Oracle® Cloud

Using Oracle Configuration and Compliance

E78230-24
August 2019

Oracle Cloud Using Oracle Configuration and Compliance,

E78230-24

Primary Author: Oracle Corporation

Contents

Preface

Oracle Configuration and Compliance is a cloud-first solution enabling the compliance assessment of your on-premises, cloud, or hybrid cloud environments based on your business objectives.

Topics:

Target Audiences

Oracle Configuration and Compliance offers solutions targeted at the following audiences:

Oracle Configuration and Compliance is intended for users who want to manage a complete, integrated suite of systems management solutions designed to assess systems for compliance vulnerabilities. With Oracle Configuration and Compliance, you can test and evaluate systems to follow Security Technical Implementation Guide (STIG) compliance standards, check for SLA (service-level agreement) violations, be compliant with LOB (line of business) standards, remediate violations, and optimize your work on fixing vulnerabilities based on a prioritization and risk level chart.

Audience

Oracle Configuration and Compliance is intended for users who want to manage a complete, integrated suite of systems management solutions designed to assess systems for compliance vulnerabilities. With Oracle Configuration and Compliance, you can test and evaluate systems to follow Security Technical Implementation Guide (STIG) compliance standards, check for SLA (service-level agreement) violations, be compliant with LOB (line of business) standards, remediate violations, and optimize your work on fixing vulnerabilities based on a prioritization and risk level chart.

Related Resources

Apart from Oracle Configuration and Compliance, you can refer to the following resources for more information about Oracle Management Cloud.

- Oracle Cloud Home
- Using Oracle Application Performance Monitoring
- Using Oracle Log Analytics

- Using IT Analytics
- Getting Started with Oracle Infrastructure Monitoring

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 http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

1

Get Started with Oracle Configuration and Compliance

Topics:

About Configuration and Compliance

> **Note:**
>
> **As of September 2019, no enhancements have been made to this service and this functionality is no longer available to new customers.**

Oracle Configuration and Compliance is a cloud-first solution that helps you assess the compliance of your on-premises, cloud, or hybrid cloud environments based on your business objectives.

Oracle Configuration and Compliance automatically assesses, scores, and reports on the compliance posture of your enterprise. If your service level is low, or needs improvement, you can automate remediation at scale.

Here's how various stakeholders in your organization benefit:

- Oracle Management Cloud Users benefit from rapid, enterprise-wide assessment snapshots that provide compliance score trending data.
- Oracle Management Cloud Administrators receive a compliance violation dashboard, this dashboard includes a road map that shows the most severe violations impacting the compliance score.

Your business objectives may be derived from multiple compliance requirements mapped to your IT infrastructure. When you create an assessment template, you can select any combination of supported industry-standard benchmarks, custom rules, or cloud rules, and then execute those standards against the corresponding entities in your enterprise. Oracle Configuration and Compliance consists of the following functional areas:

- Results consumption and scoring of automated industry-standard benchmarks, such as Security Technical Implementation Guides (STIGs) in the Extensible Configuration Checklist Description Format (XCCDF).

- Execution of out-of-the box REST-based cloud rules against cloud provider endpoints, such as Oracle Cloud or Amazon Web Services (AWS).
- Execution and scoring of custom scripts or processes. You can map exit codes or text results to an assessment rule or to violation observations.

> **Note:**
>
> For the latest information on Oracle Configuration and Compliance Cloud Service, check My Oracle Support Configuration and Compliance Cloud Service Master Note 2223305.1.

About Oracle Configuration and Compliance Roles and Users

Once you are an Oracle Cloud customer and you create an Oracle Management Cloud instance, the following user roles are provisioned:

- Oracle Management Cloud Administrator
- Oracle Management Cloud User

Role	Tasks
Oracle Management Cloud Administrator	• Set up Oracle Configuration and Compliance. • Monitor your compliance score. • Create and administer new rules and rule sets. • Create, administer, and run assessments and assessment templates.
Oracle Management Cloud User	• Analyze rules and rule sets. • View and share completed assessments.

For more information about the tasks that the users assigned with the above roles can perform, see Adding Users and Assigning Roles in *Getting Started with Oracle Management Cloud*.

Before You Begin with Oracle Configuration and Compliance

Here are some basic terms used when discussing Oracle Configuration and Compliance.

Term	Definition
Assessment	An evaluation of a ruleset against an entity
Assessment template	A container defining how and when assessments run
Benchmark	A standard or point of reference that entities can be compared against

Term	Definition
Cloud rule	A check based on REST API
Custom (Script) rule	A check based on a host script
Compliance	The measurement of how your system meets a security standard
Compliance score	A numerical score by which you can measure your system's compliance
Deviation	How your system differs from the accepted standard
Entity	A monitored resource such as a database, a host server, a computer resource, or an application server
Entity type	The type of monitored resource
Open Vulnerability and Assessment Language (OVAL)	A standard for assessing and reporting the machine state of a computer system
Rule	A single check returning zero or more violations
Ruleset	A set of rules that run during the execution phase of a compliance assessment
Ruleset-Entity score	The score derived from an evaluation of a ruleset against an entity
Ruleset-Entity violations	The specific issues discovered during an evaluation of a ruleset against an entity

Configure Oracle Configuration and Compliance

Here are the prerequisites you will need to complete before you can start using Oracle Configuration and Compliance.

Task	Description	Configuration Information
Define SSH Host Credential	**Required** to assess the compliance of resources that require elevated privileges.	• Define SSH Host Credentials
Define Database Credential	**Required** to assess the compliance of Oracle Databases.	• Define Oracle Database Credentials
Define Cloud Credential	**Required** to assess the compliance of resources that run in Oracle Cloud or Amazon Web Services (AWS) by creating and configuring your Cloud Credential.	• Define Cloud Credentials

Task	Description	Configuration Information
Optional Configuration	**Configure Benchmark Engines** Execute an industry-standard benchmark assessment configuring a third party Security Content Automation Protocol (SCAP) certified engine, such as Open SCAP. **Configure your Custom Rules** Execute user-defined, language-independent custom scripts or standard output, and it can map multiple exit codes on pass or fail compliance violations.	• Configure Benchmark Engines • Configure a User-Defined Rule

Define SSH Host Credentials

With the Secure Socket Shell (SSH) host credential, you can run custom and industry-standard assessments.

