

ORACLE

EM Security Essentials

Recent Enhancements

Anand Prabhu

Principal Member of Technical Staff
Enterprise Manager



Safe harbor statement

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, timing, and pricing of any features or functionality described for Oracle's products may change and remains at the sole discretion of Oracle Corporation.

Agenda

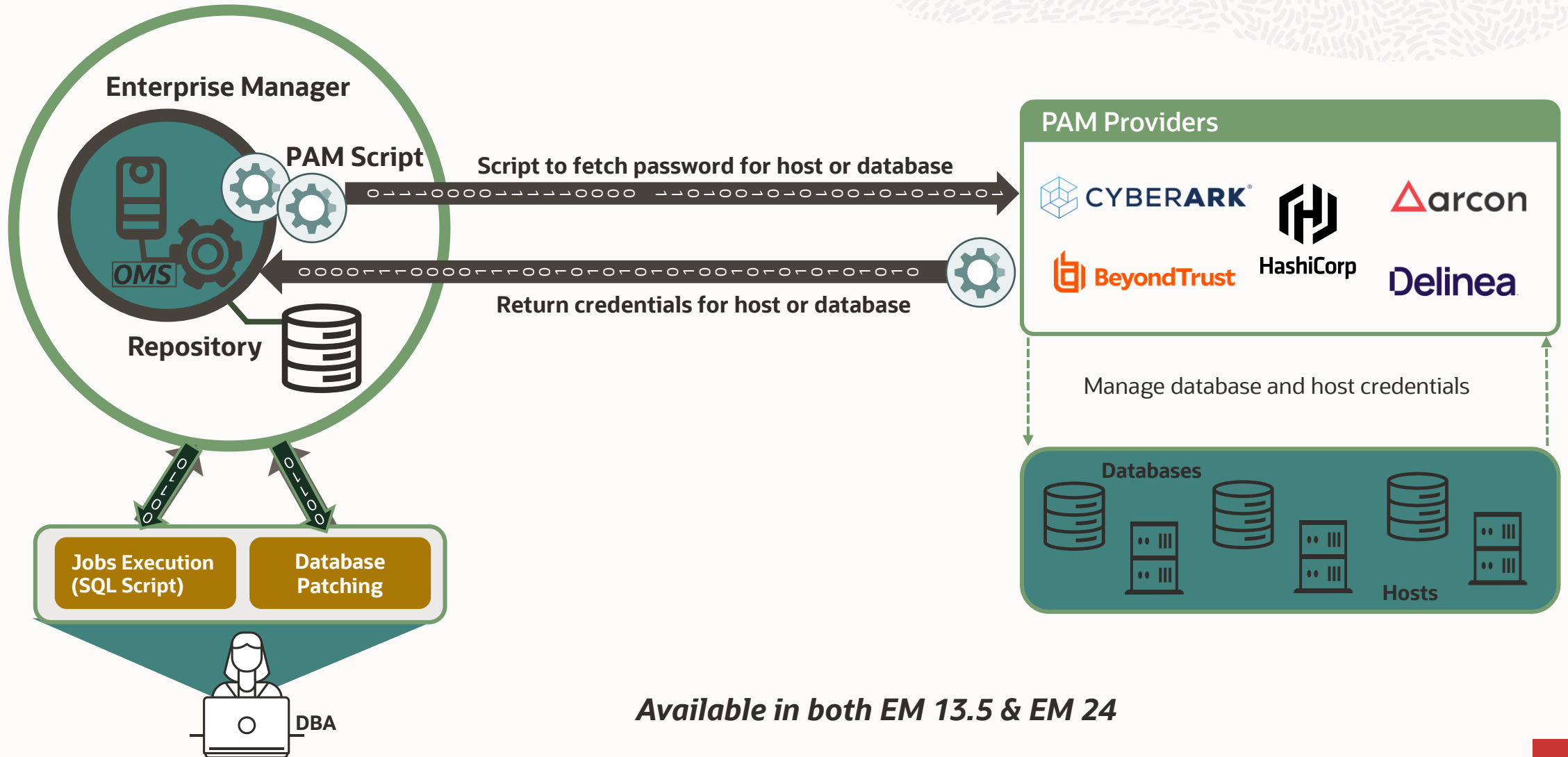


- Privilege Access Management (PAM) Integration
- Credentials Management REST API Operations
- Holistic Patching – Streamlining Security Updates
- Increased Kerberos & RADIUS Credential Support
- Monitor Oracle Key Vault
- Data Masking and Subsetting
- Enterprise Manager 24: Essential Security Insights

