solaris.Recommended.html
```

Assess

The `assess` command tests the current system configuration against a benchmark and creates a result repository. The user must have all zone privileges and the `solaris.compliance.assess` authorization to conduct assessments; a user assigned the Compliance Assessor rights profile has the rights to conduct assessments.

The syntax for the `compliance assess` command is:

```
compliance assess [-p profile] [-b benchmark] [-a assessment]
Compliance assess -t tailoring [-a assessment]
```

For more details about tailoring (customizing) an assessment, please refer to the section “Creating Tailorings from Compliance Benchmarks” on page 6.

For example, the following command creates an assessment using the Baseline profile. The command creates a directory in `/var/share/compliance/assessments` named `complianceitest` that contains the assessment in three files: a log file, an XML file, and an HTML file. If you run this command again, the files are not replaced. You must remove the files before reusing an assessment directory.

```
root@blade9:~# compliance assess -p Baseline -a compliancetest
Title Package integrity is verified
Rule OSC-54005
Result          fail

Title The OS version is current
Rule OSC-53005
Result          pass
...

root@blade9:/var/share/compliance/assessments/compliancetest# ls
log                report.html        results.xccdf.xml
```

Figure 2 contains an example assessment report showing passes and failures. Specifically, information about the failed rule OSC-73010 and the recommended remediation steps are shown.

Service svc:/system/avahi-bridge-dsd is disabled or not installed medium pass

ssh(1) requires passwords

Rule ID	OSC-73010
Result	fail
Time	2015-09-04T15:55:39
Severity	medium
Identifiers and References	
Description	Logins without a password put the system at risk. In the default remote login service, Secure Shell, the PermitEmptyPasswords parameter in the /etc/ssh/ssh_config file should remain set to no. See the sshd_config(4) man page.

Remediation description:

Ensure that PermitEmptyPasswords value in the /etc/ssh/sshd_config file has not been changed. The default value is no. If you reset the value, restart the ssh service.

Remediation script:

```
# cd /etc/ssh
# grep PermitEmpty sshd_config
...
PermitEmptyPasswords no

# svcadm restart svc:/network/ssh
```

Figure 2. Compliance reporting and checking 'fail' in the report – Rule ID OSC-73010.

In this case, it is necessary to ensure that the `PermitEmptyPasswords` value has not been changed in the `/etc/ssh/sshd_config` file. To fix this issue, you would need to set the `PermitEmptyPasswords` value to `no`. When you set the described variable to the correct value and restart the `ssh` service, this rule will report as 'pass' in the next compliance report.

Report

The `report` command provides the location of a report in the desired format for an assessment, generating the required format report if necessary. The command can be run by anyone, but the range of functionality varies according to 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.

The syntax for the `compliance report` command is:

```
compliance report [-f format] [-s what] [-a assessment] [-o file]
```

The following example creates a report that contains failed, not selected, and passed items in HTML format. The report is run against the most recent assessment.

```
root@blade9:/var/share/compliance/assessments/recommended# compliance report
-s pass, fail, notselected
/var/share/compliance/assessments/recommended/report.fail,notselected,pass.html

root@blade9:/var/share/compliance/assessments/recommended# ls
log report.html
report.fail,notselected,pass.html results.xccdf.xml
```

Delete

The `delete` removes the results repository for the specified assessment, including all associated reports.

The syntax for the compliance delete command is:

```
compliance delete assessment
```

Creating Tailorings from Compliance Benchmarks

The following sections contain information about tailoring security policy.

Compliance Tailor

The compliance framework in Oracle Solaris 11.2 provided no easy way to customize (tailor) the policies to suit individual machine or site deployment needs. The benchmarks that Oracle Solaris provides might report failures or false positives that do not reflect the compliance of particular systems. Since Oracle Solaris 11.3 users can create their own benchmarks from existing Oracle Solaris and PCI-DSS benchmarks according to their requirements using the new `compliance tailor` command.

This command enables the creation of tailorings, which specify inclusions or exclusions of rules. The user can create a tailoring by including or excluding rules from a benchmark, profile, or tailoring, then save the new rule set under a different name. The initial release of tailoring in Oracle Solaris 11.3 allows the enabling and disabling of individual checks. In addition, the user can create multiple tailoring from a source benchmark, and the tailorings are independent of each other. Every tailoring has a unique name.

The `compliance tailor` command provides two editing options: an interactive command-line editor and a curses-based editor called the *pick screen*. The following example sets options on the command line and opens the pick screen:

