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, timing, and pricing of any features or functionality described for Oracle's products may change and remains at the sole discretion of Oracle Corporation.

ORACLE

Detect, Protect, Predict

Oracle Enterprise Manager: Database Lifecycle Management

Martin Peña
Senior Director,
Product Management

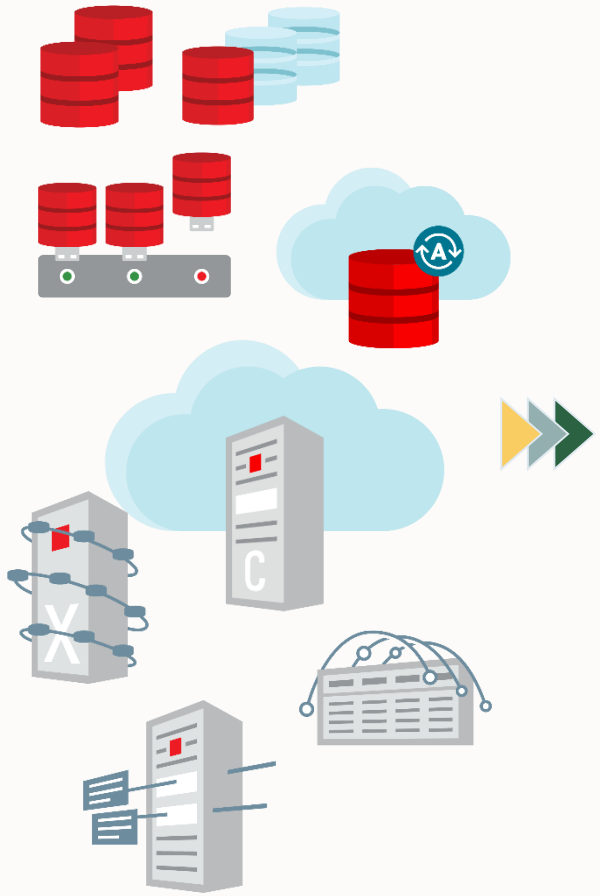
Pankaj Chandiramani
Director, Product
Management

Harish Niddagatta
Senior Principal
Product Manager

Agenda

1. Enterprise Manager Overview
2. Security Challenges
3. Fleet Maintenance
4. Compliance Management
5. Q&A

Monitoring, Management and Control for Oracle Database and Engineered Systems: Enterprise Manager



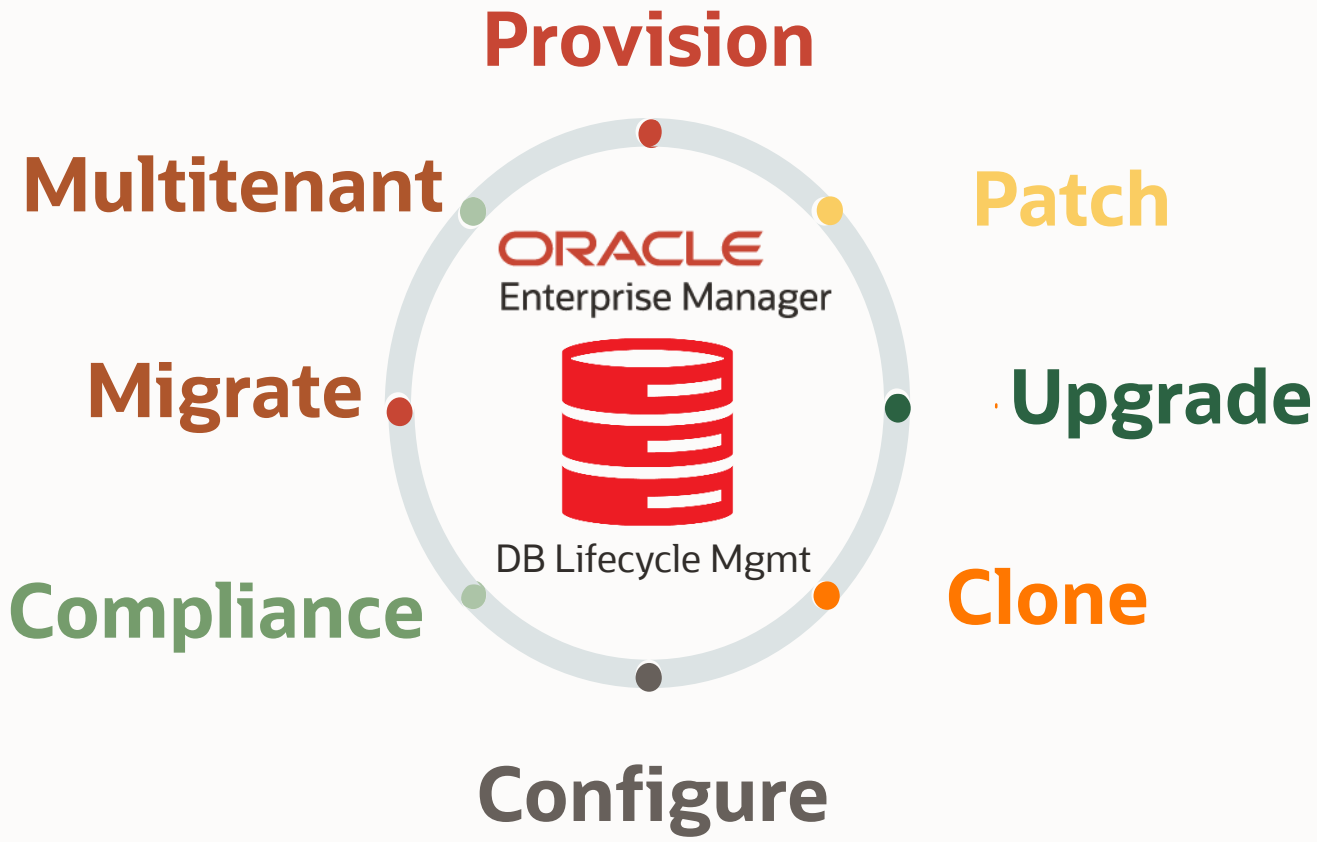
ORACLE
Enterprise Manager

- Comprehensive management for Oracle Database and Oracle Engineered Systems
- Fleet-wide automation and visibility across Oracle cloud and on-premises assets
- Centralized control of integrated diagnostic, tuning and lifecycle activities

Database Lifecycle Management Pack Overview

Comprehensive solution that helps database, system and application administrators automate the processes required to manage the Oracle Database Lifecycle.

Eliminates manual and time consuming tasks related to discovery, initial provisioning, patching, configuration management, and ongoing change management.



Today's Security Challenges

Unknown Security Vulnerabilities

Undetected insecure changes increases the risk of security exposure

Security Patches Not Applied

Complexity of task makes admins not want to bother

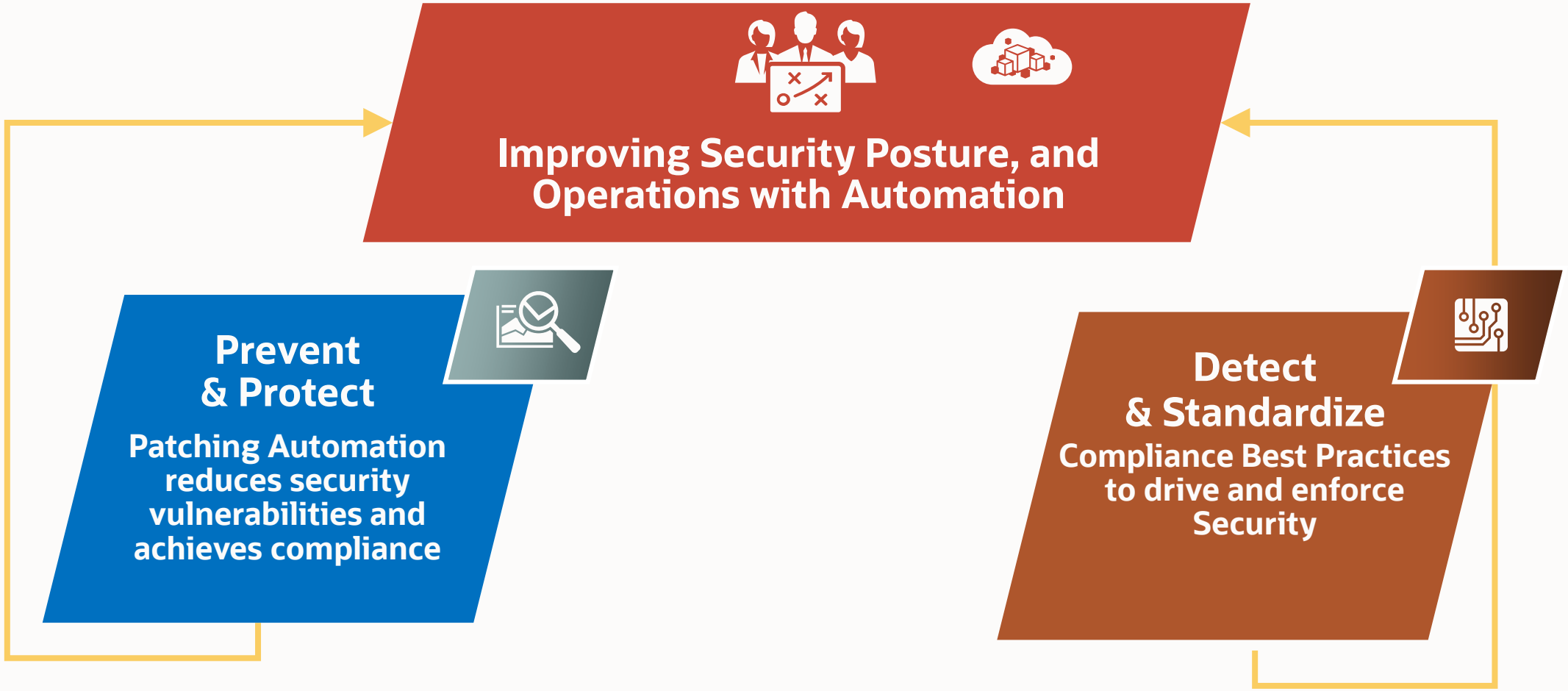
Unprotected Data

Thousands of databases with unprotected sensitive data; limited auditing, privileges and security policies

Lack of Enterprise-wide Tools

Complexity in assessing databases for security posture

Database Lifecycle Management for Security



Fleet Maintenance

Patching automation reduces security vulnerabilities and achieves compliance

Why do you “need” to Patch and Upgrade your database estate?

