Oracle® Linux 8

Using OpenSCAP for Security Compliance
Oracle Legal Notices

Copyright © 2020 Oracle and/or its affiliates.

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, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software" or "commercial computer software documentation" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. 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 Inside 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, Epyc, and the AMD 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 about 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 unless otherwise set forth in an applicable agreement between you and Oracle. 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, except as set forth in an applicable agreement between you and Oracle.

Abstract

Oracle® Linux 8: Using OpenSCAP for Security Compliance describes tasks for using OpenSCAP to scan your Oracle Linux system for security vulnerabilities to make them comply to security standards.

Document generated on: 2020-06-08 (revision: 10129)
# Table of Contents

Preface ................................................................................................................................. v  
1 Deploying OSCAP .............................................................................................................. 1  
   1.1 About SCAP Implementation in Oracle Linux .............................................................. 1  
   1.2 About the oscap Command .......................................................................................... 1  
2 Checking Compliance With OSCAP ................................................................................... 3  
   2.1 Displaying Available SCAP Information ...................................................................... 3  
   2.2 Displaying Information About a SCAP File ................................................................. 4  
   2.3 Displaying Available Profiles ....................................................................................... 4  
   2.4 Validating OVAL and XCCDF Files ............................................................................. 5  
   2.5 Running a Scan Against a Profile ................................................................................ 5  
   2.6 Generating a Full Security Guide .................................................................................. 7  
   2.7 Running an OVAL Auditing Scan ................................................................................ 8
Preface

*Oracle® Linux 8: Using OpenSCAP for Security Compliance* describes how to use OpenSCAP tools to inspect your Oracle Linux systems for security compliance by checking vulnerabilities to prevent the system from risk of security breaches.

**Audience**

This document is intended for administrators who need to configure and administer Oracle Linux systems. It is assumed that readers are familiar with web technologies and have a general understanding of using the Linux operating system, including knowledge of how to use a text editor such as *emacs* or *vim*, essential commands such as *cd*, *chmod*, *chown*, *ls*, *mkdir*, *mv*, *ps*, *pwd*, and *rm*, and using the *man* command to view manual pages.

**Document Organization**

The document is organized into the following chapters:

- **Chapter 1**, *Deploying OSCAP*
- **Chapter 2**, *Checking Compliance With OSCAP*

**Related Documents**

The documentation for this product is available at:

*Oracle® Linux 8 Documentation*

**Conventions**

The following text conventions are used in this document:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>boldface</strong></td>
<td>Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.</td>
</tr>
<tr>
<td><strong>italic</strong></td>
<td>Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.</td>
</tr>
<tr>
<td><strong>monospace</strong></td>
<td>Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.</td>
</tr>
</tbody>
</table>

**Documentation Accessibility**

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at [https://www.oracle.com/corporate/accessibility/](https://www.oracle.com/corporate/accessibility/).

**Access to Oracle Support**

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit [https://www.oracle.com/corporate/accessibility/learning-support.html#support-tab](https://www.oracle.com/corporate/accessibility/learning-support.html#support-tab).
Chapter 1 Deploying OSCAP

Table of Contents

1.1 About SCAP Implementation in Oracle Linux ................................................................. 1
1.2 About the oscap Command ............................................................................................. 1

This chapter describes Security Content Automation Protocol (SCAP) and its implementation in Oracle Linux. It also provides an overview of the oscap command, its useful subcommands, and the modules it supports.

1.1. About SCAP Implementation in Oracle Linux

The Security Content Automation Protocol (SCAP) provides an automated, standardized methodology for managing system security, including measuring and managing system vulnerability, and evaluating policy compliance against security standards such as the Federal Information Security Management Act (FISMA). The U.S. government content repository for SCAP standards is the National Vulnerability Database (NVD), which is managed by the National Institute of Standards and Technology (NIST).

Oracle Linux provides the following SCAP packages for Oracle Linux 8:

- **openscap-utils**: Contains command-line tools that use the OpenSCAP library.
- **openscap-scanner**: Provides the oscap command-line configuration and vulnerability scanner for performing compliance checking against SCAP content, including the SCAP Security Guide.
- **openscap**: Provides the OpenSCAP open-source libraries for generating SCAP-compliance documentation.
- **scap-security-guide**: Provides system-hardening guidance in SCAP format, including links to government requirements. The guide provides security profiles that you can modify to comply with the security policies that you have established for your site.

For information about SCAP package features and other changes in Oracle Linux 8, see the release notes for the various Oracle Linux 8 releases at [https://docs.oracle.com/en/operating-systems/oracle-linux/8/](https://docs.oracle.com/en/operating-systems/oracle-linux/8/).

