Oracle Data Safe und CMU

Sichere Verwaltung von Datenbankbenutzern im großen Maßstab

Bettina Schäumer & Stefan Oehrli

DOAG Konferenz

November 2023

Speakers

Bettina Schäumer

Senior Principal Product Manager

Oracle

Stefan Oehrli

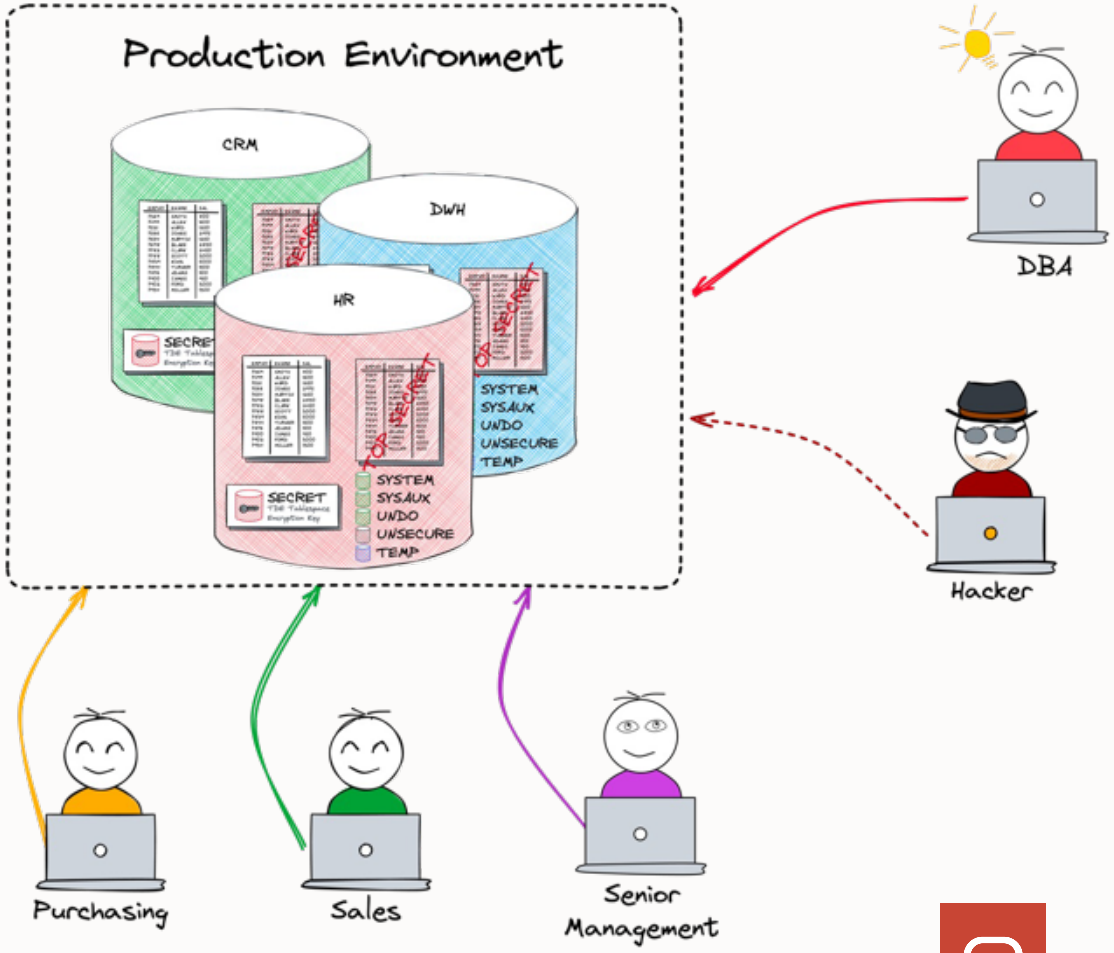
Tech Architecture Manager

Accenture

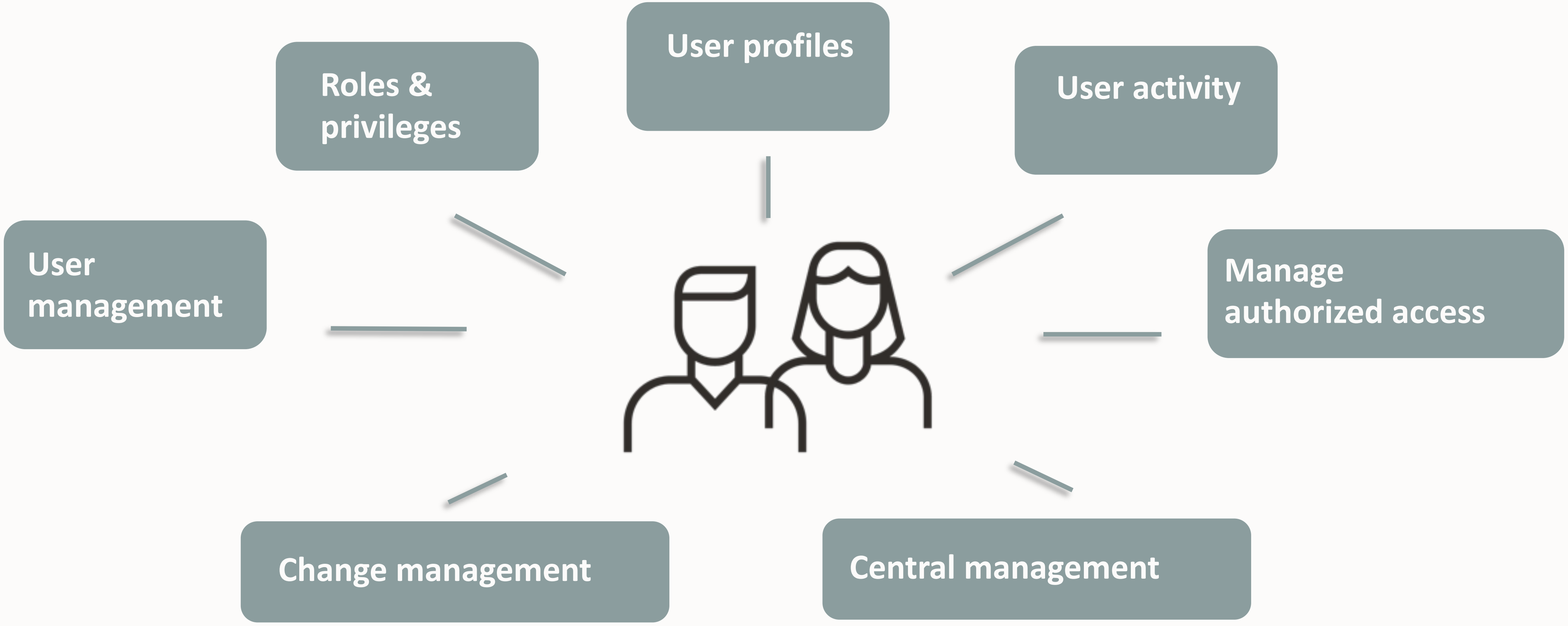
The challenges of user management

Why is user Management still an issue at all?

- **Who accesses which data** / database where?
  - Authentication and authorization
  - Production, test and development environments
- Who are my highly **privileged users**?
- How do I know if users or entitlements **were changed**?
- What are those **users doing** on the database?
- What activities do I **audit**?
- How are **permissions managed**?
  - Individual / decentralized by administrators
  - What happens with mutations
    (function changes, terminations, etc.)?
- Is there a role concept?



Different aspects of user management



Roles & privileges

User profiles

User activity

User management

Manage authorized access

Change management

Central management

Oracle Data Safe

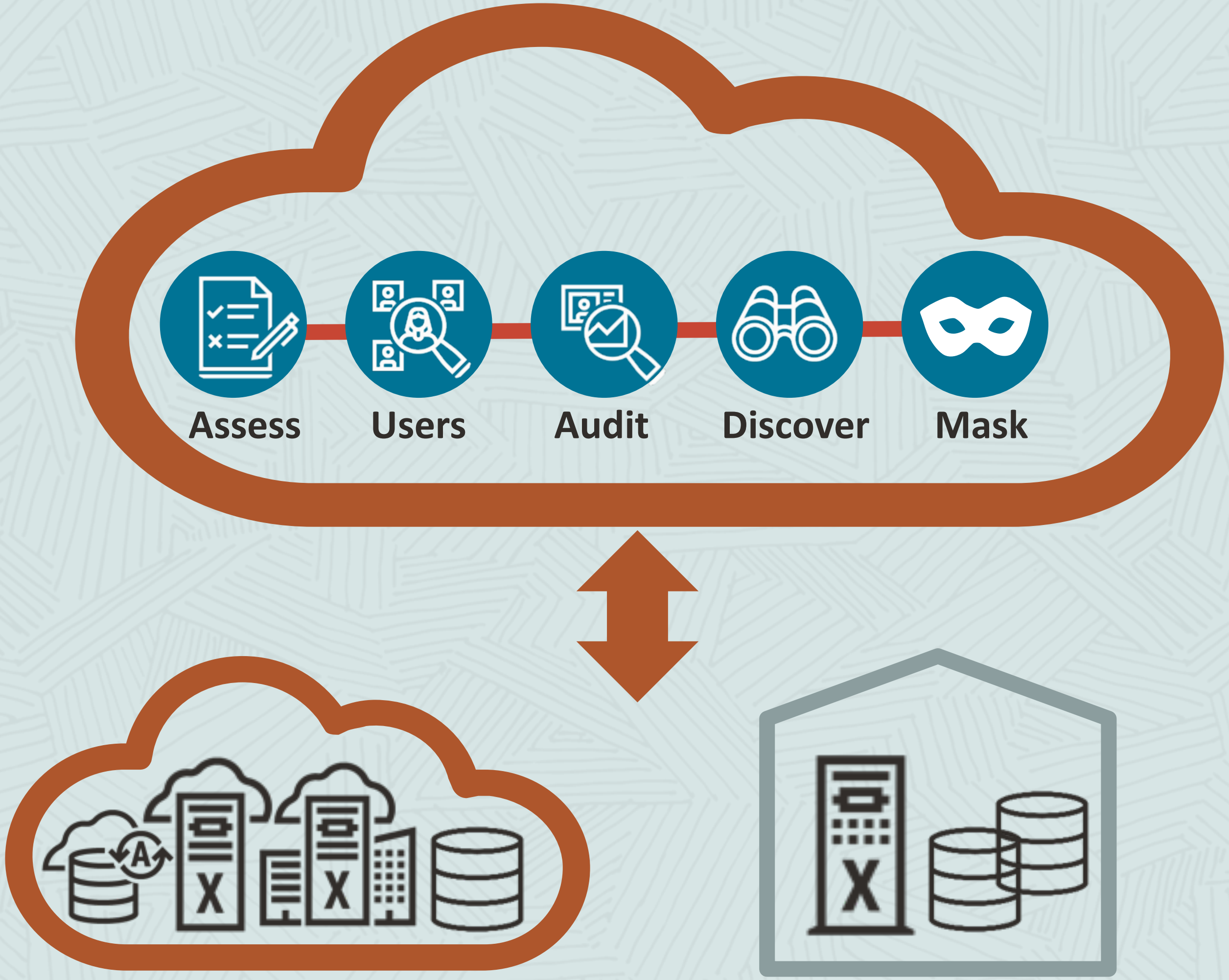
Unified database security control center

- Risk dashboard: configuration, data, users
- Monitor user activity
- Mask data for test environments
- Extensible - more features to come…

Benefits

- ✓ No special expertise needed: click-and-secure
- ✓ Saves time and mitigates security risks
- ✓ Defense-in-depth security for all customers