The biggest reason is **SECURITY**!

In 2019, there were more than 4,000 publicly disclosed breaches, exposing 8 billion compromised records, including addresses, credit card numbers and phone numbers.

Security | Why Patch and Upgrade Database

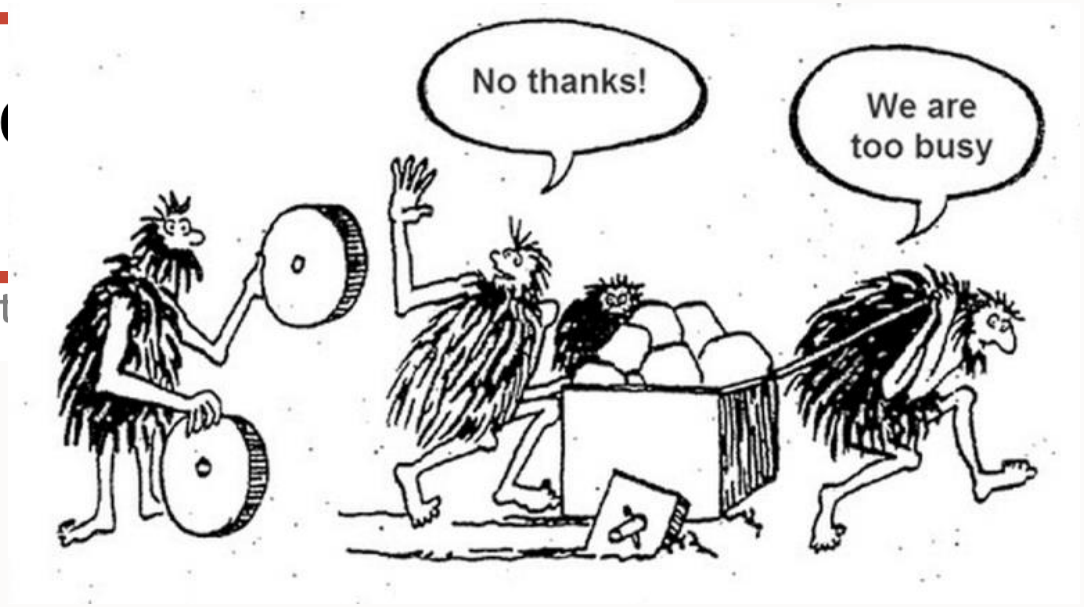
COMPUTERWORLD UNITED STATES WINDOWS MOBILE OFFICE SOFTWARE APPLE SHARK TANK EVENTS RESOURCE LIBR

Home > Security

NEWS

Update: Two-thirds of Ora security patches

Complexity of task makes admins not want t



Challenges with Typical Patch Management Process

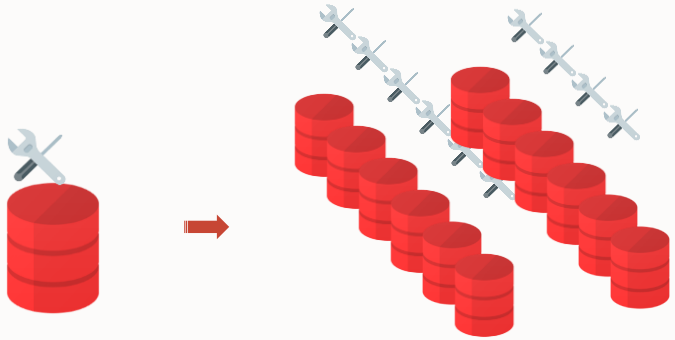
Complex, time consuming and multiple stakeholder dependency

High Downtime

Lack of standardization makes patching success unpredictable

Fleet Maintenance using EM | Key Attributes

Automated to achieve minimum downtime



Scalable

Production-ready

Increase productivity, Achieve enterprise goals, Innovate more

Database Patching and Upgrade using Fleet Maintenance

Automated, Scalable Patching and Upgrades

- Out-of-place solution for both patching and upgrades
- Subscription-based software maintenance reduces maintenance windows
- Scalable: Patch ~100 Clusters-~1000 DBs in a single patching window
- Supports PSU, RU's and all DB versions from 11.2.0.4

Software Standardization Advisor

- Scans environment for the unique patching configurations
- Recommends standardized configurations and lists all the Oracle Homes on which the configurations should be applied

Database Patching and Upgrade using Fleet Maintenance

Enhanced Patching Operations

- Visual patch tracking
- Inject and automate environmental specific customizations.
- Supports Rollback
- Self service option available for application teams who want to choose their own patching window.

Complete Native Integration with EM

- Leverages EM blackouts for targets being patched to avoid unwanted notification/alerts.
- Leverages EM Named Credentials and privilege delegation for better and secure credential management.

Database Fleet Maintenance

Simplified Software Configuration Standardization at Scale

Discover Configuration Pollution

a. Run Advisor to analyze the database estate
b. Identify required standard configurations
c. Prepare Reference environments for each standard configuration

Create Gold Image

a. List available images
b. List versions of an image
c. Make a version “Current”

Subscribe Databases to a Gold Image

a. List subscriptions of an image
b. Validate subscriptions

Deploy Image

a. Shadow Home is created

Switch Database

a. Migrate Listener
b. Update Database: SI, GI, RAC, Standby

Database Fleet Maintenance

Detect “Configuration Pollution”

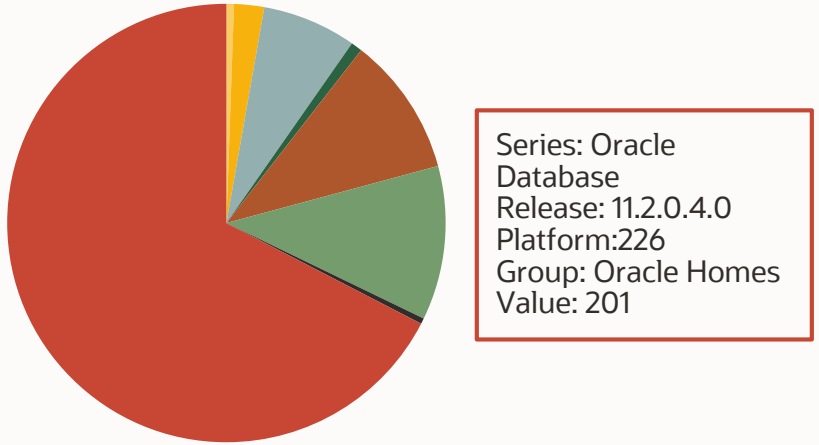
Advisor scans the fleet for configuration variations provides recommendations to standardize.

Analysis of Your Enterprise (2693 database installations)

Current Software Configurations (295)

Analysis:
1 in every 6 Oracle Home are different

Recommended Software Configurations (8)



Criteria Used:
Platform, Release, Product

To get started, use Database Image Advisor. The database image advisor helps you group database and define an image for each group.

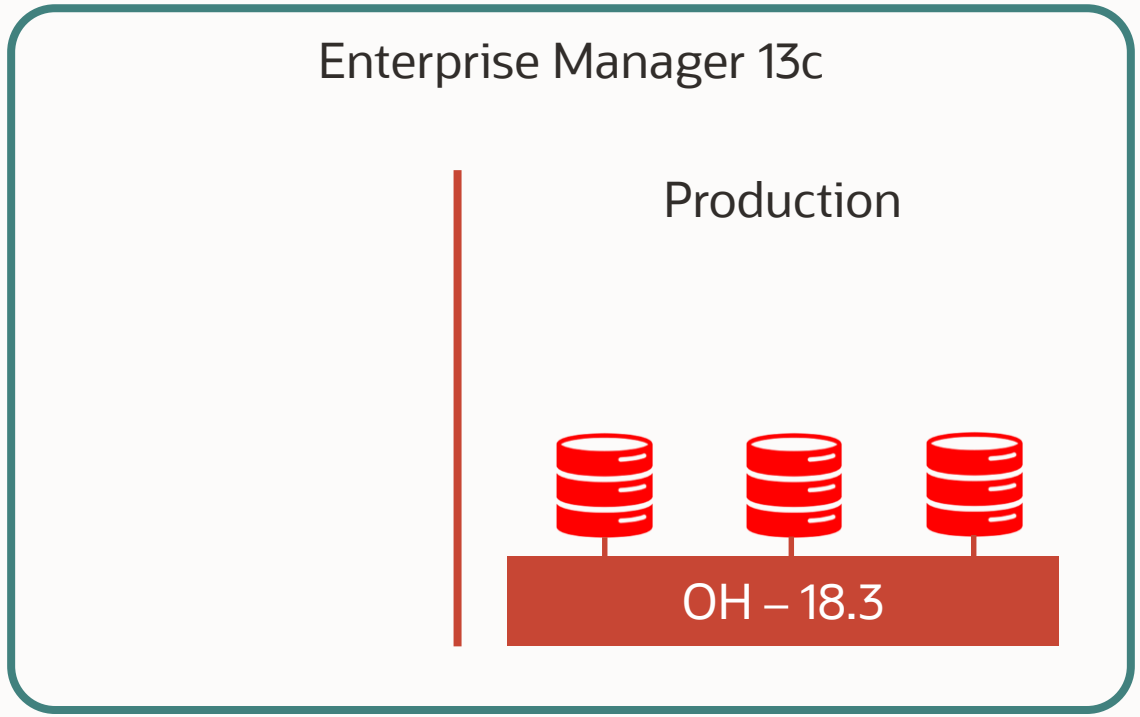
Fleet Maintenance – Simplified Gold Image Creation

