ORACLE®

Streamline IT Management processes with Oracle Enterprise Manager 13c

Eric Rudie
Master Principal Sales Consultant
Oracle Public Sector
27 September 2016

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.

Current Landscape: Reality Check

1 Most enterprises are adopting a pragmatic, phased, co-existing approach towards hybrid cloud

2 Consolidation, standardization and automation are still in early stages

3 Management is highly fragmented, too many tools for managing different parts

50% of enterprises will have hybrid cloud by 2017

Gartner 2013

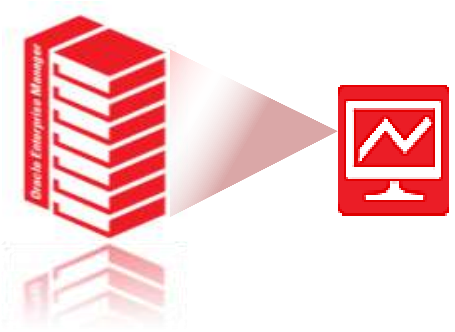
Less the 50% of databases have consolidated

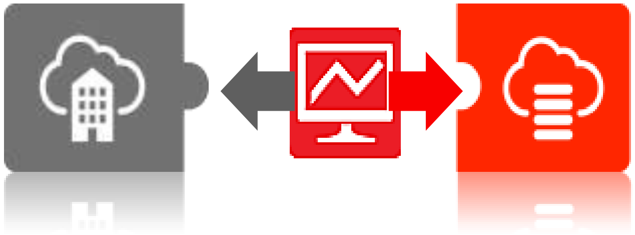
IOUG Survey, 2014

96% survey have more than 3 management tools, 27% more than 10

Gartner survey, 2014

Enterprise Management Strategy



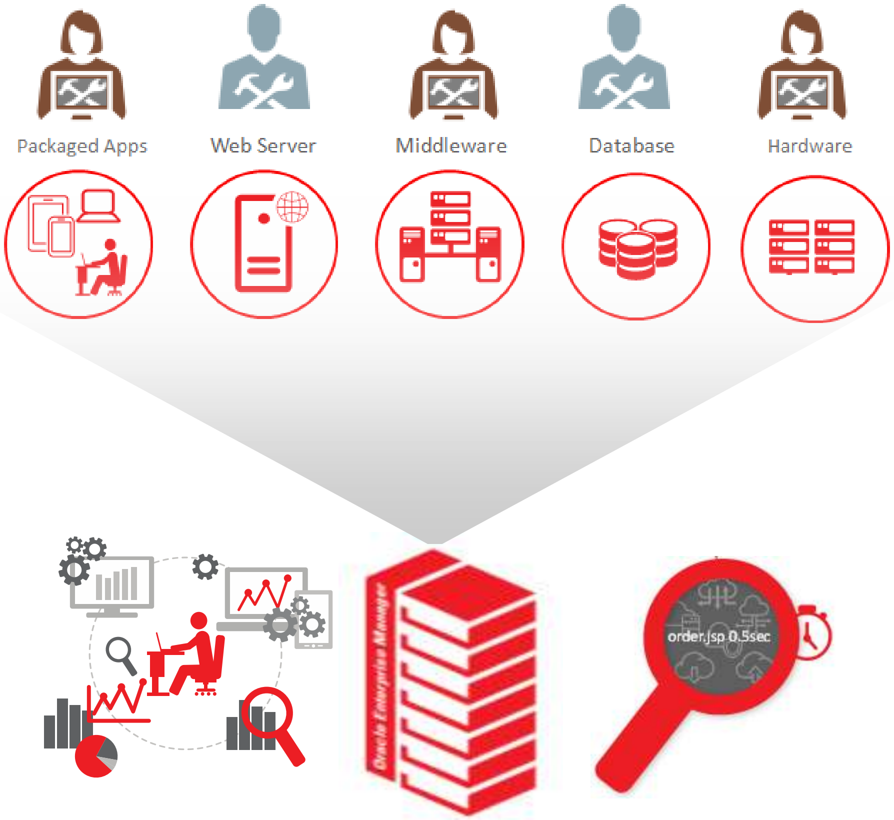


Single pane of glass for managing

- Across the stack
  - Provide unified solution for hardware and software management
  - Complete solution for performance management, lifecycle management and cloud management
- Across on-premise and Oracle Cloud
  - Provide comprehensive hybrid cloud management at-par with on-premise capabilities

“The Communication Hub of Oracle”

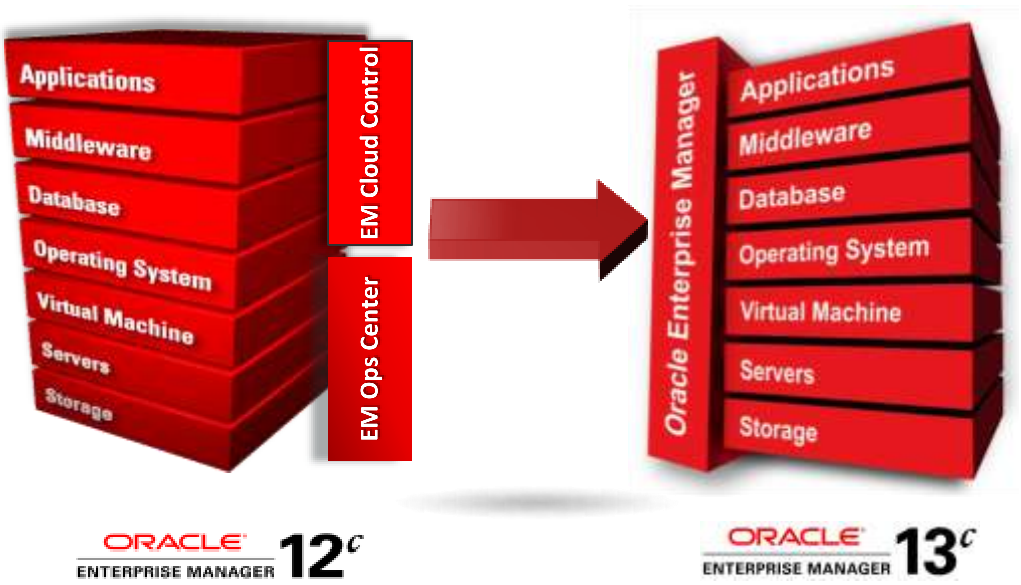
ORACLE ENTERPRISE MANAGER 13c



- Single pane of glass for hardware and software management
- Centralized communication & collaboration for diagnostics and troubleshooting
- Designed to share critical information while maintaining sandboxes
- Integrated named credentials & auditing

ORACLE

Unified hardware and software monitoring



- Single pane of glass for hardware and software monitoring
- Ease of diagnostics with drill down from application
- Single framework for complete stack monitoring
  - Groups and Systems
  - Alerting and Incident Management
  - Security and Credentialing
  - Job system

Database Lifecycle Management (DBLM)

1 DBLM Overview

2 Database Provisioning

3 Patch Automation

4 Configuration Standardization

5 STIG Compliance

Key Challenges and Solutions

Unmanaged asset sprawl

- 28% have an annual database instance growth of more than 20%
- Less than 50% have consolidated

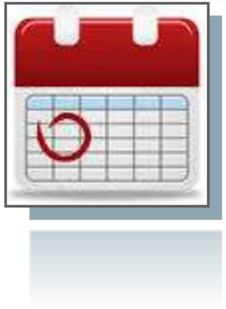
Consolidation

Configuration Pollution

- Too many versions, patch levels and sizes
- 1400 variants across 3 major releases for a large telecom customer