Privilege Access Management (PAM) integration

Securing the future: credential management reimaged with EM

Privilege Access Management (PAM) integration – solution overview



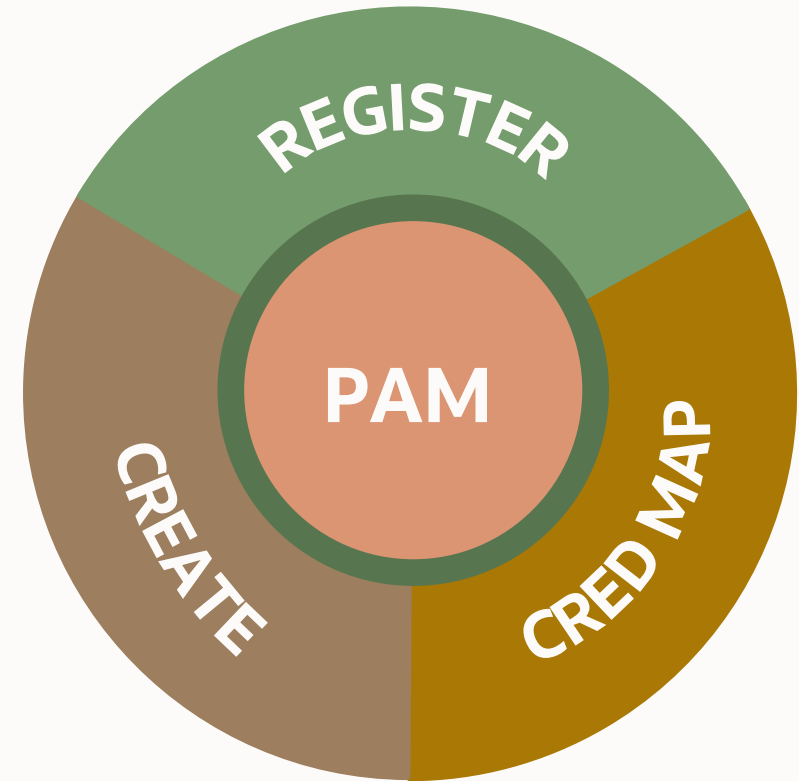
Available in both EM 13.5 & EM 24



Simplified integration of PAM with EM



- 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



Console-driven PAM named credential management | New

- Console shows PAM option only when PAM script and credential mapping are registered with credential framework
- PAM named credential creation support is available from RU21 onwards
- New credential property is added to retrieve the credentials from repository or PAM store
- Registered credential provider name is displayed for credential creation
- Credential mapping attributes are displayed for credential type
- Credential key value is required to retrieve the credentials for host or database

ORACLE Enterprise Manager Cloud Control 13c Enterprise

Security

Named Credentials > Create Credential

General Properties

- * Credential name: PAM store host
- Credential description: Cred managed in CyberArk
- * Authenticating Target Type: Host
- * Credential type: Host Credentials
- Scope: Target Global
- * Target type: Host
- * Target Name: emcc.marketplace.com

Credential Properties

- Credential Store: Repository PAM
- * Credential Provider: CyberArk
- * Credential Mapping: CyberArktoEMHostCreds
- * Credential Key: host33
- * UserName: oracle

PAM – modify and create ad-hoc named credential | New

On-demand named credential creation

- New named credential creation from database login page using PAM store
- PAM credential attributes are then saved as named credential for database instance

The screenshot shows the Oracle Enterprise Manager Cloud Control 13c interface. The breadcrumb trail is 'hr.subnet.vcn.oraclevcn.com / ↑ HRPDB'. The navigation menu includes 'Oracle Database', 'Performance', 'Availability', 'Security', 'Schema', and 'Administration'. The 'Database Login' section is active, with 'Database' set to 'HRPDB'. The 'Credential' type is set to 'New' (radio button selected), and the 'Credential Store' is set to 'PAM' (radio button selected). The 'Credential Provider' is 'CyberArk', 'Credential Mapping' is 'CyberArktoEMDBCredits', 'Credential Key' is 'sys54', and 'Username' is 'sys'. The 'Role' is 'SYSDBA'. The 'Save As' checkbox is checked, and the name 'SYS_PAM' is entered in the text field. There are 'Login' and 'Cancel' buttons at the bottom.

Modify named credential

- Existing named credential can be modified from repository to PAM store
- PAM credential attributes needs to be modified to update the credential properties

The screenshot shows the Oracle Enterprise Manager Cloud Control 13c Security page. The breadcrumb trail is 'Named Credentials > Edit Credential Properties'. The 'Credential name' is 'SALES_SYS'. The 'Authenticating Target Type' is 'Database Instance'. The 'Credential type' is 'Database Credentials'. The 'Scope' is 'Target' (radio button selected). The 'Target type' is 'Database Instance'. The 'Target Name' is 'sales.subnet.vcn.oraclevcn'. The 'Credential Properties' section is expanded, showing the 'Credential Store' set to 'PAM' (radio button selected). The 'Credential Provider' is 'CyberArk', 'Credential Mapping' is 'CyberArktoEMDBCredits', 'Credential Key' is 'sys53', and 'Username' is 'sys'. The 'Role' is 'SYSDBA'.



