Oracle Linux 8

Using OpenSCAP for Security Compliance

F28156-11
October 2022

Oracle Linux 8 Using OpenSCAP for Security Compliance,

F28156-11

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.

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/.

For information about the accessibility of the Oracle Help Center, see the Oracle Accessibility Conformance Report at https://www.oracle.com/corporate/accessibility/templates/t2-11535.html.

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 monitoring a system for vulnerabilities and make sure 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 can be parsed easily and can be modified 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 facilitates scanning a system against a SCAP Security Guide profile which is usually 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 multiple profiles that apply to different use cases. 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 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 is released by the Defense Information Systems Agency (DISA) and to provide remediation steps to help bring a system in line with a particular recommendation.

The Oracle Linux installer also provides options to install the operating system to match a specific security profile or policy as defined by the XCCDF profiles available in the the `scap-security-guide` package. By enforcing a policy at install time, you can make sure that your system starts running with a compliant base. See Oracle Linux 8: Installing Oracle Linux for more information.

OSCAP enables auditing your systems against Open Vulnerability and Assessment Language (OVAL) definition files that are used to test whether a system may 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, usually named with the file name suffix `.ds`. OSCAP can process data stream files similarly to XCCDF files. Oracle recommends using data stream files whenever possible as they help to reduce overhead and can contain references to external resources that can be kept current.

2
Installing SCAP Packages

Use `dnf` to install the SCAP packages from the Oracle Linux 8 AppStream repository.

1. Verify the `ol8_appstream` repository is enabled.
2. Use dnf to install the packages. For example:

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

Available Packages

The following SCAP packages are available:

- **`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 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 Oracle Linux 8 documentation.

3
OSCAP Information and Reference

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

The `oscap` command includes several subcommands that control different behaviors and that 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 plug-in 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) 1.3.6
Copyright 2009--2021 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 within the `scap-security-guide` package .

oscap Command Reference

The general command syntax of `oscap` is:

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

`oscap` supports the following module types:

- **`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).

Generally, the most useful modules are `info`, `oval`, and `xccdf` for scanning Oracle Linux systems. 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 subcommand 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 your system complies with a security compliance checklist. OSCAP can generate reports and display information about your system by using XCCDF profiles that can help you harden a system to meet particular security requirements, recommendations or guidelines. Note that 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

Use `oscap xccdf validate` and examine the exit code to validate an XCCDF file against its schema. This confirms that the file is properly structured.

For example, to validate an XCCDF file you can run:

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

If the file is valid, the command example returns:

```
ok
```

XCCDF files are shipped along with several other SCAP security guide files as part of the `scap-security-guide` package.

Similarly, use `oscap ds sds-validate` and examin the exit code to validate a source data stream file against its schema. 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 a number of SCAP related artifacts.

To validate a source data stream file, you can run:

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

If the file is valid, the command example returns:

```
ok
```

Displaying Available Profiles

Use `oscap info` to display profiles that are supported by a checklist file such as the SCAP Security Guide XCCDF file or a SCAP data stream that contains XCCDF content.

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. The listed profiles 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.

View available profiles

```
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: 2022-07-05T20:10:04

Stream: scap_org.open-scap_datastream_from_xccdf_ssg-ol8-xccdf-1.2.xml
Generated: (null)
Version: 1.3
Checklists:
    Ref-Id: scap_org.open-scap_cref_ssg-ol8-xccdf-1.2.xml
WARNING: Datastream component 'scap_org.open-scap_cref_security-oval-
com.oracle.elsa-all.xml.bz2' points out
 to the remote 'https://linux.oracle.com/security/oval/com.oracle.elsa-
all.xml.bz2'.
 Use '--fetch-remote-resources' option to download it.
WARNING: Skipping 'https://linux.oracle.com/security/oval/com.oracle.elsa-
all.xml.bz2' file which is referenced
 from datastream
        Status: draft
        Generated: 2022-07-05
        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: 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-all.xml.bz2
                system: http://oval.mitre.org/XMLSchema/oval-definitions-5
Checks:
  Ref-Id: scap_org.open-scap_cref_ssg-ol8-oval.xml
  Ref-Id: scap_org.open-scap_cref_ssg-ol8-ocil.xml
  Ref-Id: scap_org.open-scap_cref_--builddir--build--BUILD--scap-security-
guide-0.1.60--build--ssg-ol8-cpe-oval.xml
  Ref-Id: scap_org.open-scap_cref_security-oval-com.oracle.elsa-all.xml.bz2
Dictionaries:
  Ref-Id: scap_org.open-scap_cref_--builddir--build--BUILD--scap-security-
guide-0.1.60--build--ssg-ol8-cpe-dictionary.xml
```

