Enterprise Manager 12c Compliance Management
Part 3

Custom Compliance Example using SQL Configuration Extension
(Example using Department of Defense STIG for Oracle DB)
Example Overview
SQL Based Configuration Extension and Check

- This example will use a real check from the Department of Defense – Oracle Database 11g STIG (Secure Technical Implementation Guide).
- STIG provides the SQL to run which we will use to build a custom compliance rule against.
- We will use STIG Check DG0008-ORACLE11
  - Check Description: Application objects should be owned by accounts authorized for ownership.
  - Check Details: Check all dba_objects and ensure the owner is an approved application user.
Oracle DB 11g STIG Check DG0008-ORACLE11

Explanation of check:

Database object ownership implies full privileges to the owned object including the privilege to create a table. If the owner is uncontrolled then a table can be created on the database.

Explanation of check:

Application objects are owned by accounts not authorized for ownership.

Details:

- Review the object owner accounts as generated. Confirm the accounts are documented.
- Document the object owner accounts to ensure ownership of objects is tracked.
- Execute the actual SQL query to check for violation.

Check:

- Actual SQL Query to check for violation is given in the document.
Custom Compliance Methodology

Follow the flow for each custom validation.

- Compliance Rule Exists?
  - No → Required Data Collected?
  - No → Extend Target Using Configuration Extension
  - Yes → Create Custom Compliance Rule
- Yes → Add Compliance Rule to Compliance Standard
Follow Custom Compliance Methodology

1. Following the standard methodology we first check if there is an Oracle provided rule that matches our needs.
   a) Answer = No

2. Next we check if the default configuration data of the DB contained the data we need to validate.
   a) Answer = No

3. So we must build a configuration extension first, deploy it to the targets and then create a custom rule using the newly collected data. Be sure to follow the Custom Configuration Setup steps later in this presentation to setup monitoring credentials BEFORE continuing (only if you are using EM Version <12.1.0.3)
Guidelines for Custom SQL based Configuration Extension used in Compliance

- Perform the actual check for violations ON the agent and only return results which ARE ONLY violations.
- Only return 1 column. If you want to see more than 1 item then concatenate them in the collection output.
  - For example “select username||’ :’||profile from …”
Start at the Configuration Extensions Page

Go to Enterprise->Configuration->Configuration Extensions
Create new Configuration Extension
Click Create
Enter basic Configuration Extension information.

Enter Name. Select Target Type, Sample Target and Creds. Click Add.

Select Monitoring Database Credential which is the default monitoring credential using dbsnmp user. If you are using <12.1.0.3 select the Custom monitoring credentials you created following the appendix of this presentation.
Populate the SQL details
Enter SQL, Alias and select parser. Click Preview

Copied verbatim from STIG document as only 1 column returned and only violations.

Alias will be important later when creating compliance rule!
Ensure Results returned properly
Click DG0008 to see results. Click OK.

Select Alias to see results.

1 Attribute with 1 Value
Save Configuration Extension

Click Save
Deploy to Targets
Click Manage Deployments
Select Targets to deploy
Click Add
Chose only targets with Credentials configured
Select 1 or more targets. Click Select
Click Save
Wait for deployment
Click Refresh until Successfully Deployed
Check configuration of one of the targets
Go to the target’s Last Collected page to see results.
View parsed configuration

Select Alias, verify results
We are now ready to create a custom compliance rule against the Configuration Extension.
Start at the Compliance Library
Go to Compliance->Library
Create a new Rule
Click Create on Compliance Standard Rules tab
Create a repository rule
Select Repository Rule and Click Continue
Add rule overview details
Enter basic rule information. Click Next.

Taken direct from STIG document.
Use to SQL Modeler!

