ORACLE

# Reduce database security vulnerabilities by automating continuous compliance checks and hardening following Industry Standard Best Practices

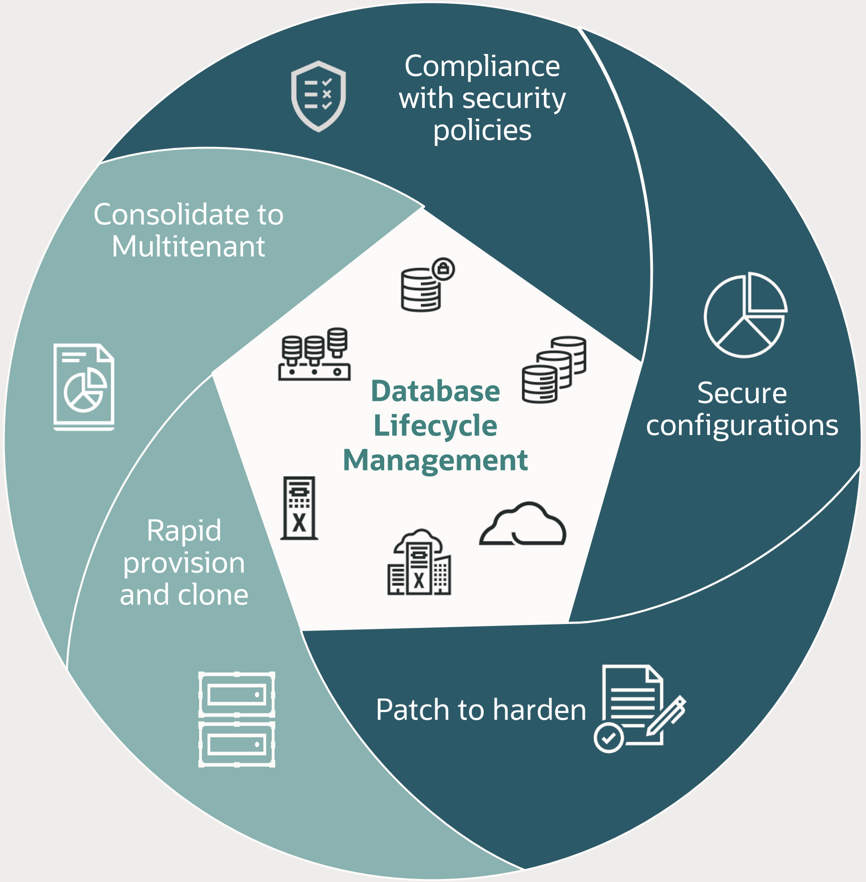
## with Enterprise Manager

**Shiva Prasad**

Product Management

# Automate database lifecycle operations

## Database Lifecycle Management Pack (DBLM)


Compliance with security policies
Consolidate to Multitenant
Secure configurations
Database Lifecycle Management
Rapid provision and clone
Patch to harden

### Protect from breaches

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

### Audit and manage compliance

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

### Manage configuration drift and deviation

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

### Automate repetitive provision and clone activities

Deploy standardized database configuration

### Multiple interfaces – REST APIs, EMCLI and UI

# Manage compliance

Modernize compliance to enhance security posture and mitigate risks

# Stakeholders in your organization to secure assets

Security hardening is a strategic priority

### CFO

Influencer

- Ensure corporate or regulatory compliance
- Reduce risk across multicloud environment
- Secure data by masking, apply security patches
- Audit for compliance

### CISO

Influencer

- Protect data and ensure regulatory compliance
- Intrusion attempts, mean time to detect and resolve
- Average time to patch vulnerabilities
- Security audit and apply recommendations

### CIO/Architect

Influencer

- Identify regulatory compliance to be met
- Automate to secure multicloud environment
- Patch to secure and protect data, align with compliance
- Audit every activity on each asset

### DBA

Decision Maker/Influencer

- Complexity in managing multiple databases for security
- Manage privileged, and orphaned accounts
- Number of known (un)resolved vulnerabilities
- 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.

