ORACLE

Get Time Back in Your Day and Be More Secure

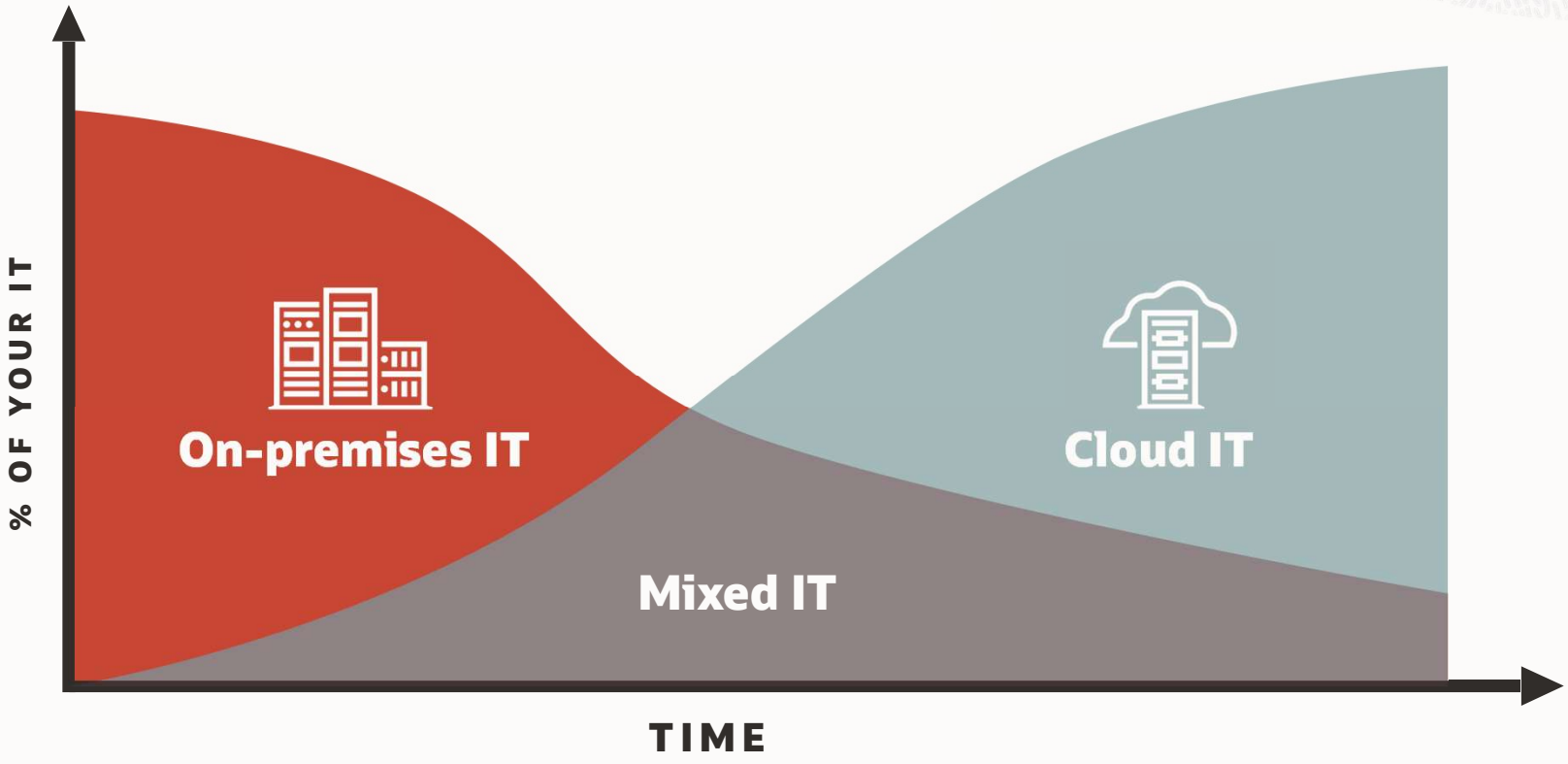
Best Practices for Automating Vulnerability Detection, Patching, and Compliance of your Databases and Infrastructure

