HOL4645: Assessing, Reporting and Customizing the Security Compliance in Oracle Solaris 11

Hunter Li

Principal Software Engineer, Oracle

Richard Liu

Principle Software Engineer, Oracle

Qianqian Chen

Software Engineer, Oracle


ORACLE

Table of Contents

Introduction

Security Compliance is a new feature introduced in Oracle Solaris 11.2. It provides a framework for assessing and reporting the compliance of an Oracle Solaris system to a given security benchmark. With the release of Oracle Solaris 11.3, this feature has been further enhanced to support benchmark tailoring. It allows system administrators to tweak security policy benchmarks according to their company's security standards. With Security Compliance, system administrators will be able to better understand their Oracle Solaris systems in data centers with respect to the security deviation to the predefined benchmarks over time.

In this lab, you will install the Compliance software in the given Oracle Solaris virtual machine first. Then, you will grant proper system rights to a specific normal user who will be able to handle compliance assessments and reports. You will run an assessment and view the default report with the specific user. Lastly, you will create a tailoring from the Oracle Solaris Baseline Benchmark, and run the customized assessments before and after a quick remediation.

At the end of this lab, you will understand what Oracle Solaris Security Compliance is and how it works to help with the security compliance check.

Prerequisites

This hands-on lab assumes you have some basic knowledge about the following technologies.

- Administration of Oracle Solaris or a similar UNIX or Linux OS

Hardware/Software Requirements

- Oracle VM Virtualbox 5.0.2 or later (host OS: Oracle Enterprise Linux or Windows 7/8)
  - CPU requirement: 2 CPUs
  - Memory requirement: 4 GB
  - Disk space requirement: 30 GB
  - Network: One Host-only network adapter
  - Guest Operating System: Oracle Solaris 11.3 or later

Environment Preparation

Preparing the Virtual Machine

For this hands-on lab, you need to create a virtual machine named HOL4645 in the Oracle VM VirtualBox 5.0.2 or later prior to execute all lab exercises. You can download Oracle VirtualBox software here. Please refer to **Hardware/Software Requirements** for the virtual machine configuration in the Oracle VirtualBox Manager.

The Figure 1 below shows the virtual machine HOL4645 in the Oracle VirtualBox Manager.

Figure 1: The Virtual Machine HOL4645 shown in the VirtualBox Manager

The virtual machine HOL4645 should be pre-installed with Oracle Solaris 11.3 or later version. The Oracle Solaris 11.3 x86 live CD is suggested for the OS installation. You may download the Oracle Solaris 11.3 OS live CD from Oracle website.

To better cope with the lab instructions in all exercises, the following configuration should be applied during Oracle Solaris 11.3 OS installation and post-installation.

- During Oracle Solaris 11.3 OS installation from live CD
  - When prompted for root password, specify *root123*.
  - When prompted for OS user creation, create a user name as *admin*, the password is *admin123*.

Note - Since Oracle Solaris 11 GA, *root* is no longer a user but a role. You can't login into the Oracle Solaris system as *root* from anywhere by default. This is so called "secure by default" installation of Oracle Solaris. To login as *root*, one must login into the system with a normal user first, then *su* to *root*. It adds more protection to the Oracle Solaris system. If required, *root* can be changed back to a normal user using *rolemod* command.

- Post-installation
  - Download Oracle Solaris 11.3 Repository file from Oracle website, then upload all files to the virtual machine in the *root* home directory.
  - Build the Oracle Solaris 11.3 local repository from the downloaded files in the virtual machine as *root* following the steps in the README file on the download web page.
  - Set the IPS publisher to the Oracle Solaris 11.3 local repository you just built in the last step. The command is similar to the following.

 # pkg set-publisher -G '' -g <full_path_to_local_repository> solaris*

- Run *pkg fix* as *root* to fix all potential package integrity problems if there are any.

When all these steps are done, the virtual machine configuration is all set.

Login Into the Virtual Machine - HOL4645

Login into HOL4645 as *admin* using the credential shown in Figure 2.

Figure 2: Login into HOL4645 as admin

Notes for Users

Most of the lab is done from the Oracle Solaris command line in a terminal window on the HOL4645 virtual machine. After you are logged in, please start a terminal window by clicking on the terminal icon on the top GNOME panel as shown below in Figure 3.

