Central User Administration of Databases

Central User Administration of Oracle Databases

Stefan Oehrli

@stefanoehrli   www.oradba.ch

trivadis

Stefan Oehrli

Platform Architect, Trainer and Partner at Trivadis
- Since 1997 active in various IT areas and since 2008 with Trivadis AG
- More than 20 years of experience in Oracle databases
- Live with my family (wife and two kids) in Muri in a small village in CH

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 Security, Advanced Security, Database Vault, …
- Oracle Directory Services

@stefanoehrli   www.oradba.ch

ORACLE® ACE

DER ORACLE DBA
Handbuch für die Administration der Oracle Database 12c

trivadis

trivadis

FOUNDED IN **1994**

16 TRIVADIS WORKSPACES

SWITZERLAND, GERMANY, AUSTRIA, DENMARK, ROMANIA

118 MILLION CHF TURNOVER

300 SLA's (SERVICE LEVEL AGREEMENTS)

4000 TRAINING PARTICIPANTS PER YEAR

800 CUSTOMERS

**700** EMPLOYEES

5 MILLION CHF BUDGET FOR SCIENCE AND DEVELOPMENT PER YEAR

1900 PER YEAR PROJECTS

Agenda

- Overview Authentication and Authorization

- Variants for central user administration of Oracle databases

- Integration of Oracle Database 18c/19c with Active Directory

- CMU Configuration Live Demo

- Troubleshooting

- Distinction Oracle EUS / CMU

- Overview Trivadis LAB

- Summary

Agenda

trivadis
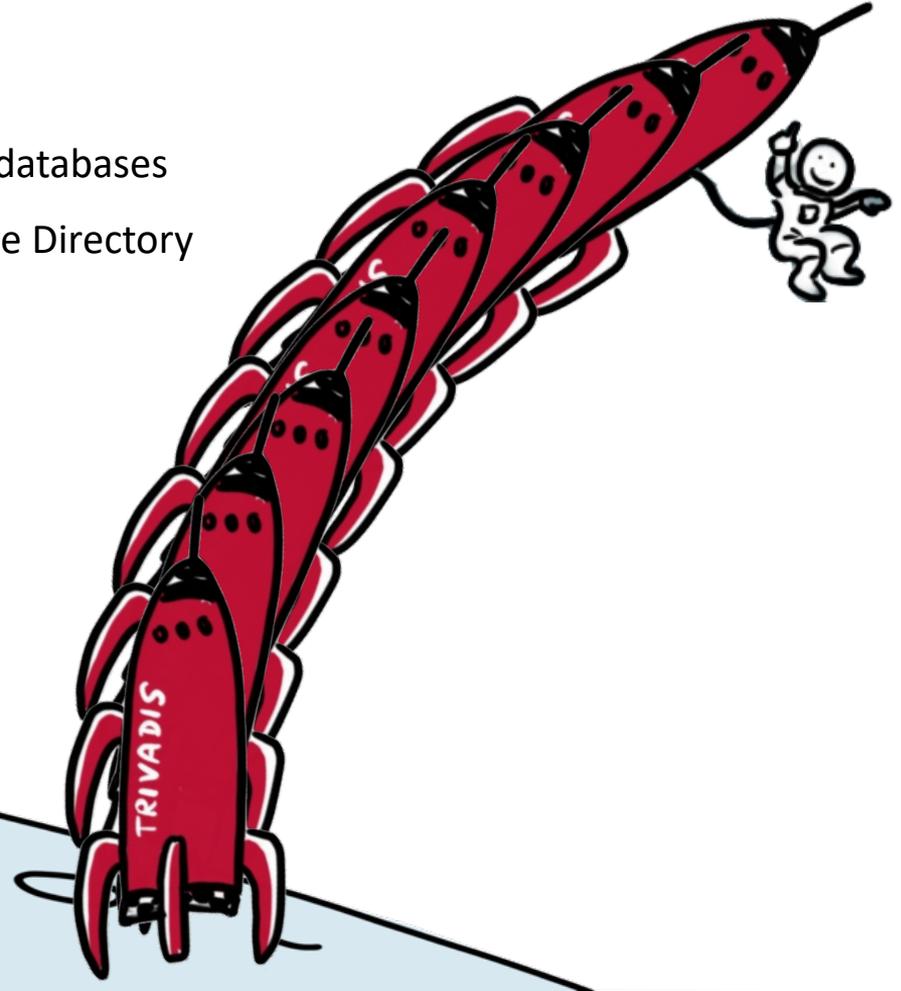
- **Overview Authentication and Authorization**

- Variants for central user administration of Oracle databases

- Integration of Oracle Database 18c/19c with Active Directory

- CMU Configuration Live Demo

- Troubleshooting

- Distinction Oracle EUS / CMU

- Overview Trivadis LAB

- Summary

Authentication

trivadis
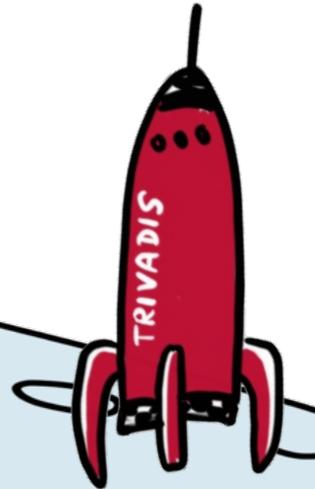
- Verification of the identity of a person who wants to access data, resources or applications.

- The person can be a user, a device or a unit.