An SSH host credential enables you to run custom or industry standard compliance assessments. You first configure the credential store, and then add the SSH host credential to the credential store. Note that the credential global name must be the reserved value `emcosComplianceCred`. On the host where the Oracle Cloud Agent is installed, perform the following steps from the agent installation directory (such as `<AGENT_BASE_DIR>/agent_inst/bin`):

Before you begin to create a SSH Host Credential, create and save a JSON file, for example **`cred.json`**, with your credential information as follows.

- **Option 1:** SSH Key (Recommended)

```
[
  {
    "name": "<HOST_NAME>-HostSSHCreds",
    "type": "AsAgentCreds",
    "globalName": "emcosComplianceCred",
    "description": "SSH Credential for the host agent",
    "disabled": false,
    "properties": [
     { "name":"USERNAME", "value":"CLEAR[oracle]" },
     { "name":"SSH_PVT_KEY", "value":"FILE[<YourUsername>/.ssh/
id_rsa]" },
     { "name":"SSH_PUB_KEY", "value":"FILE[<YourUsername>/.ssh/
id_rsa.pub]" }
   ]
  }
]
```

- **Option 2:** Password

```
[
  {
    "name":"<HOST_NAME>-HostSSHPwdCreds",
    "type":"AsAgentCreds",
    "globalName":"emcosComplianceCred",
    "description":"SSH Credential for the host agent",
    "disabled": false,
    "properties":[
      { "name":"USERNAME", "value":"CLEAR[YourUsername]"},
      { "name":"PASSWORD", "value":"CLEAR[YourPassword]"}
    ]
  }
]
```

Where:

- **HOST_NAME** is the fully qualified name of your host. For example: host1.example.com
- **Name** is any name for your credential. We recommend that you name this credential your host name followed by `HostSSHPwdCreds`. For example: `host1.example.com-HostSSHPwdCreds`.
- **YourUsername** is the username used as your SSH credential.
- **YourPassword** is the password for your SSH credential.
- All other field values must remain as listed. They are reserved values.

Create a SSH Host Credential:

1. Login as the user who installed the agent.

   ```
   $ su oracle
   ```

2. Stop the agent.

   ```
   $ omcli stop agent
   ```

3. Configure the agent to use a wallet-based credential store.

   ```
   $ omcli add_credential_store agent -no_password
   ```

4. Start the agent.

   ```
   $ omcli start agent
   ```

5. Add the credential to the credentials store.

   ```
   $ omcli add_credentials agent -credential_file cred.json -
   allow_entityless
   ```

6. Verify that the credential was installed correctly.

   ```
   $ omcli list_credentials agent

   Oracle Management Cloud Agent Copyright (c) 1996, 2018 Oracle
   Corporation. All rights reserved.
   Credential Name Type Entity Global Name Usage host1.example.com-
   ```

```
HostSSHPwdCreds
HostSSHPwdCreds (host1.example.com) "emcosComplianceCred"
```

> **Note:**
>
> If the SCAP benchmark or custom rules require root access, make sure **YourUsername** and **YourPassword** have root privileges. SCAP benchmark rules require administrator privileges to evaluate configuration information owned by and restricted to the root user.
>
> Many benchmarks require elevated privileges, either a root or a privileged user can run the benchmarks.

> **Note:**
>
> For the latest information on SSH Host Credentials, check My Oracle Support Configuration and Compliance Cloud Service Master Note 2223305.1 .

Define Oracle Database Credentials

A database credential is needed in addition to the host credential for proper rule-set evaluation as the rules in database assessments are evaluated using SQL.

Prerequisites

- The SSH credential is configured.
- The credential store has been created.
- The cloud agent is on the same host as the database.
- The user has privileges to execute the compliance SQL scripts.

Add Oracle Database Credentials

Add a database credential to run compliance assessments of your Oracle Database using Oracle Configuration and Compliance.

Oracle Configuration and Compliance will automatically use the database credentials being used by Oracle Infrastructure Monitoring to assess databases if you do not specify a database credential in the agent wallet. This functionality requires agent version 1.35+. If you already created a monitoring user, skip to Grant Oracle Database Privileges.

1. Open a terminal on the agent host and search for your `<DB_NAME>, <entity_type>` pair using the following command:

   ```
   $ omcli config agent listtargets
   ```

   You will need this information in order to add a new monitoring agent using `omcli`.

2. Create and save a JSON file, for example `test_db_cred.json`, with your credential information as follows:

```
[
  {
    "entity":"omc_oracle_db.<DB_NAME>",
    "name":"omc_oracle_<DB_NAME>-DBUserCreds",
    "type":"DBUserCreds",
    "globalName":"DBCred",
    "description":"DB Credential for the db entity",
    "properties":[
      { "name":"USERNAME", "value":"CLEAR[YourUserName]" },
      { "name":"PASSWORD", "value":"CLEAR[YourPassword]" }
    ]
  }
]
```

   Where:

   - **DB_NAME** is the name of your database. For example: dbserver.example.com
   - **Name** is any name for your credential. For example, as best practice, name this credential your entity type followed by `DB_NAME` and `DBUserCreds`, for example: `omc_oracle_db-dbserver.example.com-DBUserCreds`
   - **YourUserName** is the username used as your DB credential.
   - **YourPassword** is the password for your DB credential.
   - All other field values must remain as listed. They are reserved values.

3. Add the credential to the credentials store using the `test_db_cred.json` file.

```
$ omcli add_credentials agent -credential_file test_db_cred.json
```

4. Verify that the credential was installed correctly:

```
$ omcli list_credentials agent

Oracle Management Cloud Agent Copyright (c) 1996, 2018 Oracle
Corporation. All rights reserved.
Credential Name Type Entity Global Name Usage

omc_oracle_db-dbserver.example.com-DBUserCreds DBUserCreds
(dbserver.example.com) "DBCred"
```

Grant Oracle Database Privileges

Before you can monitor your database using out-of-the-box rule sets you need to grant the following privileges to your monitoring user.