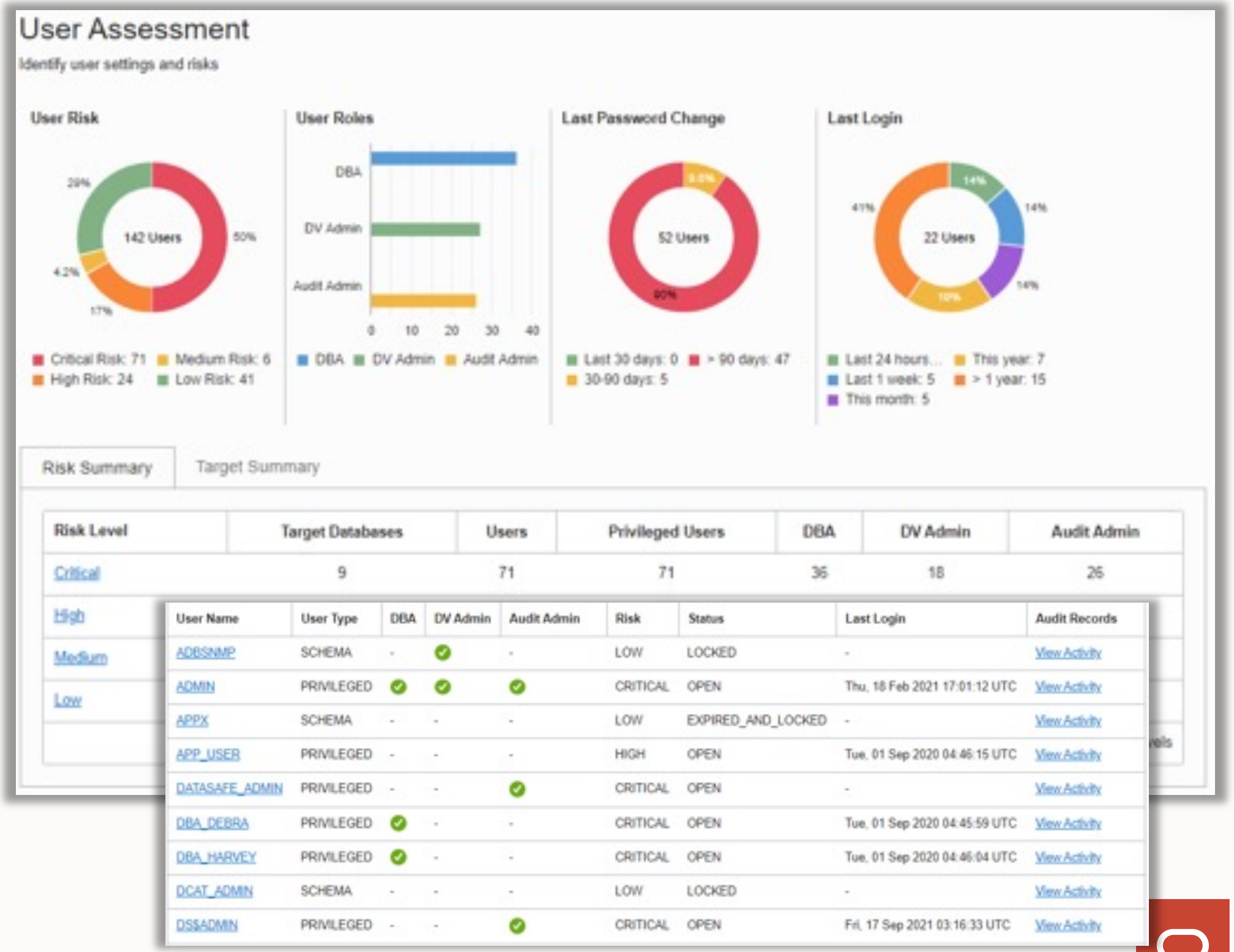
Securing both your cloud and on-premises databases



User Risk Assessment

Reduce risk from users by managing roles/privileges

- Identify highly privileged users
- Understand the potential risk level for each user
- Review their roles and privileges
- Evaluate user details like last login, password change, database activity



User Assessment

Identify user settings and risks

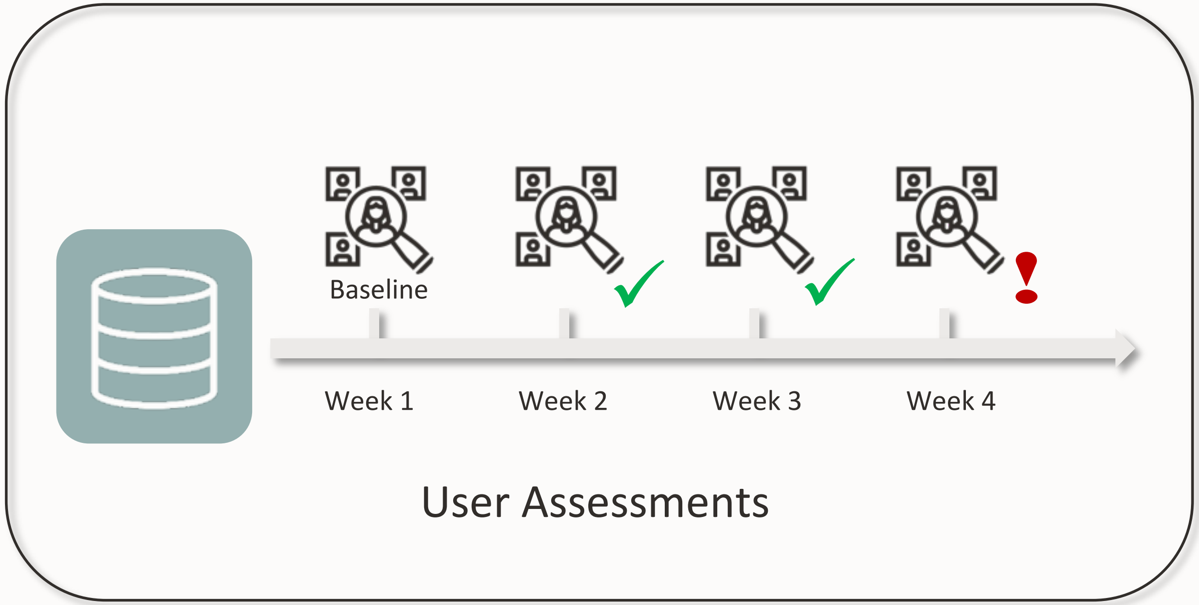
Risk Level	Target Databases	Users	Privileged Users	DBA	DV Admin	Audit Admin
Critical	9	71	71	36	18	26
High						
Medium						
Low						

User Name	User Type	DBA	DV Admin	Audit Admin	Risk	Status	Last Login	Audit Records
ADBSNMP	SCHEMA	-	✓	-	LOW	LOCKED	-	View Activity
ADMIN	PRIVILEGED	✓	✓	✓	CRITICAL	OPEN	Thu, 18 Feb 2021 17:01:12 UTC	View Activity
APPX	SCHEMA	-	-	-	LOW	EXPIRED_AND_LOCKED	-	View Activity
APP_USER	PRIVILEGED	-	-	-	HIGH	OPEN	Tue, 01 Sep 2020 04:46:15 UTC	View Activity
DATASAFE_ADMIN	PRIVILEGED	-	-	✓	CRITICAL	OPEN	-	View Activity
DBA_DEBRA	PRIVILEGED	✓	-	-	CRITICAL	OPEN	Tue, 01 Sep 2020 04:45:59 UTC	View Activity
DBA_HARVEY	PRIVILEGED	✓	-	-	CRITICAL	OPEN	Tue, 01 Sep 2020 04:46:04 UTC	View Activity
DCAT_ADMIN	SCHEMA	-	-	-	LOW	LOCKED	-	View Activity
DS$ADMIN	PRIVILEGED	-	-	✓	CRITICAL	OPEN	Fri, 17 Sep 2021 03:16:33 UTC	View Activity

User Risk Assessment

Detecting User and Entitlement Changes

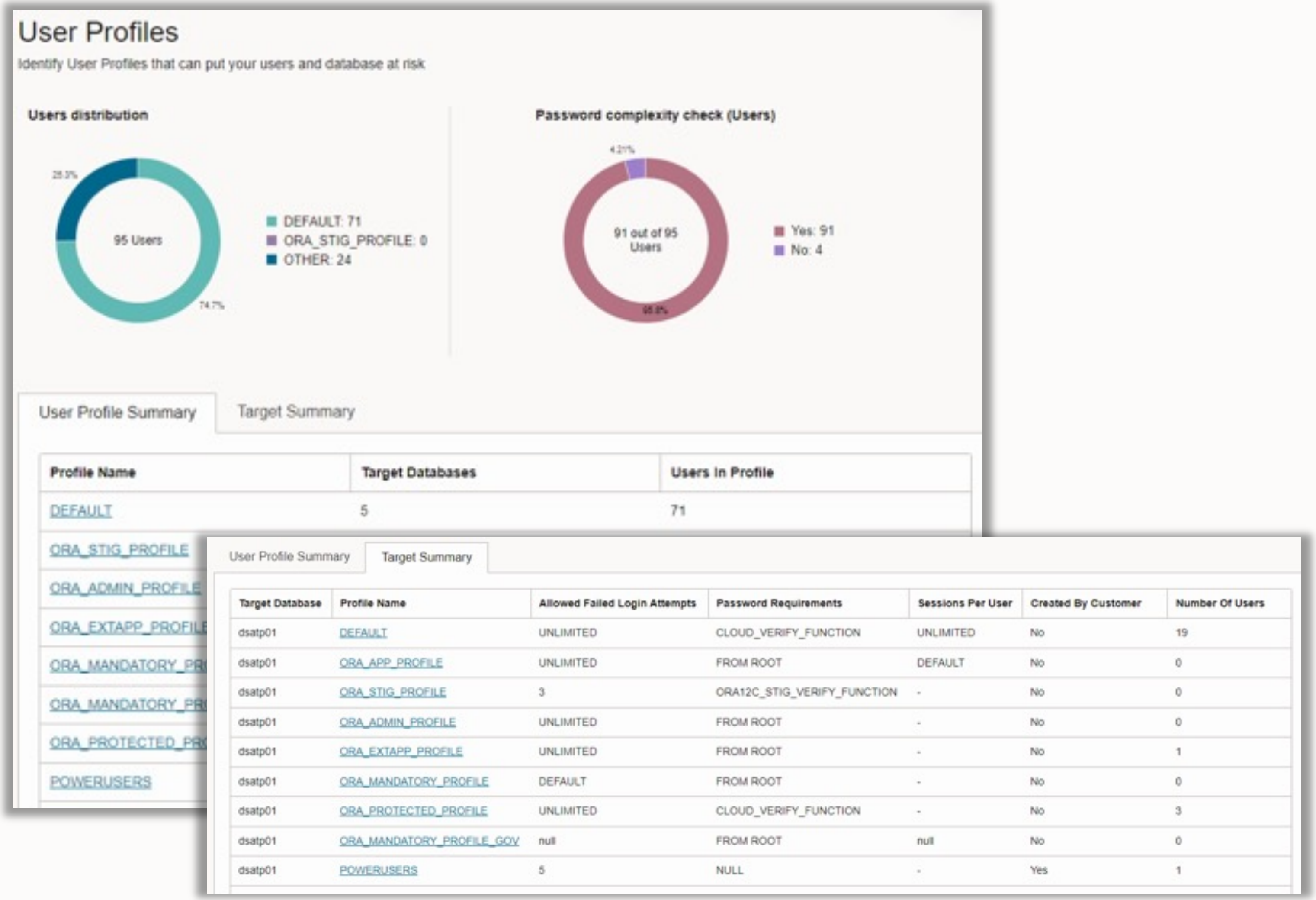
- Run periodic user assessments
- Compare new assessments against previous assessments
- Get notified and identify newly added users or changed entitlements



User Profile Insight

Evaluate password-related attributes associated with user profiles

- Review existing user profiles and their parameters
- Identify which profiles are assigned to which users
- Easily identify users and profiles without a password complexity function



User Profiles

Identify User Profiles that can put your users and database at risk

User Profile Summary | Target Summary

Profile Name	Target Databases	Users In Profile
DEFAULT	5	71
ORA_STIG_PROFILE		
ORA_ADMIN_PROFILE		
ORA_EXTAPP_PROFIL		
ORA_MANDATORY_PR		
ORA_MANDATORY_PR		
ORA_PROTECTED_PR		
POWERUSERS		