Enterprise Manager has flexible options to create the gold image for Fleet Maintenance:

- Option 1 : Create gold image by pointing to existing pre-patched Oracle Home
- Option 2 : EM can clone existing Oracle Home and apply patches to create gold image
- Option 3 : EM can deploy existing gold image and then apply patches to that to create an updated gold image .
- Option 4 : EM can apply patches to existing Oracle Home (empty , if they are pre provisioned) and then create the gold image
- Option 5 : EM can export-import the gold images across EM's

Database Fleet Maintenance – Process

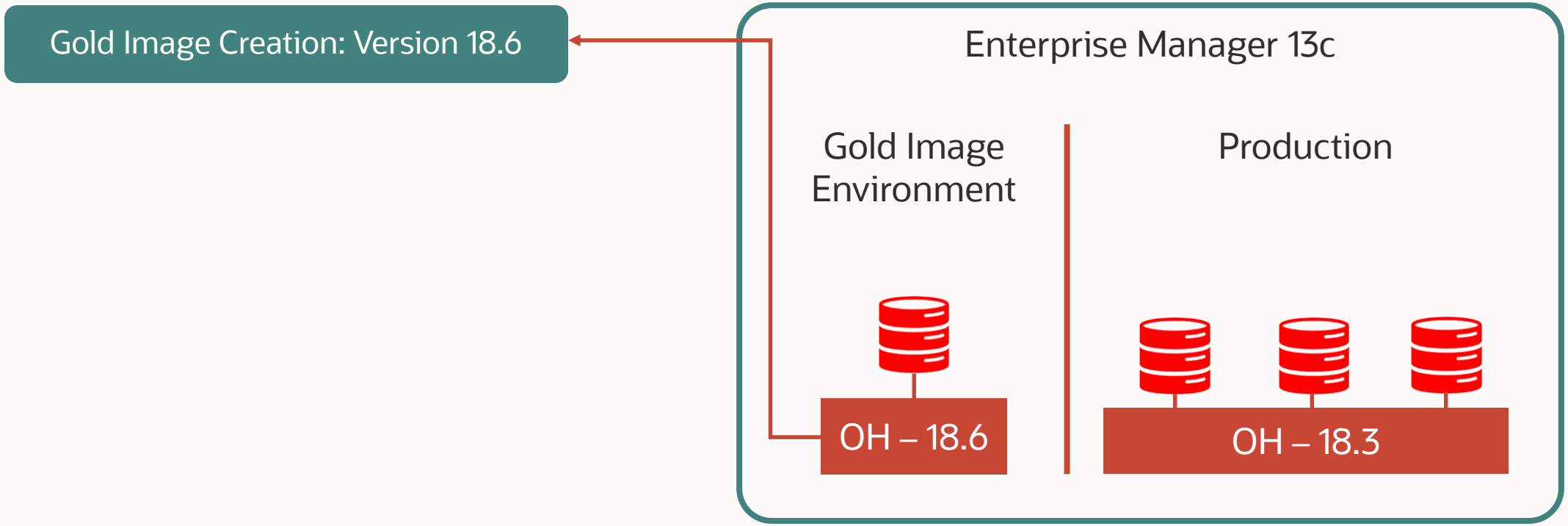
Patching Cycle 1 Goal: Patch Production 18.3 DBs to 18.6



*OH = Database Oracle Home

Database Fleet Maintenance – Process

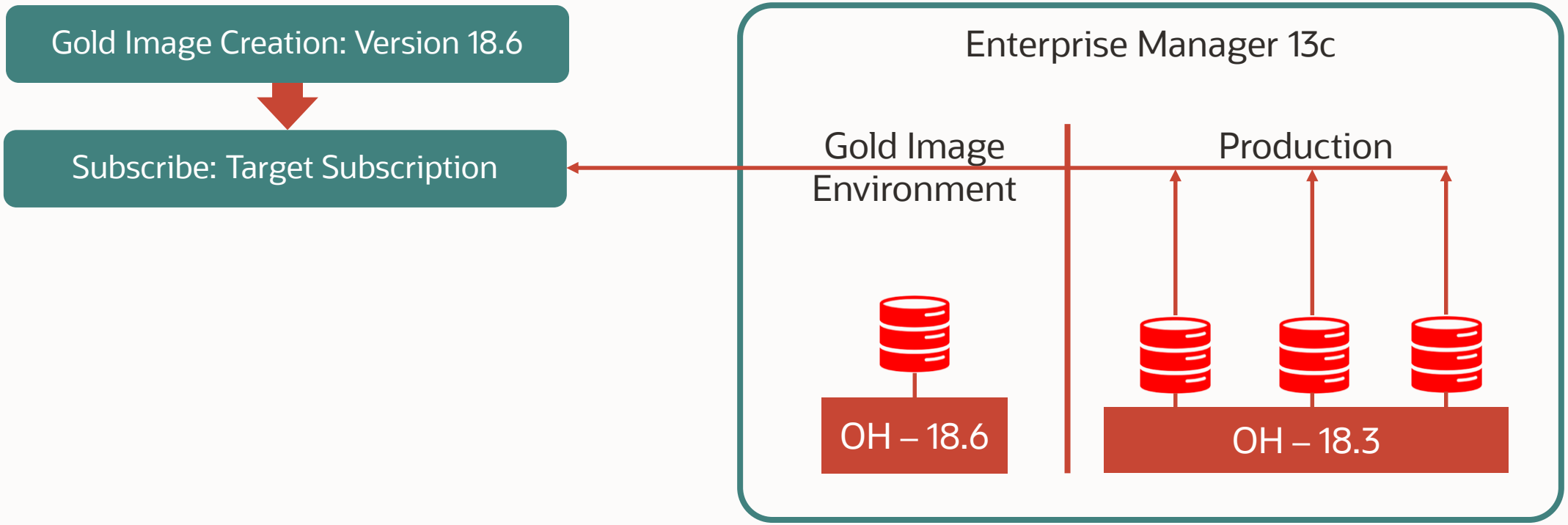
Patching Cycle 1 Goal: Patch Production 18.3 DBs to 18.6



*OH = Database Oracle Home

Database Fleet Maintenance – Process

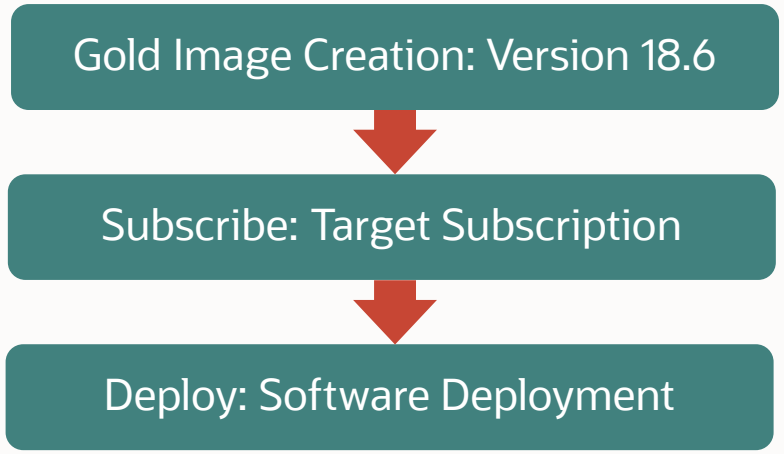
Patching Cycle 1 Goal: Patch Production 18.3 DBs to 18.6