Standardization

Slow time to delivery



- Days to Weeks to provision database services for key projects
- Weeks to clone a complete middleware stack, such as SOA

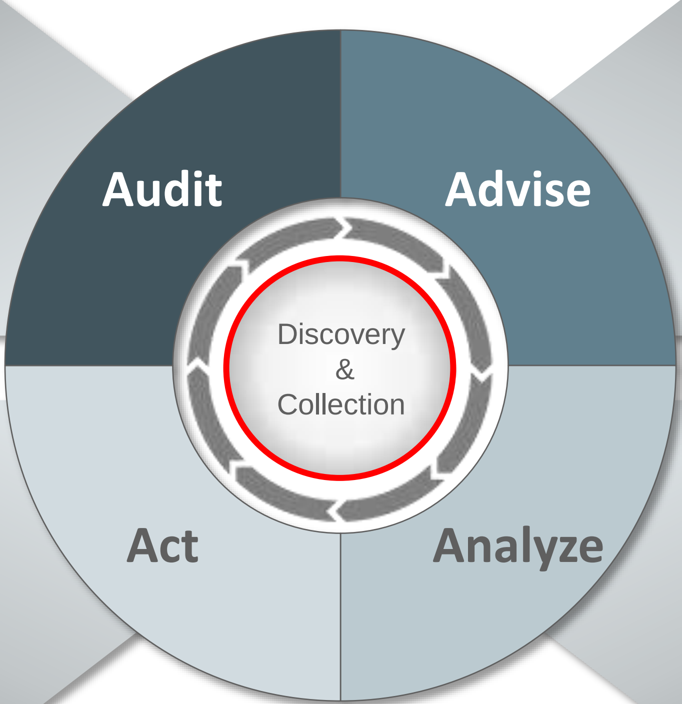
Automation

*IOUG Survey, 2013

Database Lifecycle Management

How Do All These Come Together

- Real-Time Monitoring – Who/When
- Compliance Score
  - Best Practices
  - Oracle Recommendations
  - Regulatory (STIG)
- Report
  - Inventory &Trend
- Automatic Change Reconciliation
  - Authorized vs Unauthorized



- Patch Advisories via MOS
- Upgrade Advisories from MOS
- Configuration Policy Violations

- Patch/Upgrade database and GI
- Mass deployment/Provisioning
- Cloning/migration of binaries and database (incl' pluggable)
- Schema Synchronization
- Settings, Drift & Policy Actions
- Configuration Changes

- Topology guided Impact Analysis
- Config Comparison for Drift Analysis
  - To Gold & Baseline
  - 1 to 1, 1 to N
  - Target and System
- DB Change Management
- Data Comparison
- Data Governance
- Patch Plans: Conflict & PreReq Analysis

Program Agenda

1 DBLM Overview

2 **Database Provisioning**

3 Patch Automation

4 Configuration Standardization

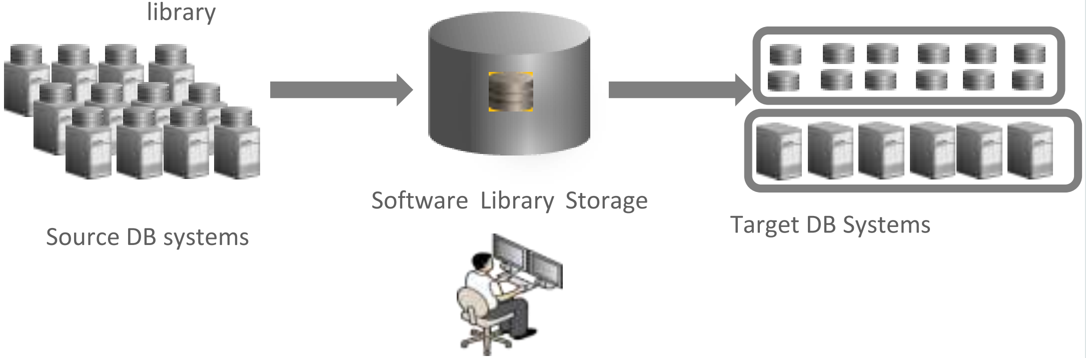
5 STIG Compliance

ORACLE

Databases Cloning using Oracle Enterprise Manager 13c Provisioning

Database Provisioning

- Mass Deployment of Oracle Software (Database, Real Application Clusters)
- Supports all versions up to 12.1 including Pluggable Databases
- Gold Image cloning and standardized software deployment via *Profiles*
- *Lock down* access for controlled and error free deployments



Save **Gold** image (and optionally data) from source systems to EM software library

Deploy saved Image and data to target systems with customizations

Source DB systems

Software Library Storage

Target DB Systems

Program Agenda

1. DBLM Overview
2. Database Provisioning
3. **Patch Automation**
4. Configuration Standardization
5. STIG Compliance

Overview: Patch Automation Solution

ORACLE ENTERPRISE MANAGER 13c

Traditional Estate

- Automated Patching via Patch Plans
- Advice/recommend patches based on configuration
- Minimize Downtime, identify issues with pre requisite check
- Patch Templates and Compliance Standards
- EMCLI Support

Multi-Tenant

adds…

Plug/unplug

Container DB Patching

Continuous Drift and Configuration Auditing for PDB's

Cloud

adds…

Self Service maintenance

Simple Subscription using "Gold-Image"

Real time Patch Tracking which helps in real time compliance

Engineered Systems

adds…

Extending Patching beyond the Database software

Patch the database grid

Patch storage grid

Patch InfiniBand network

Patch recommendations for the Quarterly Full Stack Download Patch.

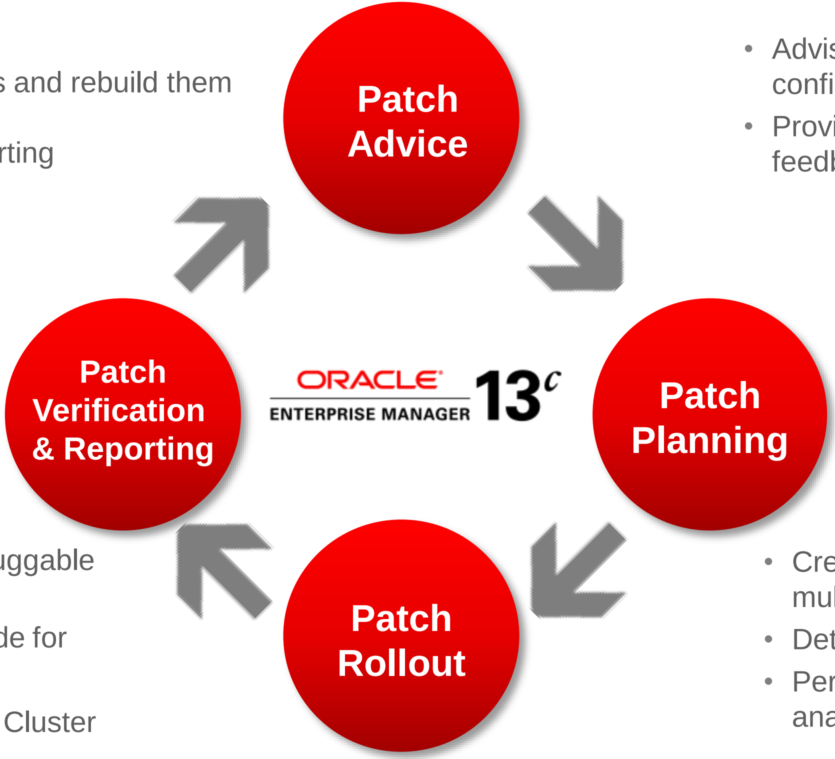
Comprehensive dashboard of the maintenance status and needs.

