ORACLE

An easier way for DBAs to self-audit and report databases comply with an Industry Regulations

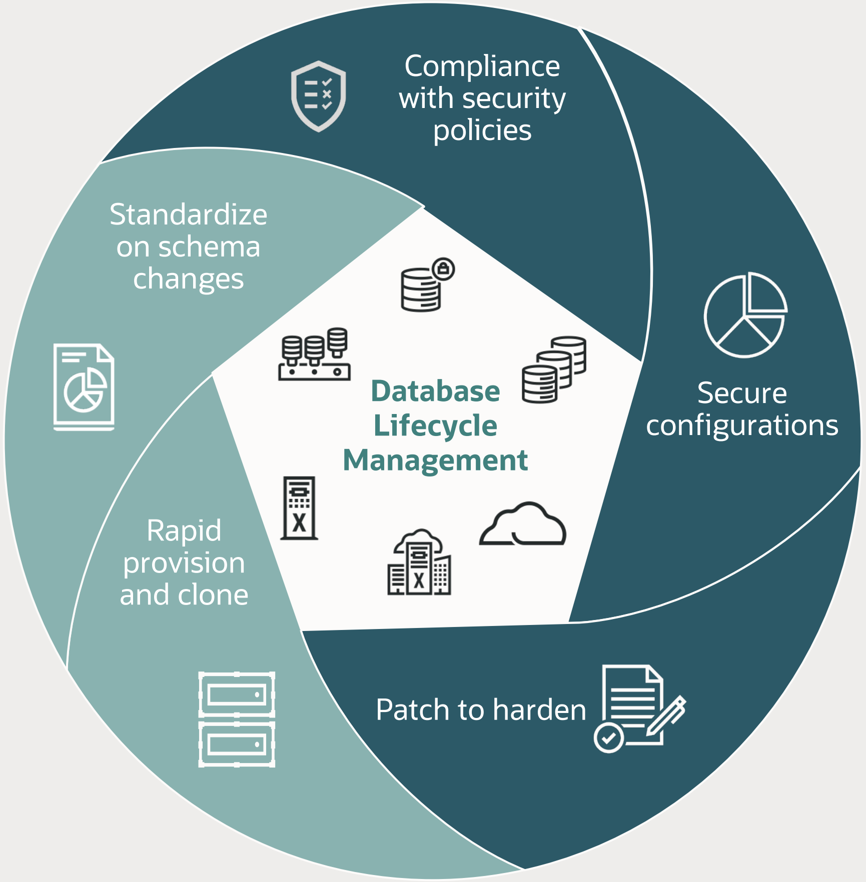
Using Industry and Regulatory Best Practices reduces Security Vulnerabilities and risks with Standard repeatable solution

Shiva Prasad
Product Management - Enterprise Manager
Oracle Observability & Management

NYOUG

Security hardening

Database Lifecycle Management (DBLM)


Compliance with security policies
Standardize on schema changes
Secure configurations
Database Lifecycle Management
Rapid provision and clone
Patch to harden

Compliance management

Regulatory and industry standards (CIS, STIG, HIPAA, PCI-DSS, custom)
Secure infrastructure with Oracle Autonomous Health Framework
EXAchk

Protect from breaches

Automated security patch recommendations, intuitive interface to patch and secure assets

Automate repetitive provision and clone activities

Deploy standardized database configuration

Standardize on database schema changes

Baseline definition and compare to detect differences, export/import baselines between development and production

Multiple interfaces – REST APIs, EMCLI and UI

Database management scenarios

Lifecycle management

Higher productivity

Automate complex and time consuming tasks for database patching

Patch recommendations

Security patches

Deploy recommended patches with ease, reduce breaches

Configuration sprawl

Standardization

Use well defined secure configurations, reduce maintenance and risks

Security compliance

Compliance

Secure assets with out-of-box standards and audit for compliance

Inventory insight

Reduce cost

Get insight into inventory utilization, reduce CapEx, and OpEx

Secure databases and enforce compliance with IT policies

Security compliance best practices to drive and enforce security

Stakeholders in your organization to secure assets

Security hardening is a strategic priority

CFO	CISO	CIO/Architect	DBA
Influencer	Influencer	Influencer	Decision Maker/Influencer
Ensure corporate or regulatory compliance	Protect data and ensure regulatory compliance	Identify regulatory compliance to be met	Complexity in managing multiple databases for security
Reduce risk across multicloud environment	Intrusion attempts, mean time to detect and resolve	Automate to secure multicloud environment	Manage privileged, and orphaned accounts
Secure data by masking, apply security patches	Average time to patch vulnerabilities	Patch to secure and protect data, align with compliance	Number of known (un)resolved vulnerabilities
Audit for compliance	Security audit and apply recommendations	Audit every activity on each asset	Provide audit reports

Modernizing your security compliance addresses key business concerns

Breaches due to insecure configuration

45%

Misconfigurations

Misconfigurations and insecure configuration changes are preferred ways for bad actors to exploit and get hold of sensitive information

Privileged credential abuse

74%

Administrative Privileges

Lack of security policies with principles of least privileges to users for database components leads to anomalous behavior

IT risk assessment priority

#2

Risk Management and Compliance

Business interruption implies revenue loss. Reputation / negative brand can reduce market value. May face penalties besides additional scrutiny. Customers with bad experience may not return.

Key use cases to enhance security posture

Monitor and remediate to align with compliance

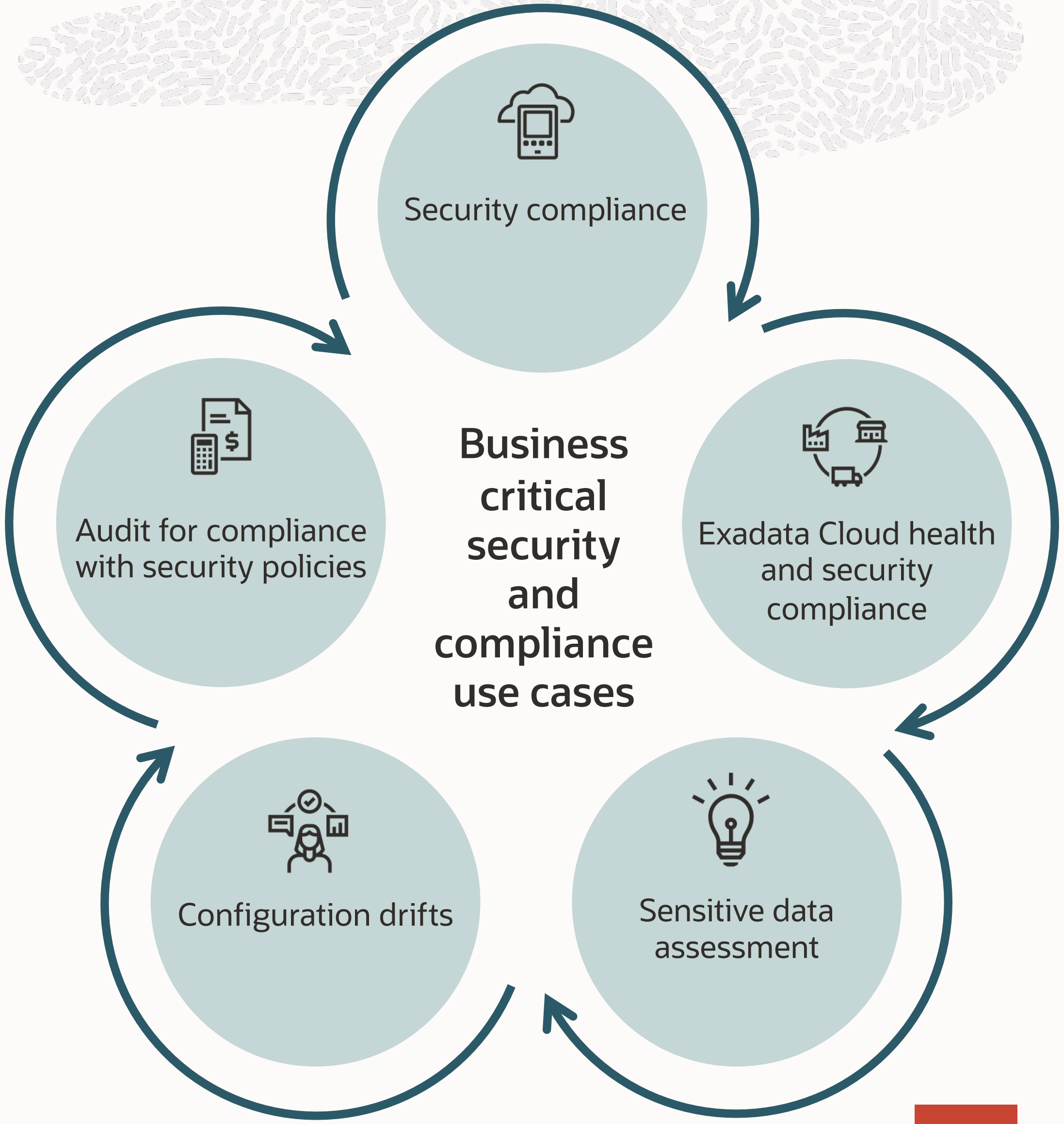
Secure database and underlying infrastructure

