Oracle Linux 8

Using OpenSCAP for Security Compliance

F28156-13
July 2025

Oracle Linux 8 Using OpenSCAP for Security Compliance,

F28156-13

Contents

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.

Documentation License

Conventions

The following text conventions are used in this document:

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

Documentation Accessibility

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

Access to Oracle Support for Accessibility

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.

Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also

mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

1

About SCAP

The Security Content Automation Protocol (SCAP) provides an automated, standardized method for evaluating a system's compliance against security standards. SCAP helps automate the monitoring of a system for vulnerabilities and ensuring that the system is in compliance with security policies, 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).

All SCAP files are released in XML format so that they're straightforward to parse and change for custom requirements.

OpenSCAP (OSCAP) is an open source utility that can use a SCAP Security Guide (SSG) profile as a basis for testing security compliance. You can use the OSCAP utilities with Oracle Linux to automate compliance testing.

OSCAP scans a system against a SCAP Security Guide profile, which is typically available as an Extensible Configuration Checklist Description Format (XCCDF) file or within a SCAP data stream file. An XCCDF file contains a structured collection of security configuration rules that can be applied to meet certain security recommendations or requirements. Each XCCDF file can contain several profiles that apply to different use cases. A profile contains generic security recommendations that apply to all Oracle Linux installations and extra security recommendations that are specific to the intended usage of a particular system. Commonly used XCCDF files that are intended for use with Oracle Linux are included within the SCAP packages and are available for use immediately after install. XCCDF profiles are often used to assess whether a system's security configuration aligns with the Security Technical Implementation Guide (STIG) that's released by the Defense Information Systems Agency (DISA) and to provide remediation steps to implement a particular recommendation.

The Oracle Linux installer also provides options to install the OS to match a specific security profile or policy as defined by the XCCDF profiles available in the `scap-security-guide` package. By applying a policy during installation, you can ensure the system is compliant when it begins operation. See Oracle Linux 8: Installing Oracle Linux for more information.

You can use OSCAP to audit systems against Open Vulnerability and Assessment Language (OVAL) definition files to test whether a system might be vulnerable to publicly known vulnerabilities or configuration issues. Oracle releases OVAL definitions for all errata on the Unbreakable Linux Network (ULN).

SCAP artifacts such as XCCDF profiles can be bundled into a single SCAP data stream file which by convention has the file name suffix `.ds`. OSCAP can process data stream files similarly to XCCDF files. We recommend using data stream files whenever possible as they reduce overhead and can contain references to external resources that can be kept current.

2 SCAP Packages

Describes the SCAP Packages available in the Oracle Linux AppStream repository.

openscap-utils
Contains command line tools that use the OpenSCAP library.

openscap-scanner
Provides the oscap command line configuration and vulnerability scanner, which can perform compliance checking against SCAP content including the SCAP Security Guide. This is automatically installed as a dependency of the openscap-utils package.

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 change to comply with site security policies.

openscap-engine-sce
The openscap-engine-sce package lets OpenSCAP run Script Check Engine (SCE) compliance checks included by content authors, such as those in the scap-security-guide. SCE checks are used when OVAL is insufficient for certain compliance requirements. This package is for checking compliance only and not for remediation.

scap-workbench
A graphical utility for working with OpenSCAP. See: https://www.open-scap.org/tools/scap-workbench/.

For information about SCAP package features and other changes in Oracle Linux 8, see the release notes in the Oracle Linux 8 documentation.

Installing SCAP Packages

Describes how to install the SCAP packages from the Oracle Linux 8 AppStream repository.

1. Verify that the ol8_appstream repository is enabled.

   Enter the following command:

   ```
   dnf repolist | grep appstream
   ```

   If the ol8_appstream repository is enabled, it's listed in the output:

   ```
   ol8_appstreamOracle Linux8 Application Stream Packages (x86_64)
   ```

2. Use dnf to install the required packages.

For example:

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

3 OSCAP Information and Reference

You can obtain information about the installation of OSCAP that can help you understand how the tool is configured and what it provides. This information can be helpful when debugging issues within OSCAP.

The `oscap` command includes several sub commands that control different behaviors and enable the tool to interact with several different file types.

Displaying Information About OSCAP

Use `oscap -V` to display the following information about the OSCAP tool:

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

Sample output:

```
OpenSCAP command line tool (oscap) 1.3.12
Copyright 2009--2023 Red Hat Inc., Durham, North Carolina.

==== Supported specifications ====
SCAP Version: 1.3
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
CVRF 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

==== Inbuilt CPE names ====
...

==== Supported OVAL objects and associated OpenSCAP probes ====
OVAL family   OVAL object              OpenSCAP probe
----------    ----------               ----------
independent   environmentvariable      probe_environmentvariable
```

```
independent   environmentvariable58      probe_environmentvariable58
independent   family                     probe_family
...
```

> **Note**
>
> Inbuilt Common Platform Enumeration (CPE) dictionaries are deprecated and will be removed in a future release. CPE dictionaries are used to provide standard naming schemes for hardware, software, and packages so that they can be easily referenced within code. CPE dictionaries can be included as part of a data stream and the dictionaries used for Oracle Linux platforms are included in the data stream files shipped in the scap-security-guide package.

oscap Command Reference

oscap Command Syntax

The general command syntax of oscap is:

oscap [*options*] *module operation* [*operation_options_and_arguments*]

oscap Command Modules

oscap works with the following modules:

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.

cvrf
Extracts information from Common Vulnerability Reporting Framework (CVRF) files.