ORACLE

Patch Management with Oracle Enterprise Manager 13c

- Detect and verify patching success
- Detect drift from existing gold images and rebuild them for future software rollouts
- Patch Compliance tracking and reporting
- Revert to previous version in case of regression**

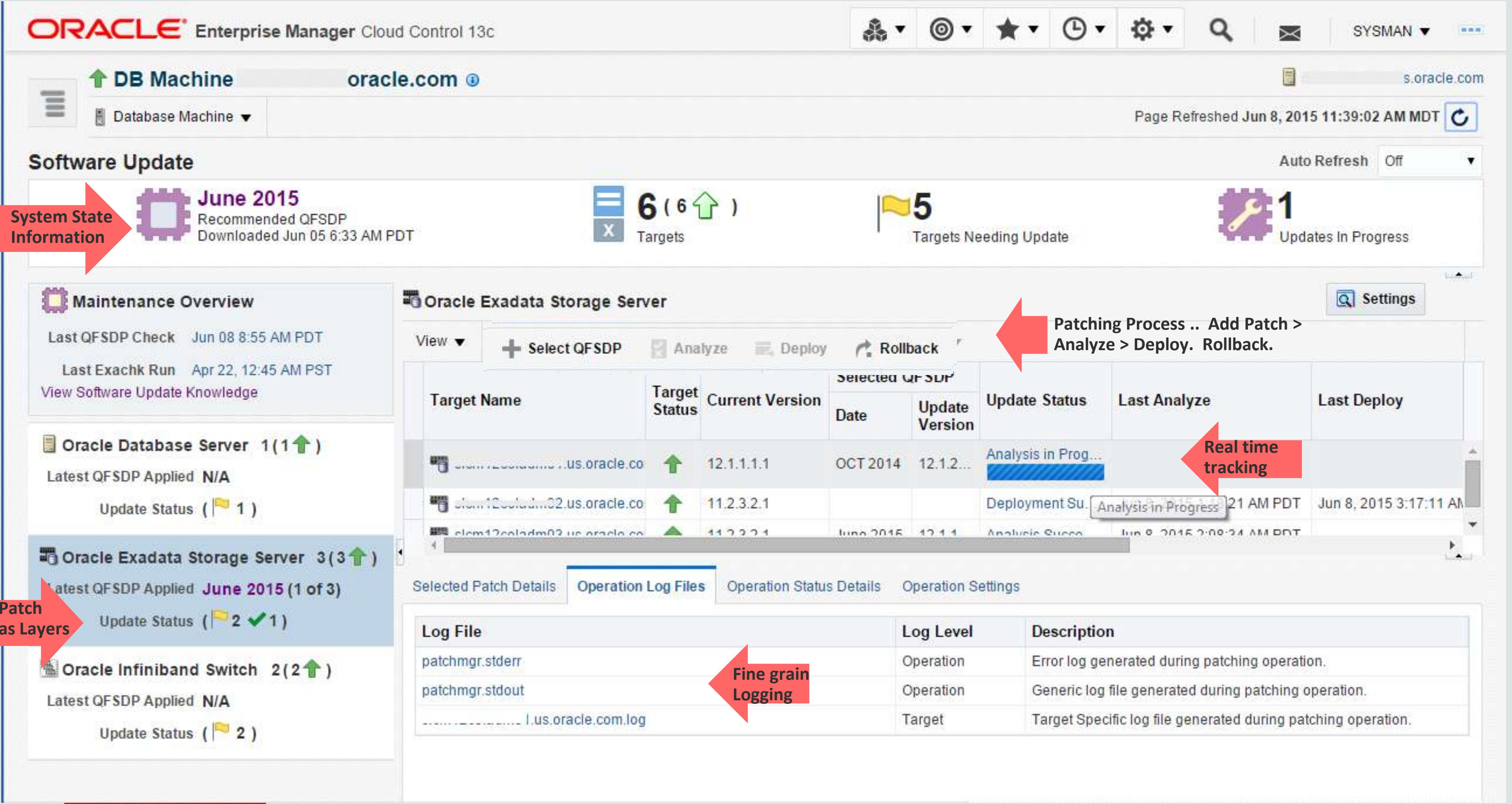
- Advise/recommend patches based on configuration
- Provides patch rating and community feedback



- Support Rolling patches for RAC, Pluggable DBs**
- Support out-of-place patching/upgrade for single instance databases**
- Support patching Exadata Database Cluster Stack**
- Support Group based patching**
- Push button Patching by “Operators”

- Create Patch Plans & templates to apply multiple patches in a single downtime**
- Detect conflicts and file merge requests
- Perform pre-flight dependency and impact analysis**

*****New or Significantly Enhanced***



ORACLE Enterprise Manager Cloud Control 13c

SYSMAN

DB Machine [redacted] oracle.com

[redacted] s.oracle.com

Database Machine ▾

Page Refreshed Jun 8, 2015 11:39:02 AM MDT

Software Update

Auto Refresh: Off

June 2015
Recommended QFSDP
Downloaded Jun 05 6:33 AM PDT

6 (6 ↑)
Targets

5
Targets Needing Update

1
Updates In Progress

System State Information

Maintenance Overview

Last QFSDP Check: Jun 08 8:55 AM PDT

Last Exachk Run: Apr 22, 12:45 AM PST

View Software Update Knowledge

Oracle Database Server 1 (1 ↑)
Latest QFSDP Applied: N/A
Update Status (1)

Oracle Exadata Storage Server 3 (3 ↑)
Latest QFSDP Applied: June 2015 (1 of 3)
Update Status (2 ✓ 1)

Oracle Infiniband Switch 2 (2 ↑)
Latest QFSDP Applied: N/A
Update Status (2)

Patch as Layers

Oracle Exadata Storage Server

Settings

Patching Process .. Add Patch > Analyze > Deploy. Rollback.

Target Name	Target Status	Current Version	Selected QFSDP		Update Status	Last Analyze	Last Deploy
			Date	Update Version			
[redacted].us.oracle.co	↑	12.1.1.1.1	OCT 2014	12.1.2...	Analysis in Prog...		
[redacted]2.us.oracle.co	↑	11.2.3.2.1			Deployment Su...	Jun 8, 2015 ...21 AM PDT	Jun 8, 2015 3:17:11 AM
slcm12celadm03.us.oracle.co	↑	11.2.3.2.1	June 2015	12.1.1...	Analysis Succe...	Jun 8, 2015 2:08:34 AM PDT	

Analysis in Progress

Real time tracking

Selected Patch Details | Operation Log Files | Operation Status Details | Operation Settings

Log File	Log Level	Description
patchmgr.stderr	Operation	Error log generated during patching operation.
patchmgr.stdout	Operation	Generic log file generated during patching operation.
[redacted]l.us.oracle.com.log	Target	Target Specific log file generated during patching operation.