Secure Oracle Engineered System for security

Identify sensitive data in Oracle Databases

Manage and target configuration drifts and consistency

Audit for compliance with security policies



Business critical security and compliance use cases

Security compliance

Exadata Cloud health and security compliance

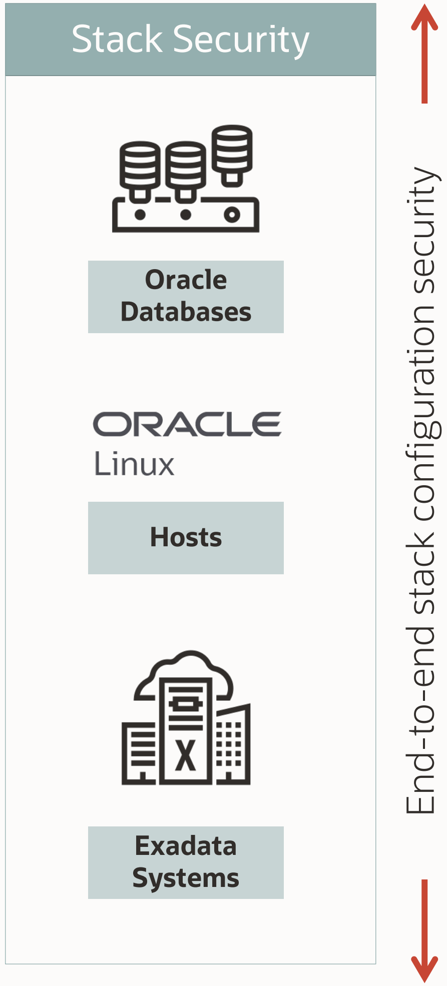
Sensitive data assessment

Configuration drifts

Audit for compliance with security policies

Secure databases and infrastructure stack

Reduce risks by securing entire stack assets



Stack Security

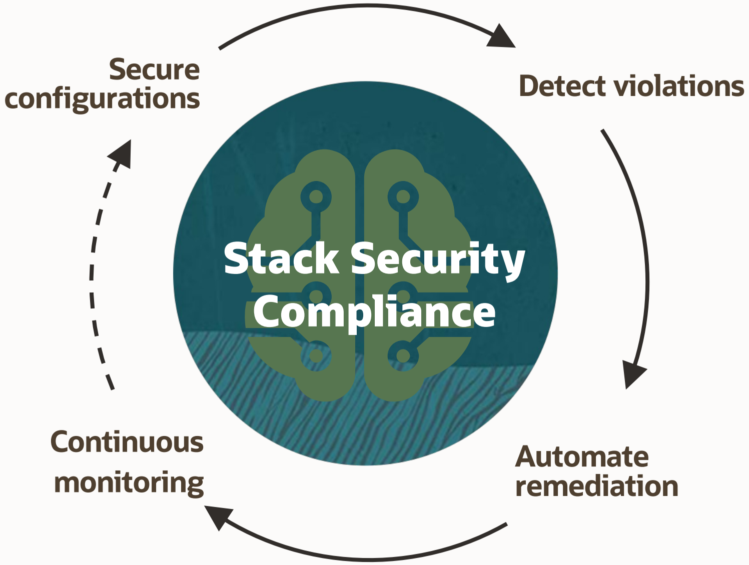
Oracle Databases

ORACLE Linux

Hosts

Exadata Systems

End-to-end stack configuration security



Stack Security Compliance

Secure configurations

Detect violations

Automate remediation

Continuous monitoring

Oracle Databases

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

Linux Hosts

- Secure configuration, drive compliance with industry, and regulatory security standards or any XCCDF format standards

Exadata and Exadata Cloud Infrastructure

- Secure underlying Exadata infrastructure from breaches, leverage AHF EXAchk for health, performance and security checks

Database security compliance standards

Assess, detect, and remediate

Database Security Compliance

Oracle Databases

- CIS Benchmark guidelines
- DISA STIG security controls
- DBSAT based assessments
- Oracle security best practices

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

Database Security Assessment Tool (DBSAT)

- Assess Oracle Database security: configuration, risky users and sensitive data

CIS Benchmarks for Oracle Database

Continuous vulnerability management
Ensure mission-critical databases are secure

Secure configuration
Automate database configuration to security policies

Minimize administrative privileges
Restrict privileges to users and monitor activities

Analysis of audit logs
Audit database activities, and protect audit trail from targeted alterations

Connection and login restrictions

Block unauthorized access to data and services by setting access rules

User access and authorization restrictions

Implement Users, privileges, grants, and access control list (ACL)

Parameter settings

Ensure auditing is enabled, listeners are confined and appropriate authentications configured

Minimize administrative privileges

User access and authorization restrictions

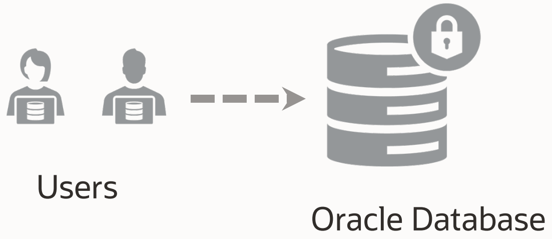
Principles of least privilege – grant privileges only for the job to get done for ongoing security checks and to align with internal security policies

Restrict *ANY*, EXP*, and IMP* privileges

Enterprise Manager compliance checks restrictions are in place, flags any violations, and auto-remediate

Enterprise Manager compliance check

- Monitors excessive System, Object and Role privileges
- Monitors excessive Table and View privileges



