



# New Enhancements in Oracle Database monitoring

---

**Desiree Abrokwa**

Product Manager

Enterprise and Cloud Manageability



# Agenda



Monitoring using database service name

OMS-to-database connectivity across networks

Pluggable Database (PDB) monitoring enhancements

Listener error monitoring

Enhanced diagnosability for database guided discovery

Complying with new database password policies

Monitoring Primary and Standby databases

# Monitoring using database service name

Service name- alias used to connect to the database

Oracle Database discovery, monitoring and admin operations

- SID is used for database connections (default)

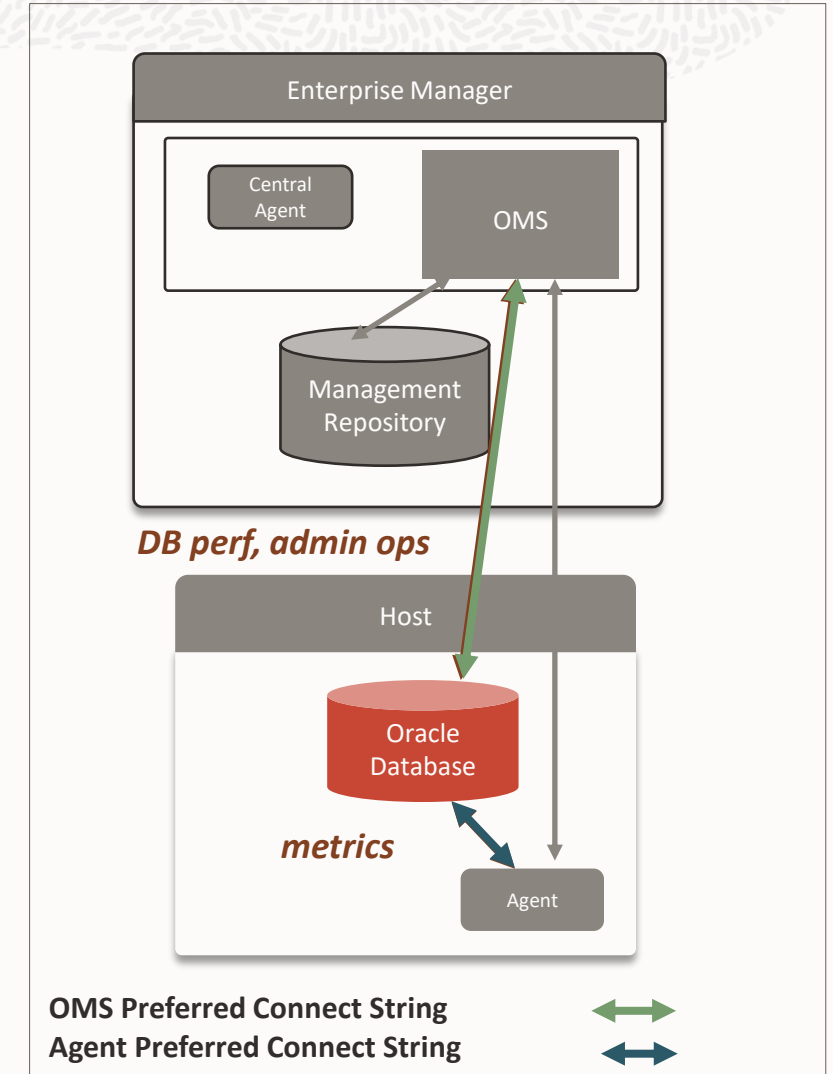
## 2 Types of Connections

- OMS-to-database
- Agent-to-database

**Service name** is supported through **Preferred Connect Strings**

- Preferred Connect String
  - Overrides default connection with a preferred method of connection
  - Fully qualified connect string  
(DESCRIPTION=(ADDRESS=(PROTOCOL=tcp) (HOST=myhost) (PORT=1521))  
(CONNECT\_DATA= (SERVICE\_NAME=MyDBService)))
- OMS Preferred Connect String
  - OMS-to-database connection
- Agent Preferred Connect String
  - Agent-to-database connection

To use Preferred Connect Strings, make sure EM and Agent are at least EM 13.5RU15



# Setting up Preferred Connect Strings - 1



Supported for Single Instance, RAC, PDB databases

- For RAC database: specify for each RAC instance, HOST = virtual IP of the RAC node

2 ways for setting up preferred connect strings

- `emcli add_target` or `modify_target` verb
- UI (Discovery or Monitoring Configuration)

`emcli`

OMS Preferred Connect String:

- `emcli modify_target -name="<target_name>" -type="<target_type>" -properties="PreferredConnectString:<connect string> " -on_agent`

Agent Preferred Connect String

- `emcli modify_target -name="<target_name>" -type="<target_type>" -properties="AgentPreferredConnectString:<connect string> " -on_agent`

# Setting up Preferred Connect Strings - 2

## UI setup

- `emctl set property -name oracle.sysman.db.showapcs -value true -sysman_pwd <pwd>`
- Bounce OMS

## Target's Monitoring Configuration UI

- Specify both OMS Preferred Connect String and Agent Preferred Connect String

## Log out/Log in to the console

- Updates OMS-DB cached connection

**Edit Cluster Database Instance**

Edit a cluster database instance by modifying target details.

Target Name db  
Target Type Cluster Database Instance  
Host p

Name	Value
Monitoring Username	dbsnmp
Monitoring Password	*****
Role	NORMAL
Oracle home path	/sc
Listener Machine Name	p
Port	1521
Connection Protocol	TCP
Database SID	db
OMS Preferred Connect String	(DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)(HOST=...)(PORT=1521))(CONNECT_DATA=(SERVICE_NAME=rac_apcs_test2)(INSTANCE_NAME=db232)))
Agent Preferred Connect String	(DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)(HOST=...)(PORT=1521))(CONNECT_DATA=(SERVICE_NAME=rac_apcs_test2)(INSTANCE_NAME=db232)))