# Automate hardening of Security Compliance

## Secure entire stack assets, and reduce risks

### Stack Security Compliance

**Oracle Databases**

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

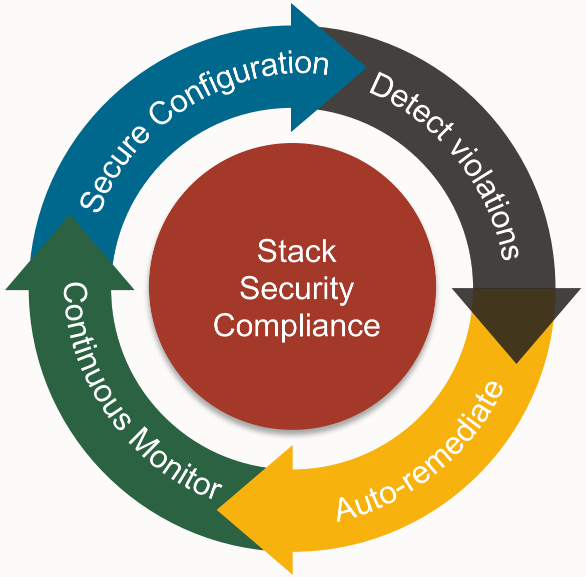
ORACLE Linux

**Hosts**

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

**Exadata Systems**

Exadata best practices and security recommendations



- Stack-level security posture by continuous monitoring
- Leverage industry, and regulatory standards
- Audit security reports for compliance
- Reduce OpEx by auto-remediation of security violations

# 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 12c and 19c

### Security Technical Implementation Guide (STIG)

- DoD published standards for Oracle Database 12c and 19c

### Oracle Security Best Practices

- Basic security configuration
- High security configuration
- Storage best practices
- Configuration best practices

### Database Security Assessment Tool (DBSAT)

- Oracle Database security assessment: configuration, risky users and sensitive data
- Sensitive data discovery: identify amount of sensitive data and its residency

# 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

# CIS Critical Security Controls

1. Continuous Vulnerability Management
2. Secure Configuration of Enterprise Assets
3. Account Management
4. Access Control Management
5. Audit Log Management
6. Inventory and Control of Software Assets
7. Data Protection

**Security framework for configuration guidelines to mitigate risks**

# CIS critical security controls implementation

CIS for DB 19c controls Implementation Groups (IGs)

### IG1 - Essential Cyber Hygiene

- Minimum security controls
- Foundational safeguards with 56 controls

Enable or disable auditing

Login authentication attempts

Revoke EXECUTE from PUBLIC on packages

### IG2 – Additional Safeguards

- Security posture builds on top of IG1
- Elevate compliance with 74 unique controls

Apply remote user' OS roles to DB management

Ensure DBA users are not authenticated by remote OS to allow access to databases with full authorization

### IG3 – Secure Data

- Secure Sensitive and confidential Data
- 11 unique controls in addition to IG1

Revoke EXECUTE from PUBLIC on DBMS_CREDENTIAL package

pdb_os_credential setting determines what OS user will be utilized to run jobs at OS level

# Minimize administrative privileges

## User access and authorization restrictions

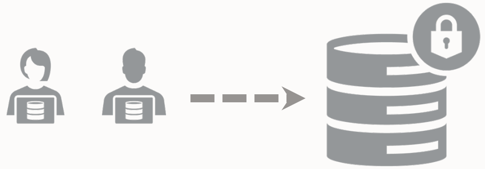
Principles of least privilege – grant privileges only for the job to get done for ongoing security checks and to align with internal security policies

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<br>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 |
| Implementation Group | IG 1 – Essential Cyber Hygiene |

# Comcast

## *Use Case: Risk Management*

### Objective

- Adhere to prioritized **risk management** policies related to DB operations, security & compliance aligned with customized CIS Benchmark
- Ensure secure Oracle Databases by implementing processes to apply Critical Patch Updates (CPUs) as they come out, along with any other critical patches to ensure high availability of business applications performing as per defined requirements