Fine grain Logging

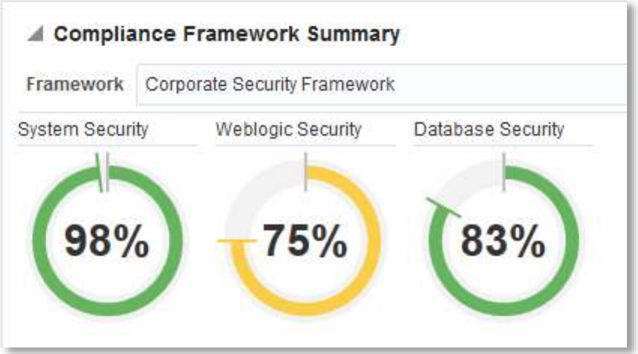
Program Agenda

1. DBLM Overview
2. Database Provisioning
3. Patch Automation
4. **Configuration Standardization**
5. STIG Compliance

ORACLE

Continuous Drift and Configuration Auditing

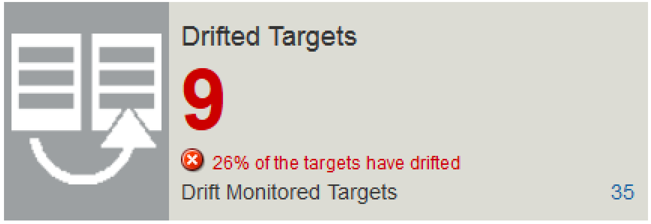
- Configuration Audit
  - Validate conformance to standards or benchmarks using discrete logic
  - Best for Industry and internal standards (STIG,CIS)
- Continuous Drift NEW
  - Validate conformance to standards using Reference configuration
  - Best for critical and rapidly changing configuration settings



Compliance Framework Summary

Framework: Corporate Security Framework

System Security	Weblogic Security	Database Security
98%	75%	83%



Drifted Targets

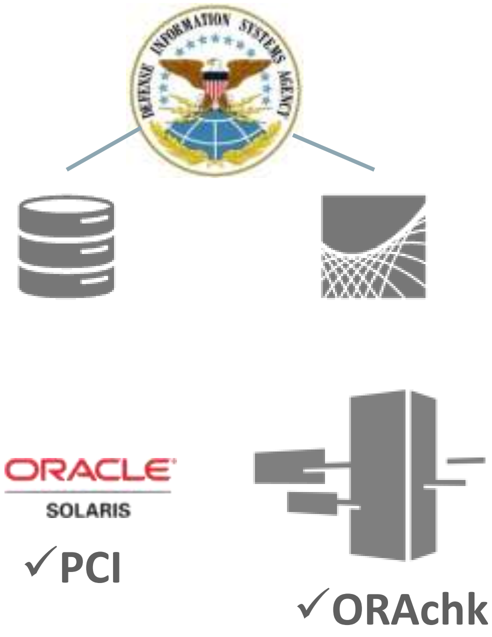
9

26% of the targets have drifted

Drift Monitored Targets 35

Ready to Use Compliance Standards

- Available Standards based on :
  - Oracle’s best practices and Security recommendations
  - Oracle Database and WebLogic STIG Benchmarks
  - ORAchk for Engineered Systems and Databases
- 1,000s of checks in Compliance Library
- Automated remediation with corrective actions NEW
- 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



Configuration & Compliance Management

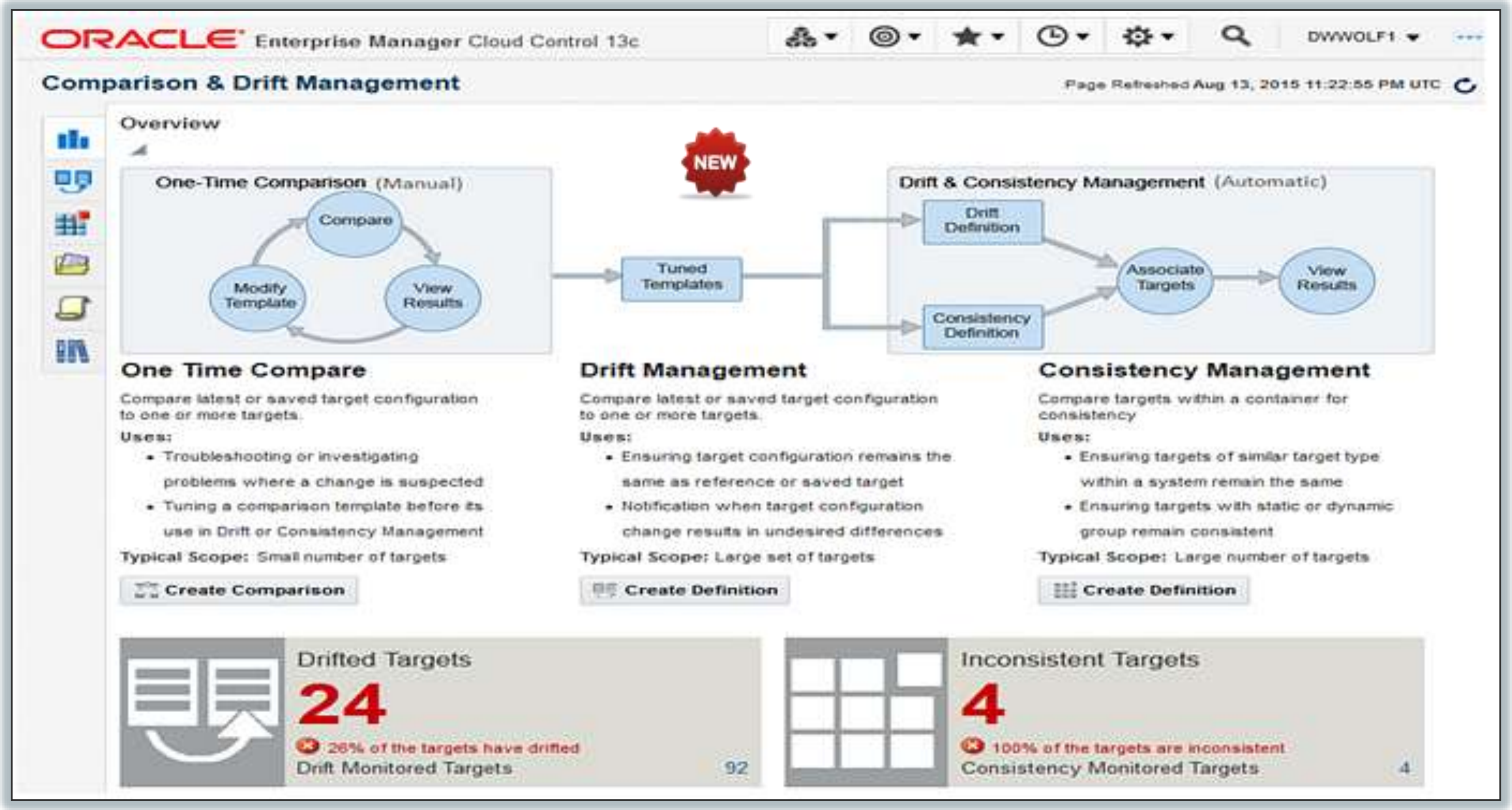
Key Features

Setup and Maintenance

- Comparison Templates – Ignore expected differences
- Group Association NEW
  - Current and future members
  - Supported – Admin, Dynamic, Static
- Test Mode NEW
  - Test Definition before mass deploy
  - Option for new group members can be tested before results added

Operational

- Summary Dashboards
  - Compliance and Drift NEW
- Side by Side Results NEW
  - Compare CIs across N targets in single view
- Incident Management Integration
  - Standard ruleset notification methodology
- Corrective Actions – Manual/Auto



Comparison & Drift Management

Page Refreshed Aug 13, 2015 11:22:55 PM UTC

One Time Compare

Compare latest or saved target configuration to one or more targets.

