ORACLE

Secure Multitenant Databases and Hosts

with Enterprise Manager Security Compliance Framework

Amol Chiplunkar

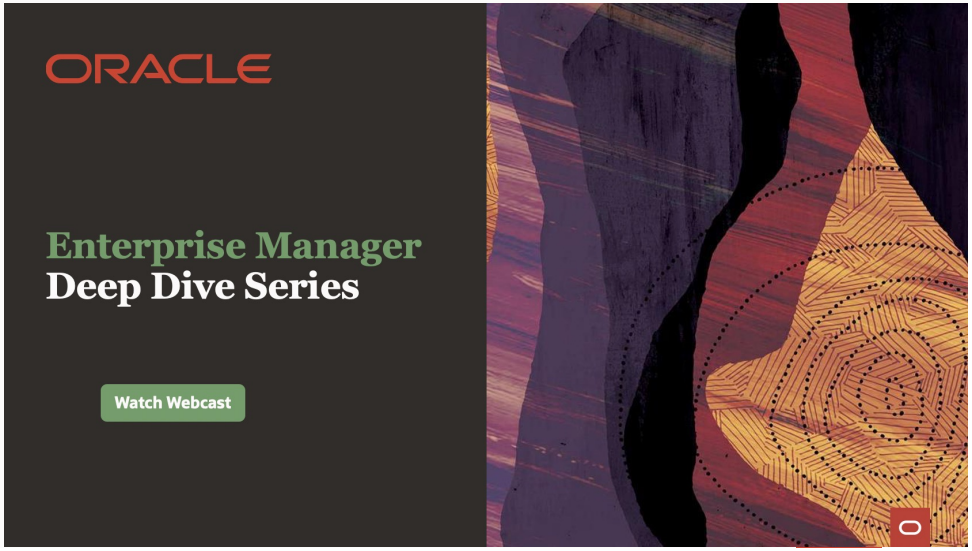
Senior Manager, Software Development

Harish Niddagatta

Senior Principal Product Manager

Timothy Mooney

Product Marketing Director



Agenda

- Overview
- Security Challenges
- Securing Databases and Hosts
- Demo
- Q&A

Database Lifecycle Management: Overview

Provision and Clone

Automated, repeatable, and scheduled deployment of standardized configuration of single instance, RAC and multitenant databases in on-premises and cloud environments

End-to-end solution to clone masked production databases for backup and new application dev-test requirements

Patch and Upgrade

Automatically patch, and upgrade large number of databases with minimal downtime

Configuration and Compliance

Monitor standardized configuration, detect misconfigurations, and apply corrective actions to comply, reduce security risks

Secure configuration of databases, hosts and engineered systems, comply with industry and regulatory standards, harden security posture


TDE Database


RAC


Multitenant


Active Data Guard


Exadata


OCI


ExaCC/ExaCS

Security Challenges

Configuration Sprawl

Insecure configuration change by user with elevated privileges increases risk of misconfiguration

Patch Recommendations

Unpatched systems increase risk of breach. How do you figure out which patches to apply?

Security Compliance

Security vulnerabilities with unprotected data. How to ensure secure environment?

Best Practices to Boost Security and Compliance

Reduce configuration sprawl

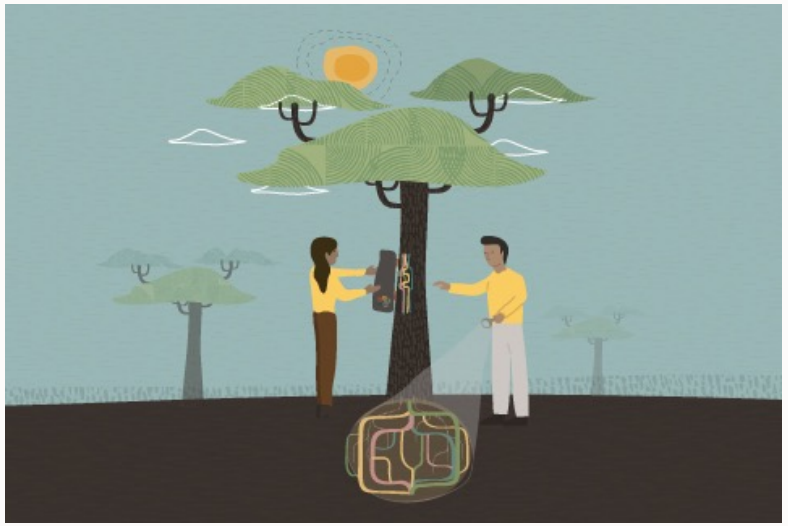
- Standardize on secure target configurations
- Secure configurations using standard