SYS.AUD$ table contains all audit records for the database of non-Data Manipulation Language (DML) events, such as ALTER, DROP, CREATE, and so forth. **Unauthorized grantees should not have full access to that table**

CIS Benchmark Controls	Ensure the 'ALL' is Revoked from Unauthorized 'GRANTEE' on 'AUD$'
Rationale	Permitting non-privileged users authorization to manipulate SYS.AUD$ table can allow distortion of audit records, hiding unauthorized activities
Remediation	AUDIT ALL ON AUD$ FROM <grantee>;
CIS Controls v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications

Host Compliance

Host security compliance standards

Assess, detect, and remediate

Host Security Compliance

ORACLE Linux

Hosts

- PCI-DSS Compliance
- HIPAA privacy rules
- DISA STIG security controls
- Import XCCDF based policies

PCI DSS COMPLIANT

HIPAA Health Insurance Portability & Accountability Act

DEFENSE INFORMATION SYSTEMS AGENCY

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

PCI DSS assessment

Compliance standard with 125 unique rules to secure various system settings and services like

- Maintaining secure network configuration
- Implement strong access control measures
- Monitor and test networks regularly

Checks for any misconfiguration and deviation from the security rules defined in the standard

System Settings

Account and access controls, file permissions and masks, and audit service with Linux Audit daemon (auditd)

Services

Controls recommending software components to disable for high security posture

PCI DSS Assessment for Linux

Goal 1: Build and maintain a secure network

- Install and maintain a firewall configuration to protect cardholder data
- Do not use vendor-supplied defaults for system passwords and other security parameters

Goal 2: Protect cardholder data

- Protect stored cardholder data
- Encrypt transmission of cardholder data across open, public

Goal 3: Maintain a vulnerability management program

- Use and regularly update anti-virus software or programs
- Develop and maintain secure systems and application

Goal 4: Implement strong access control measures

- Restrict access to cardholder data by business need-to-know
- Assign a unique ID to each person with computer access
- Restrict physical access to cardholder data
- Revoke role privileges

Goal 5: Regularly monitor and test networks

- Track and monitor all access to network resources and cardholder data
- Regularly test security systems and processes

Goal 6: Maintain an information security policy

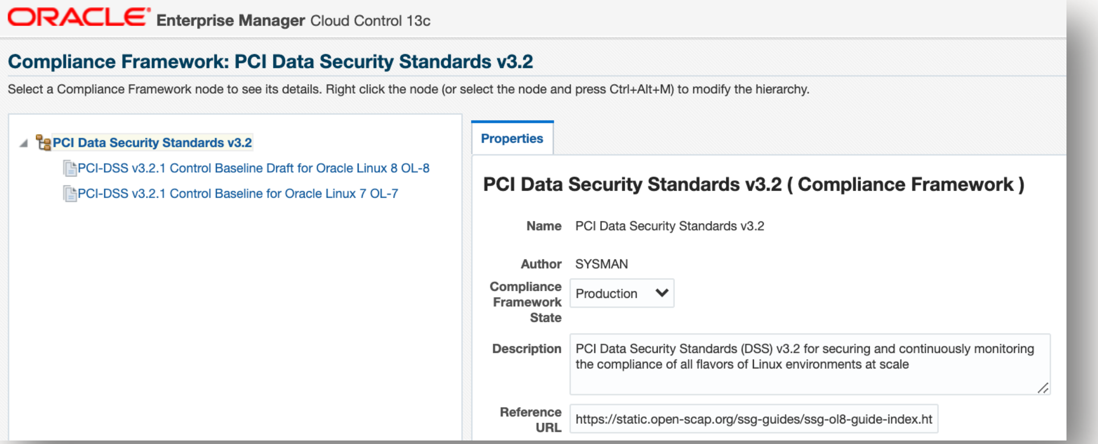
- Maintain a policy that addresses information security for employees and contractors

Ensures comprehensive secure monitoring of Linux host configuration

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



ORACLE Enterprise Manager Cloud Control 13c

Compliance Framework: PCI Data Security Standards v3.2

Select a Compliance Framework node to see its details. Right click the node (or select the node and press Ctrl+Alt+M) to modify the hierarchy.

- PCI Data Security Standards v3.2
  - PCI-DSS v3.2.1 Control Baseline Draft for Oracle Linux 8 OL-8
  - PCI-DSS v3.2.1 Control Baseline for Oracle Linux 7 OL-7

PCI Data Security Standards v3.2 (Compliance Framework)

Name: PCI Data Security Standards v3.2

Author: SYSMAN

Compliance Framework State: Production

Description: PCI Data Security Standards (DSS) v3.2 for securing and continuously monitoring the compliance of all flavors of Linux environments at scale

Reference URL: https://static.open-scap.org/ssg-guides/ssg-ol8-guide-index.ht

HIPAA assessment

Compliance standard with 140 unique rules to secure various system settings and services like

- Account and access control
- System accounting
- Secure network configuration and Firewalls
- File permissions and masks

Checks for any misconfiguration and deviation from the security rules defined in the standard