- The validation of this identity creates a relationship of trust for further interactions.
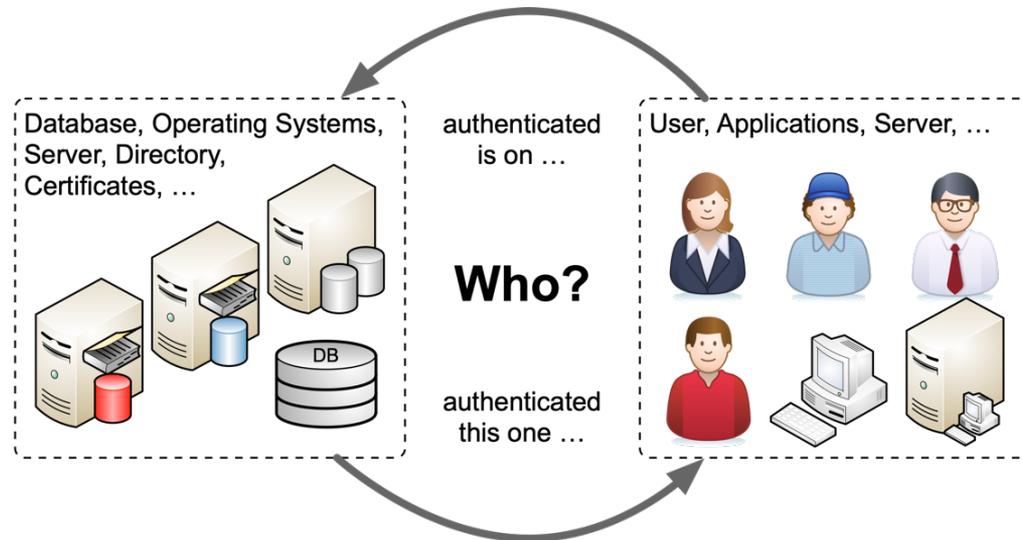
Authorization

- In the broadest sense, a consent or permission or the granting of rights to a person.

- The assignment of privileges to users or user groups.

- Oracle can grant authorizations at different levels.

Authentication Methods
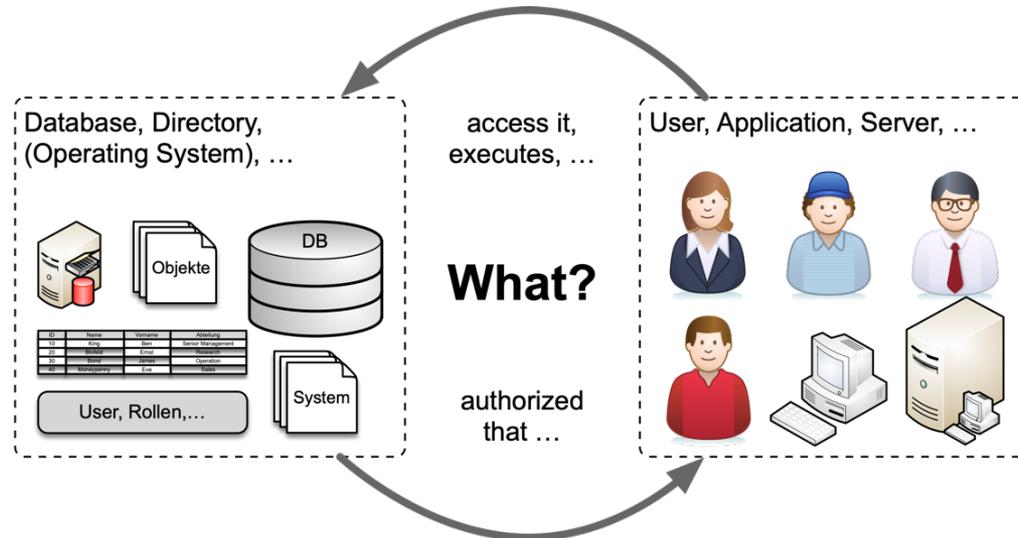
- Database Authentication
  - Authentication at the database with username / password
  - Database checks password hashes
  - Different hashes and protocol versions depending on the Oracle release.

- Database Administration Authentication
  - Authentication of SYSDBA, SYSOPER, SYSBACKUP, SYSRAC, SYSDG, SYSKM and SYSASM
  - Based on OS groups (local) or password file (remote)
  - Allows administrative tasks and authentication when database is stopped.

- OS Authentication
  - Authentication using the operating system sser
  - Passing on responsibility to the operating system

Authentication Methods

trivadis

- Network / Strong authentication
  - Using a network service to authenticate users
  - **Kerberos** authentication
  - **RADIUS** authentication
  - **SSL** or certificate-based authentication
- Directory based authentication
  - Administration of users and roles / groups in an external directory service
  - Mandatory use of an Oracle Directory
  - Oracle Enterprise User Security (EUS)
  - Oracle Centrally Managed User 18c /19c (CMU)
  - Combination of password, Kerberos or SSL authentication

Special Authentication Methods

- Proxy authentication
    - Authentication with alternative credentials
    - User X connects as user Y but authenticates with X
- NO authentication
    - introduced with Oracle 18c
    - *Schema only* Accounts
    - No authentication and therefore no logon possible
    - For application schemas
- Claim based authentication like **SAML**, **OAuth**, etc. as well as **two-factor** authentication are not directly possible with Oracle databases.

Agenda

- Overview Authentication and Authorization

- **Variants for central user administration of Oracle databases**

- Integration of Oracle Database 18c/19c with Active Directory

- CMU Configuration Live Demo

- Troubleshooting

- Distinction Oracle EUS / CMU

- Overview Trivadis LAB

- Summary
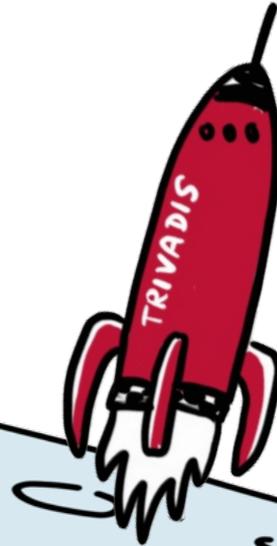
The challenge of user management