By default, the credential being used by Oracle Infrastructure Monitoring will be used to connect to the database by Oracle Configuration and Compliance. If the monitoring credential user (e.g. `moncs`) was created using the script provided by

Oracle, additional privileges will need to be granted to the monitoring user for proper evaluation of the rule sets.

For proper evaluation of the Oracle Database 12c STIG Benchmark and CIS Oracle Database 12c Benchmark, it is recommended that a second privileged user be used as granting the necessary privileges to the monitoring user (e.g. `moncs`) will cause violations in these rule sets. It is recommended you use **`dbsnmp`** (a built-in user in Oracle Database) as this user has the necessary privileges by default with a few exceptions.

Required Privileges for User `dbsnmp`

These are the required privileges you will need to grant to user `dbsnmp` for the following rule sets.

Basic Security Configuration for Oracle Database

```
grant select on sys.link$ to dbsnmp;
```

Required Privileges for User `moncs`

These are the required privileges you will need to grant to user `moncs` for the following rule sets.

To create user `moncs`, see Oracle Database in *Using Oracle Infrastructure Monitoring*.

Basic Security Configuration for Oracle Database

```
grant select on dba_tab_privs to moncs;
grant select on dba_profiles to moncs;
grant select on dba_role_privs to moncs;
grant select on sys.link$ to moncs;
grant select on dba_users to moncs;
grant select on dba_users_with_defpwd to moncs;
```

Oracle Database 12c Single Instance Database STIG Configuration

```
grant select on dba_tab_privs to moncs;
grant select on dba_profiles to moncs;
grant select on dba_role_privs to moncs;
grant select on sys.link$ to moncs;
grant select on dba_users to moncs;
grant select on dba_users_with_defpwd to moncs;
grant select on dba_db_links to moncs;
grant select on v_$controlfile to moncs;
grant select on v_$log to moncs;
grant select on dba_sys_privs to moncs;
grant select on dba_tables to moncs;
grant select on dba_external_tables to moncs;
grant select on dba_objects to moncs;
grant select on dba_sys_privs to moncs;
grant select on dba_roles to moncs;
grant select on v_$encrypted_tablespaces to moncs;
grant select on v_$tablespace to moncs;
```

```
grant select on dba_encrypted_columns to moncs;
grant select on dba_constraints to moncs;
```

CIS Oracle Database 12c Benchmark Level 1

```
grant select on dba_tab_privs to moncs;
grant select on dba_profiles to moncs;
grant select on dba_role_privs to moncs;
grant select on sys.link$ to moncs;
grant select on dba_users to moncs;
grant select on dba_users_with_defpwd to moncs;
grant select on dba_db_links to moncs;
grant select on v_$controlfile to moncs;
grant select on v_$log to moncs;
grant select on dba_sys_privs to moncs;
grant select on dba_tables to moncs;
grant select on dba_external_tables to moncs;
grant select on dba_objects to moncs;
grant select on dba_sys_privs to moncs;
grant select on dba_roles to moncs;
grant select on v_$encrypted_tablespaces to moncs;
grant select on v_$tablespace to moncs;
grant select on dba_encrypted_columns to moncs;
grant select on dba_constraints to moncs;
grant select on dba_proxies to moncs;
grant select on dba_stmt_audit_opts to moncs;
grant select on dba_priv_audit_opts to moncs;
grant select on dba_obj_audit_opts to moncs;
```

> **Note:**
>
> Violations will be generated using these privileges to user **`moncs`**. It is recommended that you use user **`system`** for the *CIS Oracle Database 12c Level 1*rule set.

Once complete, you must assign a tag on each entity with key equal to **`complianceusedbcred`**. This will cause Oracle Configuration and Compliance to use the Database Credential configured in the wallet instead of the Oracle Infrastructure Monitoring credential.

Remove the Wallet Credential Requirement for Database Assessments

Apply this configuration to your hosts and database targets to remove the wallet credential requirement.

Using this tag will cause root privilege rules to be skipped because applying this tag to Host targets will run all assessments with the privilege level associated to the Cloud Agent. Typically SCAP benchmarks require root level privileges in order to execute all rules. Database targets don't have this limitation since the rules are always executed with the secondary Database Credential.

1. From the menu, select **Administration**, and click **Entity Configuration**

2. Add a new tag with **Name** *UseAsAgentCredential*, leave the **Value** empty.
3. Assign the Entities you want to configure.
4. Click **OK**.
5. Log in to each of the entities you want to configure and open a command-line interface. Run the following command:

```
$ <AGENT_BASE_DIR>/agent_inst/bin/omcli setproperty agent -
allow_new -name _enableAsAgentCredential -value
    true
```

Define Cloud Credentials

You need cloud credentials to access some information from your cloud resources.

For example, Amazon Web Services (AWS), requires access keys and secret keys. Oracle Public Cloud requires a user name, password, and domain ID.

> **Note:**
>
> We recommend that you use a credential with read-only access to the resources against which you want to execute cloud rules.

1. From the main menu, select **Administration**, and click **Cloud Discovery Profiles**.
2. To create a new cloud resource credential, click **Add Profile**.
3. Enter the **Profile Name** and **Cloud Service Provider**.
4. Enter the **Oracle Identity Domain** or **Identification Number** of another service.
5. Add the **Region** and **Service**.
6. Select **New Credentials**, enter a **Credential Name** and select a **Credential Type**.
7. Enter the credentials for your cloud provider, and click **Start Discovery**.

Configuring credentials creates a row in the discovery table, displaying the discovery status of each credential. The discovery status also displays the number of entities discovered by using the credential.

Optional Configuration

Configure Benchmark Engines

To execute an industry-standard benchmark assessment, you must configure a third party Security Content Automation Protocol (SCAP) certified engine, such as Open SCAP.

If the operating system, entity type, and version combination is not available in Oracle Configuration and Compliance, you can create a new engine configuration.

