Oracle Centrally Managed Users (CMU)

Real-World Lessons Learned

August 2023
Stefan Oehrli

Stefan Oehrli – Data Platforms

Oracle ACE
Pro

stefan.oehrli@accenture.com

Tech Architecture Manager

- Since 1997 active in various IT areas
- More than 25 years of experience in Oracle databases
- Focus: Protecting data and operating databases securely
  - Security assessments and reviews
  - Database security concepts and their implementation
  - Oracle Backup & Recovery concepts and troubleshooting
  - Oracle Enterprise User and Advanced Security, DB Vault, …
  - Oracle Directory Services
- Co-author of the book The Oracle DBA (Hanser, 2016/07)

oradba.ch

@stefanoehrli

Terraform
ASSOCIATE
HashiCorp
CERTIFIED

mirko HOTZY
andrea HELD
marek ADAR
christian ANTOGNINI
ronny EGNER
markus FLECHTNER
angelika GALLNITZ
stefan OEHRLI
daniel STEIGER

2. Auflage

DER
ORACLE
DBA

Handbuch für die Administration
der Oracle Database 12c

EXTRA: E-Book inside

Im Internet: sqlplus-Kommandos, Datentypen, v$ Views u.v.m.

HANSER

DATA PLATFORMS

WHY? We are the game changer for our client's data platform projects

HOW? Maximum automation, maximum efficiency, maximum quality!

WHAT? We build innovative data platforms based on our blueprints, assets and tools.

3 key benefits

1 Architecture expertise from hands-on projects

2 Delivery of tailor-made data platforms

3 Integrated Teams - Like a Rowing team, perfect alignment and interaction.

Tools and Blueprints

Key enabler for the implementation of modern data platforms at a high speed and quality.

Continuous Optimization

Tools and Blueprints are continuously optimized to the customer and project’s needs.

Expertise

Expert group for modern data platforms from technical implementation to project management and organization

Oracle CMU

What needs to be considered besides the configuration of Oracle CMU?

1 Introduction

2 CMU in a Nutshell

3 Authentication

4 Conceptual Considerations

5 Good Practice

6 Special Use Cases

7 Troubleshooting

8 Conclusion

1

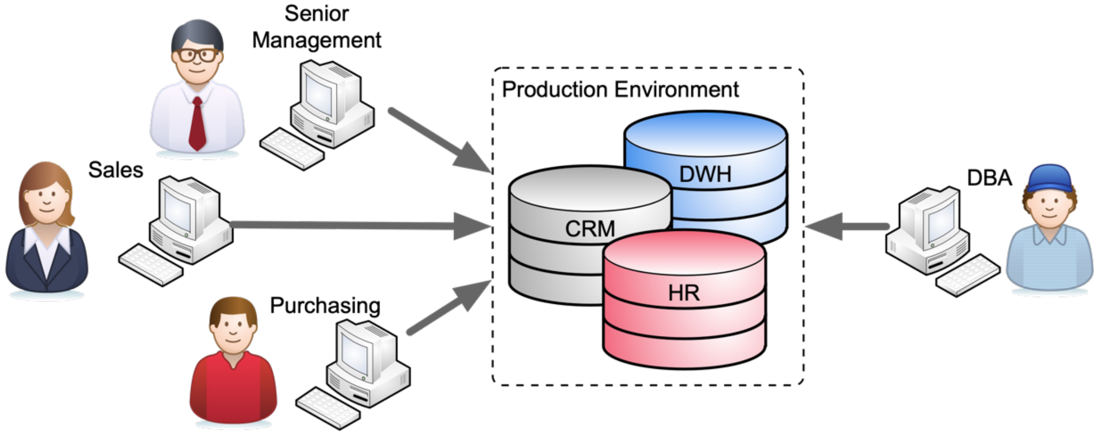
Introduction

Why is Oracle CMU needed at all?

The challenge 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
- How are permissions managed?
  - Individual / decentralized by administrators
  - What happens with mutations (function changes, terminations, etc.)?
- Is there a role concept?
  - Will it also be implemented?
- Redundancies
- Integration with Oracle Feature



Projects

Where was or is Oracle CMU being implemented?