User, Roles, and Credentials management REST API operations

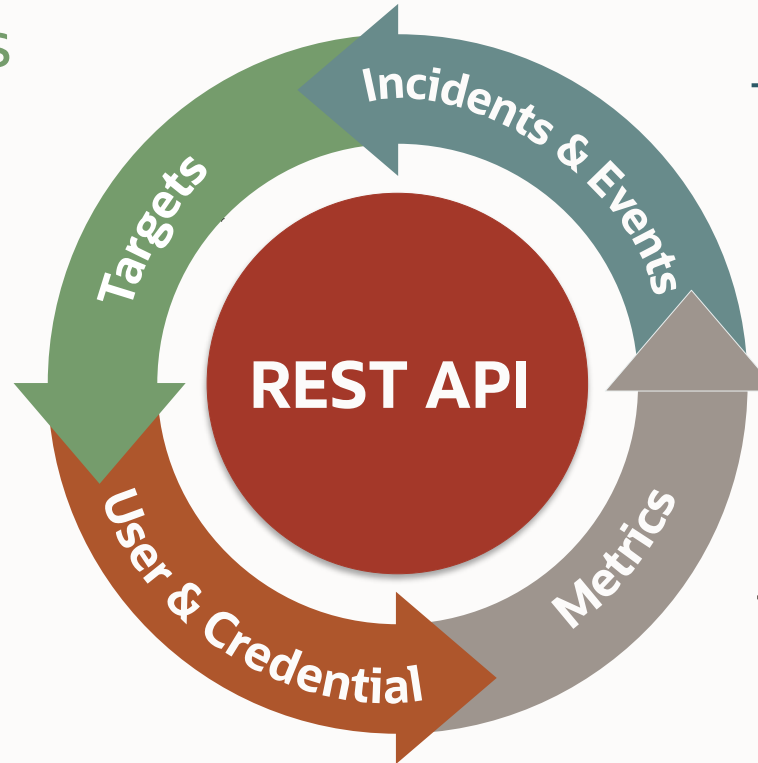
Enterprise Manager – platform API features

Targets & Target Properties

Create new target, modify existing target, list targets, get target properties, delete target, create new global target properties, list global target properties

User & Credential

Create users, list users with roles and privileges, delete user, create/test/update named credential, list named credential



Incidents & Events

Search for incidents, get events details, clear an incident, list incident details, suppress/unsuppress incidents

Metrics

Get metric groups for the target, metric group details for a target, latest values for the metrics in the group

Available in both EM 13.5 & EM 24

Enterprise Manager automation

Credentials Management

GET

- Get named credential with given id
- List named credentials

POST

- Create a new named credential
- Test the named credential against the target
- Test the named credential provided in the list

New

- *Create a monitoring credential*
- *Set a named cred as preferred credential*
- *Clear a monitoring cred*
- *Clear a preferred credential*
- *Search for monitoring credential*
- *Search for preferred credential*
- *Test the monitoring credential against the target*
- *Test the preferred credential against the target*

DELETE

Delete named credentials with given id

PUT

Update an existing named credentials

REST API operation – set monitor credentials

set monitor credentials for a database instance

POST https://EM_HOST:EM_CONSOLE_HTTPS_PORT/em/api/namedCredentials/actions/setMonitoringCredential

Payload

```
{
  "setName": "DBCredsMonitoring",
  "targetTypeName": "oracle_database",
  "targetName": "finance.subnet.vcn.oraclevcn.com",
  "credentialType": "DBCreds",
  "attributes": {
    "DBPassword": "welcome1",
    "DBUserName": "dbsnmp",
    "DBRole": "Normal"
  }
}
```

Response

The screenshot shows a REST client interface with the following details:

- Method:** POST
- URL:** https://129.../em/api/namedCredentials/actions/setMonitoringCredential
- Body:** raw
- Status:** 200 OK (528 ms, 1.03 KB)
- Response Body (JSON):**

```
1 {
2   "targetTypeName": "oracle_database",
3   "targetName": "finance.subnet.vcn.oraclevcn.com",
4   "targetGuid": "04B44ED4D463E2A6D88EE939C984CBC5",
5   "setName": "DBCredsMonitoring",
6   "credentialType": "DBCreds",
7   "attributes": {
8     "DBPassword": "*****",
9     "DBRole": "Normal",
10    "DBUserName": "dbsnmp"
11  },
12   "targetUserName": "dbsnmp",
13   "links": {
14     "credentialSet": {
15       "href": "/em/api/targetTypes/oracle_database/credentialSets/DBCredsMonitoring"
16     },
17     "target": {
18       "href": "/em/api/targets/04B44ED4D463E2A6D88EE939C984CBC5"
19     }
20   }
21 }
```

REST API operation – set preferred credentials

set named credential “ORACLE_HOST” as preferred credentials of the host

POST https://EM_HOST:EM_CONSOLE_HTTPS_PORT/em/api/namedCredentials/actions/setPreferredCredential

Payload

```
{
  "targetName": "emcc.marketplace.com",
  "targetTypeName": "host",
  "setName": "HostCredsNormal",
  "isDefault": "false",
  "isGlobal": "false",
  "credName": "ORACLE_HOST",
  "credOwner": "sysman"
}
```

Response

The screenshot shows a REST client interface for a POST request to `https://129.../em/api/namedCredentials/actions/setPreferredCredential`. The response is a 201 Created status with a 1.06 KB body. The response body is displayed in JSON format and is highlighted with a red box. The response JSON is as follows:

```
1 {
2   "targetTypeName": "host",
3   "targetName": "emcc.marketplace.com",
4   "targetGuid": "AEEA9C06474AB3D80540FFFB94C98CB",
5   "setName": "HostCredsNormal",
6   "isGlobal": false,
7   "isDefault": false,
8   "isCredSetConfigured": true,
9   "credGuid": "950B5DEFA6A3745FE0530300000A0242",
10  "links": {
11    "credentialSet": {
12      "href": "/em/api/targetTypes/host/credentialSets/HostCredsNormal"
13    },
14    "namedCredential": {
15      "href": "/em/api/namedCredentials/950B5DEFA6A3745FE0530300000A0242"
16    },
17    "target": {
18      "href": "/em/api/targets/AEEA9C06474AB3D80540FFFB94C98CB"
19    }
20  }
21 }
```



