



Deploy and Automate Multitenant Database Operations at Scale Onsite and in the Cloud



Sravanth Mouli
Product Manager - Enterprise Manager



Enterprise and Cloud Manageability strategy

Maximum customer choice

Provide ***maximum choice to customers*** through continued investment in both Enterprise Manager and cloud services

Enterprise Manager (EM)

- Tool for deep management of Oracle stack
- Hybrid and multicloud support
- Enhanced Ops automation
- Platform modernization for improved resilience and extensibility

Management Cloud Services

- New cloud services for APM, log analytics, database management, stack monitoring, and big data analytics
- Heterogeneous stack and language support
- Hybrid and multicloud support
- Telemetry integration with EM provides added value

Key Focus Areas



Hybrid Cloud Management

Fleet monitoring, management and data movement across entire IT estate – on-premises and in the cloud



Ops Automation

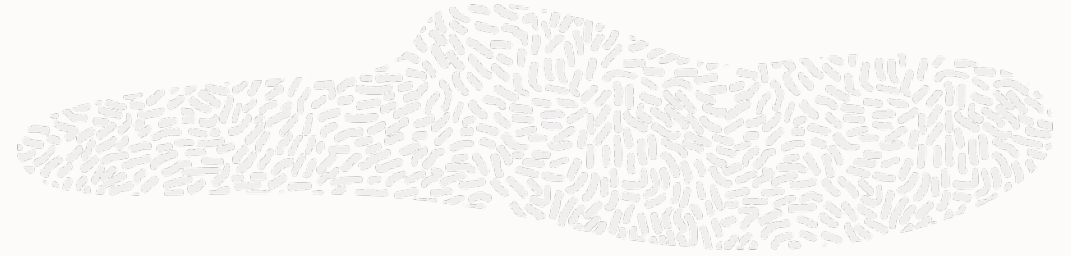
Enhanced automation and modernization of key management tasks



Extensibility & Resilience

Open standards-based extensions for interoperability with 3rd party ecosystems

Modernizing your data center helps in



Lower costs

Simplify and automate IT operations to lower CapEx and OpEx



Reduce risks

Patch to secure
Standardize configurations
Audit for compliance



Enable hybrid cloud

Hybrid PDBaaS for increased efficiency and faster innovation pace

Automate IT operations

- Consolidate to Multitenant
- Automation of database operations
- One tool for hybrid cloud platforms

Strengthen security posture

- Security-first, by default
- Modernize processes to standardize
- Continuous check for compliance

Activate DevOps model

- Increase SLAs and cater to customers faster
- Eliminate silos between IT and dev teams
- On-demand deployment of secure configuration

Multitenant management scenarios



Multitenant journey

Consolidate assets, and address complex, time consuming and stakeholder dependency for database deployment



Secure databases

Unpatched systems increase risk of breach

Misconfiguration and insecure changes by user with elevated privileges increases risks



Compliance at scale

Audit for industry and regulatory compliance

Keep databases, hosts, and infrastructure secure to protect sensitive data



Hybrid cloud management

Enable DevOps for on-demand deployment

Operational consistency across on-premises, private, and public cloud

Journey to Multitenant

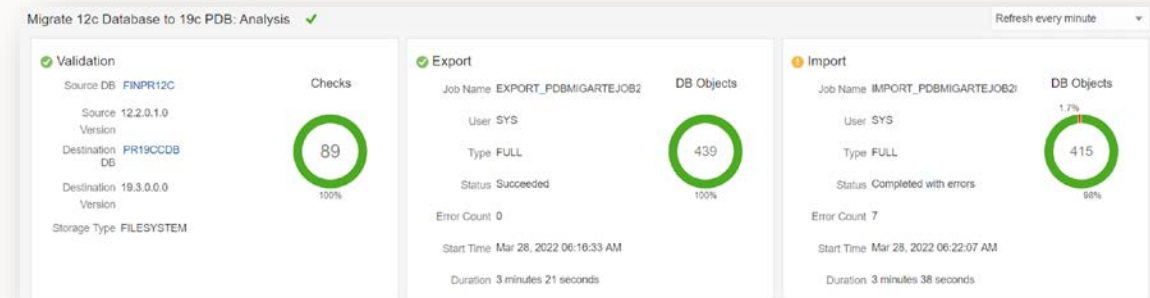
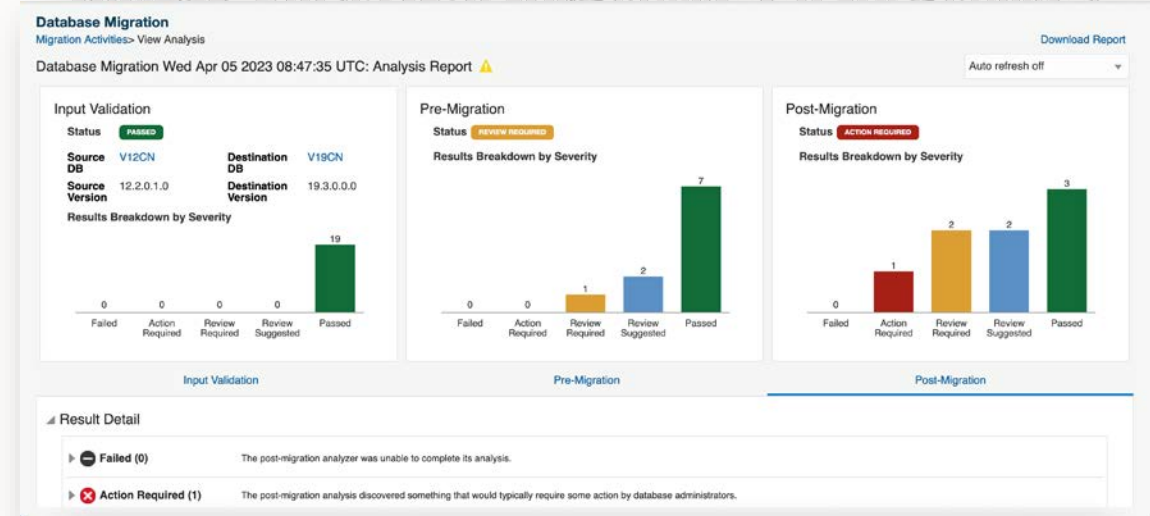
Migrate to multitenant databases on On-Premise, Exadata, and ExaCC