Automate patch recommendations

- Identify and automatically apply missing patches

Automate security compliance

- Secure database and infrastructure

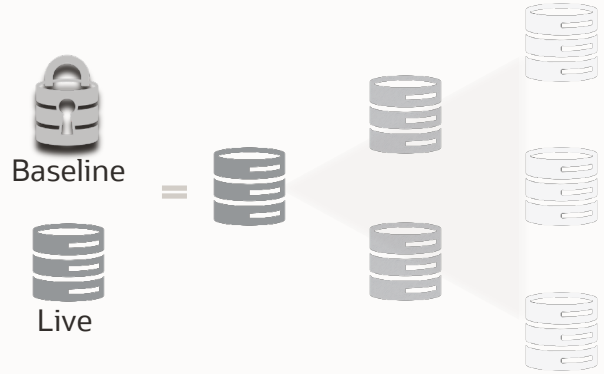


Managing Configuration Sprawl

Managing Configuration Sprawl

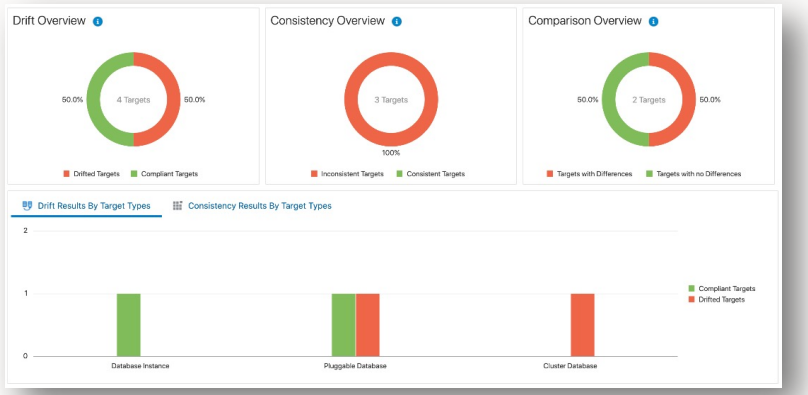
Reduce risk from insecure configurations & over-privileged users

- Quickly assess security posture to identify configuration drifts
- Identify potential bad actors or over-privileged users
- Detect and prevent insecure configuration changes
- Automate remediation; leverage resources for high-value tasks
- Audit user activities on tables with sensitive data



Standardize configuration deployment

- Reduce security exposure by deploying standardized known set of configurations



Configuration Drift and Consistency Management

Key uses

Database initialization parameters

- Saved database reference to 1200+ databases
- Compare 50 database initialization parameters only
- Detect configuration deviation, notify and remediate

Host configuration

- Live Linux host reference to 500+ hosts
- Compare extended configuration collections

RAC Database instances

- Consistency of instances WITHIN 500+ cluster databases

Data Guard standbys

- Consistency of primary databases with its Data Guard standby databases
- 100s of database systems