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

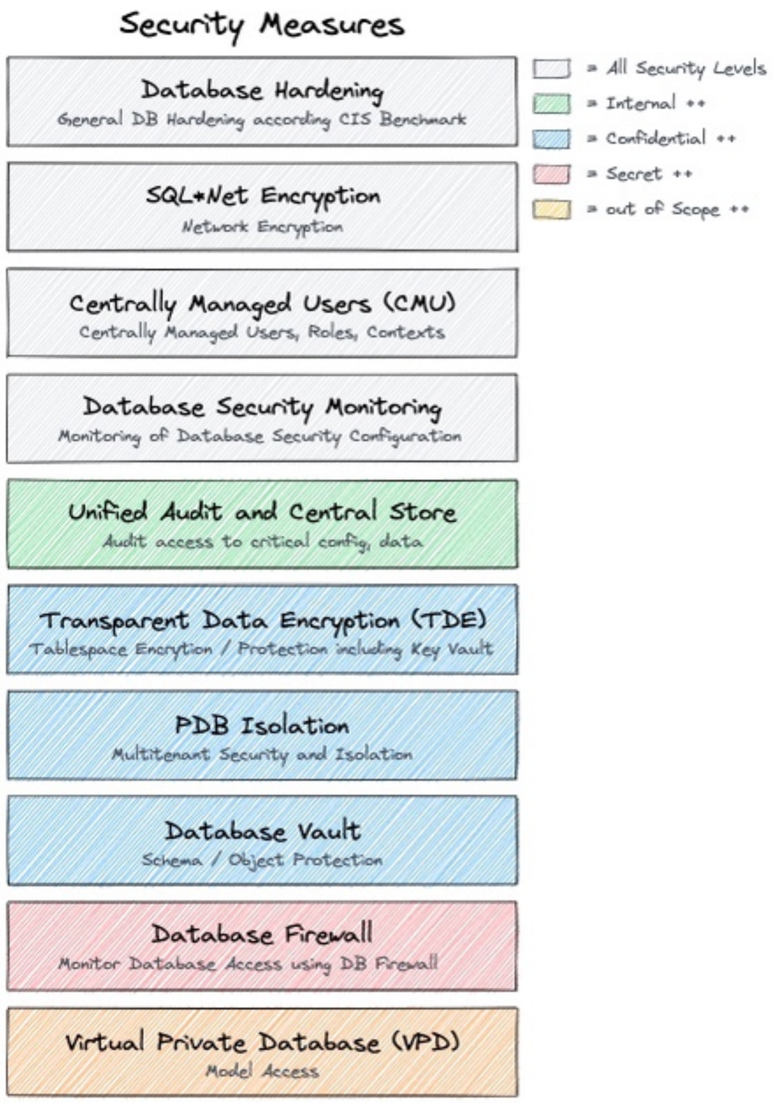
Large German Bank

- 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 ++

2

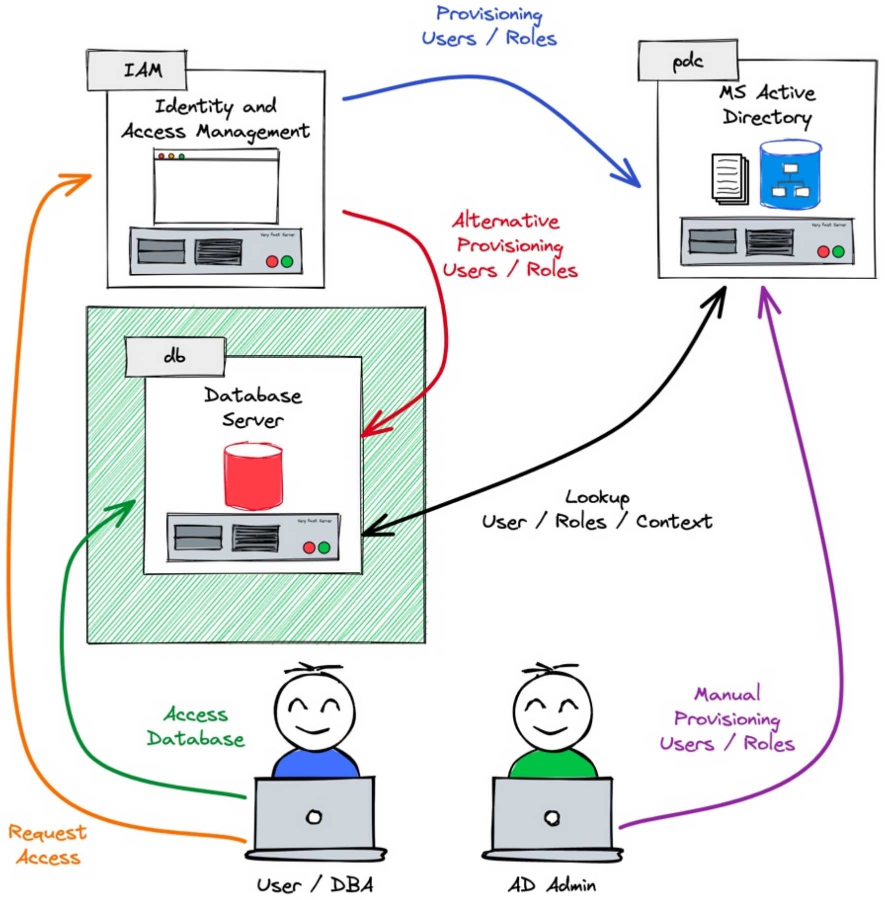
CMU in a Nutshell

Architecture, Structure and Functionality of CMU

Oracle CMU in a Nutshell

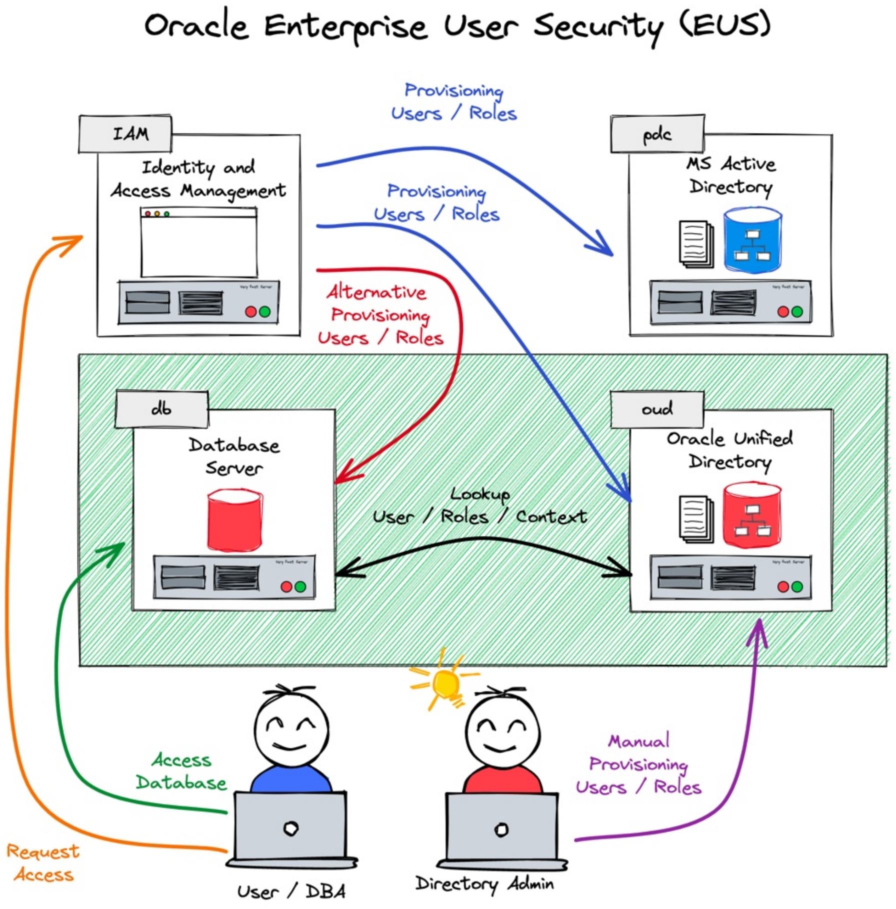
Easy Integration into Active Directory

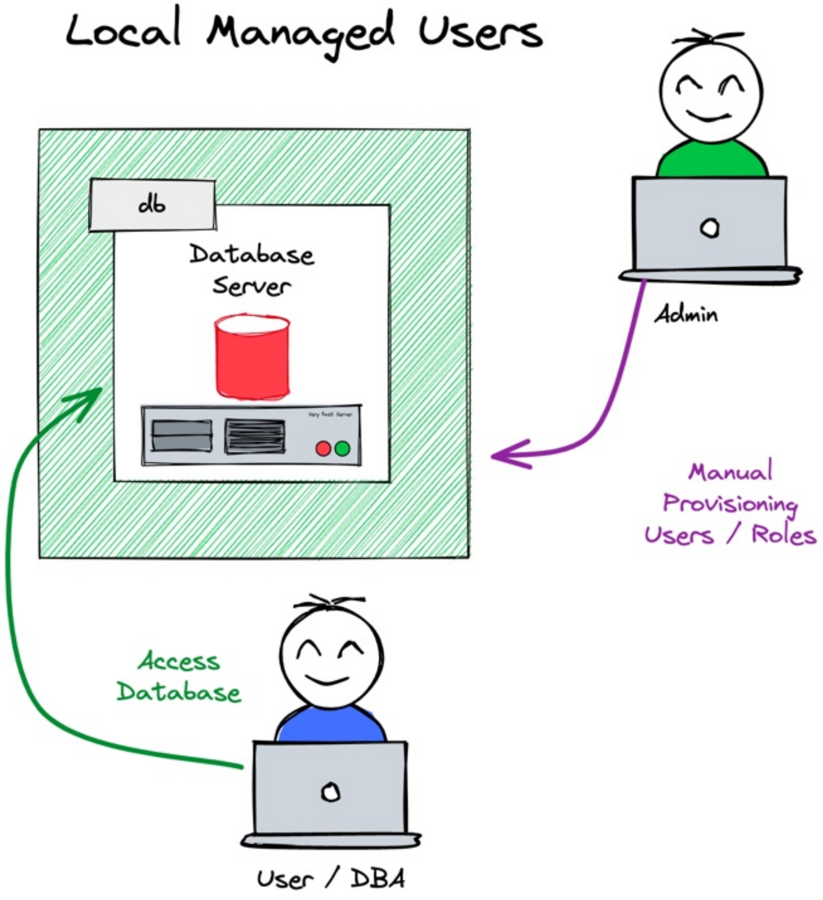
- New security feature as of Oracle Database Release 18c
- Centrally Managed User CMU…
  - … does not require an additional Oracle directory
  - … enables the administration of users directly in MS AD
  - … does not require an additional license but
  - … Supported only by Oracle Enterprise or Express 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



Alternatives?

What options are there besides CMU?


Oracle Enterprise User Security (EUS)
IAM
Identity and Access Management
Provisioning Users / Roles
Provisioning Users / Roles
pdc
MS Active Directory
Alternative Provisioning Users / Roles
db
Database Server
oud
Oracle Unified Directory
Lookup User / Roles / Context
Access Database
Request Access
User / DBA
Directory Admin
Manual Provisioning Users / Roles



3

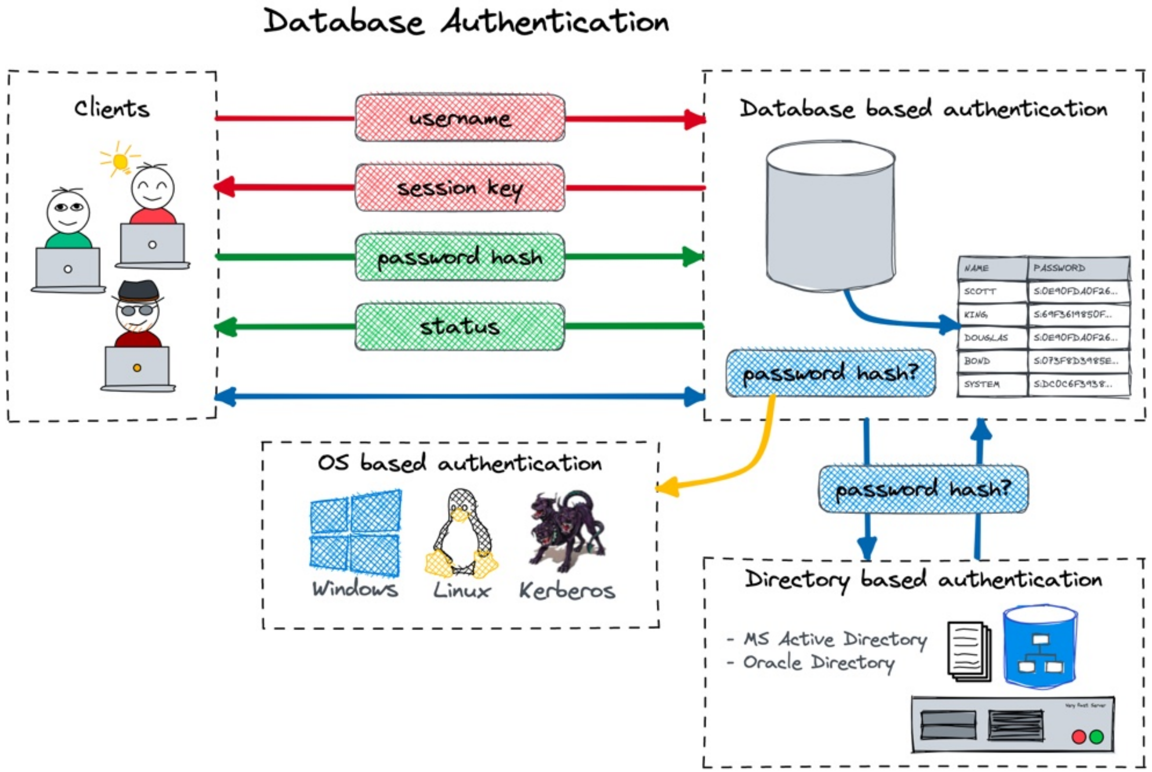
Authentication

Which Authentication Method to Choose?