1. From the menu, select **Engine Configuration**, and click **Add**.

2. Enter the engine parameters, and click **Save**.

   The populated variables are mapped to an engine operating system command. At assessment template runtime, the appropriate engine configuration is selected for the entity-benchmark combination, and the runtime arguments field will be bound and executed. The following example shows you how to configure Open SCAP to run benchmark assessments:

   ```
    $ENGINE_PATH/oscap xccdf eval --
   profile __RULESETID__ --results $RESULTS_PATH/
   __SCANID__.__ENTITYID__.results.xml $SCAP_INPUT_PATH/
   __RULESETFILENAME__
   ```

   The $ENGINE_PATH parameter maps to the absolute path of the SCAP engine, ending with the executable.

   The output location is the $RESULTS_PATH parameter, which maps to the writable directory where the results are written.

   The content location is the $SCAP_INPUT_PATH parameter, which maps to the readable SCAP benchmarks that are executed by the engine.

   If you want a different engine configuration, you can override the default for the same entity type and version engine configuration. For example, a customer can create an override engine configuration if the configuration's default output path resides on a disk partition that has insufficient disk space.

Configure a User-Defined Rule

Oracle Configuration and Compliance can execute user-defined, language-independent custom scripts or standard output, and it can map multiple exit codes on pass or fail compliance violations.

You can create user-defined custom scripts or processes are created in named rule entries. You group these named rule entries within named rulesets. In the menu, select **Library** and click **Rulesets**.

Custom rule or end-user-created custom scripts and processes are executed by the host where an Oracle cloud agent is configured and running. The custom scripts or executables must have the appropriate file system permissions and binary executable bits set so that Oracle Configuration and Compliance can invoke them.

1. From the menu, select **Library**, and click **Rules**.
2. Click **Add** to configure a new rule.
3. Enter a name for the rule.
4. Enter the fully qualified path and executable name.
5. Enter the metadata in accordance with your business objectives.
6. Add the rule to a new or existing ruleset, and click **Save**.

Table 1. Metadata descriptions

The information in this table will describe what each field expects while configuring a user-defined rule.

Name	Description
Description	A description of the rule

Name	Description
Severity	A critical, high, medium, low, informational violation value
Entity Type	The type that the rule will be mapped and executed against
Script Parameters	Optional values that are passed to the script on the command line
Reference URL	An HTTP URL provided for the loose-coupling of additional runbook remediation or metadata
Rationale	Explains the importance of this rule and the consequences of non-compliance
Fixtext	Explains the steps necessary to bring the entity into compliance with this rule
Message	The explanatory message sent to notification services upon the observation of a new violation
Tags	Comma-separated key words used for classification.

Note:

For the optional script parameters, you can specify the following key or value pairs:

`stdin:` Content to be passed to the script's standard input

`args:` A list of command-line arguments to be appended to the script path

Name	Description
Output Spec	Provides the exit code; map multiple exit codes or standard out text to pass or fail compliance violations Process exit codes have the following order of preference. Manually specified values such as the following are evaluated first: • 1 • 100 • 101 • 102 If the exit code is zero and standard output exists, regular expressions are evaluated. If the exit code is not zero and is not a manually specified value, it's mapped to a "rule error" (`nonzeroExitCode`). If the exit code is zero and isn't one of the regular mapped expressions, the rule results in a "rule pass" (`emptyOutput, nonemptyOutput`)
Enabled	Lets you disable the execution of a rule without having to removing it from a ruleset

2

Assess Host and Database Compliance with Industry Standards

Oracle Configuration and Compliance enables you to use Open Vulnerability and Assessment Language (OVAL) industry standards when you run compliance assessments.

Topics:

Users benefit from the automation of industry-standard compliance benchmarks. They also benefit when benchmarks are updated and can be immediately evaluated. Because of this, industry-standard compliance benchmarks assessments play an important part in the compliance function and can stand alone. This chapter covers this standalone configuration business use case. In addition to industry-standard compliance benchmarks assessments, Oracle Configuration and Compliance can execute corporate standards and cloud assessments independently or as part of the same assessment evaluation. On-premises, cloud-only, and hybrid cloud customers benefit because they can enforce all three capabilities within a single policy assessment.

Typical Workflow for Assessing Compliance with Industry Standards

Task	More Information
Add a Secure Socket Shell (SSH) host credential	Define SSH Host Credentials
Add a Oracle Database credential	Define Oracle Database Credentials
Run SCAP assessments with Expanded Privileges	Run SCAP Assessments with Expanded Privileges
Run an assessment with industry-standard benchmarks	Run Assessments with Industry-Standard Benchmarks

Run SCAP Assessments with Expanded Privileges

You can run SCAP Assessments from your terminal using Oracle Configuration and Compliance.

To successfully evaluate all rules in standard benchmarks, SCAP requires root access to run assessments. The following example is for OSCAP, but the same principle can be used for CISCAT or other third party tools.

1. Configure the user that is running the agent with no password sudo access.

   For example, assume the agent was installed as user `oracle`. Make the following changes in /etc/sudoers on every target system that is running the cloud agent.

   > **Note:**
   >
   > You must distribute this configuration file among all hosts that use a privileged sudo execution.

```
...

#
# Disable "ssh hostname sudo <cmd>", because it will show the
password in clear.
#         You have to run "ssh -t hostname sudo <cmd>".
#
Defaults    requiretty

# The agent user emga needs to disable tty
Defaults:emga !requiretty

...

##
## Allow root to run any commands anywhere
root    ALL=(ALL)       ALL

# Allow agent user oracle to run root commands without prompting
for password
oracle    ALL=(ALL)       NOPASSWD:ALL

....
```

2. Modify the PATH property of the relevant Engine Configuration from "`/usr/bin/oscap`" to "`sudo /usr/bin/oscap`".

Run Assessments with Industry-Standard Benchmarks

Oracle Configuration and Compliance can use the command executor to invoke third-party SCAP certified engines such as Open SCAP and consume the resulting Extensible Configuration Checklist Description Format (XCCDF) output.

Assessment templates support mixing and matching cloud resources, industry-standard benchmarks, and custom rules with an associated group of entities.

1. From the menu, select **Assessments**, and click **Templates**.
2. Click **Add**, and enter a name and description for your assessment template.
3. Select the check boxes for the industry-standard benchmark rules that you want to assess.

4. Click **Add**, and select the entities for which you want to apply the selected rulesets.
5. Select a schedule, and click **Save**.