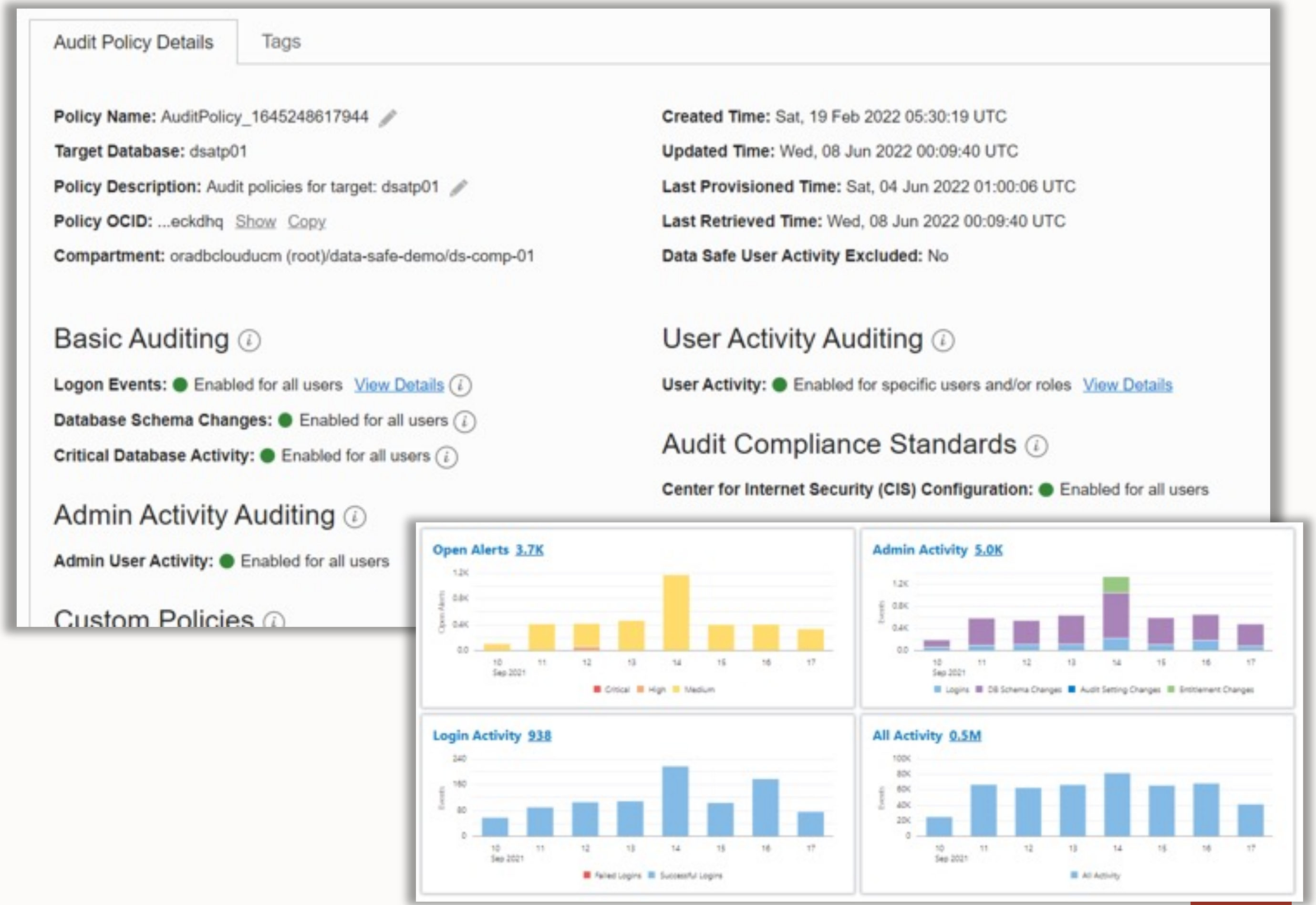
User Profile Summary | Target Summary

Target Database	Profile Name	Allowed Failed Login Attempts	Password Requirements	Sessions Per User	Created By Customer	Number Of Users
dsatp01	DEFAULT	UNLIMITED	CLOUD_VERIFY_FUNCTION	UNLIMITED	No	19
dsatp01	ORA_APP_PROFILE	UNLIMITED	FROM ROOT	DEFAULT	No	0
dsatp01	ORA_STIG_PROFILE	3	ORA12C_STIG_VERIFY_FUNCTION	-	No	0
dsatp01	ORA_ADMIN_PROFILE	UNLIMITED	FROM ROOT	-	No	0
dsatp01	ORA_EXTAPP_PROFILE	UNLIMITED	FROM ROOT	-	No	1
dsatp01	ORA_MANDATORY_PROFILE	DEFAULT	FROM ROOT	-	No	0
dsatp01	ORA_PROTECTED_PROFILE	UNLIMITED	CLOUD_VERIFY_FUNCTION	-	No	3
dsatp01	ORA_MANDATORY_PROFILE_GOV	null	FROM ROOT	null	No	0
dsatp01	POWERUSERS	5	NULL	-	Yes	1

User Activity Auditing

Track user actions and streamline auditing with robust reporting

- Provision audit, compliance, and alert policies
- Centrally collect audit data from your databases, and track sensitive operations
- Review and monitor user activity
- Audit reports
  - Interactive reports for forensics
  - Summary and detailed reports
  - PDF reports for compliance



Policy Name: AuditPolicy_1645248617944

Target Database: dsatp01

Policy Description: Audit policies for target: dsatp01

Policy OCID: ...eckdhq Show Copy

Compartment: oradbclouducm (root)/data-safe-demo/ds-comp-01

Created Time: Sat, 19 Feb 2022 05:30:19 UTC

Updated Time: Wed, 08 Jun 2022 00:09:40 UTC

Last Provisioned Time: Sat, 04 Jun 2022 01:00:06 UTC

Last Retrieved Time: Wed, 08 Jun 2022 00:09:40 UTC

Data Safe User Activity Excluded: No

Basic Auditing

Logon Events: ● Enabled for all users View Details

Database Schema Changes: ● Enabled for all users

Critical Database Activity: ● Enabled for all users

Admin Activity Auditing

Admin User Activity: ● Enabled for all users

Custom Policies

User Activity Auditing

User Activity: ● Enabled for specific users and/or roles View Details

Audit Compliance Standards

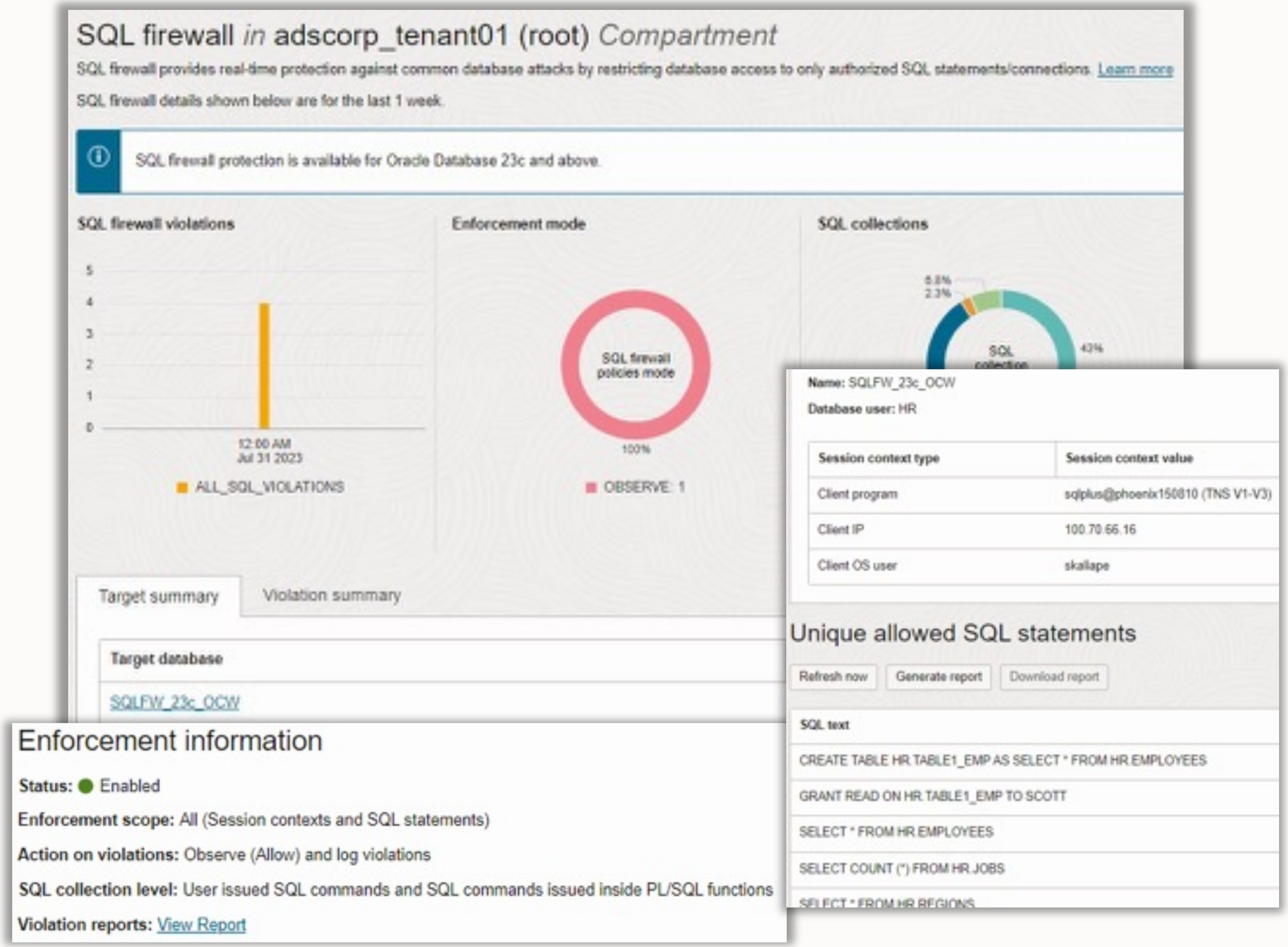
Center for Internet Security (CIS) Configuration: ● Enabled for all users

SQL Firewall

Prevent SQL injection and access from unauthorized access points

- Provides real-time protection against common database attacks by restricting database access to
  - authorized connections
  - authorized SQL statements
- Block or monitor any violations
- Mitigates risks from SQL injection attacks, anomalous access, and credential theft/abuse

Available for 23c databases only



SQL firewall *in* adscorp_tenant01 (root) *Compartment*

SQL firewall provides real-time protection against common database attacks by restricting database access to only authorized SQL statements/connections. Learn more

SQL firewall details shown below are for the last 1 week.

ⓘ SQL firewall protection is available for Oracle Database 23c and above.

