Agenda

- Compliance Overview
- Understanding Compliance Results
- Understanding Compliance Score Calculation
- Compliance Related Roles and Privileges
- Operational Aspects of Compliance
- Custom Compliance Methodology
Compliance Framework

Solution Overview

- **Auditing**
  - Automatically determine if targets have valid configuration settings and whether they are exposed to configuration-related vulnerabilities.
  - Real-time monitoring of a target's files, processes, and users to let users know where configuration changes or unauthorized actions are happening.

- **Remediation**
  - Notification on deviation from standard or change event.
  - Advises how to change configurations to bring targets and systems into compliance with respect to best practices.

- **Oracle Provided Content**
  - Reusable and customizable compliance standards that map to Oracle best practices and recommendations.
Reusable Compliance Hierarchy

- Compliance Framework
  - Group Compliance Standards different Target Types
- Compliance Standard
  - Group of Compliance Rules
  - Specific to Single Target Type
- Compliance Rule
  - Discreet Check or Test
  - Specific to Target Type
- Real Time Facet
  - Group of related entities
  - Files, Processes or Users
Maintain Compliance – Three Options

1. Repository Compliance Standard
   - Evaluated against repository data
   - Validated when target configuration changes
   - Query Builder browser to aid in rule creation

2. Real-time Compliance Standard
   - Detection of real time activities including
     - File Actions (Read, Write, Perm Change, etc)
     - Process Actions (Start, Stop)
     - Schema Actions (Select, Update)
   - Detection of “unauthorized” changes through automated correlation against Change Management

3. Weblogic Signature Rules
   - Specific to Fusion Middleware
EM 12c Configuration Management
Oracle Provided DB Compliance Content

- Compliance Standards
  - Pluggable Database (NEW)
    - Storage Best Practices for Pluggable Database
    - Configuration Best Practices for Pluggable Database
    - Basic Security Configuration for Pluggable Database
  - Single Instance Database Instance (and RAC Instance)
    - Certification for Oracle Database
    - Storage Best Practices for Oracle Database
    - Configuration Best Practices for Oracle Database
    - Basic Security Configuration for Oracle Database
    - High Security Configuration for Oracle Database
    - Patchable Configuration for Oracle Database
    - Support Policy for Oracle Database

- Compliance Standards
  - Cluster Database
    - Basic Security Configuration for Oracle Cluster Database Instance
    - High Security Configuration for Oracle Cluster Database Instance
    - Certification for RAC Database
    - Configuration Best Practices for Oracle RAC Database
    - Patchable Configuration for RAC Database
    - Storage Best Practices for Oracle RAC Database
    - Support Policy for RAC Database
  - Listener
    - Basic Security Configuration for Oracle Listener
    - High Security Configuration for Oracle Listener

- 300+ Individual Compliance Rules
Database Security Compliance Standards

- Explains how to use Database security standards
- Description of all security standards and rules

Oracle Single Instance Database Compliance Standards

These are the compliance rules for the Oracle Single Instance Database compliance standards. The compliance standards are:
- Basic Security Configuration for Oracle Database
- Configuration Best Practices for Oracle Database
- High Security Configuration for Oracle Database
- Patchable Configuration for Oracle Database
- Storage Best Practices for Oracle Database

2.1 Basic Security Configuration for Oracle Database

The compliance rules for the Basic Security Configuration for Oracle Database standard follow.

2.1.1 Oracle Net Client Log Directory Permission

- Description: Ensures that the client log directory is a valid directory owned by Oracle set with no permissions to public.
- Severity: Critical

- Rationale: Log files provide information contained in an error stack. An error stack refers to the information that is produced by each layer in an Oracle communications stack as the result of a network error. The information in log files can reveal important network and database connection details. Allowing access to the log directory can expose the log files to public scrutiny.

2.1.2 Oracle Net Client Trace Directory Permission

- Description: Ensures that the client trace directory is a valid directory owned by Oracle set with no permissions to public.
- Severity: Critical
Understanding Compliance Results
Compliance Dashboard – Single Pane Status

Gauges - Current and Lowest Score in Last Week
Target and Violation Counts per Fwk/Std

Newly Discovered Unmanaged hosts may be risk
Least Compliant Target shows where to start remediation
### Compliance Results

Results by Framework, Standard and Target

Select Standard and click "Show Details" for additional information.