3

Assess Compliance with Your Corporate Standards

The Oracle Configuration and Compliance custom corporate standards provide the ability to extend industry-standard benchmarks and cloud resource evaluations.

Topics:

Custom corporate standards let you to execute any process and map the exit code or standard out message to a compliance rule violation, whether the process passes or fails. You can extend industry-standard benchmarks or cloud resource evaluations with your own standards as part of implementing regulatory requirements. This chapter covers this standalone configuration business use case. In addition to custom corporate standards, Oracle Configuration and Compliance can execute industry-standard benchmarks and cloud assessments independently or as part of the same assessment evaluation. On-premises, cloud-only, and hybrid cloud customers benefit because they can enforce all three capabilities within a single policy assessment.

Typical Workflow for Assessing Compliance with Your Corporate Standards

Task	More Information
Add a Secure Socket Shell (SSH) host credential	Define SSH Host Credentials
Run SCAP assessments with Expanded Privileges	Run SCAP Assessments with Expanded Privileges
Run an assessment with corporate standards	Run Assessments with Corporate Standards

Run SCAP Assessments with Expanded Privileges

You can run SCAP Assessments from your terminal using Oracle Configuration and Compliance.

To successfully evaluate all rules in standard benchmarks, SCAP requires root access to run assessments. The following example is for OSCAP, but the same principle can be used for CISCAT or other third party tools.

1. Configure the user that is running the agent with no password sudo access.

   For example, assume the agent was installed as user `oracle`. Make the following changes in /etc/sudoers on every target system that is running the cloud agent.

> **Note:**
>
> You must distribute this configuration file among all hosts that use a privileged sudo execution.

```
...

#
# Disable "ssh hostname sudo <cmd>", because it will show the
password in clear.
#         You have to run "ssh -t hostname sudo <cmd>".
#
Defaults    requiretty

# The agent user emga needs to disable tty
Defaults:emga !requiretty

...

##
## Allow root to run any commands anywhere
root    ALL=(ALL)       ALL

# Allow agent user oracle to run root commands without prompting
for password
oracle    ALL=(ALL)       NOPASSWD:ALL

....
```

2. Modify the PATH property of the relevant Engine Configuration from "`/usr/bin/oscap`" to "`sudo /usr/bin/oscap`".

Run Assessments with Corporate Standards

The process of running a custom rule assessment is fundamentally the same for executing any assessment template to achieve a compliance business objective. The assessment template supports mixing and matching one or more cloud resources, industry-standard benchmarks, and custom rules with an associated grouping of entities.

1. From the menu, select **Assessment** and click **Templates**.
2. Click **Add** and enter a name and a description for your assessment.
3. Select the check boxes for the custom rulesets that you want to assess.
4. Click **Add** and select the entities for which you want to apply the selected rulesets
5. Select a schedule and click **Save.**

4

Understand Compliance Results

Oracle Configuration and Compliance uses a compliance score to give a numerical measurement to your system based on how compliant it is. This service makes use of alerts, remediations, and reports to give users a course of action.

Topics:

Create an Alert Rule

Using Oracle Configuration and Compliance, you can create rules and select users who get notifications when the desired conditions activate.

1. From the menu, select **Library**, click **Rules**, and click **Add**.
2. Enter a name for the rule.
3. Select whether this rule applies to entity types or to individual entities, and click **Add Condition**.
4. Select **Condition Type**, and click **Rule** or **Rule Set**.
5. Select the **Scope** of this alert rule.
6. Select a **Metric** with the desired **Operator**, **Warning**, and **Critical** values.
7. Click **Save**.
8. Enter the names of the users to be notified when this alert rule activates, and click **Save**.

> **Note:**
>
> You can also notify your channels by adding them to this alert rule.

Prioritize Violations

Assessment results help compliance administrators prioritize compliance violations, create a remediation plan based on business objectives, and validate that those changes have been successfully made.

You can sort the assessment results by:

- Entity Type
- Entity Instance
- Individual Violation

By evaluating the compliance violation details, you can understand compliance violations and plan the optimal remediation. The Compliance Service Assessment Results Detail page provides a scoped compliance posture snapshot. You can view the on-demand or reoccurring Assessment Template execution results scoped to a set of entities.

1. From the menu, select **Assessments**, then click **Runs**.
2. Click on a **Assessment Run ID**.
3. Select a severity such as Critical or High.
4. Click on the **Violation Name** to display the **Violations Details** page and plan your remediation.

Plan Remediations

Planning remediations will give you a clear vision on how to take care of compliance violations.

You can write and execute an automated remediation script or manually remediate the violation. Rerun your assessment template, validate successful remediation of the violation, and then verify the remaining violations.

You can find the following list located in the Compliance Violation Details Panel.

1. From the Summary page, click the **Violations** tab.
2. Click the **Violation Name**.

- Rule Description - A description of the rule.
- Entity - The host, database, or middleware target that the rule was run against.
- Rule-Set Name - representing the typed benchmark that the rule belonged to and produce the violation.
- Rationale - Explains the importance of this rule and consequences of non-compliance.
- Remedy - Explains the steps necessary to bring the entity into compliance with regard to this rule.

Upload SCAP Results

Upload SCAP results from OpenSCAP and other SCAP engines directly to Oracle Configuration and Compliance .

1. From the Oracle Configuration and Compliance landing page, click the **Upload** button.
2. Enter a **Upload Name**.
3. Select the **Entities**.
4. Upload the **Result File**.

5. Click **Upload**.

Results should be for a valid and licensed entity for an existing rule-set. Results will be available shortly after upload.

Generate Assessment Report

Generate a complete, self-contained HTML report for any historic assessment using Oracle Configuration and Compliance.

1. From the Oracle Configuration and Compliance landing page, select **Results**, then click **History**.
2. Select an **Entity**.
3. Select a **Rule-Set**.
4. Click a **Data Point** from the Stack Bar graph.
5. Click **Report**.

The Assessment Report HTML file will be generated.

A

Agent Assessment Error Messages

Information related to the issue is displayed within the brackets.