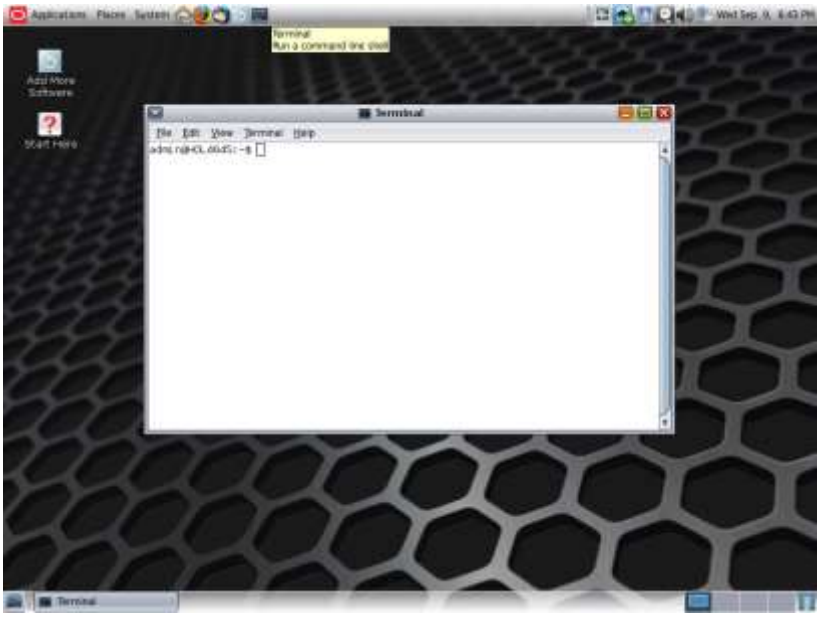

Figure 3: The Top GNOME Panel and An Terminal Window

Exercise 1: Installing Compliance Software and Granting Rights (10 Minutes)

In this exercise, you will check and install Compliance Software on the virtual machine HOL4645, and grant proper rights to the user *admin* so that *admin* can handle compliance assessments and reports.

Check the Available of Security Compliance Software

The virtual machine HOL4645 was initially installed from Oracle Solaris 11.3 live CD. By default, the live CD media does not include the Compliance software, while other Oracle Solaris installation medias do.

You can run the following command to check whether the Compliance package is installed in the system.

```
admin@HOL4645:~$ pkg info -r compliance
          Name: security/compliance
       Summary: Compliance Command and Framework
   Description: The Oracle Solaris compliance framework supports administering a
                set of security compliance policies and for assessing a system
                against compliance benchmarks.  The compliance(1m) command can
                be used to generate an assessment of a system and then create
                reports in a number of different formats.
      Category: System/Administration and Configuration
         State: Not installed
     Publisher: solaris
       Version: 0.5.11
 Build Release: 5.11
        Branch: 0.175.3.0.0.25.0
Packaging Date: June 21, 2015 10:59:25 PM
          Size: 219.03 kB
          FMRI: pkg://solaris/security/compliance@0.5.11,5.11-0.175.3.0.0.25.0:20150621T225925Z
admin@HOL4645:~$
```

If the return State is Not installed, you need to install the Compliance package with *root*. To do that, you need to *su* to *root* and run *pkg install* command. The installation might take up to 5 minutes.

Here's the *root* login credential.

Login: **root** Password: **root123**

```
admin@HOL4645:~$ su - root
Password:
Oracle Corporation      SunOS 5.11      11.3    June 2015
root@HOL4645:~# pkg install compliance
           Packages to install:  8
            Services to change:  2
       Create boot environment: No
Create backup boot environment: No

DOWNLOAD                                  PKGS         FILES    XFER (MB)   SPEED
Completed                                  8/8     1730/1730      9.2/9.2    0B/s

PHASE                                          ITEMS
Installing new actions                     1887/1887
Updating package state database                 Done
Updating package cache                           0/0
Updating image state                            Done
Creating fast lookup database                   Done
Updating package cache                           1/1
root@HOL4645:~# pkg info -r compliance
          Name: security/compliance
       Summary: Compliance Command and Framework
   Description: The Oracle Solaris compliance framework supports administering a
                set of security compliance policies and for assessing a system
                against compliance benchmarks.  The compliance(1m) command can
                be used to generate an assessment of a system and then create
                reports in a number of different formats.
      Category: System/Administration and Configuration
         State: Installed
     Publisher: solaris
       Version: 0.5.11
 Build Release: 5.11
        Branch: 0.175.3.0.0.25.0
```

```
Packaging Date: June 21, 2015 10:59:25 PM
          Size: 219.03 kB
          FMRI: pkg://solaris/security/compliance@0.5.11,5.11-0.175.3.0.0.25.0:20150621T225925Z
root@HOL4645:~#
```

Grant Compliance Rights to the User Admin

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 *admin* user should be granted with the *Compliance Assessor* rights (as a profile) to be able to perform assessments, generate reports and tailor benchmarks.

By default, *admin* does not have the rights of *Compliance Assessor*.

```
root@HOL4645:~# profiles admin | grep -i compliance
Compliance Reporter
root@HOL4645:~#
```

You can run the command below to add the *Compliance Assessor* profile to *admin*.

```
root@HOL4645:~# usermod -P "+Compliance Assessor" admin
UX: usermod: admin is currently logged in, some changes may not take effect until next login.
root@HOL4645:~# profiles admin | grep -i compliance
Compliance Assessor
Compliance Reporter
root@HOL4645:~#
```

The *Compliance Assessor* rights include the *Compliance Report* rights. They take effect immediately even if *admin* has already logged in.

When this step is completed, you can exit from *root*. All subsequent commands will be executed by *admin* until it's instructed again.

```
root@HOL4645:~# exit
logout
admin@HOL4645:~$
```

You may now proceed to *Exercise 2*.

Exercise 2: Performing an Assessment and Viewing the Full Report (30 Minutes)

In this exercise, you will run a security compliance assessment on the virtual machine to the Oracle Solaris Baseline Benchmark. Upon completion of the assessment, you will view the full report in the Firefox web browser to understand the findings.

What Security Benchmarks Are Included in Oracle Solaris 11?

Oracle Solaris supplies two security benchmarks, i.e. Oracle Solaris security policy benchmark and PCI DSS (Payment Card Industry-Data Security Standard) security policy benchmark.