<table>
<thead>
<tr>
<th>Compliance Standards</th>
<th>Applicable To</th>
<th>Compliance Standard State</th>
<th>Target Evaluations</th>
<th>Violations</th>
<th>Average Score (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>All MLS v.11 rules</td>
<td>Oracle WebLogic Domain</td>
<td>Production</td>
<td>0 0 1 7 11 10</td>
<td>99</td>
<td></td>
</tr>
<tr>
<td>Oracle HTTP Server Configuration Standard for Fusion</td>
<td>Production</td>
<td>0 0 1 0 0 0</td>
<td>100</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Oracle Fusion Instance Standard</td>
<td>Production</td>
<td>0 0 1 0 0 0</td>
<td>97</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Siebel Gateway Server Standard</td>
<td>Production</td>
<td>0 0 1 0 0 1</td>
<td>96</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Recommendations For Oracle Products</td>
<td>Host</td>
<td>2 0 23 6 0 0</td>
<td>26</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Patch Compliance Standard</td>
<td>Database Instance</td>
<td>5 0 0 5 0 0</td>
<td>26</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Siebel Server Standard</td>
<td>Production</td>
<td>0 0 2 0 0 2</td>
<td>98</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Patchable Configuration For Oracle Database</td>
<td>Database Instance</td>
<td>0 0 1 0 0 0</td>
<td>98</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Oracle Identity Manager Cluster Configuration Compliance</td>
<td>Oracle Identity Manager Cluster</td>
<td>Production</td>
<td>0 0 1 0 0 0</td>
<td>100</td>
<td></td>
</tr>
<tr>
<td>Oracle Access Manager Cluster Configuration Compliance</td>
<td>Oracle Access Manager Cluster</td>
<td>Production</td>
<td>0 0 1 0 0 0</td>
<td>99</td>
<td></td>
</tr>
<tr>
<td>Secure Configuration for Host</td>
<td>Host</td>
<td>0 4 0 99 8 0</td>
<td>57</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Oracle Internet Directory Configuration Compliance</td>
<td>Oracle Internet Directory</td>
<td>Production</td>
<td>0 0 1 0 0 0</td>
<td>99</td>
<td></td>
</tr>
<tr>
<td>Basic Security Configuration For Oracle Listener</td>
<td>Listener</td>
<td>0 0 4 1 0 0</td>
<td>96</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Compliance Standard Result Details

Trend Overview – by Day, Week or Month
Compliance Standard Result Details
Violation Events – Actionable Details

- Offending target
- Violation Details
- When did it occur?
- What caused the violation

Violation message with context
- How to fix it
Each violation generates an event.
Users can update event to inform others of actions taken to address the violation
Understanding Compliance Score Calculation
Compliance Scores

- A target's compliance score for a compliance standard is used to reflect the degree of the target's conformance with respect to that standard.
- Score is in the range of 0% to 100% inclusive.
- Score of 100% indicates a target fully complies with the compliance standard.
Compliance Scores

- A Standard’s score is a weighted average of the results of all contained rules.
- A Framework’s score is a weighted average of all contained Standards.
- Rules and Standards have an importance and severity which together determine its impact on score.
- Severity is set during Standard/Rule creation.
- Importance is set when Standard/Rule added to Framework/Standard.
Compliance Score Calculation

Process Overview

1. Determine score for each target-rule combination in the standard.
   1. Use the following chart to find hirange and lorange for a rule

<table>
<thead>
<tr>
<th>Importance</th>
<th>Critical Severity (lo-hi)</th>
<th>Warning Severity (lo-hi)</th>
<th>Minor Warning Severity (lo-hi)</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>0-25</td>
<td>66-75</td>
<td>95-96</td>
</tr>
<tr>
<td>Normal</td>
<td>26-50</td>
<td>76-85</td>
<td>97-98</td>
</tr>
<tr>
<td>Low</td>
<td>51-75</td>
<td>86-95</td>
<td>99-99</td>
</tr>
</tbody>
</table>

2. Formula for single rule-target score:
   
   \[
   \text{hirange} - (\text{hirange} - \text{lorange}) \times \left( \frac{\text{number of violations}}{\text{number of rows evaluated}} \right)
   \]