Table A-1 Agent DB Assessments Errors

Error Message / Error Code	Solution
Make sure the database credentials are correct. {} (6230)	See Define Oracle Database Credentials for more information on how to define and add Oracle Database credentials.
Check the SID to make sure it is correct. {} (6231)	See Entities Attributes and Properties for more information on how to find the instance name (SID) of your Oracle Database.
Check the database host/port configuration to make sure it is correct. {} (6232)	See Entities Attributes and Properties for more information on how to find the host and port information of your Oracle Database.
Check that the database user has proper grant privileges for the tables. {} (6233)	See Define Oracle Database Credentials for more information on how to grant the correct database privileges.
Check that the database user has sufficient privileges to run custom rule checks. {} (6236)	See Define Oracle Database Credentials for more information on how to create a new Oracle Database Credential and grant the correct database privileges for custom rule sets.

Table A-2 General Agent Assessment Issues

Error Message / Error Code	Solution
Check the engine configuration path exists on the agent. {} (6260)	See Configure Benchmark Engines to edit the engine's parameters.
Agent returned no result data. {} (6235)	Make sure the assessment is running with the correct entities.
The custom rule returned no output. {} (6251)	Make sure the assessment is running with the correct entities and the custom rule is not empty.
Corrupt data returned by the agent. {} (6252)	Reinstall the agent.
Result exceeded the maximum result size. {} (6253)	The number that appears indicates the file size in MB that was truncated from the output.

Table A-2 (Cont.) General Agent Assessment Issues

Error Message / Error Code	Solution
Agent was unable to execute the assessment. Check agent configuration. {} (6254)	Occurs if Oracle Configuration and Compliance was unable to execute the assessment due to a configuration issue. e.g. Failure to specify wallet credentials, incorrect wallet credentials. Specific reason message is propagated from the agent framework: e.g. Agent was unable to execute the assessment. The credential named `emcosComplianceCred` for the omc_host_linux.example.oracle.com entity does not exist.
Required agent files are missing. {} (6255)	Reinstall the agent.
Check that the agent user has executable permissions. {} (6256)	Make sure the user has expanded privileges.

Table A-3 SCAP Assessment Errors

Error Message	Solution
The SCAP benchmark file version is not present on the agent OS. {} (6257)	Run the assessment with the correct SCAP benchmark.
There was a problem executing the SCAP operation on the agent. Try running the command manually. {} (6258)	Try running the command manually from the command line where the agent is installed.
The SCAP benchmark version on the agent may not match the rule set version. {} (6259)	See Appendix: Rule Sets for the list of supported rule sets by Oracle Configuration and Compliance.

B
Rule Sets

Here is a list with descriptions of every Rule Set you can find in Oracle Configuration and Compliance.

Linux

Rule Set	Description
Guide to the Secure Configuration of Oracle Linux 7-Criminal Justice Information Services (CJIS) Security Policy	This profile is derived from FBI's CJIS v5.4 Security Policy. A copy of this policy can be found at the CJIS Security Policy Resource Center: https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center.
Guide to the Secure Configuration of Oracle Linux 7-United States Government Configuration Baseline (USGCB / STIG)	This profile is developed in partnership with the U.S. National Institute of Standards and Technology (NIST), U.S. Department of Defense, the National Security Agency, and Red Hat. The USGCB is intended to be the core set of security related configuration settings by which all federal agencies should comply. This baseline implements configuration requirements from the following documents: - Committee on National Security Systems Instruction No. 1253 (CNSSI 1253) - NIST Controlled Unclassified Information (NIST 800-171) - NIST 800-53 control selections for MODERATE impact systems (NIST 800-53) - U.S. Government Configuration Baseline (USGCB) - NIAP Protection Profile for General Purpose Operating Systems v4.0 (OSPP v4.0) - DISA Operating System Security Requirements Guide (OS SRG) For any differing configuration requirements, e.g. password lengths, the stricter security setting was chosen. Security Requirement Traceability Guides (RTMs) and sample System Security Configuration Guides are provided via the scap-security-guide-docs package. This profile reflects U.S. Government consensus content and is developed through the OpenSCAP/SCAP Security Guide initiative, championed by the National Security Agency. Except for differences in formatting to accommodate publishing processes, this profile mirrors OpenSCAP/SCAP Security Guide content as minor divergences, such as bugfixes, work through the consensus process.
Guide to the Secure Configuration of Red Hat Enterprise Linux 6-Red Hat Corporate Profile for Certified Cloud Providers (RH CCP)	This is a SCAP profile for Red Hat Certified Cloud Providers.

Rule Set	Description
Guide to the Secure Configuration of Oracle Linux 7-DISA STIG for Oracle Linux 7	This is a profile for STIG for Oracle Linux 7.

Rule Set (0.9)	Description
Guide to the Secure Configuration of Red Hat Enterprise Linux 6-C2S for Red Hat Enterprise Linux 6 [v0.9]	This profile demonstrates compliance against the U.S. Government Commercial Cloud Services (C2S) baseline. This baseline was inspired by the Center for Internet Security (CIS) Red Hat Enterprise Linux 6 Benchmark, v1.2.0 - 06-25-2013. For the SCAP Security Guide project to remain in compliance with CIS' terms and conditions, specifically Restrictions(8), note there is no representation or claim that the C2S profile will ensure a system is in compliance or consistency with the CIS baseline.
Guide to the Secure Configuration of Red Hat Enterprise Linux 6-CSCF RHEL6 MLS Core Baseline [v0.9]	This profile reflects the Centralized Super Computing Facility (CSCF) baseline for Red Hat Enterprise Linux 6. This baseline has received government ATO through the ICD 503 process, utilizing the CNSSI 1253 cross domain overlay. This profile should be considered in active development. Additional tailoring will be needed, such as the creation of RBAC roles for production deployment.
Guide to the Secure Configuration of Red Hat Enterprise Linux 6-Common Profile for General-Purpose Systems Server Baseline [v0.9]	This profile contains items common to general-purpose desktop and server installations.This profile is for RHEL 6 acting as a server.
Guide to the Secure Configuration of Red Hat Enterprise Linux 6-United States Government Configuration Baseline (USGCB) [v0.9]	This profile is a working draft for a USGCB submission against RHEL6 Server.
Guide to the Secure Configuration of Red Hat Enterprise Linux 6-Common Profile for General-Purpose Systems [v0.9]	This profile contains items common to general-purpose desktop and server installations.
Guide to the Secure Configuration of Red Hat Enterprise Linux 6-Example Server Profile [v0.9]	This profile is an example of a customized server profile.