Active Directory plug-in or not

Why do we need a plug-in?

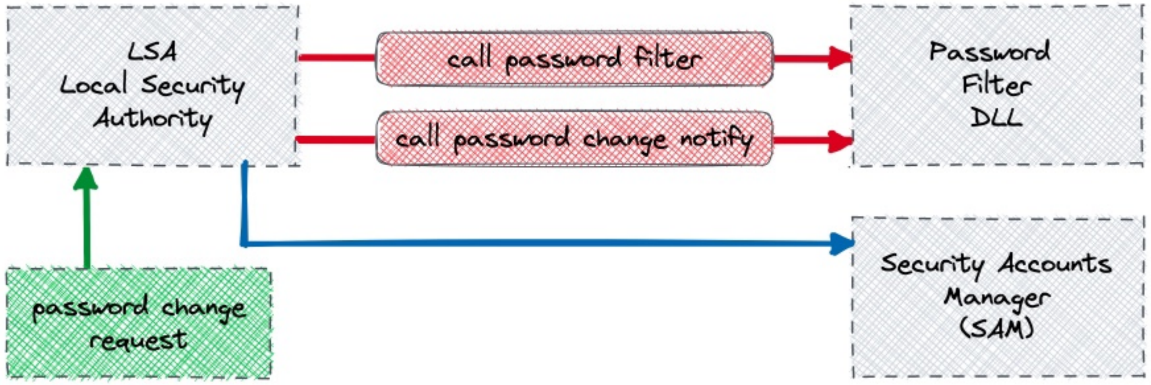
- Authentication at Oracle is either…
  - … external i.e. OS, Kerberos, SSL, etc.
  - … password respectively hash based
- For password based authentication Oracle must have access to a password hash
  - **USER$** for database authentication
  - **userPassword** for LDAP EUS based
  - **orclCommonAttribute** 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:073F8D3985E…
SYSTEM	S:DC0C6F3938…

Oracle Password Filter Plugin

A few insights into the Password Plugin…



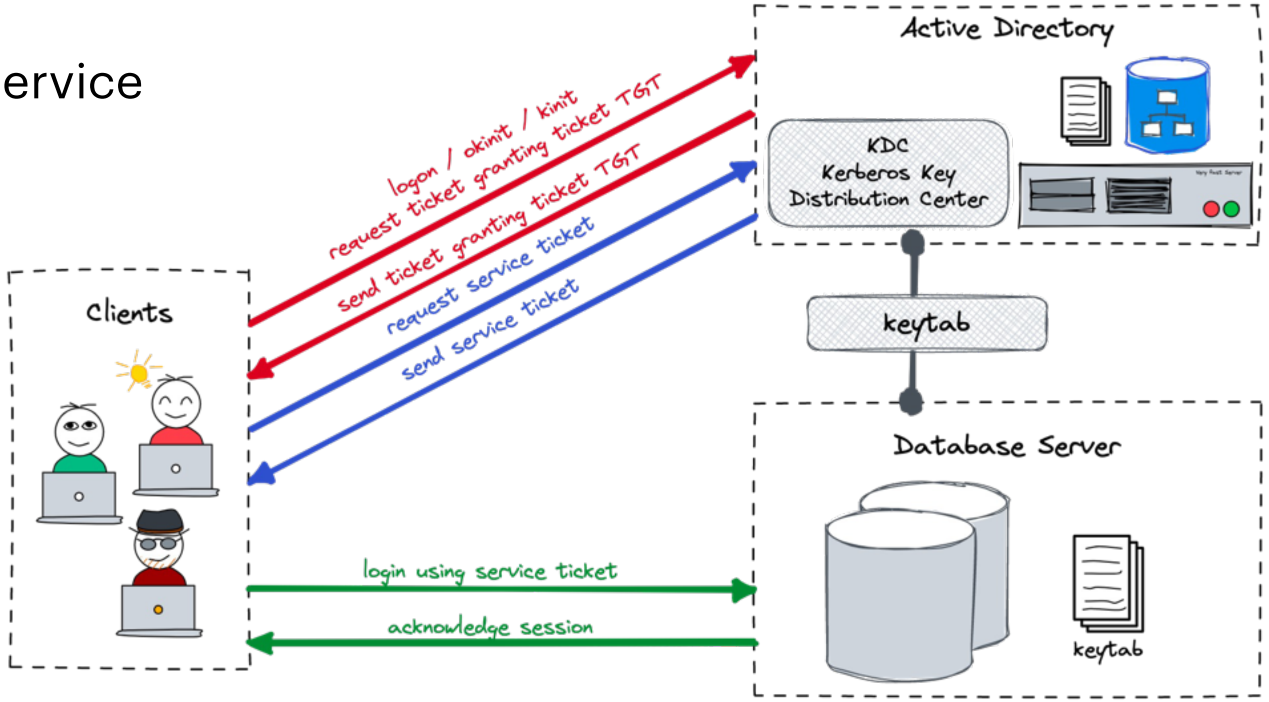
MAXIMUM FLEXIBILITY AND COMPATIBILITY ONLY WITH THE PLUGIN

- The AD Plugin is installed using *opwdintg.exe*
- The following changes are performed
  - Install a filter DLL
  - Introduce AD schema extension
  - Add default groups ORA_VFR_11G, ORA_VFR_12G, ORA_VFR_11G
- 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

Oracle “**strong**” respectively network 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



4

Conceptual Considerations

What to consider when introducing CMU

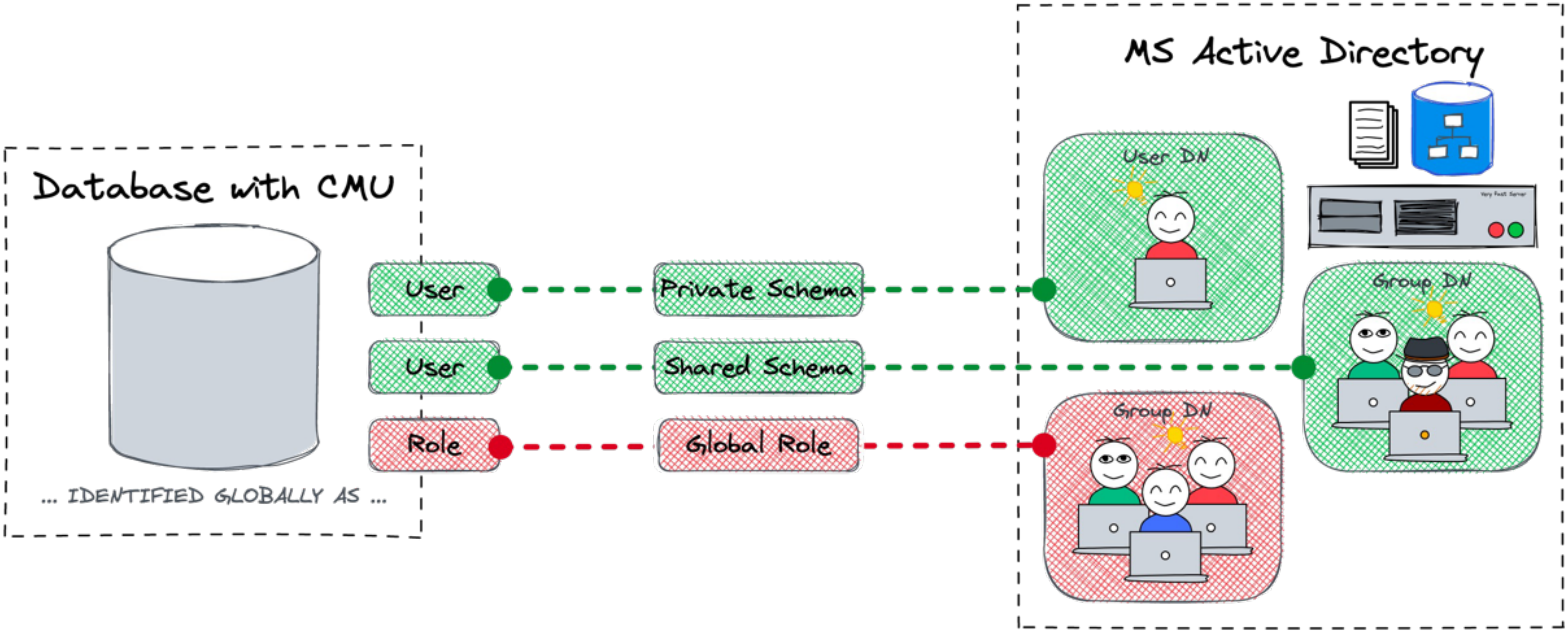
Shared or exclusive mapped Schemas

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

Simple sketch of the Shared / Private Schemas



Proxy User with Oracle CMU

- Early version of Oracle CMU used to have issues with proxy connect
- As of now proxy permissions or GRANT CONNECT TRHOUGH does work

```
SQL> ALTER USER scott GRANT CONNECT THROUGH cmu_user;

User altered.
```