- 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
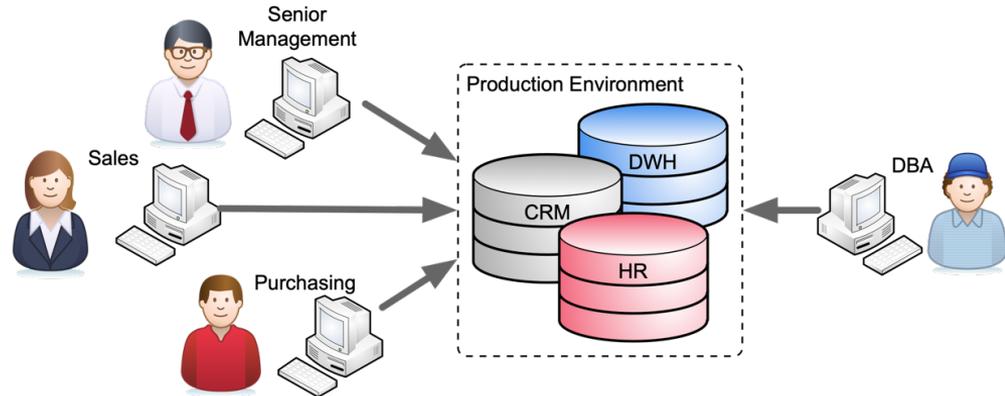
Maximal Data Security Architecture
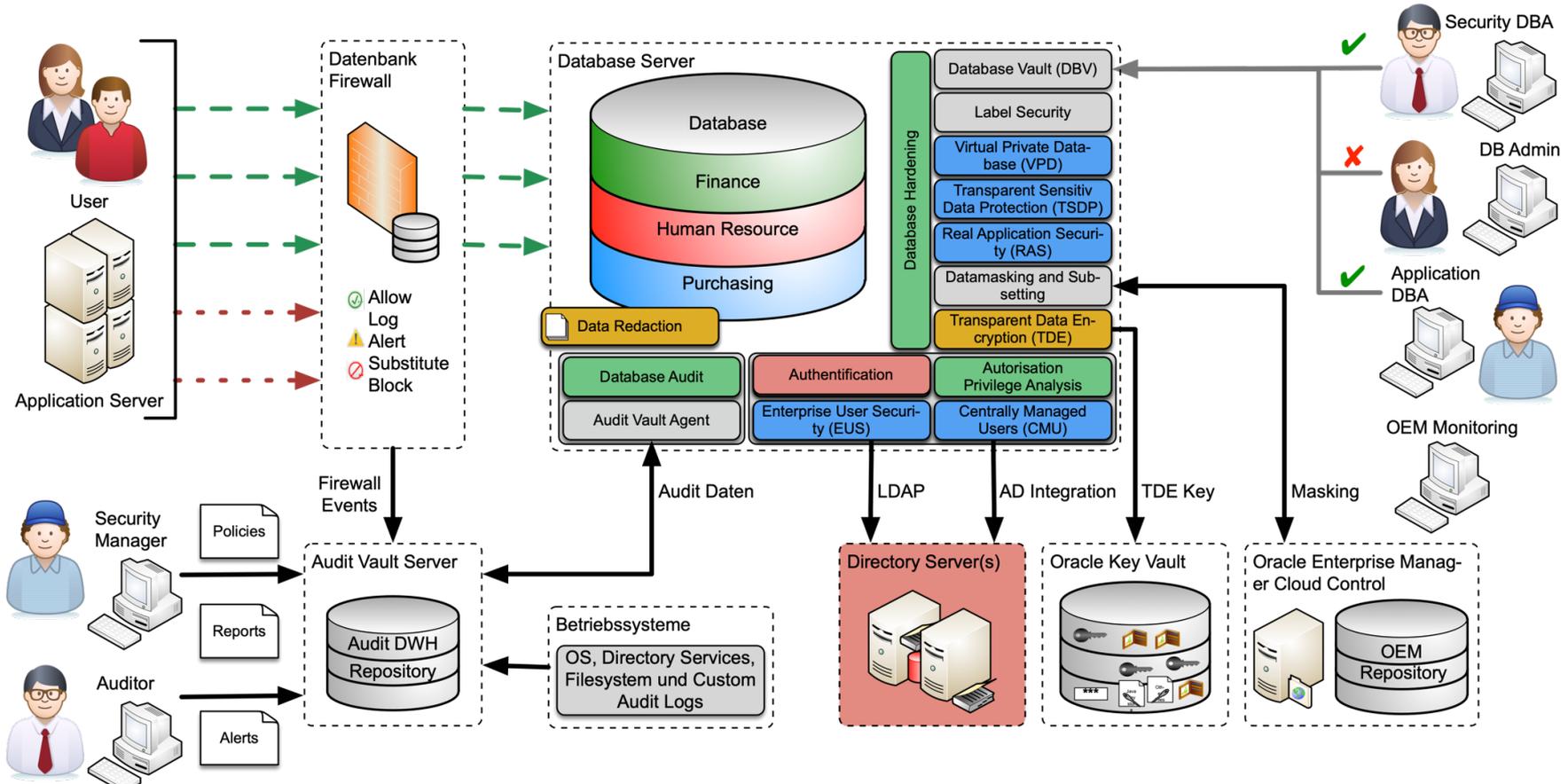
EUS with standalone Directory
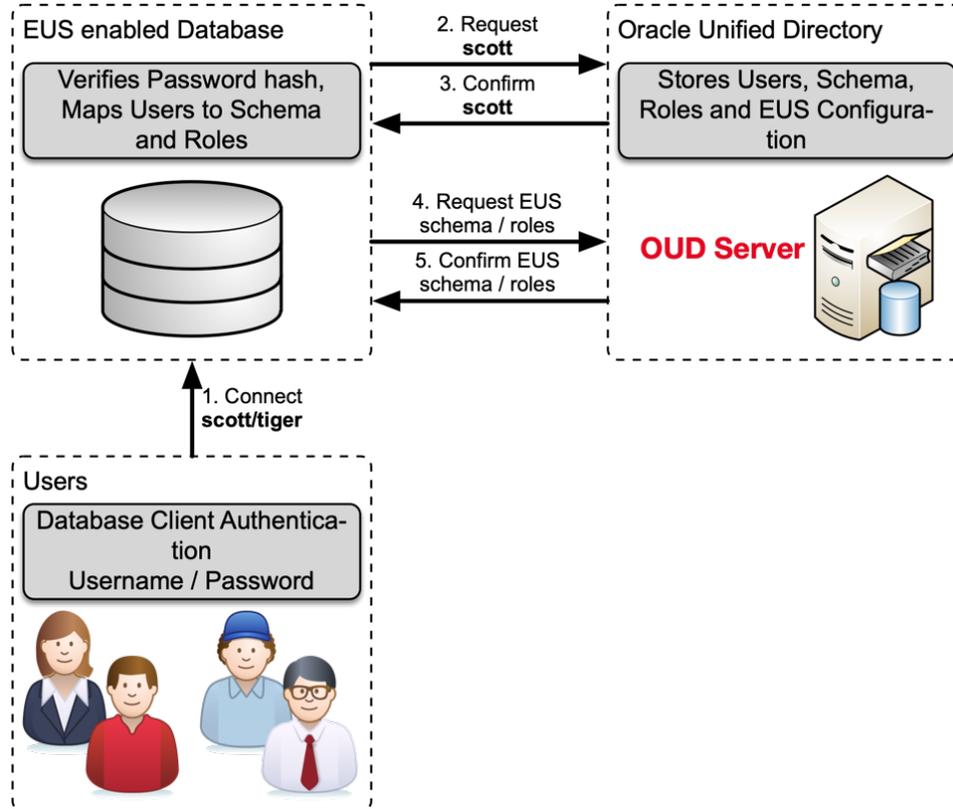
EUS with DIP Integration