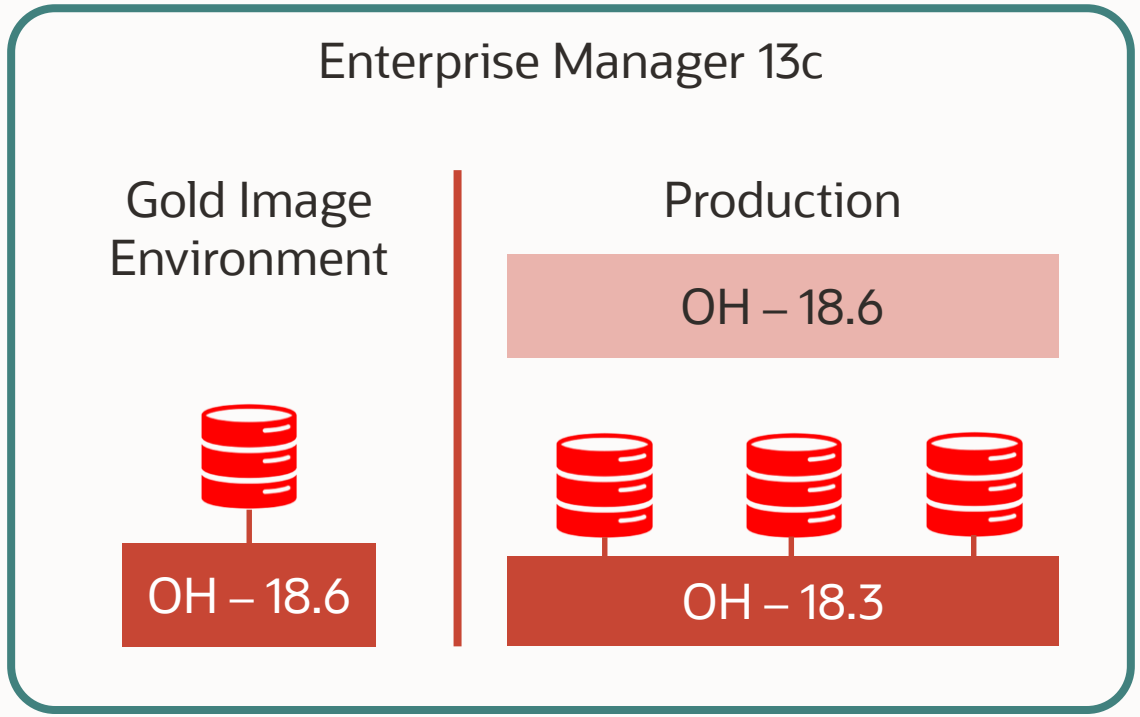


*OH = Database Oracle Home

Database Fleet Maintenance – Process

Patching Cycle 1 Goal: Patch Production 18.3 DBs to 18.6

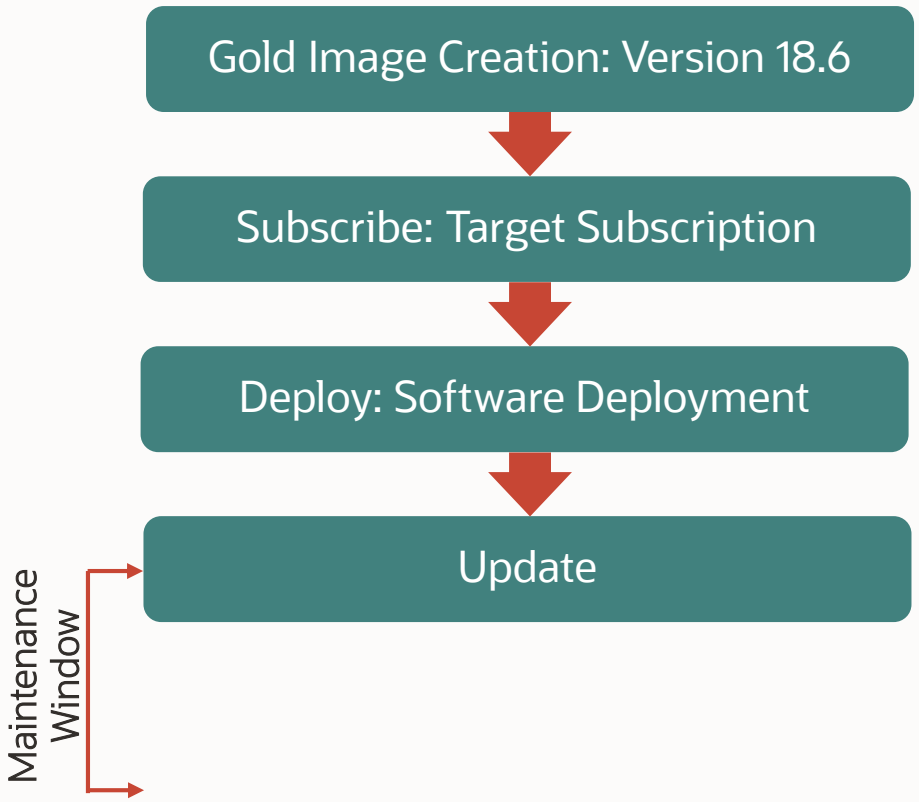


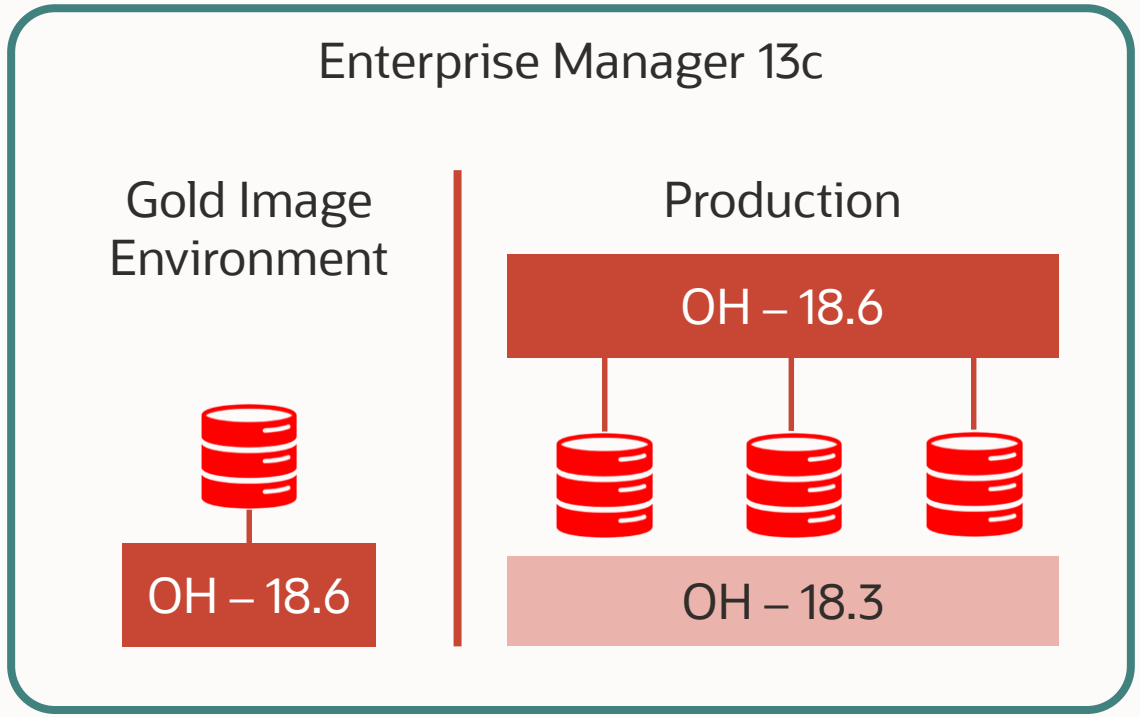


*OH = Database Oracle Home

Database Fleet Maintenance – Process

Patching Cycle 1 Goal: Patch Production 18.3 DBs to 18.6

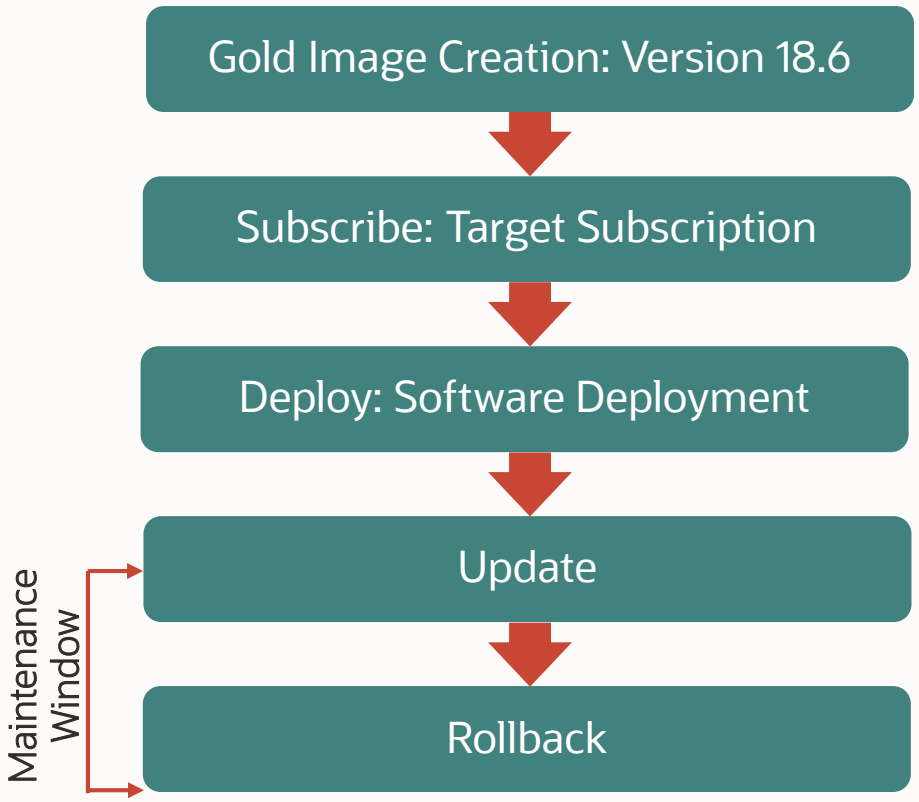


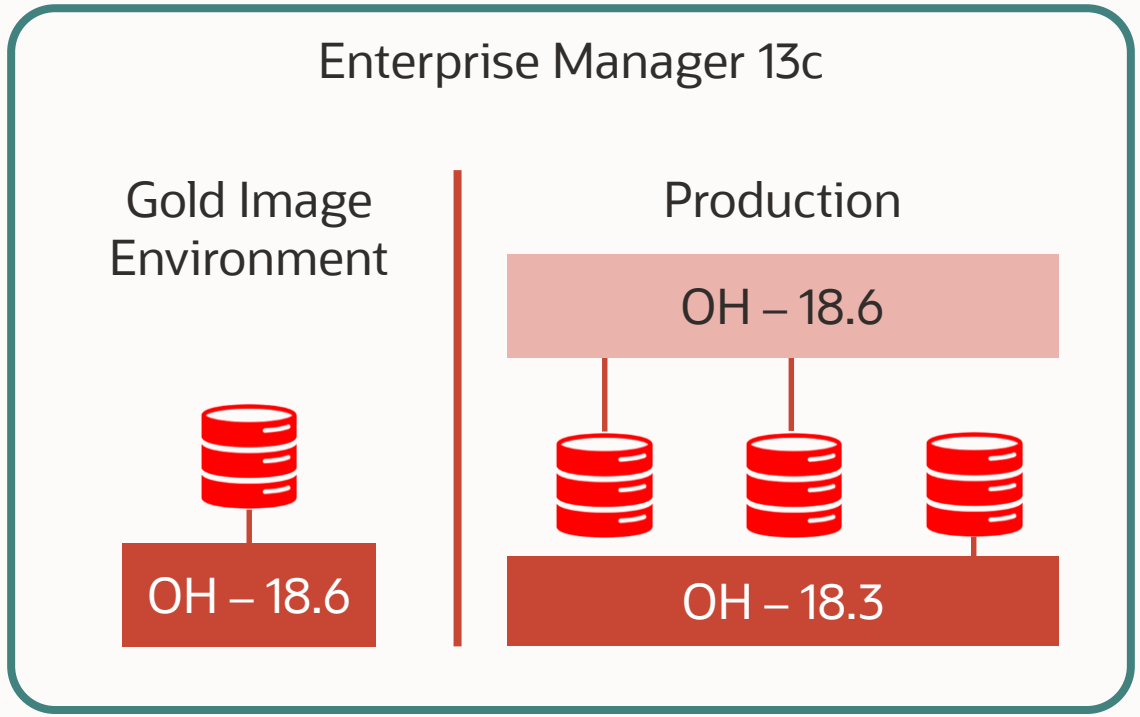


*OH = Database Oracle Home

Database Fleet Maintenance – Process

Patching Cycle 1 Goal: Patch Production 18.3 DBs to 18.6

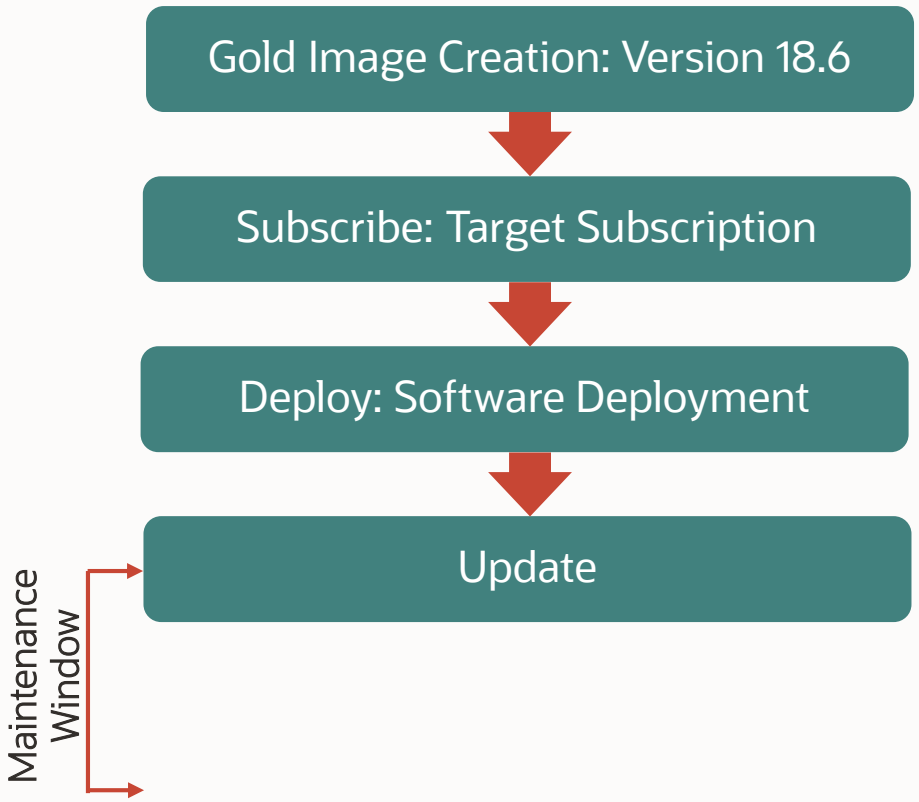


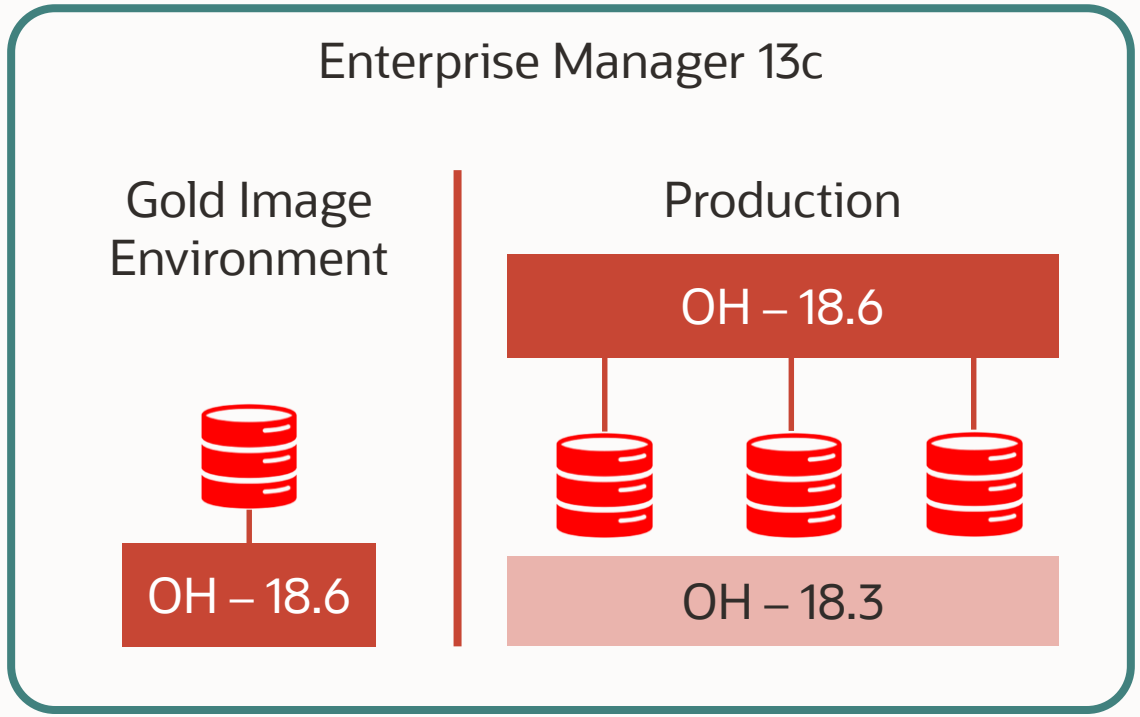


*OH = Database Oracle Home

Database Fleet Maintenance – Process