Use the dnf command to install the SCAP packages from the Oracle Linux 8 AppStream repository, either on the Unbreakable Linux Network (ULN) or the Oracle Linux yum server, for example:

```
$ sudo dnf install openscap openscap-utils scap-security-guide
```

**Note**

The openscap-scanner package is automatically installed as a dependency.

1.2. About the oscap Command

The oscap command uses the following general syntax:

```
$ oscap [options] module operation [operation_options_and_arguments]
```

oscap supports the following module types:
About the oscap Command

**cpe**
Performs operations using a Common Platform Enumeration (CPE) file.

**cve**
Performs operations using a Common Vulnerabilities and Exposures (CVE) file.

**cvss**
Performs operations using a Common Vulnerability Scoring System (CVSS) file.

**ds**
Performs operations using a SCAP Data Stream (DS).

**info**
Determines a file's type and prints information about the file.

**oval**
Performs operations using an Open Vulnerability and Assessment Language (OVAL) file.

**xccdf**
Performs operations using a file in eXtensible Configuration Checklist Description Format (XCCDF).

The **info**, **oval**, and **xccdf** modules are the most generally useful for scanning Oracle Linux systems.

The operations that **oscap** can perform depend on the module type. For Oracle Linux systems, the following operations are the most useful to run and using the **oval** and **xccdf** modules:

**eval**
For an OVAL file, **oscap** probes the system, evaluates each definition in the file, and then prints the results to the standard output.

For a specified profile in an XCCDF file, **oscap** tests the system against each rule in the file and prints the results to the standard output.

**generate**
For an OVAL XML results file, **generate report** converts the specified file to an HTML report.

For an XCCDF file, **generate guide** outputs a full security guide for a specified profile.

**validate**
Validates an OVAL or XCCDF file against an XML schema to check for errors.

For more information, see the **oscap(8)** manual page.
Chapter 2 Checking Compliance With OSCAP

Table of Contents

2.1 Displaying Available SCAP Information ................................................................. 3
2.2 Displaying Information About a SCAP File .............................................................. 4
2.3 Displaying Available Profiles ................................................................................... 4
2.4 Validating OVAL and XCCDF Files ............................................................................ 5
2.5 Running a Scan Against a Profile .............................................................................. 5
2.6 Generating a Full Security Guide ................................................................................ 7
2.7 Running an OVAL Auditing Scan .............................................................................. 8

This chapter contains sections that demonstrate how to use different options with the oscap command to perform various tasks from displaying information to generating reports.

2.1. Displaying Available SCAP Information

Use the oscap -V command to display the following information:

- Supported SCAP specifications
- Any loaded plug-in capabilities
- Locations of schema, CPE, and probe files
- Inbuilt CPE names
- Supported OVAL objects and associated SCAP probes

The following is an extracted sample output of the command:

```
$ oscap -V
OpenSCAP command line tool (oscap) 1.3.1

==== Supported specifications ====
XCCDF Version: 1.2
OVAL Version: 5.11.1
CPE Version: 2.3
CVSS Version: 2.0
CVE Version: 2.0
Asset Identification Version: 1.1
Asset Reporting Format Version: 1.1

==== Capabilities added by auto-loaded plugins ====
No plugins have been auto-loaded...

==== Paths ====
Schema files: /usr/share/openscap/schemas
Default CPE files: /usr/share/openscap/cpe
Probes: /usr/libexec/openscap

==== Inbuilt CPE names ====
...Oracle Linux 5 - cpe:/o:oracle:linux:5
Oracle Linux 6 - cpe:/o:oracle:linux:6
Oracle Linux 7 - cpe:/o:oracle:linux:7
```
2.2. Displaying Information About a SCAP File

To display information about a SCAP file, use the `oscap info` command, for example:

```
$ oscap info com.oracle.elsa-2019.xml
```

Document type: OVAL Definitions
OVAL version: 5.3
Generated: 2019-12-20T00:00:00
Imported: 2020-02-14T17:29:37

The previous output shows that the file `com.oracle.elsa-2019.xml` is an OVAL definitions file.

**Note**

Definition files are downloaded from [https://linux.oracle.com/security/](https://linux.oracle.com/security/). For download instructions, see Section 2.7, "Running an OVAL Auditing Scan".