Preferred Connect Strings in the database monitoring configuration page



# OMS-to-Database connectivity across networks

## OMS-to-database connectivity

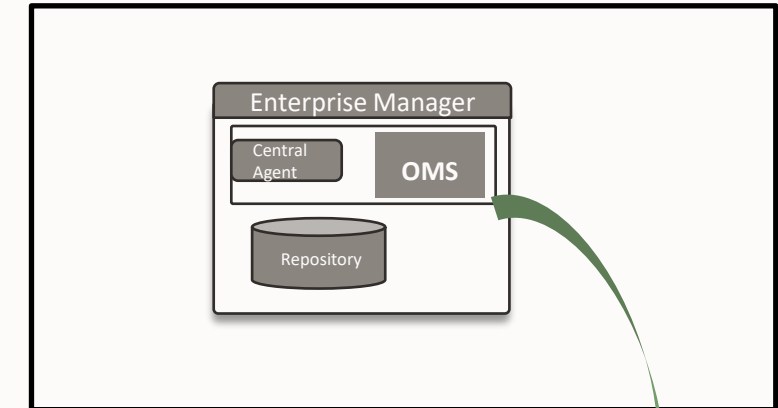
- Required to access DB performance pages and perform admin operations

OMS and target databases may be in separate datacenters or zones with no direct connectivity

To support OMS-to-database connectivity:

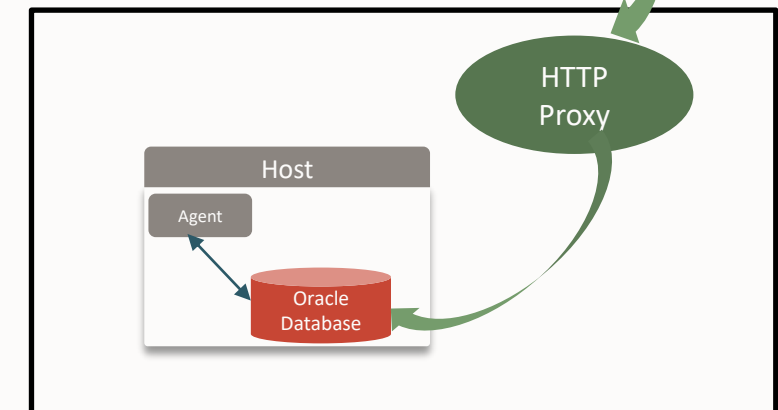
- Use HTTP Proxy server and **OMS Preferred Connect String with proxy server**
- Example:  
(DESCRIPTION= (ADDRESS=(**HTTPS\_PROXY=sales-proxy**)  
(**HTTPS\_PROXY\_PORT=8080**) (**PROTOCOL=TCPS**) (HOST=sales2-svr)  
(PORT=443)) (CONNECT\_DATA=(SERVICE\_NAME=sales.us.example.com)))
- Also requires JDBC patch for OMS [24793909](https://www.oracle.com/technetwork/database/enterprise/patches/24793909-01.htm)
- New in EM 13.5 RU18

## Data Center 1



OMS Preferred Connect String with proxy server

## Data Center 2



# Monitoring PDBs in a Cluster Database (RAC)

Current requirement for monitoring PDBs

- All PDBs must be open across all RAC instances

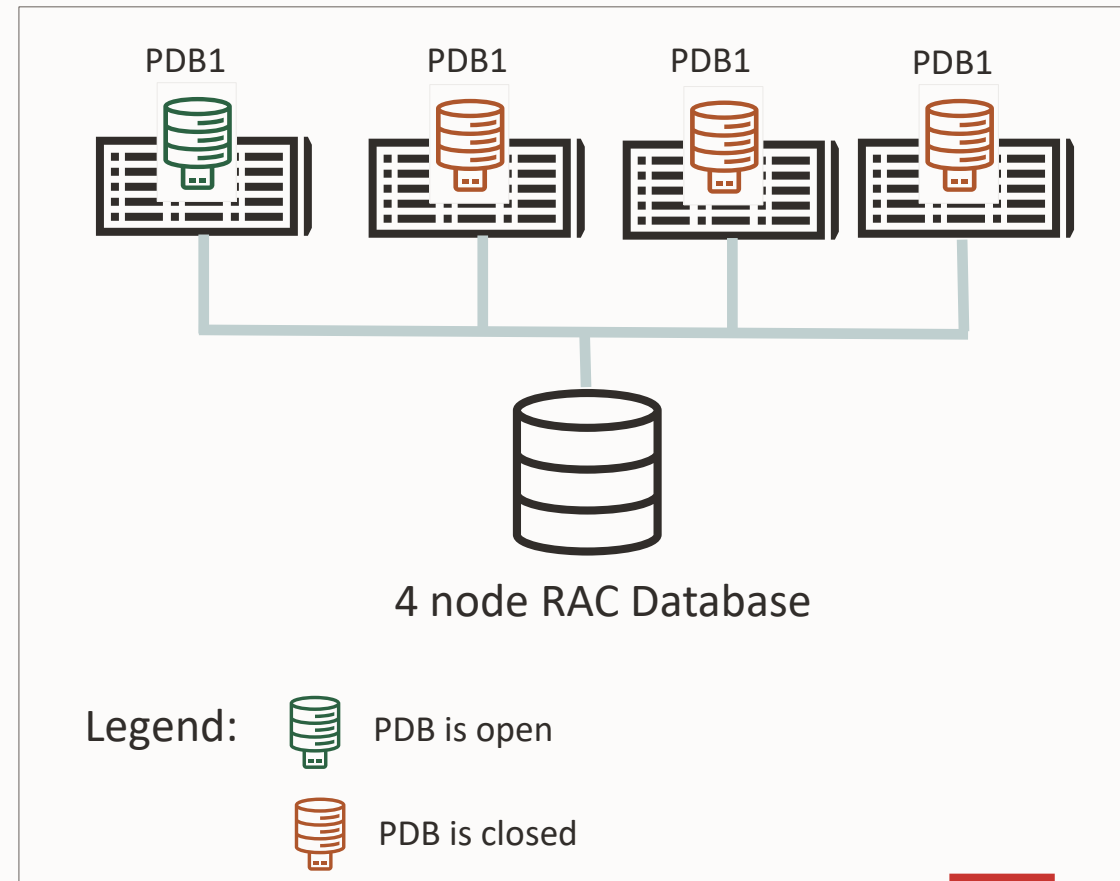
If your PDB is open only on *one specific preferred RAC instance*, use the Preferred Connect String