- But do we want to allow GRANT CONNECT TRHOUGH for all global shared users?
- Same problem applies to administrative rights such as SYSDBA

```
SQL> GRANT sysdba TO cmu_users;

Grant succeeded.
```

- **Solution:** Either map user to *exclusive schemas* or create *dedicated schemas* for these users

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

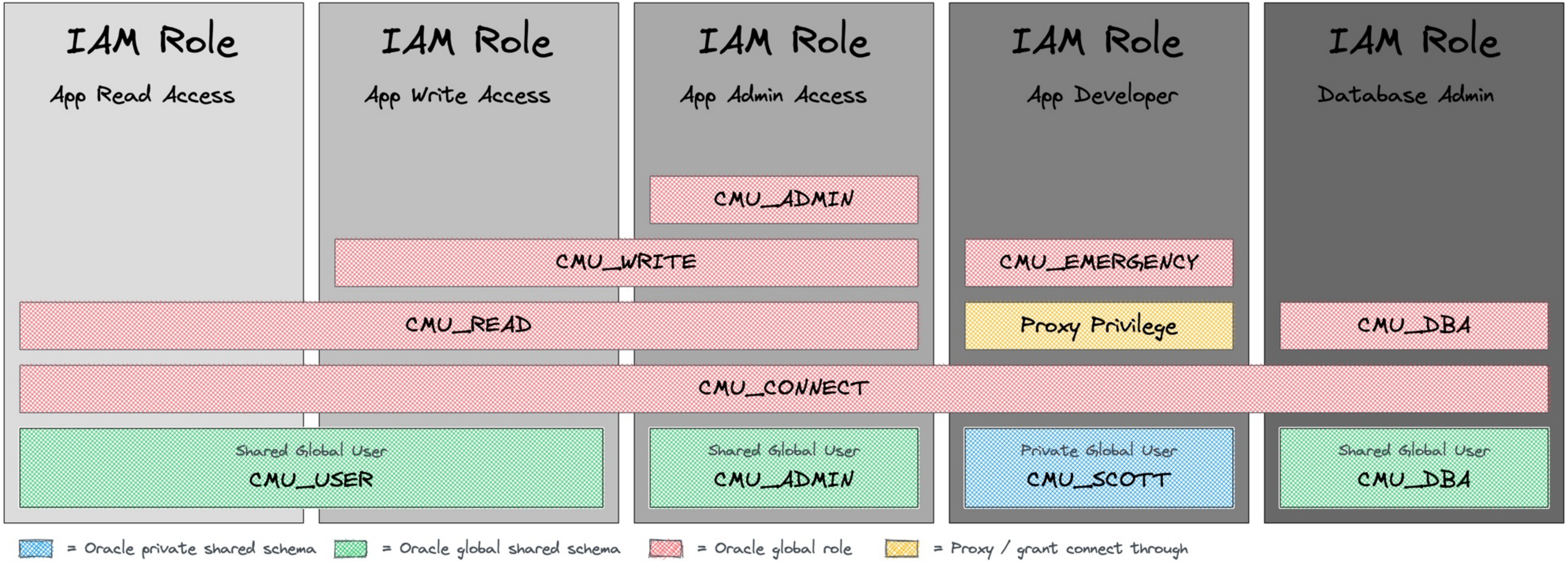
```
SQL> conn fleming/LAB42-Schulung
ERROR:
ORA-28306: The directory user has 2 groups mapped to different database global users.
Connected.
```

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

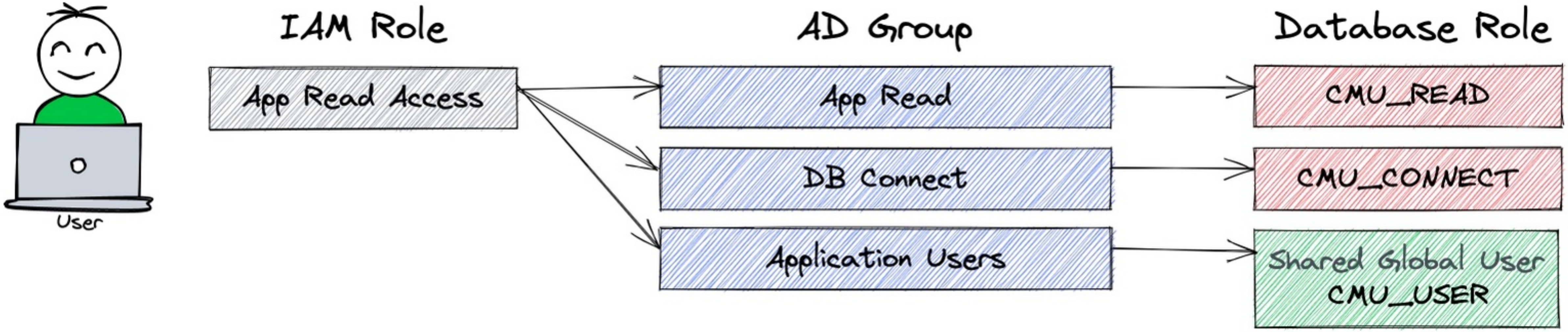
User and Role Concept

Simplified user Entitlement and Assignment



User Entitlement and Mapping - READ

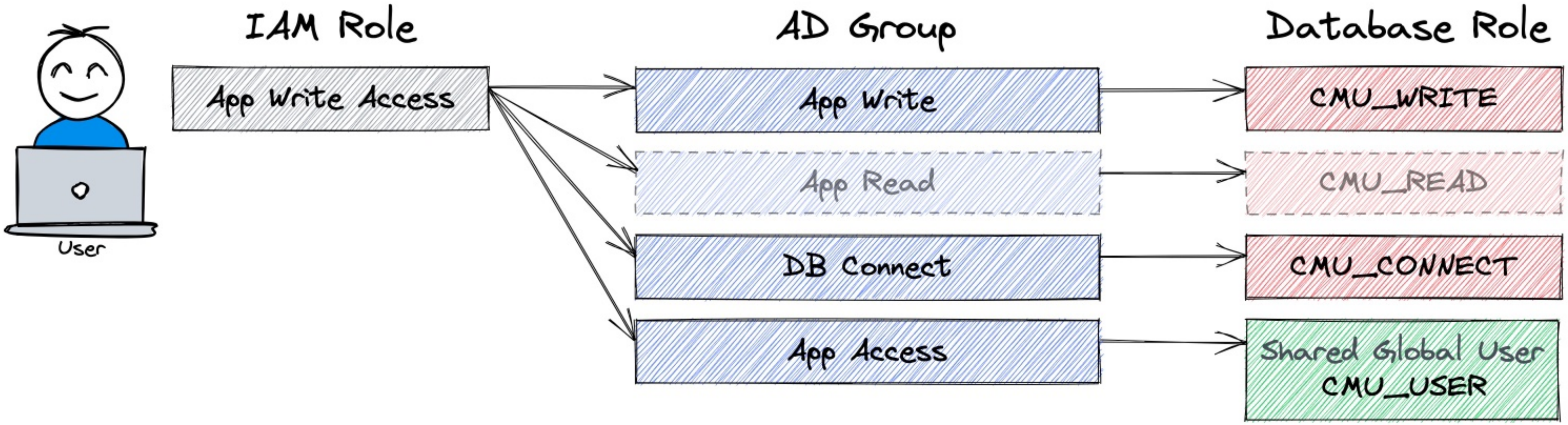
User with read only access



```
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_read IDENTIFIED GLOBALLY AS 'cn=Application Read,ou= groups,dc=trivadislabs,dc=com';
```