### Requirements

- **Enhance security** posture by detection of violations and automate remediation to align with industry security standards and audit policies
- **Automation** to deploy, upgrade and patch all types of database homes

### Business outcome

- Automated patching if 13000 databases by using Fleet Maintenance solution.
- Successfully deployed CIS compliance for security hardening
  - 24 hours monitoring & management of any violations at fleet-level
  - Used Corrective Actions to automate remediation of any violations
  - Leveraged out-of-box CIS Benchmark to align with compliance policies with specific focus on database parameters, users, privileges, grants, ACLs, and unified auditing
  - Use Enterprise Manager compliance reports for auditing requirements

# 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

### 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

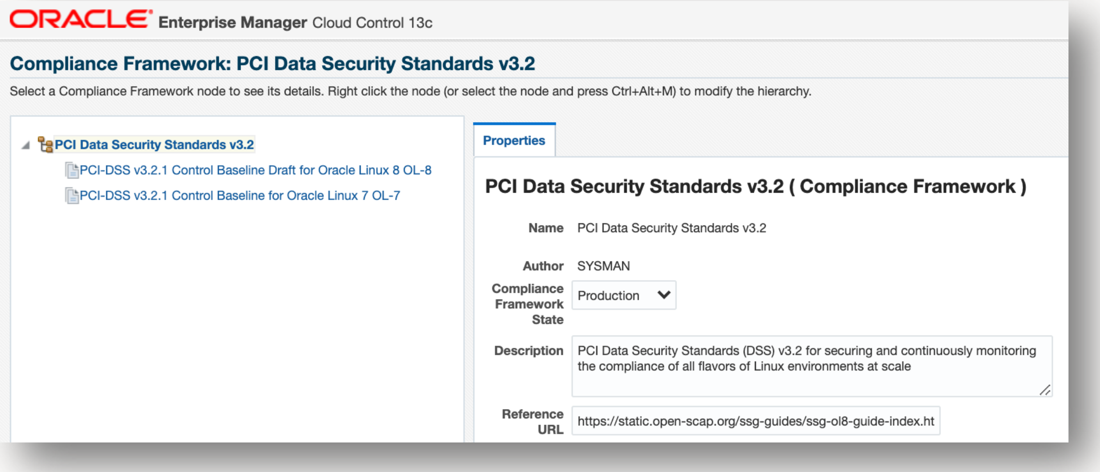
- Maintain a policy that addresses information security for employees and contractors

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



**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

# Exadata System Compliance

# Oracle Autonomous Health Framework EXAchk

## Comprehensive security checks for Exadata ecosystem

Lightweight and non-intrusive compliance check framework for Oracle Exadata Engineered systems designed to check and secure Oracle stack of software and infrastructure components ensuring seamless, reliable and secure database services for users

**Databases** + **Database Servers** + **Infrastructure**

### Security

Checks for taints, limits, insecure configuration, network separation

### Performance

Exadata critical issues, verify memory allocations, network fabric, latency

### Availability

Exadata critical issues, database protection, verify HA services startup

### Scalability

Verify database instances, memory allocation, SCAN listeners, parameters

# Oracle Autonomous Health Framework EXAchk

## Integration with Enterprise Manager

- Fleet-level automated risk identification and proactive remediations
- Scans for security, performance, availability and scalability issues for all components in the system
- Out-of-box AHF EXAchk security compliance standards for Exadata Database Machine and Exadata Cloud
- Comprehensive reports of individual components – both native and EM compliance evaluation reports for audit

Benefits

- Single pane of glass for fleet-level Exadata compliance management
- Remediation using corrective actions