1. Create service for PDB
2. Create fully qualified connect string that uses the SCAN listener and service for the PDB  
(DESCRIPTION = (ADDRESS\_LIST = (ADDRESS = (PROTOCOL = tcp)  
(HOST = <hostname of the scan listener>)(PORT = 1521)))  
(CONNECT\_DATA = (SERVICE\_NAME = <service for the PDB)))
3. Monitoring configuration of the PDB
  - Specify **Preferred Connect String** for **OMS** and **agent**

Agent will connect, via scan listener, to the open PDB on the preferred RAC instance



PDB1 on a 4 node RAC

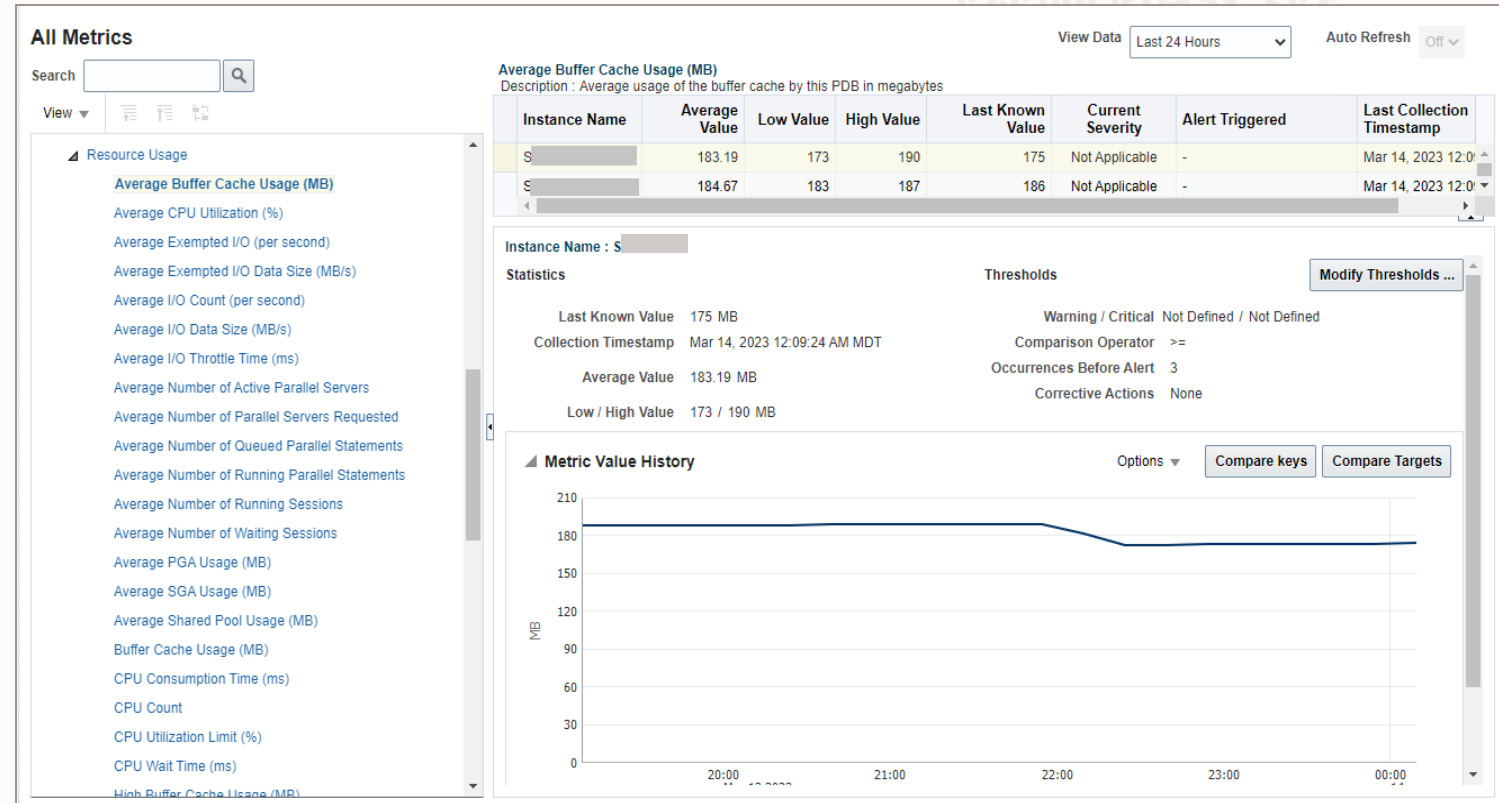


# Resource usage monitoring for PDBs

Rich set of metrics for the **PDB on a per instance** basis:

- CPU
- Buffer Cache
- I/O
- Avg number of running sessions, waiting sessions
- SGA and PGA usage etc.

Refer to [PDB Resource Usage](#) metrics in the Oracle Database Metric Reference





# Monitoring PDB Open Mode

## PDB Mode metric

- Monitors PDB open mode on per PDB/Instance basis
- Mode:
  - READ WRITE, READ WRITE RESTRICTED, READ ONLY, READ ONLY RESTRICTED, MOUNTED (closed)

For each RAC Instance, you can be alerted for these:

You want an alert on...	Metric	Alert threshold
PDB is closed on a RAC instance	Mode	MOUNTED
PDB is open in restricted mode	Any Restricted	YES
PDB is open in read only restricted mode	Read Only Restricted	YES

Monitor PDB open mode across all RAC instances

<b>PDB Mode</b> Description : Open mode of the PDB on each instance. These scenarios are covered: READ ONLY, READ WRITE, MOUNTED, READ ONLY RESTRICTED, READ WRITE RESTRICTED, MOUNTED (closed) Collection Schedule N/A Upload Interval Server Generated Last Upload Mar 18, 2023 5:33:42 AM GMT						
		Instance Name	Any Restricted	Mode	Read Only Restricted	Read Write Restricted
	▶	orcl19111	YES	READ WRITE	NO	YES
	▶	orcl19112		MOUNTED		

Alert: PDB is open in restricted mode on a RAC instance

Metric Alert History		
Severity	Timestamp	Message
⚠	Mar 17, 2023 5:29:41 AM...	Pluggable Database orcl1911_PDB1 is open in restricted mode on database instance orcl19111



