Oracle Linux Server Hardening and CIS Benchmark Compliance

On Oracle Linux and Oracle Cloud Infrastructure

Oracle Linux was created as a secure, high-performance alternative to Red Hat Enterprise Linux (RHEL). In theory, implementing CIS benchmarks or installing it as a CIS benchmark-hardened image makes the platform almost impregnable. Unfortunately, the Support Information for CIS Benchmarks and CIS Hardened Images for Oracle Linux (Doc ID 2949651.1) webpage states:

"Oracle currently does not support CIS Benchmarks for Oracle Linux. Customers obtain support directly from CIS and its community."

Conversely, for Oracle Cloud Infrastructure (OCI) instances, CIS benchmarks into the platform. In this article, we compare and contrast Oracle's various approaches to implementing the CIS benchmark and their impact on you.

What You Learn

- What hardening frameworks does Oracle support?
- Why STIG is Oracle's preferred option
- Understand STIG, CIS Benchmarks, and NIST SP 800-53 shared heritage
- How to install and run STIG's OpenScap locally
- Running CIS benchmarks on OCI

Local Oracle Linux Hardening

Just because Oracle doesn't support CIS benchmarks or hardened images doesn't mean they are opposed to all hardening frameworks; it just doesn't help one of the most popular options. Later in the support page, it asks this question:

"Is there any alternative to CIS Benchmarks and CIS hardened images for Oracle Linux that are provided by Oracle?"

And answers:

"Yes, Oracle provides Oracle Linux STIG image, an implementation of Oracle Linux that follows the Security Technical Implementation Guide (STIG), released by the Defense Information Systems Agency (DISA)."

Let's now examine what this means.

Hardening Oracle Linux with STIG

STIG's origin as a government defence program and CIS's roots as an industry initiative mean they are mutually opposed. In practice, they share many similarities. First, they were both created as a means of reducing an organization's attack surface and mitigating malicious exploits. Second, they share DNA with a common ancestor, as specified in the National Institute of Standards and Technology (NIST)'s NIST-SP-800-53. STIG is a secure version of the framework, while many CIS Benchmarks reference it as a source of information. Another similarity is that both frameworks provide downloadable baseline images.

While they share many similarities, there are also notable differences, particularly in implementation and execution. CIS benchmarks are prescriptive. You download a PDF of an Excel file and build your own solution. Your solution could be manual, partially automated by writing your own scripts, or automated using a tool like CalCom's CHS. You can install and run STIG directly from the command line.

First, you download and install the STIG package and security guide:

```
sudo dnf install -y openscap openscap-scanner scap-security-guide
```

Next, you list and verify the available packages:

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

This displays a list of packages:

```
Profile ID: xccdf_org.ssgproject.content_profile_stig
Title: DISA STIG for Oracle Linux 8
Profile ID: xccdf_org.ssgproject.content_profile_cis
Title: CIS Benchmark for Oracle Linux 8
```