Patching Cycle 1 Goal: Patch Production 18.3 DBs to 18.6

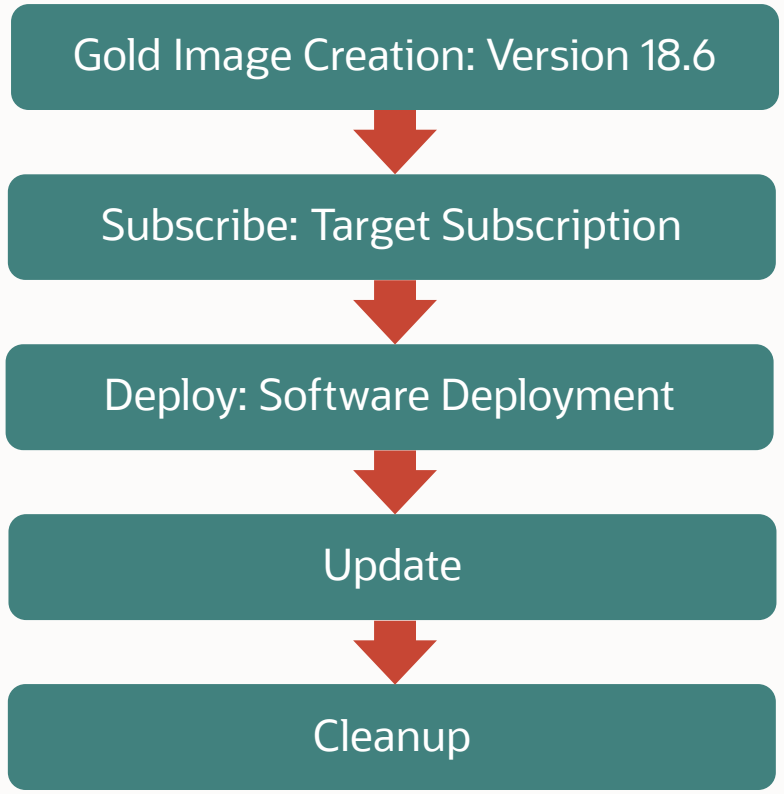


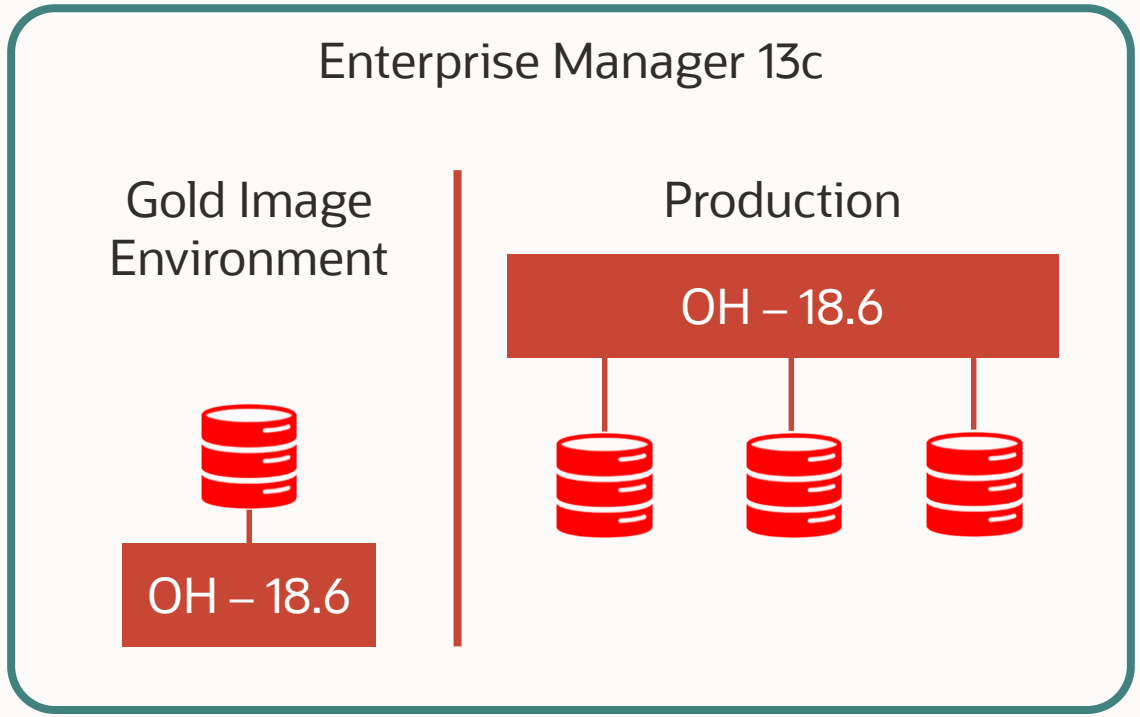


*OH = Database Oracle Home

Database Fleet Maintenance – Process

Patching Cycle 1 Goal: Patch Production 18.3 DBs to 18.6

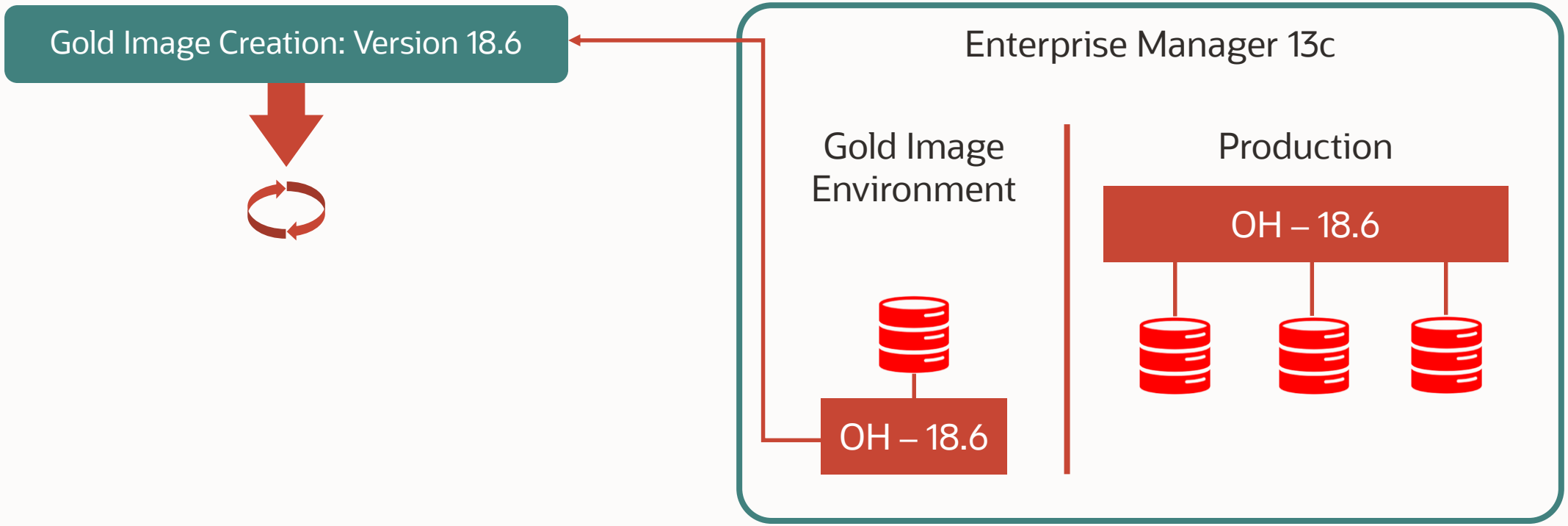




*OH = Database Oracle Home

Database Fleet Maintenance – Process

Patching Cycle 2 Goal: Patch Production 18.6 DBs to 18.7

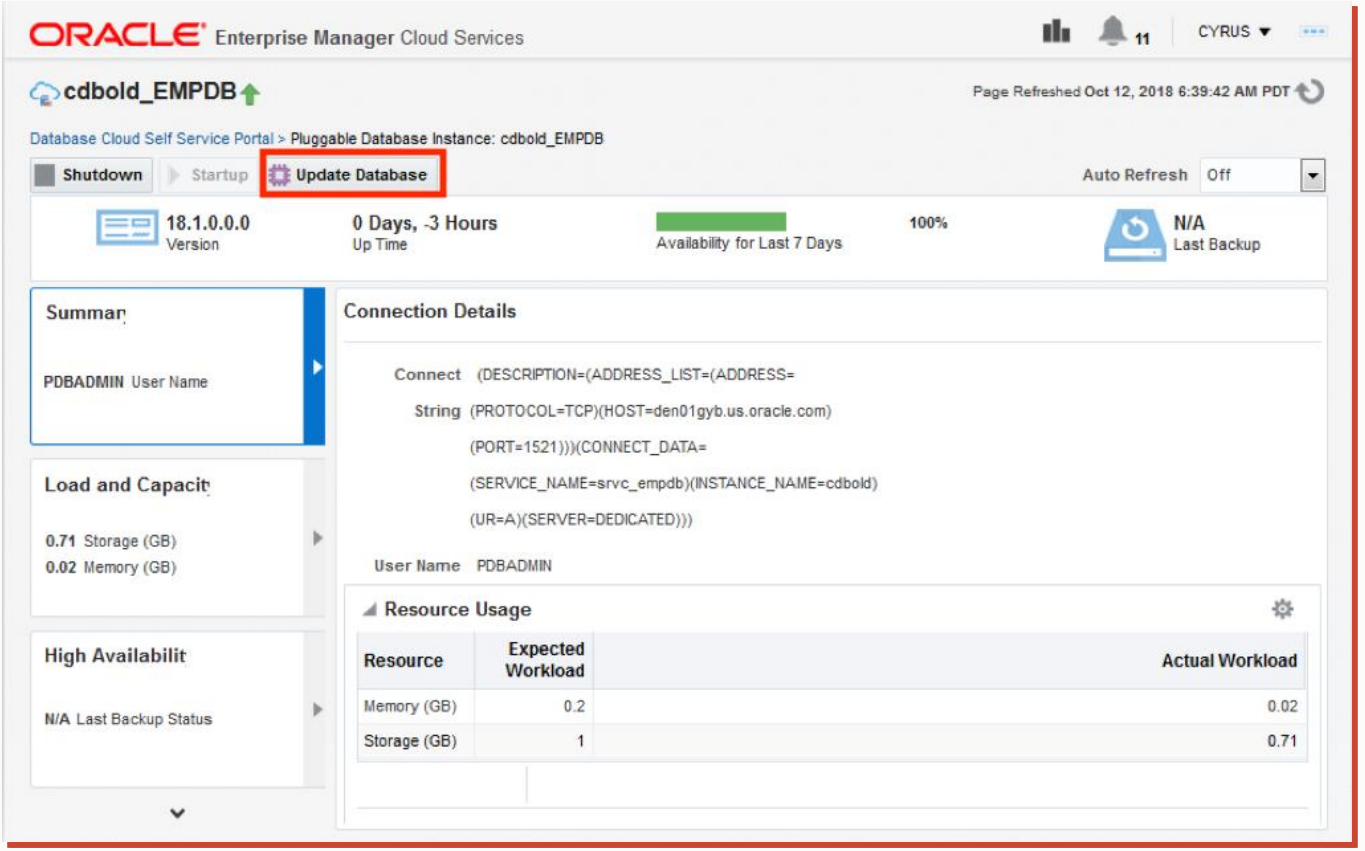


*OH = Database Oracle Home

Self Service Portal: Fleet Maintenance

Patch Self Service Databases in convenient Patching Window

- Fleet Maintenance integration with Self Service Portal
- Update Database allows application administrators to patch Self Service databases in convenient patching window
- Update Database relocates PDB to new CDB
- REST APIs for integrating with 3rd party applications



Fleet Maintenance

New Enterprise Manager 13.4 Features (**Enhancements)**

- Minimize downtime using Rolling Patching for Oracle DB Embedded JVM (OJVM) – OJVM rolling patches including support drain-timeout
- Export - Import Gold images between EM's
- Ability to run pre and post scripts as Root
- Ability to patch databases with Transparent Data Encryption(TDE)
- Enhancements to Gold Image creation - added capability to apply patches during creation of gold image (now you don't need a pre patched system)
- Emergency Patching - applying one off patches without creating gold images .

