Security Compliance and Data Governance: Dual problems, single solution

David Wolf
Director of Product Management
Oracle Development, Enterprise Manager

Steve Ries
Senior Systems Architect
Technology Services Organization
United State Marine Corps
Session: CON8015

Title: Security Compliance and Data Governance: Dual problems, single solution

Description: Ensuring your databases comply is standards and sensitive data is protected can be difficult and time consuming task. This session will demonstrate how to use Oracle Enterprise Manager 12c for continuous security compliance auditing of your Oracle databases and underlying infrastructure against configuration standards such as the Department of Defense (DoD) Security Technical Implement Guide (STIG). You’ll also learn how the new Data Governance feature can help find unsecured sensitive data throughout your environment and aid your data masking decisions.
Safe Harbor Statement

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle’s products remains at the sole discretion of Oracle.
Program Agenda

1. Data Governance and Security Compliance – Commonalities
2. EM12c Compliance Framework Overview
3. Automated STIG Compliance Auditing @ US Marine Corp
4. EM12c Data Governance – Sensitive Data Discovery
5. Conclusion and Q & A
Oracle Database Security Solutions Defense in Depth

<table>
<thead>
<tr>
<th>PREVENTIVE</th>
<th>DETECTIVE</th>
<th>ADMINISTRATIVE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption &amp; Redaction</td>
<td>Activity Monitoring</td>
<td>Key &amp; Wallet Management</td>
</tr>
<tr>
<td>Masking &amp; Subsetting</td>
<td>Database Firewall</td>
<td>Privilege &amp; Data Discovery</td>
</tr>
<tr>
<td>Privileged User Controls</td>
<td>Auditing &amp; Reporting</td>
<td>Configuration Management</td>
</tr>
</tbody>
</table>

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.
Oracle Database Security Solutions Defense in Depth

<table>
<thead>
<tr>
<th>PREVENTIVE</th>
<th>DETECTIVE</th>
<th>ADMINISTRATIVE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption &amp; Redaction</td>
<td>Activity Monitoring</td>
<td>Key &amp; Wallet Management</td>
</tr>
<tr>
<td>Masking &amp; Subsetting</td>
<td>Database Firewall</td>
<td>Privilege &amp; Data Discovery</td>
</tr>
<tr>
<td>Privileged User Controls</td>
<td>Auditing &amp; Reporting</td>
<td>Configuration Management</td>
</tr>
</tbody>
</table>
Security Compliance and Data Governance

Common Goals
• Achieve compliance with standards or regulations
• Manage risk
• Improve (Data) Security
• Minimizing or eliminating rework
• Optimize Staff effectiveness

Common Challenges
• Data centers have thousands of databases some containing sensitive data
• Enterprises lack enterprise-wide tools to scan databases regularly
• Limited visibility into compliance status (encryption, masking, database vault) of sensitive data
• Hard to remediate non-compliance
Security Compliance and Data Governance

Common Solution Requirements

• Highly automated
• Continuous auditing
• Proactively alert on findings and issues
• Provide remediation automation or guidance
• Provide robust and flexible reporting
Program Agenda

1. Data Governance and Security Compliance – Commonalities
2. EM12c Compliance Framework Overview
3. Automated STIG Compliance Auditing @ US Marine Corp
4. EM12c Data Governance – Sensitive Data Discovery
5. Conclusion and Q & A
Enterprise Manager Compliance Framework

Overview

Continuous Configuration Auditing

Real-Time File Integrity Monitoring

Cloud Scale

Ready to use Standards
Enterprise Manager Compliance Framework
Continuous Configuration Auditing

• Tightly integrated with configuration collection framework.
  – Evaluation “triggered” by detected configuration changes.
  – Efficient mechanism vs full scheduled evaluation.
  – Always up to date.

• Violations automatically cleared after remediation.
• Alert on each violation or score threshold.
Enterprise Manager Compliance Framework

Real-Time File Integrity Monitoring

• Know the “who”, “what” and “when” the change was made.
• Detect “Unauthorized” changes automatically.
• Required for many Industry regulations like PCI.
• Capable of monitoring users, processes and database actions in addition to files.
• Oracle provided standards for Critical Oracle Linux and Exadata files.
Enterprise Manager Compliance Framework

Cloud Scale

• Efficient re-evaluation on change reduces network and host resource consumption.