trivadis
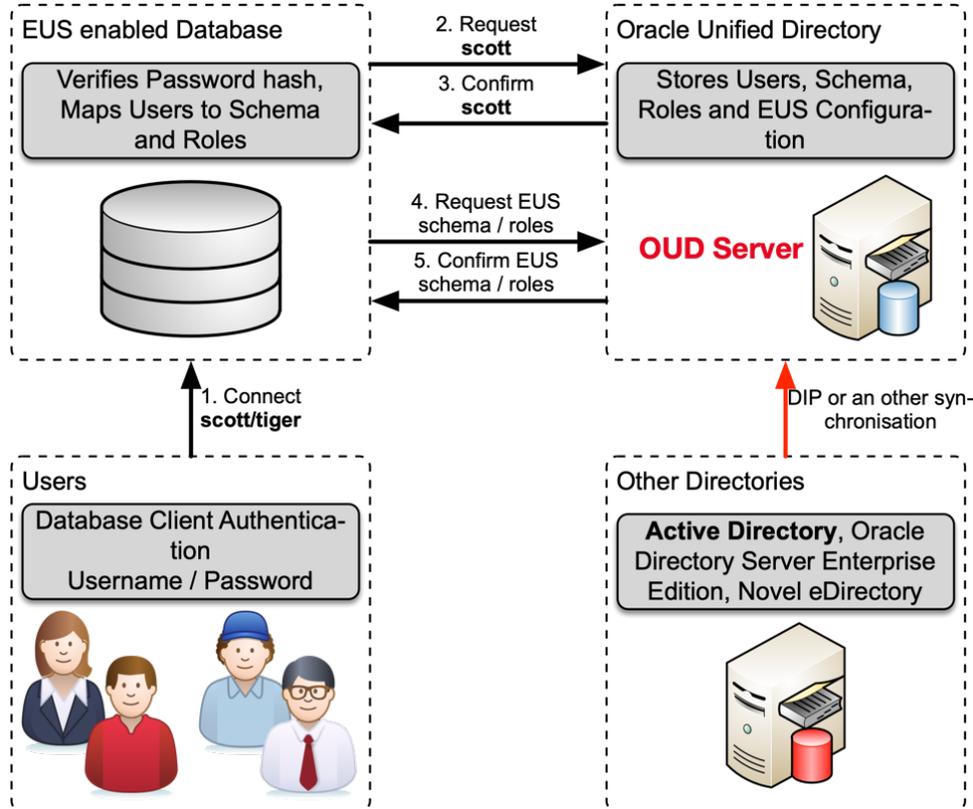
EUS with Proxy Integration
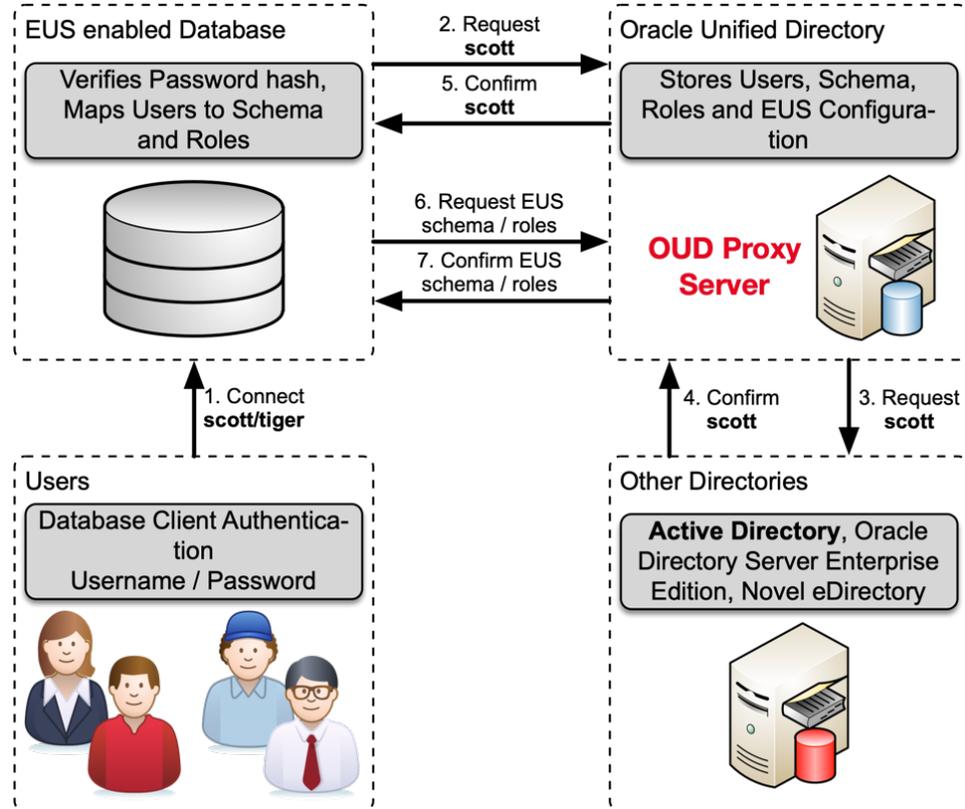
Centrally Managed Users
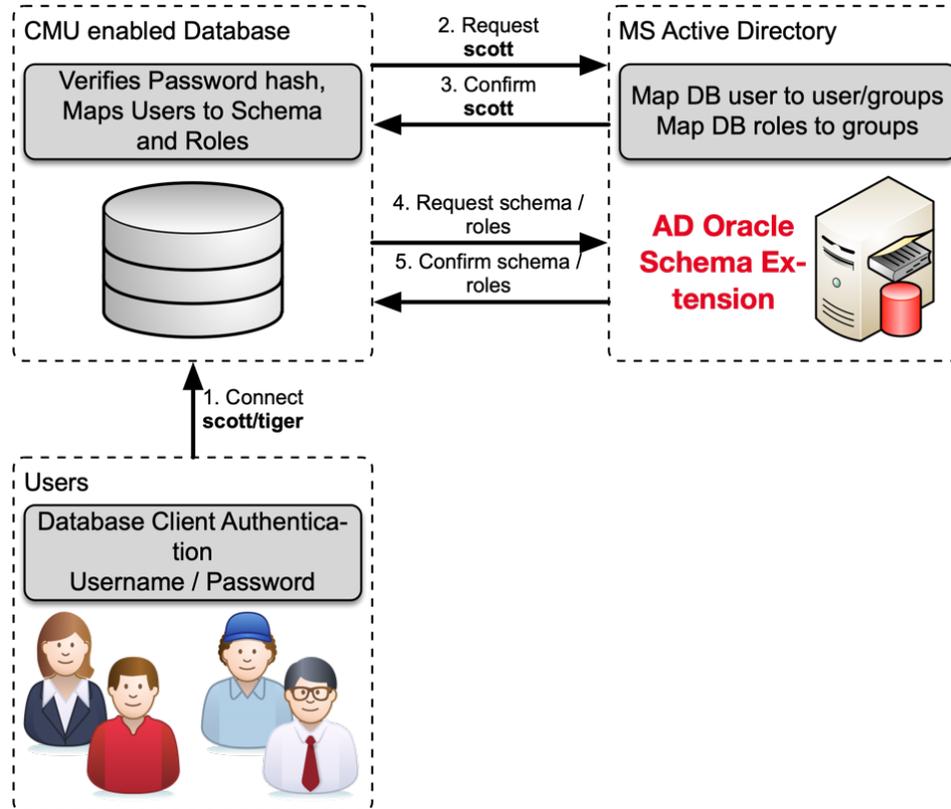
UKOUG Techfest 2019 - Oracle Centrally Managed Users 18c / 19c