Romit Acharya
Product Manager

NYOUG

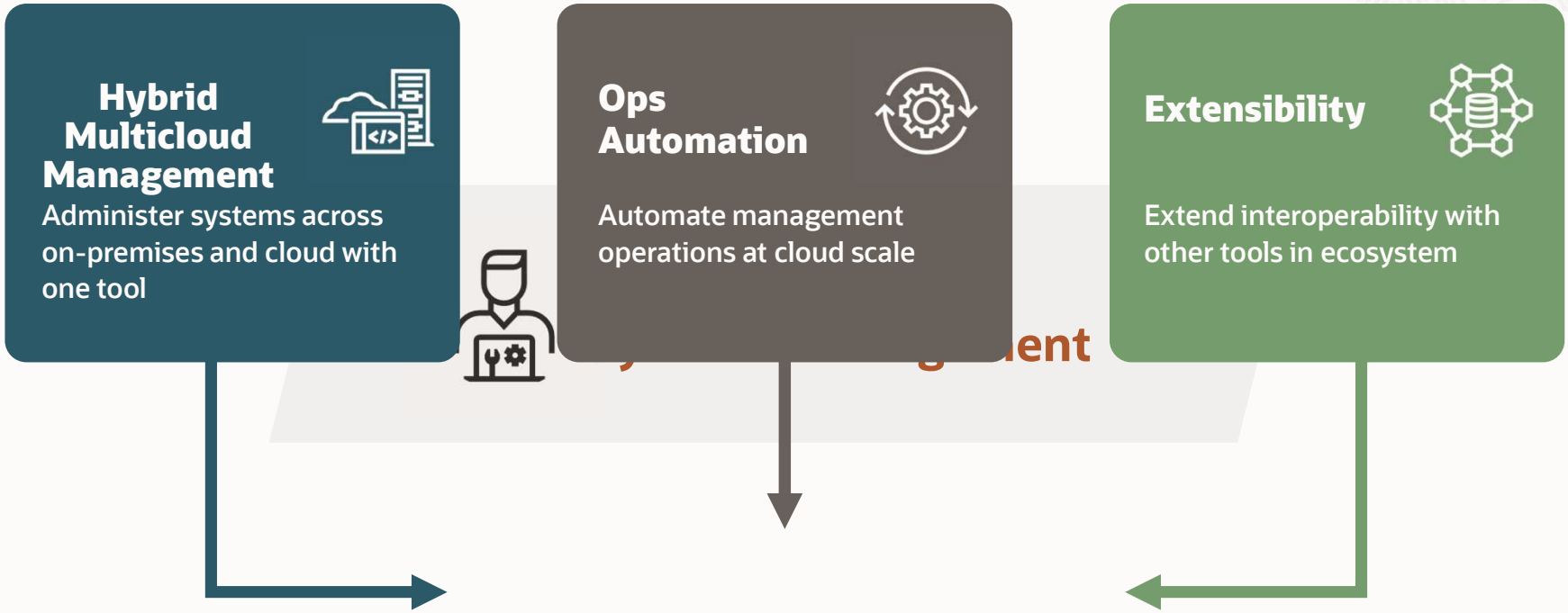
IT management cloud transition

Most enterprises have mixed IT



Copyright © 2023, Oracle and/or its affiliates

Systems Management requirements are also evolving



Copyright © 2023, Oracle and/or its affiliates

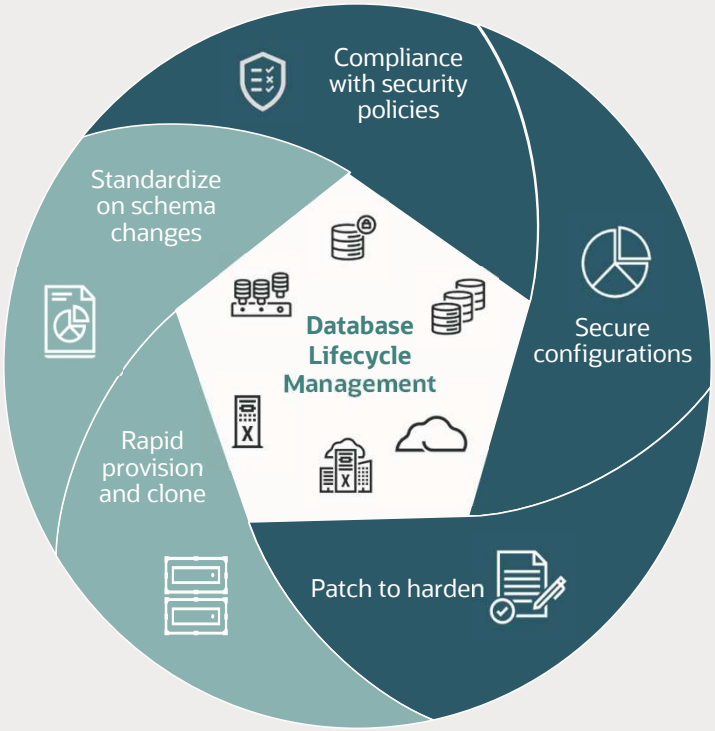
Ops Automation

Database Lifecycle Management

Copyright © 2023, Oracle and/or its affiliates

Security hardening

Database Lifecycle Management (DBLM)



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

Copyright © 2023, Oracle and/or its affiliates

Database Lifecycle Management

Benefits

Lower costs

Consolidate assets for ease of deployment and management in hybrid environment, reduce CapEx and OpEx cost with inventory utilization assessment and trends

Reduce risk

Standardize and secure configurations to manage risks, and compliance with security

Deploy security patches at scale to strengthen overall security posture

Accelerate innovation

Automate delivery of time-consuming and error prone operations like deployment of infrastructure for applications, secure and audit for compliance

Copyright © 2023, Oracle and/or its affiliates

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

Copyright © 2023, Oracle and/or its affiliates

Automate active management in Exadata (On-premises and Cloud)

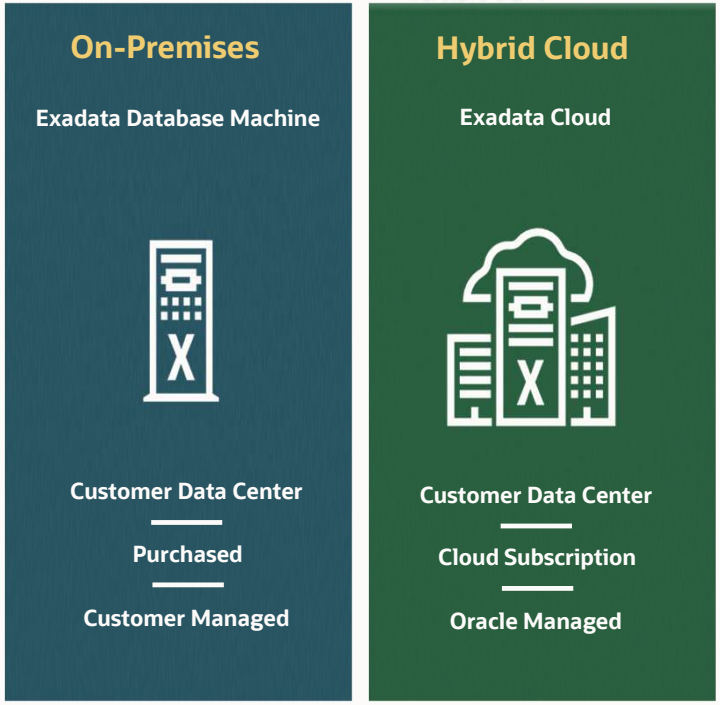
One management tool for hybrid multicloud environment

Database management

- Compliance with industry and regulatory security policies
- Secure configuration deviations with baselines
- AHF EXAchk for Exadata health and performance management
- Upgrade and patch all supported databases at scale
- Automate database deployment – provision, create, unplug, plug, clone

Hybrid cloud management

- Enable DevOps users for on-demand deployment
- Tenant isolation, and security
- Database-as-a-service options: DBaaS, PDBaaS, Hybrid-as-a-Service
- Rapidly clone and save storage with Snap clone
- Chargeback and metering



Copyright © 2023, Oracle and/or its affiliates

Compliance

Database Lifecycle Management

Copyright © 2023, Oracle and/or its affiliates

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 security posture by continuous monitoring
- Security policy management across heterogeneous targets and hybrid environments
- Leverage industry, and regulatory standards
- Audit security reports for compliance
- Reduce DBA time by auto-remediation of security violations

Copyright © 2023, Oracle and/or its affiliates

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

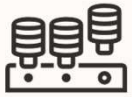
Import Linux compliance standard in Extensible Configuration Checklist Description Format (XCCDF)

Copyright © 2023, Oracle and/or its affiliates

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

CIS. Center for Internet Security®

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

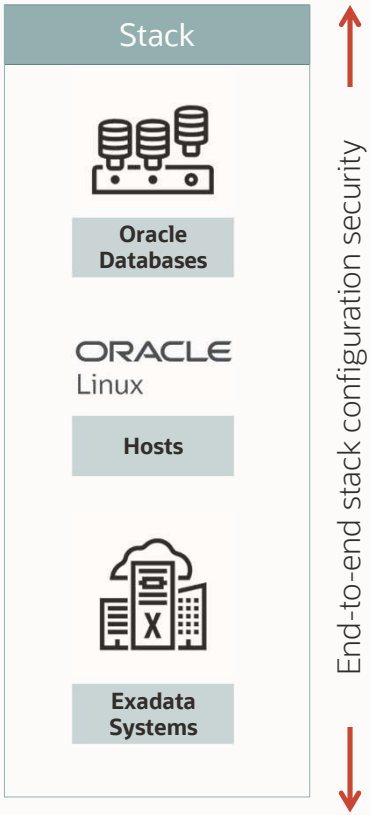
Database Security Assessment Tool (DBSAT)