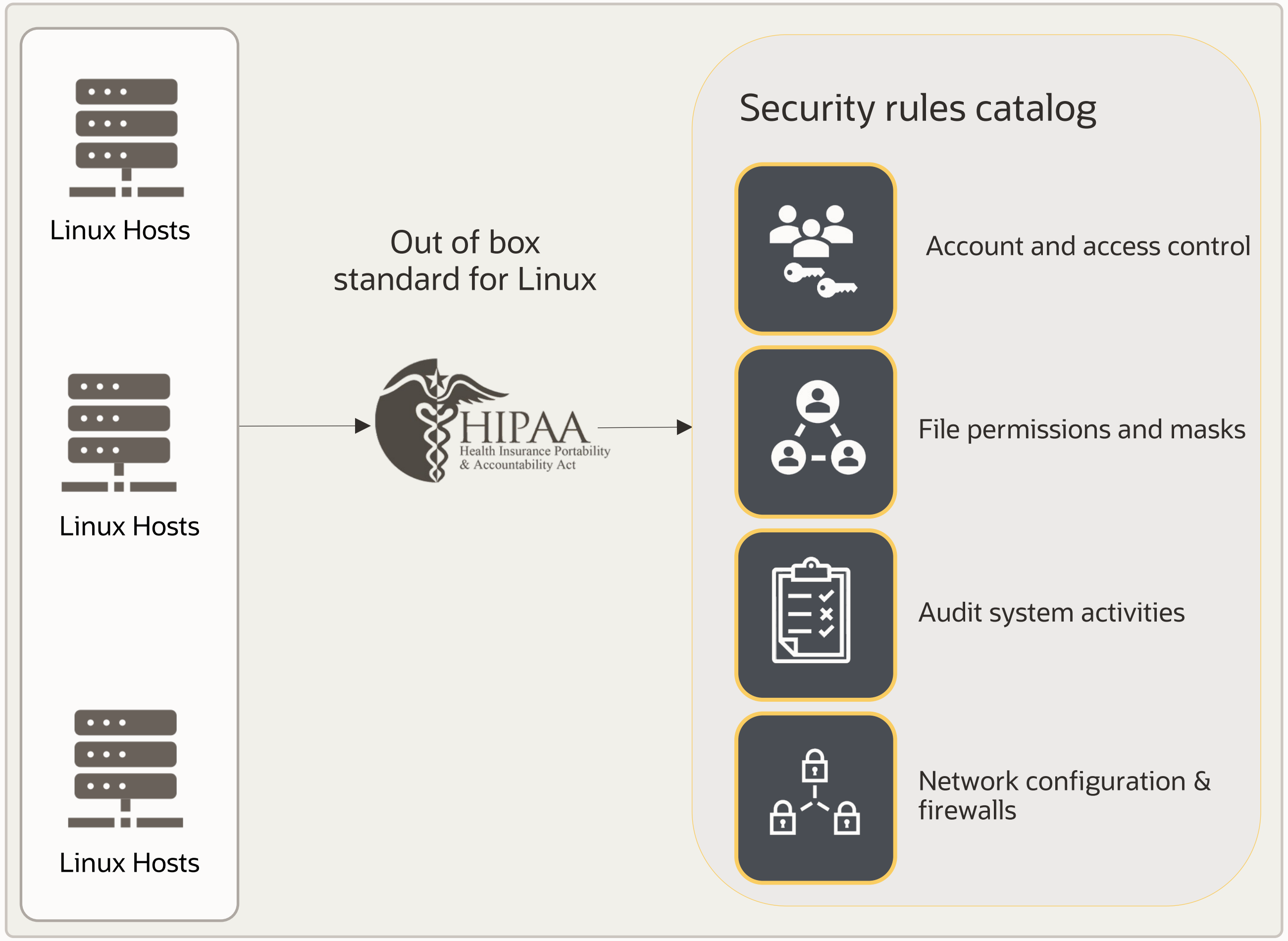
System Settings

Account and access controls to minimize administrative privileges, and audit system activities

Services

Controls recommending software components to disable unnecessary system services for high security posture

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.

Exadata System Compliance

Exadata compliance management

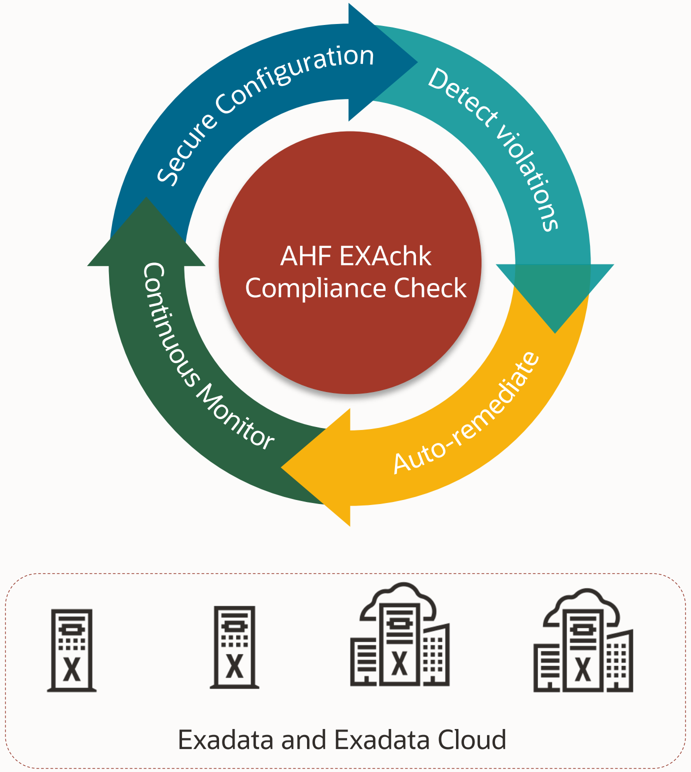
Out-of-box AHF EXAchk security compliance standards for Exadata systems (on-premises and cloud)

Single pane of glass for Exadata compliance management

Scans for performance and reliability issues all components in the system

Automated risk identification and proactive notifications

Comprehensive reports of individual components – both native and EM compliance evaluation reports for audit



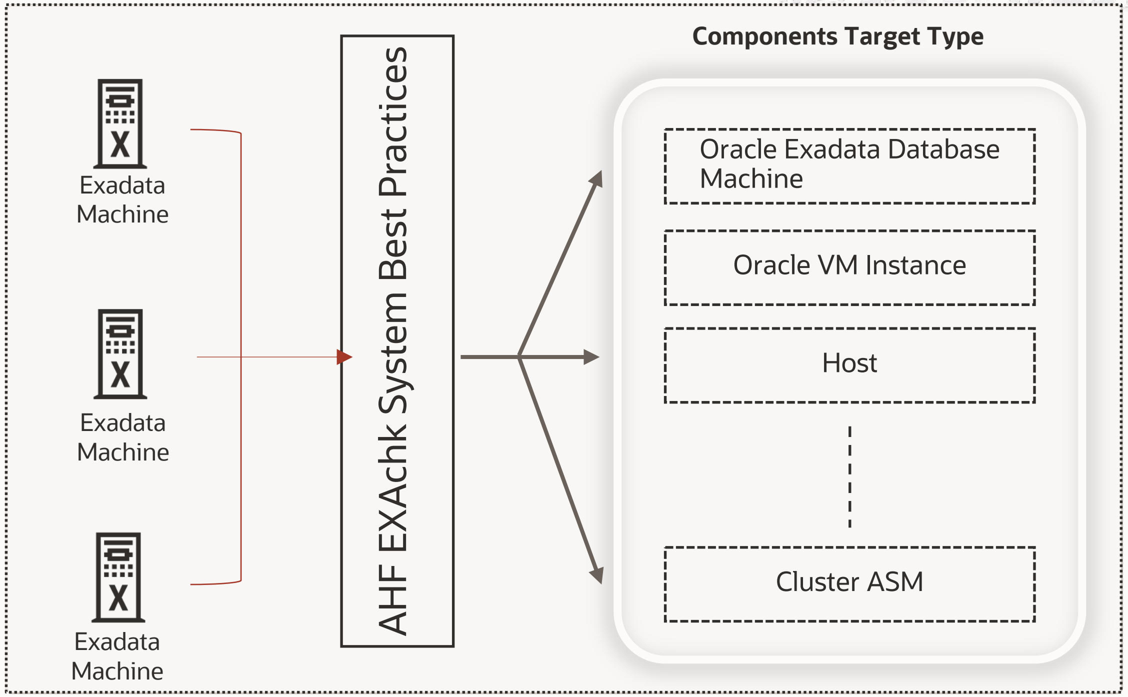
AHF EXAchk Compliance with Oracle Engineered System

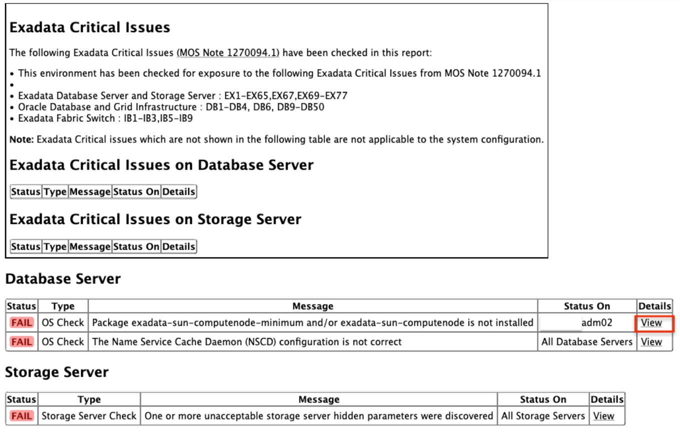
Automated risk identifications

Proactive notification of issues for each component

Non-intrusive overall health monitoring

Configuration checks





Exadata Critical Issues

The following Exadata Critical Issues (MOS Note 1270094.1) have been checked in this report:

- This environment has been checked for exposure to the following Exadata Critical Issues from MOS Note 1270094.1
-
- Exadata Database Server and Storage Server : EX1-EX65,EX67,EX69-EX77
- Oracle Database and Grid Infrastructure : DB1-DB4, DB6, DB9-DB50
- Exadata Fabric Switch : IB1-IB3,IB5-IB9

Note: Exadata Critical issues which are not shown in the following table are not applicable to the system configuration.