Agenda

- Overview Authentication and Authorization

- Variants for central user administration of Oracle databases

- **Integration of Oracle Database 18c/19c with Active Directory**

- CMU Configuration Live Demo

- Troubleshooting

- Distinction Oracle EUS / CMU

- Overview Trivadis LAB

- Summary

Integration of MS Active Directory

trivadis
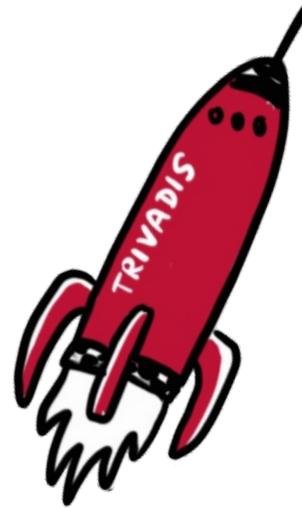
- New security feature of Oracle Database Relase 18c

- Centrally Managed User CMU…

    - … does not require an additional Oracle directory

    - … enables the administration of users directly in MS Active Directory

    - … 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 Authentifizierung

- Requires a password filter and an AD schema extension for password authentication.

- Requires an AD service account

- Perfect for small and medium-sized businesses

Centrally Managed User mit MS AD

- AD Benutzern, die über gemeinsames Schema auf die DB zugreifen
  - Alle Benutzer verwenden das gleiche DB Schema

- Exklusive Zuordnung von AD Benutzern zu einem privaten Schema
  - Benutzer hat eigenes DB Schema mit direkten Berechtigungen
  - Benutzer kann eigene Datenbankobjekte erstellen und verwalten

- Zuweisen einer AD Gruppe zu einer globalen Rolle
  - Vergabe zusätzlicher Rechte aufgrund der AD-Gruppenmitgliedschaft

- Administrative globale Benutzer mit Administratorrechten
  - SYSDBA, SYSOPER, SYSDG, SYSKM oder SYSRAC
  - Kann nicht über globale Rollen gewährt werden

- Kombination von CMU, Net Name Services und Directory Services **ist** möglich
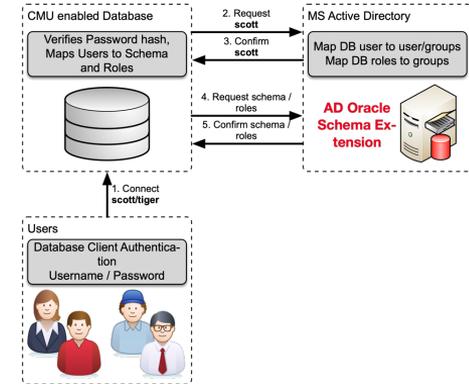
Agenda

- Overview Authentication and Authorization

- Variants for central user administration of Oracle databases

- Integration of Oracle Database 18c/19c with Active Directory

- **CMU Configuration Live Demo**

- Troubleshooting

- Distinction Oracle EUS / CMU

- Overview Trivadis LAB

- Summary

Live Demo

trivadis
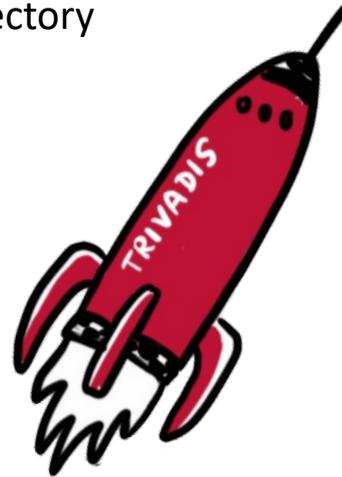
- MS Active Directory Configuration

- SQLNet Configuration

- Database Configuration

- Authentication and Authorization

MS Active Directory Configuration

trivadis

- The database needs access to MS Active Directory
  - Read permissions for searching users/groups
  - Write permissions for updating login information

- Creating an Oracle Service Account
  - MS Active Directory Domain Architecture specifies where the Oracle Service Account is to be created.