Let EM help build the query. Click Model Query
Use the Target Model
Click Add Properties

<table>
<thead>
<tr>
<th>New Search Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target Type: Database Instance</td>
</tr>
</tbody>
</table>

## Commonly Used Search Criteria

### Database Instance
- **Search**
- **Reset**

---

The following table displays the valid licensed target’s configuration search results that satisfies the search criteria defined above.

<table>
<thead>
<tr>
<th>View</th>
<th>Export</th>
<th>Print</th>
<th>Detach</th>
</tr>
</thead>
</table>

No data to display
Select the Parsed data.
Select all four Parsed Properties. Click OK.
Notice the Alias specified in the Custom Configuration is the Data Source Name. We will use it to make sure we only get results of this single query.

The Container and Attribute do not contain useful data for the violation context. We will choose not to display them therefore.
Narrow the results

Narrow results using Data Source. Undisplay non-distinguishing columns. Search to verify. Then click OK
Add messages text

Add Compliant and Non-Compliant Messages. Click Next.

This hard coded text column is added to ensure you will have at least 1 non-key column which is required for compliance rules. We will hide it in next step.
Enter conditions

Select SQL Condition. Enter 1=1. Click Next.

Choose Value as Key column

Choose not to display info column

Select SQL Condition

Enter 1=1 which means ALL results are violations.
Choose a target

Select target selector:
Select target with custom configuration

Select Sample target and click Select.
Run Test

Click Run Test

Select the target against which you want to test the rule.

Target Name: testdb1

TIP: Click the icon to select a target from the list of available targets.
Review and confirm violations

Review violations. Click Next.

Create Rule: Repository Rule: Test

Select the target against which you want to test the rule.

Target Name: testdb1

Compliance Score: 76%

Rule Violations

<table>
<thead>
<tr>
<th>Target Name</th>
<th>VALUE</th>
</tr>
</thead>
<tbody>
<tr>
<td>testdb1</td>
<td>ORACLE_OCM</td>
</tr>
<tr>
<td>testdb1</td>
<td>FLOWS_FILES</td>
</tr>
<tr>
<td>testdb1</td>
<td>SCOTT</td>
</tr>
<tr>
<td>testdb1</td>
<td>OWBSYS_AUDIT</td>
</tr>
<tr>
<td>testdb1</td>
<td>ORDDATA</td>
</tr>
<tr>
<td>testdb1</td>
<td>APEX_030200</td>
</tr>
<tr>
<td>testdb1</td>
<td>OWBSYS</td>
</tr>
<tr>
<td>testdb1</td>
<td>APPQOSSYS</td>
</tr>
</tbody>
</table>
Finish rule creation

Review. Click Finish.
Confirm creation
Rule Created.

<table>
<thead>
<tr>
<th>Rule</th>
<th>Applicable To</th>
<th>Description</th>
<th>Rule Type</th>
<th>Compliance Rule State</th>
<th>Keywords</th>
<th>Author</th>
<th>Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>STIG DG0008</td>
<td>Database Instance</td>
<td>Database object ownership implies full privileges to the owned object including the privilege to assign access to the owned objects to other subjects. Unmanaged or uncontrolled ownership of objects can lead to unauthorized object grants and alterations.</td>
<td>Repository Rule</td>
<td>Production</td>
<td></td>
<td>DWW/OLF</td>
<td>Critical</td>
</tr>
</tbody>
</table>
Add a new Compliance standard
Click Create on Compliance Standard tab.
Enter basic information

Enter Compliance Details. Click Continue.
Enter Standard details
Enter Descriptions and select Production State.

Select a Compliance Standard node to see its details. Right click the node to modify the hierarchy.

STIG Example Standard (Compliance Standard)

- Name: STIG Example Standard
- Applicable To: Database Instance

Target Property Filter
- Author: DWOLF

Description: Sample Sap Compliance Standard

Compliance Standards State: Production

Reference URL:  

Version: 1

Keywords:
- Keyword
  No data to display.
Add rule to standard
Right Click Standard Name. Select Add Rules...
Add Custom Rule
Search for Rule. Select rule. Click OK.
Change Importance
Optionally, change Importance. Click Save.