Exadata storage cells

- Consistency of storage cells within Exadata

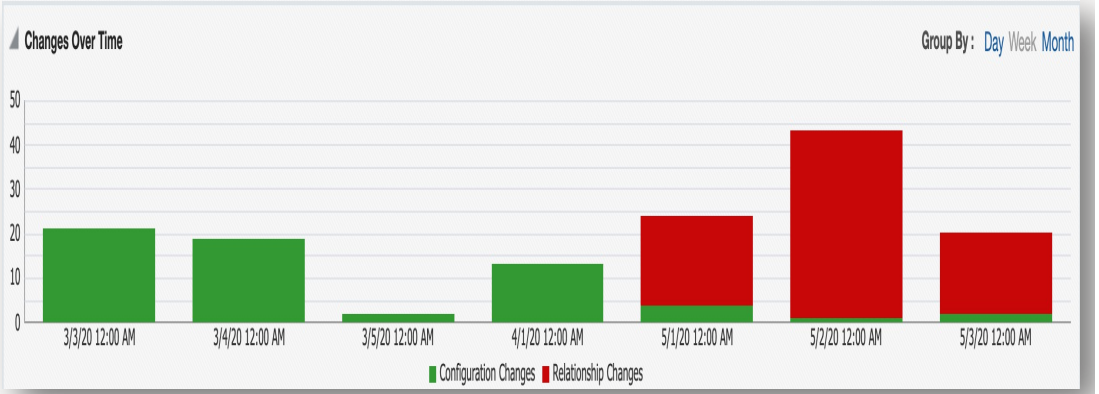
Key Features and Benefits

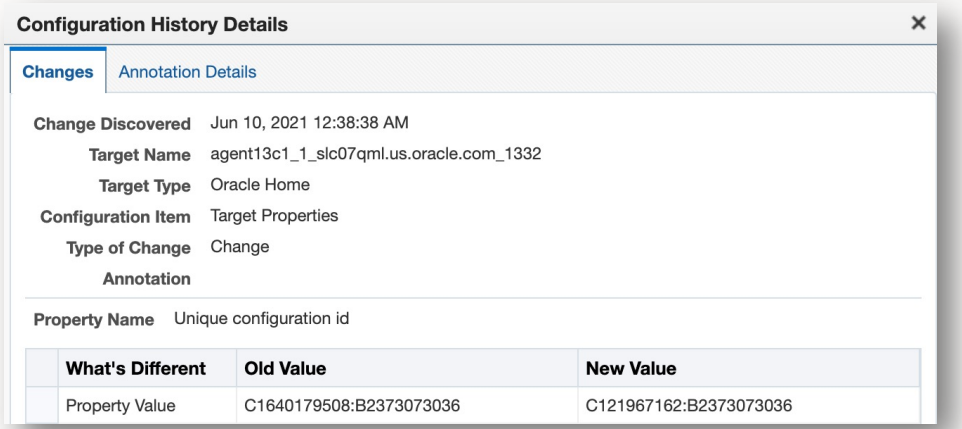
- On-demand configuration comparison against a baseline
- Track configuration drift and maintain consistency with baseline
- Configuration extensions for customized collections
- Auto-remediation of violations
- Monitor configuration history for changes
- Perform root cause analysis and impact analysis

Manage Configuration Changes

Configuration History

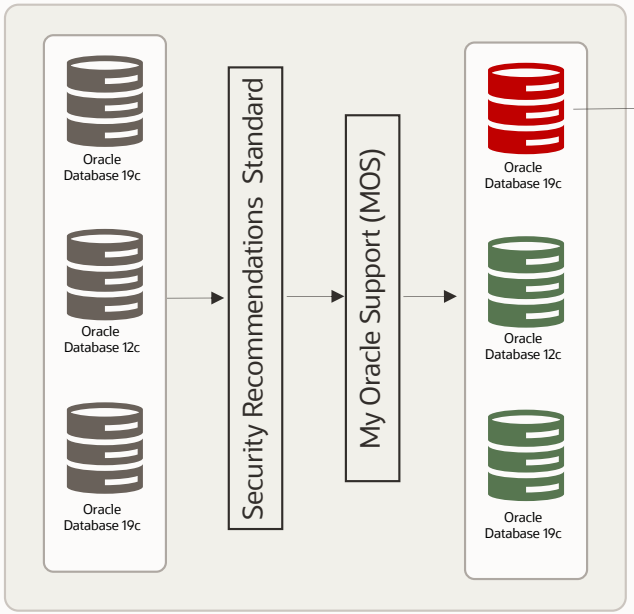
- Track changes to targets over a year
- View change history and manipulate how the information is presented.
- Annotate change records with comments, becomes part of history along with timestamp and owner
- Schedule a history search to capture future changes
- View the status of scheduled history jobs
- Notify others of future change detection
- Save change history details to a file





Automate Patch Recommendations

Automated Recommendation For Missing Patches



Not Compliant

Rule: Security Recommendations — Fail

Description	Checks targets in your host for missing security patches
Severity	Critical
Rationale	To help ensure a secure and reliable configuration, all relevant and current security patches should be applied.
Remediation	Apply one of the identified security patches to the corresponding target in your host.
Violation Message	The target ı in host ı ı is vulnerable. The security patch 32399816 is applicable to it.