- For complex AD domains in the root directory
  - Oracle Service Account must "see" all groups/users

- Service account in the Windows Active Directory root domain when
  - ...the AD users are in different domains
  - ...Active Directory has several Windows domains, which are

Oracle Service Account

- One Oracle Service Account for multiple CMU databases
  - Not every database with CMU requires an individual account.

Password Authentication
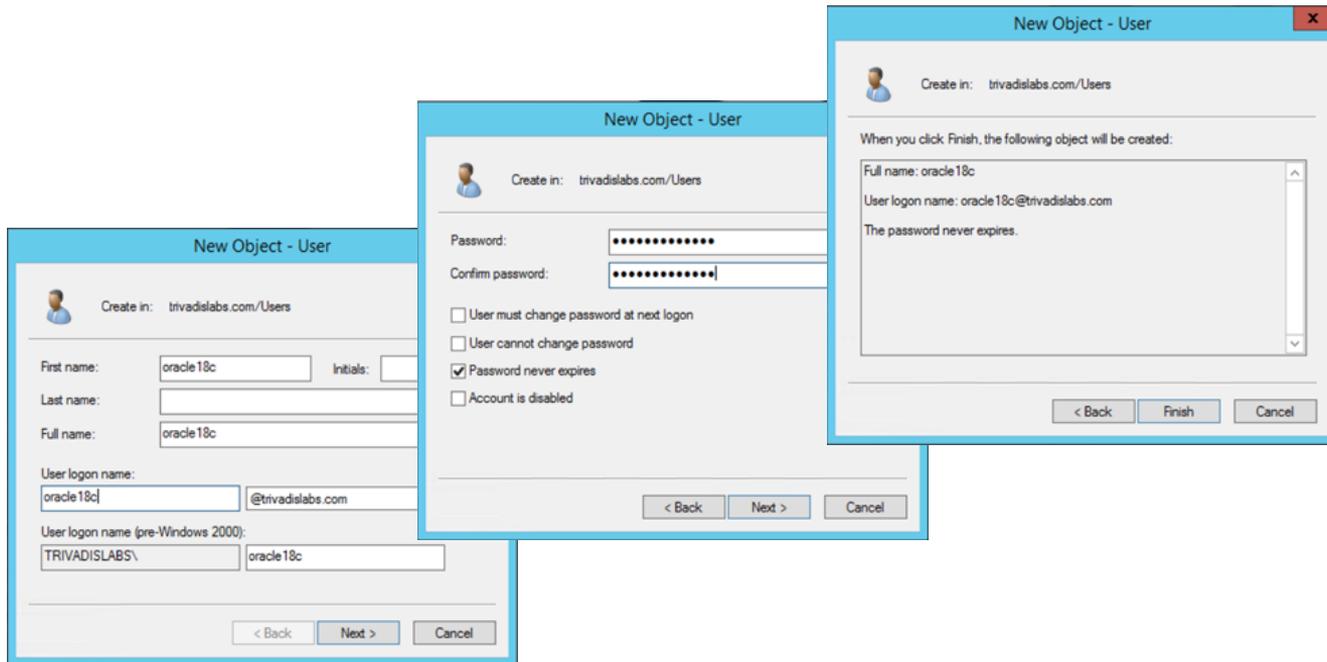
- MS Active Directory customization required for password authentication
  - By default, database or password authentication does not work with MS Active Directory.

- Extension of the MS Active Directory Schema
  - Adds the attribute **orclCommonAttribute** to the schema.
  - Enables Oracle Database password authentication

- The AD groups ORA_VFR_MD5, ORA_VFR_11G and ORA_VFR_12C are created.
  - Required by password filter to generate hashes

- Attention: Create backup before schema customization
  - AD Schema extension can otherwise not be undone

Installation Password Filter

trivadis

- Example output of **opwdintg.exe**

```
Administrator@AD:C:\u00\app\oracle\work\ [CL18300] opwdintg.exe
Do you want to extend AD schema? [Yes/No]:yes
Schema master is ad.trivadislabs.com
================================================================
Extending AD schema with orclCommonAttribute for user object in AD domain:
DC=trivadislabs,DC=com
================================================================
Schema extension for this domain will be permanent. Continue?[Yes/No]:yes
Connecting to "ad.trivadislabs.com"
Logging in as current user using SSPI
Importing directory from file "etadschm.ldf"
Loading entries.....
4 entries modified successfully.

The command has completed successfully
.
Done. Press Enter to continue...
```

Finish Installation Password Filter

trivadis

- Corresponding groups / users must be adapted

- Assignment of the new groups
  - ORA_VFR_MD5 is used for Oracle Database WebDAV Clients
  - ORA_VFR_11G allows you to use the Oracle 11g Password Verifier
  - ORA_VFR_12C enables the use of the Oracle 12c Password Verifier

- Password adjustment or password reset necessary
  - **orclCommonAttribute** is not set until password is reset
  - Check whether the attribute orclCommonAttribute is set.

SQLNet Configuration

- The SQLNet configuration for CMU in dsi.ora or ldap.ora
  - Contains information about Active Directory Server, Ports and Admin Context

- Oracle searches for the file **dsi.ora** in the following order
  - In WALLET_LOCATION if specified in *sqlnet.ora*
  - In the default WALLET_LOCATION if not configured in *sqlnet.ora*

- Then the directories are searched analogously for *ldap.ora*
  - *$LDAP_ADMIN* environment variable
  - *$ORACLE_HOME/ldap/admin* directory
  - *$TNS_ADMIN* environment variable
  - *$ORACLE_HOME/network/admin* directory

- If *dsi.ora* and *ldap.ora* are defined, **dsi.ora** has priority.