### Infrastructure Security Compliance

Exadata

On-Premises

Best practices for health and security recommendations

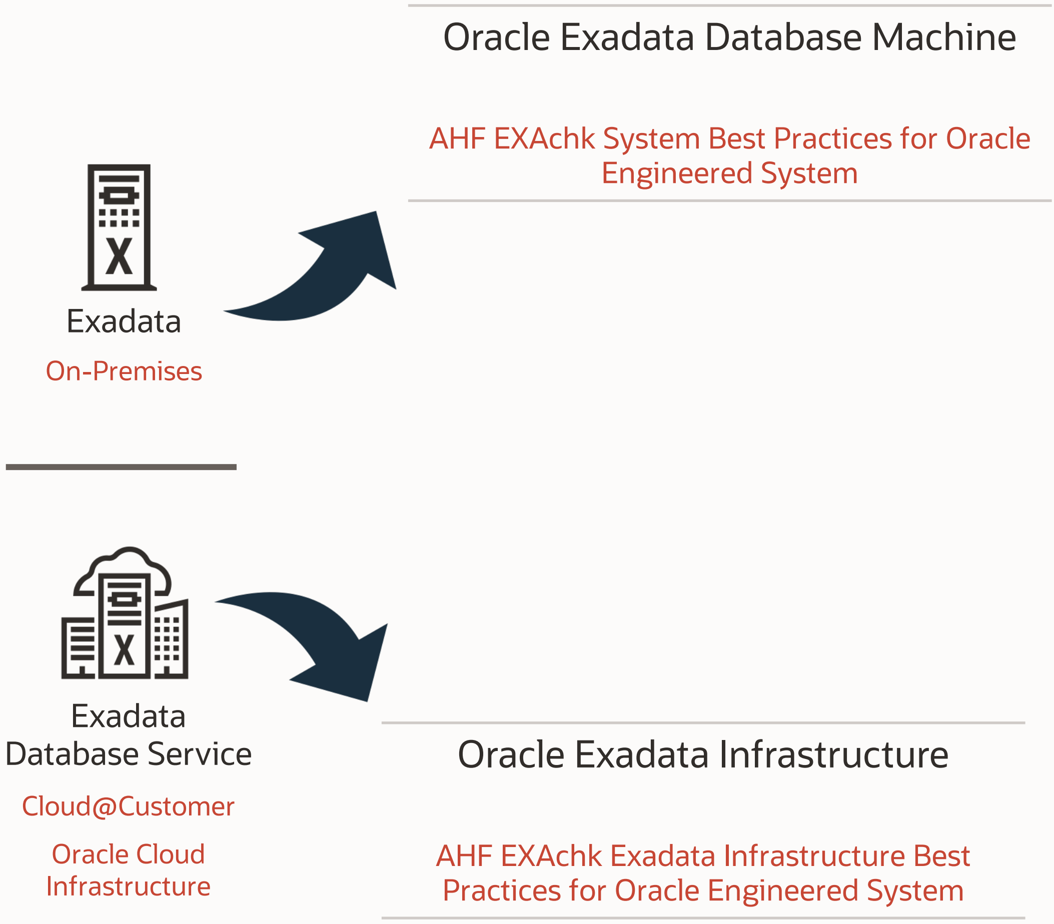
Exadata Database Service

Cloud@Customer

Oracle Cloud Infrastructure

# Exadata compliance management

## Fleet-level health checks



Oracle Exadata Database Machine

AHF EXAchk System Best Practices for Oracle Engineered System

Exadata

On-Premises

Exadata Database Service

Cloud@Customer

Oracle Cloud Infrastructure

Oracle Exadata Infrastructure

AHF EXAchk Exadata Infrastructure Best Practices for Oracle Engineered System

Fleet level association of Engineered Systems for immediate health checks

All components in each Exadata will automatically get associated to its corresponding compliance standards

| | |
|---|---|
| Database Instance Best Practices | InfiniBand Switch Best Practices |
| Cluster Database Best Practices | ASM Best Practices |
| Oracle Home Best Practices | High Availability Service Best Practices |
| Host Best Practices | Systems Infrastructure Switch Best Practices |
| Cluster Best Practices | Virtual Server Best Practices |
| ASM Cluster Best Practices | Virtual Platform Best Practices |
| Storage Server Best Practices | |