Compliance Standard Rule Security Recommendations
Target Name slc07qmk.us.oracle.com

Export To Excel

Patch Name	Description
28186730	OPATCH 13.9.4.2.5 FOR EM 13.4, FMW/WLS 12.2.1.3.0, 12.2.1.4.0 AND 14.1.1.0.0
31544353	ADR FOR WEBLOGIC SERVER 12.2.1.4.0 JULY CPU 2020
32755791	WLS STACK PATCH BUNDLE 12.2.1.4.210411
32499990	APACHE PLUGIN BUNDLE PATCH 12.2.1.4.210420
32499990	APACHE PLUGIN BUNDLE PATCH 12.2.1.4.210420
31544353	ADR FOR WEBLOGIC SERVER 12.2.1.4.0 JULY CPU 2020
32698246	WLS PATCH SET UPDATE 12.2.1.4.210330
32673423	OHS (NATIVE) BUNDLE PATCH 12.2.1.4.210324
32698246	WLS PATCH SET UPDATE 12.2.1.4.210330
32755791	WLS STACK PATCH BUNDLE 12.2.1.4.210411
28186730	OPATCH 13.9.4.2.5 FOR EM 13.4, FMW/WLS 12.2.1.3.0, 12.2.1.4.0 AND 14.1.1.0.0

- Proactive security automation, including automated patching, can reduce the risk of data breaches occurring after common vulnerability and exposure alerts have been issued
- Pre-set Security Recommendations compliance standard lists missing security patches for each database target
  - Compliant: when all security patches posted on My Oracle Support (MOS) is applied on a target
  - Non-Compliant: when at least one security patch is not applied on a target

Automate Security Compliance

Automate Hardening For Security Compliance

Secure assets, reduce risks

Secure Database

CIS Benchmark, DISA STIG, and Oracle Security Best Practices

Secure Host

PCI-DSS, HIPAA, DISA STIG, and System Security Standard

Secure Engineered Systems

Exadata Best Practices and Security Recommendations

- Security policy management across **heterogeneous** targets and environments
- Improve infrastructure stack security **posture** by continuous monitoring
- **Audit** security report to ensure compliance
- Reduce DBA time by **auto-remediation** of security violations

Pre-built For Database Security Compliance Standards

Assess, detect, and remediate

Center for Internet Security (CIS)

- Certified support of CIS benchmarks for Oracle Database

Security Technical Implementation Guide (STIG)

- DoD published standards for Oracle Database

Oracle Security Best Practices

- Basic Security Configuration
- High Security Configuration
- Storage Best Practices
- Configuration Best Practices

ORACLE DATABASE

CIS. Center for Internet Security®

SCAP Supported Security Standards

Supports Security Content Automation Protocol (SCAP) XCCDF Compliance benchmarks

- Leverage built-in Open SCAP engine in Linux

SCAP standards in Oracle Linux 7 and 8

- Health Insurance Portability and Accountability Act (HIPAA)
- Payment Card Industry Data Security Standard (PCI-DSS v3.2.1)
- Security Technical Implementation Guide (STIG)
- Standard System Security Profile

Security rules catalog maps to various standards

- ISO 27001: Information Security Management
- CIS Controls
- CJIS Security Policy
- DoD Control Correlation Identifier
- Critical Infrastructure Cybersecurity
- COBIT framework

Import any Linux specific compliance standard in Extensible Configuration Checklist Description Format (XCCDF)