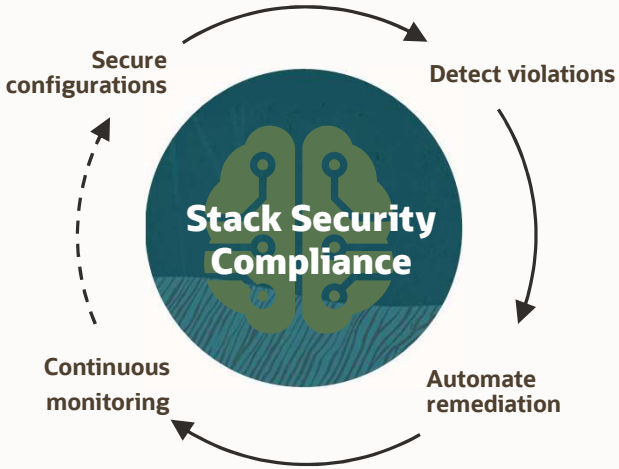
- Assess Oracle Database security: configuration, risky users and sensitive data

Copyright © 2023, Oracle and/or its affiliates

Secure databases and infrastructure stack

Secure entire stack assets, and reduce risks





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

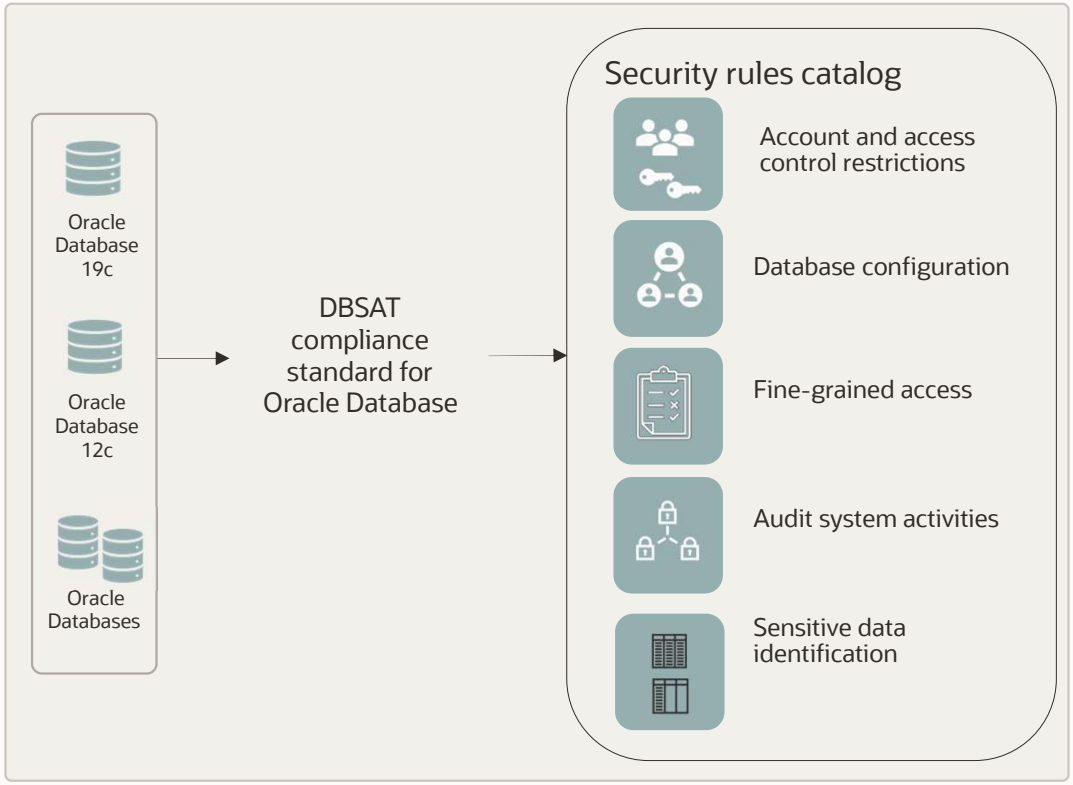
Exadata and Exadata Cloud Infrastructure

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

Copyright © 2023, Oracle and/or its affiliates

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

Copyright © 2023, Oracle and/or its affiliates

Secure databases

Automated timely patching reduces downtime, enhances security posture and achieves compliance with IT security policies

Copyright © 2023, Oracle and/or its affiliates

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

Copyright © 2023, Oracle and/or its affiliates

Modernizing your patching model addresses key business concerns

Unpatched systems

High risk of breaches

21% of breaches[1] due to unpatched systems even though patches were available

Misconfigurations

Preferred ways to exploit are misconfiguration and insecure configuration changes

45% of breaches[1] were due to misconfigurations

Compromised credentials

Contributes to breaches and security incidents

82% of breaches[1] in 2022 leveraged stolen and/or weak credentials

Configuration sprawl

Lack of standardized configurations increases vulnerability

Scripts are error prone and high maintenance cost

Copyright © 2023, Oracle and/or its affiliates

Source : 1 - Verizon report

Enterprise Manager Fleet Maintenance

Features

- Security patch recommendations
- Configuration standardization advisor
- Out of place, end state driven patching
- Custom pre-scripts and post-scripts
- Automate with Orchestration and DevOps tools
- Zero downtime rolling patch at scale

Benefits

- Security-first processes
- Compliance with regulatory
- Insights to vulnerabilities
- Lower OpEx with standardization
- Reduce maintenance window
- Near zero-downtime

Copyright © 2023, Oracle and/or its affiliates

Patching across hybrid environment

Guided Intelligent Workflows

- Smart security patch recommendations
- Automated risk assessment
- End-to-end automation to apply patches

Robust Operational Control

- Consistent interfaces – API, EMCLI and UI
- Patch lifecycle operations scheduling
- Troubleshoot, retry, and resume operations

Copyright © 2023, Oracle and/or its affiliates

Fleet Maintenance – upgrade and patch at scale

1. **Scan fleet, discover configuration pollution**
   - Advisor scans the fleet for configuration variations
   - Provides recommendations to standardize

2. **Create new image and subscribe**
   - Define end states for software as images
   - Subscribe databases/pools to the images

3. **Push image and switch**
   - Deploy image and schedule the subscribes to switch

11.2.0.4
12c
18c
19c
21c+

Multitenant (CDB and PDB) | Oracle RAC and RAC One | Oracle Restart
Database Instance | Grid Infrastructure | Data Guard configurations

Exadata | Exadata Cloud | Commodity hardware

Public Cloud

Windows | AIX | ORACLE Solaris

Copyright © 2023, Oracle and/or its affiliates

New features in Fleet Maintenance

UI enhancements

Fleet Maintenance Hub

Multitenant upgrade and patching operations

Upgrade non-multitenant to multitenant

Scheduling flexibility for Oracle home deploy and update operations

Automation

Patch recommendations for creating/refreshing gold images

Rollback support for DB/RAC patching and upgrade failures

Rollback support for GI and Oracle Restart patching and upgrade failures

Security

Privileged Access Management (PAM) based authentication support for patching operations