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

info
Shows 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).

oscap Command Module Operations

The most useful modules for scanning Oracle Linux systems are info, oval, and xccdf. When using the oval and xccdf modules, the most useful operations are:

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.

You can use the -h command option to view help for each sub command available. For example:

```
oscap -h
oscap xccdf -h
oscap xccdf generate -h
```

For more information, see the oscap(8) manual page.

4

Checking Compliance With XCCDF Profiles

Use the the oscap command to check how the system complies with a security compliance checklist. OSCAP can generate reports and display information about the system by using XCCDF profiles. These can help you harden a system to meet particular security requirements, recommendations, or guidelines. XCCDF profiles can be contained either in an XCCDF file or within a SCAP data stream file.

Validating an XCCDF File or Data Stream File

This task shows how to use oscap sub commands to check that XCCDF and data stream files are correctly formatted.

To check that an XCCDF file is valid, use oscap xccdf validate and examine the exit code. This validates the file against its schema.

To validate an XCCDF file, run the following command:

```
oscap xccdf validate /path/to/xccdf-file.xml \
 && echo "ok" || echo "exit code = $? not ok"
```

If the XCCDF file is valid, the command example returns:

```
ok
```

> **Note**
>
> Various XCCDF files and other SCAP security guide files are included in the scap-security-guide package.

To validate a source data stream file against its schema, use oscap ds sds-validate. XCCDF content can be bundled and included within a single source data stream file, often included as part of the scap-security-guide package and are preferred for shipping many SCAP related artifacts.

To validate a source data stream file, run the following command:

```
oscap ds sds-validate /path/to/ds-file.xml \
 && echo "ok" || echo "exit code = $? not ok"
```

If the source data stream file is valid, the command example returns:

```
ok
```

Displaying Available Profiles

A profile contains generic security recommendations that apply to all Oracle Linux installations and other security recommendations that are specific to the intended usage of a system. You can use these unmodified, or adapt them to create profiles that test the system's compliance with site security policies.

Use `oscap info` to display profiles that work with a checklist file such as the SCAP Security Guide XCCDF file or a SCAP data stream that contains XCCDF content. The syntax is as follows:

```
oscap info path/file.xml
```

For example:

```
oscap info /usr/share/xml/scap/ssg/content/ssg-ol8-ds.xml
```

Sample output:

```
Document type: Source Data Stream
Imported: date and time

Stream: scap_org.open-scap_datastream_from_xccdf_ssg-ol8-xccdf.xml
Generated: (null)
Version: 1.3
Checklists:
   Ref-Id: scap_org.open-scap_cref_ssg-ol8-xccdf.xml
WARNING: Datastream component 'scap_org.open-scap_cref_security-oval-com.oracle.elsa-ol8.xml.bz2' points out to the
     remote 'https://linux.oracle.com/security/oval/com.oracle.elsa-ol8.xml.bz2'. Use '--fetch-remote-resources'
     option to download it.
WARNING: Skipping 'https://linux.oracle.com/security/oval/com.oracle.elsa-ol8.xml.bz2' file which is referenced
     from datastream
      Status: draft
      Generated: date
      Resolved: true
      Profiles:
         Title: ANSSI-BP-028 (enhanced)
            Id: xccdf_org.ssgproject.content_profile_anssi_bp28_enhanced
         Title: ANSSI-BP-028 (high)
            Id: xccdf_org.ssgproject.content_profile_anssi_bp28_high
         Title: ANSSI-BP-028 (intermediary)
            Id: xccdf_org.ssgproject.content_profile_anssi_bp28_intermediary
         Title: ANSSI-BP-028 (minimal)
            Id: xccdf_org.ssgproject.content_profile_anssi_bp28_minimal
         Title: Unclassified Information in Non-federal Information Systems and Organizations (NIST 800-171)
            Id: xccdf_org.ssgproject.content_profile_cui
         Title: DRAFT - Australian Cyber Security Centre (ACSC) Essential Eight
            Id: xccdf_org.ssgproject.content_profile_e8
         Title: Health Insurance Portability and Accountability Act (HIPAA)
            Id: xccdf_org.ssgproject.content_profile_hipaa
         Title: Australian Cyber Security Centre (ACSC) ISM Official
            Id: xccdf_org.ssgproject.content_profile_ism_o
         Title: DRAFT - Protection Profile for General Purpose Operating Systems
```

```
    Id: xccdf_org.ssgproject.content_profile_ospp
  Title: PCI-DSS v4.0 Control Baseline for Oracle Linux 8
    Id: xccdf_org.ssgproject.content_profile_pci-dss
  Title: Standard System Security Profile for Oracle Linux 8
    Id: xccdf_org.ssgproject.content_profile_standard
  Title: DISA STIG for Oracle Linux 8
    Id: xccdf_org.ssgproject.content_profile_stig
  Title: DISA STIG with GUI for Oracle Linux 8
    Id: xccdf_org.ssgproject.content_profile_stig_gui
Referenced check files:
  ssg-ol8-oval.xml
    system: http://oval.mitre.org/XMLSchema/oval-definitions-5
  ssg-ol8-ocil.xml
    system: http://scap.nist.gov/schema/ocil/2
  security-oval-com.oracle.elsa-ol8.xml.bz2
    system: http://oval.mitre.org/XMLSchema/oval-definitions-5
```

Note

You can ignore warnings about remote data stream components when viewing information about XCCDF profiles, but when performing an evaluation you must either use the `--fetch-remote-resources` option for OSCAP to automatically download these resources, or manually download the resources beforehand and use the `--local-files` option to provide the path of these components.

The `ssg-ol8-ds.xml` data stream file contains information about where to download OVAL definitions so that evaluations can audit against the most recent version of these definitions.

