Custom Compliance using Default Configuration data
Example Overview

Building a Custom Compliance Rule using Default Configuration

- This example will show how to build a custom compliance rule (check) using configuration data collected by the database target by default.

- Sample check overview:
  - Ensure the Default Profile is used for only approved accounts.

- Sample check details:
  - No database users should have ‘DEFAULT’ profile except the following IDs (SYS, DBSNMP, ORDSYS, OUTLN, SYSTEM, MDSYS, WMSYS, XDB, DBA, ORDPLUGINS, DIP, TSMSYS, ANONYMOUS)

- Example of query DBA would use to check for violations:
  - Select username from dba_users where profile= 'DEFAULT' and username not in ('SYS', 'CTXSYS', 'DBSNMP', 'ORDSYS', 'OUTLN', 'SYSTEM', 'MDSYS', 'WMSYS', 'XDB', 'DBA', 'ORDPLUGINS', 'DIP', 'TSMSYS', 'ANONYMOUS')

We will follow the Custom Compliance Methodology to build our custom validation.
Custom Compliance Methodology

Follow the flow for each custom validation.

Compliance Rule Exists? Yes
  No

Required Data Collected? Yes
  No

Extend Target Using Configuration Extension

Create Custom Compliance Rule

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 contains the data we need to validate.
Custom Compliance Methodology – Step 2

Check if configuration in default collection.

Yes, the default collection has the needed data.
Follow Custom Compliance Methodology

Since Enterprise Manager already collects the data needed to be validated, we will:

1. Build a custom rule based on default data
2. Add the custom rule to a compliance standard.
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.
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</td>
</tr>
<tr>
<td>Database Instance</td>
</tr>
<tr>
<td>Commonly Used Search Criteria</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Database Instance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search</td>
</tr>
<tr>
<td>Reset</td>
</tr>
</tbody>
</table>

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

No data to display
Select the configuration data.
Choose User Name and Profile. Click Next.
Narrow to only Default Profile

Enter DEFAULT for Profile filter.
View the results
Click Search. Verify Results.
Return to rule wizard.
Click OK.
Do not remove!
Enter Compliance and Non-Compliant Message. Click Next.

Adding an Alias to a column allows the parameter to be used in the compliant/non-compliant message when surrounded by %.
Define violation conditions
Select Key cols, SQL Condition and enter violation condition. Click Next

Choose the combination of columns that uniquely identify a violation. You must have at least 1 non-key value. (which is why INFO added in query generator. Leave it unchecked.)

Pre-Pend: to Column Name to use in SQL condition. Here we add the user exceptions from the original rule requirement.
Test the rule

Use target selector to choose sample. Click Run Test.
Validate Test

Review violations. Click Next.

Create Rule: Repository Rule : Test

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

Target Name: endb

Run Test

Compliance Score: 81%

Rule Violations

<table>
<thead>
<tr>
<th>Target Name</th>
<th>INFO</th>
<th>PROFILE</th>
<th>USERNAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>endb</td>
<td>attrvalue</td>
<td>DEFAULT</td>
<td>XS$NULL</td>
</tr>
<tr>
<td>endb</td>
<td>attrvalue</td>
<td>DEFAULT</td>
<td>ORACLE_OCM</td>
</tr>
<tr>
<td>endb</td>
<td>attrvalue</td>
<td>DEFAULT</td>
<td>APPQOSSYS</td>
</tr>
<tr>
<td>endb</td>
<td>attrvalue</td>
<td>DEFAULT</td>
<td>EXPSYS</td>
</tr>
<tr>
<td>endb</td>
<td>attrvalue</td>
<td>DEFAULT</td>
<td>DWYOLF</td>
</tr>
<tr>
<td>endb</td>
<td>attrvalue</td>
<td>DEFAULT</td>
<td>HARSJINI</td>
</tr>
</tbody>
</table>
Final Review.

Review summary. Click Finish.
Create a New Compliance Standard

Click Create…
Create Compliance Standard
Enter Compliance Standard Basic information. Click Continue.
Add Custom Rule

Change State to Production. Select Add Rules…

Right Click on Compliance Standard name to get to this menu.
Search and add custom rule.
Use Search to find rule. Select rule. Click OK.
Set Rule Properties.
Change Importance (Optional) and click Save
Associate target to Standard
Select Standard. Click Associate Targets…

Use Search to find Standard
Add Target.
Click Add
Choose targets.
Select 1 or more targets. Click Select

Select 1 or more Targets to associate to Standard
Confirm Selection

Review Targets and Click ok.
Confirm Association

Click Yes
Confirm Association

Ensure Association Count correct.
View Results
Enterprise->Compliance->Results. Select Standard. Click Show Details.
Review Standard Summary Results

Compliance Standard Result Detail

CustomComplianceStandard1 (Compliance Standard)

Summary  Trend Overview  Violations

Target Scorecard  Rule Evaluations

Targets By Severity  Rule Evaluations

Compliant  Critical  Warning  Minor

Result By Target  Result By Compliance Standard Rule

<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>Default</td>
<td>Yes</td>
<td>6 0 0</td>
<td>14</td>
<td>11/11/2012</td>
</tr>
</tbody>
</table>

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.
Review Rule Results

Select Rule in tree.
Review violation
Select Violation Events tab
Custom Rule using default Configuration
Select Violation Event to review Details

Notice the Username substitution in message.

Non-Compliant message from Rule

Violation details as will be seen in notifications and event.

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