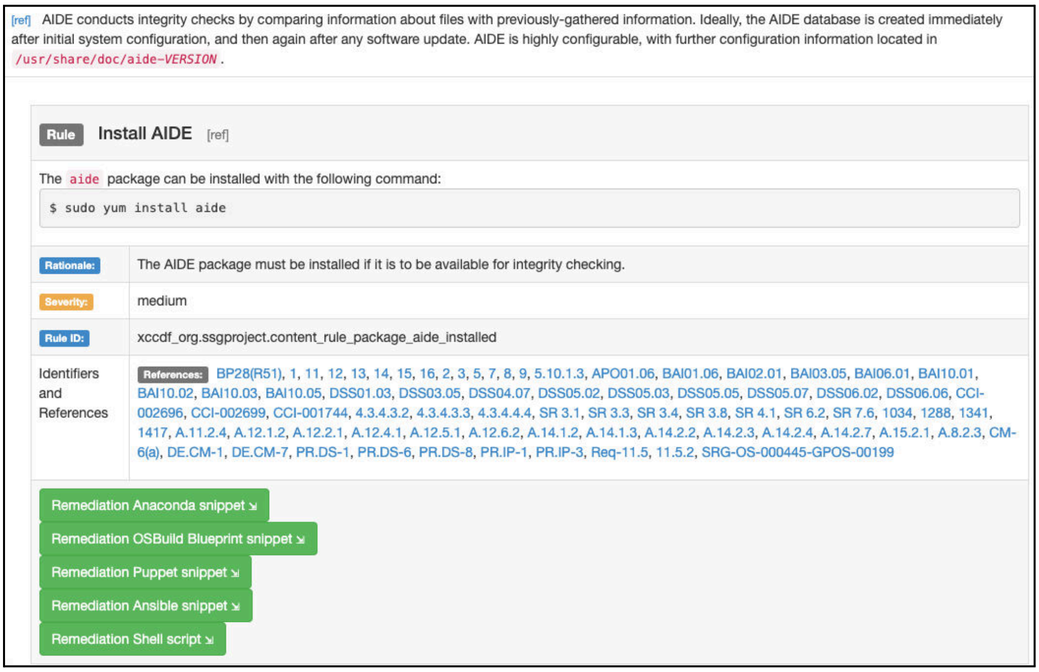
Now, you can run a scan.

```
sudo oscap xccdf eval --profile xccdf_org.ssgproject.content_profile_stig
--results /tmp/ol8-stig-results.xml --report /tmp/ol8-stig-report.html
/usr/share/xml/scap/ssg/content/ssg-ol8-ds.xml
```

After the scan, you display the report:

```
xdg-open /tmp/ol8-stig-report.html
```

Here is a sample report:



[ref] AIDE conducts integrity checks by comparing information about files with previously-gathered information. Ideally, the AIDE database is created immediately after initial system configuration, and then again after any software update. AIDE is highly configurable, with further configuration information located in `/usr/share/doc/aide-VERSION`.

Rule Install AIDE [ref]

The `aide` package can be installed with the following command:

```
$ sudo yum install aide
```

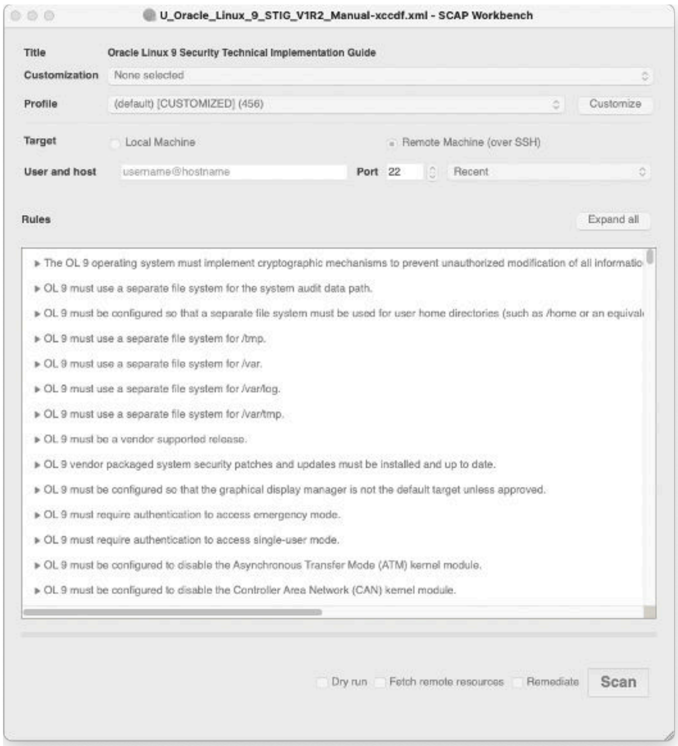
Rationale:	The AIDE package must be installed if it is to be available for integrity checking.
Severity:	medium
Rule ID:	xccdf_org.ssgproject.content_rule_package_aide_installed
Identifiers and References	References: BP28(R51), 1, 11, 12, 13, 14, 15, 16, 2, 3, 5, 7, 8, 9, 5.10.1.3, APO01.06, BAI01.06, BAI02.01, BAI03.05, BAI06.01, BAI10.01, BAI10.02, BAI10.03, BAI10.05, DSS01.03, DSS03.05, DSS04.07, DSS05.02, DSS05.03, DSS05.05, DSS05.07, DSS06.02, DSS06.06, CCI-002696, CCI-002699, CCI-001744, 4.3.4.3.2, 4.3.4.3.3, 4.3.4.4.4, SR 3.1, SR 3.3, SR 3.4, SR 3.8, SR 4.1, SR 6.2, SR 7.6, 1034, 1288, 1341, 1417, A.11.2.4, A.12.1.2, A.12.2.1, A.12.4.1, A.12.5.1, A.12.6.2, A.14.1.2, A.14.1.3, A.14.2.2, A.14.2.3, A.14.2.4, A.14.2.7, A.15.2.1, A.8.2.3, CM-6(a), DE.CM-1, DE.CM-7, PR.DS-1, PR.DS-6, PR.DS-8, PR.IP-1, PR.IP-3, Req-11.5, 11.5.2, SRG-OS-000445-GPOS-00199