User Entitlement and Mapping - Write

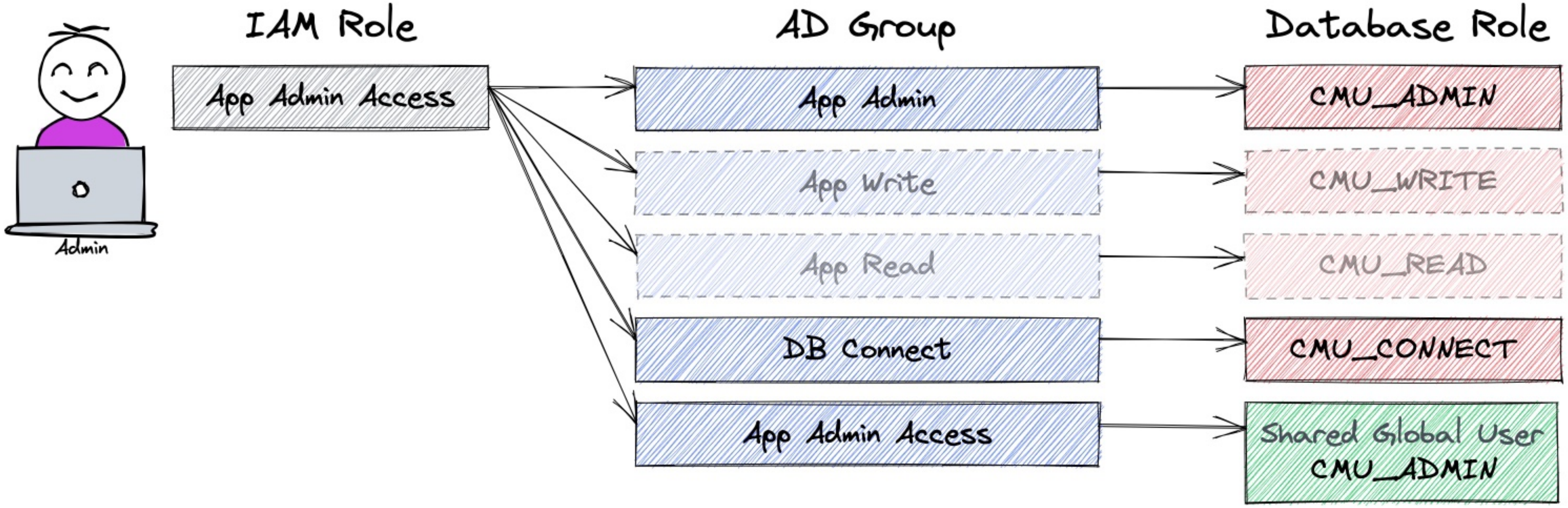
User with read write access



```
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 - Admin

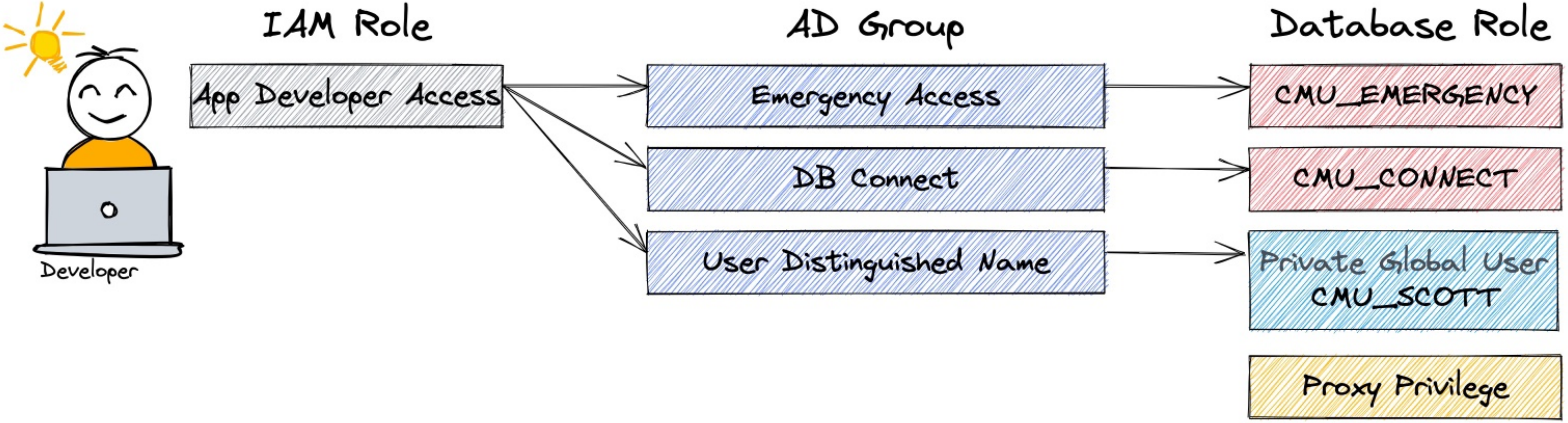
User with admin access



```
CREATE USER cmu_admin IDENTIFIED GLOBALLY AS 'cn=Application 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_admin IDENTIFIED GLOBALLY AS 'cn= Application Admins,ou= groups,dc=trivadislabs,dc=com';
GRANT cmu_read TO cmu_write;
GRANT cmu_write TO cmu_admin;
```

User Entitlement and Mapping - Developer

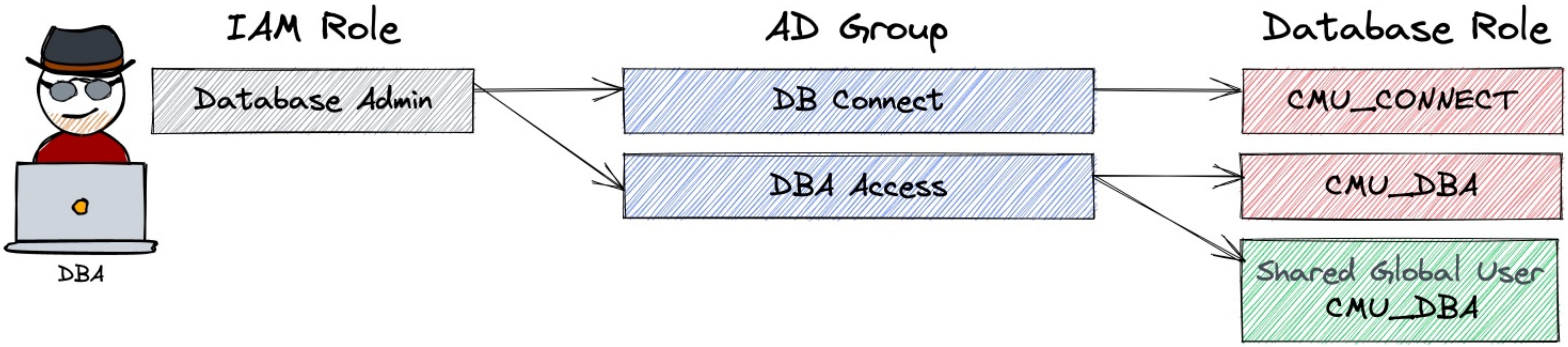
User with development access



```
CREATE USER cmu_scott IDENTIFIED GLOBALLY AS 'cn=Scott,ou=peoples,dc=trivadislabs,dc=com';
CREATE ROLE cmu_connect IDENTIFIED GLOBALLY AS 'cn=DB Access,ou= groups,dc=trivadislabs,dc=com';
CREATE ROLE cmu_emergency IDENTIFIED GLOBALLY AS
    'cn=Application Emergency,ou= groups,dc=trivadislabs,dc=com’;
ALTER USER app_schema GRANT CONNECT THROUGH cmu_scott;
```

User Entitlement and Mapping - DBA

User with DBA access



IAM Role

AD Group

Database Role

Database Admin

DB Connect

DBA Access

CMU_CONNECT

CMU_DBA

Shared Global User CMU_DBA

DBA

```
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;
```

5

Good Practice

Tips on how to avoid common mistakes

Configuration via DB Property

How to configure CMU?

- Configuration is done for early versions of 18c / 19c via *sqlnet.ora* and *dsi.ora*
  - *sqlnet.ora* is used to specify the WALLET_LOCATION
  - *dsi.ora* or *ldap.ora* is used to specify the Active Directory
- Newer version allows the configuration via **directory object** and database property **CMU_WALLET**
  - Functionality requires patch 31404487 up to and including *19.9.0.0*
- **CMU_WALLET** allows the configuration on a per PDB level
  - Database property can be set on the PDB
- The **directory object** must point to a folder containing the following files:
  - *dsi.ora* used to specify the Active Directory
  - *Oracle Wallet* with the Active Directory service credentials i.e. username, password, distinguished name and AD root certificate

Configuration via DB Property– Example

Simple example of configuring CMU with DB properties…

- *dsi.ora* configuration file