> **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 to allow OSCAP to automatically download these resources, or you should manually download the resources beforehand and use the `--local-files` option to provide the path that should be used for these components. The ssg-ol8-ds.xml data stream file contains information about where to download OVAL definitions so that evaluations are able to audit against the most recent version of these definitions.

View information about a profile

Specify the `--profile` option.

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

For example:

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

Sample output:

```
Document type: Source Data Stream
Imported: 2022-07-05T20:10:04

Stream: scap_org.open-scap_datastream_from_xccdf_ssg-ol8-xccdf-1.2.xml
Generated: (null)
Version: 1.3
Profile
    Title: Standard System Security Profile for Oracle Linux 8
    Id: xccdf_org.ssgproject.content_profile_standard

    Description: 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.
```

In the example the full profile ID is used, but OSCAP also recognizes short profile IDs and these are commonly used.

Running a Scan Against an XCCDF Profile

Use the `oscap xccdf eval` command to scan a system against an XCCDF profile and generate a compliance evaluation report.

1. Determine which profile to use. See Displaying Available Profiles.
2. Run a scan specifying the specific profile.

   ```
   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 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 allows OSCAP to connect to the internet to download remote resources that are required for the XCCDF profile evaluation. If your systems are in a disconnected environment, you can use the `--local-files` option to allow OSCAP to use pre-downloaded resources at a specified path. The ssg-ol8-ds.xml data stream file includes a reference to the remotely hosted OVAL definitions that should be used when evaluating whether a system is properly patched.
If you use an XCCDF file instead of the recommended data stream, you must alos specify the location of the CPE dictionaries by using 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
```

Any rule in a profile that results in a `fail` potentially requires the system to be reconfigured.