• Standards can be automatically applied using Administrative groups or composite targets (DBaaS Pools, Application Systems)

• New Agent-Side rules control repository growth

• Summary reporting via BI Publisher
Enterprise Manager Compliance Framework

Ready to use Compliance Standards and Checks

- 1000s of Oracle provided Checks (Rules)
  - 25+ Standards for Database components (RAC, SI, Listener, etc)
- Based on Oracle’s best practices and Security recommendations
- Customizable to meet Internal best practices
  1. Leverage Oracle provided rules matching your own
  2. Tailor Oracle provided rules with known exceptions
  3. Build custom rules to exactly match requirement

- New in 12.1.0.4 – Oracle Database 11g STIG Standards
Program Agenda

1. Data Governance and Security Compliance – Commonalities
2. EM12c Compliance Framework Overview
3. Automated STIG Compliance Auditing @ US Marine Corp
4. EM12c Data Governance – Sensitive Data Discovery
5. Conclusion and Q & A
ABOUT THE SPEAKER

Steve Ries
Senior Systems Architect
Technology Services Organization
United State Marine Corps
October 2, 2014
About Technology Services Organization

- Software development and systems integrator of enterprise level pay and personnel systems for the United States Marine Corps and other branches of the military

<table>
<thead>
<tr>
<th>Enterprise Manager 12c Environment</th>
<th>Monitored Targets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Hardware</td>
<td>Dell 3800</td>
</tr>
<tr>
<td>Operating System</td>
<td>Redhat 5.8</td>
</tr>
<tr>
<td>Processors</td>
<td>8</td>
</tr>
<tr>
<td>RAM</td>
<td>16GB</td>
</tr>
<tr>
<td>Repository DB</td>
<td>11.2.0.3</td>
</tr>
<tr>
<td>Hosts</td>
<td>~300</td>
</tr>
<tr>
<td>Databases</td>
<td>~100</td>
</tr>
<tr>
<td>Oracle Middleware</td>
<td>~150</td>
</tr>
</tbody>
</table>
Database Security at Department of Defense

• STIG – Security Technical Implementation Guide
  • A guide for Information Security - a compendium of DoD policies, security regulations and best practices
  • Includes security configurations for OS, database and application servers, network switches, routers, etc
  • Mandated by DOD regulations

• Current Oracle Database STIG is Version 8 Release 1.11
  • http://iase.disa.mil/stigs/app-security/database/Pages/index.aspx
Challenge

- In the DoD, your security posture is determined by your configuration management strategy
  - The database STIG is primarily a manual process.
  - Maintaining proper security posture is similarly manual. “Compliance drift”
  - Need a solution to automatically check and report on proper security configurations.
Our STIG Auditing Automation Evolution

Enterprise Manager 12c Version 12.1.0.4

- Complete out of the box solution for STIG monitoring
- Easy to deploy
- Multiple dimensions in which to view finding data
- Reporting capabilities
- Can be used for single-instance and clustered databases
- Complies with DoD, but any company can use it

In House Scripts

EM 11g
- User-Defined Metrics and Policies

EM 12c Pre-R4
- Custom Configuration Extensions and Rules

EM 12c R4
- Complete Out of Box Solution
Using Oracle STIG Standard
See Results in Minutes

- Deploy to database(s) in 2 steps
  1. Select Standard
  2. Select Targets

- Almost immediate results
- Checks run daily by default
- Configurable Notification on violation
Dealing with Manual Checks

- **Challenge**
  - Some checks cannot be automated
  - Need to include status in report

- **Manual Rule Type**
  - Define Check to be manually performed
  - Generates single violation per target
  - Must be cleared manually (attested)
  - Clear permanently or temporarily by date
  - User and reason for attestation captured
Dealing with Exception and Grace Periods

• Challenge
  • Some issues require time (Grace period) to address
  • Approved exceptions cannot impact results, but must be reported

• Violation suppression feature
  • Hide violation from results temporarily or permanently
  • User and reason captured
  • Violation re-appears upon suppression expiration
Robust and Flexible Reporting

How compliant is my environment?

How compliant are we for each finding?