Rule Set (0.9)	Description
Guide to the Secure Configuration of Red Hat Enterprise Linux 6-Common Profile for General-Purpose SystemsUpstream STIG for RHEL 6 Server [v0.9]	This profile contains items common to general-purpose desktop and server installations.This profile is developed under the DoD consensus model and DISA FSO Vendor STIG process, serving as the upstream development environment for the Red Hat Enterprise Linux 6 Server STIG. As a result of the upstream/downstream relationship between the SCAP Security Guide project and the official DISA FSO STIG baseline, users should expect variance between SSG and DISA FSO content. For official DISA FSO STIG content, refer to http://iase.disa.mil/stigs/os/unix/red_hat.html. While this profile is packaged by Red Hat as part of the SCAP Security Guide package, please note that commercial support of this SCAP content is NOT available. This profile is provided as example SCAP content with no endorsement for suitability or production readiness. Support for this profile is provided by the upstream SCAP Security Guide community on a best-effort basis. The upstream project homepage is https://fedorahosted.org/scap-security-guide/. https://fedorahosted.org/scap-security-guide/.

Rule Set (1.28)	Description
Guide to the Secure Configuration of Oracle Linux 6-CNSSI 1253 Low/Low/Low Control Baseline for Oracle Linux 6 [v0.1.28]	This profile follows the Committee on National Security Systems Instruction (CNSSI) No. 1253, "Security Categorization and Control Selection for National Security Systems" on security controls to meet low confidentiality, low integrity, and low assurance."
Guide to the Secure Configuration of Oracle Linux 6-PCI-DSS v3 Control Baseline for Oracle Linux 6 [v0.1.28]	This is a *draft* profile for PCI-DSS v3.
Guide to the Secure Configuration of Oracle Linux 6-C2S for Oracle Linux 6 [v0.1.28]	This profile demonstrates compliance against the U.S. Government Commercial Cloud Services (C2S) baseline. This baseline was inspired by the Center for Internet Security (CIS) Oracle Linux 6 Benchmark, v1.2.0 - 06-25-2013. For the SCAP Security Guide project to remain in compliance with CIS' terms and conditions, specifically Restrictions(8), note there is no representation or claim that the C2S profile will ensure a system is in compliance or consistency with the CIS baseline.

Rule Set (1.28)	Description
Guide to the Secure Configuration of Oracle Linux 6-CSCF OL6 MLS Core Baseline [v0.1.28]	This profile reflects the Centralized Super Computing Facility (CSCF) baseline for Oracle Linux 6. This baseline has received government ATO through the ICD 503 process, utilizing the CNSSI 1253 cross domain overlay. This profile should be considered in active development. Additional tailoring will be needed, such as the creation of RBAC roles for production deployment.
Guide to the Secure Configuration of Oracle Linux 6-Oracle Profile for Cloud Providers [v0.1.28]	This is a SCAP profile for Cloud Providers.
Guide to the Secure Configuration of Oracle Linux 6-United States Government Configuration Baseline (USGCB) [v0.1.28]	This profile is a working draft for a USGCB submission against RHEL6 Server.
Guide to the Secure Configuration of Oracle Linux 6-Upstream STIG for Oracle Linux 6 Server [v0.1.28]	This is a *draft* profile for STIG. As a result of the upstream/downstream relationship between the SCAP Security Guide project and the official DISA FSO STIG baseline, users should expect variance between SSG and DISA FSO content. For official DISA FSO STIG content, refer to http://iase.disa.mil/stigs/os/unix-linux/Pages/oracle-linux.aspx. While this profile is packaged by Oracle as part of the SCAP Security Guide package, please note that commercial support of this SCAP content is NOT available. This profile is provided as example SCAP content with no endorsement for suitability or production readiness. Support for this profile is provided by the upstream SCAP Security Guide community on a best-effort basis. The upstream project homepage is https://fedorahosted.org/scap-security-guide/.
Guide to the Secure Configuration of Oracle Linux 6-Server Baseline [v0.1.28]	This profile is for Oracle Linux 6 acting as a server.
Guide to the Secure Configuration of Oracle Linux 6-Common Profile for General-Purpose Systems [v0.1.28]	This profile contains items common to general-purpose desktop and server installations.
Guide to the Secure Configuration of Oracle Linux 6-Example Server Profile [v0.1.28]	This profile is an example of a customized server profile.
Guide to the Secure Configuration of Oracle Linux 6-Standard System Security Profile [v0.1.28]	This profile contains rules to ensure standard security base of Oracle Linux 6 system. Regardless of your system's workload all of these checks should pass.

Rule Set (1.36)	Description
Guide to the Secure Configuration of Oracle Linux 7-Oracle Profile for Cloud Providers [v0.1.36]	This is a SCAP profile for Cloud Providers.

Rule Set (1.36)	Description
Guide to the Secure Configuration of Oracle Linux 7-PCI-DSS v3 Control Baseline for Oracle Linux 7 [v0.1.36]	This is a profile for PCI-DSS v3.
Guide to the Secure Configuration of Oracle Linux 7-Standard System Security Profile [v0.1.36]	This profile contains rules to ensure standard security baseline of Oracle Linux 7 system. Regardless of your system's workload all of these checks should pass.
Guide to the Secure Configuration of Oracle Linux 7-Unclassified Information in Non-federal Information Systems and Organizations (NIST 800-171) [v0.1.36]	From NIST 800-171, Section 2.2: Security requirements for protecting the confidentiality of CUI in nonfederal information systems and organizations have a well-defined structure that consists of: (i) a basic security requirements section; (ii) a derived security requirements section. The basic security requirements are obtained from FIPS Publication 200, which provides the high-level and fundamental security requirements for federal information and information systems. The derived security requirements, which supplement the basic security requirements, are taken from the security controls in NIST Special Publication 800-53. This profile configures Oracle Linux 7 to the NIST Special Publication 800-53 controls identified for securing Controlled Unclassified Information (CUI).
Guide to the Secure Configuration of Oracle Linux 7-Common Profile for General-Purpose Systems [v0.1.36]	This profile contains items common to general-purpose desktop and server installations.
Guide to the Secure Configuration of Oracle Linux 7-Standard Docker Host Security Profile [v0.1.36]	This profile contains rules to ensure standard security baseline of Oracle Linux 7 system running the docker daemon. This discussion is currently being held on open-scap-list@redhat.com and scap-security-guide@lists.fedorahosted.org.