TDE Support: DB 19c/21c/ExaCC provisioning and patching support

TDE Support: Patching for Init param based config

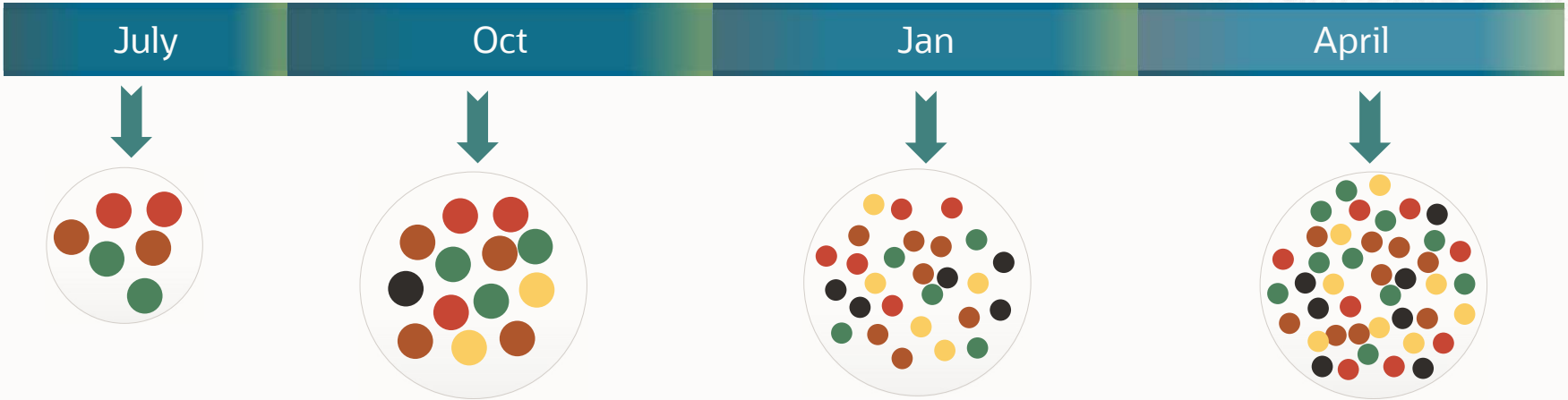
Copyright © 2023, Oracle and/or its affiliates

Protect and enhance security posture

Fleet Maintenance Hub

Copyright © 2023, Oracle and/or its affiliates

Security patch recommendations



Patch severities and affected targets determine priorities to patch now or later

Insight into **patch recommendations and severities** helps in faster decisions

High OpEx for manual patch analysis. Automated prioritized list leads to quicker response

Quickly apply **to secure and manage risks** from multiple sources

Copyright © 2023, Oracle and/or its affiliates

Critical High Medium Low Info

Simplify security across hybrid environment

Security patch recommendations
for all database versions and types supported

Insight into affected database targets
assets across on-premises and cloud

Apply to be patch compliant
deploy security patches to all targets

Single pane of glass for patch recommendations, patching and patch compliance

Copyright © 2023, Oracle and/or its affiliates

Fleet Maintenance Hub

One stop place for operational control, and enhanced security

Security patch recommendations

Database compliance with patch policies

Automated insight into affected gold images

Risk assessment of targets to subscribe

Seamless end-to-end fleet-level integrated story across hybrid environment

Copyright © 2023, Oracle and/or its affiliates

Fleet Maintenance Hub

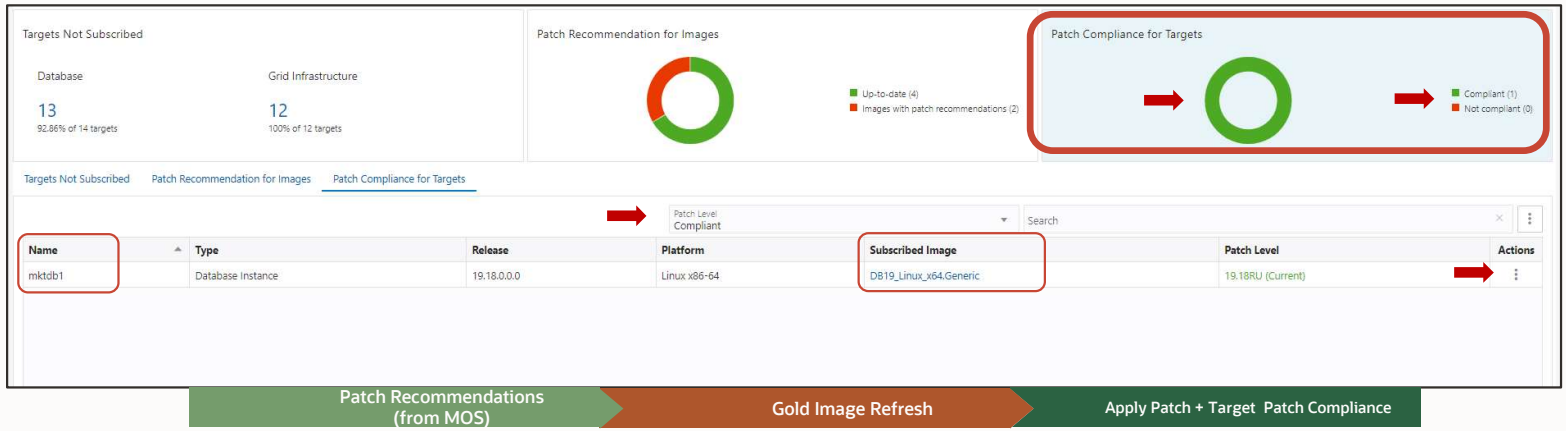
One stop place for operational control, and enhanced security

Security patch recommendations

Automated insight into affected gold images

Database compliance with patch policies

Risk assessment of targets to subscribe



Patch Recommendations (from MOS) → Gold Image Refresh → Apply Patch + Target Patch Compliance