Uses:

- Troubleshooting or investigating problems where a change is suspected
- Tuning a comparison template before its use in Drift or Consistency Management

Typical Scope: Small number of targets

Create Comparison

Drift Management

Compare latest or saved target configuration to one or more targets.

Uses:

- Ensuring target configuration remains the same as reference or saved target
- Notification when target configuration change results in undesired differences

Typical Scope: Large set of targets

Create Definition

Consistency Management

Compare targets within a container for consistency

Uses:

- Ensuring targets of similar target type within a system remain the same
- Ensuring targets with static or dynamic group remain consistent

Typical Scope: Large number of targets

Create Definition

Drifted Targets

24

26% of the targets have drifted

Drift Monitored Targets 92

Inconsistent Targets

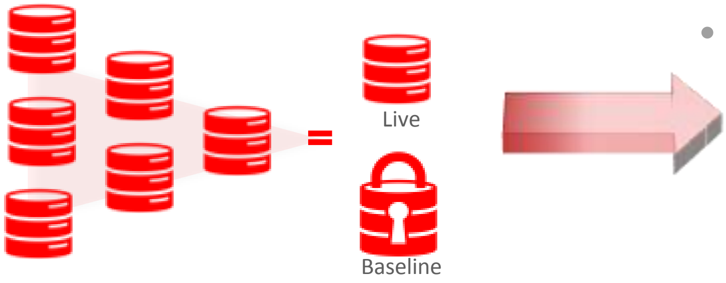
4

100% of the targets are inconsistent

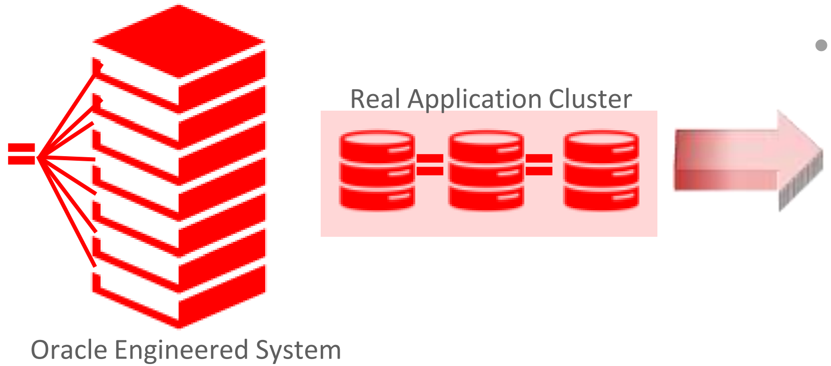
Consistency Monitored Targets 4

Drift and Consistency Management

NEW



- Drift Management – INTER Target
  - Large scale and dynamic INTER target configuration difference tracking
  - Source can be live or saved baseline



- Consistency Management – INTRA Target
  - Auto comparison of member targets
  - System targets only (Exadata, Cluster DB, etc)

Drift and Consistency Management

Key Customer Use Cases

Drift

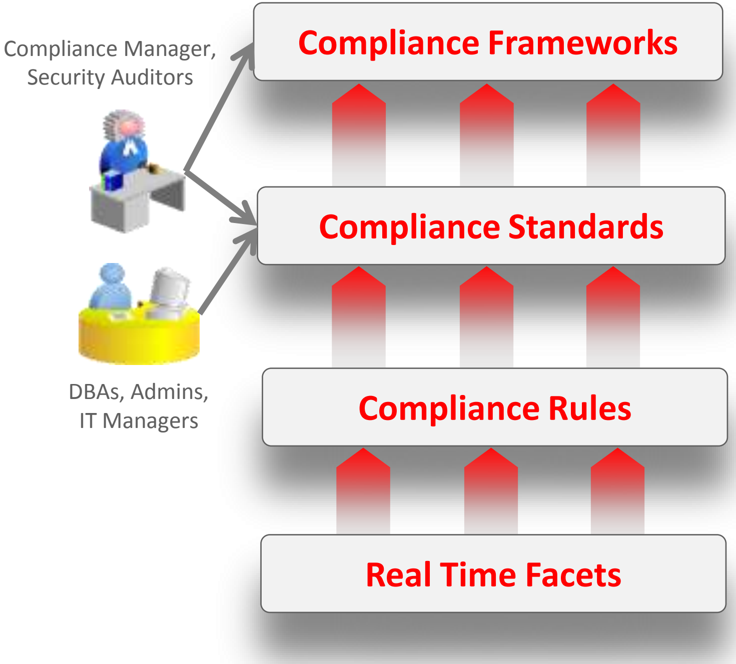
- DB Initialization Parameters
  - Saved DB Reference to 1200+ DBs
  - Compare 50 DB Initialization Parameters Only
- Application Patches
  - Live Fusion App Instance Ref to 1000+
  - Compare ONLY Patches
- Host Configuration
  - Live Linux Host Reference to 500+ Hosts
  - Compare Extended configuration collections

Consistency

- RAC DB Instances
  - Consistency of instances WITHIN 500+ Cluster DBs
- Data Guard Standbys
  - Consistency of Primary DB with it’s DG Standby Databases
  - 100s of DB systems
- Exadata Storage Cells
  - Consistency of Storage Cells within Exadata

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



Program Agenda

1. DBLM Overview
2. Database Provisioning
3. Patch Automation
4. Configuration Standardization
5. **STIG Compliance**

ORACLE

About STIGs

- STIGs - **S**ecurity **T**echnical **I**mplementation **G**uides
- Published by US **D**efense **I**nformation **S**ystems **A**gency
- According to the DISA website, "The STIGs contain technical guidance to 'lock down' information systems/software that might otherwise be vulnerable to a malicious computer attack."
- Available for Operating Systems, Applications(App Svr, **Databases**, etc) and much more.
- Who uses them?
  - Many US Government agencies are *required* to follow them.
  - Many US and non-US commercial companies *voluntarily* follow or base their internal standards on these benchmarks.