ORACLE Linux

Secure Databases and Hosts

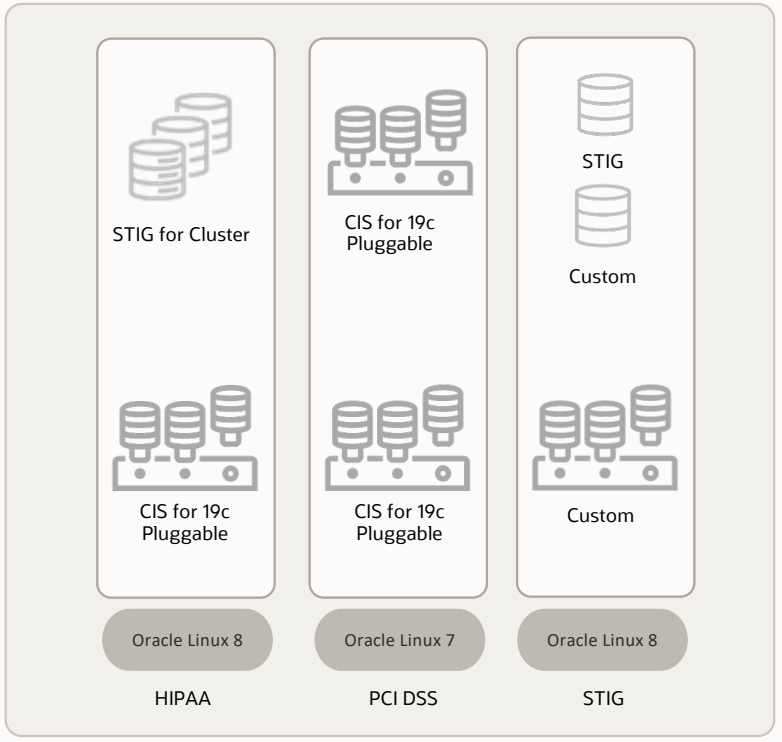
Reduce risks and breaches

Oracle Databases

- Secure configuration, drive compliance with industry, and regulatory security standards like CIS, and STIG

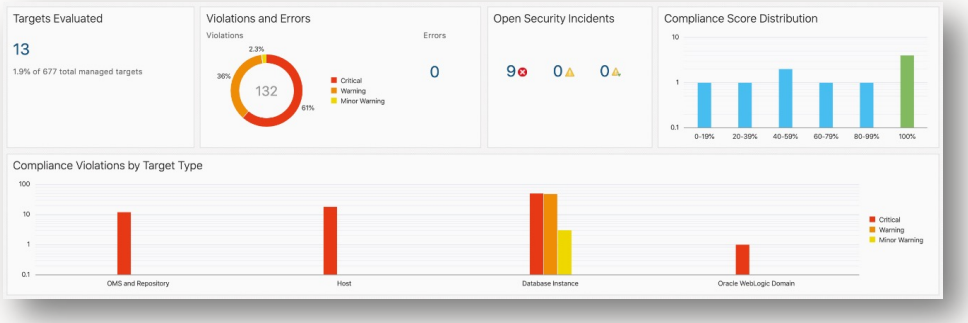
Linux Hosts

- Secure configuration, drive compliance with industry, and regulatory security standards like HIPAA, PCI DSS, and STIG



Automate Day-to-day Operations

- Continuous assessment for configuration violations
- Minimize and audit administrative privileges
- Analyze and remediate violations

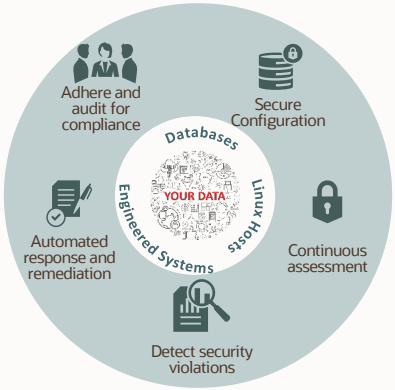


Security compliance dashboards for all managed targets

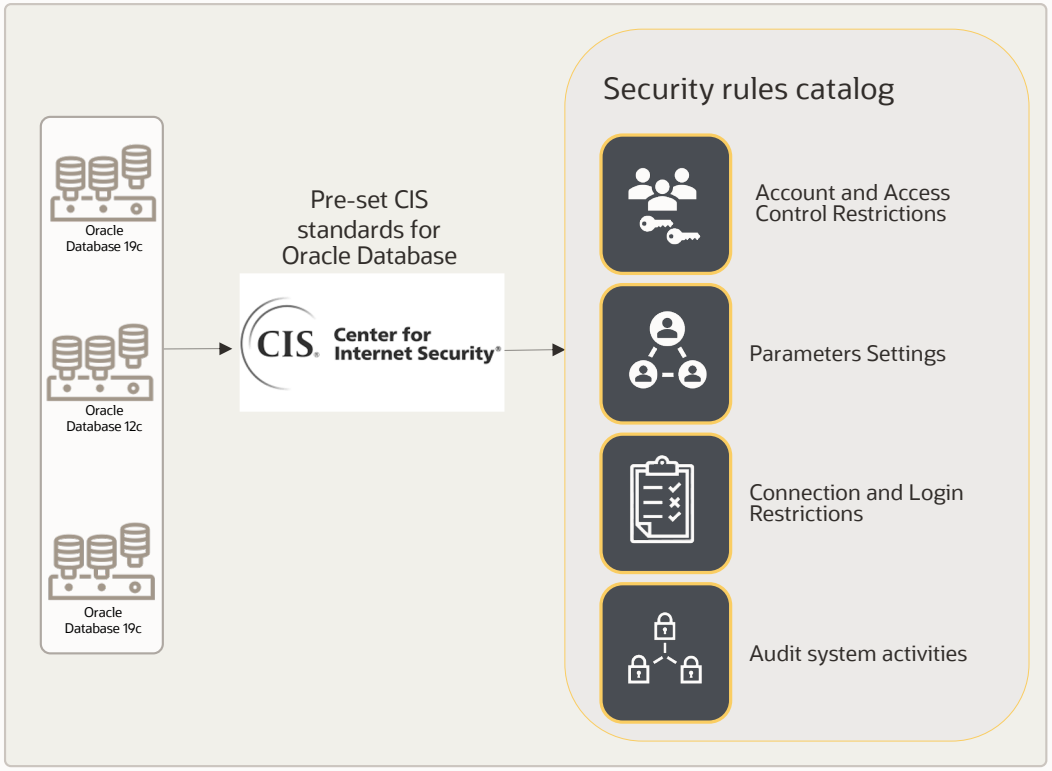
Drilldown each target, review deviations and remediate