Target database
SQLFW_23c_OCW

Name: SQLFW_23c_OCW

Database user: HR

Session context type	Session context value
Client program	sqlplus@phoenix150810 (TNS V1-V3)
Client IP	100.70.66.16
Client OS user	skallape

Unique allowed SQL statements

SQL text
CREATE TABLE HR.TABLE1_EMP AS SELECT * FROM HR.EMPLOYEES
GRANT READ ON HR.TABLE1_EMP TO SCOTT
SELECT * FROM HR.EMPLOYEES
SELECT COUNT (*) FROM HR.JOBS
SELECT * FROM HR.REGIONS

Enforcement information

Status: ● Enabled

Enforcement scope: All (Session contexts and SQL statements)

Action on violations: Observe (Allow) and log violations

SQL collection level: User issued SQL commands and SQL commands issued inside PL/SQL functions

Violation reports: View Report

SQL Firewall

Easy configuration, management, and monitoring in Data Safe

1

Collect

Turn on the SQL statement and user connection collection

2

Review & Modify

Review the SQL collection

Review and modify the allowed user connections (as required)

3

Enforce

Block or monitor any unauthorized SQL and/or user connections

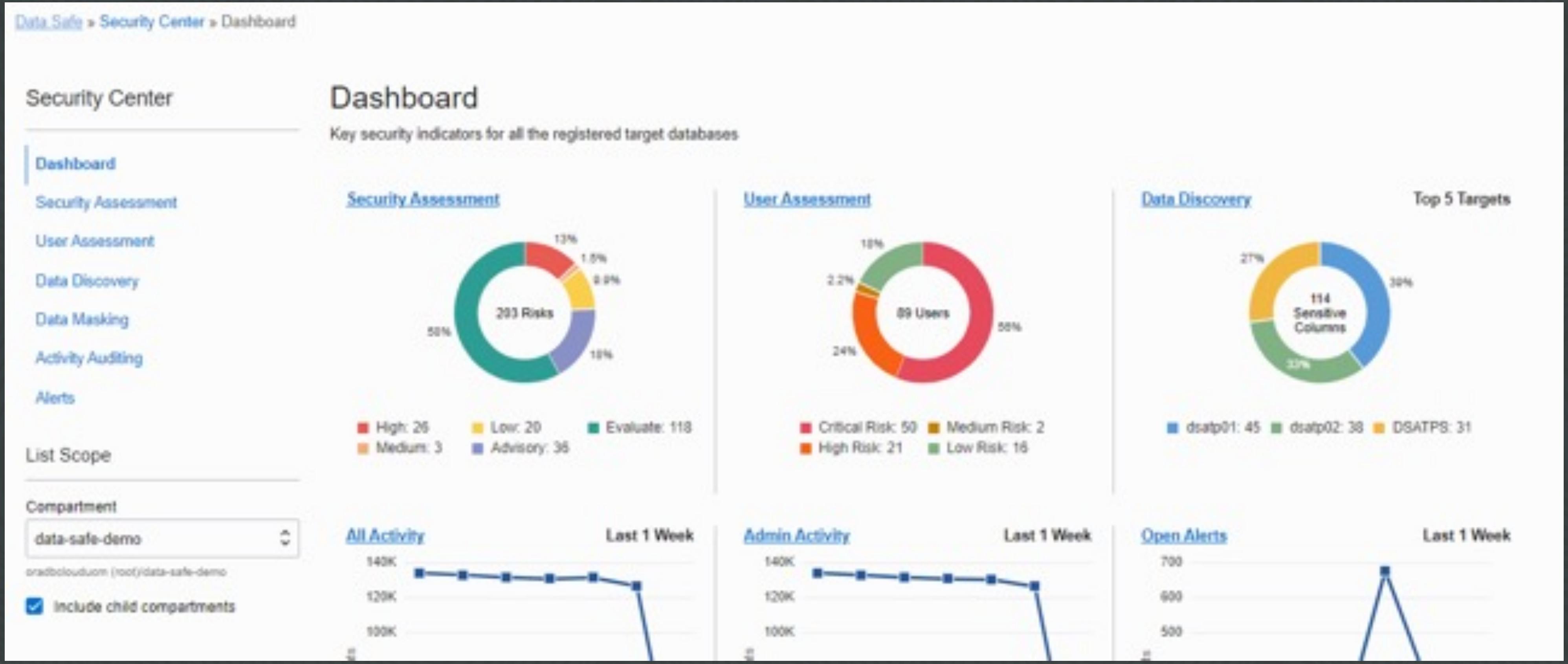
4

Monitor

Monitor any violations

Available for 23c databases only

Demo



Data Safe » Security Center » Dashboard

Security Center

- Dashboard
- Security Assessment
- User Assessment
- Data Discovery
- Data Masking
- Activity Auditing
- Alerts

List Scope

Compartment: data-safe-demo

oradbclouducm (root)/data-safe-demo

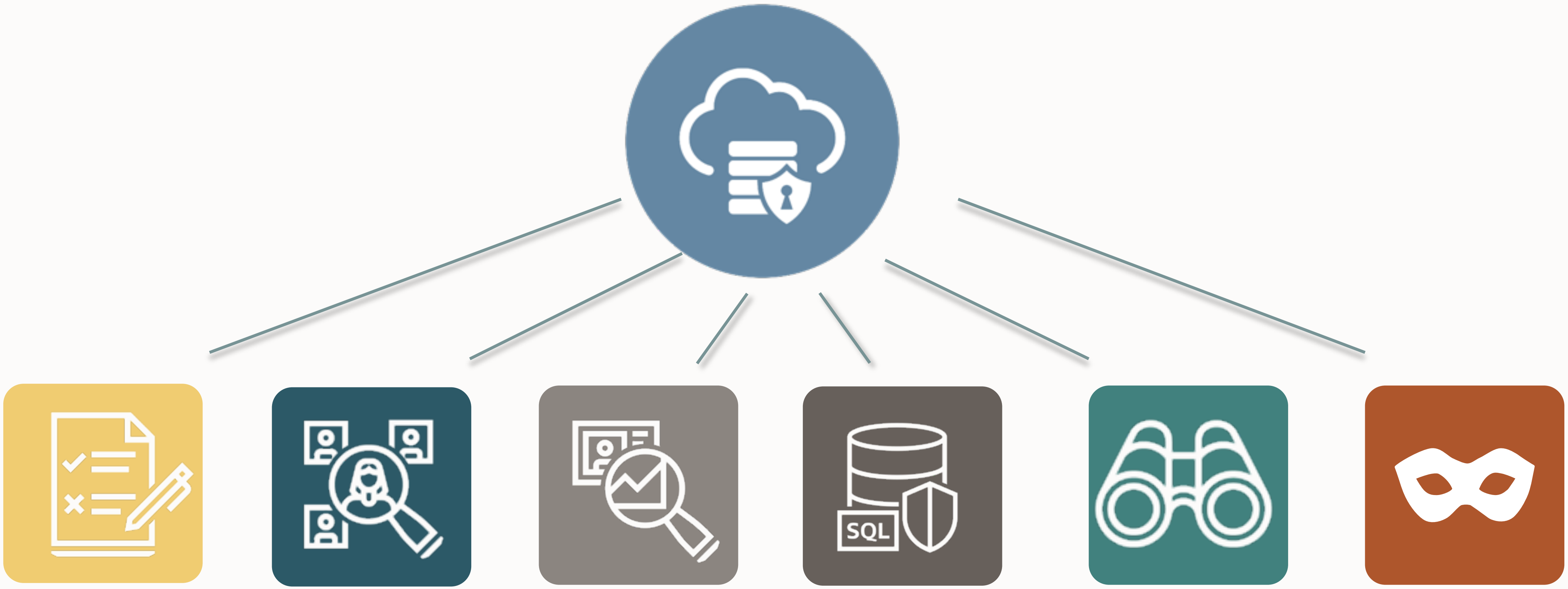
☑ Include child compartments

Dashboard

Key security indicators for all the registered target databases

Oracle Data Safe

Secure your Oracle Databases



Security Assessment

User Assessment

Activity Auditing

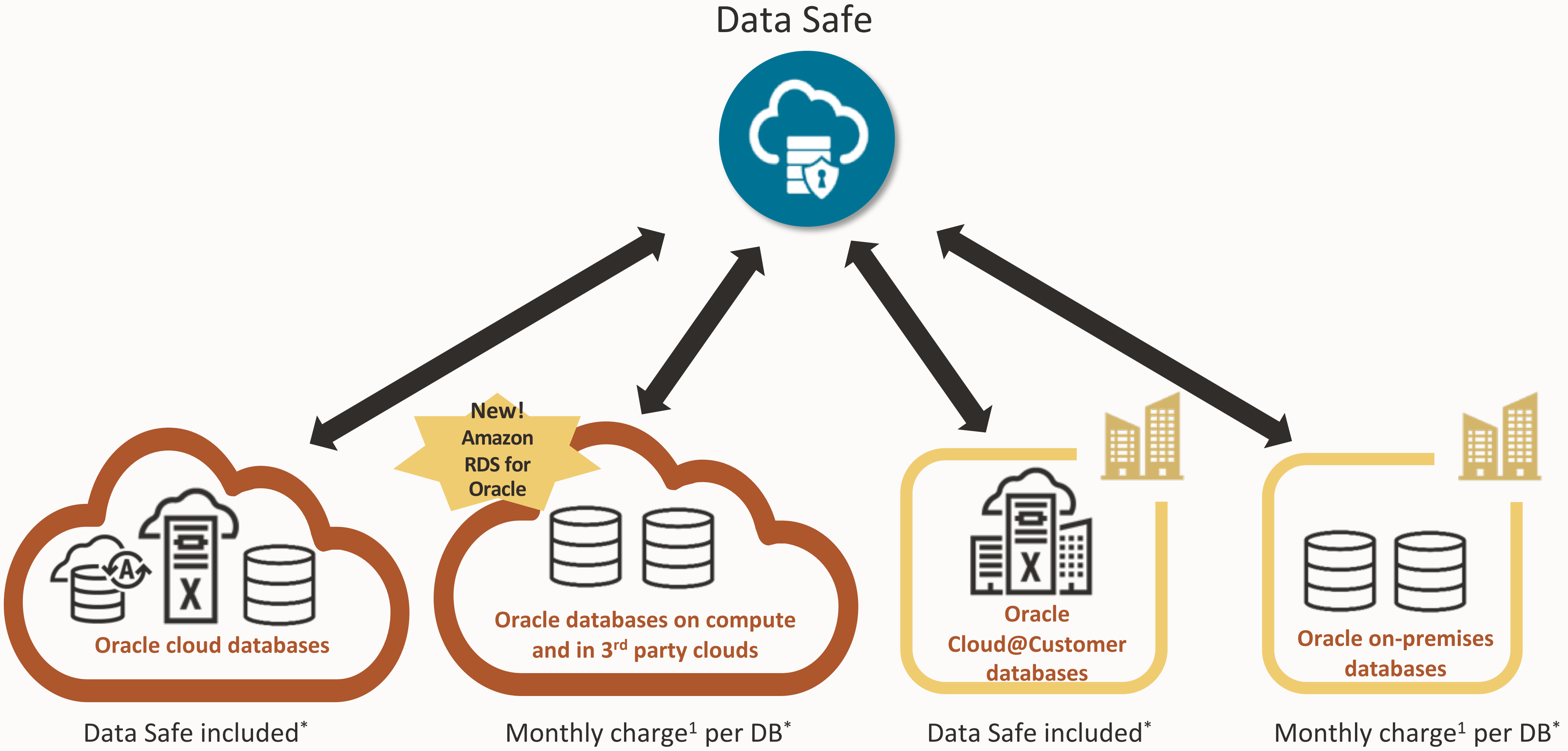
SQL Firewall*

Sensitive Data Discovery

Data Masking

**available for 23c target databases only*

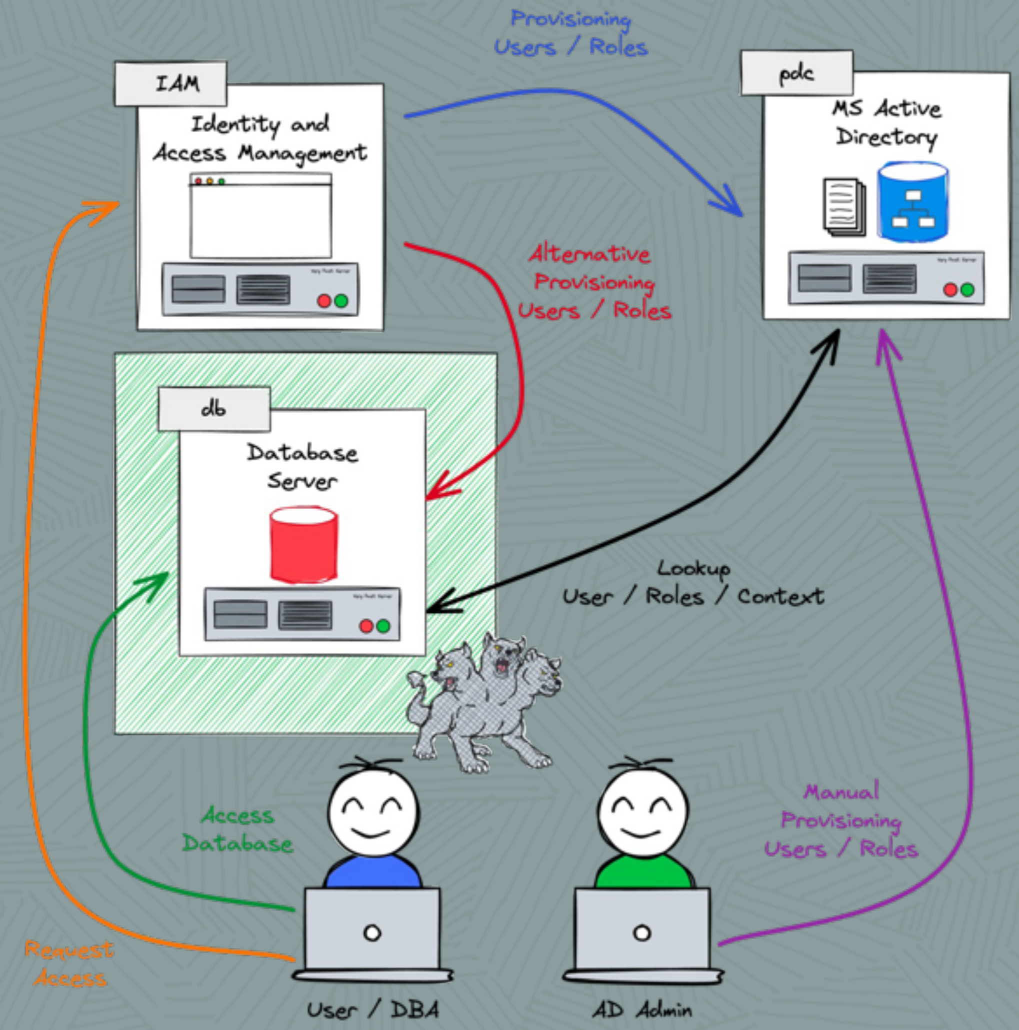
Data Safe is available for all your Oracle Databases