# Enhanced support for PDB Metric Extensions

## Use Case:

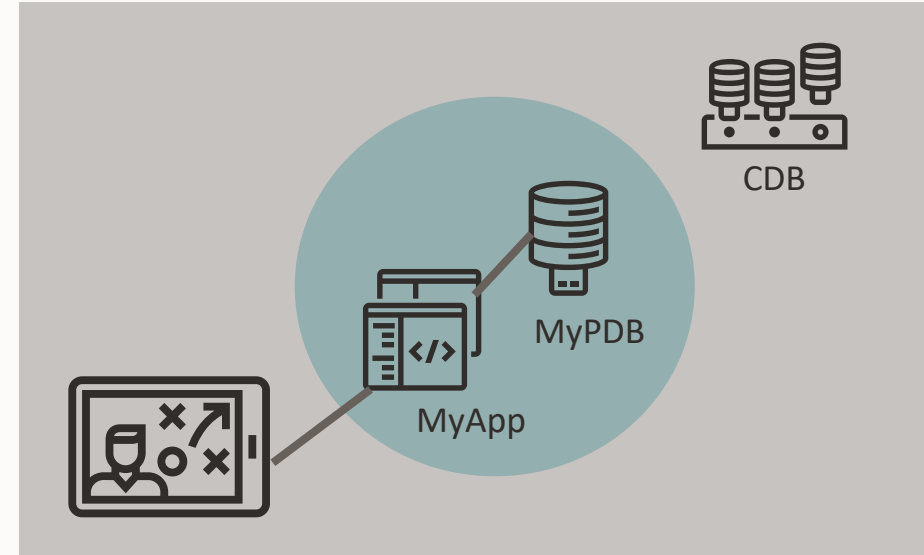
You want to monitor application metrics for a PDB

## Solution:

Create a metric extension for the PDB using a PDB local user

By default, metric extensions use the monitoring credentials for the target

- PDB targets are monitored using CDB common user (DBSNMP)
- Need to create a custom monitoring credential set for the PDB target type to be used with the metric extension

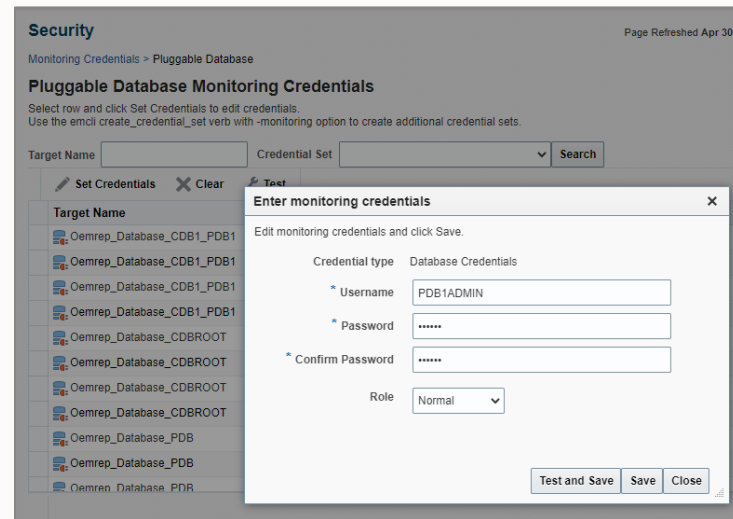


# Solution: PDB metric extension using a PDB local user

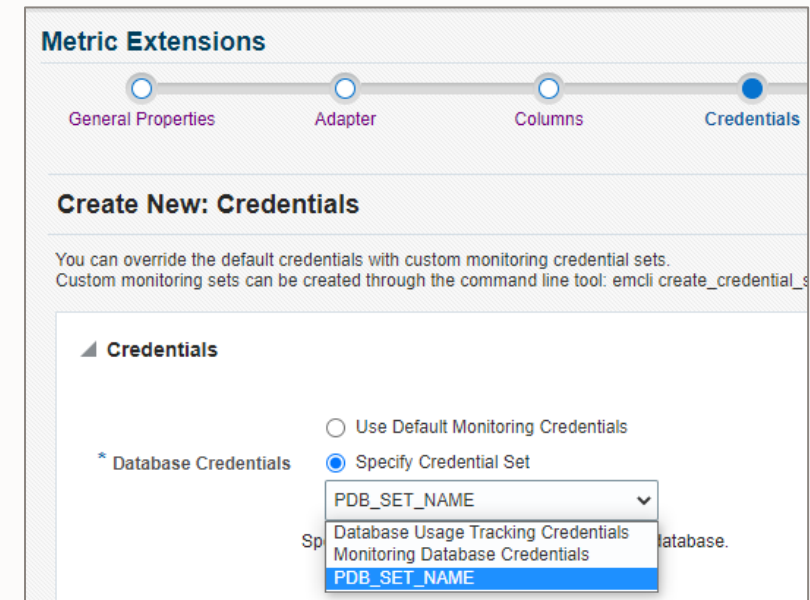
1. Create monitoring credential set for PDB target type

```
emcli create_credential_set -  
set_name="PDB_SET_NAME" -  
target_type="oracle_pdb" -  
supported_cred_types="DBCreds"  
-monitoring -description="PDB creds"
```

2. In the PDB credential set, specify your PDB local user



3. In metric extension, choose the PDB credential set



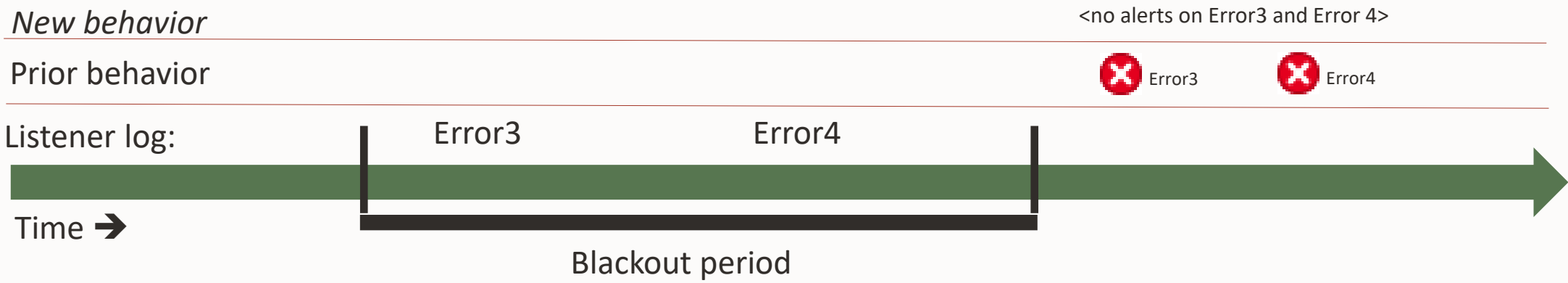
# Listener error monitoring

TNSError metric - used to monitor errors in the listener log file

Updated semantics:

- If Listener is in blackout for a time period, when blackout is stopped, expected errors that occurred during blackout will *not* generate alerts
- Prior behavior: Errors occurred during the blackout will generate alerts after blackout stops

If you would still like to get alerts on listener log errors during maintenance, use Notification Blackouts instead of (regular) Blackouts.