The Oracle Solaris security policy benchmark is a standard based on the "secure by default" (SBD) default installation of Oracle Solaris. It provides two profiles: Baseline and Recommended.

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

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.

How Does Oracle Solaris Compliance Work with Other Standards?

The Oracle Solaris Compliance framework uses scripts for security checks. 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.

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.

Additional scripts can be used to meet other regulatory environment standards. But this is beyond the scope of this hands-on-lab.

List All Available Benchmarks and Profiles

To list all benchmarks installed in Oracle Solaris, you can run *compliance list -b*.

```
admin@HOL4645:~$ compliance list -b

pci-dss solaris

admin@HOL4645:~$
```

To list all profiles in Oracle Solaris, you can run *compliance list -p*.

```
admin@HOL4645:~$ compliance list -p
Benchmarks:
pci-dss:        Solaris_PCI-DSS
solaris:        Baseline, Recommended
Assessments:
        No assessments available
admin@HOL4645:~$
```

The above output shows that there are two benchmarks included in Oracle Solaris 11: *pci-dss* and *solaris*. The benchmark *pci-dss* includes one profile named *Solaris_PCI-DSS*, while the benchmark *solaris* includes two profiles. They are *Baseline* and *Recommended*.

Run an Assessment to the Oracle Solaris Baseline Benchmark

A standard benchmark usually contains a lot of rules, therefore running a standard assessment will take some time. The Oracle Solaris Baseline Benchmark is by default the simplest benchmark. Even though, it might take up to 15 minutes to complete depending on the disk I/O performance.

For this hands-on-lab, you will run an assessment to the Oracle Solaris Baseline Benchmark. You can give a name for the new assessment. The example below names the assessment as *baseline*. If you don't specify a name, the system will automatically name it in the format of *benchmark-name.profile-name.timestamp*.

```
admin@HOL4645:~$ pfexec compliance assess -b solaris -p Baseline -a baseline
Title   Package integrity is verified
Rule    OSC-54005
Result  pass

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

Title   Package signature checking is globally activated
Rule    OSC-53505
Result  pass

        ...
```

```
Title   DISABLETIME is set for logins
Rule    OSC-32500
Result  pass

Title   SLEEPTIME following an invalid login attempt is set to 4
Rule    OSC-33500
Result  pass

Title   Address Space Layout Randomization (ASLR) is enabled
Rule    OSC-01511
Result  pass

Title   Check all default audit properties
Rule    OSC-02000
Result  fail

admin@HOL4645:~$
```

The new assessment *baseline* is now created in */var/share/compliance/assessments*. You can list all assessments in the system by *compliance list -vp* command.

```
admin@HOL4645:~$ pfexec compliance list -vp
Benchmarks:
pci-dss:        Solaris_PCI-DSS
                Payment Card Industry Data Security Standard
solaris:        Baseline, Recommended
                Oracle Solaris Security Policy
Assessments:
baseline:       log report.html results.xccdf.xml
admin@HOL4645:~$
```

The above output shows that there is one assessment named *baseline* in the system.

An assessment is actually created as a sub-directory under */var/share/compliance/assessments*. By default, it includes a result log file in the text form, a browser-ready full report in the HTML form, and a result file in the XML form.

View the Compliance Report

To view the *baseline* assessment report, you need to figure out the full path of the report. You can do it by running the command as shown below.

```
admin@HOL4645:~$ pfexec compliance report -a baseline

/var/share/compliance/assessments/baseline/report.html

admin@HOL4645:~$
```

The report is in the HTML format. You need a web browser to view it. You can start up the Firefox web browser by clicking on the *Firefox* icon on the top GNOME panel as shown below in Figure 4.

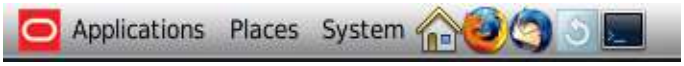

Figure 4: Partial of the Top GNOME Panel

When the web browser is up, you can open the report by entering the full path of the report prefixed by *file:///* in the address bar as shown below in Figure 5, then hit *Enter*.

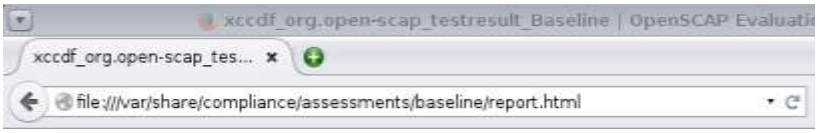

Figure 5: The Example Report Path in Full

Understand the Compliance Report

The Compliance Report consists of three parts: Evaluation Characteristics, Compliance and Scoring, and Rule Overview.

The Evaluation Characteristics briefs when the assessment is done on which system using what benchmark. An example is shown in Figure 6.