EM Compliance showcases compliance score distribution across your data center, prioritize targets to assess and remediate

Insight into compliance score trends over a period per target or per standard, confirm to ensure score at desired policy level



CIS Benchmark Standards for Oracle Database



Secure Oracle Database to CIS compliance standards

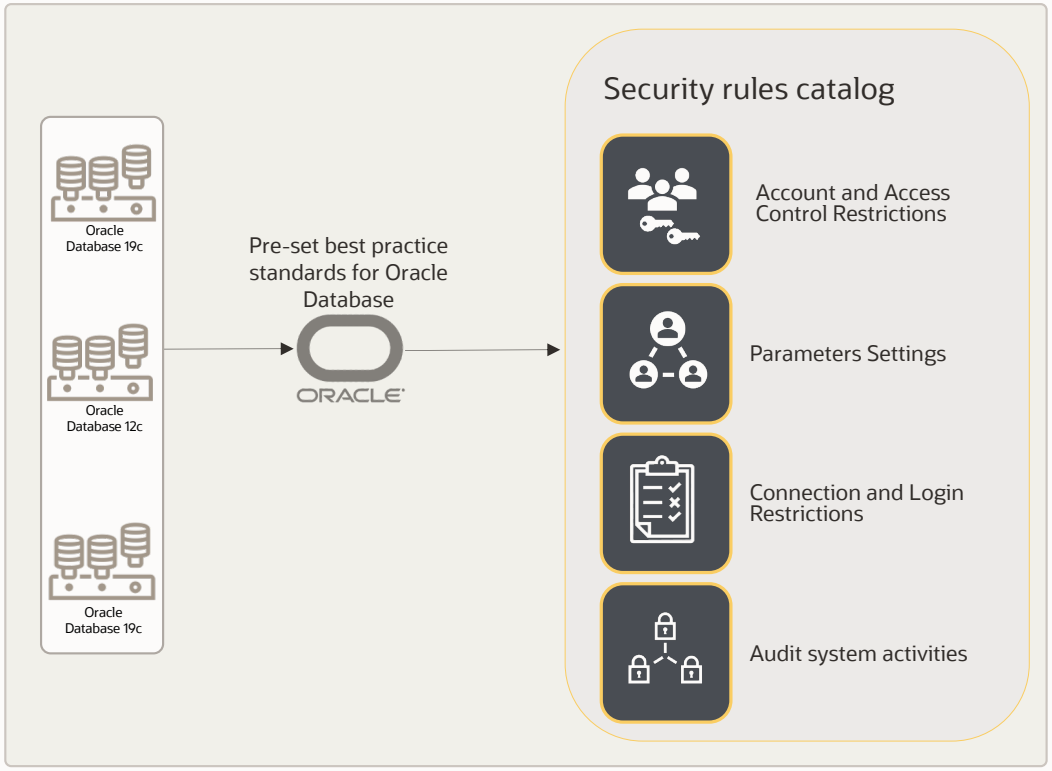
Catalog of CIS rules for

- User access and restrictions
- Database parameter settings
- Database connectivity and login
- Auditing system activities