```
root@blade9:~# compliance tailor -t start
*** compliance tailor: No existing tailoring 'start', initializing
tailoring:start> set benchmark=solaris
tailoring:start> exclude -a
tailoring:start> pick
```

In this example:

- » `start` is the name of the tailoring
- » `solaris` is the source benchmark
- » `exclude -a` loads the `solaris` benchmark rules with none of the rules included
- » `pick` opens the pick screen

The pick screen (see Figure 3) displays all rules in the Oracle Solaris benchmark. On the pick screen, use the keyboard to include particular rules, exclude rules, and navigate.

```
File Edit View Terminal Help
Tailoring: start, on Benchmark: solaris
x OSC-49501 Passwords require at least one uppercase character
x OSC-50003 Passwords cannot be changed for at least three weeks
x OSC-45513 Passwords must be changed at least every 13 weeks
x OSC-50500 NAMECHECK for passwords is set to YES
x OSC-46006 Passwords require at least six characters
x OSC-46008 Passwords require at least eight characters
x OSC-46014 Passwords require at least 14 characters
x OSC-52000 Passwords allow whitespace
x OSC-59000 root is a role
x OSC-56000 Role details are unchanged
x OSC-33000 Logins require passwords
x OSC-51005 shadow(4) password fields are not empty
x OSC-94501 Local users are assigned home directories
x OSC-61001 root is the only user with UID=0
x OSC-24505 All groups specified in /etc/passwd are defined in /etc/group
x OSC-93505 Home directories for all users exist
x OSC-25505 Reserved system accounts remain unused
x OSC-93005 User home directories have appropriate permissions
x OSC-22500 Find and list duplicate GIDs
x OSC-23000 Find and list duplicate group names
x OSC-23500 Find and list duplicate UIDs
x OSC-24000 Find and list duplicate usernames
x OSC-26005 Default system accounts are locked
x OSC-51505 Default system accounts are no-login
x OSC-60000 The root password is hashed with the SHA-256 algorithm
x OSC-27505 Service svc:/network/ipfilter is enabled
x OSC-34510 msg(1) prevents talk(1) and write(1) access to remote terminals
x OSC-25000 Inactive user accounts will be locked after 35 days
Section 6 Check various system configuration items
x OSC-94000 The default user UMASK is 022
x OSC-59510 root access is console-only
x OSC-32500 DISABLETIME is set for logins
x OSC-33500 SLEEPTIME following an invalid login attempt is set to 4
x OSC-36500 Name services are set to all local (files) only
x OSC-01511 Address Space Layout Randomization (ASLR) is enabled
x OSC-04511 Booting the system should require a password
x OSC-75511 Stacks are non-executable
x OSC-69010 Remote serial logins are disabled
Section 7 Verify audit configuration
x OSC-02000 Check all default audit properties
ESC/q-exit, ARROW-UP/DOWN-move, SPACE/x-pick/unpick, F/B-page frwd/back
```

Figure 3. The pick screen displays all rules in the benchmark.

The above example shows the interactive mode where using `x` or `space` allows users to enable or disable an individual test. Note that since the Oracle Solaris 11.2 release, all tests have been renumbered and now have unique rule identifiers that are stable across releases of Oracle Solaris. The same rule number always refers to the same test in all of the security benchmark policy files delivered with Oracle Solaris. When exiting from the interactive pick mode, just type `commit` to write this information to a locally installed tailoring; this will create an `XCCDF` tailoring file under `/var/share/compliance/tailorings`. These tailoring files should not be copied from release to release.

For example, you might exclude the rules `OSC-53005` and `OSC-16005` and include the rule `OSC-17000`. Commit your changes, then exit the command-line interface. At the end you can verify if the tailoring is in stable storage. The following commands illustrate this example scenario:

```

root@blade9:~# compliance tailor -t start
*** compliance tailor: No existing tailoring 'start', initializing
tailoring:start> set benchmark=solaris
tailoring:start> set profile=Baseline
tailoring:start> exclude OSC-53005
tailoring:start> exclude OSC-16005
tailoring:start> include OSC-17000
tailoring:start> commit
tailoring:start> exit
root@blade9:~# compliance tailor list
start

```

Export a Tailoring

There is also an export action for the `tailor` command that allows users to save the customizations for importing into a different system for further testing. The export file contains comments that describe the rules that are included and excluded. The `-o` option specifies the file name. In this example, the administrator uses the `.txt` file extension to indicate that the file is in plain text. When the new tailoring is ready for production, export it in XML format by using the `-x` option. The saved command file can then be used for input redirection to create the same tailoring on another system.

The following commands illustrate creating a tailoring export file:

```

root@blade9:~# compliance tailor
Documented commands (type help <topic>):
=====
clear  delete  exit    include list  pick
commit exclude export  info    load  set
Miscellaneous help topics:
=====
tailoring
tailoring> list
      mysite
      start
      twomore
tailoring> load start
tailoring:start> export -o start.tailor.txt

```

```
tailoring:start> exit
root@blade9:~# compliance tailor -t start export
set tailoring=start
# version=2015-08-21T10:46:35.000+00:00
set benchmark=solaris
set profile=Baseline
# OSC-53005: The OS version is current
exclude OSC-53005
# OSC-16005: All local filesystems are ZFS
exclude OSC-16005
# OSC-17000: Non-root ZFS filesystems are encrypted
include OSC-17000
tailoring:start> export -x -o start.xccdf.xml
```

Compliance Report with SAP Applications

The compliance assessment with the Oracle Solaris benchmark and Baseline profile was tested on an Oracle Solaris system running SAP ABAP and JAVA Application Netweaver 7.40 SP08.

The report showed that Rule ID: OSC-73505 is 'failed' with the result of "ssh (1) is the only service binding a listener to non-loopback addresses" because SAP has some open ports (see Table 1).

TABLE 1. SAP RUNNING PORTS