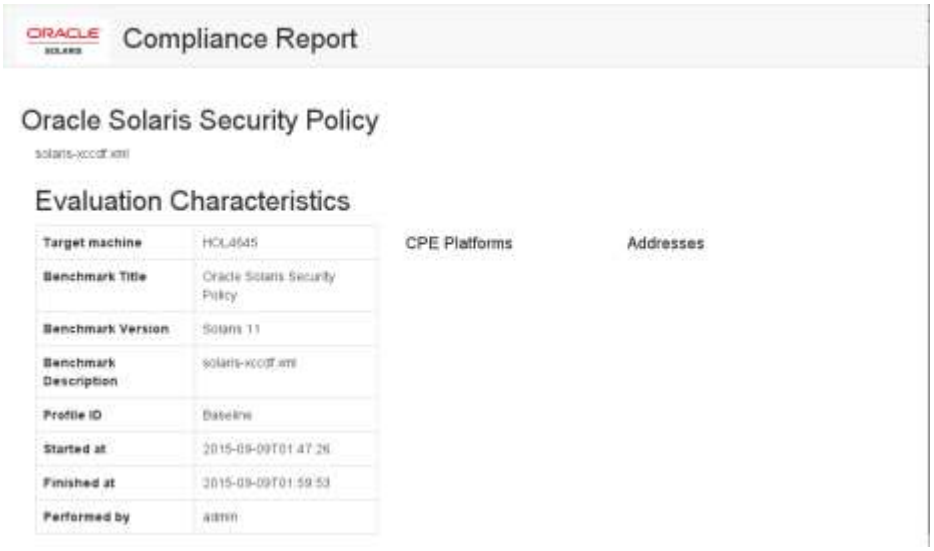

Figure 6: Compliance Report Part 1 - Evaluation Characteristics

The Compliance and Scoring summaries the total numbers of checked rules, the number of problems found by severity and the score. The example shown in Figure 7 reported 7 failed rules out of 138. Among them, there are 6 medium risks and 1 low risk. The score is 84.34 out of 100.

Figure 7: Compliance Report Part 2 - Compliance and Scoring

To learn the results of all rules, you need to review the Rule Overview as illustrated in Figure 8.

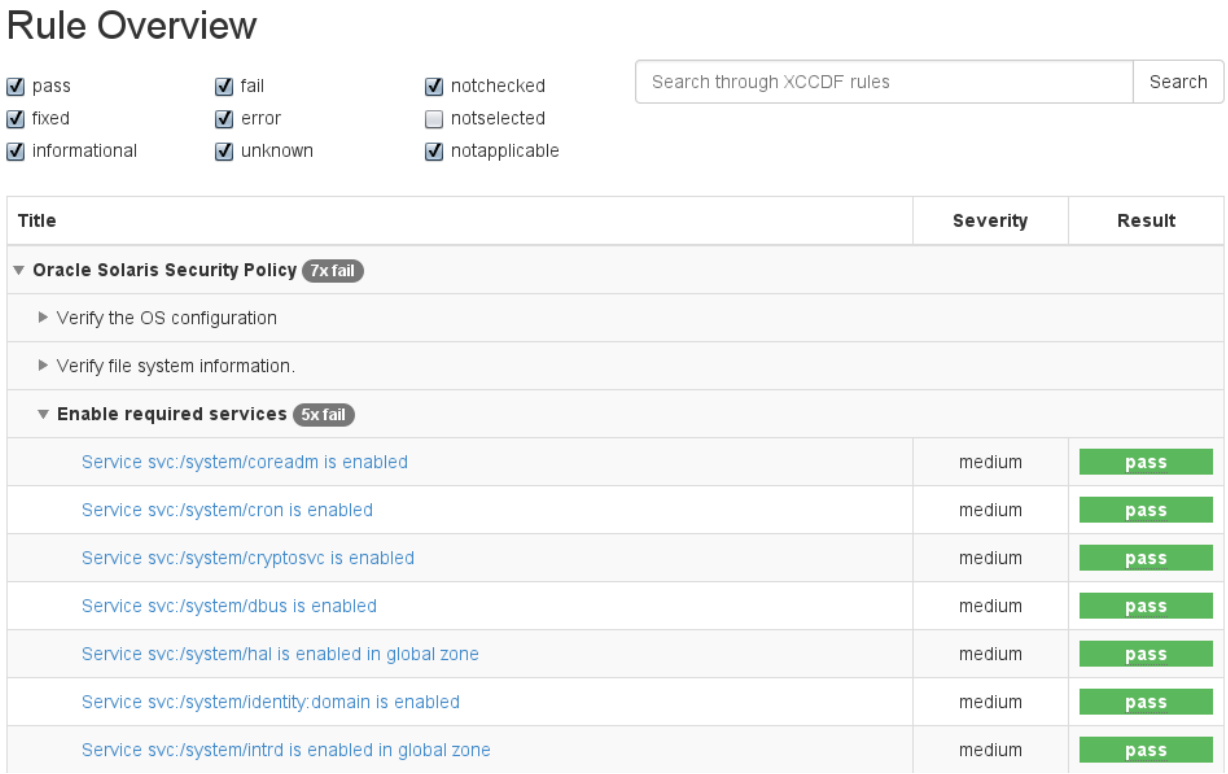

Figure 8: Compliance Report Part 3 - Rule Overview

Rules are listed by category. Failed results are colored in red, while the green color means pass.

You may click on a specific rule to view the details. An example rule detail is shown below in Figure 9.

Figure 9: An Example Rule Details

The rule detail includes a description of the rule, and the remediation method.

For failed rules, you need to analyze the report to understand why they fail. Are they real risks or not for your system? If they are, you may follow the remediation guides in the report, or do the similar if you know how, with a privileged user to mitigate the risks. If they are not real risks, you may choose to exclude the relevant rules by creating a tailored benchmark for your systems. You may also add extra rules to a benchmark if they are necessary for your systems.