Seamless end-to-end fleet-level integrated story across hybrid environment

Copyright © 2023, Oracle and/or its affiliates

Fleet Maintenance Hub

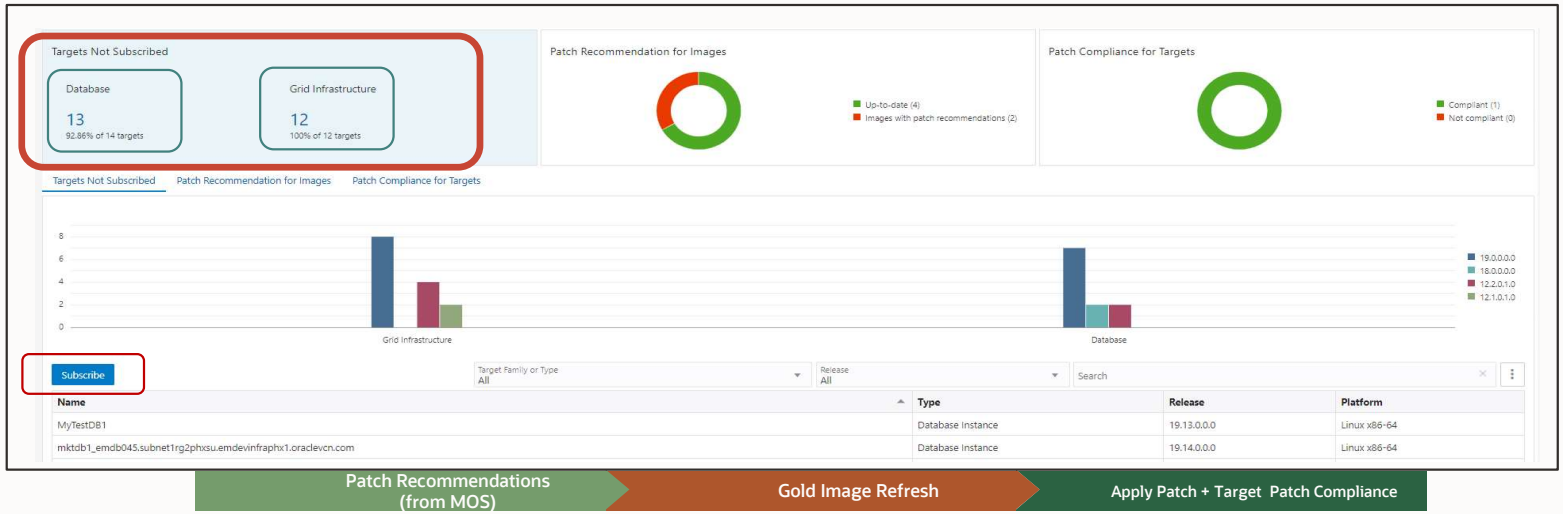
One stop place for operational control, and enhanced security

Security patch recommendations

Database compliance with patch policies

Automated insight into affected gold images

Risk assessment of targets to subscribe



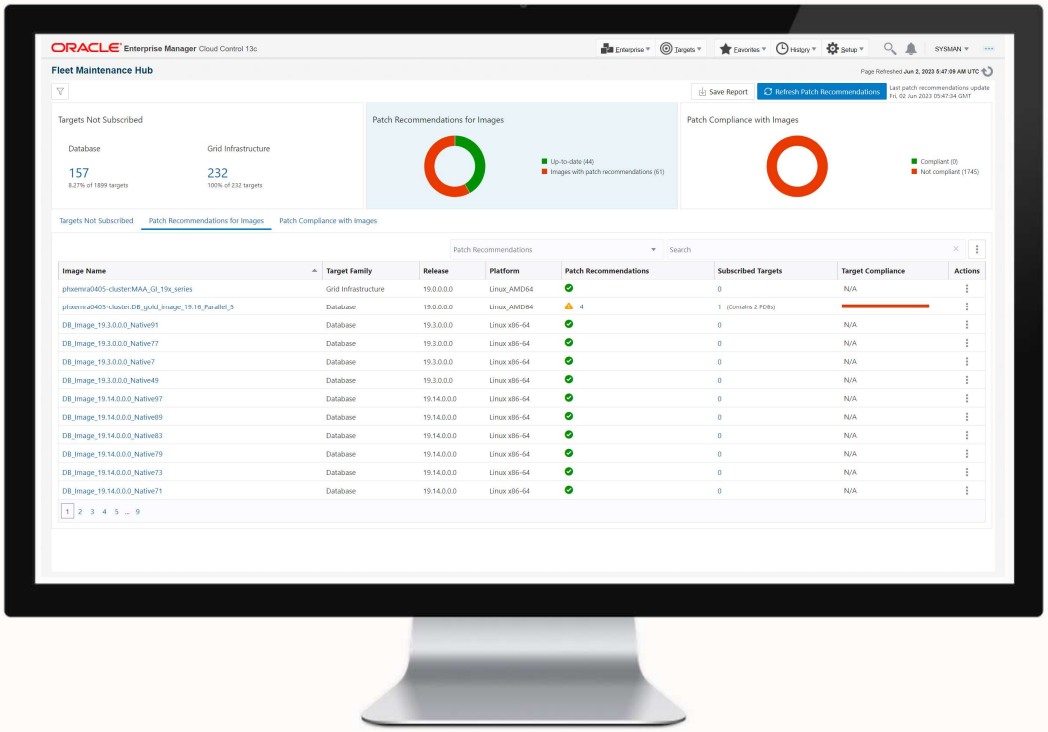
Patch Recommendations (from MOS) → Gold Image Refresh → Apply Patch + Target Patch Compliance

Seamless end-to-end fleet-level integrated story across hybrid environment

Copyright © 2023, Oracle and/or its affiliates

Fleet Maintenance Hub

Benefits



Fleet Maintenance Hub

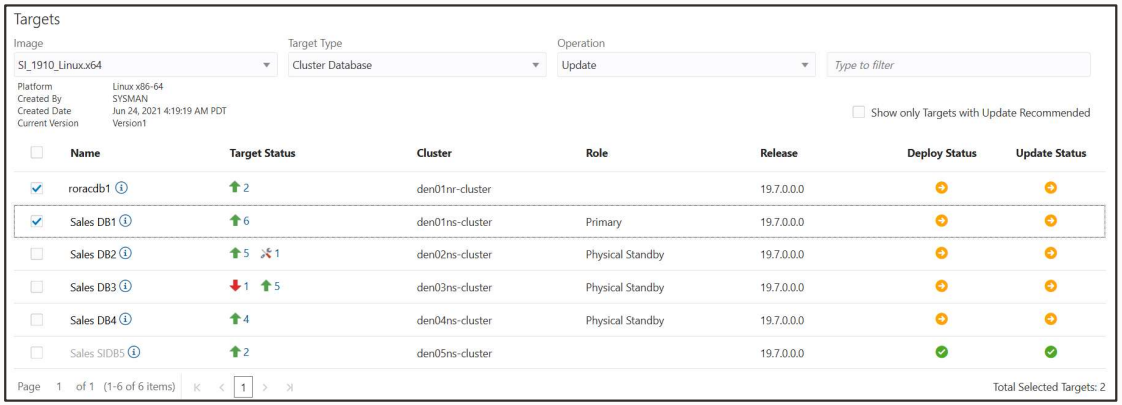
- Tangible OpEx savings
- Eliminate human error
- Proactively keep security posture at higher levels
- Reduce long maintenance downtime

Copyright © 2023, Oracle and/or its affiliates

Fleet Maintenance User Interface

Intuitive User Interface

- Simplifies patch and upgrade of entire database fleet, including grid infrastructure
- Perform Deploy, and Update operations
- Include custom pre and post scripts in the same maintenance window
- Intelligent interface assists tracking of operations at every step and provides actionable insights
- Built-in library of pre-checks to improve reliability and diagnosability