Security Compliance Management

Compliance Best Practices to drive and enforce Security

Today's Security Challenges

Weak account controls and audits

- Insecure user accounts, no limits on privileges and roles leads to accessing restricted tables
- Lack of auditing database activities means no visibility into compliance

Unprotected Data

- Thousands of databases with unprotected sensitive data
- Lack of security policies to protect tables with sensitive data elevates vulnerability

Unknown Security Vulnerabilities

- Undetected insecure configuration changes increase the risk of security exposure
- Limited visibility into com

Lack of Enterprise-wide Tools

- Complexity in monitoring and assessing databases for security posture
- Hard to remediate non-compliance

Security Compliance Pain Points

CISO, CIO, CFO, Auditors

How do I know databases are Complaint with Security policy?

Is the compliance posture sufficiently improving?

What do I need to do to fix SLAs Violations?

Information Security Officer

Am I meeting my LOB compliance SLAs for Finance and HR specific database instances?

Current security posture of database instances?

Are my resources deployed effectively to ensure compliance?

Administrator or IT Compliance Analyst

What violations do I need to remediate at this moment?

What vulnerability do I fix next based on prioritization & risk level?

How do I remediate violations?

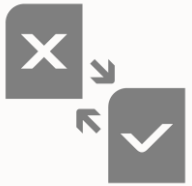
Security Compliance Management with Enterprise Manager

Continuous Security & Compliance Management

Secure Database

Automated Remediation via Corrective Actions

Violation Notification



At Scale

Homogenous, Heterogenous targets

Ready to use Standards

Out-of-box Industry Standards and Best Practices

Ready to Use Compliance Security Standards

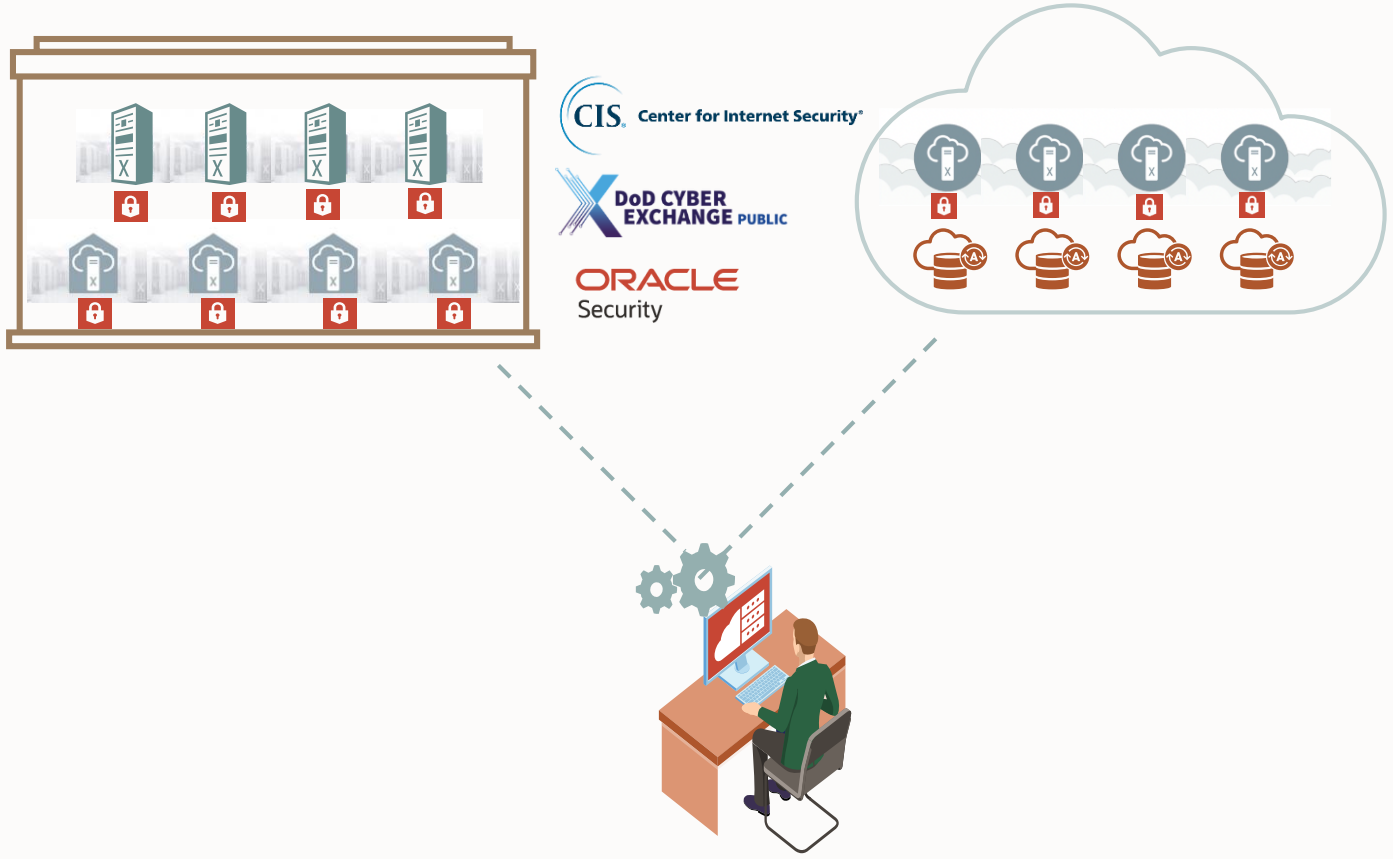
- Out of the box Security Standards
  - CIS Benchmark v2.1.0 and v3.0.0 for Oracle 12c Database
  - STIG Standards Oracle Databases 11g and 12c
  - Oracle' best practices and Security recommendations
- 1,000s of checks in Compliance Library
- Automated remediation with corrective actions
- Customizable to meet Internal best practices
  - Leverage Oracle provided rules matching your own
  - Tailor Oracle provided rules with known exceptions
  - Build custom rules to exactly match requirement

Maximize Data Security Posture with Industry and Oracle Standards

Improve security posture by continuous monitoring

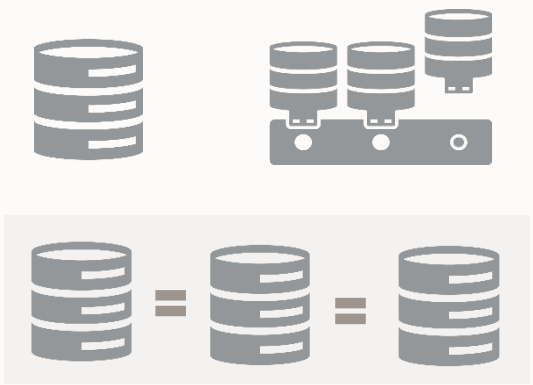
Audit security report to ensure compliance

Reduce DBA time by auto-remediation of security violations



CIS Benchmark Standards for Oracle Database 12c

Center for Internet Security (CIS) Standard for Oracle 12c Database



- CIS certified, best practices for the secure configuration of DB 12c
- EM13.4 GA: CIS Benchmark for Oracle DB 12c- Traditional Audit Profile
- EM 13.4 RU3: CIS Benchmark for Oracle DB 12c- Unified Audit Profile
- 117 individual checks for RDBMS profile; agent side rules
- Sub-controls provides best practices for
  - Continuous vulnerability management
  - Secure configuration of database instances
  - Minimize administrative privileges
  - Audit administrative privileges
  - Analysis of audit logs

CIS Benchmark Standards for Oracle Database 12c

Oracle Database Installation and Patching Requirements

- Ensure default passwords are changed
- Ensure all sample data and users have been removed

Oracle Parameter Settings

- Listener settings
- Database settings

Oracle Connection and Login Restrictions

- Block unauthorized access to data and services by setting access rules

Oracle User Access and Authorization Restrictions

- Default public privileges for packages and object types
- Revoke non-default privileges for packages and object types
- Revoke excessive system privileges
- Revoke role privileges
- Revoke excessive table and view privileges

Audit/Logging Policies and Procedures

- Traditional auditing
- Unified auditing

CIS provides comprehensive configuration coverage for Oracle database across:

- Installation
- Parameters
- Connectivity
- User Privileges
- Auditing

STIG Standards for Oracle Database 11.2g & 12c

STIG Standard for Oracle 12c and 11.2g Database

- Best practices by DISA to ensure DoD-mandated security compliance
- EM13.4 RU3:
  - Oracle Database 12c STIG - Ver 1, Rel 16 (SI and Cluster)
  - Oracle 11.2g Database STIG - Ver 1, Rel 16 (SI and Cluster)
- EM 13.4 GA
  - Oracle Database 12c STIG - Ver 1, Rel 11 and Rel 12 (SI and Cluster)
  - Oracle Database 11.2g STIG - Ver 1, Rel 14 (SI and Cluster)
- All are agent side rules