Security Technical Implementation Guide (STIG Version 1.8) for Oracle Database

Summary

Rule Evaluations

Target Scorecard

Targets By Severity

Result By Target

Result By Compliance Standard Rule

<table>
<thead>
<tr>
<th>Compliance Standard Rules</th>
<th>Targets</th>
<th>Non-Compliant Targets</th>
<th>Compliant Targets</th>
<th>Violations</th>
<th>Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>DG0016 DBMS unused components</td>
<td>0</td>
<td>0</td>
<td>43</td>
<td>0</td>
<td>Warning</td>
</tr>
<tr>
<td>DG0017 DBMS shared production/development use</td>
<td>0</td>
<td>0</td>
<td>43</td>
<td>0</td>
<td>Warning</td>
</tr>
<tr>
<td>DG0020 DBMS backup and recovery testing</td>
<td>0</td>
<td>0</td>
<td>43</td>
<td>0</td>
<td>Warning</td>
</tr>
<tr>
<td>DG0021 DBMS software and configuration baseline</td>
<td>0</td>
<td>0</td>
<td>43</td>
<td>0</td>
<td>Warning</td>
</tr>
<tr>
<td>DG0025 DBMS encryption compliance</td>
<td>0</td>
<td>0</td>
<td>43</td>
<td>0</td>
<td>Warning</td>
</tr>
<tr>
<td>DG0029 Database auditing</td>
<td>0</td>
<td>0</td>
<td>43</td>
<td>0</td>
<td>Warning</td>
</tr>
<tr>
<td>DG0030 DBMS audit data maintenance</td>
<td>0</td>
<td>0</td>
<td>43</td>
<td>0</td>
<td>Warning</td>
</tr>
<tr>
<td>DG0031 DBMS audit of changes to data</td>
<td>0</td>
<td>0</td>
<td>43</td>
<td>0</td>
<td>Warning</td>
</tr>
<tr>
<td>DG0032 DBMS audit record access</td>
<td>0</td>
<td>0</td>
<td>43</td>
<td>0</td>
<td>Warning</td>
</tr>
</tbody>
</table>

CSC Proprietary and Confidential
Robust and Flexible Reporting

How compliant is each database?

How compliant is a given database?

Security Technical Implementation Guide (STIG Version 1.8) for Oracle Database

Target Scorecard

Rule Evaluations

Targets By Severity

Rule Evaluations

Result By Target

Result By Compliance Standard Rule

Target Name | Score (%) | Violations | Last Evaluation Date
--- | --- | --- | ---
 | | | |

Compliance Standard | Security Technical Implementation Guide (STIG Version 1.8) for Oracle Database
Target Name

Violations

Violations Count

Compliance Standard Rules

DG0004 DBMS application object owner accounts
DG0008 DBMS application object ownership
DG0012 DBMS software storage location
DG0073 DBMS failed login account lock
DG0077 Production data protection on a shared system
DG008S Minimum DBA privilege assignment
DG0116 DBMS privileged role assignments
DG0117 DBMS administrative privilege assignment
DG0118 DBMS application user privilege assignment
DG0123 DBMS Administrative data access
DG0125 DBMS account password expiration
DG0129 DBMS warning banner
DG0231 Oracle application object owner tablespaces
DG0340 Oracle application administration roles enablement
DG050 Oracle system privilege assignment
DG0540 Oracle DBA role assignment
DG0536 Oracle DDL_TIME profile parameter
DG0689 Oracle object permission assignment to PUBLIC
DG06751 SQLNET.ALLOWED_LOGON_VERSION

CSC Proprietary and Confidential
Robust and Flexible Reporting

What are the individual findings?

How compliant are we for a given finding?

- DG0029 Database auditing
- DG0030 DBMS audit data maintenance
- DG0031 DBMS audit of changes to data
- DG0032 DBMS audit record access
- DG0060 DBMS shared account authorization
- DG0065 DBMS PKI authentication
- DG0070 DBMS user account authorization
- DG0071 DBMS password change variance
- DG0073 DBMS failed login account lock
- DG0074 DBMS inactive accounts
- DG0075 DBMS links to external databases
- DG0076 Sensitive data import to development DBMS
- DG0077 Production data protection on a shared system
- DG0078 DBMS individual accounts
- DG0079 DBMS password complexity
- DG0080 DBMS application user privilege assignment review
- DG0085 Minimum DBA privilege assignment
Experiences, Benefits and Gains

• Consolidated view of your security posture – learn in minutes what would have taken hours to compile
• Manual STIG time – 4 to 8 hours per target
• OEM Compliance Framework – < 1 hour
• Faster checks = tighter security
• RAC enabled out-of-the-box
• Future possibility of a comprehensive STIG framework that includes operating systems through SCAP and applications servers such as Weblogic
EM Compliance Best Practices

- Leverage Administrative groups for automated application of standards
- Configure Notification rules to receive emails when new violation detected
- Clear Manual findings for X months to ensure compliance
- Leverage Public Views to leverage compliance data in other systems
- Create custom Operator role removing “Manage Target Compliance” to reduce list of users capable of suppressing violations.
Program Agenda