Consolidate with Migration Workbench

- On-premises and cloud migrations
 - Non-multitenant to multitenant
 - New Exadata infrastructure
 - Oracle Base Database service
 - Autonomous databases
- Integrated SPA for automated performance analysis and recommendation
- Pre and post migration analysis
- Automation and orchestration with DevOps tools

Benefits

- One tool for all migrations
- Migrate and upgrade in one flow
- Encrypted data migration



Pre Migration
Source database readiness

Migration
Derive best migration method for business

Post Migration
Business validation (data & performance)

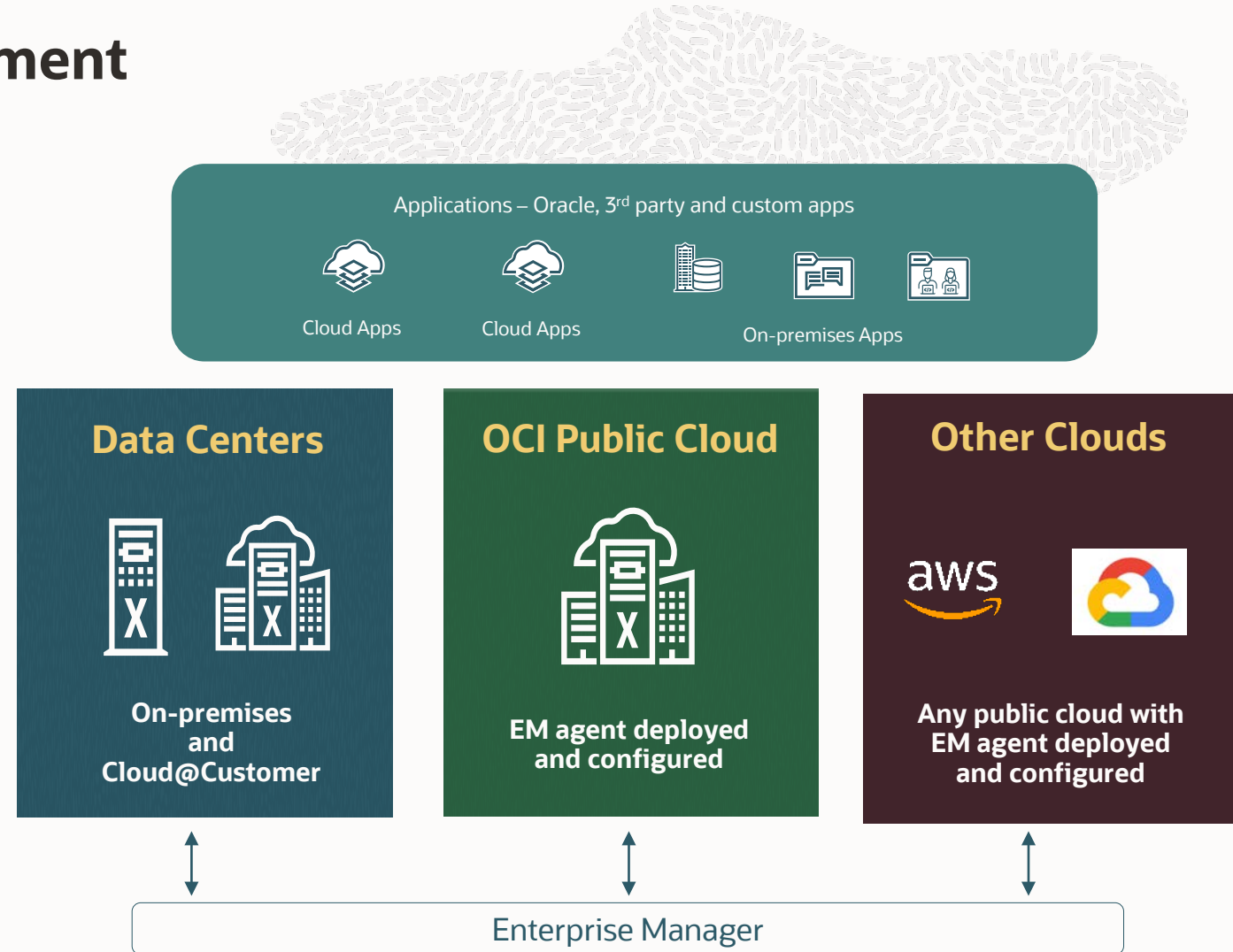
Patching across hybrid environment

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



Patch, Upgrade Oracle Multitenant Databases

Flexibility in patching multitenant assets

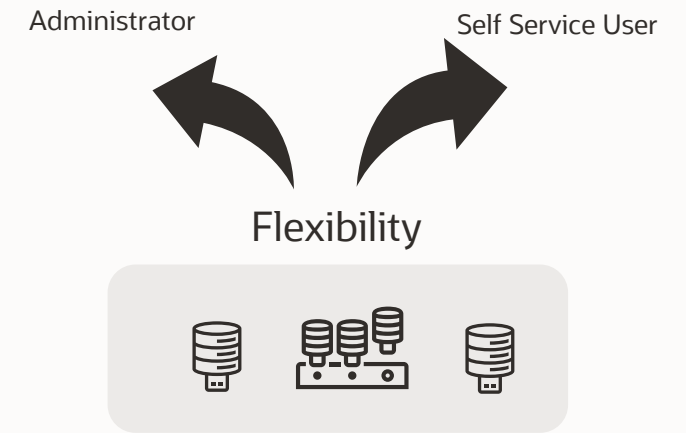
Administrator driven upgrade and patch options

- At CDB level, saves time it takes to patch
- Selective PDB at a time, provides ability to decide on downtime at PDB level

Self-service user driven upgrade and patch options

- Option to choose convenient window by application owner
- Relocate PDB to new CDB

REST APIs for integrating with 3rd party applications