```
DSI_DIRECTORY_SERVERS = (ad.trivadislabs.com::636)
DSI_DEFAULT_ADMIN_CONTEXT = "dc=trivadislabs,dc=com"
DSI_DIRECTORY_SERVER_TYPE = AD
```

- Create the CMU wallet using *orapki*

```
orapki wallet create -wallet $TNS_ADMIN/cmu -pwd <WALLET PASSWORD> -auto_login
```

- Add the CMU user credentials to the wallet

```
mkstore -wrl . -createEntry ORACLE.SECURITY.USERNAME cmuread
mkstore -wrl . -createEntry ORACLE.SECURITY.DN CN=cmuread,CN=Users,DC=trivadislabs,DC=com
mkstore -wrl . -createEntry ORACLE.SECURITY.PASSWORD <CMU PASSWORD>
```

- Add the root certificate to the wallet

```
orapki wallet add -wallet . -pwd <WALLET PASSWORD> -trusted_cert -cert $TNS_ADMIN/cmu/root.crt
```

Configuration via DB Property– Example

Simple example of configuring CMU with DB properties…

- Create the directory object for the CMU configuration

```
CREATE OR REPLACE DIRECTORY cmu_conf_dir AS '/u01/app/oracle/network/admin/cmu';
```

- Set the database property CMU_WALLET

```
ALTER DATABASE PROPERTY SET cmu_wallet='CMU_CONF_DIR';
```

- Set additional parameter for password based LDAP authentication

```
ALTER SYSTEM SET ldap_directory_access='PASSWORD';
ALTER SYSTEM SET ldap_directory_sysauth ='YES' scope=spfile;
```

- Start to create global users and roles

```
CREATE USER cmu_users IDENTIFIED GLOBALLY AS 'cn=Trivadis LAB Users,ou=Groups,dc=trivadislabs,dc=com';
CREATE ROLE cmu_connect IDENTIFIED GLOBALLY AS 'cn=Trivadis LAB Users,ou=Groups,dc=trivadislabs,dc=com';
```

Hidden Parameter

Is there anything else that can be configured?

- A couple of hidden parameter available to control CMU / LDAP behavior

```
Parameter                                Instance Description
---------------------------------------- -------- ------------------------------------------------------
_ldap_adaptive_to_no_nested_group_search TRUE     LDAP adaptive to no nested group search
_ldap_config_force_sync_up               FALSE    LDAP configure force sync up
_ldap_config_ssl_for_sasl_md5            TRUE     LDAP configure SSL for SASL-DIGEST-MD5
_ldap_no_nested_group_search             FALSE    LDAP no nested group search
_ldap_password_oneway_auth               FALSE    Use oneway auth for password based LDAP directory bind
_ldap_reset_user_account_flc             TRUE     LDAP reset user account lockout counter
_ldap_use_all_direct_groups_only         TRUE     LDAP use all direct groups only
_ldap_warning_on_multi_shared_mappings   TRUE     LDAP warning on multiple shared mappings
ldap_directory_access                    PASSWORD RDBMS's LDAP access option
ldap_directory_sysauth                   YES      OID usage parameter
```

- Interesting in connection with CMU **_ldap_no_nested_group_search, _ldap_use_all_direct_groups_only, _ldap_warning_on_multi_shared_mappings**
- But use them wisely. May have impact on the LDAP query performance

Multiple Group DN

Multiple user Mapping…

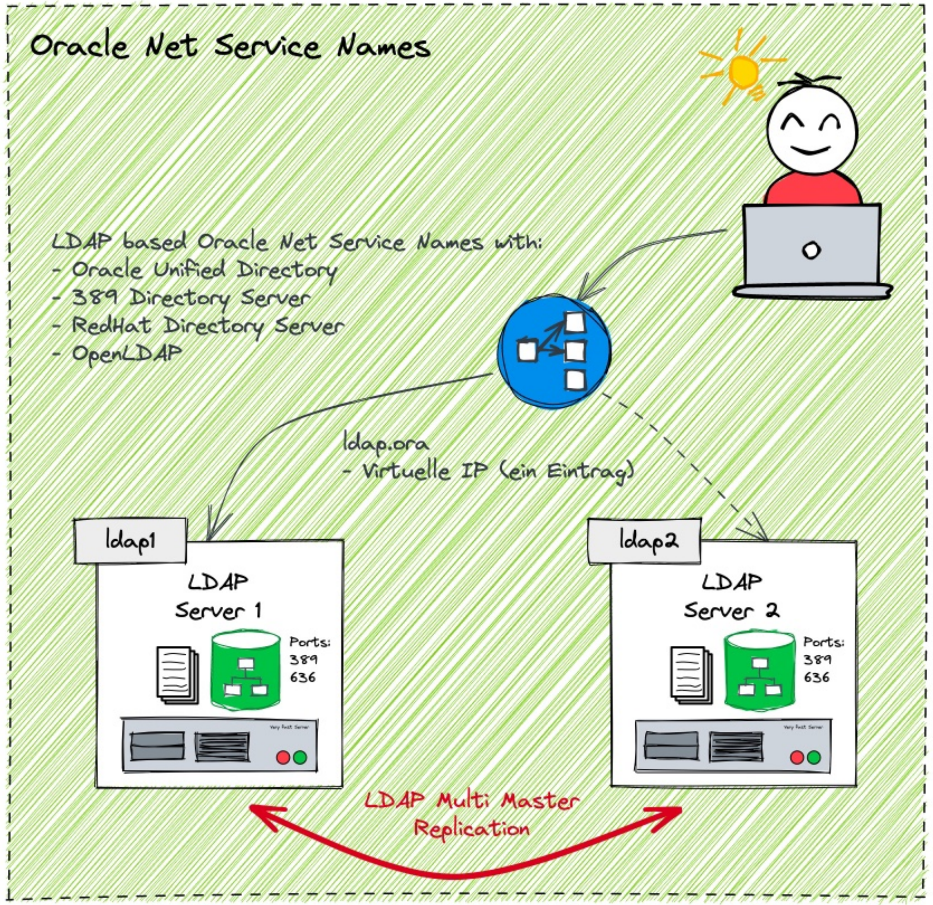
- Keep the mapping of global shared users low
  - The more you have the more you have to maintain
- Avoid users in multiple AD groups
  - The mapping of the users is not explicit
  - You may run into ORA-28306: The directory user has 2 groups mapped to …
  - Depending on the Database version and / or setting of parameter **_ldap_warning_on_multi_shared_mappings**
- Explicit set the parameter **_ldap_warning_on_multi_shared_mappings** to get a user information