Displaying Profile Information

This task shows you how to find out more information about a specific profile.

To view information about a profile, use the `oscap info` command with the `--profile` option. The syntax is as follows:

```
oscap info --profile profile_id path/file.xml
```

For example, to find out information about the Health Insurance Portability and Accountability Act (HIPAA) profile, `xccdf_org.ssgproject.content_profile_hipaa`:

```
oscap info --profile xccdf_org.ssgproject.content_profile_hipaa /usr/share/xml/scap/ssg/content/ssg-ol8-ds.xml
```

Tip

Most examples in this guide use the full profile ID, but you can specify a profile by using its short ID instead. The short ID is whatever appears after `profile_` in the full profile ID. For example, instead of `--profile xccdf_org.ssgproject.content_profile_hipaa`, you can use `--profile hipaa`.

Sample output:

```
Document type: Source Data Stream
Imported: date and time

Stream: scap_org.open-scap_datastream_from_xccdf_ssg-ol8-xccdf.xml
Generated: (null)
Version: 1.3
WARNING: Datastream component 'scap_org.open-scap_cref_security-oval-com.oracle.elsa-ol8.xml.bz2' points out to the remote
    'https://linux.oracle.com/security/oval/com.oracle.elsa-ol8.xml.bz2'. Use '--fetch-remote-resources' option to download it.
WARNING: Skipping 'https://linux.oracle.com/security/oval/com.oracle.elsa-ol8.xml.bz2' file which is referenced from datastream
Profile
   Title: Health Insurance Portability and Accountability Act (HIPAA)
   Id: xccdf_org.ssgproject.content_profile_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. Use of this profile in no way guarantees or makes claims against legal
        compliance against the HIPAA Security Rule(s).
```

Running a Scan Against an XCCDF Profile

This task describes how to use the `oscap xccdf eval` command to scan a system against an XCCDF profile and generate a compliance evaluation report.

1. Decide which profile to use.

   See Displaying Available Profiles.

2. Run a scan using that profile.

   The syntax is as follows:

   ```
   sudo oscap xccdf eval --profile profile-name \
     --fetch-remote-resources \
     --results path/results-name.xml \
     --report path/report-name.html \
         /usr/share/xml/scap/ssg/content/file.xml
   ```

   For example:

   ```
   sudo oscap xccdf eval --profile xccdf_org.ssgproject.content_profile_standard \
     --fetch-remote-resources \
     --results /var/www/html/ssg-results.xml \
   ```

```
  --report /var/www/html/ssg-results.html \
    /usr/share/xml/scap/ssg/content/ssg-ol8-ds.xml
```

The --fetch-remote-resources option lets OSCAP connect to the internet to download remote resources that are required for the XCCDF profile evaluation. Or, you can use the --local-files option for OSCAP to access those resources at the specified path. The ssg-ol8-ds.xml data stream file includes a reference to the remotely hosted OVAL definitions that can verify whether a system is patched appropriately.
If you use an XCCDF file instead of the recommended data stream, you must also specify the location of the CPE dictionaries by using the --cpe option, for example:

```
sudo oscap xccdf eval  --profile standard \
  --fetch-remote-resources \
  --results /var/www/html/ssg-results.xml \
  --report /var/www/html/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
```

Sample output:

```
--- Starting Evaluation ---

Title   Verify File Hashes with RPM
Rule    xccdf_org.ssgproject.content_rule_rpm_verify_hashes
Result  pass

Title   Verify and Correct File Permissions with RPM
Rule    xccdf_org.ssgproject.content_rule_rpm_verify_permissions
Result  pass

...

Title   Disable At Service (atd)
Rule    xccdf_org.ssgproject.content_rule_service_atd_disabled
Result  fail

...
```

> **Note**
>
> Any rule in a profile that results in a fail might require system reconfiguration.

3. View the HTML report in a browser.

   Sample report:

OpenSCAP Evaluation Report

Guide to the Secure Configuration of Oracle Linux 8

with profile Standard System Security Profile for Oracle Linux 8

— This profile contains rules to ensure standard security baseline of Oracle Linux 8 system. Regardless of your system's workload all of these checks should pass.

The SCAP Security Guide Project
https://www.open-scap.org/security-policies/scap-security-guide
This guide presents a catalog of security-relevant configuration settings for Oracle Linux 8. It is a rendering of content structured in the eXtensible Configuration Checklist Description Format (XCCDF) in order to support security automation. The SCAP content is is available in the `scap-security-guide` package which is developed at https://www.open-scap.org/security-policies/scap-security-guide.

Providing system administrators with such guidance informs them how to securely configure systems under their control in a variety of network roles. Policy makers and baseline creators can use this catalog of settings, with its associated references to higher-level security control catalogs, in order to assist them in security baseline creation. This guide is a *catalog, not a checklist*, and satisfaction of every item is not likely to be possible or sensible in many operational scenarios. However, the XCCDF format enables granular selection and adjustment of settings, and their association with OVAL and OCIL content provides an automated checking capability. Transformations of this document, and its associated automated checking content, are capable of providing baselines that meet a diverse set of policy objectives. Some example XCCDF *Profiles*, which are selections of items that form checklists and can be used as baselines, are available with this guide. They can be processed, in an automated fashion, with tools that support the Security Content Automation Protocol (SCAP). The DISA STIG, which provides required settings for US Department of Defense systems, is one example of a baseline created from this guidance.

Do not attempt to implement any of the settings in this guide without first testing them in a non-operational environment. The creators of this guidance assume no responsibility whatsoever for its use by other parties, and makes no guarantees, expressed or implied, about its quality, reliability, or any other characteristic.