Secure databases

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



Stakeholders in your organization to secure assets

Security hardening is a strategic priority

			
CFO Influencer	CISO Influencer	CIO/Architect Influencer	DBA 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

Modernize your security compliance and patching process

Unpatched systems

High risk of breaches

21% of breaches¹ are due to unpatched systems even though patches were available, but not applied

Compromised administrative privileges

74% of breaches leveraged weak credentials

Lack of security policies with principles of least privileges to users contributes to breaches and security incidents

Vulnerability risks management

Risk management and compliance

#2 in IT risk assessment priorities

Business interruption directly impacts revenue, reputation and market value. Customers with bad experience are unlikely to return

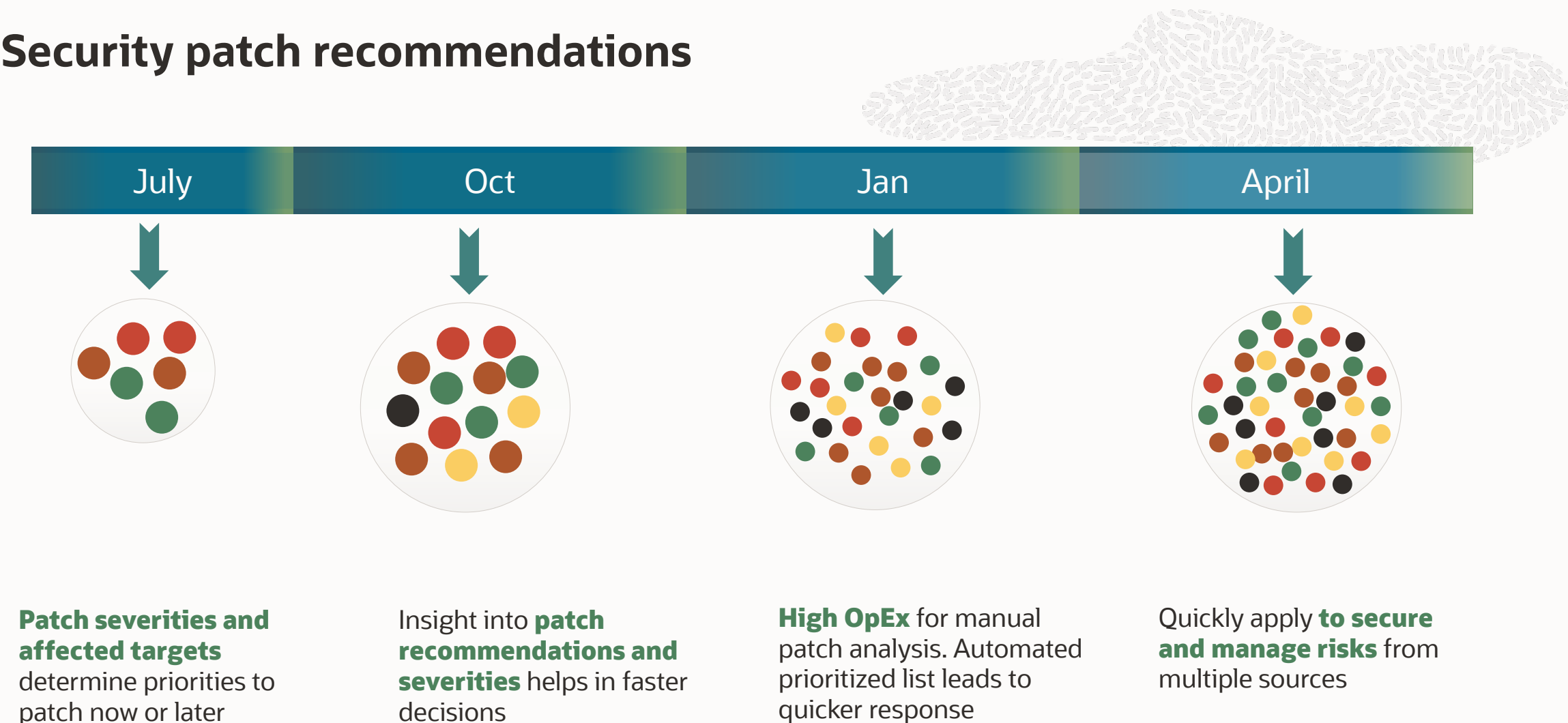
Misconfigurations and sprawl

45% of breaches were due to misconfigurations¹

Preferred way to exploit are misconfigurations, insecure configuration changes and sprawl. Home grown scripts increases vulnerability and maintenance cost²