Exadata Critical Issues on Database Server

Status	Type	Message	Status On	Details

Exadata Critical Issues on Storage Server

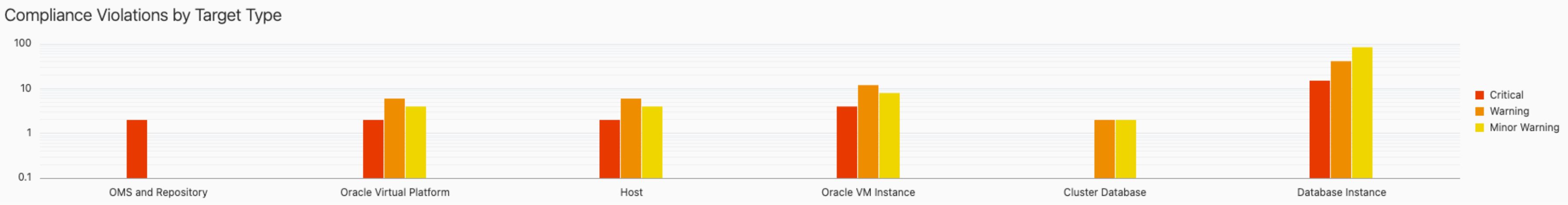
Status	Type	Message	Status On	Details

Database Server

Status	Type	Message	Status On	Details
FAIL	OS Check	Package exadata-sun-computenode-minimum and/or exadata-sun-computenode is not installed	[redacted]adm02	View
FAIL	OS Check	The Name Service Cache Daemon (NSCD) configuration is not correct	All Database Servers	View

Storage Server

Status	Type	Message	Status On	Details
FAIL	Storage Server Check	One or more unacceptable storage server hidden parameters were discovered	All Storage Servers	View

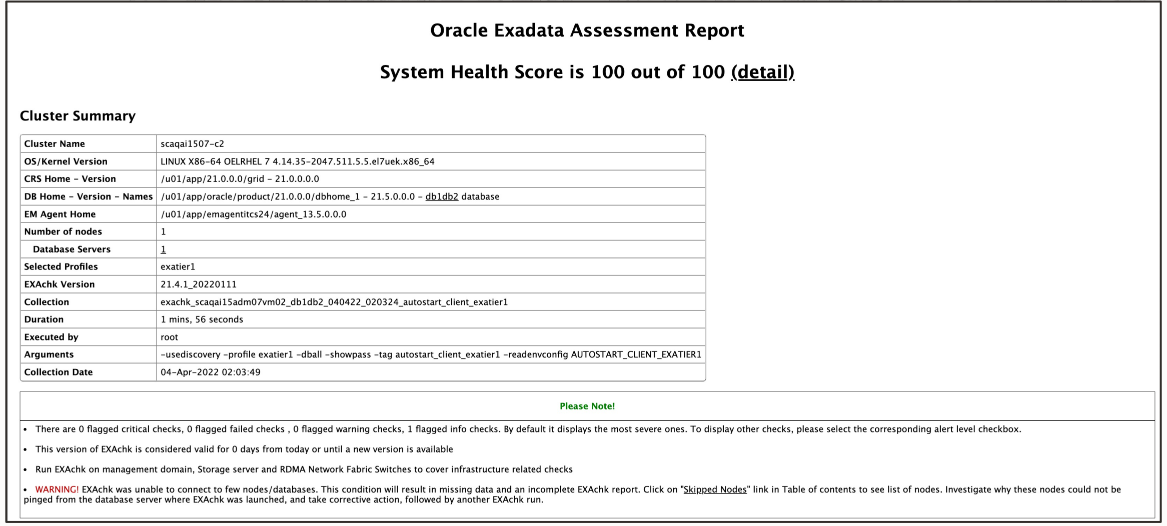


Autonomous Health Compliance Checks

Comprehensive centralized solution for EXAchk reports

Notifies DBAs to with fix issues and guidance for implement best practices

Easily establish baselines and compare reports after fixes, patching and upgrades



Oracle Exadata Assessment Report

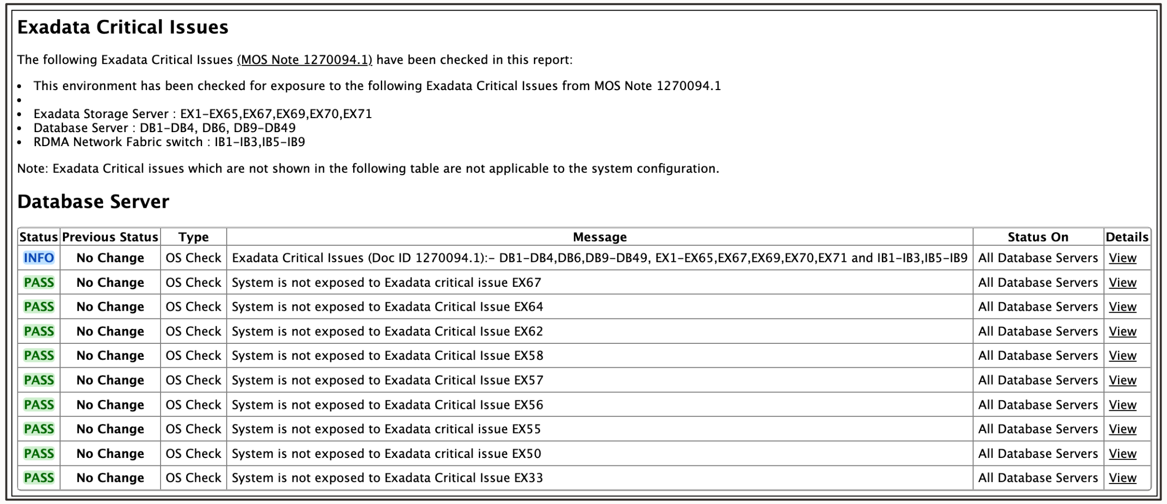
System Health Score is 100 out of 100 (detail)

Cluster Summary

Cluster Name	scaqai1507-c2
OS/Kernel Version	LINUX X86-64 OELRHEL 7 4.14.35-2047.511.5.5.el7uek.x86_64
CRS Home - Version	/u01/app/21.0.0.0/grid - 21.0.0.0.0
DB Home - Version - Names	/u01/app/oracle/product/21.0.0.0/dbhome_1 - 21.5.0.0.0 - db1db2 database
EM Agent Home	/u01/app/emagentitcs24/agent_13.5.0.0.0
Number of nodes	1
Database Servers	1
Selected Profiles	exatier1
EXAchk Version	21.4.1_20220111
Collection	exachk_scaqai15adm07vm02_db1db2_040422_020324_autostart_client_exatier1
Duration	1 mins, 56 seconds
Executed by	root
Arguments	-usediscovery -profile exatier1 -dball -showpass -tag autostart_client_exatier1 -readenvconfig AUTOSTART_CLIENT_EXATIER1
Collection Date	04-Apr-2022 02:03:49

Please Note!