Evaluation Characteristics

Evaluation target	[redacted]
Benchmark URL	#scap_org.open-scap_comp_ssg-ol8-xccdf-1.2.xml
Benchmark ID	xccdf_org.ssgproject.content_benchmark_OL-8
Benchmark version	0.1.60
Profile ID	xccdf_org.ssgproject.content_profile_standard
Started at	2022-08-17T12:12:15+00:00
Finished at	2022-08-17T12:17:33+00:00
Performed by	oracle
Test system	cpe:/a:redhat:openscap:1.3.6

CPE Platforms

- cpe:/o:oracle:linux:8

Addresses

- IPv4 127.0.0.1
- IPv4 [redacted]
- IPv6 [redacted]
- IPv6 [redacted]
- MAC [redacted]
- MAC [redacted]

Compliance and Scoring

The target system did not satisfy the conditions of 50 rules! Please review rule results and consider applying remediation.

Rule results

27 passed | 50 failed

4. Review the resulting XML file.

   You can use the results XML file to obtain remediation scripts and other information if required. To review the results file, run:

   ```
   oscap info /var/www/html/ssg-results.xml
   ```

   The following sample output shows the Test Results section of the results file. This section includes the source profile that the results apply to. You can use this value when obtaining remediation scripts for later use. See Remediating a System For Compliance With a Security Profile for more information about remediation.

   ```
   ...
   Test Results:
     Result ID: xccdf_org.open-scap_testresult_xccdf_org.ssgproject.content_profile_standard
     Source benchmark: /usr/share/xml/scap/ssg/content/ssg-ol8-ds.xml
     Source profile: xccdf_org.ssgproject.content_profile_standard
     Evaluation started: date and time
     Evaluation finished: date and time
     Platform CPEs:
       #system_with_kernel
       #package_yum
       #not_aarch64_arch
       #not_bootc_and_not_container
       cpe:/o:oracle:linux:8
       #not_bootc
       #not_aarch64_arch_and_not_s390x_arch
       #package_audit
   ```

Generating a Full Security Guide

This task shows how to use the `oscap xccdf generate guide` command to create a full security guide. The security guide provides a catalog of security configuration settings for the system and often includes example bash remediation scripts and Ansible snippets that can be run to automatically resolve issues.

> ⚠ **Caution**
>
> Always test remediation scripts before applying them to production systems.

1. Create a full security guide for a system based on an XCCDF profile.

   Use the `oscap xccdf generate guide` command. The syntax is as follows:

   ```
   sudo oscap xccdf generate guide --profile profile-name \
   /usr/share/xml/scap/ssg/content/file.xml > path/security-guide-name.html
   ```

For example:

```
sudo oscap xccdf generate guide --profile xccdf_org.ssgproject.content_profile_standard \
/usr/share/xml/scap/ssg/content/ssg-ol8-ds.xml > /var/www/html/security_guide.html
```

2. View the security guide in a browser.

   Open the generated security guide in a web browser. The following is a sample guide:

OpenSCAP Security Guide

Guide to the Secure Configuration of Oracle Linux 8

with profile Standard System Security Profile for Oracle Linux 8

— This profile contains rules to ensure standard security baseline of Oracle Linux 8 system. Regardless of your system's workload all of these checks should pass.

The SCAP Security Guide Project
https://www.open-scap.org/security-policies/scap-security-guide
This guide presents a catalog of security-relevant configuration settings for Oracle Linux 8. It is a rendering of content structured in the eXtensible Configuration Checklist Description Format (XCCDF) in order to support security automation. The SCAP content is is available in the `scap-security-guide` package which is developed at https://www.open-scap.org/security-policies/scap-security-guide.

Providing system administrators with such guidance informs them how to securely configure systems under their control in a variety of network roles. Policy makers and baseline creators can use this catalog of settings, with its associated references to higher-level security control catalogs, in order to assist them in security baseline creation. This guide is a *catalog, not a checklist*, and satisfaction of every item is not likely to be possible or sensible in many operational scenarios. However, the XCCDF format enables granular selection and adjustment of settings, and their association with OVAL and OCIL content provides an automated checking capability. Transformations of this document, and its associated automated checking content, are capable of providing baselines that meet a diverse set of policy objectives. Some example XCCDF *Profiles*, which are selections of items that form checklists and can be used as baselines, are available with this guide. They can be processed, in an automated fashion, with tools that support the Security Content Automation Protocol (SCAP). The DISA STIG, which provides required settings for US Department of Defense systems, is one example of a baseline created from this guidance.

Do not attempt to implement any of the settings in this guide without first testing them in a non-operational environment. The creators of this guidance assume no responsibility whatsoever for its use by other parties, and makes no guarantees, expressed or implied, about its quality, reliability, or any other characteristic.

Profile Information

Profile Title	Standard System Security Profile for Oracle Linux 8
Profile ID	xccdf_org.ssgproject.content_profile_standard

CPE Platforms

- cpe:/o:oracle:linux:8

Revision History

Current version: **0.1.60**

- **draft** (as of 2022-07-05)

Table of Contents

Checklist

Group Guide to the Secure Configuration of Oracle Linux 8 Group contains 29 groups and 78 rules

Group System Settings Group contains 25 groups and 72 rules

[ref] Contains rules that check correct system settings.

Group Installing and Maintaining Software Group contains 6 groups and 13 rules

[ref] The following sections contain information on security-relevant choices during the initial operating system installation process and the setup of software updates.