Security patch recommendations



Fleet Maintenance Hub

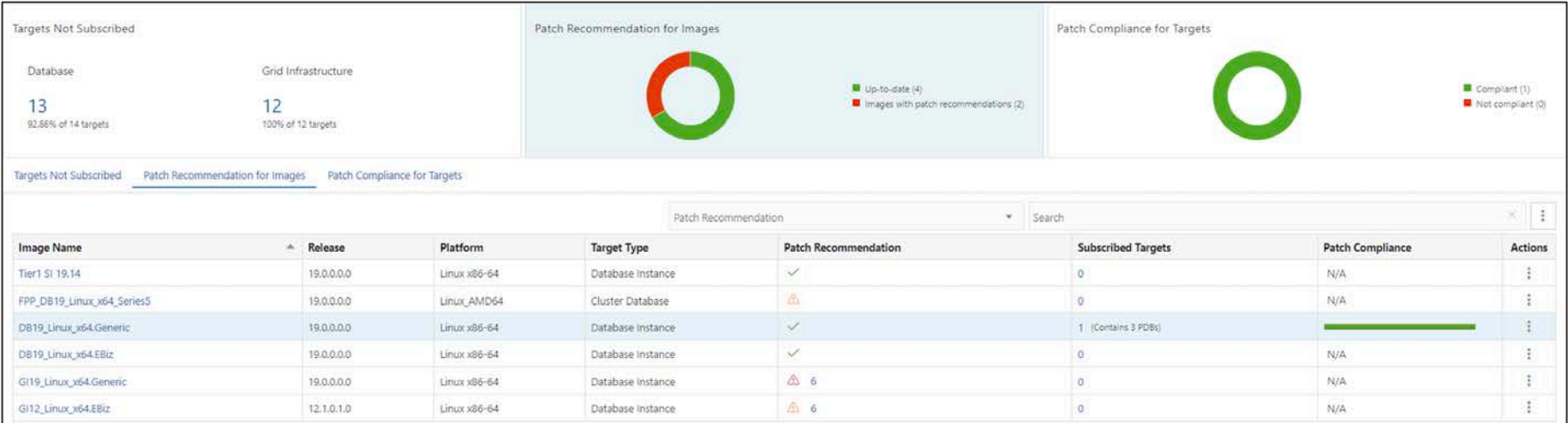
One stop place for operational control, and enhanced security

Security patch recommendations

Automated insight into affected gold images

Database compliance with patch policies

Risk assessment of targets to subscribe

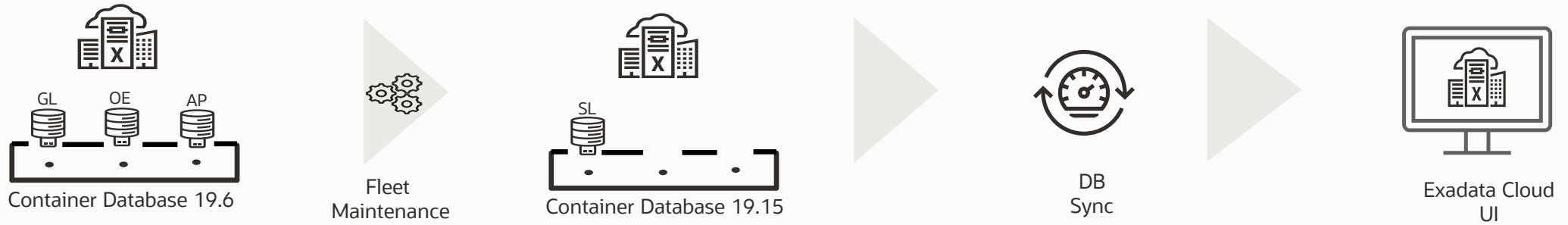


Seamless end-to-end fleet-level integrated story across hybrid environment



Patch and Upgrade PDB on ExaCC

Fleet Maintenance support PDB Patching and Upgrade on ExaCC



Prerequisites

- Create a new CDB of target patch level using cloud console (or)
Use an existing CDB at the target patch level
- Create a gold image and subscribe the PDB targets
- Available only for Oracle Database version 19.6 and later
- Enterprise Manager 13.5 RU10 or later is required.