Review and remediate violations

Audit report for compliance

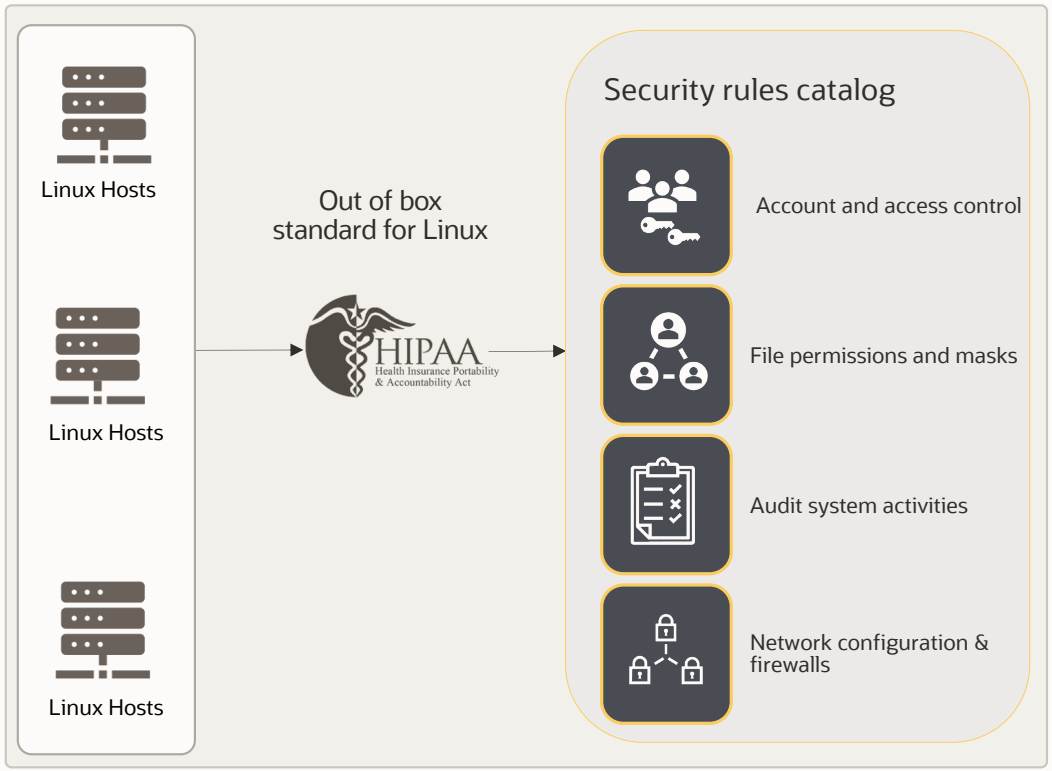
Oracle Best Practices Database Security Compliance Standards



Flexibility to choose out-of-box standards

- Basic Security Configuration for Oracle Pluggable Database
- High Security Configuration for Oracle Pluggable Database
- Storage Best Practices for Oracle Pluggable Database
- Configuration Best Practices for Oracle Pluggable Database

Linux Compliance with HIPAA



Secure Linux for HIPAA-compliance

Catalog of HIPAA rules for

- Protecting console access
- Restricting root access
- Access control
- File access permissions
- Auditing system activities