2. Aggregate rule scores to find compliance standard score

3. Aggregate standard scores to find compliance framework score
Compliance Score Calculation Example

Example:
Rule (Security Recommendations) has Severity **Critical** and Importance **Low**
Rule-Target has 16 evaluations ALL of which are violations

Substitute numbers from chart and violation into:
\[ \text{hirange} - (\text{hirange} - \text{lorange}) \times (\text{number of violations} / \text{number of rows evaluated}) \]

\[ 75 - (75-51) \times \frac{16}{16} \]
\[ 75 - 24 = 51 \]

Note: If NO evaluations have violation, score is set to 100%
Compliance Score Calculation – Step 2
Compliance Standard -Target

- CS – Compliance Score
- Rule – Compliance Standard Rule. There are 3 rules: Rule1, Rule2 and Rule3
- I1: importance for Rule1
- I2: importance for Rule2
- I3: importance for Rule3
- S1: compliance score for rule1-target
- S2: compliance score for rule2-target
- S3: compliance score for rule3-target

Compliance Score of Compliance Standard-Target

\[
\frac{(S_1 \times i_1) + (S_2 \times i_2) + (S_3 \times i_3)}{(i_1 + i_2 + i_3)}
\]

<table>
<thead>
<tr>
<th>Importance</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>3</td>
</tr>
<tr>
<td>Normal</td>
<td>2</td>
</tr>
<tr>
<td>Low</td>
<td>1</td>
</tr>
</tbody>
</table>
Compliance Score Calculation – Step 3
Compliance Framework - Target

• CF – Compliance Framework
• CS1: compliance score 1
• CS2: compliance score 2
• iCS₁: importance for CS1
• iCS₂: importance for CS2
• iCS₃: importance for CS3
• ST₁: compliance score for CS1-t₁
• ST₂: compliance score for CS1-t₂
• ST₃: compliance score for CS2-t₃

Compliance Score of Compliance Framework

\[
(ST₁ \times iCS₁) + (ST₂ \times iCS₂) + (ST₃ \times iCS₃) \]

\[
\frac{------------------------------------------}{(iCS₁ + iCS₂ + iCS₃)}
\]

<table>
<thead>
<tr>
<th>Importance</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>3</td>
</tr>
<tr>
<td>Normal</td>
<td>2</td>
</tr>
<tr>
<td>Low</td>
<td>1</td>
</tr>
</tbody>
</table>
Compliance Score Thresholds
Understanding and Changing

- Each Compliance Standard can have its own thresholds for Compliant, Warning, and Critical.
- Default Thresholds
  - Critical = 0-60
  - Warning = 61-80
  - Compliant = 81-100
- Change thresholds using “Override Target Type Settings”
Compliance Results – Adding Exceptions

Global Exceptions

- Exceptions can be added globally or for an individual target
- Can be used for Oracle provided or custom rules
- To add Global exception:
  1. Select Standard and Click Override Target Type
  2. Select Rule in navigator
  3. Click Add and enter Exception
  4. Click OK.

User SYSMAN will no longer generate a violation for this rule on ANY target.
Compliance Results – Adding Exceptions

Target Instance Exceptions

- Target Instance exceptions are for a single target only.
- To add Target Instance exception:
  1. Select Standard and Associate Targets
  2. Select target and click Edit
  3. Select Rule in Navigator
  4. Click Add and enter Exception
  5. Click OK.

User SYSMAN will no longer generate a violation for this target ONLY.
Compliance Related Roles and Privileges
Three Primary Compliance Roles

**Compliance Designer**
- Creates Standards, Rules and Facets
- Typically SME for a specific software (DB, Weblogic)
- Not necessarily an administrator or owner of any target.

**Compliance Officer**
- Creates Frameworks using Standards developed by Designer
- Needs compliance visibility across datacenter
- Typically not an administrator or owner of any target.