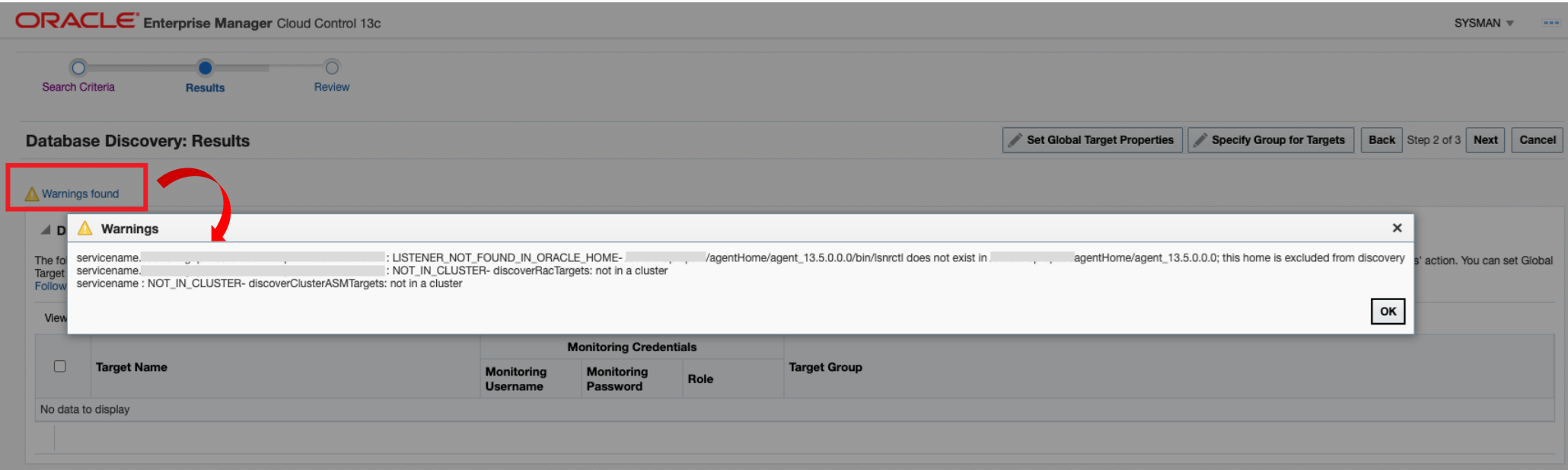


# Enhanced diagnosability for database system guided discovery

Database system is discovered and created using guided database discovery: *Oracle Database, Listener and Automatic Storage Management*

In addition to errors, warnings encountered with discovery are now also shown:

- Enables users to troubleshoot and not miss potential targets that could have been discovered



# Meeting changing database password policies

## Enhanced database password job with new 'reference password'

Two job types to change the database password:

- Change the Password for the *Database Monitoring User*
- Change the Password for a *Database User*

If database password policy changes, **specify a 'reference password' that complies with new password policy**

Example:

- New password policy – minimum characters increased from 8 to 12 and add special characters
- Solution: Auto-generate password with reference password of 12 characters with special characters
- Job generates a new password in the target database, EM monitoring credentials, EM preferred credentials

Blog: [Meet changing database password policies using Enterprise Manager](#)

### Job

#### Create 'Change the Password for the Database Monitoring User' Job

General

Parameters

Credentials

Schedule

Access

Auto-Generate New Password

Yes (Based on Reference Password) ▾  
Auto-Generated password will use the format of the current password or reference password as the basis for generating a new password.

Reference Password if Auto-Generated

.....  
Enter a sample password whose format will be used to auto-generate a new password. This value is used only if Auto-Generate New Password is 'Yes (Based on Reference Password)'.

Confirm Reference Password

.....  
Confirm the Reference Password value if specified.

New Password if Non Auto-Generated

Password for the Database Monitoring User. This value is used only if Auto-Generate New Password is 'No'.

Confirm New Password

Confirm the new Password if specified.

Use the *reference password* as a template for a new password that complies with new security policies

## Meeting changing database password policies – 2

You can use the job *Change the Password for the Database Monitoring User* in these 2 ways:

- Job submitted against a group of database target OR
- Corrective Action when the password is about to expire
  - Associate it with the *Monitoring User Expiry* metric which alerts when account will expire in xx hours
  - Associate it with your own metric extension (which alerts when password needs to be changed)
    - See AT&T blog and video:  
*More secure and efficient: Changing DBSNMP password using automation*  
<https://blogs.oracle.com/observability/post/more-secure-and-efficient-changing-dbsnmp-password-using-automation>

# Monitoring Primary and Standby databases

## Monitoring Credentials

If your Standby database is in read only mode (Active Data Guard), you can use regular monitoring credentials (e.g., DBSNMP)

Otherwise, grant monitoring user either SYSDBA role or SYSDG privilege

- Granting SYSDG aligns with principle of least privileges (security best practice)

If the monitoring user (e.g., DBSNMP) is used...