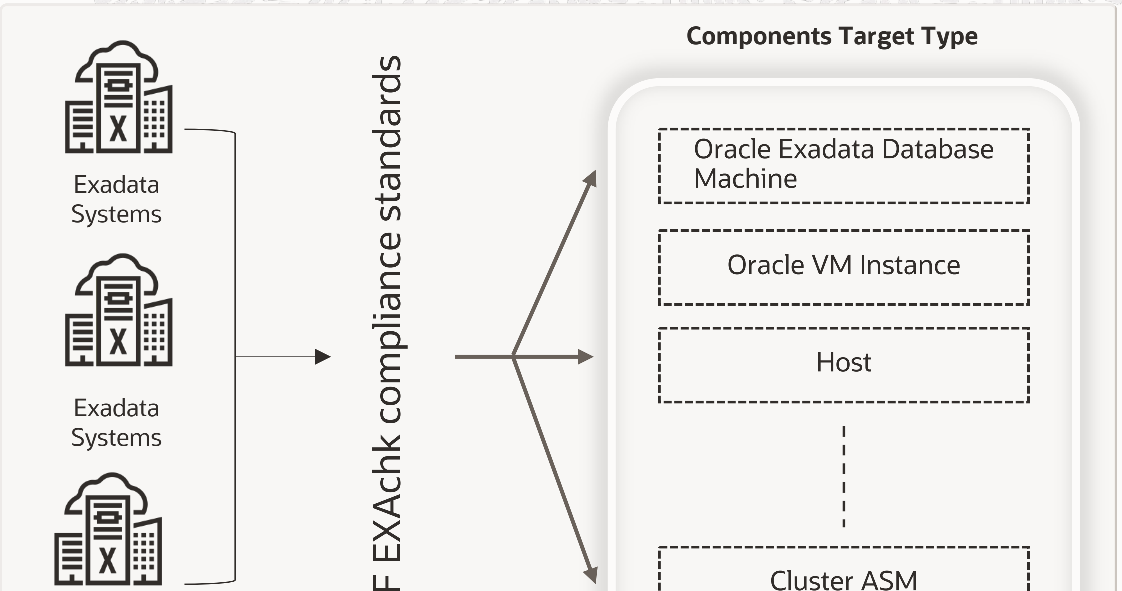
# Automated risk assessment of Exadata systems