```
ALTER SYSTEM SET "_ldap_warning_on_multi_shared_mappings"=TRUE SCOPE=BOTH;
```

Oracle Net Service Names

What happens to the Oracle Net Service Names?

- Oracle CMU covers only authentication and authorization
- Database services are **not registered** in active directory
- *Oracle Net Service Names* as configured in *sqlnet.ora*
  - TNSNAMES, EZCONNECT,…
- Directory Based *Oracle Net Service Names* highly recommended
- Various options available:
  - **Active Directory**: requires AD schema updates
  - **Oracle Directory**: Could either be *Oracle Unified Directory* (OUD) or *Oracle Internet Directory* (OID) without any additional license
  - **Other LDAP Servers**: OpenLDAP, 389-DS, RHDS etc. requires corresponding LDAP schema for *Oracle Net Service Names*


Oracle Net Service Names
LDAP based Oracle Net Service Names with:
- Oracle Unified Directory
- 389 Directory Server
- RedHat Directory Server
- OpenLDAP
ldap.ora
- Virtuelle IP (ein Eintrag)
ldap1
LDAP Server 1
Ports: 389 636
ldap2
LDAP Server 2
Ports: 389 636
LDAP Multi Master Replication

6

Special Use Cases

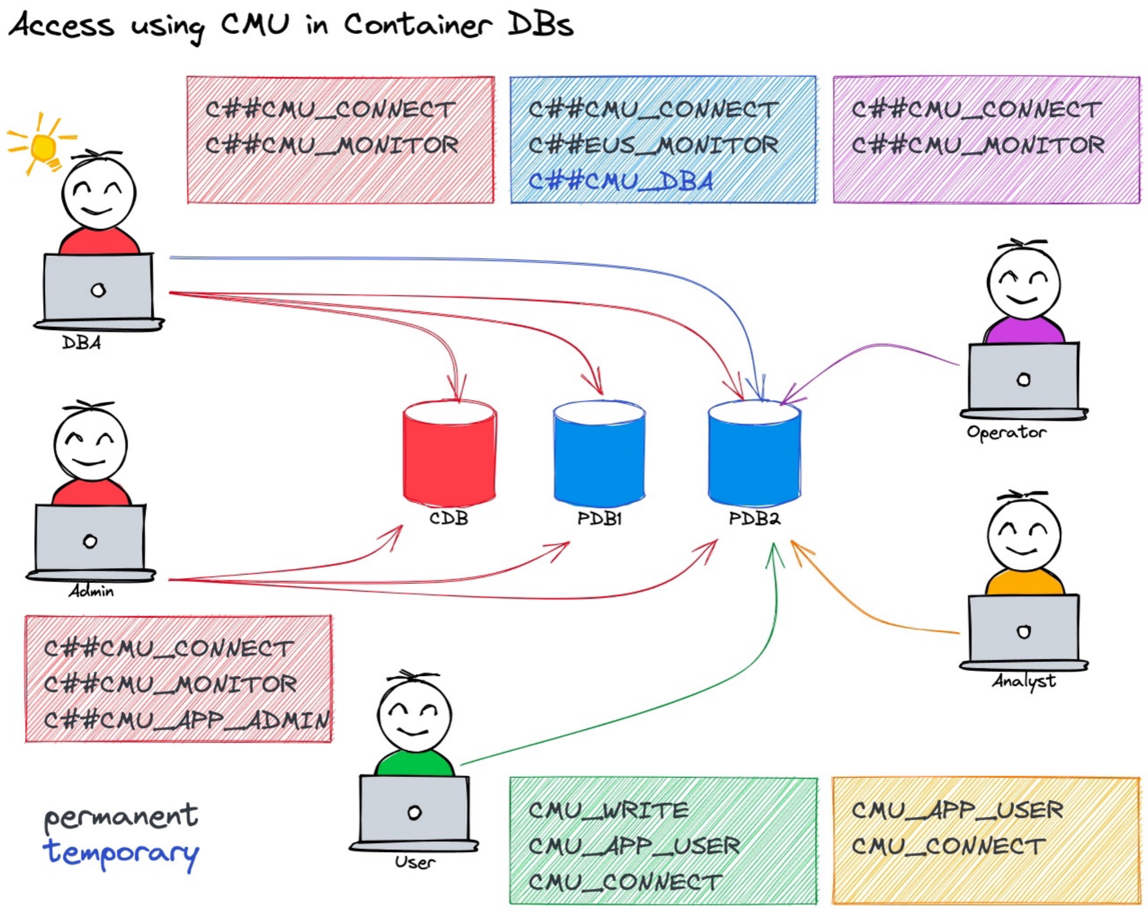
How much does it cost?

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

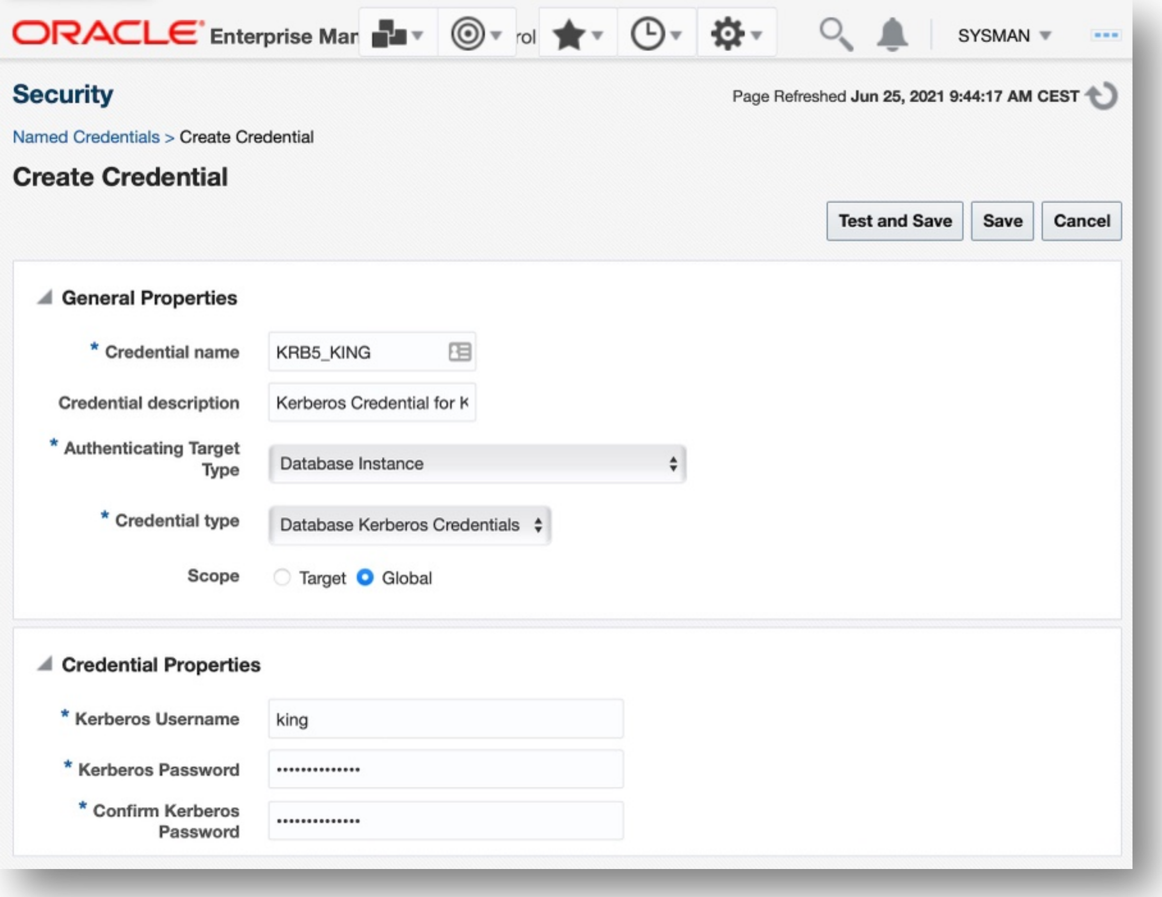
Comprehensive user and role concept gets even more important



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: ••••••••••••••

Use Case Emergency Access

Method for temporarily granting higher privileges

Problem

- Certain power user, developer etc. requires more privileges e.g., DBA like privileges
- These critical privileges should be granted only for a specified period of time e.g., for troubleshooting, schema update etc.
- Must be done without DBA intervention
- Active session roles per user not globally ”visible”

Solution

- Create a global role with corresponding privileges
  - Mapped to some kind of emergency access AD group
- Add user temporary to this AD group => Implemented via IAM self-service
- Check that sessions do not exceed the time limit

Preparations

Simple example of configuring emergency access…

- Create global role **CMU_DBA_EMERGENCY** with **DBA** privileges

```
CREATE ROLE cmu_dba_emergency IDENTIFIED GLOBALLY AS 'cn=Emergency
Access,ou=Groups,dc=trivadislabs,dc=com';
GRANT dba TO cmu_dba_emergency;
```

- Audit Policies to collect emergency access information

```
CREATE AUDIT POLICY cmu_emergency_access ACTIONS LOGON
WHEN 'SYS_CONTEXT(''SYS_SESSION_ROLES'',''CMU_DBA_EMERGENCY'')=''TRUE'''
EVALUATE PER SESSION;
AUDIT POLICY cmu_emergency_access BY CMU_USERS;
```

- Enable the Audit for the **SYS_SESSION_ROLES** Context for **CMU_USERS**

```
AUDIT CONTEXT NAMESPACE sys_session_roles ATTRIBUTES cmu_dba_emergency BY CMU_USERS;
```

Monitor Usage

Simple example of configuring emergency access…

- Query **unified_audit_trail** and **v$session** to get information on emergency access

```
SELECT
    a.event_timestamp,
    a.dbusername,
    a.external_userid,
    s.osuser,
    s.sid,
    s.serial#,
    a.application_contexts,
    CASE WHEN event_timestamp < sysdate-1/1440 THEN 'EXPIRED’
    ELSE 'VALID' END EM_ACCESS_STATUS
FROM
    unified_audit_trail a, v$session s
WHERE
    a.sessionid=s.audsid AND a.dbusername = 'CMU_USERS';
```

Kill the expired sessions

Simple example of configuring emergency access…

- Kill expired sessions manually using **ALTER SYSTEM KILL SESSION**
- Create a **PROCEDURE** to kill expired sessions
  - Using query example as basis
  - Define role name and valid time as parameter
- Create a **DBMS_SCHEDULER** job to automatically kill expired sessions regularly
  - Scheduler kill job on an hourly intervall

7

Troubleshooting

Alternative Solutions and Products

Get Information about the current User

Who is logged in as shared / private global user?

- *v$session* may show OS user in case of Kerberos authentication
- Each user can query his session context *USERENV* using the function *sys_context*
  - SESSION_USER, PROXY_USER, AUTHENTICATION_METHOD, IDENTIFICATION_TYPE, AUTHENTICATED_IDENTITY, ENTERPRISE_IDENTITY, etc