Select a Compliance Standard node to see its details. Right click the node to modify the hierarchy.

Properties

STIG DG0008 (Compliance Standard Rule)

Name: STIG DG0008
Description: Database object ownership implies full privileges to the owned object including the privilege to assign access to the owned objects to other subjects. Unmanaged or uncontrolled ownership of objects can lead to unauthorized object grants and alterations.

Compliance: Production
Rule State: [ ]
Importance: High [ ]
Associate Targets
Select Compliance Standard. Click Associate Targets.
Add targets

Click Add
Select targets with Custom Configuration

Select Target. Click Select.
Confirm selection and continue
Click OK.

![Compliance Standard Target Association](image)

**Compliance Standard Target Association**

**Target Association for Compliance Standard: STIG Example Standard**

This table lists the targets that are associated with the compliance standard selected in the Compliance Standard Library.

<table>
<thead>
<tr>
<th>View</th>
<th>Add</th>
<th>Remove</th>
<th>Edit</th>
<th>Enable</th>
<th>Disable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target Name</td>
<td>Target Type</td>
<td>Evaluation Status</td>
<td>Customized</td>
<td>Transfer Status</td>
<td>Association Time Stamp</td>
</tr>
<tr>
<td>testdb1</td>
<td>Database Instance</td>
<td>Enabled</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Confirm message
Click YES
View Results

View Results. Go to Compliance->Results
Find Standard and view details
Select Standard. Click Show Details.
Review standard summary page

View Summary

Compliance Standard Result Detail

STIG Example Standard (Compliance Standard)

Summary  Trend Overview  Violations

Target Scorecard  Rule Evaluations

<table>
<thead>
<tr>
<th>Target Name</th>
<th>Required Data Available</th>
<th>Violations</th>
<th>Score (%)</th>
<th>Last Evaluation Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>testdb1</td>
<td>Yes</td>
<td>8</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
View Custom rule details
Select Rule. Select Violation Events Tab. Select a Violation to see details.
Note violation details

Expanded view of Details.

Important information like when violation detected, Notifications sent and Incident ID.

Non-Compliant message from Rule

We could have entered a recommendation on how to address the violation in the rule which would show here.

Violation details as will be seen in notifications and event.
Example
End
Custom Compliance Setup when using Custom Configuration Collections
Setup for Compliance leveraging Custom Collections

- Custom Configuration use Monitoring Credentials
  - File Based
    - CAN use agent credentials if files accessible to user
    - If not, you must create custom monitoring credentials for target type
  - SQL Based
    - Default DB Monitoring Credentials not available in 12.1.0.1 or 12.1.0.2. 12.1.0.3 allows its use.
    - Setup New SQL Monitoring Credentials (for 12.1.0.1, 12.0.1.2)
  - Command
    - Cannot use Agent credentials
    - Setup New Host Monitoring Credentials
SQL Based Custom Configuration Setup
SQL Based Custom Configuration Setup
Use Custom Configuration to Create Monitoring Credentials
Enter any text for a name, select Database Instance target type, and click Create.
SQL Based Custom Configuration Setup

Create Monitoring Credential Set

Enter a name for the Credential Set

Name: Custom_DB_Creds
Note: A Monitoring Credential of this name is now associated with every target of this type. We must now set the credential values for at least 1 sample target so we can use it during test.
Choose the Target Type and select Manage Credentials
SQL Based Custom Configuration Setup

Select a sample target and new credentials set and click “Set Credentials”
SQL Based Custom Configuration Setup

Set Monitoring Credential Values for the target

Enter username and password then click Test and Save.

NOTE: Only NORMAL DB Role is currently supported.
SQL Based Custom Configuration Setup

Ensure Credential Test Successful

We can now create a SQL Configuration Extension using this Monitoring Credentials set and sample target.