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

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 | 1

4. Review the results 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 ssg-results.xml
   ```

   Note that the Test Results 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.

Generating a Full Security Guide

Use the `oscap xccdf generate guide` command to create a full security guide which provides a catalog of security-relavant configuration settings for the system. Security guides often include example bash remediation scripts and Ansible snippets that can be helpful when run against the system to automatically resolve issues. Be aware that you should test remediation scripts on systems within a test environment as actions taken by scripts may not be desirable for your enterprise.

To create a full security guide:

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

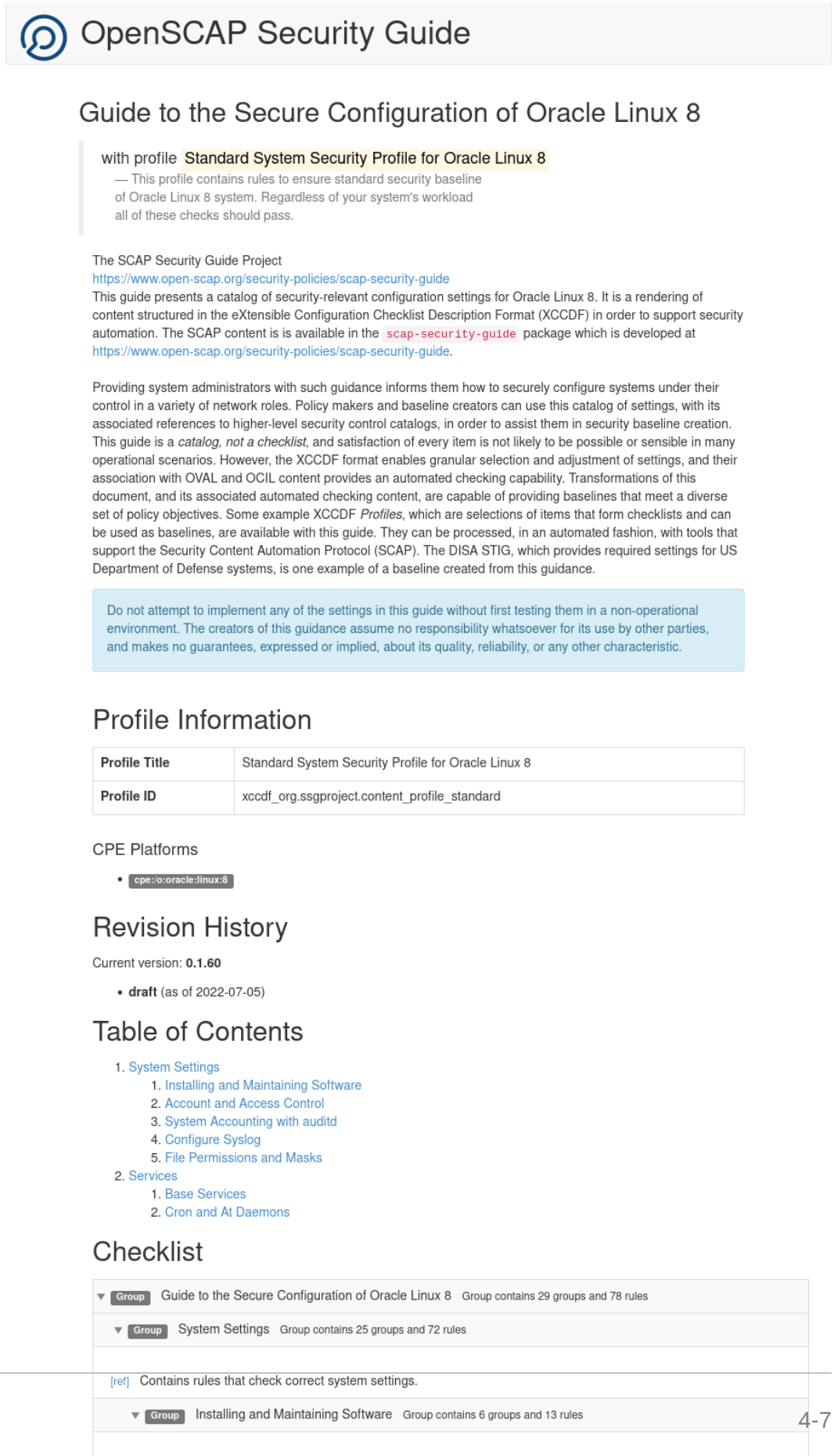
   ```
   sudo oscap xccdf generate guide --profile <profile-name> \
   /usr/share/xml/scap/ssg/content/<file>.xml > <path>/<security-guide-
   name>.html
   ```

   For example:

   ```
   sudo oscap xccdf generate guide --profile 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, as shown in the following figure.

Figure 4-1 Sample Security 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

1. System Settings
    1. Installing and Maintaining Software
    2. Account and Access Control
    3. System Accounting with auditd
    4. Configure Syslog
    5. File Permissions and Masks
2. Services
    1. Base Services
    2. Cron and At Daemons

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

Remediating a System For Compliance With a Security Profile

Security Guides and Evaluation Reports that are generated from an XCCDF profile may contain remediation information that can help you to resolve potential compliance issues. Remediation information is usually provided in the form of a bash script or Ansible playbook that can be run on the system where the report or guide was generated.

OSCAP also provides commands that can automatically apply remediation steps where the system fails to comply with the XCCDF profile. Remediation steps are typically performed against a fresh install to provide an initial configuration that is compliant with a baseline XCCDF profile.

> **WARNING:**
>
> Remediation steps can make changes to a system that may restrict accesses or alter how a system functions. There is no way to automatically revert a remediation once it is applied. Remediation steps are also designed to be run against a base install of the operating system. If you have changed system configuration, a remediation step does not guarantee compliance with the XCCDF profile. Do not apply remediation steps to production systems without testing them first.

> **Note:**
>
> Although Ansible playbook remediation is available for large portions of the Oracle Linux SCAP content provided, these are currently considered to be less complete than bash script remediation.

Immediate Remediation

To allow OSCAP to automatically apply remediation steps immediately during the scan against an XCCDF profile, 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.

This process is generally recommended after installation where a security profile was not selected at the time that the system was installed.

Generating Remediation Scripts For Later Use

It is possible to generate remediation scripts for later use, so that you can review the remediation actions and modify them before applying the changes to a system.