Customizing a Profile

You can customize an OpenSCAP security profile to tailor security rules and variable values for an organization's requirements. To customize an OpenSCAP security profile, you use the autotailor tool, which is provided by the scap-security-guide package.

The autotailor command syntax is as follows:

autotailor *[options]* -o *tailoring_file* -p *profile_id datastream profile*

[options]
Use --var-value *VARIABLE=VALUE* to set variable values, --select *RULE_ID* or --unselect *RULE_ID* to select and clear rules, or other available autotailor options.

-o tailoring_file
Output file to write the tailoring data.

-p profile_id
Identifier for the custom profile.

datastream
Path to the source datastream file. autotailor requires a SCAP datastream as input and doesn't work with individual XCCDF files.

PROFILE
The profile to base the customization on.

1. Generate a tailoring file for the custom profile.

   Use the autotailor tool to create a profile, select, or clear rules, and set variable values. For example, the following command creates a new profile named tailored_profile, selects a specific rule, and sets two variables. The output is saved as tailoring.xml:

   ```
   autotailor --select gconf_gnome_screensaver_idle_delay \
     --var-value var_screensaver_lock_delay=120 \
     --var-value inactivity_timeout_value=600 \
     -o tailoring.xml \
     -p tailored_profile \
     /usr/share/xml/scap/ssg/content/ssg-ol8-ds.xml \
     anssi_bp28_minimal
   ```

   The contents of the tailoring.xml file are as follows:

   ```
   <?xml version="1.0" ?>
   <ns0:Tailoring xmlns:ns0="http://checklists.nist.gov/xccdf/1.2" id="xccdf_auto_tailoring_default">
     <ns0:benchmark href="file:///usr/share/xml/scap/ssg/content/ssg-ol10-ds.xml"/>
     <ns0:version time="date and time">1</ns0:version>
     <ns0:Profile id="xccdf_org.ssgproject.content_profile_tailored_profile"
   extends="xccdf_org.ssgproject.content_profile_anssi_bp28_minimal">
       <ns0:title override="false"/>
       <ns0:select idref="xccdf_org.ssgproject.content_rule_gconf_gnome_screensaver_idle_delay"
   selected="true"/>
       <ns0:set-value idref="xccdf_org.ssgproject.content_value_inactivity_timeout_value">600</ns0:set-value>
   ```

```
        <ns0:set-value idref="xccdf_org.ssgproject.content_value_var_screensaver_lock_delay">120</ns0:set-
value>
    </ns0:Profile>
</ns0:Tailoring>
```

2. Use the tailored profile for scanning.

   When scanning, specify both the customized profile and the tailoring file. For example:

   ```
   oscap xccdf eval \
   --profile tailored_profile \
   --tailoring-file tailoring.xml \
   /usr/share/xml/scap/ssg/content/ssg-ol8-ds.xml
   ```

   This command evaluates compliance using the customized profile.

For more information on the autotailor tool, see the autotailor(8) manual page.

5

Remediating a System For Compliance With a Security Profile

In addition to identifying security and compliance issues through automated scanning, OSCAP can help by generating remediation steps to resolve those issues. The remediation steps might include configuration changes, package installations, or changes to system settings so that the system conforms to selected security baselines.

- Security guides and evaluation reports generated from XCCDF profiles often include remediation information, such as bash scripts or Ansible playbooks, that you can run to apply recommended changes.
- OSCAP can automatically apply remediation steps during a scan when the system fails to comply with the specified XCCDF profile, or these remediation steps can be generated during the scan and applied later.
- You can also generate remediation content for every rule in a profile without scanning the system first. These remediation steps can be produced in several formats, including Bash, Ansible, Puppet, Kickstart files, and resources suitable for integration into automation workflows such as Image Builder blueprints.

> **Warning**
>
> Remediation steps are designed to be run on a base install of the OS and can be applied by selecting a compliance profile using the "Security Profile" option in the Oracle Linux installer. If you changed the system configuration after installing the OS, a remediation step doesn't guarantee compliance with the XCCDF profile.
>
> Remediation steps can restrict accesses or change how a system functions. After the remediation has been applied, it can't be automatically reverted. Don't apply remediation steps to production systems without testing them first.

Applying Remediation Steps During a Scan

This task shows you how to instruct OSCAP to apply remediation steps during the scan of an XCCDF profile. We recommended performing this process after installation of the OS, where a security profile wasn't selected at the time that the system was installed.

To have OSCAP automatically apply remediation steps while an XCCDF profile scan is in progress, include the `--remediate` option.

For example:

```
sudo oscap xccdf eval --profile standard \
        --remediate /usr/share/xml/scap/ssg/content/ssg-ol8-ds.xml
```

Changes are applied automatically as the system is evaluated.

After the command has finished running, reboot the system. You can scan the system again to validate the changes.

Generating Remediation Steps During a Scan for Later Application

You can have the scan generate remediation scripts without applying them, so that you can review the remediation actions and, if required, change them before implementing them.

To generate a remediation script that provides fixes specific to a system, first perform a scan against an XCCDF profile and output an XML file by using the `--results` option. See Running a Scan Against an XCCDF Profile.

Using the XML results file, run the `oscap xccdf generate fix` command to generate a bash script that you can use, for example:

```
oscap xccdf generate fix --profile profile id --fix-type bash --output remediations.sh ssg-results.xml
```

You can change the value of the `--fix-type` option to `ansible` to generate an Ansible remediation script in YAML format. Other options include `puppet`, `anaconda`, `ignition`, and `kubernetes`. The default is `bash`.