Automated risk identifications

Proactive notification of issues for each component

Non-intrusive overall health monitoring

Configuration checks for deviations



Components Target Type

Exadata Systems

Exadata Systems

Exadata Systems

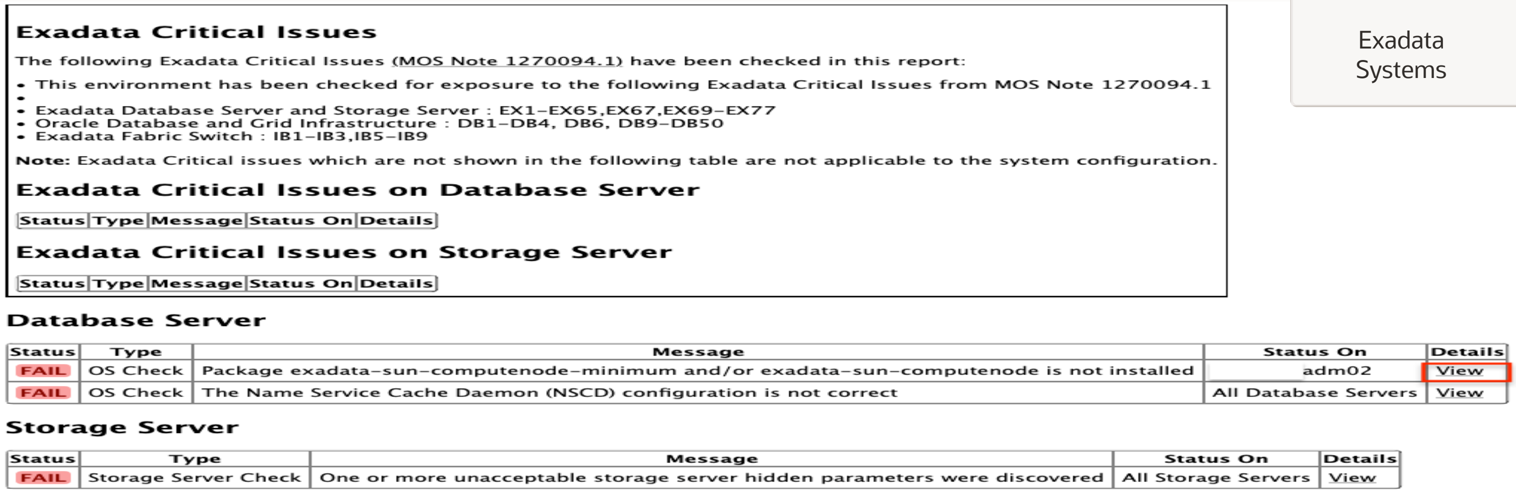
AHF EXAchk compliance standards

Oracle Exadata Database Machine

Oracle VM Instance

Host

Cluster ASM



## 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 | adm02 | View |
| FAIL | OS Check | The Name Service Cache Daemon (NSCD) configuration is not correct | All Database Servers | View |

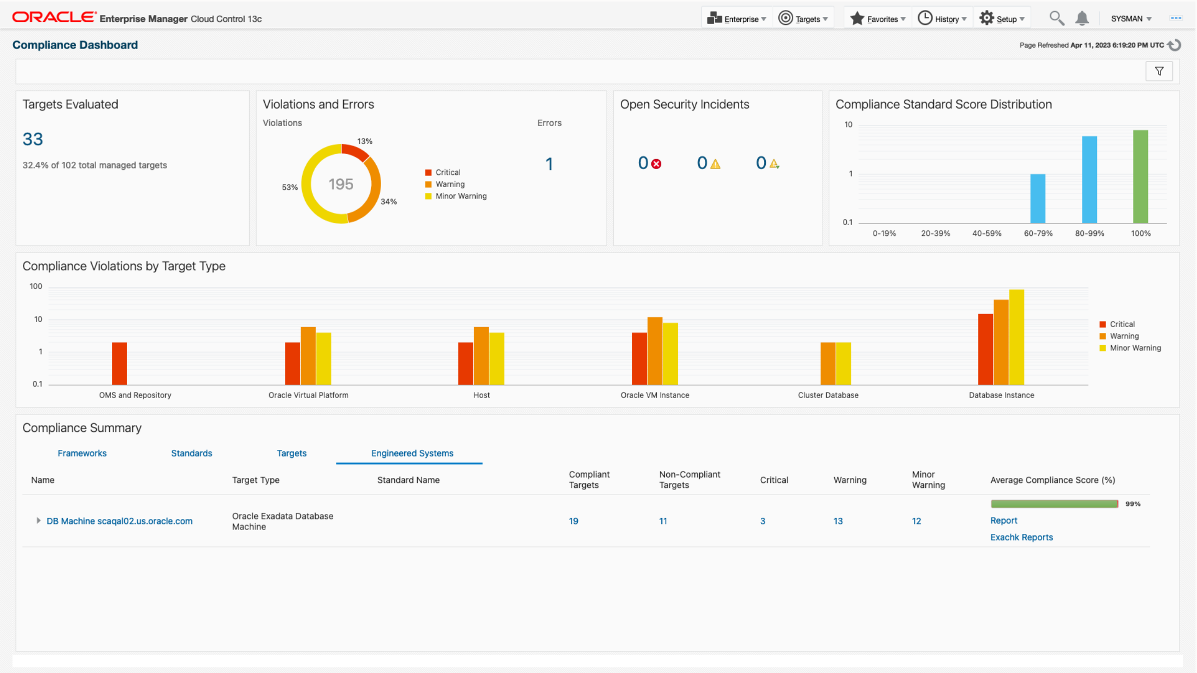
### Storage Server

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

# Automated risk assessment of Exadata systems

## Engineered Systems Dashboard

- Dedicated one-stop place for all Exadata Engineered systems
- Detection of issues and result analysis at Engineered System or at component level
- Drill down analysis of each issue and affected components
- EXAchk native report integration