- There are 0 flagged critical checks, 0 flagged failed checks , 0 flagged warning checks, 1 flagged info checks. By default it displays the most severe ones. To display other checks, please select the corresponding alert level checkbox.
- This version of EXAchk is considered valid for 0 days from today or until a new version is available
- Run EXAchk on management domain, Storage server and RDMA Network Fabric Switches to cover infrastructure related checks
- WARNING! EXAchk was unable to connect to few nodes/databases. This condition will result in missing data and an incomplete EXAchk report. Click on "Skipped Nodes" link in Table of contents to see list of nodes. Investigate why these nodes could not be pinged from the database server where EXAchk was launched, and take corrective action, followed by another EXAchk run.



Exadata Critical Issues

The following Exadata Critical Issues (MOS Note 1270094.1) have been checked in this report:

- This environment has been checked for exposure to the following Exadata Critical Issues from MOS Note 1270094.1
-
- Exadata Storage Server : EX1-EX65,EX67,EX69,EX70,EX71
- Database Server : DB1-DB4, DB6, DB9-DB49
- RDMA Network Fabric switch : IB1-IB3,IB5-IB9

Note: Exadata Critical issues which are not shown in the following table are not applicable to the system configuration.

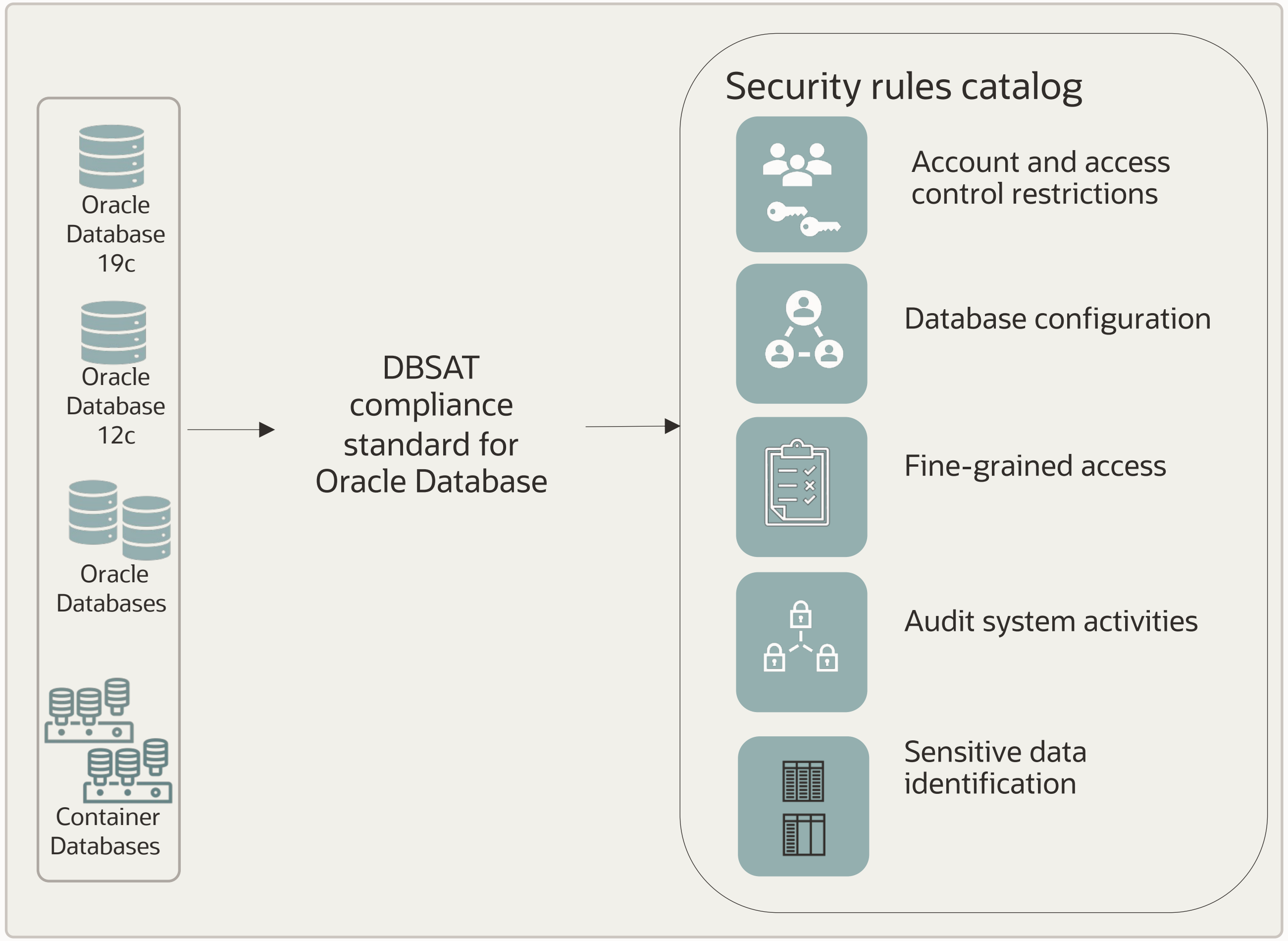
Database Server

Status	Previous Status	Type	Message	Status On	Details
INFO	No Change	OS Check	Exadata Critical Issues (Doc ID 1270094.1):- DB1-DB4,DB6,DB9-DB49, EX1-EX65,EX67,EX69,EX70,EX71 and IB1-IB3,IB5-IB9	All Database Servers	View
PASS	No Change	OS Check	System is not exposed to Exadata critical issue EX67	All Database Servers	View
PASS	No Change	OS Check	System is not exposed to Exadata Critical Issue EX64	All Database Servers	View
PASS	No Change	OS Check	System is not exposed to Exadata Critical Issue EX62	All Database Servers	View
PASS	No Change	OS Check	System is not exposed to Exadata Critical Issue EX58	All Database Servers	View
PASS	No Change	OS Check	System is not exposed to Exadata Critical Issue EX57	All Database Servers	View
PASS	No Change	OS Check	System is not exposed to Exadata Critical Issue EX56	All Database Servers	View
PASS	No Change	OS Check	System is not exposed to Exadata critical issue EX55	All Database Servers	View
PASS	No Change	OS Check	System is not exposed to Exadata critical issue EX50	All Database Servers	View
PASS	No Change	OS Check	System is not exposed to Exadata Critical Issue EX33	All Database Servers	View

Database security Assessment Tool (DBSAT)

Security assessment with DBSAT

Assess, detect, and remediate



Add a layer of security compliance check

Catalog of rules for

- User access and restrictions
- Database configuration
- Fine-grained access control
- Auditing system activities
- Sensitive data identification