Holistic Patching: streamlining security updates

Holistic Patching – streamlining security updates | New

Stack Patch Bundle (SPB)

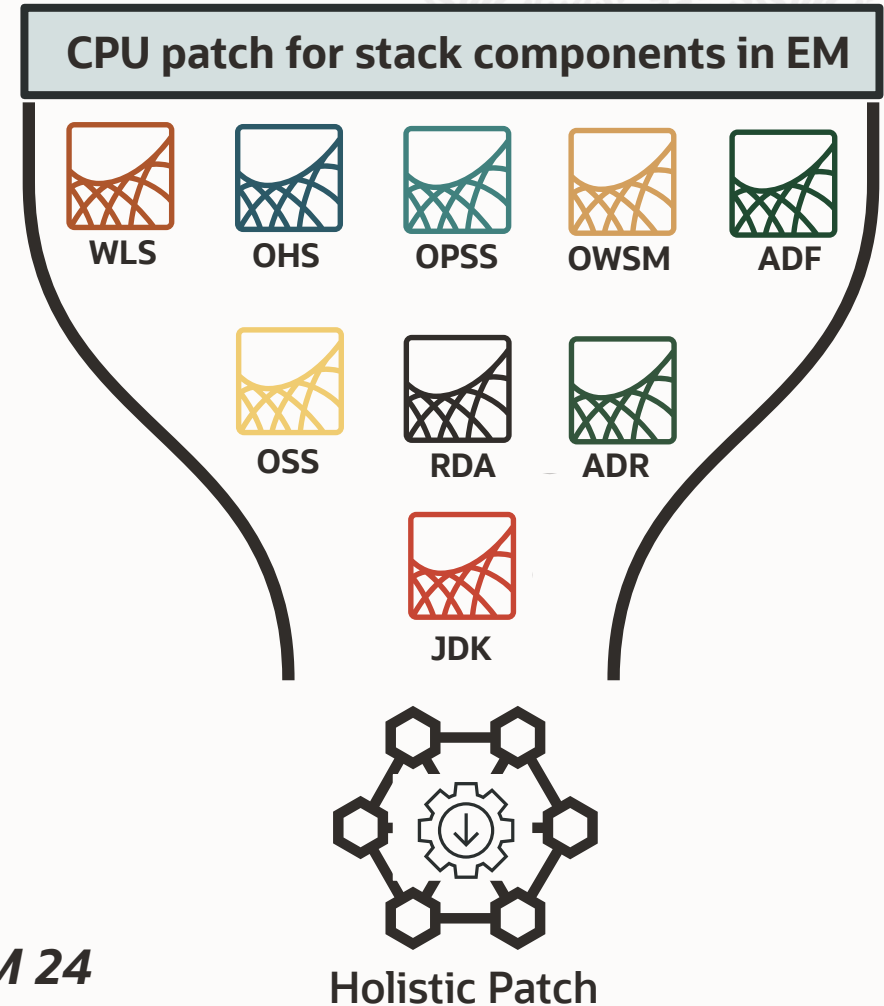
- Big bundle stack patch that includes the components such as OHS, OPSS, WLS, JDK, etc. in EM
- SPB is orchestrated through omspatcher utility

Ease of applying CPU patches

- Download single holistic patch from MOS for quarterly CPU cycle
- Apply SPB through omspatcher to reduce security risks
- JDK inside the OMS home will be updated to be in compliant with the latest certified version

Reduce maintenance window

- Single downtime window to apply holistic patch and release updates
- System and environment prechecks are performed once hence reducing the overall apply time



Available in both EM 13.5 & EM 24

Holistic Patching – new parameters to OMSPatcher command

Analyze Holistic Patch

```
omspatcher apply <patch location> -spb_patch -analyze
```

Apply Holistic Patch

```
omspatcher apply <patch location> -spb_patch
```

Apply Holistic Patch – Silent mode

```
omspatcher apply <patch location> -spb_patch -silent
```

Apply Holistic Patch + JDK Update

```
omspatcher apply <patch location> -spb_patch -jdk_update  
<jdk location>
```