To generate a remediation script that provides fixes specific to a system 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 standard --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 compatible remediation script in YAML format.

To generate a script that provides all of the remediations present in a profile, run the same command against the data stream or XCCDF file, for example:

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

5

Auditing for Vulnerabilities By Using OVAL Definitions

You can use OVAL definition files to audit your system for known vulnerabilities and configuration issues. By performing an OVAL auditing scan, you are able to determine whether available security patches have been properly applied to a system.

Additionally, OVAL definition entries within a SCAP data stream file can be leveraged to run audits and to automatically download and use remote OVAL definitions, such as those provided by Oracle at https://linux.oracle.com/security.

If you have a disconnected environment, you can manually download OVAL definition files to make available to systems within your environment. Scans can be performed using the `--local-files` option to use pre-downloaded definitions.

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 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 of the OVAL definitions represented either by year or platform. For example, `com.oracle.elsa-2022.xml.bz2` contains all of the definitions for the year 2022. A complete archive of all of 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 in the format `com.oracle.elsa-ol<x>.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. If you downloaded a compressed file, extract the OVAL definitions file:

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

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

Displaying Information About an OVAL File

Use `oscap info` to display information about an OVAL file.

```
oscap info <path>/<OVAL-file>
```

For example:

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

Sample output:

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

> **Note:**
>
> You can download OVAL definition files (such as `com.oracle.elsa-2019.xml`) from https://linux.oracle.com/security/.

Validating OVAL Files

Use `oscap validate` and examine the exit code to validate an OVAL file against its schema. This confirms that the files are properly structured.

For example, to validate an OVAL file you can run:

```
oscap oval validate com.oracle.elsa-2019.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. 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 a specific OVAL definition file.

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

   ```
   sudo oscap oval eval --results <path>/<results-name>.xml \
   --report <path>/<report-name>.html <path>/<OVAL-definition-file>.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:20229690: false
Definition oval:com.oracle.elsa:def:20229689: true
Definition oval:com.oracle.elsa:def:20229683: false
Definition oval:com.oracle.elsa:def:20229682: false
Definition oval:com.oracle.elsa:def:20229680: false
Definition oval:com.oracle.elsa:def:20229676: false
Definition oval:com.oracle.elsa:def:20229675: false
Definition oval:com.oracle.elsa:def:20229670: false
Definition oval:com.oracle.elsa:def:20229669: false
Definition oval:com.oracle.elsa:def:20229668: false
Definition oval:com.oracle.elsa:def:20229667: false
Definition oval:com.oracle.elsa:def:20229612: false
Definition oval:com.oracle.elsa:def:20229609: false
Definition oval:com.oracle.elsa:def:20229602: false
Definition oval:com.oracle.elsa:def:20229601: true
...
Evaluation done.
```

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

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)

6
Scanning Container Images and Containers

Use `oscap-podman` to scan containers or container images.

`oscap-podman` 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 additional tools are required within the container or image.

1. Obtain the ID of your container or image. Run either:

   ```
   podman ps -a

   podman images
   ```

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

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

3. 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.

7
Scanning Offline File Systems

Use `oscap-chroot` to perform an offline scan of a file system that is mounted at a specified path.

You can use `oscap-chroot` for scanning custom objects that are not supported by `oscap-podman`, like containers that use an alternate format or for virtual machine disk files. The options for this tool are similar to the `oscap` command.

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

```
sudo oscap-chroot /mnt oval eval --results /tmp/elsa-results-oval.xml \
  --report elsa-report-oval.html com.oracle.elsa-2021.xml
```

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

8
Scanning Remote Systems

Use `oscap-ssh` to scan remote systems over an SSH connection. By using remote scanning you can audit systems that you do not have physical access to and that may not have a current version of the SCAP Security Guide or current OVAL definitions available. Most typically, this command can be used to scan multiple 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 should also be configured with a user account that you connect with and that has sudo privileges to be able to 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 are 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 your local user SSH configuration file or by setting the environment variable SSH_ADDITIONAL_OPTIONS. For more information about configuring your SSH connections, see Oracle Linux: Connecting to Remote Systems With OpenSSH.

Although, it may be possible to connect as the root user on a remote system directly over SSH, Oracle recommends against this practice. 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.