In this exercise, if you have followed the steps exactly as instructed, the assessment should report the following failed rules as shown in Table 1.

Failed Rule	Why	Risk?
OSC-12510 Service svc:/network/nfs/fedfs-client is disabled or not installed	The nfs/fedfs-client service is online while the Federatd Filesystem (FedFS) is not in use.	Yes
OSC-38010 Service svc:/network/nfs/mapid is disabled or not installed	The nfs/mapid is online while there's no NFSv4 in use.	No. NFSv4 will be used and preferred
OSC-63005 Service svc:/network/rpc/gss is enabled if and only if Kerberos is configured	The rps/gss is online while the Kerberos is not configured in the system.	Yes
OSC-73505 ssh(1) is the only service binding a listener to non-loopback addresses	The gnome-session that you are currently using opened a port, which fails the rule.	No

OSC-73010 ssh(1) requires passwords	The PermitEmptyPasswords parameter in the /etc/ssh/sshd_config is not set by default. It should be explicitly specified with a value of no.	Yes
OSC-25505 Reserved system accounts remain unused	Reserved account ocm is not in use	No
OSC-02000 Check all default audit properties	No permission for *admin* to run audit	No

Table 1: Result Analysis of the initial Assessment

In this exercise, you are not expected to fix the problems as reported above. You will be doing that in the next exercise.

By now, you have finished *Exercise 2*. You may proceed to *Exercise 3*.

Exercise 3: Tailoring a Benchmark (20 Minutes)

The benchmarks that Oracle Solaris provides might report failures or false positives that do not reflect the compliance of particular systems. For these systems, you can create tailorings, which are inclusions or exclusions of rules from installed benchmarks. You can then use tailorings to assess the security posture of your site.

In this exercise, you will create a tailoring from the Oracle Solaris Baseline Benchmark. You will exclude some rules while include some others. You will run the tailored assessment, then fix problems that are revealed in the compliance report. After a quick remediation, you will rerun the tailored assessment to make sure that all problems are resolved.

Open the Compliance Editor

You can create a tailoring using *compliance tailor* command. It opens an interactive tailor editor.

```
admin@HOL4645:~$ pfexec compliance tailor


Documented commands (type help <topic>):

========================================

clear   delete   exit    include  list  pick

commit  exclude  export  info     load  set


Miscellaneous help topics:

==========================

tailoring


tailoring>
```

You may type *help* to show the above screen.

To know more about a specific subcommand, you may type *help <topic>*. For example, to learn what the *info* subcommand is, type *help info*.

```
tailoring> help info

Syntax: info

 print information about the current tailoring, including all properties.
```

Create a Tailoring from Oracle Solaris Baseline Benchmark

A tailoring is a profile based on an installed benchmark. It may be an extension of an existing profile (named via the profile property) or it may be a new profile (if the profile property is not set).

In the tailor editor, you can use *info* subcommand to show the current properties.

```
tailoring> info
Properties:
        tailoring: not set
        benchmark: not set
        profile: not set
tailoring>
```

Supported properties are:

- Tailoring: The name of the tailoring
- Benchmark: The installed benchmark from which the tailoring is derived
- Profile: The profile of the benchmark from which the tailoring is extended

To create a new tailoring, you need to specify a new name for the tailoring.

```
tailoring> set tailoring=mytailoring
tailoring:mytailoring> info
Properties:
        tailoring=mytailoring
        benchmark: not set
        profile: not set
tailoring:mytailoring>
```

You need to specify a benchmark from which *mytailoring* will be derived. You may use *set benchmark=<installed-benchmark>* subcommand to do so, or use a more user friendly subcommand *pick* for the same purpose. It will present you a screen to pick a benchmark.

```
tailoring:mytailoring> pick
Tailoring: mytailoring


  benchmark=pci-dss           Payment Card Industry Data Security Standard
_   profile=Solaris_PCI-DSS     Solaris PCI-DSS Profile
_   profile: not set


  benchmark=solaris           Oracle Solaris Security Policy
+   profile=Baseline            Solaris Baseline Security Policy
_   profile=Recommended         Solaris Recommended Security Policy
```

```
_   profile: not set


 ESC/q-exit, ARROW-UP/DOWN-move, SPACE/x-pick/unpick, F/B-page frwd/back
```

This screen lists all installed benchmarks and the related profiles. Use *UP* or *DOWN* arrow key to move the cursor to the benchmark or profile entry from which *mytailoring* will be derived. Use *SPACE* or *x* key to select or deselect an entry. Use *ESC* or *q* key to exit from the pick screen.

You should choose the profile *Baseline*. A plus sign (+) will be marked beside the entry *profile=Baseline*. You exit the pick screen by pressing *ESC*.

The *info* subcommand will show you all current properties. You will see all properties are populated as shown below. The new tailoring is named as *mytailoring*. It is based on the *Baseline* profile of the Oracle *Solaris* security policy benchmark.

```
tailoring:mytailoring> info

Properties:

        tailoring=mytailoring

        benchmark=solaris

        profile=Baseline

tailoring:mytailoring>
```

Now, you are ready to tailor the rules upon the Baseline profile of the Oracle Solaris security policy benchmark.