Data Safe
New! Amazon RDS for Oracle
Oracle cloud databases
Oracle databases on compute and in 3rd party clouds
Oracle Cloud@Customer databases
Oracle on-premises databases
Data Safe included*
Monthly charge¹ per DB*
Data Safe included*
Monthly charge¹ per DB*

*Includes 1M audit records per database per month; $0.10 per 10K records over the limit

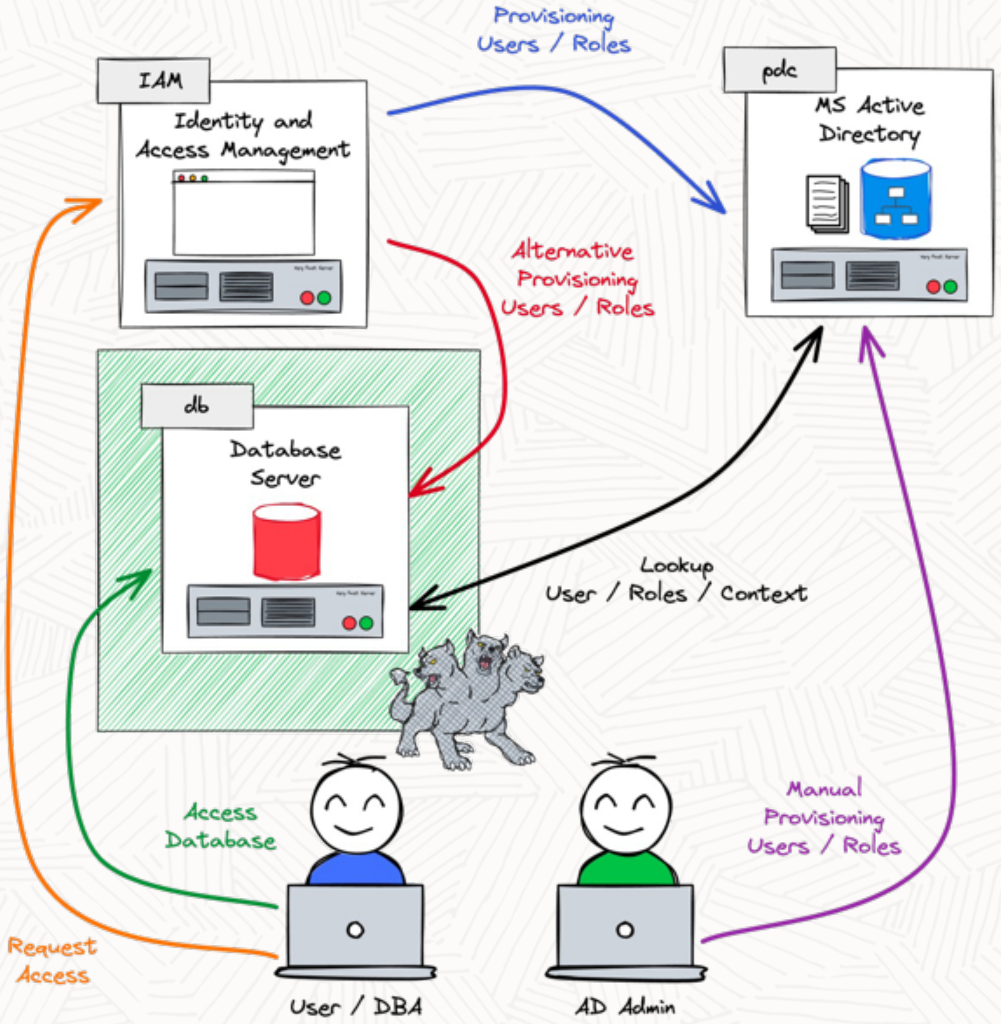
[1] tiered pricing applies (price list)

Oracle Centrally Managed Users (CMU)



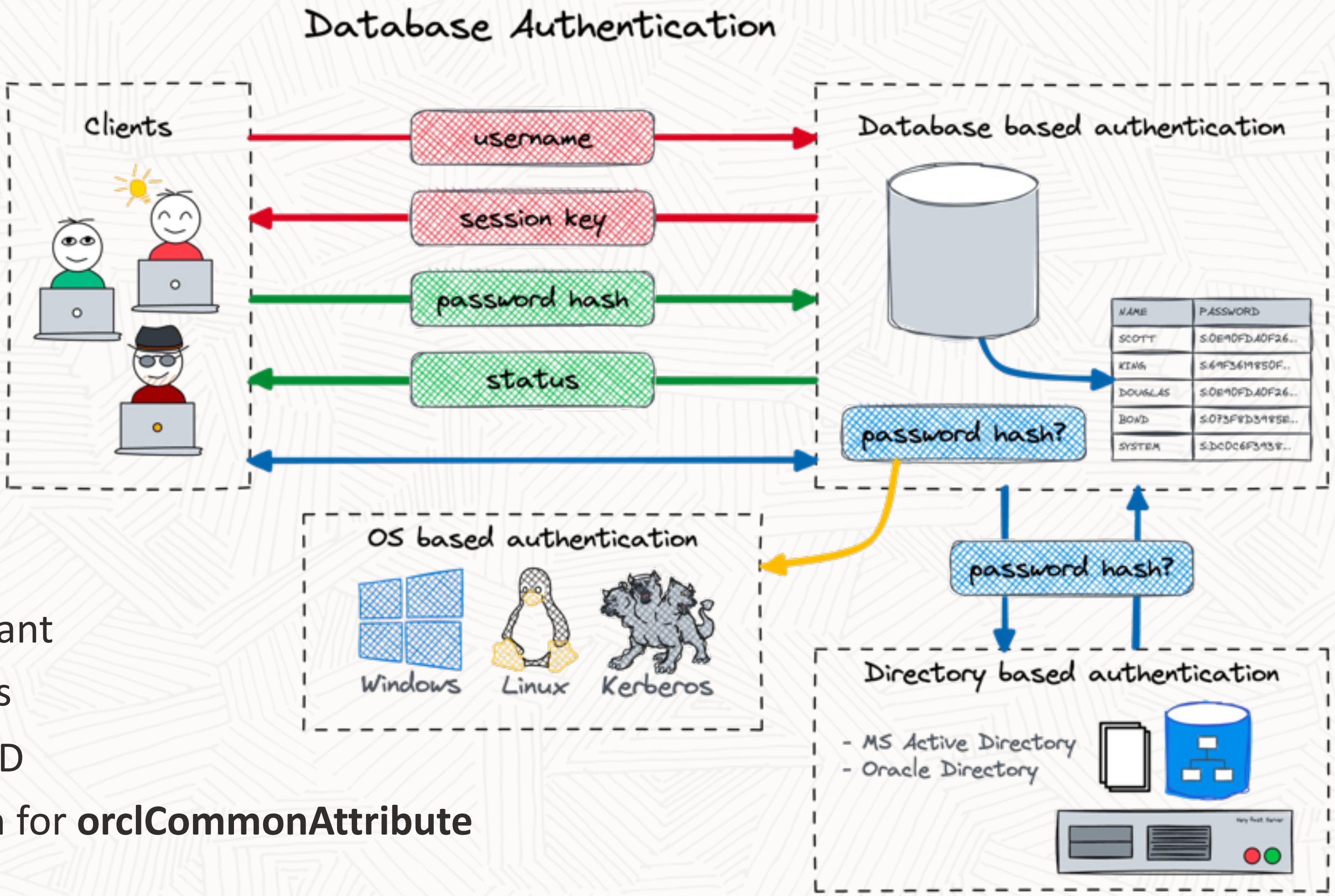
CMU in a Nutshell

- New security feature as of Oracle Database Release 18c
- **Centrally Managed User CMU…**
  - … does not require an additional Oracle directory
  - … enables the administration of users directly in MS AD
  - … does not require an additional license but
  - … Supported only by Oracle Enterprise or Free Edition ☺
  - … not supported in Oracle Standard Edition ☹
- Supports common authentication methods
  - **Password-** , **Kerberos-** und **PKI / SSL** authentication
- Requires a **password filter** and an AD schema extension
- Requires an AD service account
- Perfect for small and medium-sized businesses
  - Oracle EUS **deprecated** in 23c



Active Directory plug-in or not

- Authentication at Oracle is either...
  - ... external i.e. OS, Kerberos, SSL, etc.
  - ... password respectively hash based
- For password based authentication Oracle must have access to a password hash
  - **USER$** for database authentication
  - **userPassword** for LDAP EUS based
  - **orclCommonAttribute** for AD based
- Active Directory is not fully LDAP v3 compliant
  - It use its on method to store credentials
- CMU as well EUS requires a Plugin on MS AD
  - Filter DLL with an AD Schema extension for **orclCommonAttribute**



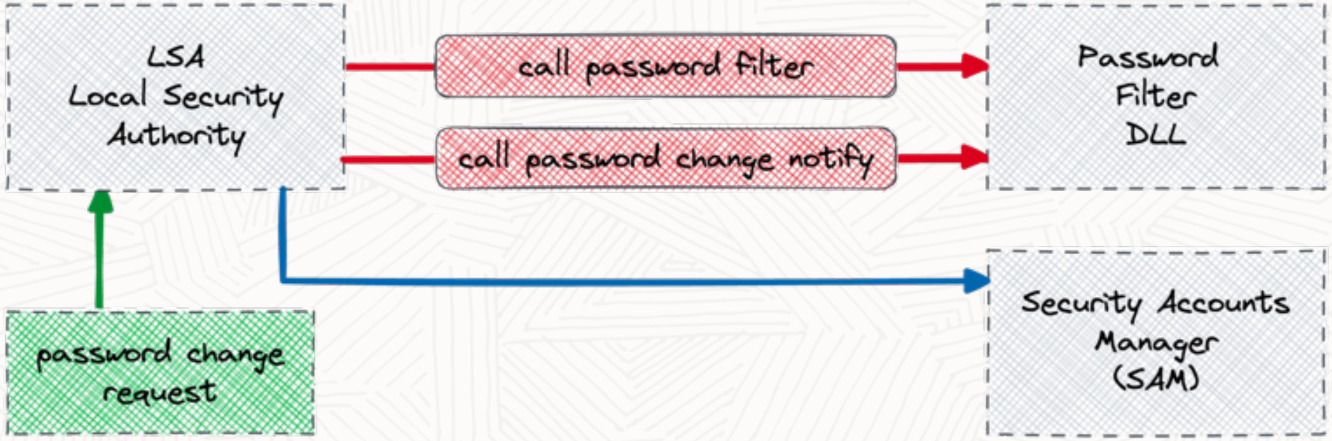
NAME	PASSWORD
SCOTT	S:0E90FDA0F26..
KING	S:69F3619850F..
DOUGLAS	S:0E90FDA0F26..
BOND	S:073F8D39858..
SYSTEM	S:DC0C6F3938..