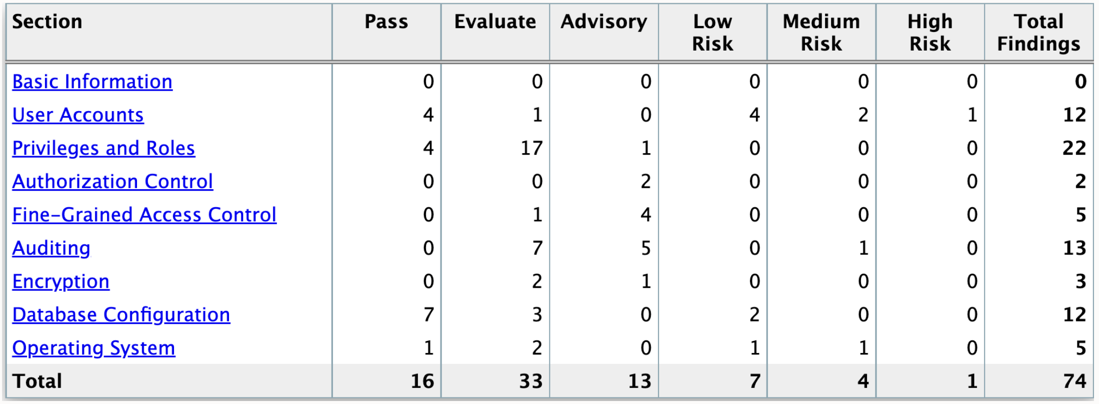
Review and remediate violations

Audit report for compliance

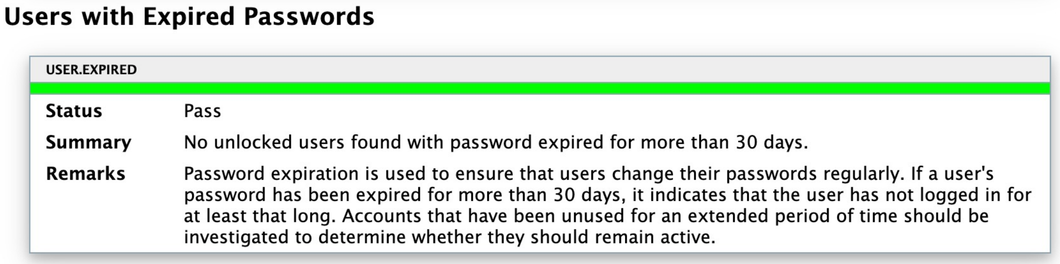
DBSAT Actionable Reports

Security Assessment

- Detect security configuration issues
- Findings mapped to CIS, STIG and GDPR benchmarks



Section	Pass	Evaluate	Advisory	Low Risk	Medium Risk	High Risk	Total Findings
Basic Information	0	0	0	0	0	0	0
User Accounts	4	1	0	4	2	1	12
Privileges and Roles	4	17	1	0	0	0	22
Authorization Control	0	0	2	0	0	0	2
Fine-Grained Access Control	0	1	4	0	0	0	5
Auditing	0	7	5	0	1	0	13
Encryption	0	2	1	0	0	0	3
Database Configuration	7	3	0	2	0	0	12
Operating System	1	2	0	1	1	0	5
Total	**16**	**33**	**13**	**7**	**4**	**1**	**74**



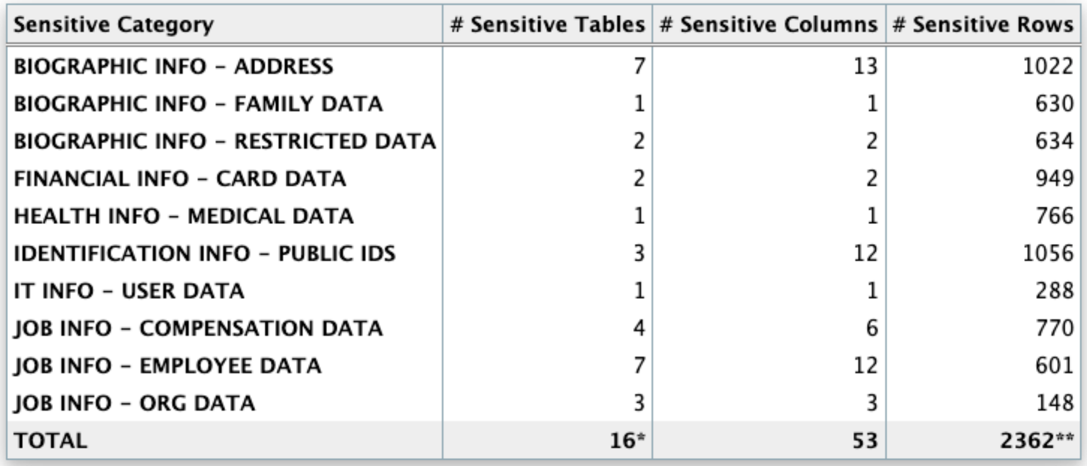
Users with Expired Passwords

USER.EXPIRED

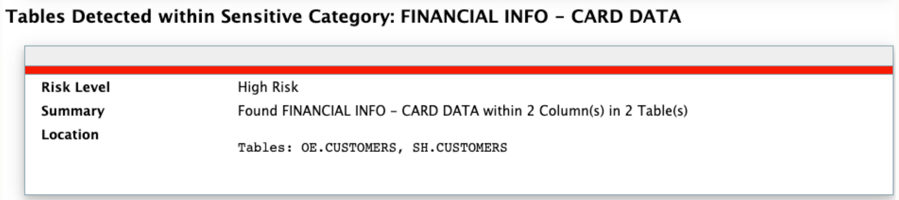
Status	Pass
Summary	No unlocked users found with password expired for more than 30 days.
Remarks	Password expiration is used to ensure that users change their passwords regularly. If a user's password has been expired for more than 30 days, it indicates that the user has not logged in for at least that long. Accounts that have been unused for an extended period of time should be investigated to determine whether they should remain active.

Sensitive data identification

- Assess sensitive data in database targets
- Audit reports for compliance with policies



Sensitive Category	# Sensitive Tables	# Sensitive Columns	# Sensitive Rows
BIOGRAPHIC INFO - ADDRESS	7	13	1022
BIOGRAPHIC INFO - FAMILY DATA	1	1	630
BIOGRAPHIC INFO - RESTRICTED DATA	2	2	634
FINANCIAL INFO - CARD DATA	2	2	949
HEALTH INFO - MEDICAL DATA	1	1	766
IDENTIFICATION INFO - PUBLIC IDS	3	12	1056
IT INFO - USER DATA	1	1	288
JOB INFO - COMPENSATION DATA	4	6	770
JOB INFO - EMPLOYEE DATA	7	12	601
JOB INFO - ORG DATA	3	3	148
TOTAL	16*	53	2362**



Tables Detected within Sensitive Category: FINANCIAL INFO - CARD DATA

Risk Level	High Risk
Summary	Found FINANCIAL INFO - CARD DATA within 2 Column(s) in 2 Table(s)
Location	`Tables: OE.CUSTOMERS, SH.CUSTOMERS`

Configuration Management

Manage configuration drift and strive for standardized configuration

Security configuration management

Control configuration deviations from baseline

Features

- Continuous comparison against baseline
- Track drift to maintain consistency with baseline
- Customize out-of-box baselines for compliance
- Configuration extension for custom collections
- Automated remediation of deviations
- Monitor configuration history for changes
- Perform root cause and impact analysis

Benefits

- Improved security posture
- Standardize on configurations
- Audit for compliance with policies
- Remediation recommendations
- Reduce ops time with automation
- Minimize maintenance window