**DBA, Administrator**
- Associates targets to Standards created by Designer
- Typically an administrator or owner of targets.
- Acts upon compliance results of their targets
## EM Compliance Roles and Privileges

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EM_COMPLIANCE_DESIGNER</td>
<td>Using this role you can create, modify, and delete compliance standards, compliance standard rules, and Real-time Monitoring facets.</td>
</tr>
<tr>
<td>EM_COMPLIANCE_OFFICER</td>
<td>Using this role you can view compliance framework definitions and results.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Resource Type Privileges</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create Compliance Entity</td>
<td>Allows you to create compliance standards, compliance standard rules, and Real-time Monitoring facets</td>
</tr>
<tr>
<td>Full any Compliance Entity</td>
<td>Allows you to edit and delete compliance standards and compliance standard rules</td>
</tr>
<tr>
<td>View any Compliance Framework</td>
<td>Allows you to view compliance framework definition and results</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Target Type Privileges</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage Target Compliance</td>
<td>Ability to associate compliance standard to the target</td>
</tr>
<tr>
<td>View</td>
<td>View the compliance results of a target</td>
</tr>
</tbody>
</table>

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.
## Compliance Tasks and Required Privs/Roles

<table>
<thead>
<tr>
<th>Task</th>
<th>Privileges and Roles Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create compliance framework</td>
<td>CREATE_COMPLIANCE_ENTITY privilege, VIEW_ANY_COMPLIANCE_FWK privilege</td>
</tr>
<tr>
<td>Edit and delete compliance framework</td>
<td>FULL_ANY_COMPLIANCE_ENTITY privilege, VIEW_ANY_COMPLIANCE_FWK privilege</td>
</tr>
<tr>
<td>Create, edit, and delete compliance framework</td>
<td>EM_COMPLIANCE_DESIGNER role, EM_COMPLIANCE_OFFICER role</td>
</tr>
<tr>
<td>Associate a compliance standard to a target</td>
<td>MANAGE_TARGET_COMPLIANCE privilege</td>
</tr>
<tr>
<td>Import or export a compliance framework</td>
<td>EM_COMPLIANCE_DESIGNER role, EM_COMPLIANCE_OFFICER role</td>
</tr>
<tr>
<td>Create a real-time monitoring rule</td>
<td>EM_COMPLIANCE_DESIGNER role</td>
</tr>
<tr>
<td>Create a real-time monitoring facet</td>
<td>EM_COMPLIANCE_DESIGNER role</td>
</tr>
</tbody>
</table>
Operational Aspects of Compliance
Support for incident lifecycle operations

- Manage by Incidents
  - Significant events
  - Combination of events related to the same issue (e.g. events raised from database, host, storage indicating lack of space)

- Centralized incident management console
  - View, manage, diagnose and resolve incidents from one location

- Support for incident lifecycle operations
  - Assign, acknowledge, prioritize, track status, escalate, suppress
  - Notify and open helpdesk ticket

- Integrated Oracle expertise
  - Access to My Oracle Support (MOS) knowledge base
  - Accelerates incident and problem diagnosis and resolution
Proactive Compliance
Notification using Incident Manager

- Use Incident Rule Set to configure notification.
- Events Available:
  - Compliance Standard Rule Violation
    - Generated for each violation
  - Compliance Standard Score Violation
    - Generated when standard score drops below threshold
Administration Groups and Template Collections

- **Administration Groups**
  - Auto-deploys management settings to targets when they join the group
  - Defined by membership criteria

- **Template Collections**
  - Set of management settings (monitoring templates, compliance standards, cloud policies)
  - Associated with administration groups

- **Automated monitoring setup**
  - When adding new target, set its properties
  - Enterprise Manager adds it to group, auto-applies management settings

Set *Lifecycle Status* = “Production” to join PROD group
Administration Group Hierarchy

Membership criteria:

- Lifecycle Status = Production

Membership criteria:

- Lifecycle Status = Production AND
- Line of Business = Finance

One administration group hierarchy per Enterprise Manager site
Updating Content
Self-Update and Plugins

- Self Update
  - Any Target type
  - New or updated Frameworks
- Plug-in
  - Type Type Specific
  - Plugin may or may not bundles Compliance Standards.

[Image of Self Update interface]

Oracle periodically provides new functionality and updates for existing features in Enterprise Manager. The Self Update home allows administrators to receive notifications and view downloads, and apply such updates. While these updates...

Oracle compliance content framework, standards, rules with support of add and delete on these entities.

<table>
<thead>
<tr>
<th>Type</th>
<th>Available Updates</th>
<th>Downloaded Updates</th>
<th>Applied Updates</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent Software</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Compliance Content</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Diagnostic Checks</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>EM Desktop’s Prerequisites</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Database Configuration Tools</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Externally Developed Kit</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Management Connector</td>
<td>9</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Middleware Profiles and Grid</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Oracle Database Provisioning Profiles</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Oracle Virtual Product Mapping</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Oracle VM Templates and Oracle Virtual</td>
<td>14</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Plugin</td>
<td>2</td>
<td>9</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Provisioning Bundles</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

[Copyright © 2014, Oracle and/or its affiliates. All rights reserved.]