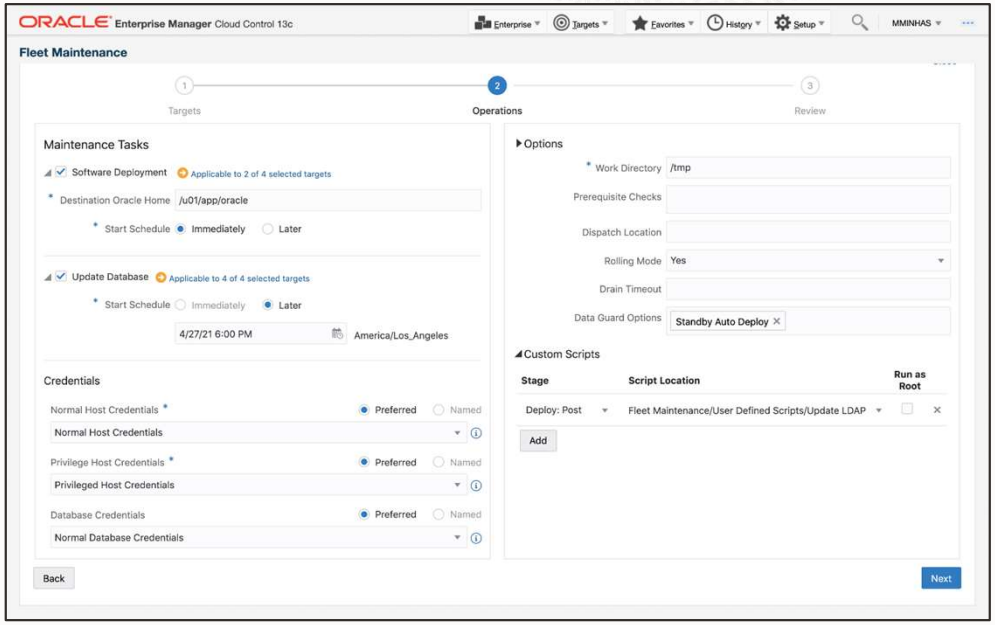


Copyright © 2023, Oracle and/or its affiliates

Fleet Maintenance User Interface

Patch and upgrade database fleet with ease

- Maintenance Tasks
  - Deploy software now or schedule for later
  - Update database now or schedule for later
  - Chain Update task to start right after Deploy is complete
- Options: Smart listing of target context parameters
  - List RAC parameters if RAC is selected
  - Drain Timeout enables duration to drain the resources in action
  - List Data Guard parameters if DG is selected



Copyright © 2023, Oracle and/or its affiliates

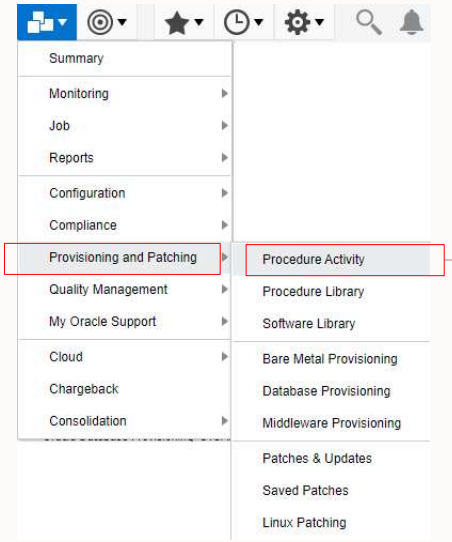
Track, Fix and Resume Operations

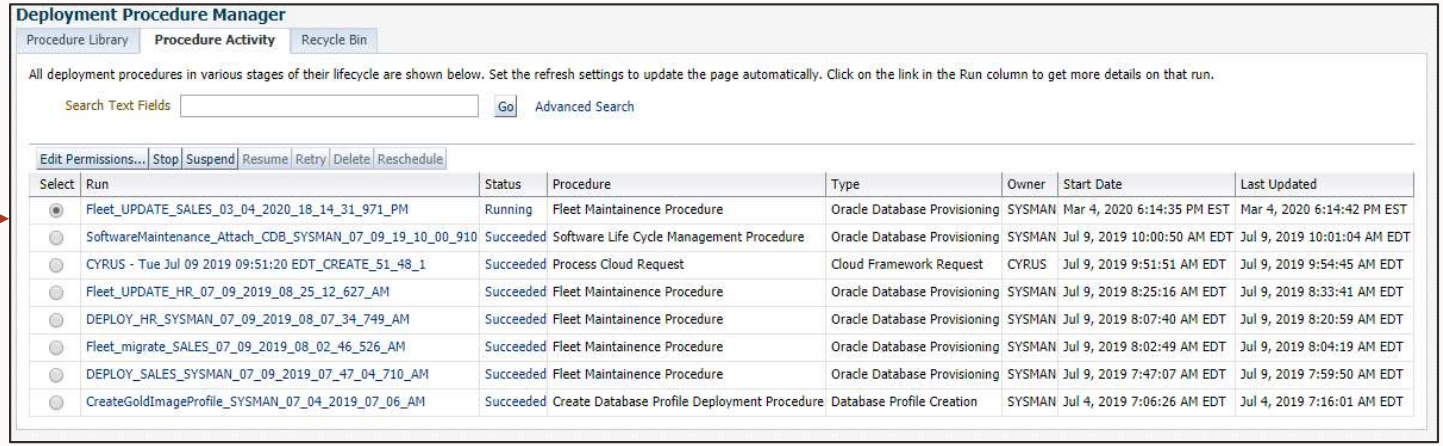
Reduce Mean-Time-To-Recover (MTTR) by providing actionable insights

Single pane of glass for monitoring and managing patching/upgrade operations

Quickly identify what things went wrong by looking at exact logs

Total control of the deployment procedures. Stop, Suspend, Resume, Retry, Delete and Reschedule





Select	Run	Status	Procedure	Type	Owner	Start Date	Last Updated
	Fleet_UPDATE_SALES_03_04_2020_18_14_31_971_PM	Running	Fleet Maintainence Procedure	Oracle Database Provisioning	SYSMAN	Mar 4, 2020 6:14:35 PM EST	Mar 4, 2020 6:14:42 PM EST
	SoftwareMaintenance_Attach_CDB_SYSMAN_07_09_19_10_00_910	Succeeded	Software Life Cycle Management Procedure	Oracle Database Provisioning	SYSMAN	Jul 9, 2019 10:00:50 AM EDT	Jul 9, 2019 10:01:04 AM EDT
	CYRUS - Tue Jul 09 2019 09:51:20 EDT_CREATE_51_48_1	Succeeded	Process Cloud Request	Cloud Framework Request	CYRUS	Jul 9, 2019 9:51:51 AM EDT	Jul 9, 2019 9:54:45 AM EDT
	Fleet_UPDATE_HR_07_09_2019_08_25_12_627_AM	Succeeded	Fleet Maintainence Procedure	Oracle Database Provisioning	SYSMAN	Jul 9, 2019 8:25:16 AM EDT	Jul 9, 2019 8:33:41 AM EDT
	DEPLOY_HR_SYSMAN_07_09_2019_08_07_34_749_AM	Succeeded	Fleet Maintainence Procedure	Oracle Database Provisioning	SYSMAN	Jul 9, 2019 8:07:40 AM EDT	Jul 9, 2019 8:20:59 AM EDT
	Fleet_migrate_SALES_07_09_2019_08_02_46_526_AM	Succeeded	Fleet Maintainence Procedure	Oracle Database Provisioning	SYSMAN	Jul 9, 2019 8:02:49 AM EDT	Jul 9, 2019 8:04:19 AM EDT
	DEPLOY_SALES_SYSMAN_07_09_2019_07_47_04_710_AM	Succeeded	Fleet Maintainence Procedure	Oracle Database Provisioning	SYSMAN	Jul 9, 2019 7:47:07 AM EDT	Jul 9, 2019 7:59:50 AM EDT
	CreateGoldImageProfile_SYSMAN_07_04_2019_07_06_AM	Succeeded	Create Database Profile Deployment Procedure	Database Profile Creation	SYSMAN	Jul 4, 2019 7:06:26 AM EDT	Jul 4, 2019 7:16:01 AM EDT