Compliance Dashboard

Page Refreshed Apr 11, 2023 6:19:20 PM UTC

Targets Evaluated

33

32.4% of 102 total managed targets

Violations and Errors

Open Security Incidents

Compliance Standard Score Distribution

Compliance Violations by Target Type

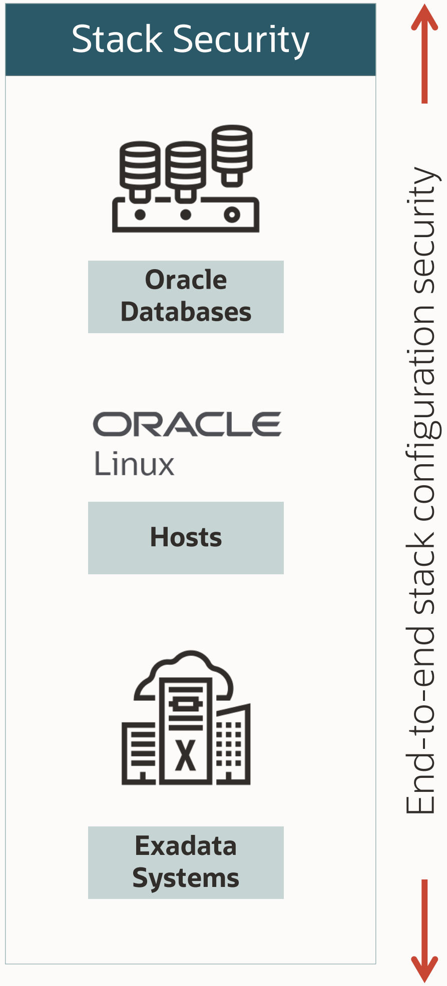
Compliance Summary

Frameworks | Standards | Targets | Engineered Systems

| Name | Target Type | Standard Name | Compliant Targets | Non-Compliant Targets | Critical | Warning | Minor Warning | Average Compliance Score (%) |
|---|---|---|---|---|---|---|---|---|
| DB Machine scaqal02.us.oracle.com | Oracle Exadata Database Machine | | 19 | 11 | 3 | 13 | 12 | 99%<br>Report<br>Exachk Reports |

# Secure databases and infrastructure stack

## Reduce risks by securing entire stack assets



Stack Security

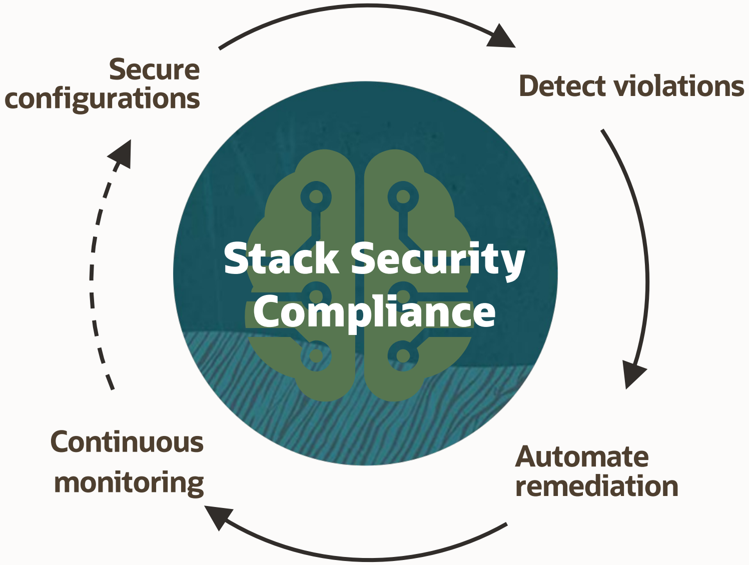
Oracle Databases

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, leverage AHF EXAchk for health, performance and security checks

# Demo on CIS Compliance Corrective Action

# Q&A
# Learn More

Web: oracle.com/enterprisemanager

Videos: youtube.com/OracleEnterpriseMgr

How-to-Videos: CIS Violation Corrective Action

Blogs: blogs.oracle.com/observability

CIS Compliance Blog

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

# Thank you
# Q & A