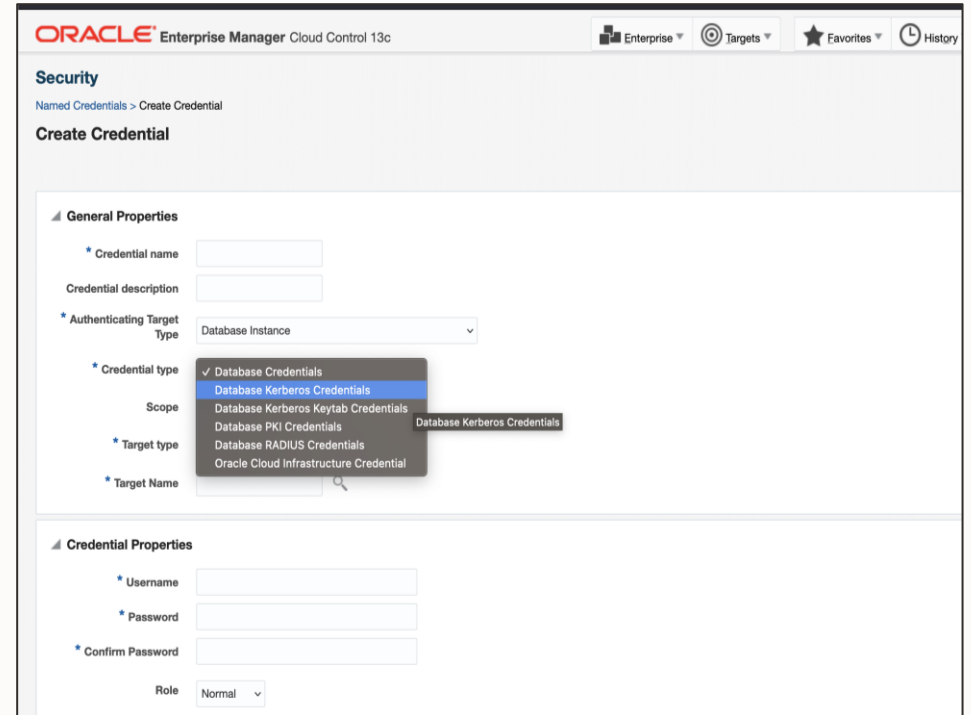
Rollback Holistic Patch

```
omspatcher rollback -id <patch id list> -spb_patch
```

Increased Kerberos/RADIUS credential support

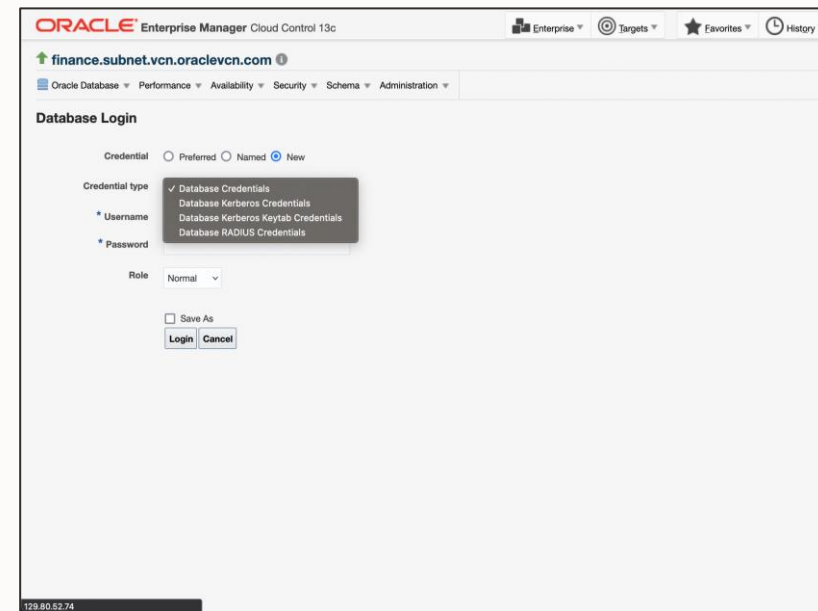
Kerberos/RADIUS authentication for a database

1. Create database named credentials
2. Provide Kerberos Credentials or Kerberos Keytab Credentials or RADIUS credentials
3. Use these named credentials to connect to database(CDB/PDB) in EM jobs (like backup database, create standby database, SQL script, PL/SQL etc...) or Enterprise Manager (EM) database pages



Kerberos/RADIUS authentication for one-time database login

1. Enable multiple credential types
`emctl set property -name oracle.sysman.db.multiCredTypeLogin -value true`
2. Enable RADIUS credential type
`emctl set property -name oracle.sysman.db.enable_radius_auth -value true`
3. Enable Kerberos credential type
`emctl set property -name oracle.sysman.db.enable_kerberos_auth -value true`





Kerberos versus RADIUS

Authentication support in Enterprise Manager

Kerberos

Basic management

Database performance pages

Execute SQL and SQL script jobs

Use in preferred credentials **New**

Support in Migration Workbench **New**

Add Space to Tablespace Corrective Action **New**

RADIUS

Basic management

Database performance pages

Execute SQL and SQL script jobs

Use in preferred credentials **New**

Available in both EM 13.5 & EM 24



Monitor Oracle Key Vault

Monitoring Oracle Key Vault (OKV) | New

- Discover and monitor
 - OKV Clusters
 - OKV Servers
- Monitor across the cluster
 - OKV Server status
 - Naming conflicts
 - Open incidents
- Metrics & alerts
 - Response
 - Process Status
 - Service Status
 - Performance
 - Certificate Expiry
 - Backup status

The screenshot displays the Oracle Enterprise Manager 24 interface for monitoring an Oracle Key Vault cluster named 'okvdemocluster1'. The page is titled 'Oracle Key Vault Cluster' and includes a search bar and a refresh button. The main content is divided into three panels: Summary, Naming Conflicts, and Open Metric Events. The Summary panel shows cluster details: Cluster Name (cluster_adbd), Cluster Version (21.9.0.0.0), Cluster Subgroups (cluster_sg_adbd), and Maximum Disable Node Duration (24 hours). The Naming Conflicts panel indicates 'No Naming Conflicts found'. The Open Metric Events panel shows 0 Open, 0 Critical, and 0 Warning events. Below these panels is a 'Nodes Information' table with columns for Target Name, Target Status, Version, Name, IP Address, Peer Node, Cluster Subgroup, Node Status, Cluster Service, Mode, and a set of icons for alerts.