Remediation Anaconda snippet ↘
Remediation OSBuild Blueprint snippet ↘
Remediation Puppet snippet ↘
Remediation Ansible snippet ↘
Remediation Shell script ↘

You can also generate remediation scripts:

```
sudo oscap xccdf generate fix --profile
xccdf_org.ssgproject.content_profile_stig
/usr/share/xml/scap/ssg/content/ssg-ol8-ds.xml  > /tmp/stig-fixes.sh
```

Another way to use STIG is with a viewer, such as the OpenSCAP Workbench.



U_Oracle_Linux_9_STIG_V1R2_Manual-xccdf.xml - SCAP Workbench

Title Oracle Linux 9 Security Technical Implementation Guide
Customization None selected
Profile (default) [CUSTOMIZED] (456)
Target ○ Local Machine ● Remote Machine (over SSH)
User and host username@hostname Port 22 Recent

Rules

- ▸ The OL 9 operating system must implement cryptographic mechanisms to prevent unauthorized modification of all informatio
- ▸ OL 9 must use a separate file system for the system audit data path.
- ▸ OL 9 must be configured so that a separate file system must be used for user home directories (such as /home or an equival
- ▸ OL 9 must use a separate file system for /tmp.
- ▸ OL 9 must use a separate file system for /var.
- ▸ OL 9 must use a separate file system for /var/log.
- ▸ OL 9 must use a separate file system for /var/tmp.
- ▸ OL 9 must be a vendor supported release.
- ▸ OL 9 vendor packaged system security patches and updates must be installed and up to date.
- ▸ OL 9 must be configured so that the graphical display manager is not the default target unless approved.
- ▸ OL 9 must require authentication to access emergency mode.
- ▸ OL 9 must require authentication to access single-user mode.
- ▸ OL 9 must be configured to disable the Asynchronous Transfer Mode (ATM) kernel module.
- ▸ OL 9 must be configured to disable the Controller Area Network (CAN) kernel module.

□ Dry run □ Fetch remote resources □ Remediate

CIS Benchmarks and Oracle Cloud Infrastructure (OCI) Hardening

Unlike its downloadable sibling, OCI openly supports CIS Oracle Linux benchmarks. In fact, OCI offers open-source tools for generating benchmarking reports. These tools are publicly available on GitHub. Even more surprising is that OCI directly integrates its control console with OCI. This enables running host scans and viewing the results directly from the command line.

The first step is to create a CIS-enabled host scan recipe:

```
oci vulnerability-scanning host-scan-recipe create --compartment-id
<compartment_ocid> --display-name "OL9-CIS-Recipe" --agent-settings
'{"scanLevel":"STANDARD"}' --cis-benchmark-settings
'{"scanLevel":"LEVEL_1","scanMode":"ENABLED"}' --operating-system
"ORACLE_LINUX" --schedule-type "DAILY"
```

Next, you create a Host Scan Target:

```
oci vulnerability-scanning host-scan-target create --compartment-id
<compartment_ocid> --display-name "OL9-CIS-Target" --host-scan-recipe-id
<recipe_ocid> --target-compartment-id <compartment_ocid>
```