STIG Implementation Issues

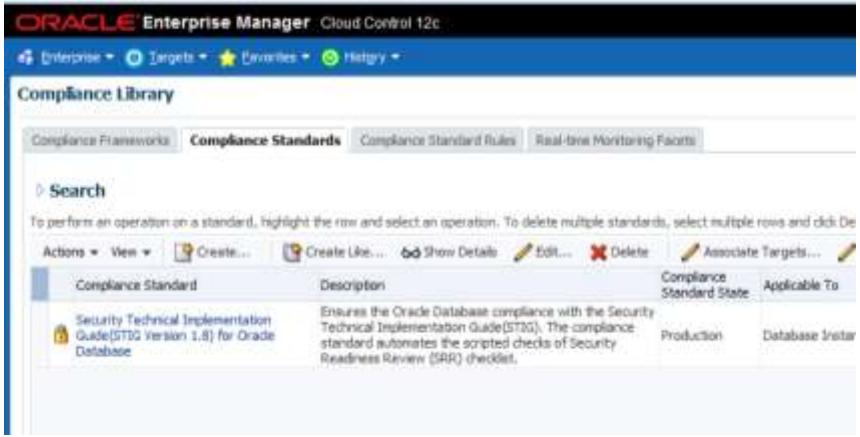
- Challenges
  - Mainly manual effort to check/validate conformance
  - Drift over time can result in undetected violations until checks repeated
  - Very costly and resource intensive to validate
- Requirement
  - Automated solution to continuously validate against the STIGs
  - Proactive alerting of change resulting in non-conformance

Oracle Database 11g STIG Compliance Standard

- What is it?
  - Turn key solution to automatically audit and report conformance of your Oracle 11g Databases against the STIG benchmark
  - Based on the DISA Security Technical Implementation Guide for Oracle Database 11g Version 1.8 Rev 1.8
- What do I need to use it?
  - Enterprise Manager and Agent must be 12.1.0.4 or later
- How is it licensed?
  - It is part of the Oracle Database Lifecycle Management Pack

Oracle Database 11g STIG Compliance Standard

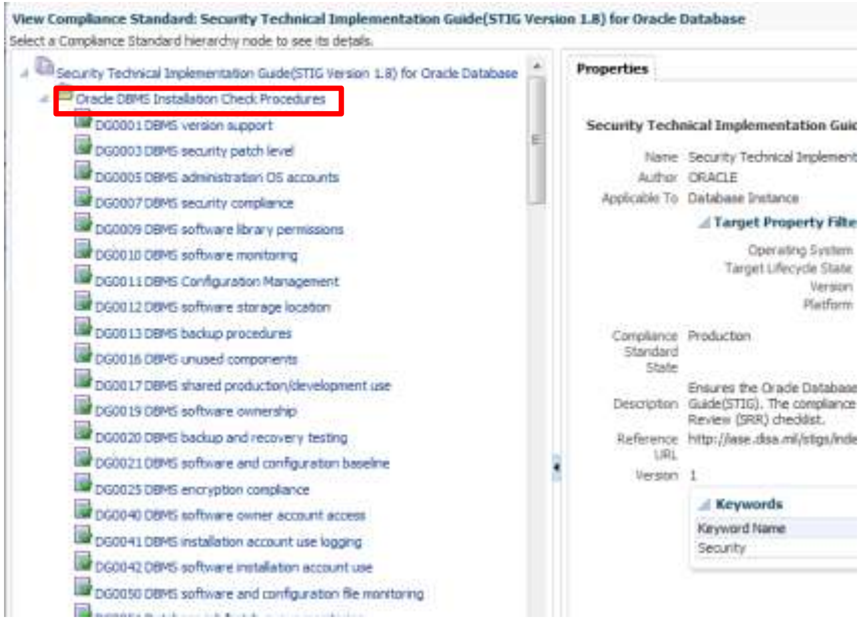
- Includes both Oracle Database and Oracle Home Checklists
- Almost all “Scripted” defined checks have been automated.
- ~20% Manual/Interview checks automated.
- Remaining require manual Attestation.



To perform an operation on a standard, highlight the row and select an operation. To delete multiple standards, select multiple rows and click De

Compliance Standard	Description	Compliance Standard State	Applicable To
Security Technical Implementation Guide(STIG Version 1.8) for Oracle Database	Ensures the Oracle Database compliance with the Security Technical Implementation Guide(STIG). The compliance standard automates the scripted checks of Security Readiness Review (SRR) checklist.	Production	Database Instar

Contains Oracle Database and Oracle Home Checks



View Compliance Standard: Security Technical Implementation Guide(STIG Version 1.8) for Oracle Database

Select a Compliance Standard hierarchy node to see its details.

- Security Technical Implementation Guide(STIG Version 1.8) for Oracle Database
  - Oracle DBMS Installation Check Procedures
    - DG0001 DBMS version support
    - DG0003 DBMS security patch level
    - DG0005 DBMS administration OS accounts
    - DG0007 DBMS security compliance
    - DG0009 DBMS software library permissions
    - DG0010 DBMS software monitoring
    - DG0011 DBMS Configuration Management
    - DG0012 DBMS software storage location
    - DG0013 DBMS backup procedures
    - DG0016 DBMS unused components
    - DG0017 DBMS shared production/development use
    - DG0019 DBMS software ownership
    - DG0020 DBMS backup and recovery testing
    - DG0021 DBMS software and configuration baseline
    - DG0025 DBMS encryption compliance
    - DG0040 DBMS software owner account access
    - DG0041 DBMS installation account use logging
    - DG0042 DBMS software installation account use
    - DG0050 DBMS software and configuration file monitoring

Properties

Security Technical Implementation Guid

Name: Security Technical Implement
Author: ORACLE
Applicable To: Database Instance

Target Property Filte

Operating System
Target Lifecycle State
Version
Platform

Compliance Standard State: Production

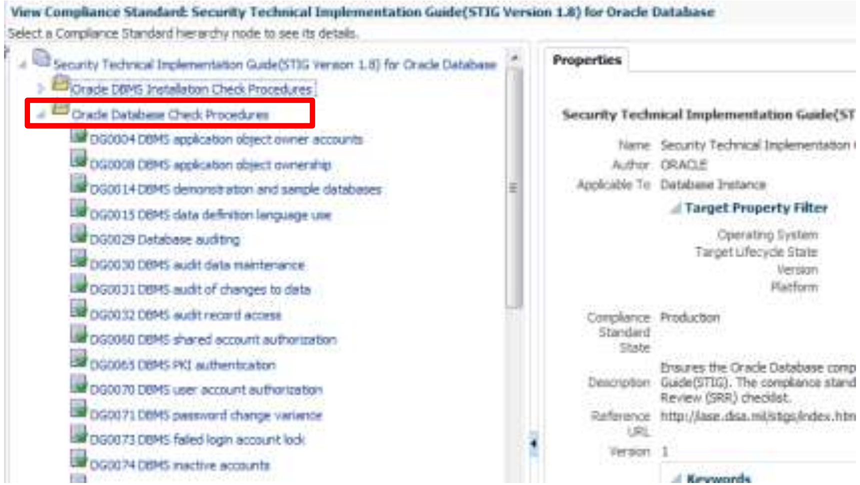
Description: Ensures the Oracle Database Guide(STIG). The compliance Review (SRR) checklist.

Reference URL: http://iase.disa.mil/stigs/inde

Version: 1

Keywords

Keyword Name
Security



View Compliance Standard: Security Technical Implementation Guide(STIG Version 1.8) for Oracle Database

Select a Compliance Standard hierarchy node to see its details.

- Security Technical Implementation Guide(STIG Version 1.8) for Oracle Database
  - Oracle DBMS Installation Check Procedures
  - Oracle Database Check Procedures
    - DG0004 DBMS application object owner accounts
    - DG0008 DBMS application object ownership
    - DG0014 DBMS demonstration and sample databases
    - DG0015 DBMS data definition language use
    - 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
    - DG0063 DBMS PKI authentication
    - DG0070 DBMS user account authorization
    - DG0071 DBMS password change variance
    - DG0073 DBMS failed login account lock
    - DG0074 DBMS inactive accounts

Properties

Security Technical Implementation Guide(ST

Name: Security Technical Implementation
Author: ORACLE
Applicable To: Database Instance

Target Property Filter

Operating System
Target Lifecycle State
Version
Platform

Compliance Standard State: Production

Description: Ensures the Oracle Database comp Guide(STIG). The compliance stand Review (SRR) checklist.