[ORACLE]
Compliance Reporting
Information Publisher Reports

- Legacy Reports (7)
- Non-configurable.
- Reports will remain until IP is decommissioned.
Compliance Reporting

Business Intelligence Reports

- Existing Reports (3)
- Configurable
  - Scope
  - Output format
  - Scheduled
  - Email delivery
- Look for more reports in future releases.
Custom Compliance Standards

- Can I create a customize Compliance Standard? YES!

- Start with Oracle provided
- Rich Out of the box content:
  - >1700 Compliance Rules
  - >30 Compliance Standards
- Security Recommendations/Best Practices
Custom Compliance Methodology

Automating Compliance Reporting with Enterprise Manager

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

Check Compliance Library

- Go to: Enterprise->Compliance->Library
- Use Search to filter
  - Set Applicable to: Target Type
  - Put keywords in Description
- Review Descriptions and Rationale to find match to your check
Custom Compliance Methodology

Automating Compliance Reporting with Enterprise Manager

1. Compliance Rule Exists? (No → Required Data Collected?; Yes → Add Compliance Rule to Compliance Standard)
2. Required Data Collected? (No → Extend Target Using Configuration Extension; Yes → Create Custom Compliance Rule)
Required Data Collected?

Check Default Collection

- Go to: `<Target Home> -> Configuration -> Last Collected`
- Click each folder to see data
- If found, make note of folder and property names

If found, make note of folder and property names.
Extend Target Collection

Configuration Extension (CE)

- Go to Enterprise->Configuration->Configuration Extension
- Extend ANY target
- Multiple Collection Methods:
  - Entire File
  - OS Command Output
  - SQL Query
- Choose a parser that matches data format
Custom Compliance Methodology

Automating Compliance Reporting with Enterprise Manager

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

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.
Create Custom Rule

Add to Compliance Library

- Go to Enterprise->Compliance->Library
- Add details to be seen in Violation for user to understand and take action
  - Description
  - Rationale
  - Recommendation
  - Keywords
Create Custom Rule

Add to Compliance Library

- Use SQL Modeler to write the SQL for you!
- Leverages Configuration Search
- No more manual SQL Entry

Create Rule: Repository Rule : Check Definition ( Query )

Specify the query which returns data that is to be verified against the Simple or $ search criteria.

```
* SQL Source
SELECT
   s1.target_guid,
   s2.LOG_MODE
FROM
   CM$MGMT_DB_DBNINSTANCEINFO_ECM s2,
   MGMT$ECM_CURRENT_SNAPSHOTS s1gen1,
   MGMT$TARGET s1
WHERE
   (
      s1gen1.TARGET_GUID = s1.TARGET_GUID
      AND s1gen1.ECM_SNAPSHOT_ID = s2.ECM_SNAPSHOT_ID
      AND s1.TARGET_TYPE = 'oracle_database'
      AND s1gen1.SNAPSHOT_TYPE = 'oracle_dbconf'
   )
```

Compliant Message

Non-Compliant Message

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.
Custom Compliance Methodology

Automating Compliance Reporting with Enterprise Manager

- 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
Add Rule to Standard

Customize Compliance Standards

- Create New or Add to existing Standard
- Set Importance in context of Standards (Low, Normal, High)
- Organize Rules in folder hierarchy
Real Time Compliance Monitoring
Real Time Compliance Monitoring Overview

- Primary Use Cases
  - Audit adherence to change management processes
  - Proactive monitoring of critical components (tnsnames.ora)
- What can be monitored?
  - Files, processes, users, database changes, windows objects
  - Each item has unique actions that can be monitored (detailed later)
- What is captured?
  - Key attributes captured include user ID, process ID and time of action
- Which platforms are supported?
  - Linux, Solaris, AIX, Windows
Real Time Compliance Monitoring Setup