View a list of CIS Benchmarks in the scan with this command:

```
oci vulnerability-scanning host scan result cis-benchmark list
```

Display scan details with this command:

```
oci vulnerability-scanning host scan result cis-benchmark get
```

You can also export the data to a CSV file with this command:

```
oci vulnerability-scanning host scan result cis-benchmark get [OPTIONS]
```

Different Paths, Same Outcome

No matter whether your chosen environment is a physical server or an OCI instance, Oracle supports hardening frameworks. When installing locally, an Oracle-supported framework might not be your first choice, but it's still a better option than starting from scratch. An official, vendor-supported hardening solution is still a vast improvement over no solution or creating ad-hoc efforts using manual processes and scripts. Not only will the results be far superior, but in the long term, you will also reduce your maintenance overheads, both in terms of time and money. The fact that STIG and CIS Benchmarks have common roots in NIS-SP-800-53 provides additional peace of mind. When it comes to OCS, you have a far wider range of options that include and extend beyond CIS and STIG. Either way, when it comes to hardening, whatever your platform, Oracle Linux and OCI have your back.

Key Takeaways

1. Oracle Linux does not officially support CIS Benchmarks locally
2. Oracle provides a STIG-based hardening option
3. CIS Benchmarks are fully supported in Oracle Cloud Infrastructure (OCI)
4. Both CIS and STIG share a common foundation in NIST SP 800-53
5. CalCom's Hardening Suite (CHS) automates and simplifies baseline management, eliminating the manual scripting required by Oracle's CLI-based solutions.

How CalCom Can Help You

Oracle's hardening solutions are great, but you have to run them from the command line. While they can automate a wide range of tasks, you must either type in individual commands or collect them together into scripts. Each time Oracle or the framework makes changes, you will need to update and possibly rewrite these scripts by hand. Your initial scripts may save you time, but over time, your hardening suite will have the same drawbacks as building a manual solution.

What you need is CalCom's Hardening Suite. (CHS) It is a baseline hardening solution designed to address the needs of IT operations and security teams. CHS significantly reduces operational costs and eliminates service downtime by indicating the impact of a security baseline change directly on the production environment. CHS's automated process simulates the effect of a change in a production environment, thus saving the need for testing changes in a lab environment. CHS enables you to:

- Deploy security baselines without affecting the production services.
- Reduce the costs and resources for implementing compliance.
- Manage hardening baselines for your entire infrastructure from a single point.
- Avoid configuration drifts and repeated hardening processes.
- Furthermore, unlike Oracle's CLI solutions, CHS has a user-friendly interface that can visualize collected data

To learn more, go to our resources page and download our datasheets and white papers.

FAQs

Question	Answer
Does Oracle Linux support CIS Benchmarks?	No. Oracle does not officially support CIS Benchmarks for local installations. Customers must obtain support directly from the CIS community.
What hardening framework does Oracle officially support?	Oracle supports the DISA STIG (Security Technical Implementation Guide) for Oracle Linux, which can be installed and managed through OpenSCAP.
Can CIS Benchmarks be used on Oracle Cloud Infrastructure (OCI)?	Yes. OCI provides full integration for CIS Benchmark scans using its Vulnerability Scanning Service (VSS), allowing CIS checks directly from the console or CLI.
How do STIG and CIS Benchmarks relate to NIST 800-53?	Both frameworks originate from the NIST 800-53 standard, sharing a common goal of reducing attack surfaces and enforcing secure configurations.
What are the limitations of Oracle's CLI-based hardening?	While effective, it requires manual scripting and maintenance. Each framework update demands script revisions, increasing long-term complexity.
How does CalCom Hardening Suite improve this process?	CalCom CHS automates baseline management, simulates configuration impacts before deployment, prevents drift, and provides a user-friendly interface for continuous compliance.
Why should organizations consider using CHS with Oracle Linux?	It reduces operational costs, eliminates manual errors, and ensures consistent, auditable hardening across Oracle Linux and OCI environments.