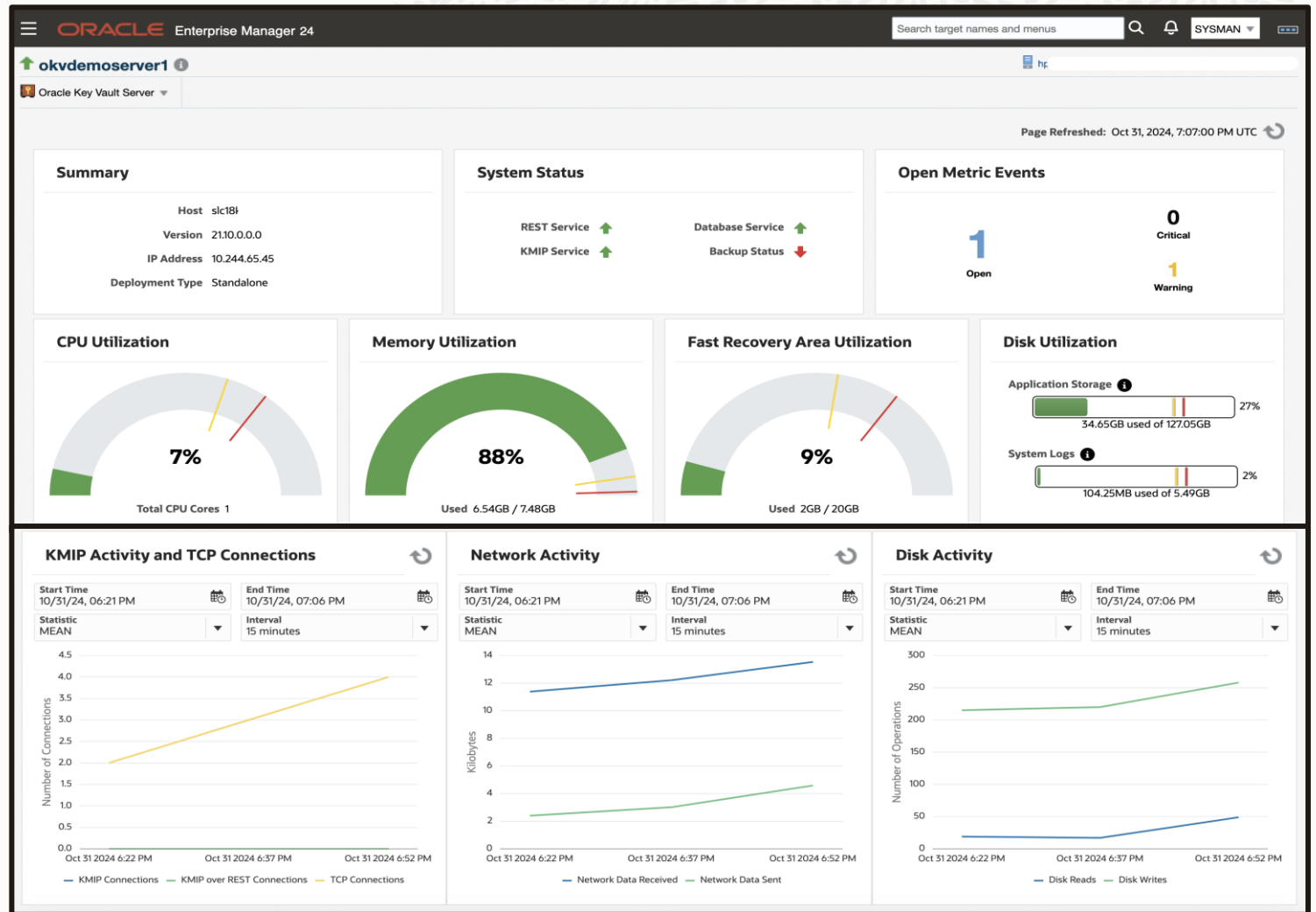
Target Name	Target Status	Version	Name	IP Address	Peer Node	Cluster Subgroup	Node Status	Cluster Service	Mode	Alerts
okvdemocluster1_node1_adbd_okv219	↑	21.9.0.0.0	node1_adbd_okv219	100.7	node2_adbd_okv219	cluster_sg_adbd	ACTIVE	↑	Read-Write	0 Critical, 1 Warning
okvdemocluster1_node2_adbd_okv219	↑	21.9.0.0.0	node2_adbd_okv219	100.7	node1_adbd_okv219	cluster_sg_adbd	ACTIVE	↑	Read-Write	0 Critical, 1 Warning

Available in EM 24



Monitoring Oracle Key Vault (OKV) | New

- Understand status and performance of each OKV Server
- Resource usage (CPU, Memory, Fast Recovery Area, Disk)
- KMIP Activity and TCP Connections
- Network Activity
- Disk Activity



Data Masking and Subsetting

Oracle Data Masking and Subsetting

Secure data sharing for application testing, business analytics, and ML model development