Reference URL: http://iase.disa.mil/stigs/index.htm

Version: 1

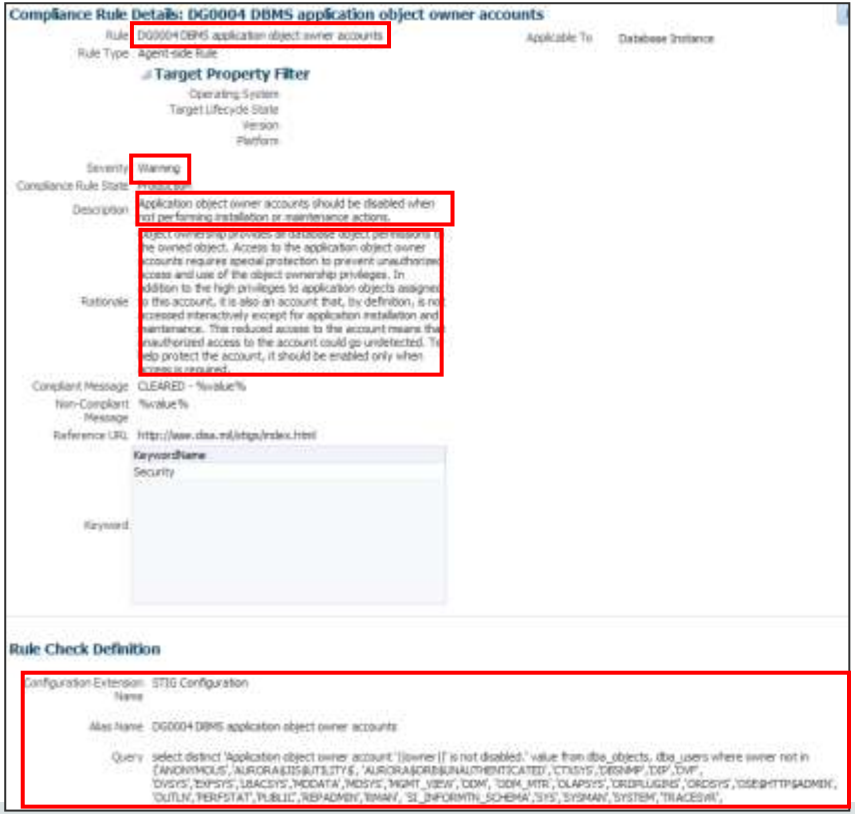
Keywords

Compliance Rule to STIG Mapping

Compliance Rule Type	STIG Check
Agent-Side	Script
Manual	Manual/Interview

Compliance Rule	STIG Check
Name	STIG ID + Description
Severity	Severity
Description	Check Long Name
Rationale	Vulnerability Discussion
Configuration Extension	Script

* Exceptions Noted in *Oracle Database Compliance Standards* Reference guide in EM Documentation



Compliance Rule Details: DG0004 DBMS application object owner accounts

Rule: DG0004 DBMS application object owner accounts

Applicable To: Database Instance

Rule Type: Agent-side Rule

Target Property Filter

Operating System

Target Lifecycle State

Version

Platform

Severity: Warning

Compliance Rule State: Production

Description: Application object owner accounts should be disabled when not performing installation or maintenance actions.

Rationale: Object ownership provides all database object permissions to the owned object. Access to the application object owner accounts requires special protection to prevent unauthorized access and use of the object ownership privileges. In addition to the high privileges to application objects assigned to this account, it is also an account that, by definition, is not accessed interactively except for application installation and maintenance. This reduced access to the account means that unauthorized access to the account could go undetected. To help protect the account, it should be enabled only when access is required.

Compliant Message: CLEARED - %value%

Non-Compliant Message: %value%

Reference URL: http://iase.disa.mil/stigs/index.html

KeywordName
Security

Keyword

Rule Check Definition

Configuration Extension Name: STIG Configuration

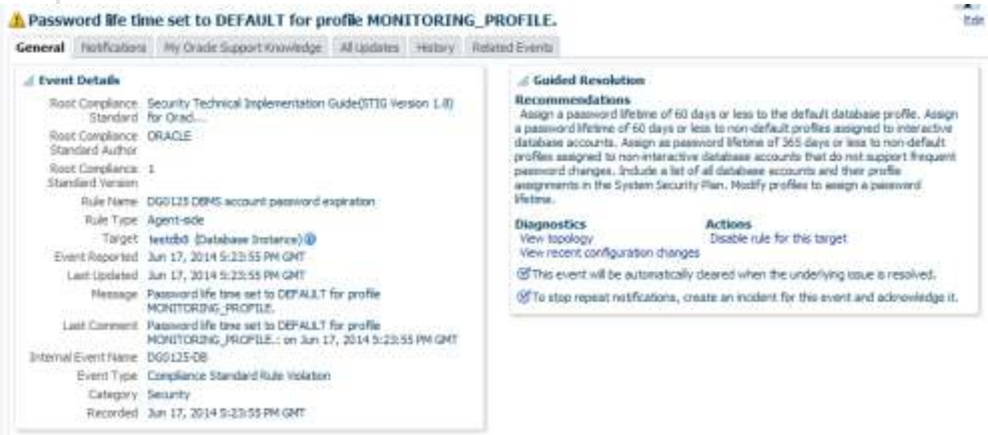
Alias Name: DG0004 DBMS application object owner accounts

Query:

```
select distinct 'Application object owner account '||owner||' is not disabled.' value from dba_objects, dba_users where owner not in
('ANONYMOUS','AURORA$JIS$UTILITY$','AURORA$ORB$UNAUTHENTICATED','CTXSYS','DBSNMP','DIP','DVF',
'DVSYS','EXFSYS','LBACSYS','MDDATA','MDSYS','MGMT_VIEW','ODM','ODM_MTR','OLAPSYS','ORDPLUGINS','ORDSYS','OSE$HTTP$ADMIN',
'OUTLN','PERFSTAT','PUBLIC','REPADMIN','RMAN','SI_INFORMTN_SCHEMA','SYS','SYSMAN','SYSTEM','TRACESVR',
```

Detailed and Actionable Findings

- Findings include violation context
  - Offending database
  - Specific Check findings
  - Date discovered
  - Guided Resolution
- Recommendation offered (as per STIG documentation.)



Password life time set to DEFAULT for profile MONITORING_PROFILE.

Event Details

Root Compliance Standard	Security Technical Implementation Guide(STIG Version 1.8) for Oracl...
Root Compliance Standard Author	ORACLE
Root Compliance Standard Version	1
Rule Name	DG0125 DBMS account password expiration
Rule Type	Agent-side
Target	testdb0 (Database Instance)
Event Reported	Jun 17, 2014 5:23:55 PM GMT
Last Updated	Jun 17, 2014 5:23:55 PM GMT
Message	Password life time set to DEFAULT for profile MONITORING_PROFILE.
Last Comment	Password life time set to DEFAULT for profile MONITORING_PROFILE.: on Jun 17, 2014 5:23:55 PM GMT
Internal Event Name	DG0125-DB
Event Type	Compliance Standard Rule Violation
Category	Security
Recorded	Jun 17, 2014 5:23:55 PM GMT

Guided Resolution

Recommendations

Assign a password lifetime of 60 days or less to the default database profile. Assign a password lifetime of 60 days or less to non-default profiles assigned to interactive database accounts. Assign as password lifetime of 365 days or less to non-default profiles assigned to non-interactive database accounts that do not support frequent password changes. Include a list of all database accounts and their profile assignments in the System Security Plan. Modify profiles to assign a password lifetime.