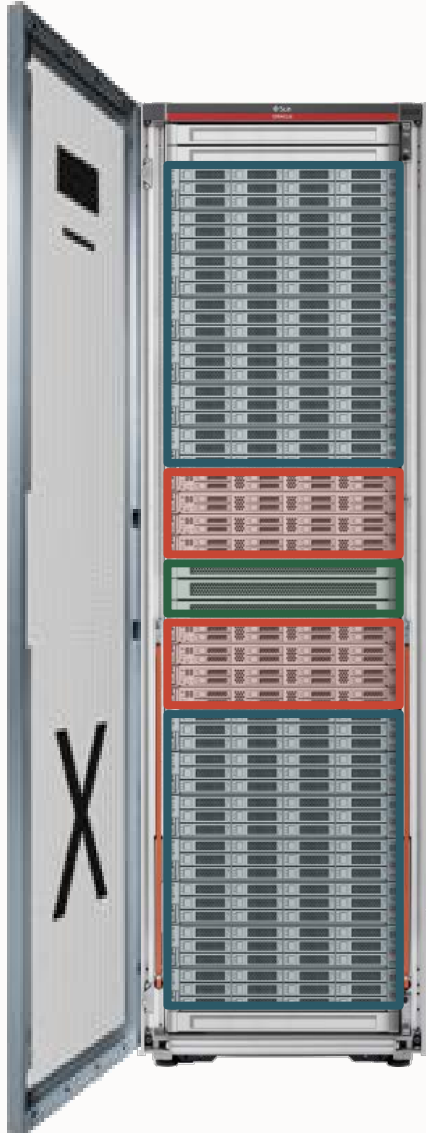
DB Sync¹ job runs every 10 minutes to reflect changes in Exadata Cloud UI

Supports patching using RESTAPI, EMCLI and UI

Out of place patching only

Preview

Exadata Software Patching



Exadata software patching with REST APIs and EMCLI

- Physical/Virtual Compute nodes
- Storage Cells
- KVM and Xen DomU guests
- InfiniBand network switches

Features

- Patch multiple components across Exadata Database Machine
- Rollback to last known good state in case of failure
- Rollback to previous version, if required
- Schedule deploy and update operations to align with preferred maintenance window

AutoUpgrade Integration with Enterprise Manager

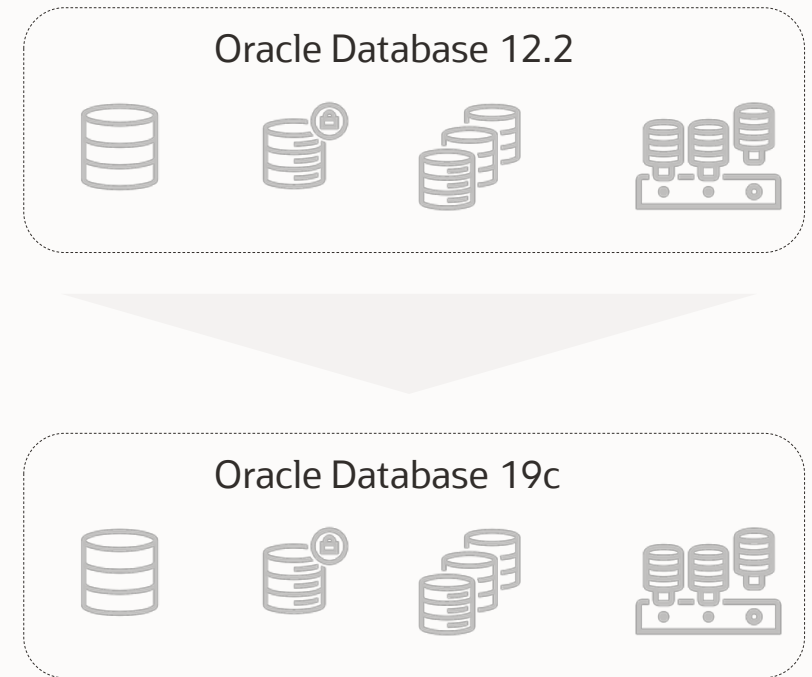
Modernized backend for upgrade operations

Integration will support fleet level upgrades

- Non-multitenant to non-multitenant
- Multitenant to multitenant
- Non-rolling logical standby
- TDE and non-TDE configurations

Benefits

- Upgrade databases at fleet level with intuitive workflow
- Hub to assess vulnerabilities of upgraded databases
- Security patch recommendations and remediation
- Activity tracking, triage, resolve and resume upgrades



Secure credential management ^{New} Privilege Access Management integration (PAM) with Enterprise Manager

Seamless integration

PAM integration bolsters security by enabling secure, controlled access to privileged accounts

Protect from security breaches

Protects against privilege abuse by centralizing and controlling privileged account access, periodic password rotations

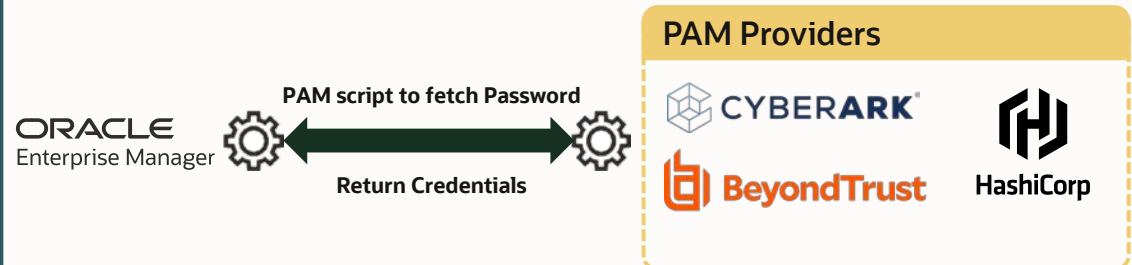
Elevated security posture

EM-PAM integration aligns security policies, ensuring privileged credentials are handled securely and transparently within EM's framework