Using OSCAP Remediation to Automate Compliance

You can use the OpenSCAP tool (`oscap`) to automatically assess a system's compliance with a selected security profile and apply remediation steps for many of its rules using available formats such as Bash, Ansible, Kickstart, or Image Builder blueprints for automated installation and configuration. Not all compliance rules have automated remediations or are available in all formats, so OpenSCAP remediation provides a strong baseline. Some extra manual configuration might be needed to achieve full compliance with the profile.

To generate a script that includes all remediation actions for a profile, run the `oscap xccdf generate` command against the data stream or XCCDF file, for example:

```
oscap xccdf generate fix --profile profile id --fix-type bash \
        --output all-remediations.sh /usr/share/xml/scap/ssg/content/ssg-ol8-ds.xml
```

Valid options for `--fix-type` are `bash`, `ansible`, `puppet`, `anaconda`, `ignition`, `kubernetes`, `kickstart`, `blueprint`, and `bootc`.

For example, to generate an Image Builder blueprint for an Oracle Cloud Infrastructure image that complies with a specific XCCDF profile, run the following command:

```
oscap xccdf generate fix --profile profile id --fix-type blueprint \
        --output blueprint.toml /usr/share/xml/scap/ssg/content/ssg-ol8-ds.xml
```

6

Auditing for Vulnerabilities By Using OVAL Definitions

You can use OVAL definition files to audit a system for known vulnerabilities and configuration issues. By performing an OVAL auditing scan, you can see whether a system has had the appropriate security patches applied.

OVAL definition entries included in a SCAP data stream file can automatically download and apply remote OVAL definitions, such as the ones provided by Oracle at https://linux.oracle.com/security.

If you're working in a disconnected environment, you can manually download OVAL definition files to make available to systems within the environment. Scans can be performed with these local definition files using the `--local-files` option.

Downloading OVAL Files

Oracle provides OVAL definitions for all errata on ULN. Use these definitions to ensure that all applicable errata are installed on an Oracle Linux system.

1. Download the definition files.

   Download the file from https://linux.oracle.com/security.

   The following file types are available:

   Individual OVAL definition files

   These files contain the definitions for specific security patches. For example, `com.oracle.elsa-20205535.xml` relates to ELSA-2020-5535.

   Consolidated OVAL definition files

   These files are compressed using the `bzip2` algorithm and contain all OVAL definitions represented either by year or platform. For example, `com.oracle.elsa-2024.xml.bz2` contains all the definitions for the year 2024. A complete archive of all the OVAL definitions for every ELSA patch is available in `com.oracle.elsa-all.xml.bz2`. Consolidated OVAL definitions are also provided for each Oracle Linux release in files named using the format `com.oracle.elsa-ol`*release*`.xml.bz2`.

   For example, to download the consolidated OVAL definitions for all ELSA patches for Oracle Linux 8, run:

   ```
   wget https://linux.oracle.com/security/oval/com.oracle.elsa-ol8.xml.bz2
   ```

2. Extract the consolidated definition files, if required.

   If you downloaded a compressed file, extract the OVAL definition file:

   ```
   bzip2 -d com.oracle.elsa-ol8.xml.bz2
   ```

3. Run a scan.

To run a scan, see Running an OVAL Auditing Scan.

Displaying Information About an OVAL File

You can display information about an OVAL file using the oscap info command.

The command syntax is as follows:

```
oscap info path/OVAL file
```

For example:

```
oscap info com.oracle.elsa-2024.xml
```

The output shows the OVAL version and when the file was generated and imported:

```
Document type: OVAL Definitions
OVAL version: 5.11
Generated: date and time
Imported: date and time
```

Validating OVAL Files

You can validate an OVAL file against its schema using the oscap validate command.

Use oscap validate and examine the exit code to validate an OVAL file against its schema. This confirms that the file is correctly formatted.

For example, to validate the com.oracle.elsa-2024.xml OVAL file, run the following command:

```
oscap oval validate com.oracle.elsa-2024.xml \
 && echo "ok" || echo "exit code = $? not ok"
```

```
ok
```

Running an OVAL Auditing Scan

Scan an Oracle Linux system against an OVAL definition file to verify that all applicable errata has been installed.

1. Obtain the OVAL definition file.

   If you need to manually download and install particular OVAL definitions, follow the instructions in Download the OVAL definition file.

2. Perform a system audit using the OVAL definition file.

   Run the following command if you have manually downloaded an OVAL definition file and you want to audit a system against it:

   ```
   sudo oscap oval eval –-results path/results-file-name.xml \
   --report path/report-file-name.html path/OVAL-definition-file-name.xml
   ```

For example:

```
sudo oscap oval eval --results /tmp/elsa-results-oval.xml \
--report /var/www/html/elsa-report-oval.html com.oracle.elsa-all.xml
```