Configuration Drift and Consistency Management

Key customer use cases

Any Database

Database Initialization Parameters

Saved database reference to 1200+ databases

Compare only required initialization parameters

Detect configuration deviation, and notify

Automated remediation mechanisms

Any Database

RAC Database Instances

Consistency of instances within 500+ Cluster databases

Monitor for consistency deviation and notify

Automated remediation mechanisms

Host Configurations

Live Linux host reference to 1000+ hosts

Compare extended configuration collections

Compare only required parameters

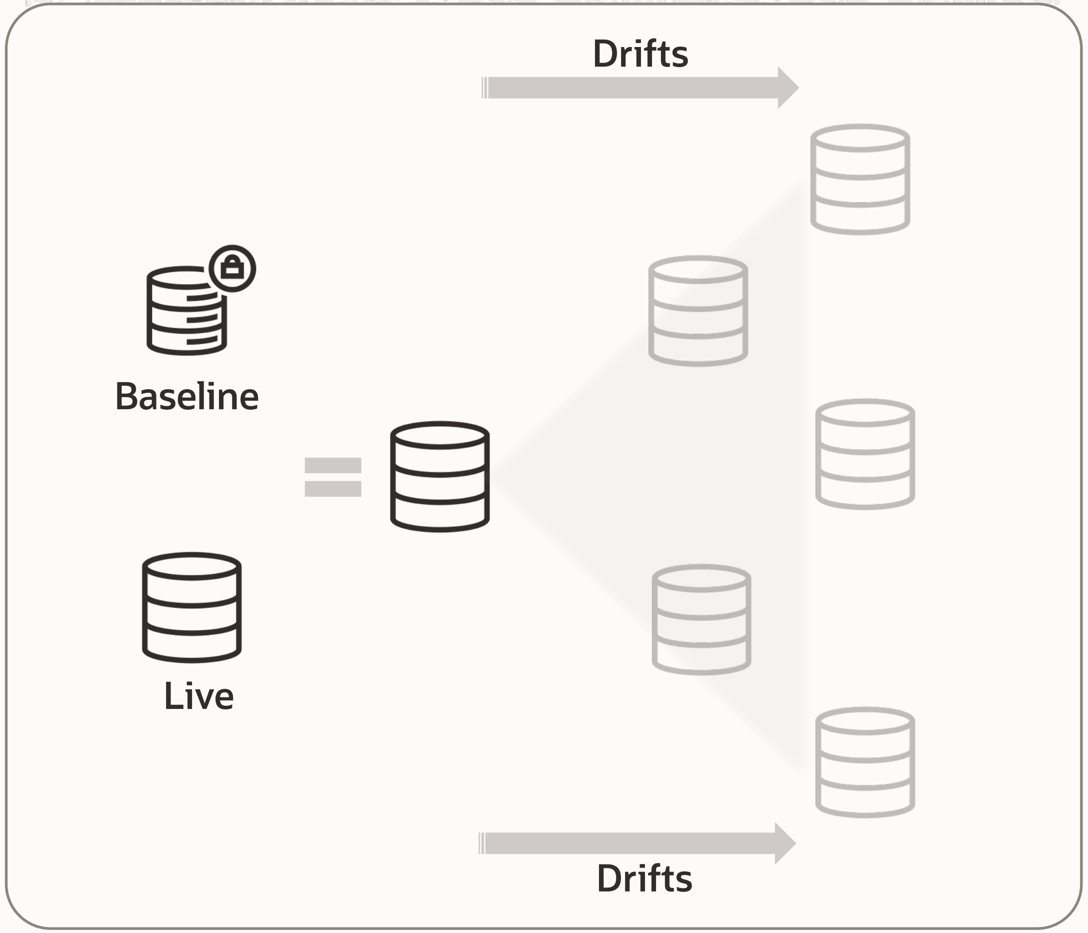
Detect configuration deviation, and notify

Engineered Systems Consistency

Consistency of Storage Cells within Exadata

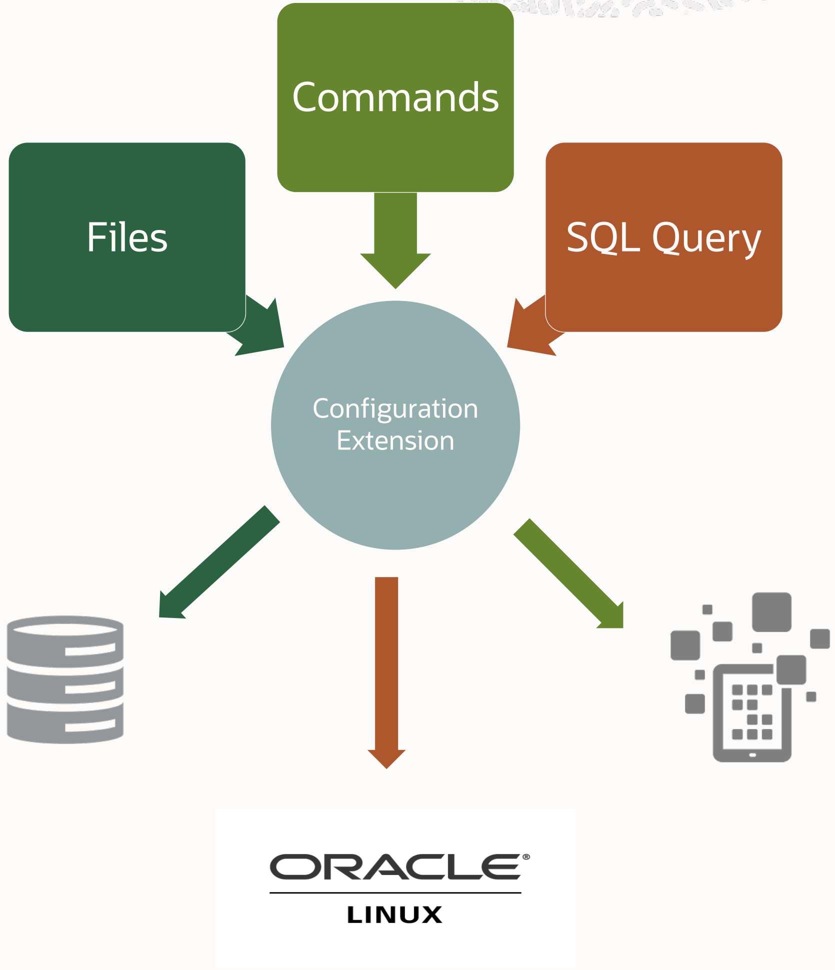
Configuration Comparison - Drift

- Large scale and dynamic same-type target configuration difference tracking
- Compare latest or saved configuration to one or more targets
- Source can be live or saved baseline
- Ensure target configuration remains the same as baseline or saved target
- Notification when configuration change results in undesired differences



Augment Configuration Collection

- Augment configuration data collected
- Collect configuration data that EM does not already collect
- All configuration management features (search, history, etc.) available for custom configuration collections
  - Compare properties between targets
  - Review history
  - Search configuration data
  - Create compliance rules
- Multiple Collection Methods:
  - Entire File
  - OS Command Output
  - SQL Query



Demo – CIS and PCI Compliance Standard

CIS Compliance Audit and Logging Policies and Procedures

PCI – DSS: File permissions rule validations to all users including root user

Q&A
Learn More

Web: oracle.com/enterprisemanager

Videos: youtube.com/OracleEnterpriseMgr

Blogs: blogs.oracle.com/observability

Docs: docs.oracle.com/en/enterprise-manager/

Try it now

Hands-on-labs

Oracle Cloud Free Tier

Always Free

Services you can use for unlimited time

+

30-Day Free Trial

Free credits you can use for more services

www.oracle.com/cloud/free

ORACLE