Setup Oracle Wallet

trivadis

- Copy Root Certificate from Active Directory Server to DB Server

- Creating a Wallet for the Logon Information from the AD Server

```
mkdir $ORACLE_BASE/admin/$ORACLE_SID/wallet
orapki wallet create -wallet $ORACLE_BASE/admin/$ORACLE_SID/wallet  -
auto_login
```

- Add the Oracle Service Account Name

```
mkstore -wrl $ORACLE_BASE/admin/$ORACLE_SID/wallet -createEntry
ORACLE.SECURITY.USERNAME oracle
```

- Add the distinguished name DN of the Oracle service account name

```
mkstore -wrl $ORACLE_BASE/admin/$ORACLE_SID/wallet -createEntry
ORACLE.SECURITY.DN CN=oracle,CN=Users,DC=trivadislabs,DC=com
```

Setup Oracle Wallet

trivadis

- Add Password for Oracle Service Account

```
mkstore -wrl $ORACLE_BASE/admin/$ORACLE_SID/wallet -createEntry
ORACLE.SECURITY.PASSWORD LAB01schulung
```

- Load MS Active Directory server root certificate

```
orapki wallet add -wallet $ORACLE_BASE/admin/$ORACLE_SID/wallet -cert
$TNS_ADMIN/ad_root_ca.cer -trusted_cert
```

- Verify content of wallet with mkstore or orapki

```
orapki wallet display -wallet $ORACLE_BASE/admin/$ORACLE_SID/wallet
```

Database Configuration

trivadis

- For the access to the Active Directory Server database parameters have to be set.

- Manual setting of parameters

```
ALTER SYSTEM SET LDAP_DIRECTORY_ACCESS = 'PASSWORD';
ALTER SYSTEM SET LDAP_DIRECTORY_SYSAUTH = YES SCOPE=SPFILE;
```

- Alternatively you can use the **dbca** in CLI or GUI mode.
  - But the **dbca** needs a *ldap.ora*, *dsi.ora* it doesn't know ☺

- MOS Note [2462012.1](#) describes the CMU configuration

Authentication and Authorization

trivadis

- Assigning an AD User to a Global DB User
    - Corresponds to a global private scheme in EUS
    - Each user has his own database schema

```
CREATE USER blofeld IDENTIFIED GLOBALLY AS 'CN=Ernst
Blofeld,OU=Research,OU=People,DC=trivadislabs,DC=com';
GRANT create session TO blofeld;
GRANT SELECT ON v_$session TO blofeld;
```

- Adapt existing users and switch to CMU

```
ALTER USER blofeld IDENTIFIED GLOBALLY AS 'CN=Ernst
Blofeld,OU=Research,OU=People,DC=trivadislabs,DC=com';
```

Authentication and Authorization

trivadis

- Assigning an AD Group to a Shared Global DB User
  - Corresponds to a globally shared schema in EUS
  - The AD users "share" the database schema

```
CREATE USER tvd_global_users IDENTIFIED GLOBALLY AS 'CN=Trivadis LAB
Users,OU=Groups,DC=trivadislabs,DC=com';
GRANT create session TO tvd_global_users ;
GRANT SELECT ON v_$session TO tvd_global_users ;
```

- Assign AD group to a global role

```
CREATE ROLE management IDENTIFIED GLOBALLY AS
'CN=Trivadis LAB Management,OU=Groups,DC=trivadislabs,DC=com';
```

- All members of the group Trivadis LAB Management receive the role **management**

Connection to the Database

trivadis

- Connecting to the User Principal Name (UPN) ...

```
SQL> connect "blofeld@TRIVADISLABS.COM"@TDB184A

Enter password:

Connected.
```

- ... or with DOMAIN\user

```
SQL> connect "TRIVADISLABS\blofeld"@TDB184A

Enter password:

Connected.
```

- Will be something a lot with "", @ and \ especially in combination with EZCONNECT and passwords
- Goes in the meantime with regular Connect String

Complex Groups / Roles

trivadis

- In addition, the object class is decisive during mapping.
    - ObjectClass group vs. ObjectClass Organization

```
SQL> connect "rider@TRIVADISLABS.COM"/LAB01schulung@TDB180S
ERROR:
ORA-28306: The directory user has 2 groups mapped to different database
global
users.

Connected.
SQL> show user;
USER is "TVD_GLOBAL_USERS"
```

- Who is in which group / role is decisive for mapping

- Double group membership leads to problems

- Dependence on the AD structure / groups / role concept

Administrative Users

trivadis

- Format 12.2 forces user profiles for SYS password
    - Password Length, Case Sensitive and Special Characters

- Specify whether Password, External or Global Authentication

```
oracle@db:~/ [TDB184A] orapwd describe file=$cdh/dbs/orapwTDB184A
Password file Description : format=12.2
```

- CMU supports administrative users such as SYSDBA, SYSOPER, etc.

- Configuring administrative users with...
    - Shared Global Schema, assignment via group Simple management
    - Private global schema, 1:1 assignment to a DB user

- **Prerequisite** Password file orapwd must be in format 12.2
    - Default if a new password file is created under 18c
    - Otherwise create new or migrate

Admin Users with Shared Global Schema

- Connect as SYSDBA

```
CREATE USER tvd_global_dba IDENTIFIED GLOBALLY AS 'CN=Trivadis LAB DB
Admins,OU=Groups,DC=trivadislabs,DC=com';
GRANT SYSDBA TO tvd_global_dba;
```

- A corresponding group must exist in the AD.

- Creating a Shared Global Schema

```
connect "fleming@TRIVADISLABS.COM"@TDB184A AS SYSDBA
```

- All users of the Trivadis LAB DB Admins group can log on as SYSDBAs.

- Working as SYSDBA with central user administration possible

Admin Users with Private Global Schema

- Connect as SYSDBA

```
CREATE USER bond IDENTIFIED GLOBALLY AS 'CN=James
Bond,OU=Operations,OU=People,DC=trivadislabs,DC=com';
GRANT SYSDBA TO bond;
```

- A corresponding user must exist in the AD.