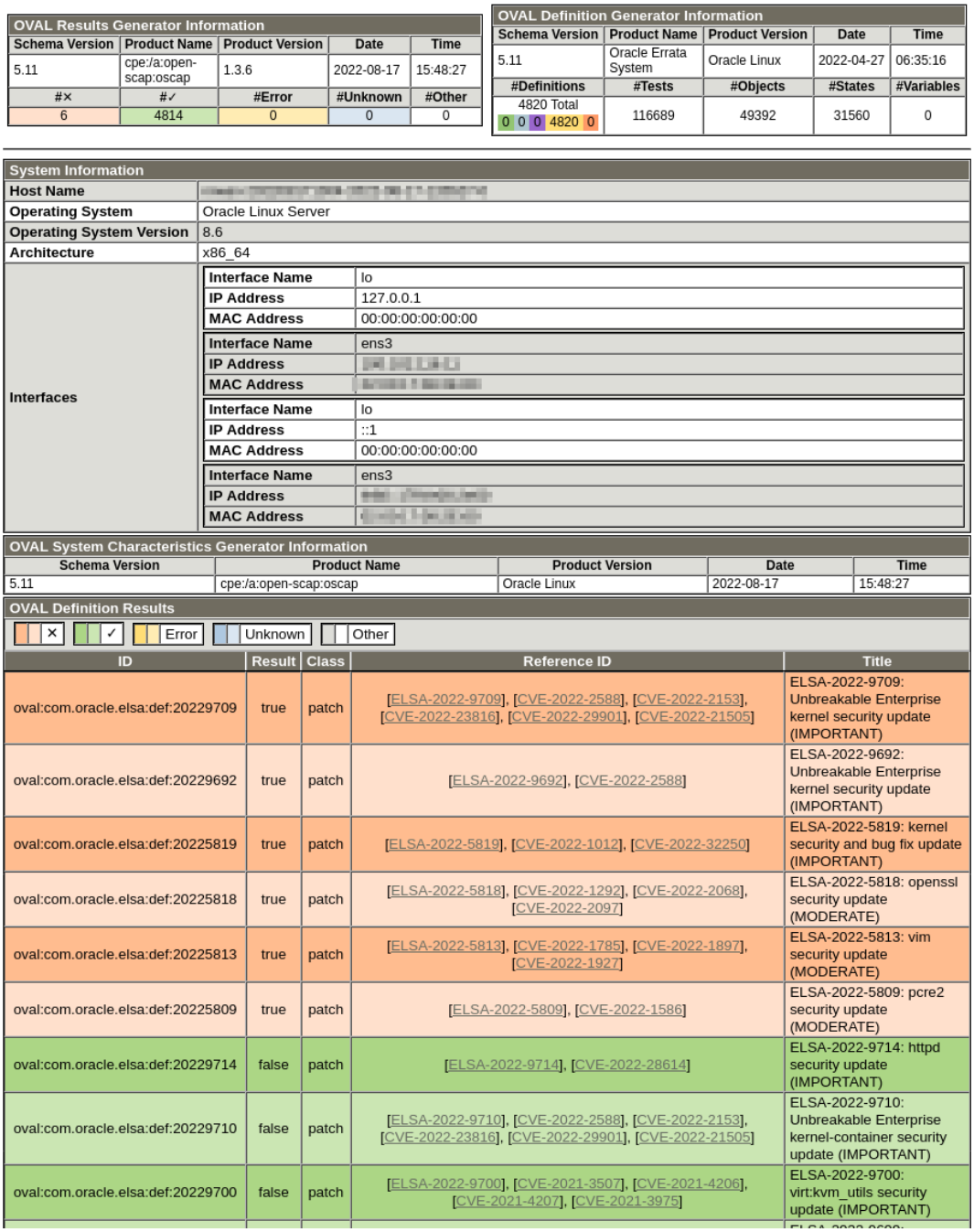
The output appears as follows:

```
...
Definition oval:com.oracle.elsa:def:20259978: false
Definition oval:com.oracle.elsa:def:20259940: false
Definition oval:com.oracle.elsa:def:20259896: true
Definition oval:com.oracle.elsa:def:20259880: false
Definition oval:com.oracle.elsa:def:20259878: false
Definition oval:com.oracle.elsa:def:20259877: false
Definition oval:com.oracle.elsa:def:20259845: false
Definition oval:com.oracle.elsa:def:20259844: false
Definition oval:com.oracle.elsa:def:20259741: false
Definition oval:com.oracle.elsa:def:20259740: false
Definition oval:com.oracle.elsa:def:20259635: false
Definition oval:com.oracle.elsa:def:20259634: false
Definition oval:com.oracle.elsa:def:20259623: false
Definition oval:com.oracle.elsa:def:20259605: false
Definition oval:com.oracle.elsa:def:20259580: false
...
Evaluation done.
```

> **Important**
>
> 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.

3. View the HTML report.

   Open the report in a browser to view it. Sample HTML report:



OVAL Results Generator Information

Schema Version	Product Name	Product Version	Date	Time
5.11	cpe:/a:open-scap:oscap	1.3.6	2022-08-17	15:48:27
#×	#✓	#Error	#Unknown	#Other
6	4814	0	0	0

OVAL Definition Generator Information

Schema Version	Product Name	Product Version	Date	Time
5.11	Oracle Errata System	Oracle Linux	2022-04-27	06:35:16
#Definitions	#Tests	#Objects	#States	#Variables
4820 Total: 0 0 0 4820 0	116689	49392	31560	0

System Information

Host Name	[redacted]
Operating System	Oracle Linux Server
Operating System Version	8.6
Architecture	x86_64
Interfaces	Interface Name: lo IP Address: 127.0.0.1 MAC Address: 00:00:00:00:00:00 Interface Name: ens3 IP Address: [redacted] MAC Address: [redacted] Interface Name: lo IP Address: ::1 MAC Address: 00:00:00:00:00:00 Interface Name: ens3 IP Address: [redacted] MAC Address: [redacted]

OVAL System Characteristics Generator Information

Schema Version	Product Name	Product Version	Date	Time
5.11	cpe:/a:open-scap:oscap	Oracle Linux	2022-08-17	15:48:27