- To monitor a database that has only the standard out-of-box metrics and metric extensions that query fixed views or standard data dictionary views: Grant SYSDG (recommended) or SYSDBA
- To monitor a database that has metric extensions that query application data: Grant SYSDBA

You can use the same user (DBSNMP with SYSDG or SYSDBA) to monitor both Primary and Standby

Refer to EM Documentation: [Monitoring with SYSDG Privileges](#)



# Operations on Primary and Standby databases – 1

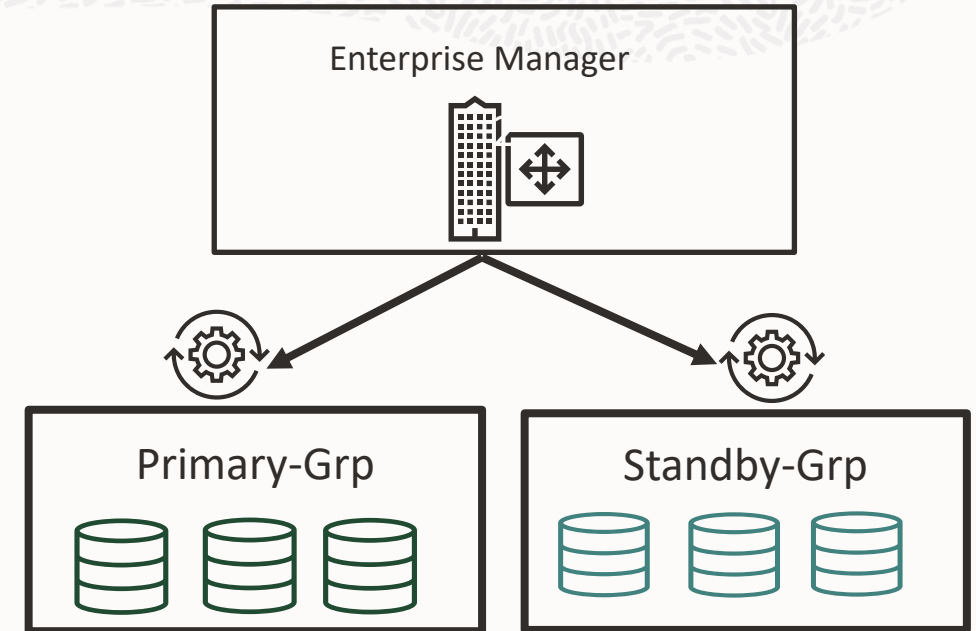
Automate all operations using groups

**Step 1:** Create dynamic group for Primary databases and another dynamic group for Standby databases

- Group membership will be maintained across DB role changes

**Step2:** Use these groups in your operations against Primary and Standby databases

- Operations will apply to the current members of the group



# Operations on Primary and Standby databases - 2

## Create dynamic groups

### Create dynamic group for Primary databases and another dynamic group for Standby databases

- Use new target property *High Availability Role* for dynamic group criteria
- *High Availability Role* identifies the database role: primary or standby
- When database role changes via switchover or failover, target property is automatically updated

Example:

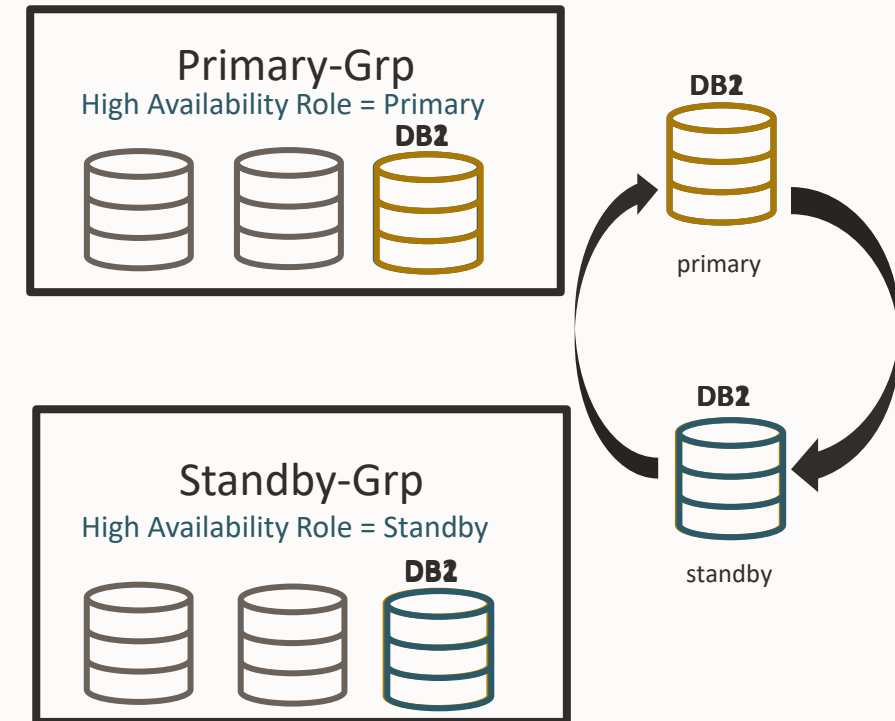
Group *Primary-Grp* (High Availability Role = Primary)

Group *Standby-Grp* (High Availability Role = Standby)

When database role changes

- *High Availability Role* property is updated accordingly
- DB1 (new standby): High Availability Role = Standby → goes to Standby-Grp
- DB2 (new primary): High Availability Role = Primary → goes to Primary-Grp

Refer to MOS note 2935430.1 (EM 13c - RU13 High Availability Role Target Property)



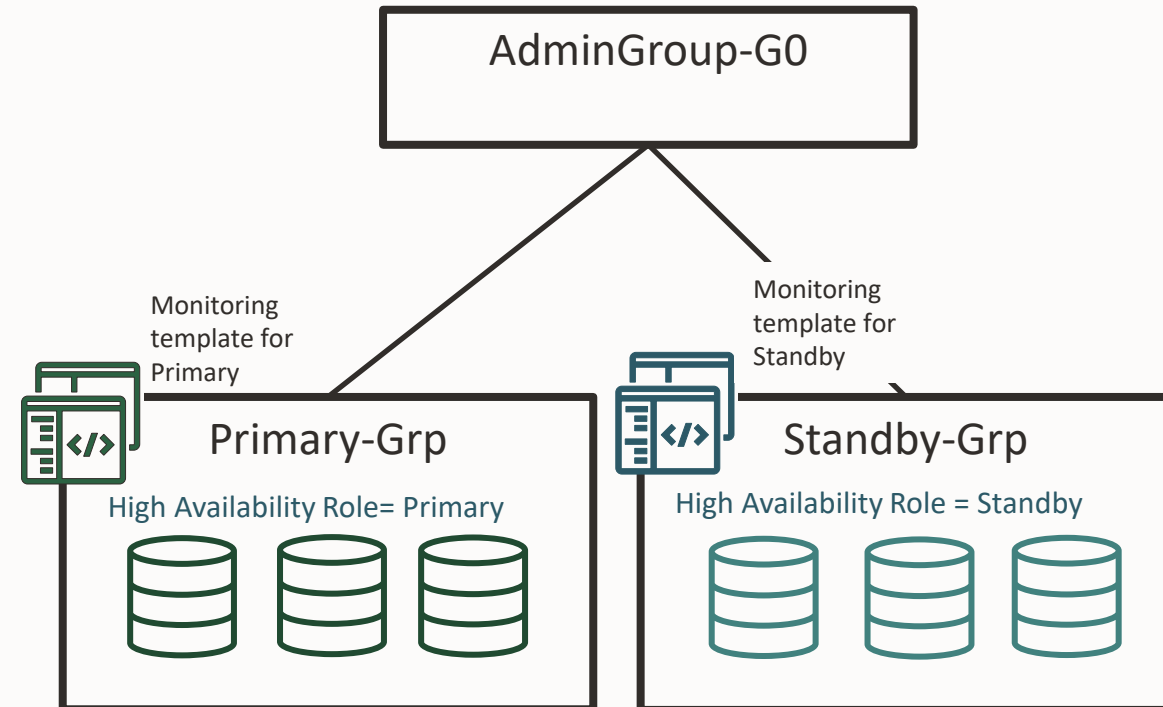
# Operations on Primary and Standby databases - 2