In *Exercise 2*, the assessment to the Oracle Solaris Baseline Benchmark reported seven risks. You were not asked to resolve the risks in *Exercise 2*. Now, you will resolve some of them.

You will exclude four rules which are not considered as risks from the tailored benchmark. In addition, the rule *OSC-54005 Package integrity is verified* will be excluded from the benchmark, as it is too time consuming for this hands-on-lab. In reality, it might be more appropriate for a check on monthly basis.

Below in Table 2 are the rules that you will exclude from the benchmark.

Symbol	Rule	Section	Why
x	OSC-54005 Package integrity is verified	1	Monthly basis preferred
x	OSC-38010 Service svc:/network/nfs/mapid is disabled or not installed	3	NFSv4 expected
x	OSC-73505 ssh(1) is the only service binding a listener to non-loopback addresses	3	Application service expected
x	OSC-25505 Reserved system accounts remain unused	5	The reserved account ocm is fine.
x	OSC-02000 Check all default audit properties	7	It is normal that admin has no permissions to run audit.

Table 2: Rules for Exclusion

You will include the rule below in Table 3 in the benchmark.

Symbol	Rule	Section	Why
>	OSC-35000 /etc/motd and /etc/issue contain appropriate policy text	2	Policy text preferred

Table 3: Rules for Inclusion

There are two ways to include/exclude rules in the tailor editor: Using the pick screen, or using the Command Line Interface.

If you prefer the pick screen, please follow the steps below in *Option 1*. Otherwise, you may try the Command Line Interface by following the steps below in *Option 2*. Either way should lead you to the same result.

Option 1: Using the pick screen to tailor the benchmark

You type *pick* as shown below. The pick screen will show all rules in the Oracle Solaris security policy benchmark regardless whether it's picked or unpicked.

Note - The Baseline profile excludes some rules already. Rules marked with *x* are **EXCLUDED** rules. Rules with a greater-than symbol (>) in reverse video are **INCLUDED** rules.

```
tailoring:mytailoring> pick

Tailoring: mytailoring, on Benchmark: solaris, Profile: Baseline

    Section_1  Verify the OS configuration

> _   OSC-54005  Package integrity is verified

> _   OSC-53005  The OS version is current

> _   OSC-53505  Package signature checking is globally activated

    Section_2  Verify file system information.

> _   OSC-16005  All local filesystems are ZFS

  x   OSC-15000  Find and list files with extended attributes

  x   OSC-14000  Find and list files with no known owner

      ...


  x   OSC-39510  Service svc:/network/nfs/server is disabled or not installed

  x   OSC-12510  Service svc:/network/nfs/fedfs-client is disabled or not installed

 ESC/q-exit, ARROW-UP/DOWN-move, SPACE/x-pick/unpick, F/B-page frwd/back
```

You can navigate rules using *UP*/*DOWN* arrow key. Use *F* to forward a page, and *B* to backward a page. Use *SPACE* or *x* key to pick or unpick an entry. Use *ESC* or *q* key to exit from the pick screen.

Upon the current Baseline profile, please exclude the rules in Table 2, and include the rule(s) in Table 3.

When you are done, please press *ESC* to exit from the pick screen to the tailor editor. Skip *Option 2* below. Proceed to **Verification**.

Option 2: Using the Command Line Interface to tailor the benchmark

In the tailor editor, you can exclude a rule using *exclude <rule-id>*. To include a rule, use *include <rule-id>*.

To exclude all rules in Table 2, run all *exclude* subcommands below.

```
tailoring:mytailoring> exclude OSC-54005
tailoring:mytailoring> exclude OSC-38010
tailoring:mytailoring> exclude OSC-73505
tailoring:mytailoring> exclude OSC-25505
tailoring:mytailoring> exclude OSC-02000
tailoring:mytailoring>
```

To include all rules in Table 3, run the *include* subcommand below.

```
tailoring:mytailoring> include OSC-35000
tailoring:mytailoring>
```

Verification

You can verify all rules excluded from / included to the benchmark using the *export* subcommand as shown below.

```
tailoring:mytailoring> export
set tailoring=mytailoring
# version=2015-09-11T05:35:16.000+00:00
set benchmark=solaris
set profile=Baseline
# OSC-54005: Package integrity is verified
exclude OSC-54005
# OSC-35000: /etc/motd and /etc/issue contain appropriate policy text
include OSC-35000
# OSC-38010: Service svc:/network/nfs/mapid is disabled or not installed
exclude OSC-38010
# OSC-73505: ssh(1) is the only service binding a listener to non-loopback addresses
exclude OSC-73505
# OSC-25505: Reserved system accounts remain unused
```

```
exclude OSC-25505

# OSC-02000: Check all default audit properties

exclude OSC-02000

tailoring:mytailoring>
```

If there's anything wrong, please re-pick the rules as shown in *Option 1*, or undo the wrong inclusions/exclusions using the *exclude*/*include* subcommands, then redo the tailoring as shown in *Option 2*.

If everything is okay, please *commit* the tailoring and *exit* from the tailor editor.

```
tailoring:mytailoring> commit

tailoring:mytailoring> exit

admin@HOL4645:~$
```

Run the Tailored Assessment

You can list all tailorings by *compliance tailor list*.

```
admin@HOL4645:~$ pfexec compliance tailor list

        mytailoring

admin@HOL4645:~$
```

To run a tailored assessment, use *compliance assess* with *-t* option to specify the tailoring. If no assessment name is specified with *-a* option, the system will automatically name it in the format of *tailoring-name.timestamp*.