OVAL Definition Results

× ✓ Error Unknown Other

ID	Result	Class	Reference ID	Title
oval:com.oracle.elsa:def:20229709	true	patch	[ELSA-2022-9709], [CVE-2022-2588], [CVE-2022-2153], [CVE-2022-23816], [CVE-2022-29901], [CVE-2022-21505]	ELSA-2022-9709: Unbreakable Enterprise kernel security update (IMPORTANT)
oval:com.oracle.elsa:def:20229692	true	patch	[ELSA-2022-9692], [CVE-2022-2588]	ELSA-2022-9692: Unbreakable Enterprise kernel security update (IMPORTANT)
oval:com.oracle.elsa:def:20225819	true	patch	[ELSA-2022-5819], [CVE-2022-1012], [CVE-2022-32250]	ELSA-2022-5819: kernel security and bug fix update (IMPORTANT)
oval:com.oracle.elsa:def:20225818	true	patch	[ELSA-2022-5818], [CVE-2022-1292], [CVE-2022-2068], [CVE-2022-2097]	ELSA-2022-5818: openssl security update (MODERATE)
oval:com.oracle.elsa:def:20225813	true	patch	[ELSA-2022-5813], [CVE-2022-1785], [CVE-2022-1897], [CVE-2022-1927]	ELSA-2022-5813: vim security update (MODERATE)
oval:com.oracle.elsa:def:20225809	true	patch	[ELSA-2022-5809], [CVE-2022-1586]	ELSA-2022-5809: pcre2 security update (MODERATE)
oval:com.oracle.elsa:def:20229714	false	patch	[ELSA-2022-9714], [CVE-2022-28614]	ELSA-2022-9714: httpd security update (IMPORTANT)
oval:com.oracle.elsa:def:20229710	false	patch	[ELSA-2022-9710], [CVE-2022-2588], [CVE-2022-2153], [CVE-2022-23816], [CVE-2022-29901], [CVE-2022-21505]	ELSA-2022-9710: Unbreakable Enterprise kernel-container security update (IMPORTANT)
oval:com.oracle.elsa:def:20229700	false	patch	[ELSA-2022-9700], [CVE-2021-3507], [CVE-2021-4206], [CVE-2021-4207], [CVE-2021-3975]	ELSA-2022-9700: virt:kvm_utils security update (IMPORTANT)

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:

```
sudo oscap oval generate report /tmp/elsa-results-oval.xml \
/var/www/html/elsa-report-oval.html
```

7

Scanning Container Images and Containers

To scan containers or container images, use the oscap-podman command. The oscap-podman command assesses vulnerabilities in the container or image and checks compliance with security policies similarly to the oscap command. The tool uses offline scanning to perform all assessments and checks by performing a temporary read-only mount of the container or image file system. No changes are made to the container or image and no other tools are required within the container or image.

1. Obtain the ID of the container or image.

   To retrieve the ID of the container or image. Run one of the following commands:

   ```
   podman ps -a
   ```

   ```
   podman images
   ```

2. Scan the image using an OVAL file.

   To scan an image for vulnerabilities using the appropriate CVE stream for the image variant and to output this information in HTML format, run the following command:

   ```
   sudo oscap-podman id oval eval --report reports.html oval-file
   ```

3. Scan the image using an XCCDF checklist.

   To scan an image for compliance with a security policy specified in an XCCDF checklist and to output the result in HTML format, run:

   ```
   sudo oscap-podman id xccdf eval \
     --fetch-remote-resources \
     --profile profile-id \
     --results results.xml \
     --report report.html \
     /usr/share/xml/scap/ssg/content/ssg-ol8-ds.xml
   ```

See the oscap-podman(8) manual page for more information.

8

Scanning Offline File Systems

To perform an offline scan of a mounted file system, use the oscap-chroot utility. You can use oscap-chroot for scanning custom objects that oscap-podman can't work with, such as containers that use a different format or virtual machine disk files. The options for this tool are similar to those of the oscap command.

For example, to audit a file system mounted at /mnt audit using an OVAL definitions file, run the following command:

```
sudo oscap-chroot /mnt oval eval --results /tmp/elsa-results-oval.xml \
  --report elsa-report-oval.html com.oracle.elsa-2024.xml
```

See the oscap-chroot(8) manual page for more information.

9
Scanning Remote Systems

Use oscap-ssh to scan remote systems over an SSH connection. By using remote scanning you can audit systems that you don't have physical access to and that might not have a current version of the SCAP Security Guide or current OVAL definitions available. The oscap-ssh is often used to scan several remote systems against a single locally stored and maintained OVAL definition file. The oscap-ssh command is provided in the openscap-utils package.

The remote system must have the openscap-scanner package installed, which provides the oscap command. This system must also be configured with a user account that you can connect with that has sudo privileges so you can run the scan correctly.

The oscap-ssh utility accepts the same sub commands and options as the oscap utility, but requires that you specify the hostname or IP address of the remote system to scan and the port number that SSH is listening on. Use the --sudo option to escalate user privileges before running the scan. Note that you're only able to use a data stream file when using oscap-ssh to perform an XCCDF scan on a remote system.

To scan a system remotely, run the oscap-ssh command as in the following example:

```
oscap-ssh --sudo oscap-user@198.51.100.157 22 \
    oval eval --results elsa-results-oval-198.51.100.157.xml \
    --report elsa-report-oval-198.51.100.157.html \
    com.oracle.elsa-ol8.xml
```

You can configure SSH options, such as the location of SSH keys, in the local user SSH configuration file or by setting the SSH_ADDITIONAL_OPTIONS environment variable . For more information about configuring SSH connections, see Oracle Linux: Connecting to Remote Systems With OpenSSH.

Although it might be possible to connect as the root user on a remote system directly over SSH, we recommend not doing this. Always use oscap-ssh with the --sudo option and configure an appropriate user on the remote system for this task. See Oracle Linux 8: Setting Up System Users and Authentication for more information.