Oracle Password Filter Plugin

A few insights into the Password Plugin…

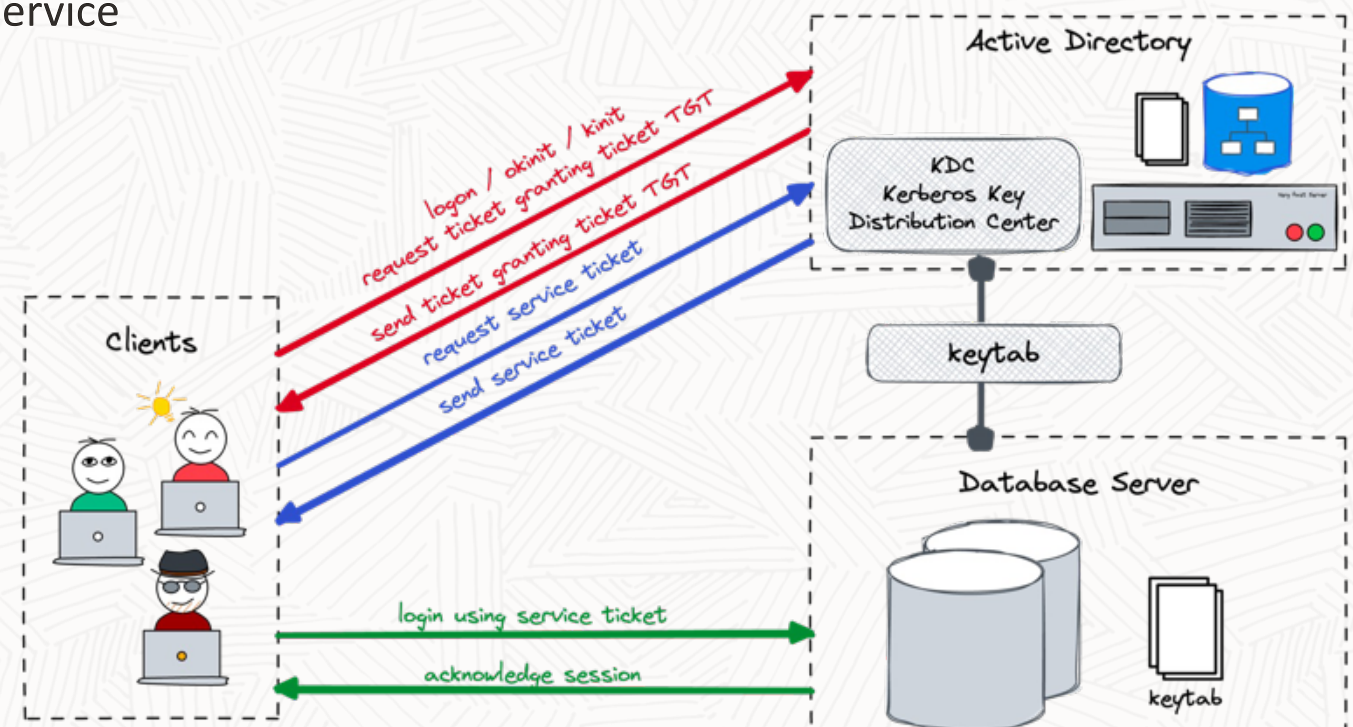
MAXIMUM FLEXIBILITY AND COMPATIBILITY ONLY WITH THE PLUGIN

- The AD Plugin is installed using opwdintg.exe
- The following changes are performed
  - Add default groups ORA_VFR_11G, ORA_VFR_12G, ORA_VFR_11G
  - Introduce AD schema extension
  - Install a filter DLL
- Latest Version is official signed and a valid LSA
- Downsides
  - Requires AD Reboot
  - Schema change **can not** be remove
- Standard Windows / AD Interface
  - Also used by other products



Alternative Kerberos Authentication

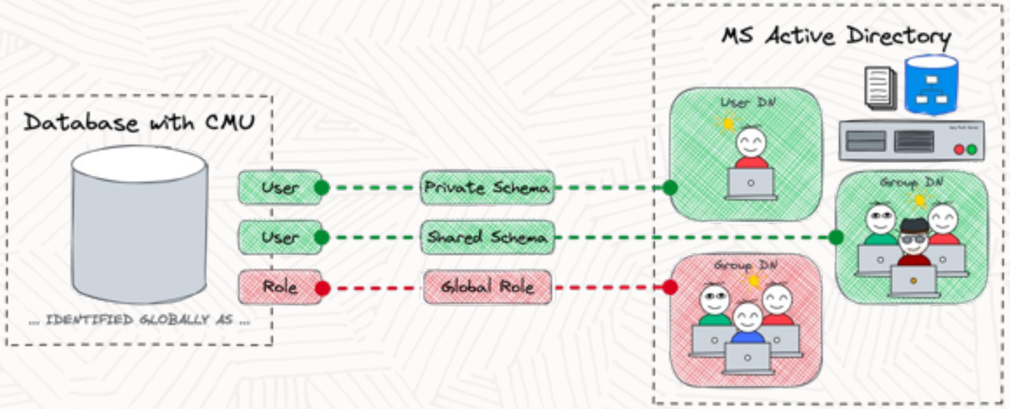
- Kerberos requires three parties
  - Key Distribution Center (KDC) providing the Authentication Service (AS) and Ticket Granting Service (TGS)
  - Service, Service Principle (SPN) providing a service
  - Client requesting access
- Other terms
  - Ticket Granting Ticket (TGT)
  - Key Table file keytab for short, stores long-term keys for one or more SPNs
  - Kerberos Credential Cache “ccache”, holds Kerberos credentials, during validity period
- Basis for a range of tools and services
- KDC is integrated with MS Active Directory



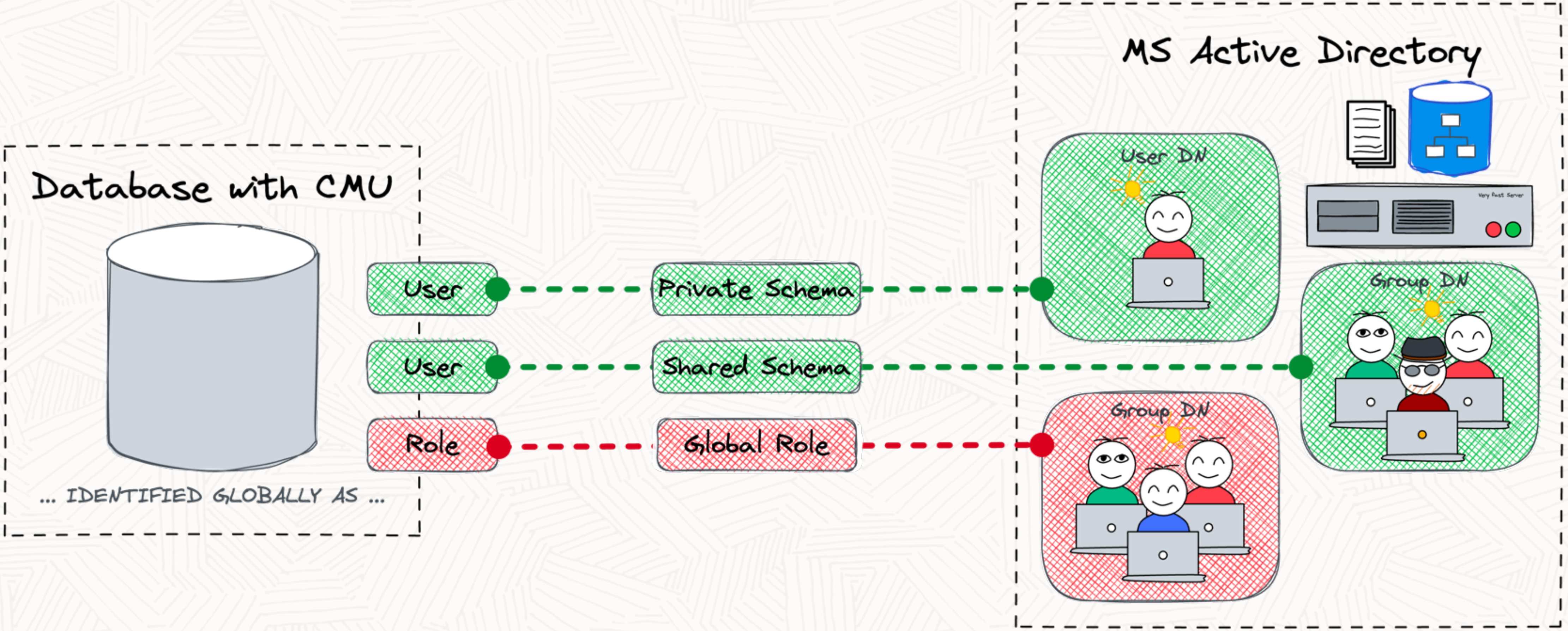
Shared or exclusive mapped Schemas

CMU, like EUS, offers two types of global user mapping

- **Shared Global Users** e.g. database user is mapped to directory group
  - Centralized management of user authorization in Active Directory
  - Reduce user management in the database
  - DB user “share” the same resources in the database
- **Private Global Users** e.g. database user is mapped to a directory user
  - Exclusive user / resource in the database
  - Users must still be created in the database
  - Recommended for users with own objects
- **Global Roles** to grant privileges to private or shared global users
  - Database global roles mapped to directory groups
  - give member users additional privilege