2.3. Displaying Available Profiles

Use the `oscap info` command to display the profiles that are supported by a checklist file such as the SCAP Security Guide. A profile contains generic security recommendations that apply to all Oracle Linux installations and additional security recommendations that are specific to the intended usage of a system.

```
$ oscap info "/usr/share/xml/scap/ssg/content/ssg-ol8-xccdf.xml"
```

Document type: XCCDF Checklist
Checklist version: 1.1
Imported: 2020-04-30T16:29:09
Status: draft
Generated: 2020-04-30
Resolved: true
Profiles:
- Title: Criminal Justice Information Services (CJIS) Security Policy
  Id: cjis
- Title: Unclassified Information in Non-federal Information Systems and Organizations (NIST 800-171)
  Id: cui
- Title: Health Insurance Portability and Accountability Act (HIPAA)
  Id: hipaa
- Title: [DRAFT] Protection Profile for General Purpose Operating Systems
  Id: ospp
- Title: PCI-DSS v3.2.1 Control Baseline Draft for Oracle Linux 8
  Id: pci-dss
- Title: Standard System Security Profile for Oracle Linux 8
  Id: standard
- Title: [DRAFT] Australian Cyber Security Centre (ACSC) Essential Eight
  Id: e8
- Title: [DRAFT] DISA STIG for Oracle Linux 8
  Id: stig

Referenced check files:
- ssg-ol8-oval.xml
- ssg-ol8-ocil.xml
Validating OVAL and XCCDF Files

system: http://scap.nist.gov/schema/ocil/2
https://linux.oracle.com/security/oval/com.oracle.elsa-all.xml.bz2

Note
The profiles that are listed might not necessarily be appropriate to your system. However, you can use them to create new profiles that test compliance with your site’s security policies.

To obtain information about a specific profile, specify the --profile option.

$ oscap info --profile hipaa "/usr/share/xml/scap/ssg/content/ssg-ol8-xccdf.xml"

Document type: XCCDF Checklist
Profile
Title: Health Insurance Portability and Accountability Act (HIPAA)
Id: hipaa
Description: The HIPAA Security Rule establishes U.S. national standards to protect individuals’ electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information. This profile configures Oracle Linux 8 to the HIPAA Security Rule identified for securing of electronic protected health information.

2.4. Validating OVAL and XCCDF Files

To validate an OVAL or XCCDF file against its schema, use the oscap validate command and examine the exit code, as shown in the following example:

$ oscap oval validate com.oracle.elsa-2019.xml
  && echo "ok" || echo "exit code = $? not ok"
ok
$ oscap xccdf validate /usr/share/xml/scap/ssg/content/ssg-ol8-xccdf.xml
  && echo "ok" || echo "exit code = $? not ok"
ok

2.5. Running a Scan Against a Profile

To scan a system against an XCCDF profile, use the oscap xccdf eval command.

The following example shows a scan operation that is run against the hipaa profile of the ssg-ol8-xccdf.xml checklist by using the ssg-ol8-cpe-dictionary.xml CPE dictionary. The results are displayed in a terminal window, as well as saved in XML and HTML formats in the /tmp and /var/www/html directories, respectively. Any rule in a profile that results in a fail potentially requires the system to be reconfigured.

$ oscap xccdf eval --profile hipaa \
  --results /tmp/`hostname`-ssg-results.xml \
  --report /var/www/html/`hostname`-ssg-results.html \
  --cpe /usr/share/xml/scap/ssg/content/ssg-ol8-cpe-dictionary.xml \
  /usr/share/xml/scap/ssg/content/ssg-ol8-xccdf.xml

Title   Disable Quagga Service
Rule    service_zebra_disabled
Result  pass

Title   Disable KDump Kernel Crash Analyzer (kdump)
Rule    service_kdump_disabled
Result  pass
## Running a Scan Against a Profile

<table>
<thead>
<tr>
<th>Title</th>
<th>Rule</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Kerberos Security on All Exports</td>
<td>use_kerberos_security_all_exports</td>
<td>pass</td>
</tr>
<tr>
<td>Enable cron Service</td>
<td>service_cron_enabled</td>
<td>pass</td>
</tr>
<tr>
<td>Ensure Oracle Linux GPG Key Installed</td>
<td>ensure_oracle_gpgkey_installed</td>
<td>pass</td>
</tr>
<tr>
<td>Ensure gpgcheck Enabled In Main yum Configuration</td>
<td>ensure_gpgcheck_globally_activated</td>
<td>pass</td>
</tr>
<tr>
<td>Enable SSH Warning Banner</td>
<td>sshd_enable_warning_banner</td>
<td>fail</td>
</tr>
<tr>
<td>Do Not Allow SSH Environment Options</td>
<td>sshd_do_not_permit_user_env</td>
<td>fail</td>
</tr>
<tr>
<td>Disable SSH Root Login</td>
<td>sshd_disable_root_login</td>
<td>fail</td>
</tr>
</tbody>
</table>