STIG Standards for Oracle 11.2g & 12c Database

Oracle Database Installation and Patching Requirements

- Ensure default passwords are changed
- Ensure all sample data and users have been removed
- Ensure unsupported software versions are not patched by vendors

Oracle Parameter Settings

- Listener settings
- Database settings

Oracle Connection and Login Restrictions

- Remove all unauthorized remote database connection definitions from the database
- Remove development accounts from production DBA OS group membership

Oracle User Access and Authorization Restrictions

- Restrict use of the WITH ADMIN OPTION to authorized administrators
- Assign permissions to custom application user roles based on job functions
- Revoke non-default privileges for packages and object types
- Revoke excessive system privileges
- Revoke role privileges
- Revoke excessive table and view privileges

Audit/Logging Policies and Procedures

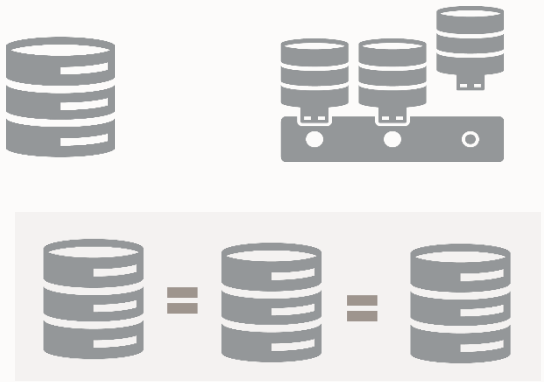
- Traditional auditing
- Unified auditing

STIG provides comprehensive configuration coverage for Oracle database across:

- Installation
- Parameters
- Connectivity
- User Privileges
- Auditing

Oracle Best Practices for Databases

High Security Configuration For Oracle Database



- High Security Configuration For Oracle Databases
  - High Security Configuration For Oracle Cluster Database Instance
  - High Security Configuration For Oracle Database
  - High Security Configuration For Oracle Cluster Database

- Set of rules, checklists, and best practices created by Oracle ensure compliance security requirements
- Adherence with advanced best-practice security configuration settings
- To protect against database-related threats and attacks
- All are repository side rules
- Each rule may generate one or more violations

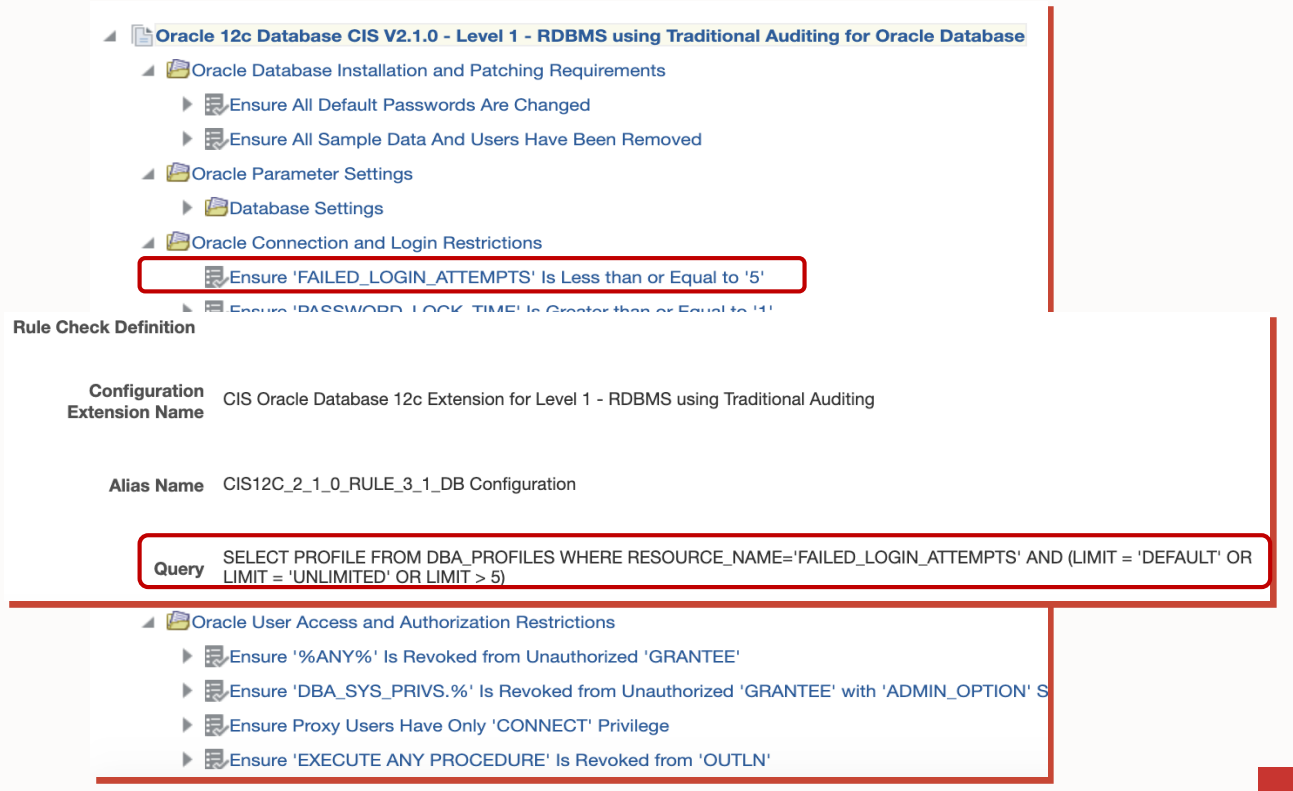
Automated Database Security Assessment with CIS Benchmark

DBA is required to assess 12c database targets against CIS Benchmarks

- Select CIS Benchmark Standard for Cluster or Single Instance
- Review CIS rule definition for each category
- Modify rule definition using SQL Query provided, if required
- Associate Single Instance targets to Standard
- Compliance check is initiated once association is confirmed
- Reviews results and violations
- Remediate violations or suppress for a given duration

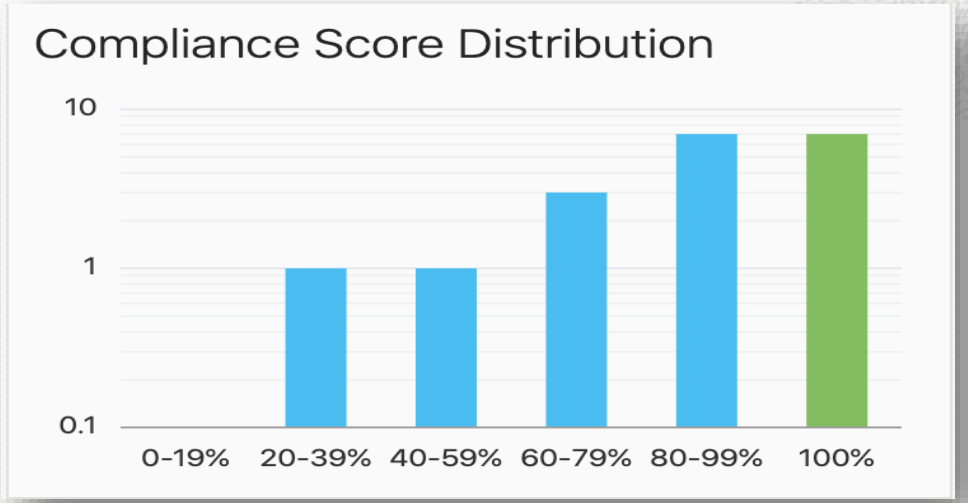
Oracle 12c Database CIS v2.1.0 for Oracle Cluster Database

Oracle 12c Database CIS v2.1.0 for Oracle Database



Continuous Compliance Auditing

- Validate conformance to standards or benchmarks using discrete logic
- Best for Industry and internal standards (STIG, CIS, Custom)



- Review target compliance scorecard & rules evaluated
- Violations: validate conformance to CIS Standards
- Remediate with SQL query for each rule violation

Violations

Compliance Standard Oracle 12c Database CIS V2.1.0 - Level 1 - RDBMS using Traditional Auditing for Oracle Database

Target Name

Compliance Standard Rules	Violation Count
Ensure All Default Passwords Are Changed	1
Ensure 'GLOBAL_NAMES' Is Set to 'TRUE'	1
Ensure 'O7_DICTIONARY_ACCESSIBILITY' Is Set to 'FALSE'	1
Ensure 'REMOTE_LOGIN_PASSWORDFILE' Is Set to 'NONE'	1
Ensure 'FAILED_LOGIN_ATTEMPTS' Is Less than or Equal to '5'	1
Ensure 'PASSWORD_LOCK_TIME' Is Greater than or Equal to '1'	1
Ensure 'PASSWORD_LIFE_TIME' Is Less than or Equal to '90'	1
Ensure 'PASSWORD_REUSE_MAX' Is Greater than or Equal to '20'	2
Ensure 'PASSWORD_REUSE_TIME' Is Greater than or Equal to '365'	1
Ensure 'PASSWORD_GRACE_TIME' Is Less than or Equal to '5'	1
Ensure 'PASSWORD_VERIFY_FUNCTION' Is Set for All Profiles	1

Thank you