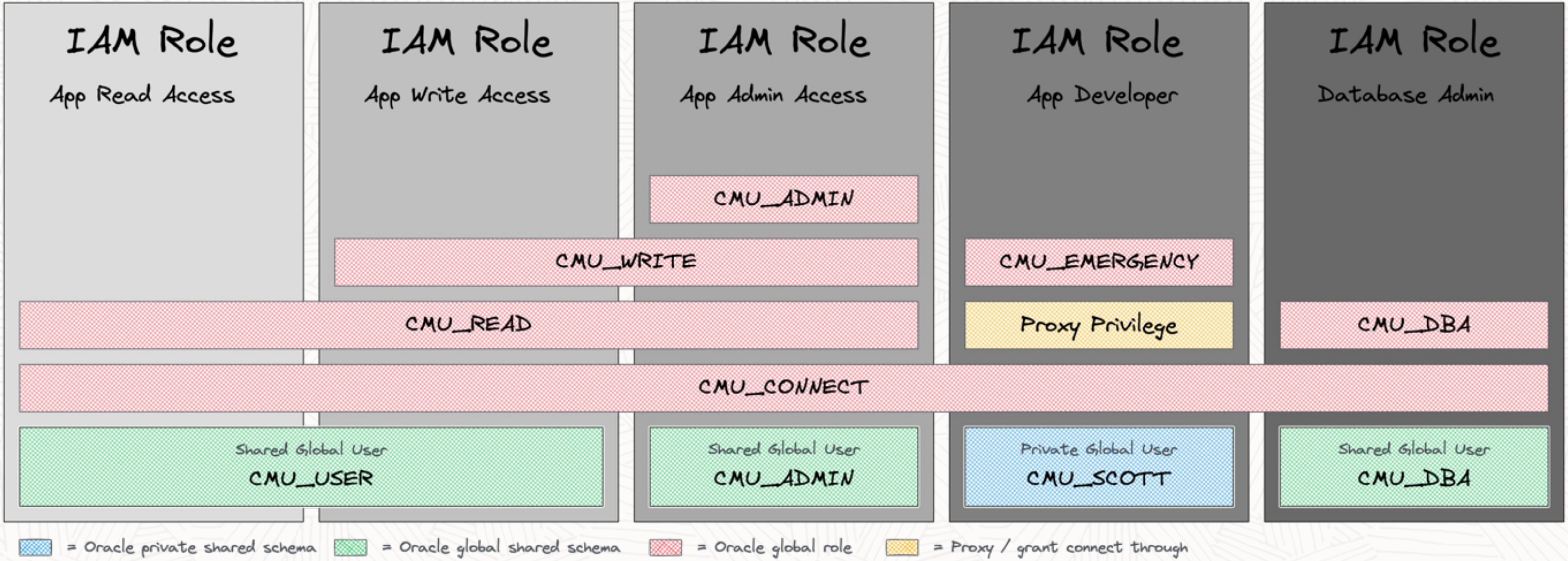


Shared or exclusive mapped Schemas



User and Role Concept

Simplified user Entitlement and Assignment



IAM Role — App Read Access

IAM Role — App Write Access

IAM Role — App Admin Access

IAM Role — App Developer

IAM Role — Database Admin

CMU_ADMIN

CMU_WRITE

CMU_EMERGENCY

CMU_READ

Proxy Privilege

CMU_DBA

CMU_CONNECT

Shared Global User CMU_USER

Shared Global User CMU_ADMIN

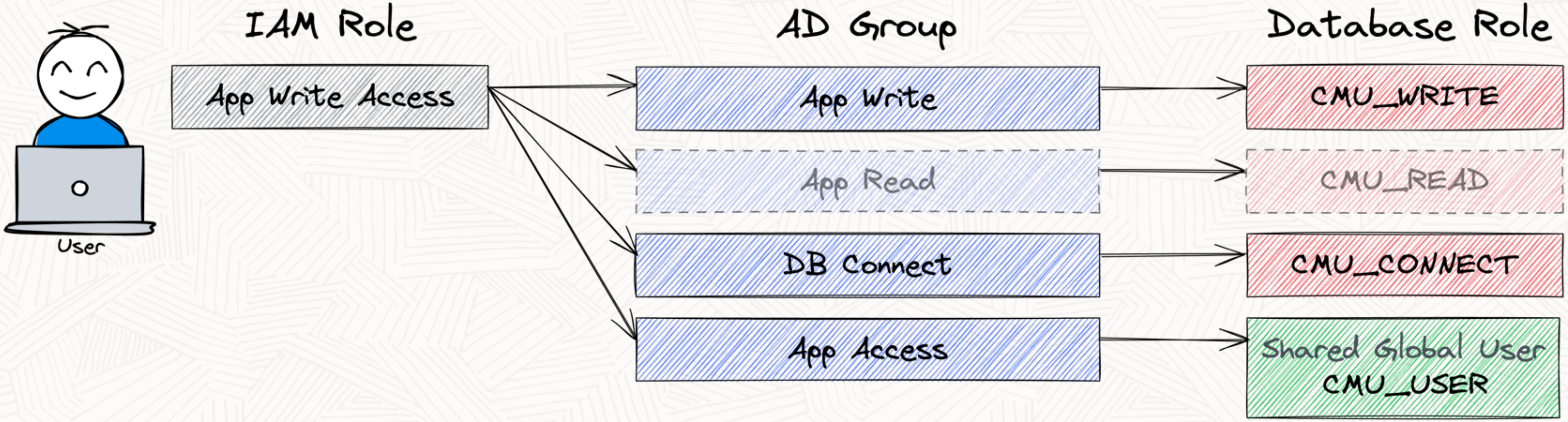
Private Global User CMU_SCOTT

Shared Global User CMU_DBA

🟦 = Oracle private shared schema 🟩 = Oracle global shared schema 🟥 = Oracle global role 🟨 = Proxy / grant connect through

User Entitlement and Mapping - WRITE

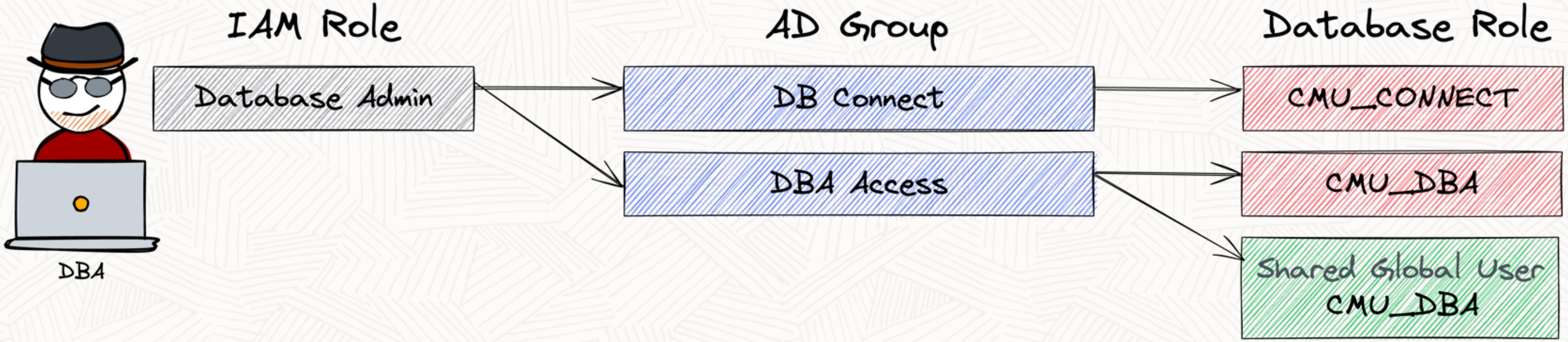
User with read write access



```
CREATE USER cmu_user IDENTIFIED GLOBALLY AS 'cn=Application Users,ou=groups,dc=trivadislabs,dc=com';
CREATE ROLE cmu_connect IDENTIFIED GLOBALLY AS 'cn=DB Access,ou= groups,dc=trivadislabs,dc=com';
CREATE ROLE cmu_write IDENTIFIED GLOBALLY AS 'cn=Application Write,ou= groups,dc=trivadislabs,dc=com';
GRANT cmu_read TO cmu_write;
```

User Entitlement and Mapping - DBA

User with DBA access



```
CREATE USER cmu_dba IDENTIFIED GLOBALLY AS 'cn=Database Admins,ou=groups,dc=trivadislabs,dc=com';
CREATE ROLE cmu_connect IDENTIFIED GLOBALLY AS 'cn=DB Access,ou= groups,dc=trivadislabs,dc=com';
CREATE ROLE cmu_dba IDENTIFIED GLOBALLY AS 'cn=Database Admins,ou=groups,dc=trivadislabs,dc=com';
GRANT sysdba TO cmu_dba;
```

User Entitlement and Mapping - Consideration

Create new roles or alter existing roles?

- Create a corresponding **user and role concept** (or adapt an existing)
- Use whenever possible **global shared schemas** rather than **private global schemas**
  - Reduce manual work on the database e.g. to create exclusive mappings
- Global shared schema has to be an AD group
  - e.g. ObjectClass GroupOfUniqueNames rather than OrganisationalUnit
  - Oracle EUS it is OrganisationalUnit
- Make sure user is only member of one group
- Grant privileges via global roles rather with direct grants

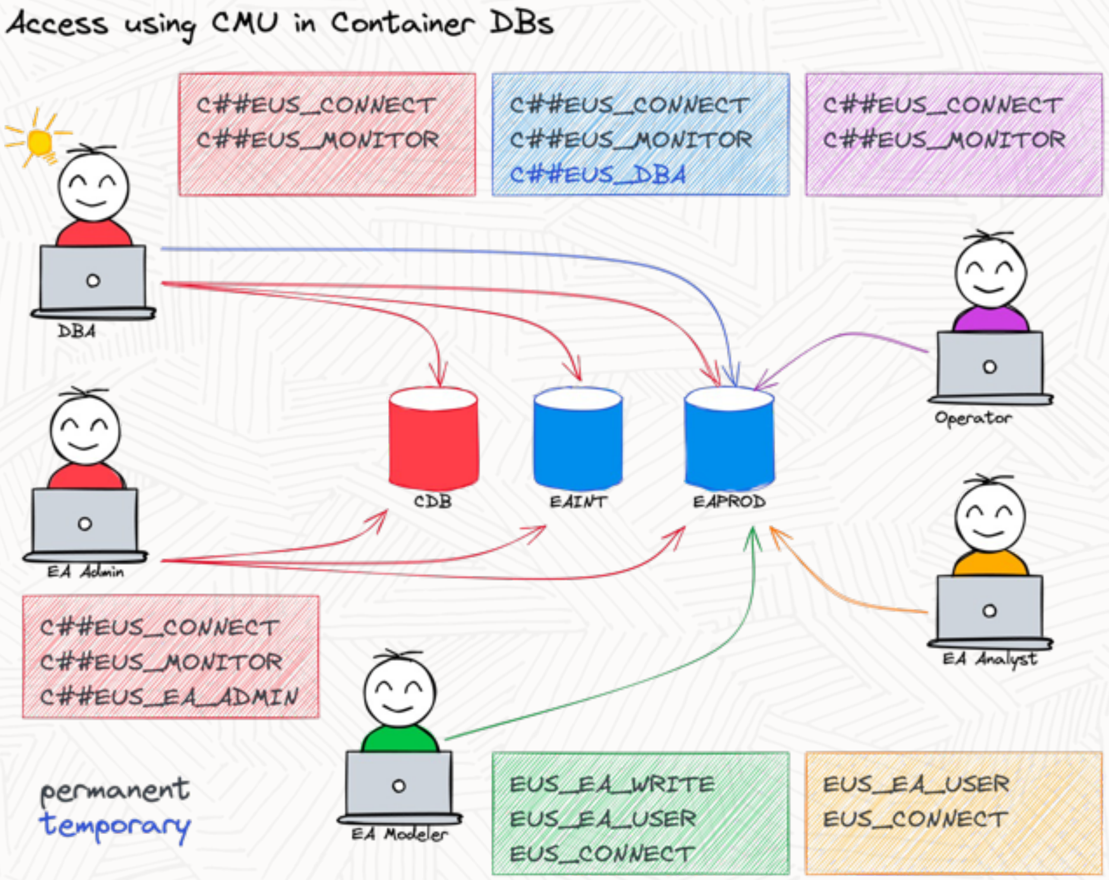
```
GRANT app_write TO cmu_write;
```

Oracle Multitenant

How to handle central Authentication / Authorisation in container databases?

- CMU also works analogously for container DBs
- Can be configured on CDB Level and/or PDB level
- Global shared users can be local or common
  - Common global shared schemas allows access across all PDB
  - Local global shared schemas only allows local access

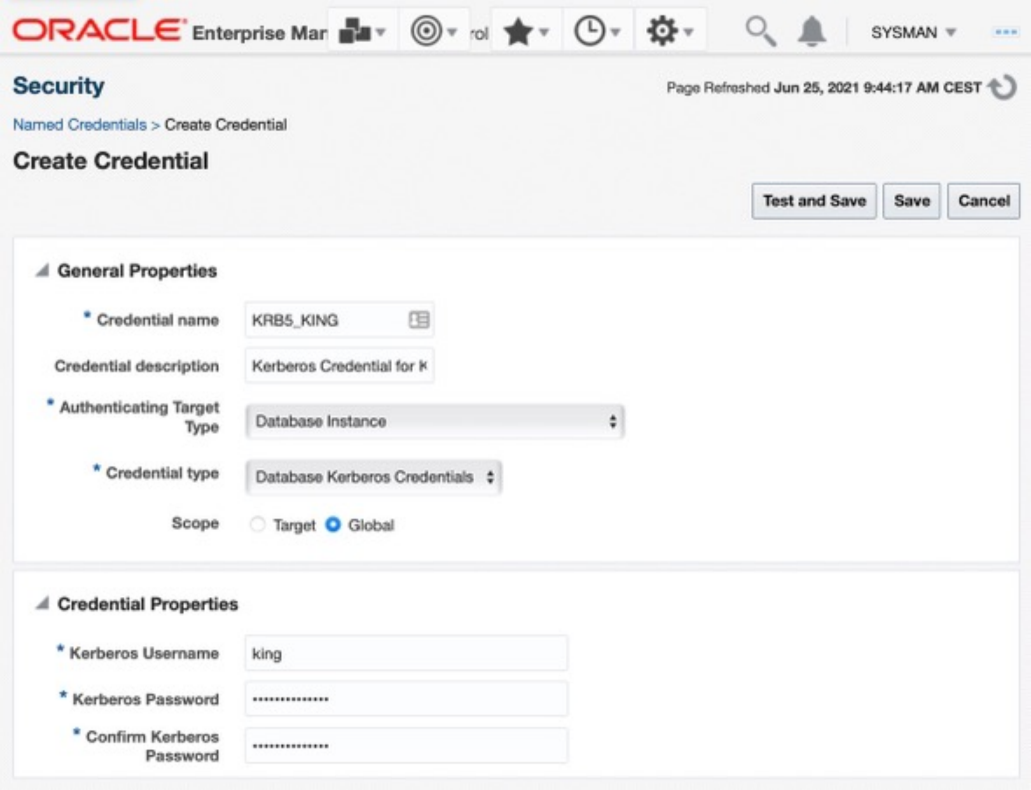
Comprehensive user and role concept gets even more important



Oracle Enterprise Manager Cloud Control

What to consider when using Oracle CMU with OEM?