You can view the HTML report in a browser, as shown in the following figure.
2.6. Generating a Full Security Guide

To create a full security guide for a system based on an XCCDF profile, use the `oscap xccdf generate guide` command, for example:

```
$ oscap xccdf generate guide --profile hipaa
   --cpe /usr/share/xml/scap/ssg/content/ssg-ol8-cpe-dictionary.xml
   /usr/share/xml/scap/ssg/content/ssg-ol8-xccdf.xml > /var/www/html/security_guide.html
```

You can view the security guide in a browser, as shown in the following figure.
2.7. Running an OVAL Auditing Scan

Oracle provides OVAL definitions for all errata on ULN. You can use these definitions to ensure that all applicable errata are installed on an Oracle Linux system. For example, Spacewalk enables you to schedule regular auditing scans.

The following types of definition files are available:

- Individual OVAL definition files for specific security patches

  The `com.oracle.elsa-20205535.xml`, for example, relates to ELSA-2020-5535.

- Consolidated OVAL definitions (bzip2 files)

  Compressed files are available for specific years, such as `com.oracle.elsa-2019.xml.bz2`. Optionally, you can download `com.oracle.elsa-all.xml`, which is the compressed archive of all of the applicable OVAL definition files for all of the available ELSA patches.

To obtain an OVAL definition file for a system audit:

1. Download the file from [https://linux.oracle.com/security](https://linux.oracle.com/security) by using either of the following methods:
Running an OVAL Auditing Scan

- Use your browser to download the selected file.
- Use the `wget` command or a similar command, for example:

  ```bash
  ```

2. If you downloaded a compressed file, extract the OVAL definitions file:

  ```bash
  $ bzip2 -d com.oracle.elsa-2019.xml.bz2
  ```

3. Perform a system audit using the definition file, for example:

  ```bash
  $ oscap oval eval --results /tmp/elsa-results-oval.xml
  
  
  path /com.oracle.elsa-2019.xml
  ...
  
  Definition oval:com.oracle.elsa:def:20193871: true
  Definition oval:com.oracle.elsa:def:20193836: false
  Definition oval:com.oracle.elsa:def:20193834: false
  Definition oval:com.oracle.elsa:def:20193832: true
  Definition oval:com.oracle.elsa:def:20193755: false
  Definition oval:com.oracle.elsa:def:20193736: false
  Definition oval:com.oracle.elsa:def:20193735: false
  Definition oval:com.oracle.elsa:def:20193707: true
  Definition oval:com.oracle.elsa:def:20193706: true
  Definition oval:com.oracle.elsa:def:20193705: false
  Definition oval:com.oracle.elsa:def:20193704: false
  Definition oval:com.oracle.elsa:def:20193703: false
  ...
  
  Evaluation done.
  ```

Caution

The flags for the patches have meanings that are different from what you might expect. For example, the `true` flag means that the patch has not been applied to a system, while the `false` flag means that the patch has been applied.

4. View the HTML report in a browser, as shown in the following figure.

Note

If you omitted the `--report` option in the command to audit the system, you can still create the report later from the results file, for example:

```bash
$ oscap oval generate report /tmp/elsa-results-oval.xml
> /var/www/html/elsa-report-oval.html
```
### Running an OVAL Auditing Scan

#### Figure 2.3 Sample OVAL Report

<table>
<thead>
<tr>
<th>OVAL Security Scanner Information</th>
<th>OVAL Definition Generating Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Schema Version</td>
<td>Product Name</td>
</tr>
<tr>
<td>1.6</td>
<td>RHEL</td>
</tr>
<tr>
<td>1.6</td>
<td>RHEL</td>
</tr>
</tbody>
</table>

#### Systems Information
- **Name**: system loneliness
- **Operating System**: Linux
- **Operating System Version**: 6.4.0-24-generic SMP 2019

#### Interfaces
- **IP Address**: 127.0.0.1
- **MAC Address**: 00:0C:29:00:00:00
- **Interface Name**: eth0
- **IP Address**: 192.168.1.1
- **MAC Address**: 00:0C:29:E0:00:00

#### OVAL System Characteristic Generating Information

<table>
<thead>
<tr>
<th>OVAL Definition Generating Information</th>
<th>OVAL Security Scanner Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Schema Version</td>
<td>Product Name</td>
</tr>
<tr>
<td>1.6</td>
<td>RHEL</td>
</tr>
</tbody>
</table>

#### OVAL Vulnerability Sources

<table>
<thead>
<tr>
<th>ID</th>
<th>Reference ID</th>
<th>Class</th>
<th>Description</th>
</tr>
</thead>
</table>

...