## Applying monitoring settings

### Use Case #1: Applying the appropriate monitoring settings for primary and standby databases

Solution:

- Create separate administration groups (which is a type of dynamic group) for Primary and Standby databases based on *High Availability Role* target property
- Create separate monitoring templates for Primary and Standby databases and associate with the appropriate administration group
- If DB role changes, databases go into the appropriate group and associated monitoring template will be applied



# Operations on Primary and Standby databases – 3

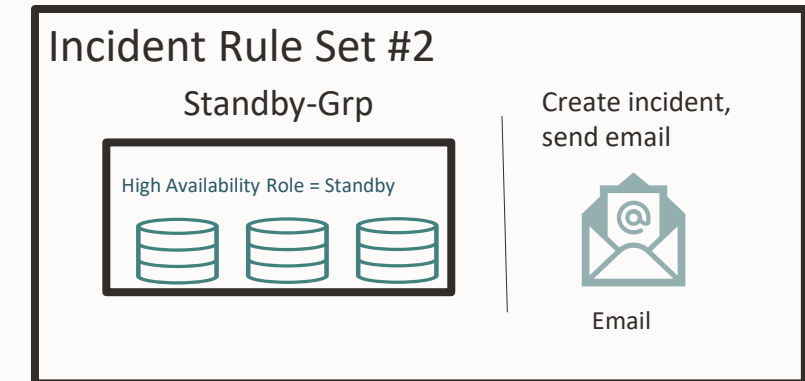
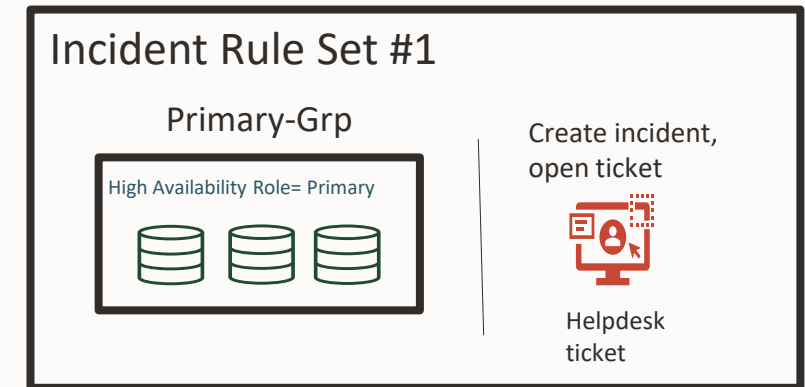
Sending appropriate notifications on incidents

## Use Case #2: Different notification requirements for Primary and Standby databases

Example: Create ServiceNow tickets incidents on Primary; send email for incidents on Standby

Solution:

- Incident Rule Set#1 for Primary group:
  - Specify Primary-Grp
  - Specify appropriate actions (e.g., open ticket for incident)
- Incident Rule Set#2 for Standby group:
  - Specify Standby-Grp
  - Specify appropriate actions (e.g., email for incident)



# Operations on Primary and Standby databases – 4

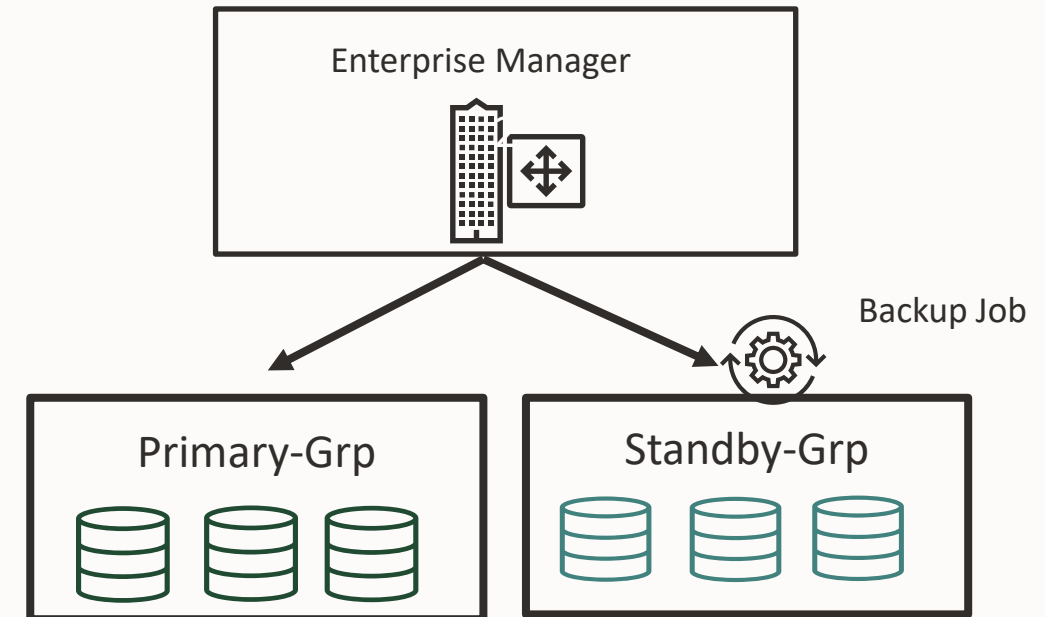
## Running Jobs

### Use Case #3: Different jobs for Primary and Standby databases

Example: Backup the database if it is Standby database

Solution:

- Create DB Backup Job on Standby-Grp
  - Backup will happen on all Standby databases (since they are part of the group)



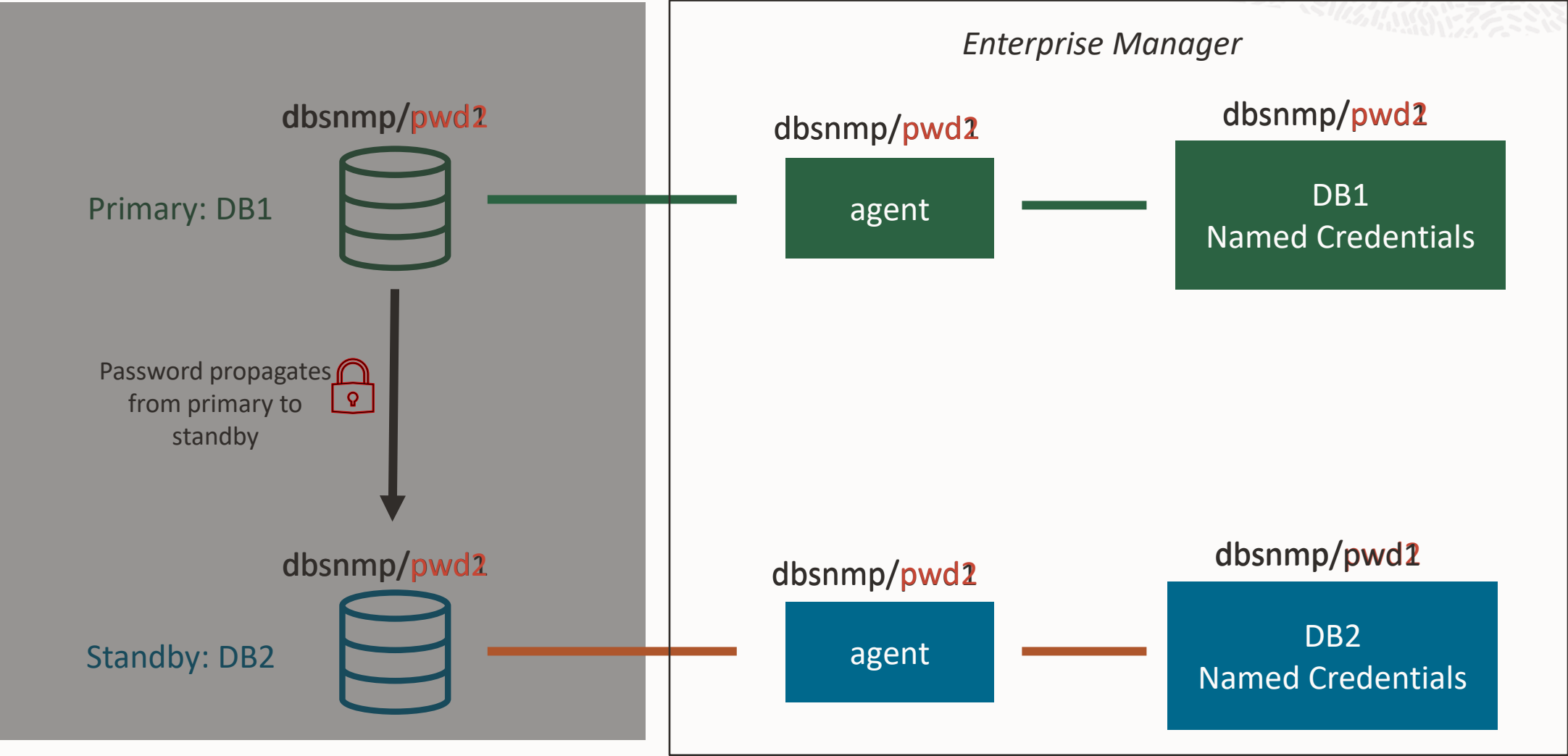
# Changing passwords on Primary and Standby databases – 1

Use job: *Change the Password for the Database Monitoring User*

Guidelines:

- Submit the job on the Primary-Grp
  - No need to include the Standby-Grp, its password will be automatically updated
- Use any of the password options:
  - Specify new password
  - Auto-generate by EM
  - Auto-generate by EM with reference password
- Job changes the password in the primary and standby database
  - Relies on DB 12.2+ feature of auto-propagating passwords from primary to standby (not supported for *Far Sync and Snapshot Standby databases*)

# Changing passwords on Primary and Standby databases – 2



# Enterprise Manager database monitoring

Enterprise Manager continues to enhance and provide solutions to meet customer requirements

- Monitoring databases using service names
- OMS-to-database connectivity across networks
- Richer PDB monitoring
- Listener error monitoring
- Comply with password policy changes
- Monitoring primary and standby databases





# Resources

Discovering and Adding Database Targets (includes the use of Preferred Connect Strings)

<https://docs.oracle.com/en/enterprise-manager/cloud-control/enterprise-manager-cloud-control/13.5/emmon/discovering-and-adding-database-targets.html#GUID-86BE0C0D-552C-4968-BF2E-BD8DC2ACD081>

PDB Metrics (part of Oracle Database Metric Reference Manual)

<https://docs.oracle.com/en/enterprise-manager/cloud-control/enterprise-manager-cloud-control/13.5/emdbm/pluggable-databases.html#GUID-BB2C32F2-06E7-4AD5-8822-C30A64A59DDD>

Automate Monitoring and Non-monitoring User Credential Password Management

<https://docs.oracle.com/en/enterprise-manager/cloud-control/enterprise-manager-cloud-control/13.5/emsec/keeping-enterprise-manager-secure.html#GUID-3F56C397-32DB-4195-B0BD-26A6CE0C505C>

MOS note 2935430.1 (EM 13c - RU13 High Availability Role Target Property)

<https://support.oracle.com/epmos/faces/DocumentDisplay?id=2935430.1>

Blog: Meet changing database password policies using Enterprise Manager

<https://blogs.oracle.com/observability/post/database-password-policies-enterprise-manager>



ORACLE