```
SELECT sys_context('userenv','SESSION_USER') FROM dual;
SELECT sys_context('userenv','ENTERPRISE_IDENTITY') FROM dual;
```

- Role information

```
SELECT role FROM session_roles ORDER BY role;
```

Get Information about the current User

Collect current user information with SYS_CONTEXT

- Excerpt of Trivadis BasEnv script *sousrinf.sql* output

```
SQL> @sousrinf
Database Information
--------------------
- DB_NAME       : TSEC02
- DB_DOMAIN     : trivadislabs.com
- INSTANCE      : 1
- INSTANCE_NAME: TSEC02
- SERVER_HOST   : db19
Authentification Information
----------------------------
- SESSION_USER               : CMU_USERS
- PROXY_USER                 :
- AUTHENTICATION_METHOD      : PASSWORD_GLOBAL
- IDENTIFICATION_TYPE        : GLOBAL SHARED
- NETWORK_PROTOCOL           :
- OS_USER                    : oracle
- AUTHENTICATED_IDENTITY.    : TRIVADISLABS\KING
- ENTERPRISE_IDENTITY        : cn=Ben King,ou=Senior Management,ou=People,dc=trivadislabs,dc=com
```

Kerberos Troubleshooting

A few tips when you have to troubleshoot Kerberos Authentication…

- In case of problems, you will usually get the error *ORA-01017 Invalid Username/Password*
- My Oracle Support Note 185897.1, 1380469.1 and 1375853.1 provide troubleshooting hints
- In general, there is no way around SQLNet tracing
- A few common errors:
- Kerberos configuration is missing or incorrect
  - Services like KDC, server and client cannot be resolved via DNS
  - Network connection problem
  - Time shift between client / server
  - Problems with the keytab file
  - Wrong / missing cipher in keytab file
  - Wrong / kvno Number due to password reset of SPN account
  - Missing Kerberos file
  - Wrong service principle name e.g., not in format *oracle\hostname@REALM*

CMU Troubleshooting

A few tips when you have to troubleshoot CMU…

- In case of problems, you will usually get the error *ORA-01017 Invalid Username/Password* or *ORA-28030*
- Error may be misleading. It really means could not validate that the credential is valid
  - Bad password
  - DC unreachable (due to setup, networking, routing, permissions, or server down)
- Good practice to search the root cause:
  1. Check if the password is correct
  2. Verify if user is locked or password expired
  3. Verify the wallet location
  4. Verify if ports are open
  5. Verify if AD credentials are correct

CMU Troubleshooting – Wallet

- Checking the Wallet information of the service account

```
cd $TNS_ADMIN/cmu
orapki wallet display -wallet . -pwd <WALLET PWD>
mkstore -wrl . -viewEntry ORACLE.SECURITY.DN
mkstore -wrl . -viewEntry ORACLE.SECURITY.PASSWORD
mkstore -wrl . -viewEntry ORACLE.SECURITY.USERNAME
```

- Check if a simple bind is possible via LDAPS port 636

```
ldapbind -h trivadislabs.com -p 636 -U 2 -W "file:/u00/app/oracle/network/admin/cmu" \
-P <WALLET PASSWORD> -D "cn=cmuread,cn=Users,dc=trivadislabs,dc=com" -w '<CMU PASSWORD>'
```

- Query the LDAP / Active Directory via LDAP port 389

```
ldapsearch -h trivadislabs.com -p 389 -D "cn=cmuread,cn=Users,dc=trivadislabs,dc=com" -w <CMU PASSWORD> \
-U 2 -W "file:/u00/app/oracle/network/admin/cmu" -P <WALLET PASSWORD> -b "dc=trivadislabs,dc=com" \
-s sub "(sAMAccountName=King)" dn orclCommonAttribute
```

CMU Troubleshooting - Tracing

- Enable CMU trace event

```
ALTER SYSTEM SET EVENTS='trace[gdsi] disk low';
```

- Analyse trace file

```
grep -i kzlg *.trc
```

- Disable CMU trace event

```
ALTER SYSTEM SET EVENTS ='trace[gdsi] off';
```

- See also Oracle Support Note 2470608.1

8

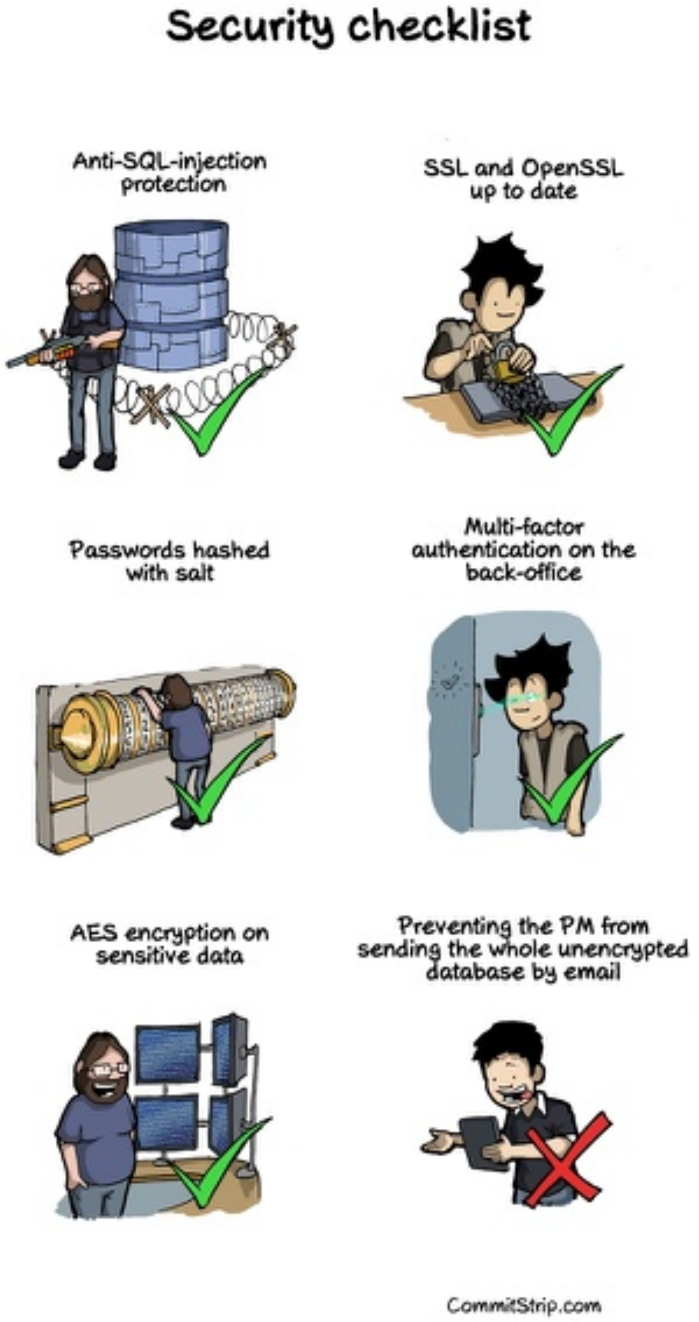
Conclusion

Is CMU a Feature for your Database Environment?

Conclusion

Is the CMU worth considering?

- Oracle Centrally Managed Users is a good alternative to EUS
  - Although some conceptual considerations must be made
  - Dedicated Oracle Net Service Names solutions
- The feature has evolved since its introduction in Oracle 18c
  - Easier configuration
  - A couple of fixed bugs
- Smooth integration AD using Kerberos authentication
- Maximum client flexibility only with the password filter
- A clear security strategy is a highly recommended


Security checklist
Anti-SQL-injection protection
SSL and OpenSSL up to date
Passwords hashed with salt
Multi-factor authentication on the back-office
AES encryption on sensitive data
Preventing the PM from sending the whole unencrypted database by email
CommitStrip.com

Even with Oracle CMU, there is no way around creating a comprehensive user and role concept

Thank You

Oracle Centrally Managed Users (CMU)

Documentation, White Papers, Support Notes and other Links

- Oracle® Database Security Guide 21c Configuring Centrally Managed Users with Microsoft Active Directory
- 2462012.1 How to Configure Centrally Managed Users For On-Premise Databases Release 18c or Later Releases
- 2470608.1 Tracing CMU connection issues
- 2595894.1 ORA-28043 Connecting Using Centrally Managed Users (CMU)
- OraDBA Blog Post Oracle Password Filter for AD, a few exciting insights
- OraDBA Blog Post Easy replacement of tnsnames.ora with LDAP Directory Server