In the example below, the tailored assessment is named as *mytailoring.2015-09-10,23:16*.

```
admin@HOL4645:~$ pfexec compliance assess -t mytailoring

Assessment will be named 'mytailoring.2015-09-10,23:16'

Title   The OS version is current

Rule    OSC-53005

Result  pass


Title   Package signature checking is globally activated

Rule    OSC-53505

Result  pass


Title   All local filesystems are ZFS

Rule    OSC-16005
```

```
Result  pass

        ...

Title   DISABLETIME is set for logins
Rule    OSC-32500
Result  pass

Title   SLEEPTIME following an invalid login attempt is set to 4
Rule    OSC-33500
Result  pass

Title   Address Space Layout Randomization (ASLR) is enabled
Rule    OSC-01511
Result  pass

admin@HOL4645:~$
```

Since the rule *OSC-54005 Package integrity is verified* has been excluded from the tailored benchmark, the assessment runs a lot faster.

View the Compliance Report of the Tailored Assessment

To view the full report of the tailored assessment, run the commands as shown below.

```
admin@HOL4645:~$ pfexec compliance list -p
Benchmarks:
pci-dss:        Solaris_PCI-DSS
solaris:        Baseline, Recommended
Assessments:
        baseline
        mytailoring.2015-09-10,23:16
admin@HOL4645:~$ pfexec compliance report -a mytailoring.2015-09-10,23:16
/var/share/compliance/assessments/mytailoring.2015-09-10,23:16/report.html
admin@HOL4645:~$
```

In the above example, the full report name with path is */var/share/compliance/assessments/mytailoring.2015-09-10,23:16/report.html*. You will get a similar report name on your terminal.

Enter the full path of your report to the address bar of the FireFox web browser that you have opened in *Exercise 2*, then hit *Enter*.

Figure 10: Enter the Path of the Example Report in the Address Bar

If you have followed all steps exactly as instructed, the tailored assessment should report four failed rules as shown below in Table 4.

Failed Rule	Why	Risk?
OSC-35000 /etc/motd and /etc/issue contain appropriate policy text	We added this rule. We should add policy text in the /etc/motd and /etc/issue.	Yes
OSC-12510 Service svc:/network/nfs/fedfs-client is disabled or not installed	The nfs/fedfs-client service is online while the Federatd Filesystem (FedFS) is not in use.	Yes
OSC-63005 Service svc:/network/rpc/gss is enabled if and only if Kerberos is configured	The rps/gss is online while the Kerberos is not configured in the system.	Yes
OSC-73010 ssh(1) requires passwords	The PermitEmptyPasswords parameter in the /etc/ssh/sshd_config is not set by default. It should be explicitly specified with a value of no.	Yes

Table 4: Result Analysis of the Tailored Assessment

Resolve all Risks

According to the remediation guides in the compliance report, you can resolve all risks with *root*.

Here's the *root* login credential.

Login: **root** Password: **root123**

```
admin@HOL4645:~$ su - root

Password:

Oracle Corporation      SunOS 5.11      11.3    June 2015

root@HOL4645:~#
```

To resolve the risk of *OSC-35000 /etc/motd and /etc/issue contain appropriate policy text*:

```
root@HOL4645:~# echo This is a proprietary server. Unauthorized access is prohibited. >>/etc/motd

root@HOL4645:~# echo This is a proprietary server. Unauthorized access is prohibited. >>/etc/issue

root@HOL4645:~#
```

To resolve the risk of *OSC-12510 Service svc:/network/nfs/fedfs-client is disabled or not installed*:

```
root@HOL4645:~# svcadm disable nfs/fedfs-client

root@HOL4645:~#
```

To resolve the risk of *OSC-63005 Service svc:/network/rpc/gss is enabled if and only if Kerberos is configured*:

```
root@HOL4645:~# svcadm disable rpc/gss
root@HOL4645:~#
```

To resolve the risk of *OSC-73010 ssh(1) requires passwords*:

```
root@HOL4645:~# cp /etc/ssh/sshd_config /etc/ssh/sshd_config.orig
root@HOL4645:~# sed 's/^#PermitEmptyPasswords no$/PermitEmptyPasswords no/g' \
> /etc/ssh/sshd_config > /tmp/sshd_config.tmp
root@HOL4645:~# mv /tmp/sshd_config.tmp /etc/ssh/sshd_config
root@HOL4645:~# svcadm restart ssh
root@HOL4645:~#
```

When all steps above are completed, you can exit from *root*. All subsequent commands will be executed by *admin* until it's instructed again.

```
root@HOL4645:~# exit
logout
admin@HOL4645:~$
```

Rerun the Tailored Assessment after Remediation and Verify the Result

After the remediation, you can rerun *mytailoring*. The assessment is named as *mytailoring-after-fix*.

```
admin@HOL4645:~$ pfexec compliance assess -t mytailoring -a mytailoring-after-fix
Title   The OS version is current
Rule    OSC-53005
Result  pass

Title   Package signature checking is globally activated
Rule    OSC-53505
Result  pass

Title   All local filesystems are ZFS
Rule    OSC-16005
Result  pass
```

```
        ...

Title   DISABLETIME is set for logins
Rule    OSC-32500
Result  pass

Title   SLEEPTIME following an invalid login attempt is set to 4
Rule    OSC-33500
Result  pass

Title   Address Space Layout Randomization (ASLR) is enabled
Rule    OSC-01511
Result  pass

admin@HOL4645:~$
```