Copyright © 2023, Oracle and/or its affiliates

Procedure Activity: Troubleshoot Patching Issues Faster

Procedure Activity: Fleet_UPDATE_SALES_03_04_2020_18_14_31_971_PM

View Data Real Time: Manual Refresh

Elapsed Time: 12 minutes, 33 seconds

Procedure Actions

Debug
Stop
Suspend
Resume
Retry
Incident

Procedure Steps

View Show All Steps

All Steps
Failed Steps
Action Required Steps
Completed with Error Steps
Steps Not Skipped

Selec Name

Update or Switches Oracle Instances
Initialize Patch DB Deployment Pr
Create the paramaters file for scri
Execute custom pre script
Switch Database
Switch Oracle Database
Initialize Patch DB Deployment Procedure
Blackout listeners and affected databases
For all hosts : Steps for source Oracle home
Disable DG Configuration
Shutdown database instance from
Migrate DB Instances for Patching
For all hosts : Steps for destination Oracle h
Start DB Instances from Destinatio
Migrate tnsnames and listener entr
Rollback Patches
Apply PSU/Patches on the databas

Migrate DB Instances for Patching

Job Summary Download Actions

Ignore
Retry
Update and Retry

Type Directive Start Date Mar 4, 2020 6:15:47 PM EST

Completed Mar 4, 2020 Date 6:15:52 PM EST

Step: Inline transfer and execution of the Software Library Entities (Succeeded)

Start Date 2020.03.04 18:15:47

Completed Date 2020.03.04 18:15:47

Targets

Inline mode not allowed, will run in normal mode

Step: Create Staging Directory (Succeeded)

Start Date 2020.03.04 18:15:49

Completed Date 2020.03.04 18:15:49

Targets

Created /tmp/JOB_A01095B8B7166CC6E0531200000A7FAE

Step: Transfer setup environment and Software Library Entity properties file (Succeeded)

Start Date 2020.03.04 18:15:49

Deployment procedure actions

Deployment procedure step actions

Deployment procedure detailed information

Select a deployment procedure to view detailed information

Copyright © 2023, Oracle and/or its affiliates

Standardize Oracle Home configurations

Standardize and reduce configuration pollutions and security risks

Copyright © 2023, Oracle and/or its affiliates

Configuration Standardization

Consolidate, Standardize Oracle Homes

Scan the Fleet

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 + Subscribe

Create Gold Image

a. Identify reference Oracle Home target

b. Store Gold Image payload in SW library

c. Make a version of image "Current"

Subscribe Databases to a Gold Image

a. List subscriptions of an image

b. Validate subscriptions

Deploy + Switch

Deploy Image

a. Shadow Home is created

Switch Database

a. Migrate Listener

b. Update Database: SI, GI, RAC, Standby

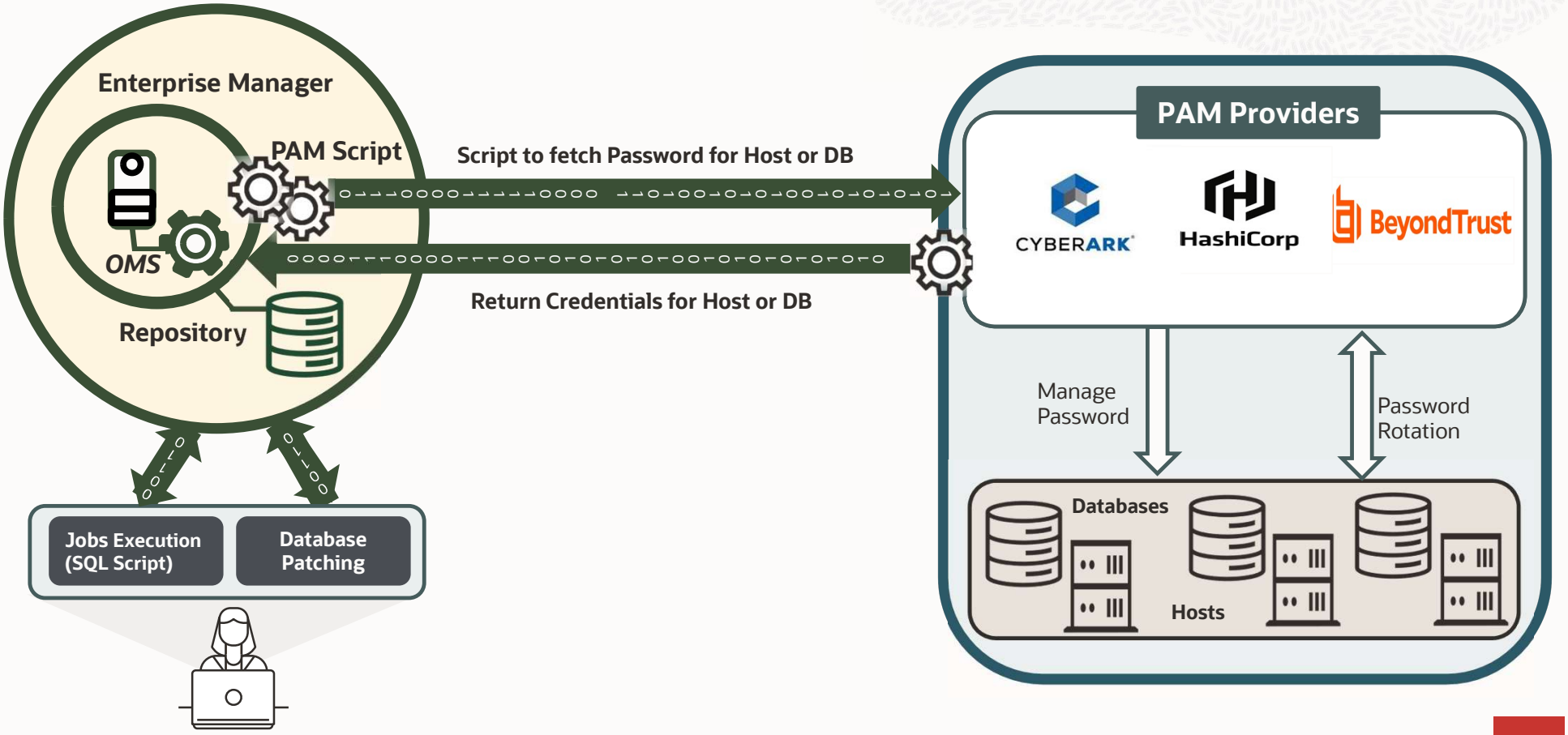
Copyright © 2023, Oracle and/or its affiliates