```
The following ports are open:
*.1128 sapstartsrv
*.50114 sapstartsrv
*.3901 msg_server
*.50113 sapstartsrv
*.3301 gwr
*.8101 msg_server
*.3201 enserv
*.40080 igsmux_mt
*.40000 igsmux_mt
*.64993 jstart
*.50000 icman
*.50004 icman
*.50007 icman
*.50020 jstart
*.53948 jstart
*.40001 igspw_mt
*.40002 igspw_mt
*.1521 tnslnsr
```



Compliance Report with the New Benchmark for SAP applications

Since Oracle Solaris 11.3, users can create their own benchmarks from existing Oracle Solaris benchmarks according to their requirements. Because of the specific requirements for SAP applications, ISV Engineering is currently working on a new compliance report benchmark for SAP applications using the OVAL language, `oscap` editor and shell scripts. Intended to increase security features on the Oracle Solaris operating system running SAP applications, this benchmark includes checks to test the required Oracle Solaris packages with SAP applications.

The compliance report with SAP Benchmark checks if the minimum required packages for SAP applications with Oracle Database 11g or 12c are installed on the system. When the required packages are not installed, the SAP benchmark accordingly reports items as failed in the report. Similar to the Oracle Solaris and PCI-DSS benchmarks, a remediation description and remediation scripts are provided for each check.

Because the gateway is an interface of the application server to external items (to other SAP systems, to external program, and so on), security criteria must be fulfilled.

To ensure the SAP gateway operates, the user has to be especially aware of interaction with external programs. Without relevant security settings, unauthorized programs may be started or servers may be registered. To protect the gateway from unauthorized access, it must maintain the two Access Control List (ACL) files: `secinfo` (restarting external programs) and `reginfo` (registering RFC servers).

The `secinfo` security file is used to prevent unauthorized launching of external programs. File `reginfo` controls the registration of external programs in the gateway. There are four rules in the compliance checking and reporting for SAP applications to check the directory and the correct values for content of these files. If the files don't exist in the system, any server process may register from all hosts. However, if a files exists but it is empty, or if it does not contain valid lines, the test is reported as failed and the user can correct the content and value according the remediation description.

Figure 4 and Figure 5 show screens from the SAP benchmark compliance report.

Oracle Security Policy for SAP Application

sap-xccdf.xml

Evaluation Characteristics

Target machine	s113beta
Benchmark Title	Oracle Security Policy for SAP Application
Benchmark Version	Solaris 11
Benchmark Description	sap-xccdf.xml
Profile ID	SAP-Baseline
Started at	2015-09-02T12:58:22
Finished at	2015-09-02T12:58:33
Performed by	sun

CPE Platforms

Addresses

Compliance and Scoring

The target system did not satisfy the conditions of 3 rules! Please review rule results and consider applying remediation.

Rule results



Severity of failed rules



Score

Scoring system	Score	Maximum	Percent
urn:xccdf:scoring:default	83.750000	100.000000	83.75%

Figure 4. Compliance reporting and checking screen with the SAP Benchmark.

Rule Overview

pass fail notchecked
 fixed error notselected
 informational unknown notapplicable

Search through XCCDF rules

Title	Severity	Result
Oracle Security Policy for SAP Application 3x fail		
Verify the OS configuration 2x fail		
The package pkg://solaris/developer/asm assembler is installed	medium	pass
The package pkg://solaris/developer/buildmake is installed	medium	pass
The package pkg://solaris/x11/diagnostic/x11-info-clients is installed	medium	fail
The package pkg://solaris/x11/library/loextst is installed	medium	pass
The package usr/ucb is installed	low	fail
Verify file system information		
Enable required services		
Service svc:/network/ftp is disabled or not installed	high	pass
Service svc:/network/ssh is enabled	medium	pass
Verify user configuration		
root login by using ssh(1) is disabled	medium	pass
root is a role	medium	pass
Check various System Configuration 1x fail		
Gateway Security Parameter "secinfo" exist in an SCS instance, AS Java	high	pass
The content of "secinfo" security file is correct	high	fail
Gateway Security Parameter "reginfo" exist	high	pass
The content of "reginfo" security file is correct	high	pass

Show all result details

Figure 5. Compliance reporting and checking screen with the SAP Benchmark.

About the Author

This document is based on Motahareh Kardeh's experience using the Oracle Solaris compliance tool for SAP installation. Motahareh Kardeh is a Senior Software Engineer in Oracle's ISV Engineering team for SAP and Security.

References

For more information about the Oracle Solaris compliance report, see the following:

- » Oracle Solaris 11 Engineered for Security, Designed for Compliance
<http://www.oracle.com/us/products/servers-storage/solaris/ds-solaris-11-security-compliance-2311193.pdf>
- » *Oracle Solaris 11.3 Security Compliance Guide*, "Creating Tailorings from Compliance Benchmarks"
http://docs.oracle.com/cd/E53394_01/html/E54817/cpltailor.html#scrolltoc
- » *Oracle Solaris 11.2 Security Compliance Guide*, "About Compliance"
http://docs.oracle.com/cd/E36784_01/html/E39067/cplov-abt.html#scrolltoc
- » Customizing Solaris Compliance Policies, by Darren Moffat
https://blogs.oracle.com/darren/entry/customising_solaris_compliance_policies
- » How to ensure Secure, Compliant Application Deployment with Oracle Solaris 11
<http://www.oracle.com/technetwork/articles/servers-storage-admin/howto-ensure-secure-compliant-apps-2240560.html>
- » Making Security Settings for External Programs
https://help.sap.com/saphelp_nw73/helpdata/en/48/b2096b7895307be10000000a42189b/content.htm
- » Gateway Security Files `secinfo` and `reginfo`
http://help.sap.de/saphelp_nw73ehp1/helpdata/en/e2/16d0427a2440fc8bfc25e786b8e11c/content.htm
- » SAP Note 1529849 - Gateway security setting in an SCS instance, AS Java
- » SAP Note 1408081 - Basic settings for `reg_info` and `sec_info`
- » SAP Note 2214056 - Solaris Compliance tool for SAP installation



Oracle Corporation, World Headquarters

500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries

Phone: +1.650.506.7000
Fax: +1.650.506.7200

CONNECT WITH US

-  blogs.oracle.com/oracle
-  facebook.com/oracle
-  twitter.com/oracle
-  oracle.com/SAP

Integrated Cloud Applications & Platform Services

Copyright © 2015, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

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. 0615

Using the Oracle Solaris Compliance Tool for SAP Installation
[October 2015](#)~~September 2015~~