Rule Set (1.40)	Description
Guide to the Secure Configuration of Oracle Linux 7-Unclassified Information in Non-federal Information Systems and Organizations (NIST 800-171)	This profile configures Oracle Linux 7 to the NIST Special Publication 800-53 controls identified for securing Controlled Unclassified Information (CUI).
Guide to the Secure Configuration of Oracle Linux 7-OSPP DRAFT - Protection Profile for General Purpose Operating Systems v. 4.2	This profile reflects mandatory configuration controls identified in the NIAP Configuration Annex to the Protection Profile for General Purpose Operating Systems (Protection Profile Version 4.2)
Guide to the Secure Configuration of Oracle Linux 7-Criminal Justice Information Services (CJIS) Security Policy	This profile is derived from FBI's CJIS v5.4 Security Policy
Guide to the Secure Configuration of Oracle Linux 7-Standard System Security Profile for Oracle Linux 7	This profile contains rules to ensure standard security baseline of a Oracle Linux 7 system.

Rule Set (1.40)	Description
Guide to the Secure Configuration of Oracle Linux 7-DISA STIG for Oracle Linux 7	This is a draft profile for STIG for Oracle Linux 7.
Guide to the Secure Configuration of Oracle Linux 7-PCI-DSS v3 Control Baseline for Oracle Linux 7	This is a draft profile for PCI-DSS v3.
Guide to the Secure Configuration of Oracle Linux 7-Oracle Profile for Cloud Providers	This is a draft Oracle SCAP profile for Cloud Providers.
Guide to the Secure Configuration of Oracle Linux 7-United States Government Configuration Baseline - DRAFT	This compliance profile reflects the core set of security related configuration settings for deployment of Oracle Linux 7.x into U.S. Defense, Intelligence, and Civilian agencies. Development partners and sponsors include the U.S. National Institute of Standards and Technology (NIST), U.S. Department of Defense, the National Security Agency, and Red Hat.
Guide to the Secure Configuration of Oracle Linux 7-Health Insurance Portability and Accountability Act (HIPAA)	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.

Cloud

Rule Set	Description
Best Practices for Oracle Java Cloud Services [v1]	Compliance Rules to check the configuration of Java Cloud Service Instances
Best Practices for Oracle Cloud Infrastructure - Compute Classic Instances [v1]	Compliance Rules to check the configuration of Compute Instances
OMC Compliance Rules for AWS Customer Gateways [v1]	Compliance Rules to check the configuration of Customer Gateways
OMC Compliance Rules for AWS Elastic IP Addresses [v1]	Compliance Rules to check the configuration of Elastic IP Addresses
OMC Compliance Rules for AWS VPCs [v1]	Compliance Rules to check the configuration of VPCs
OMC Compliance Rules for AWS Cloud Trail [v1]	Compliance Rules to check Cloud Trail Configuration
OMC Compliance Rules for AWS Internet Gateways [v1]	Compliance Rules to check the configuration of Internet Gateways
OMC Compliance Rules for AWS Elastic Block Store [v1]	Compliance Rules to check the configuration of Elastic Block Stores
OMC Compliance Rules for AWS VPN Gateways [v1]	Compliance Rules to check the configuration of VPN Gateways
OMC Compliance Rules for AWS EC2 Instances [v1]	Compliance Rules to check the configuration of EC2 Instances
OMC Compliance Rules for AWS VPN Connections [v1]	Compliance Rules to check the configuration of VPN Connections
OMC Compliance Rules for AWS Security Groups [v1]	Compliance Rules to check the configuration of Security Groups

Rule Set	Description
OMC Compliance Rules for AWS Route Tables [v1]	Compliance Rules to check the configuration of Route Tables
OMC Compliance Rules for AWS Subnets [v1]	Compliance Rules to check the configuration of Subnets

Oracle Database

Rule Set	Description
Oracle Database 12c Single Instance Database STIG Configuration	This profile contains a STIG for a single instance Oracle Database 12c.
Basic Security Configuration For Oracle Database [v1]	Ensures adherence with basic best-practice security configuration settings that help protect against database-related threats and attacks, providing a more secure operating environment for Oracle Database. Associate this compliance standard with a database and enable the collections by applying the Oracle certified monitoring template Oracle Certified-Enable Database Security Configuration Metrics to evaluate the database compliance.
Basic Security Configuration For Oracle Database 19c	Ensures adherence with basic best-practice security configuration settings that help protect against database-related threats and attacks, providing a more secure operating environment for Oracle Database. Associate this compliance standard with a database and enable the collections by applying the Oracle certified monitoring template Oracle Certified-Enable Database Security Configuration Metrics to evaluate the database compliance.
Best Practices for Oracle Database Cloud Services [v1]	Compliance Rules to check the configuration of Database Service Instances
CIS Benchmark for Oracle Database 11g v2.2.0, Level 1 RDBMS	This profile contains the Center for Internet Security Benchmark for Oracle Database 11g.
CIS Benchmark for Oracle Database 12c v2.0.0, Level 1 RDBMS using Unified Auditing	This profile contains the Center for Internet Security Benchmark for Oracle Database 12g using Unified Auditing.
Oracle Database Security Assessment Tool [v2.1]	This profile contains a security benchmark for Oracle Database Security Assessment Tool (DBSAT).

Oracle E-Business Suite

Rule Set	Description
Oracle E-Business Suite with Oracle Database 12.1 Best Practices [v1]	E-Business Suite security and best practices checks based on MOS Note 403537.1

MySQL Enterprise

Rule Set	Description
Basic Security Configuration for MySQL Enterprise Edition 5.7	**Assess the MySQL database against secure configuration setting recommended by Center for Internet Security.**