Locate and categorize sensitive data

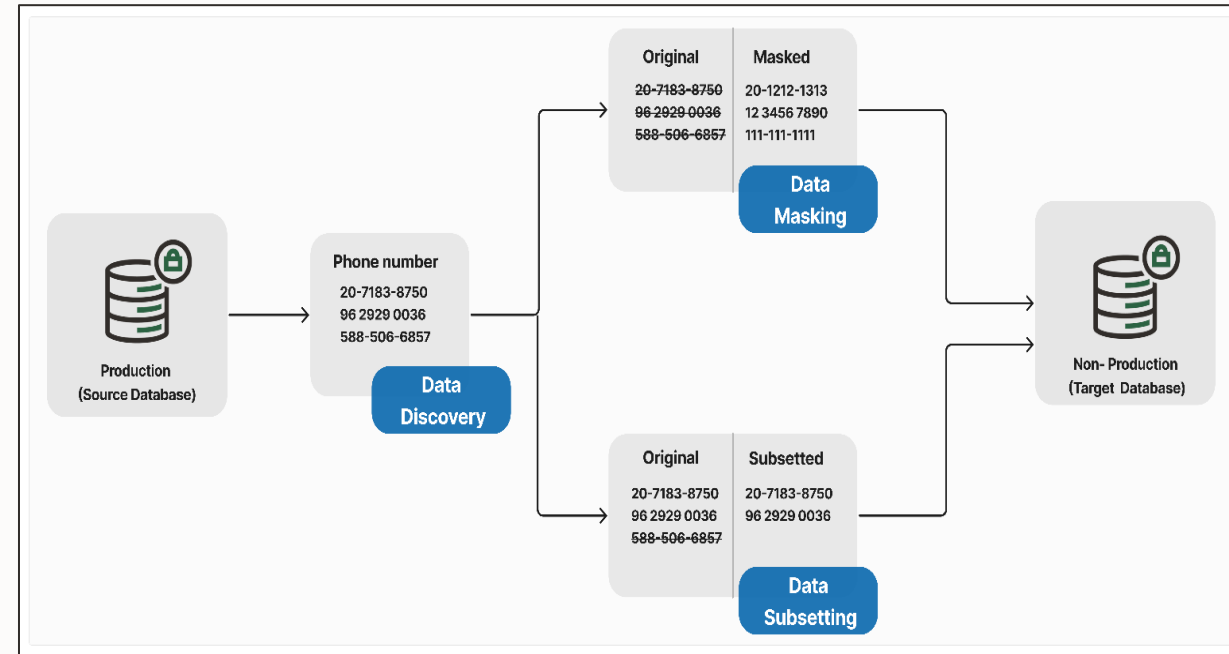
- Identify sensitive schemas for masking and other security controls
- Predefined sensitive types for PII, biographic, IT, and financial data

Mask copies of production data with anonymized values

- Support business processes while addressing compliance requirements
- Flexible masking options for in-place processing and data exports

Decrease data set size

- Reduce risks and operational costs by extracting only essential data
- Create targeted subsets based on size, conditions, or table partitions



Simple workflows guide the user through discovery, masking and subsetting



Oracle Data Masking and Subsetting

New features with Enterprise Manager 24

Modernized user interface

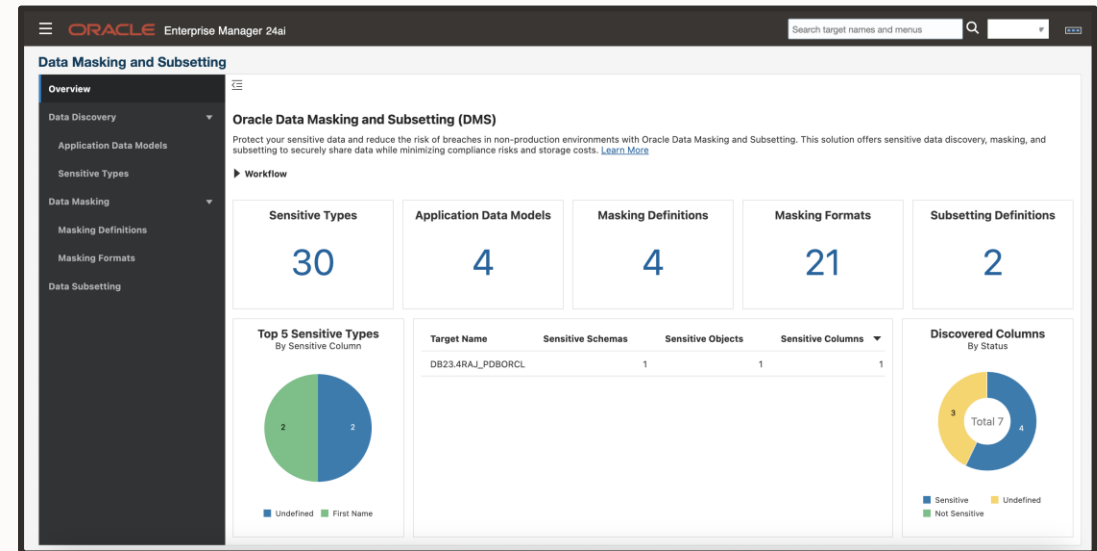
- Redesigned discovery and masking pages using advanced UI frameworks
- Clear visual guides and menu placements for seamless task completion

Improved visibility

- Key metrics dashboard for intuitive process monitoring
- Advanced search and sorting for quick and relevant data access