Streamlined credential management

PAM-integrated named credentials streamline the management of password rotations, reducing operational overhead and potential points of exploitation

Privilege Access Management (PAM) Integration



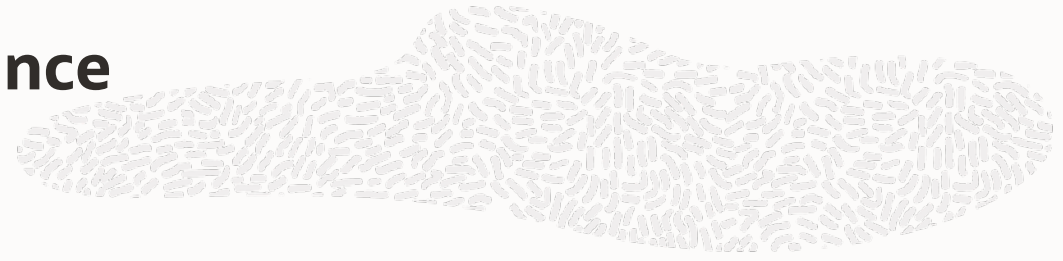
Compliance at scale

Best practices to drive and enforce security, and be compliant

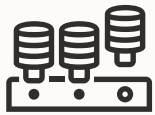


Automate hardening of Security Compliance

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

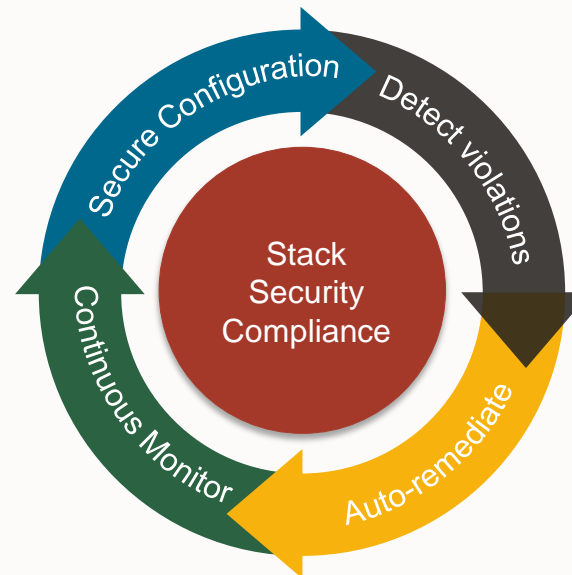
Hosts

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



Exadata Systems

Exadata best practices and security recommendations

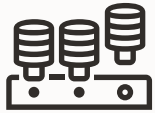


- Stack security posture by continuous monitoring
- Security policy management across heterogeneous targets and hybrid environments
- Leverage industry, and regulatory standards
- Audit security reports for compliance
- Reduce DBA time by auto-remediation of security violations

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

Host security compliance standards

Assess, detect, and remediate



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)

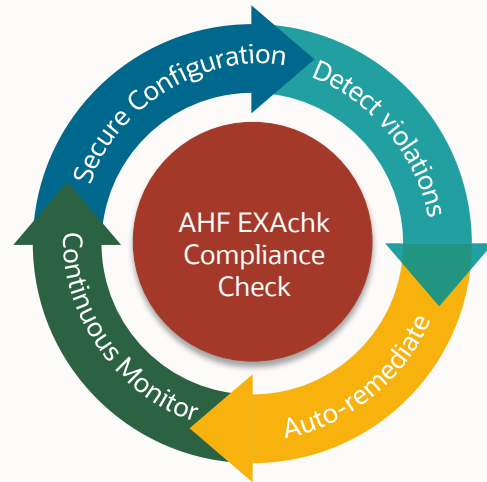


Exadata security compliance standards

Assess, detect, and remediate



- Out-of-box AHF EXAchk security compliance standards for Exadata and ExaCC Engineered Systems
- Maintains compliance with component specific best practices
- Scans for significant problems across DB servers, Software, Storage cells, InfiniBand switches, and network in the system
- Automated risk identification and proactive notification
- View compliance results at Exadata system or component level



Hybrid cloud enablement

Operational consistency across on-premises, private and public cloud



Hybrid Database-as-a-Service

Enable DevOps in hybrid environment

Private database cloud

- Build, deploy, and operate on-premises, & cloud (ExaCC, ExaCS, VM, BM, OCI)
- Maximize visibility, reporting to ensure adherence to IT policies