Diagnostics

View topology

View recent configuration changes

Actions

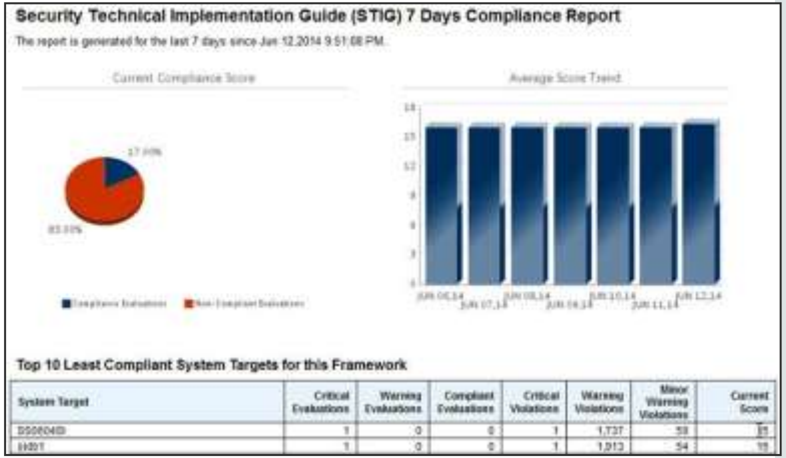
Disable rule for this target

This event will be automatically cleared when the underlying issue is resolved.

To stop repeat notifications, create an incident for this event and acknowledge it.

Reporting – Flexible and Integrated

- Results viewable:
  - Across Databases
  - For single Database
  - For single Check
- Historical trend and score information
- Schedule and Email
- Formats – PDF, HTML, CSV

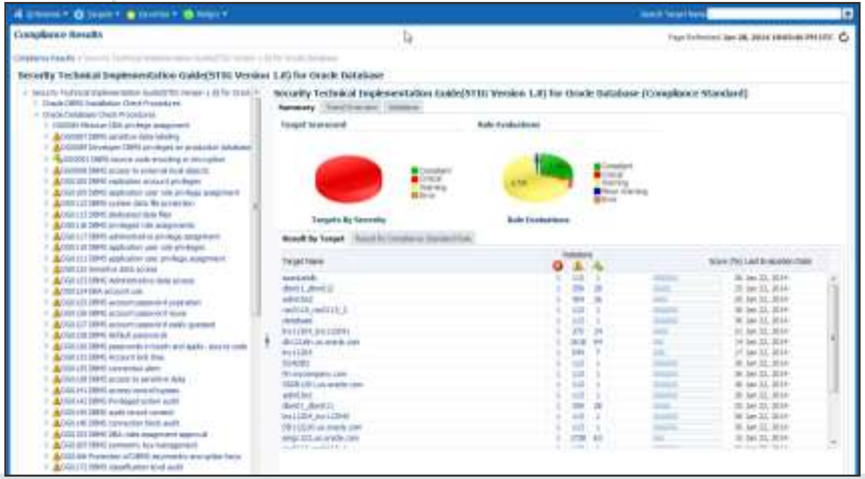


Security Technical Implementation Guide (STIG) 7 Days Compliance Report

The report is generated for the last 7 days since Jun 12,2014 9:51:08 PM.

Top 10 Least Compliant System Targets for this Framework

System Target	Critical Evaluations	Warning Evaluations	Compliant Evaluations	Critical Violations	Warning Violations	Minor Warning Violations	Current Score
DS0604DI	1	0	0	1	1,737	58	15
IHD01	1	0	0	1	1,913	54	15



Compliance Results

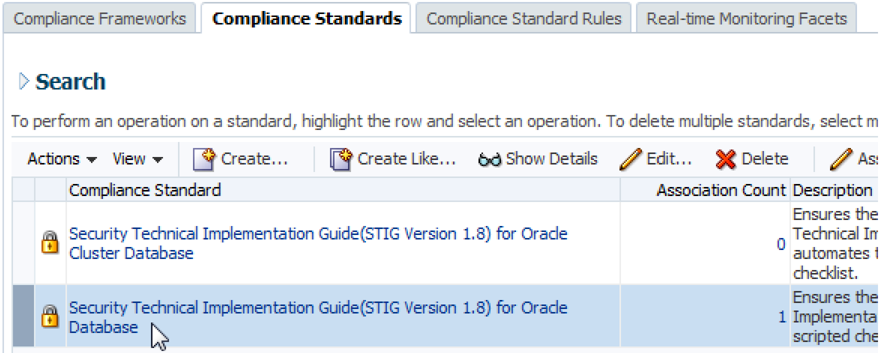
Security Technical Implementation Guide(STIG Version 1.8) for Oracle Database

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

Simple and Easy to Use

- Two Simple Steps
  1. Select Standard
  2. Select Targets
- Results – Almost Immediately
- Check run daily (by default)
- Configurable Notification on violation

1.

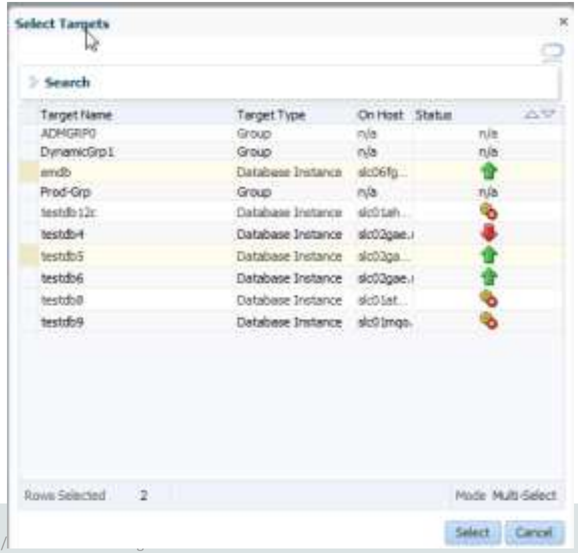


Search

To perform an operation on a standard, highlight the row and select an operation. To delete multiple standards, select m

Compliance Standard	Association Count	Description
Security Technical Implementation Guide(STIG Version 1.8) for Oracle Cluster Database	0	Ensures the Technical Im automates t checklist.
Security Technical Implementation Guide(STIG Version 1.8) for Oracle Database	1	Ensures the Implementa scripted che

2.



Target Name	Target Type	On Host	Status
ADMGRP0	Group	n/a	n/a
DynamicGrp1	Group	n/a	n/a
emdb	Database Instance	slc06fg...	↑
Prod-Grp	Group	n/a	n/a
testdb12c	Database Instance	slc01ah...	●
testdb4	Database Instance	slc02gae.i	↓
testdb5	Database Instance	slc02ga...	↑
testdb6	Database Instance	slc02gae.i	↑
testdb8	Database Instance	slc01at...	●
testdb9	Database Instance	slc01mqs.	●

Rows Selected 2

Mode Multi-Select

Enterprise Manager – Single Compliance Solution for Cloud

For Automated Security Compliance Auditing

- ☑ Highly automated
- ☑ Continuous auditing
- ☑ Proactively alert on findings and issues
- ☑ Automated remediation or guidance
- ☑ Robust and flexible reporting

ORACLE®