Database patching with secure authentication

Privileged access management

Copyright © 2023, Oracle and/or its affiliates

PAM Integration with Enterprise Manager – Solution Overview



Copyright © 2023, Oracle and/or its affiliates

PAM Integration Procedure with Enterprise Manager

1 Register PAM Script

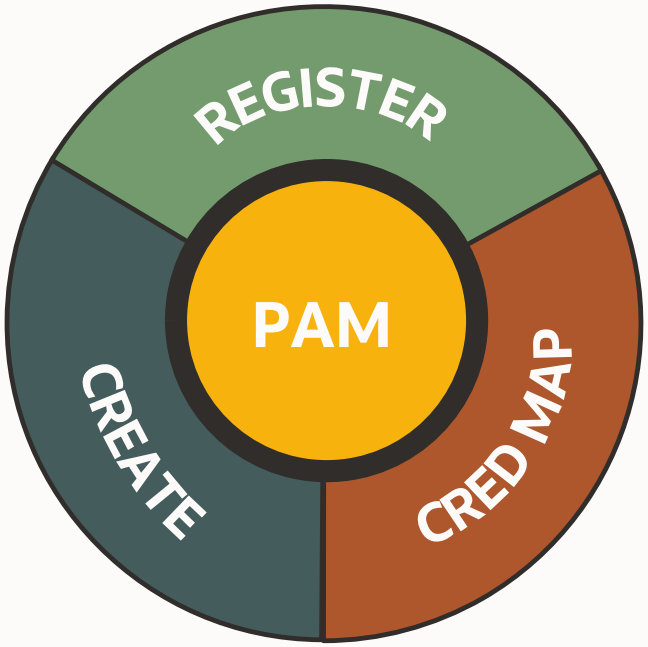
Register PAM provider script in EM

2 Credential Mapping

Map credential provider attributes to the attributes in credential type

3 Create or Modify Named Credentials

Create a new named credentials or modify an existing named credentials to access it from external store



Copyright © 2023, Oracle and/or its affiliates

PAM Integration with Enterprise Manager : Benefits

Extensible Model

- Credential framework to plug-in with any PAM provider
- Simplified integration with Enterprise Manager to retrieve password for PAM

Risk Reduction

- Protect potential operations caused by administrator errors or privilege abuse
- Reduce the risk of a potentially costly insider data breaches and address regulatory and compliance requirements

Auditing and Reporting

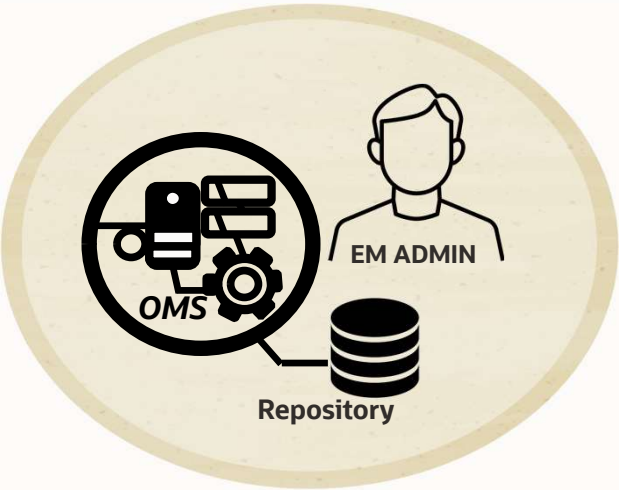
- Detailed auditing and reporting capabilities, making it easier to track privileged access activities, detect suspicious behavior

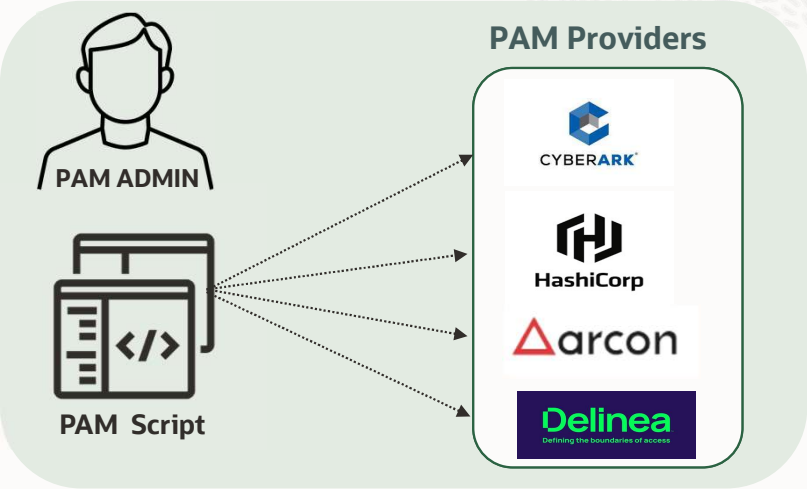
Increase Efficiency

- Controls the privileged account and streamline the access process
- PAM integration with EM help organizations become more efficient and improve their overall security posture.

Copyright © 2023, Oracle and/or its affiliates

PAM Integration with EM – Shared Responsibility Security Model





Named Credential Store

- New PAM named credential type that indicates external store
- Configure command to execute the script with parameters
- Any workflow execution like Jobs, Database patching etc. in EM executes the script to retrieve the password from PAM

PAM Script

- The script can be in Shell, Perl that consumes API or CLI calls of PAM providers like CyberArk, HashiCorp, Arcon etc. will be registered in EM
- Uses authorization tokens to get the password from PAM providers

Copyright © 2023, Oracle and/or its affiliates

Summary

Copyright © 2023, Oracle and/or its affiliates

Oracle Database Patch and Upgrade

	Process	Impact
Home Grown Scripts	Numerous manual steps	• Low success rate and error prone • One DB at a time • Longer maintenance windows • Script maintenance • Example: 2 weeks for 10 clusters
ORACLE ENTERPRISE MANAGER 13c Fleet Maintenance	• Patch Reference Environment • Upload as Gold Image • Subscribe DB to Image • Push image and Switch	• Prescriptive steps for concurrent updates • Shorter Maintenance Windows • Automate and patch at Scale • Example: < 4 hours for patching 10 clusters

Copyright © 2023, Oracle and/or its affiliates

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

Copyright © 2023, Oracle and/or its affiliates

ORACLE