1. Ensure Operating System or DB specific pre-requisites met
   a) [http://docs.oracle.com/cd/E24628_01/em.121/e27046/install_realtime_ccc.htm#autold7](http://docs.oracle.com/cd/E24628_01/em.121/e27046/install_realtime_ccc.htm#autold7)
2. Configure Privilege Delegation ( Sudo/PBRun )
3. Set Real Time Monitoring Credentials
4. Define Facet ( What to monitor )
5. Define Rule ( How to Monitor items in Facet )
6. Define/Add rule to Standard
7. Associate Standard to Targets
## Monitored Events

**Linux, Solaris, AIX**

<table>
<thead>
<tr>
<th>Files</th>
<th>Users</th>
<th>Processes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content Modified</td>
<td>Telnet Login</td>
<td>Start</td>
</tr>
<tr>
<td>Delete</td>
<td>SSH Login</td>
<td>Stop</td>
</tr>
<tr>
<td>Rename</td>
<td>SU Login</td>
<td></td>
</tr>
<tr>
<td>Create</td>
<td>Sudo</td>
<td></td>
</tr>
<tr>
<td>Permission Change</td>
<td>RDP Login</td>
<td></td>
</tr>
<tr>
<td>Ownership Change</td>
<td>Console Login</td>
<td></td>
</tr>
<tr>
<td>Read</td>
<td>FTP Login</td>
<td></td>
</tr>
</tbody>
</table>
# Monitored Events

## Windows

<table>
<thead>
<tr>
<th>Registry</th>
<th>AD Users</th>
<th>AD Computers</th>
<th>AD Groups</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create Key</td>
<td>User Create</td>
<td>Computer Create</td>
<td>Group Create</td>
</tr>
<tr>
<td>Delete Key</td>
<td>User Delete</td>
<td>Computer Delete</td>
<td>Group Delete</td>
</tr>
<tr>
<td>Create Value</td>
<td>User Attrib Modify</td>
<td>Computer Attrib Modify</td>
<td>Group Attribute Modify</td>
</tr>
<tr>
<td>Modify Value</td>
<td></td>
<td></td>
<td>Member Add</td>
</tr>
<tr>
<td>Delete Value</td>
<td></td>
<td></td>
<td>Member Delete</td>
</tr>
</tbody>
</table>
# Monitored Events – Oracle Database

<table>
<thead>
<tr>
<th>Action</th>
<th>Tables</th>
<th>Views</th>
<th>Materialized Views</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insert</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Select</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Update</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Delete</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Create</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Drop</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Truncate</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Alter</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Comment</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Rename</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Lock</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Grant</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Revoke</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Audit</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>NOAUDIT</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Flashback</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>
## Monitored Events – Oracle Database

<table>
<thead>
<tr>
<th>Action</th>
<th>Index</th>
<th>Sequence</th>
<th>Procedure</th>
<th>Function</th>
<th>Package</th>
<th>Library</th>
<th>Trigger</th>
<th>Tablespace</th>
<th>Cluster</th>
<th>Link</th>
<th>Dimension</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Drop</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Alter</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Analyze</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Select</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Grant</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Revoke</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Audit</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NOAUDIT usage</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Execute</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Truncate</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>
## Monitored Events – Oracle Database

<table>
<thead>
<tr>
<th>Action</th>
<th>Profile</th>
<th>Public Link</th>
<th>Public Synonym</th>
<th>Synonym</th>
<th>Type</th>
<th>Role</th>
<th>User</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Drop</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Alter</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Analyze</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Select</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Grant</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>Role/System</td>
</tr>
<tr>
<td>Revoke</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>Role/System</td>
</tr>
<tr>
<td>Audit</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NOAUDIT usage</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Execute</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Truncate</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Login</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Logoff</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>
Real-Time Compliance Monitoring – Facets

- Determines ‘WHAT’ to monitor
- Specific to Target type and Entity
- Define inclusion and exclusion patterns in single facet
- Select files from existing target by ‘Browsing’
Real-Time Compliance Monitoring – Rules

- Determines ‘HOW’ to monitor
- Specific to Target type and Entity
- Choose Facet to define ‘WHAT’ to monitor
Manually Authorization

Determine the default status of observations which effect compliance scoring.

- **Unauthorized = No Effect on compliance score**
- **Unauthorized = Negative effect**
- **Authorized = Positive effect**

Choose to generate an event (for notification and mgmt)

Automatic Authorization

Requires Change Request Management Connector

Remedy only supported CMS