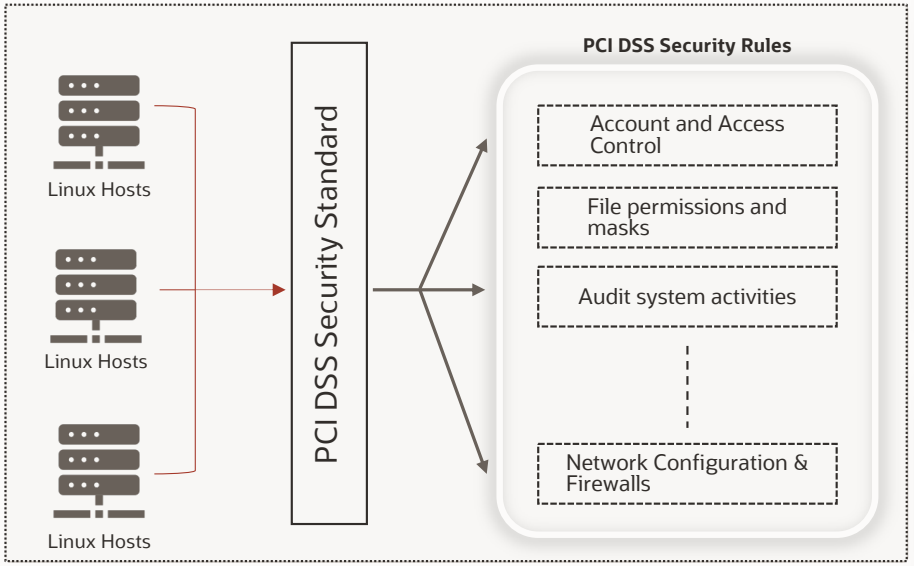
Review and remediate violations

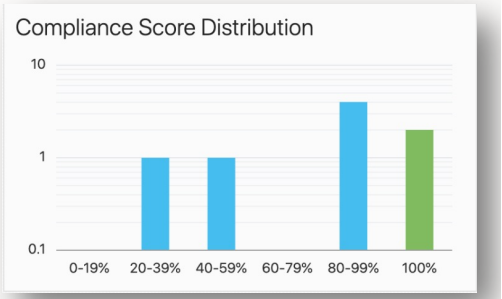
Audit report for compliance

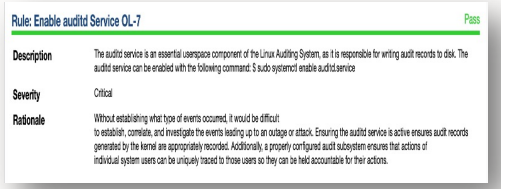
Security rules catalog maps to various other standards like ISO 27001, COBIT framework, CIS Controls, etc.

Linux Compliance with PCI DSS

- Checks for any misconfiguration and deviations from security rules defined in PCI Data Security Standard
- Controls categorized into:
  - System Settings: Rules to check correct system settings
  - Services: Rules to check and recommend disabling
- Security rules catalog maps to various other standards like ISO 27001, COBIT framework, CIS Controls, etc.

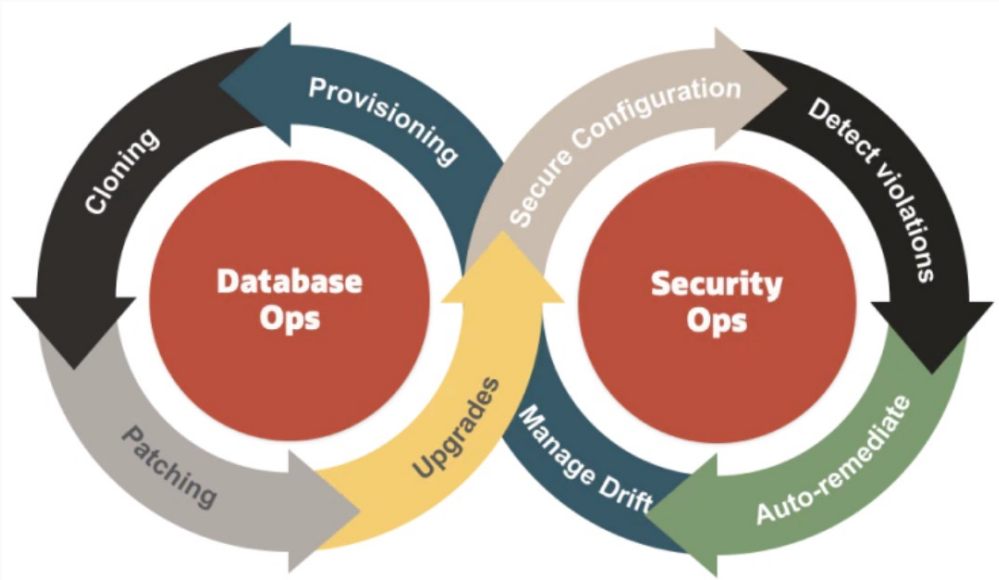






Demo (view in session recording)

What Questions Do You Want The Answers To?



Documentation:
EM 13.5 DB Lifecycle Management
>> Go to Configuration and Compliance

Webcasts/Workshops:
Enterprise Manager Deep Dives

Where can I find the slides, replay, resources?
Blogs.oracle.com/manageability …

Product Information:
oracle.com/enterprise-manager/#rc30p2
>> Go to Database Ops Automation


ORACLE

Our mission is to help people see data in new ways,
discover insights, unlock endless possibilities.