Self-service governance

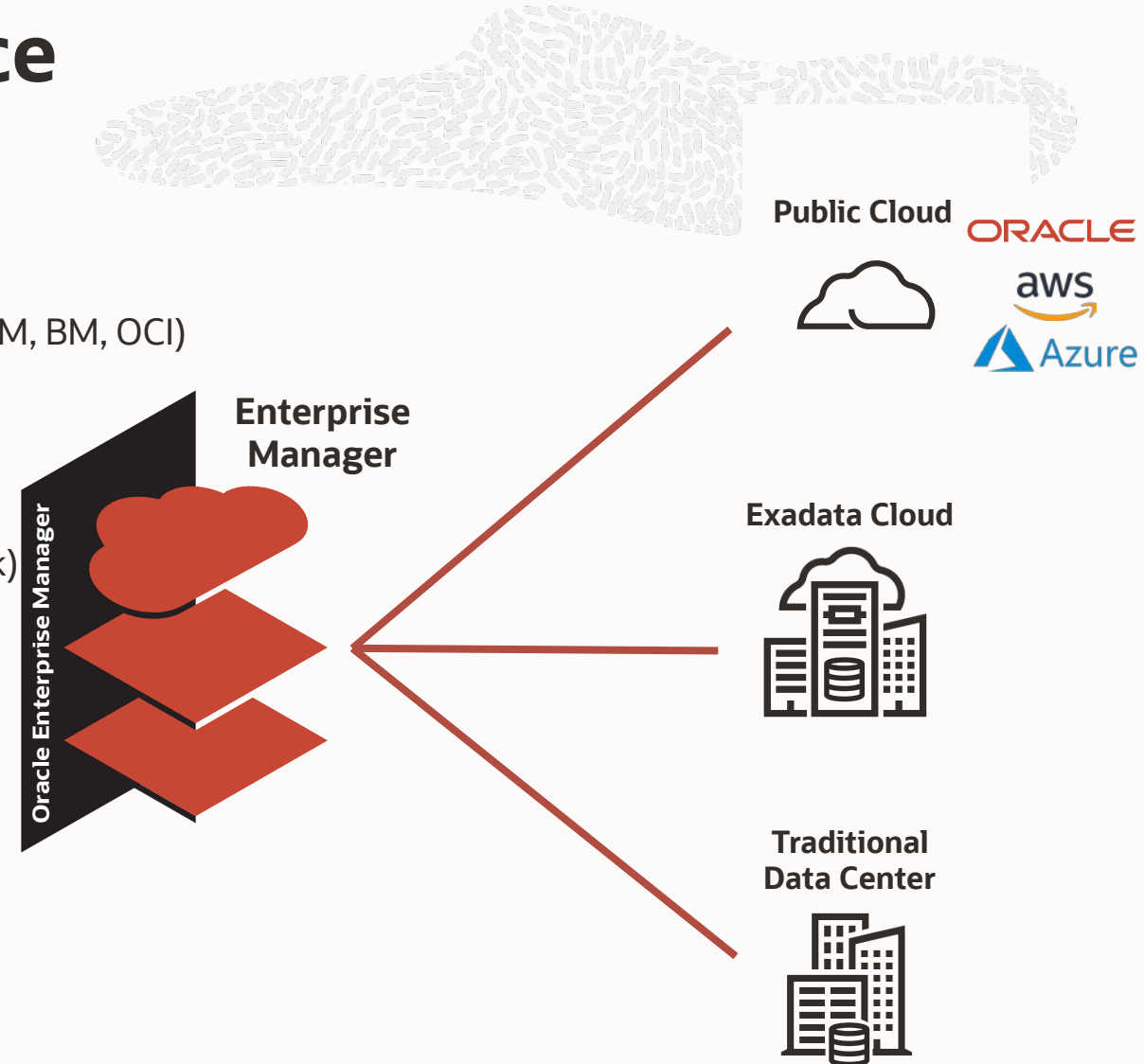
- Access controls, and cloud resource utilization (Quotas/Showback)
- Intelligent placement policies for optimal utilization of resources

Rapid provisioning

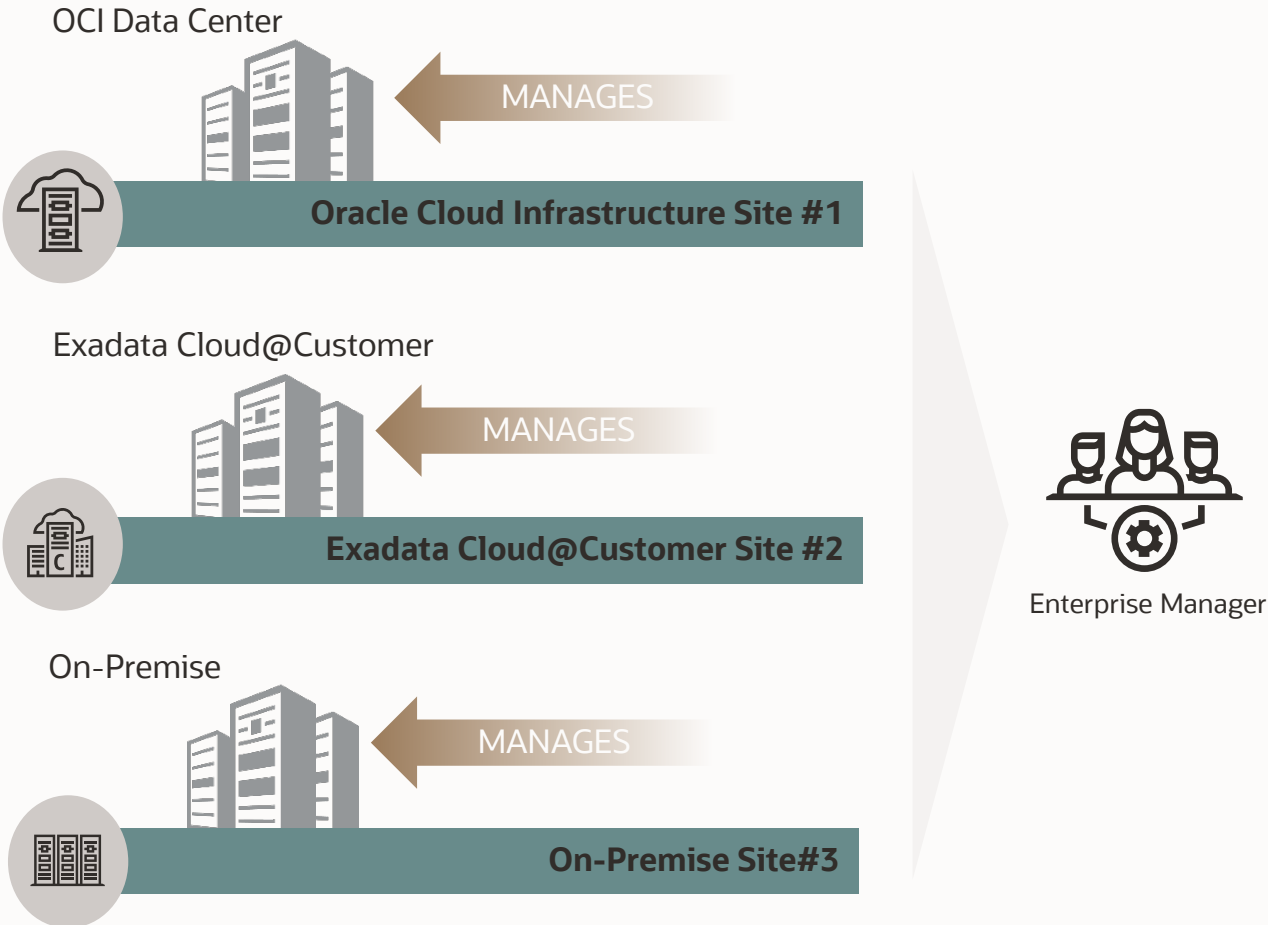
- Agility in application development
- Reduce time in deploying databases via self-service interface