Superior user experience

- Streamlined UI workflows for creating masking formats and defining masking rules, enabling faster execution
- Enhanced page load speeds, delivering a highly responsive and seamless user interface experience



Enterprise Manager 24 : essential security insights

Enterprise Manager 24 architecture overview

Key components

Modernizing EM - Dual container architecture

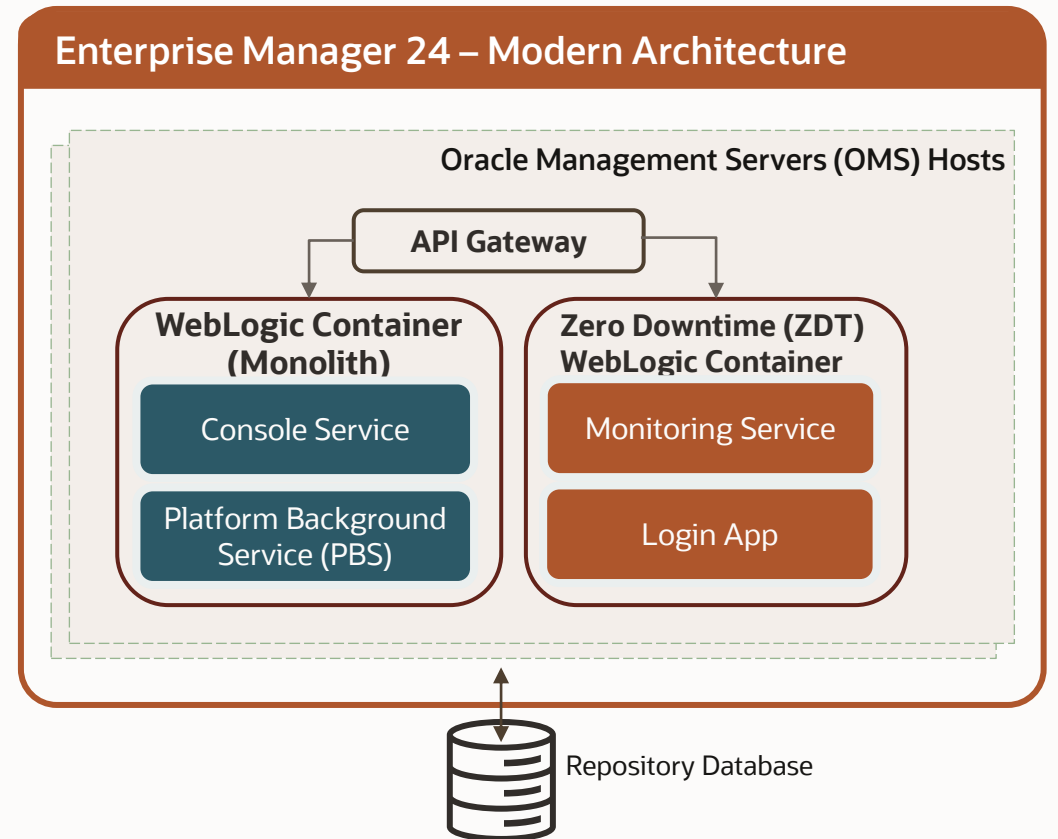
- OMS is split into two separate containers - **WebLogic container** for traditional EM services and **Zero Downtime (ZDT) WebLogic Container** for continuous monitoring
- ZDT Container runs on separate WebLogic domain ensures critical monitoring remain operational during patching

ZDT - Monitoring service and login app

- Monitoring, alert evaluation and all notifications will continue to work seamlessly in the same way as if Enterprise Manager was fully available
- Login app is deployed in the ZDT container provides authentication solution to ZDT and traditional services

API Gateway

- Single entry point for all external communications - user interface traffic, API calls, agent communication
- Monitors the health and status of dual container



Enterprise Manager 24 : essential security insights

EM 13.5

External Authentication Supported

- Oracle Single Sign-On (OSSO)
- Enterprise User Security (EUS)
- Direct LDAP integration (Oracle Internet Directory, Microsoft Active Directory)
- Security Assertion Markup Language (SAML)
- Integration with Oracle Access Manager Single Sign-On (OAM SSO)

Agent to OMS Communication

- Supports both TLS 1.1 and TLS 1.2
- OMS accepts both TLS 1.1 and TLS 1.2 requests

EM 24

External Authentication Supported

- Oracle Single Sign-On (OSSO)
- Enterprise User Security (EUS)
- Direct LDAP integration (Oracle Internet Directory, Microsoft Active Directory)
- Security Assertion Markup Language (SAML)
- If OAM SSO is configured in 13.5 then convert the OAM SSO to SAML before the upgrade
MOS notes 1620784.1 and 2976413.1

Agent to OMS Communication

- Supports only TLS 1.2
- OMS rejects any communication with TLS 1.1
- After the upgrade, communication of 13.5 agents using TLS 1.1 with OMS will be broken.
- As part of the upgrade process:
 - A list of affected agents will be generated.
 - Post upgrade to EM 24, the TLS versions for affected agents will need to be updated to restore agent-to-OMS communication.



Q&A

Learn More

Web: oracle.com/enterprisemanager

Videos: youtube.com/OracleEnterpriseMgr

Blogs: blogs.oracle.com/observability

Docs: <http://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