- CMU works **transparently** in OEM
- **No special** configuration if **password** authentication is in use
- **Kerberos** authentication requires further action
  - Use of Global Named Credential for Database Kerberos
  - OEM requires a krb5.conf file either in
  - default location /etc/krb5.conf
  - TNS_ADMIN folder configured in OEM
  - Security folder of JDK



Security

Page Refreshed Jun 25, 2021 9:44:17 AM CEST

Named Credentials > Create Credential

Create Credential

General Properties

* Credential name	KRB5_KING
Credential description	Kerberos Credential for K
* Authenticating Target Type	Database Instance
* Credential type	Database Kerberos Credentials
Scope	○ Target ● Global

Credential Properties

* Kerberos Username	king
* Kerberos Password	•••••••••••••••
* Confirm Kerberos Password	•••••••••••••••

The ORA-28306 Problem

Multiple user Mapping…

- A user could be in several groups mapped to different shared global schemas
- Default behaviour is a successful login to any of these schemas (recent Oracle releases)
- Old behaviour respectively by setting the parameter *_ldap_warning_on_multi_shared_mappings*

```
SQL> conn fleming/LAB42-Schulung
ERROR:
ORA-28306: The directory user has 2 groups mapped to different database global users.
Connected.
```

Solution

- Keep your AD groups clean e.g. User may only be member in one group used for mapping
- Use exclusive schema mapping
- Keep your user/role concept agile so that the error is not an issue

CMU Projects and Implementations

Swiss financial service provider

- Integration with IaM solution e.g. provisioning to AD
- Kerberos based authentication
- Mainly power user and DBA’s

Insurance company in Switzerland

- Replacement of Oracle Enterprise User Security
- SSL based authentication

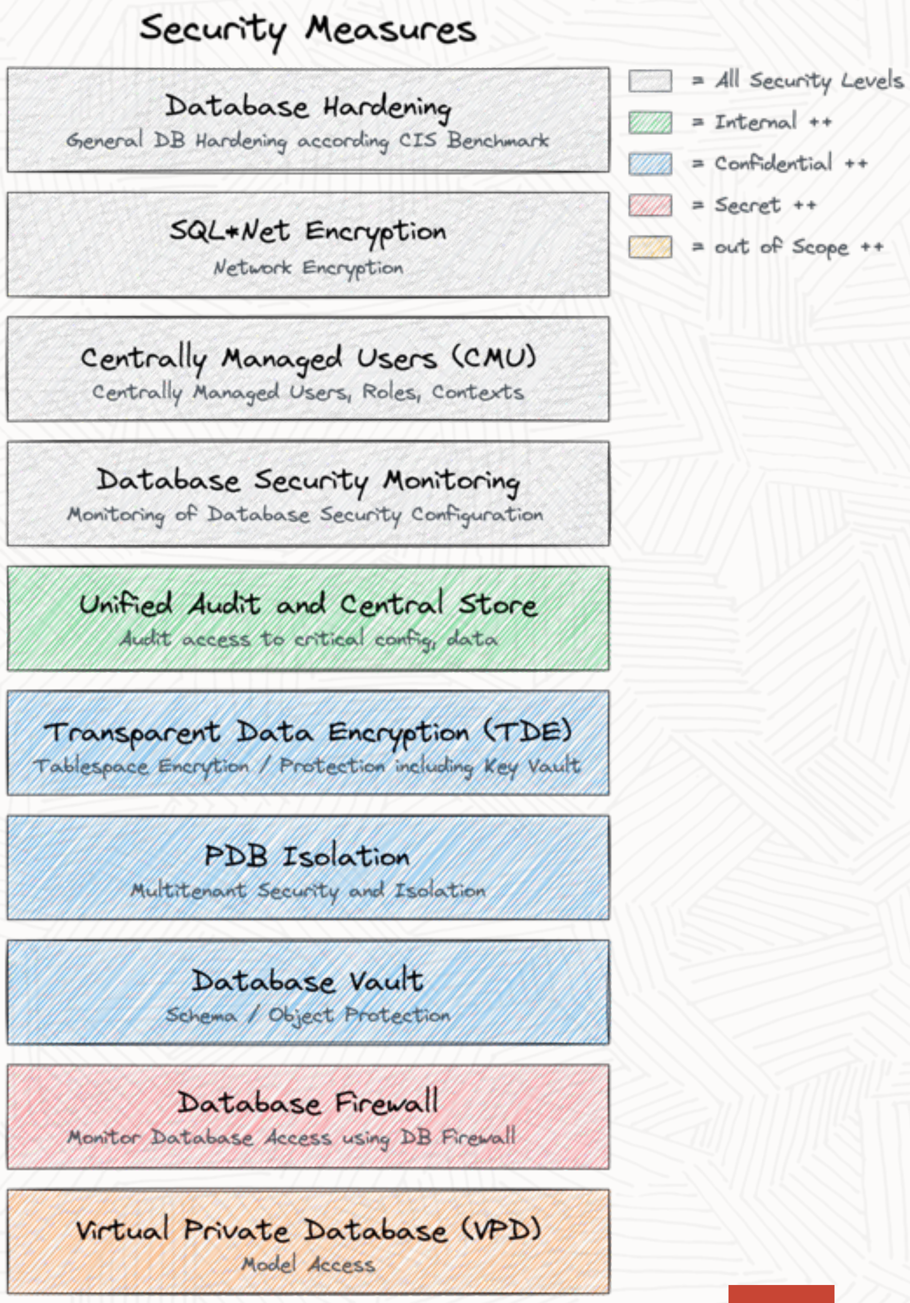
Large German Bank

- Kerberos based authentication

Swiss National Bank

- Kerberos based authentication

Several small and medium-sized enterprises



Security Measures

Database Hardening
General DB Hardening according CIS Benchmark

SQL*Net Encryption
Network Encryption

Centrally Managed Users (CMU)
Centrally Managed Users, Roles, Contexts

Database Security Monitoring
Monitoring of Database Security Configuration

Unified Audit and Central Store
Audit access to critical config, data

Transparent Data Encryption (TDE)
Tablespace Encrytion / Protection including Key Vault

PDB Isolation
Multitenant Security and Isolation

Database Vault
Schema / Object Protection

Database Firewall
Monitor Database Access using DB Firewall

Virtual Private Database (VPD)
Model Access

⬜ = All Security Levels
🟩 = Internal ++
🟦 = Confidential ++
🟥 = Secret ++
🟨 = out of Scope ++

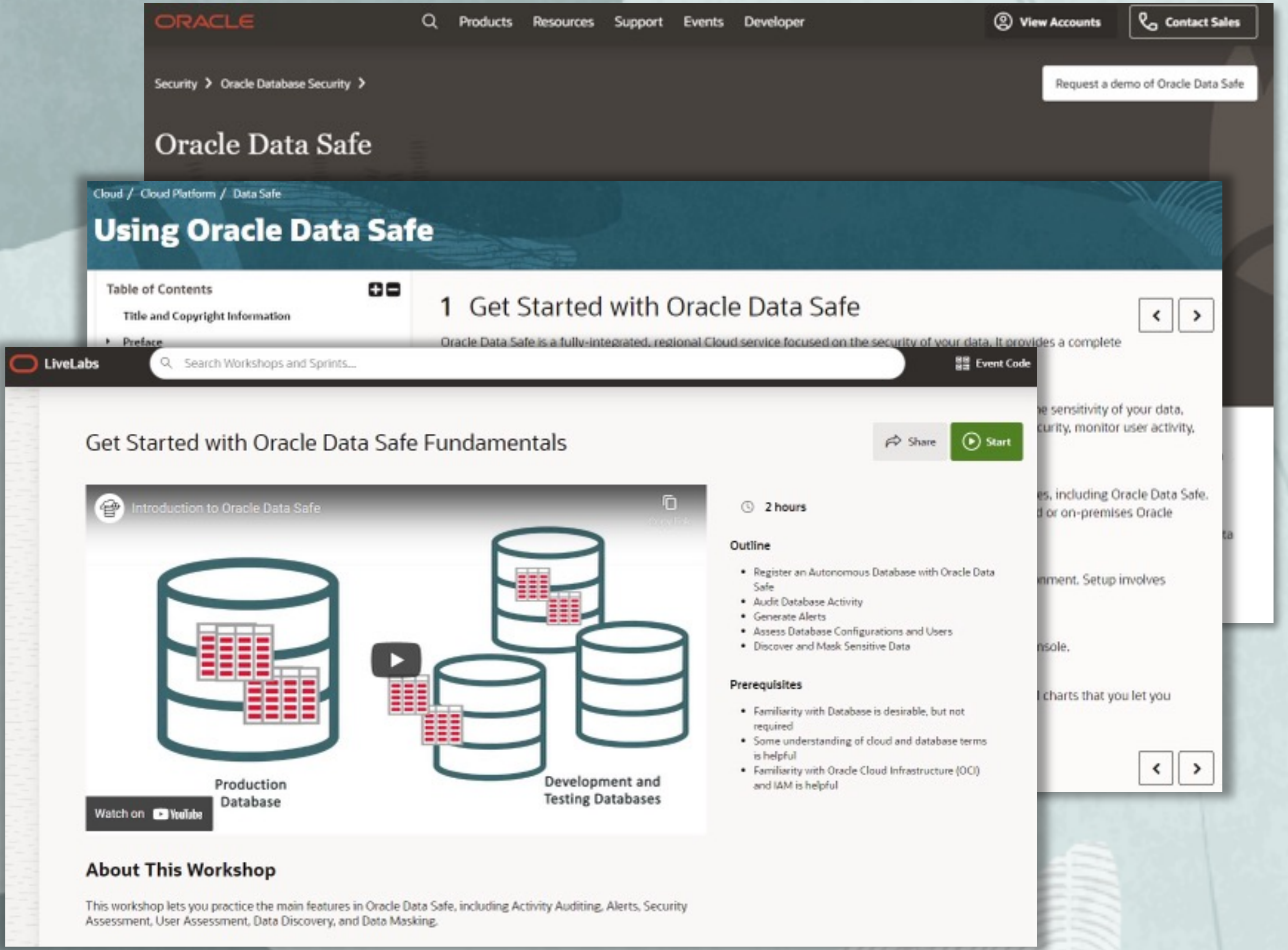
More Information

Visit Oracle LiveLabs at https://bit.ly/golivelabs

and search for "Data Safe"

[Oracle Data Safe Homepage]()

[Oracle Data Safe Documentation]()


ORACLE
Products
Resources
Support
Events
Developer
View Accounts
Contact Sales
Security > Oracle Database Security >
Request a demo of Oracle Data Safe
Cloud / Cloud Platform / Data Safe
Table of Contents
Title and Copyright Information
Preface
LiveLabs
Search Workshops and Sprints...
Event Code
Share
Start
Introduction to Oracle Data Safe
Production Database
Development and Testing Databases
Watch on YouTube

Oracle Data Safe

Using Oracle Data Safe

1 Get Started with Oracle Data Safe

Oracle Data Safe is a fully-integrated, regional Cloud service focused on the security of your data. It provides a complete

e sensitivity of your data, curity, monitor user activity,

es, including Oracle Data Safe. d or on-premises Oracle

nment. Setup involves

nsole.

charts that you let you

Get Started with Oracle Data Safe Fundamentals

2 hours

Outline

- Register an Autonomous Database with Oracle Data Safe
- Audit Database Activity
- Generate Alerts
- Assess Database Configurations and Users
- Discover and Mask Sensitive Data

Prerequisites

- Familiarity with Database is desirable, but not required
- Some understanding of cloud and database terms is helpful
- Familiarity with Oracle Cloud Infrastructure (OCI) and IAM is helpful

About This Workshop

This workshop lets you practice the main features in Oracle Data Safe, including Activity Auditing, Alerts, Security Assessment, User Assessment, Data Discovery, and Data Masking.

Thank you

Bettina Schäumer & Stefan Oehrli

ORACLE

Our mission is to help people see data in new ways, discover insights, unlock endless possibilities.