Storage agnostic, space-efficient cloning

- Instant cloning of large production databases in minutes
- Reduced storage footprint by leveraging native copy-on-write technology



Hybrid Cloud Self Service for DevOps



Simplify database management and accelerate deployment across on-premises and cloud

- Centralized governance across on-premises and cloud
- Quick deploy, same set of inputs regardless of platform
- Automate with DevOps tools and Orchestration engines

Operational consistency across hybrid environments

- One-stop visibility across on-premises and cloud assets
- Lifecycle management of database at scale, with less effort
- Enforce effective standardization, and reduce management overhead

Hybrid database as a Service

DevOps
Users



Self Service Application
Administrators



1

Consolidated

2

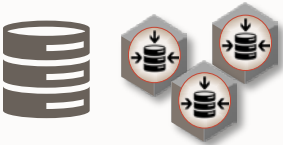
Elastic

3

Efficient

4

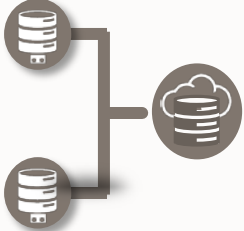
Accessible



Dedicated
Database



Thin
Clones



Pluggable
Database



On-Prem



OCI DBCS



ExaCC



Engineered Systems



ANSIBLE



vmware®

servicenow.



Standardized templates in service catalog

DevOps
Users



Self Service Application
Administrators



Operator

Access to Service Catalog and Features for users

Administrator

PLATINUM

19c PDB on OCI
VM

GOLD

19c PDB on
Exadata with
Standby

SILVER

Create 19c CDB

BRONZE

19c Pluggable
on ExaCC

Service Catalog

Service Settings

PDB Shapes

Quota Management

Placement Algorithms

Service definition

- Tiers: Platinum, Gold, Silver or Bronze
- Establish footprint for tiers: S/M/L

Service catalog

- Collection of standardized services
- On demand, self-service deployment

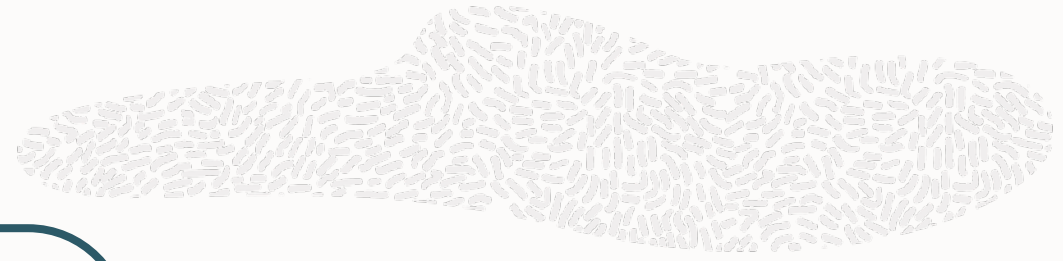
Benefits

- Enforce effective standardization
- Repeatable deployment process
- Identify service costs
- Reduce management overhead

Summary

Secure databases in hybrid architecture

Security hardening and DevOps enablement



Database lifecycle management

Detect and remediate vulnerabilities

Manage deviations and audit for compliance

Fleet level provision or clone of databases



Hybrid private cloud management

On-demand secure and standardized templates

Consolidate hybrid resources

Chargeback and metering



Reduce risk

Lower cost

Productivity

Automate end-to-end repetitive operations

Learn More

1. [Oracle.com/manageability](https://oracle.com/manageability) or oracle.com/enterprise-manager/#rc30p2
2. Video Series: youtube.com/OracleEnterpriseMgr
3. Blog: blogs.oracle.com/observability
4. Documentation: [EM 13.5 DB Lifecycle Management](#)
5. [Try it now](#)



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