1. Data Governance and Security Compliance – Commonalities
2. EM12c Compliance Framework Overview
3. Automated STIG Compliance Auditing @ US Marine Corp
4. EM12c Data Governance – Sensitive Data Discovery
5. Conclusion and Q & A
Enterprise Manager - Sensitive Data Discovery

• Scan Oracle Database sensitive data
• Built-in, extensible data definitions
• Discover application data models
• Protect sensitive data appropriately
  – encrypt
  – redact
  – mask
  – audit...
Enterprise Data Governance allows you to discover, scan and identify databases that may contain sensitive data automatically across your enterprise

- **Shallow Scan** – Meta data discovery
- **Deep Scan** – Sensitive data discovery
Enterprise Manager – Sensitive Data Discovery

How it works

- Meta-Data Discovery
  - Scans dictionary for sensitive cols
  - Uses monitoring credentials
  - Searches for:
    - Sensitive table and column name patterns
    - Application signatures to identify packaged apps
    - Objects with security protections

- Data Discovery
  - Samples data and searches for various sensitive data patterns like card number, phone, etc.
  - Requires database credentials
Enterprise Manager – Sensitive Data Discovery

Configure, Discover, Classify ➔ Protection

Configure
- Sensitive type configuration
- Application Signature configuration
- Out of the Box Data Protection configuration

Discover
- Metadata Discovery
- Data Discovery

Classify
- Classify sensitive column types, data protection and application signatures
- Associate an Application Data Model

Data Masking
Redaction
Encryption
Demonstration
Automated Sensitive Data Discovery
Program Agenda

1. Data Governance and Security Compliance – Commonalities
2. EM12c Compliance Framework Overview
3. Automated STIG Compliance Auditing @ US Marine Corp
4. EM12c Data Governance – Sensitive Data Discovery
5. Conclusion and Q & A
Enterprise Manager – The Single Solution
For Automated Security Compliance Auditing and Sensitive Data Discovery

✓ Highly automated
✓ Continuous auditing
✓ Proactively alert on findings and issues
✓ Automated remediation or guidance
✓ Robust and flexible reporting
Learn More

On Oracle Technology Network

Enterprise Manager-Lifecycle Management Page

Overview
Data Sheets, Business Whitepapers, Feature Overview

Enterprise Manager 12c
Database Lifecycle Management Pack Overview JUNE 2014
Database Lifecycle Management Pack Data Sheet JUNE 2014
Configuration Management
Previous Releases
Provisioning and Patch Automation

Getting Started
Self-Running Demos, Screenwatchs, Online Training

Enterprise Manager 12c
Using Agent-Side Compliance Rules JUNE 2014
Using the STIG Compliance Standard JUNE 2014
Complete Lifecycle Management of Pluggable Databases
Change Activity Planner
Introduction, Auto-discovery and Management of Databases
Provisioning Oracle Databases
Configuration Management of Databases
Database Compliance Management
Database Change Management and Patching
Patching Oracle Database with Minimum Down-time
Patching Databases on Oracle Cloud

Understanding
Success stories, Magazine Articles, Press Releases

Enterprise Manager 12c
British Telecom - Decreases Hardware Costs and Increases System Agility using Automated Provisioning (Success Story)
Software Library
Auto-discovery and Management of IT Assets
Patching Oracle Databases - In Place Patching
Patching Oracle Real Application Clusters
Patching Oracle Databases in Offline Mode
Provisioning Grid Infrastructure and RAC Databases using Enterprise Manager 12c

Compliance Management – Overview
Compliance Management (How To) - Custom Compliance on Default Data
Compliance Management (How To) - Custom Compliance using SQL
Configuration Extension
Compliance Management (How To) - Custom Compliance using Command
Configuration Extension

Cut configuration management effort by 90%. Reduce provisioning effort by 75%. Reduce critical patching time by 90%. Save an IT department time by up to 50%.

All of these are possible with Oracle’s Integrated Lifecycle Management solutions. Lifecycle Management is a comprehensive solution that helps database, system, and application administrators automate the processes required to manage the lifecycle of Oracle technology. It eliminates manual and time consuming tasks related to discovery, initial provisioning, patching, configuration management and ongoing change management. In addition the solution provides compliance frameworks for reporting and management of industry and regulatory compliance standards. Finally, all of the on-premise instrumentation can be connected in real-time to My Oracle Support for complete communication between Oracle and our customers.
Join the Conversation

Learn more at: oracle.com/enterprisemanager
Hardware and Software
Engineered to Work Together