When the assessment is done, please find out the report path of *mytailoring-after-fix*.

```
admin@HOL4645:~$ pfexec compliance list -p
Benchmarks:
pci-dss:        Solaris_PCI-DSS
solaris:        Baseline, Recommended
Assessments:
        baseline
        mytailoring-after-fix
        mytailoring.2015-09-10,23:16
admin@HOL4645:~$ pfexec compliance report -a mytailoring-after-fix
/var/share/compliance/assessments/mytailoring-after-fix/report.html
admin@HOL4645:~$
```

To view the final report, please enter *file:///var/share/compliance/assessments/mytailoring-after-fix/report.html* into the address bar of the FireFox web browser.

The final assessment report should contain no failed rules, and the score should be 100, as shown below in Figure 11.

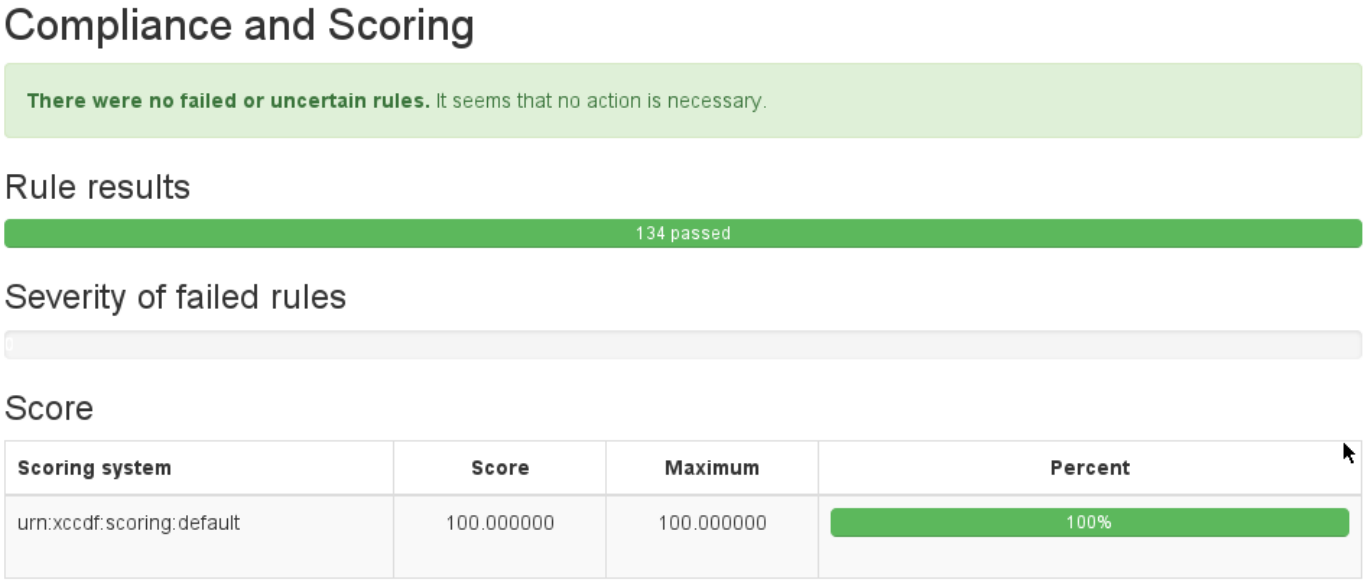

Figure 11: No Failed Rules in the Final Report

If you get the same result as shown in Figure 11, you have just finished *Exercise 3*. It is also the last exercise of this hands-on-lab.

Summary

Congratulations! You have successfully completed the “Assessing, Reporting and Customizing the Security Compliance in Oracle Solaris 11” hands-on lab. You now know what Oracle Solaris Security Compliance is, and how it helps with the system security compliance check. You also learned how to create tailorings from benchmarks for systems with special security policies. For more information about Oracle Solaris Security Compliance, you may refer to resources in the Reference below. Thank you.

Reference

- Oracle Solaris 11.3 Security Compliance Guide

About the Authors

Hunter Li is a Principle Software Engineer working for ISV Engineering at Oracle China. He focuses on supporting the local ISVs in China with application porting, performance tuning and consolidation on Oracle Solaris OS and hardware systems.

Richard Liu is a Principle Software Engineer at ISV Engineering. His main areas of focus are Oracle Solaris Operating System, Oracle Solaris Cluster and Oracle Database. He joined Oracle as part of the Sun acquisition. Prior to ISV Engineering, Richard worked at Sun Advanced Customer Services supporting Solaris and other Sun Products.

Qianqian Chen is a Software Engineer at Oracle for ISV Engineering. She is concentrated on Oracle Solaris and Java. Her duties mainly focus on doing Oracle Solaris evangelizing and supporting local ISVs to run Java applications best on Oracle Solaris and SPARC servers. She earned her master degree in software engineering from Telecom Paristech and bachelor degree from Southeast University in China.

Special thanks to Darren Moffat who works for Oracle Solaris Security Engineering Team and reviewed this manual and provided valuable advice.