- Creating a Private Global Schema

```
connect "bond@TRIVADISLABS.COM"@TDB184A AS SYSDBA
```

- In comparison to Global Shared Schema, the users in the databases have to be maintained individually => additional effort

Information about CMU users

trivadis

- Detailed Information in Session Context USERENV

  - Queries with the SYS_CONTEXT Function

  - CURRENT_SCHEMA, CURRENT_USER, SESSION_USER, AUTHENTICATION_METHOD, AUTHENTICATED_IDENTITY, ENTERPRISE_IDENTITY, IDENTIFICATION_TYPE, LDAP_SERVER_TYPE

```
SHOW USER;
SELECT ROLE FROM SESSION_ROLES ORDER BY ROLE;
```

- Basically as for existing users with SHOW USER or SESSION_ROLES.

```
SELECT SYS_CONTEXT('USERENV', 'LDAP_SERVER_TYPE') FROM DUAL;
SYS_CONTEXT('USERENV','LDAP_SERVER_TYPE')
-----------------------------------------------------------------
AD
```

Active Directory Account Policies

trivadis

- Integration of Active Directory security policies for users

- Oracle Database enforces AD guidelines when logging in

- Service Account for CMU requires corresponding rights on the AD
  - Account Properties to read
  - Certain properties such as lockout time to write

- Oracle prevents AD users with account status from logging in
  - Password expired
  - Password must be changed
  - Account blocked
  - Account deactivated

Agenda

- Overview Authentication and Authorization

- Variants for central user administration of Oracle databases

- Integration of Oracle Database 18c/19c with Active Directory

- CMU Configuration Live Demo

- **Troubleshooting**

- Distinction Oracle EUS / CMU

- Overview Trivadis LAB

- Summary

Troubleshooting CMU
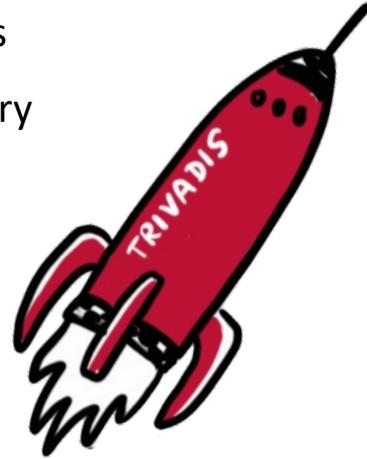
trivadis

- In addition to checking the logon information, only a trace can help.
  - Was the password really correct?

```
SQL> connect "TRIVADISLABS\blofeld"@TDB184A
Enter password:
ERROR:
ORA-01017: invalid username/password; logon denied

Warning: You are no longer connected to ORACLE.
```

- MOS Note 2470608.1 *Tracing CMU connection issues*

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

- Control the trace files and search for **kzlg** z.B `grep -i kzlg *.trc`

Troubleshooting CMU

trivadis

- ORA-01017 in all possible and impossible situations

- Alternatively, the usual trace methods for EUS, Kerberos etc. can be used.
    - MOS Note [783502.1](link) *EUS Authentication Fails With ORA-28030*
    - MOS Note [2470608.1](link) *Tracing CMU connection issues*
    - MOS Note [416946.1](link) *Tips on Using WireShark (Ethereal) to Analyse Network Packet Trace Files*

```
ALTER SYSTEM SET EVENTS '28033 trace name context forever, level 9';

ALTER SYSTEM SET EVENTS '28033 trace name context off';
```

- Troubleshooting is difficult as with Kerberos and EUS

```
ALTER SYSTEM SET EVENTS '1017 trace name errorstack level 10';
```

Troubleshooting CMU

- There are mistakes, too. They're more "obvious."
  - Sometimes I don't

- At best, however, other points are not correct, e.g.
  - UPN is wrong or does not match the DB => User@REALM

- ORA-28276: Invalid ORACLE password attribute
  - The attribute orclCommonAttribute was not set correctly.
  - Check if and what is set in orclCommonAttribute

- ORA-28030: Server encountered problems accessing LDAP directory
  - Checking the LDAP Logon Information

- ORA-28043: invalid bind credentials for DB-OID connection
  - Checking the LDAP Logon Information

- Error ORA-28030 and ORA-28043 you could also hit a bug like [28880433](#)

Checking the logon information

trivadis

- Executing an LDAP bind or LDAP search
  - Here is an example with LDAP Search for sAMAccountName=blo*.

```
mkstore -wrl $ORACLE_BASE/admin/$ORACLE_SID/wallet –list
mkstore -wrl $ORACLE_BASE/admin/$ORACLE_SID/wallet -viewEntry
ORACLE.SECURITY.DN
```

- Control what is in the wallet
  - -list shows all entries
  - -viewEntry displays the corresponding value

```
ldapsearch -h ad.trivadislabs.com -p 389 -D
"CN=oracle18c,CN=Users,DC=trivadislabs,DC=com" -w LAB01schulung -U 2 -W
"file:/u00/app/oracle/admin/TDB184A/wallet" -P LAB01schulung -b
"OU=People,DC=trivadislabs,DC=com" -s sub "(sAMAccountName=blo*)" dn
orclCommonAttribute
```

Agenda

trivadis

- Overview Authentication and Authorization

- Variants for central user administration of Oracle databases

- Integration of Oracle Database 18c/19c with Active Directory

- CMU Configuration Live Demo

- Troubleshooting

- **Distinction Oracle EUS / CMU**

- Overview Trivadis LAB

- Summary

Distinction Oracle EUS / CMU

trivadis
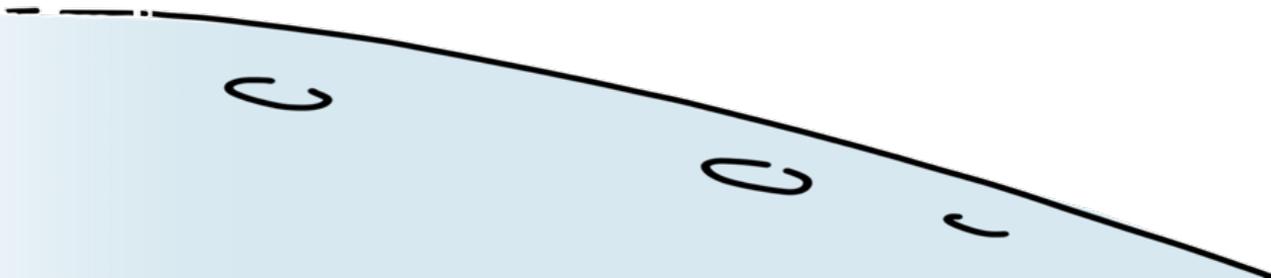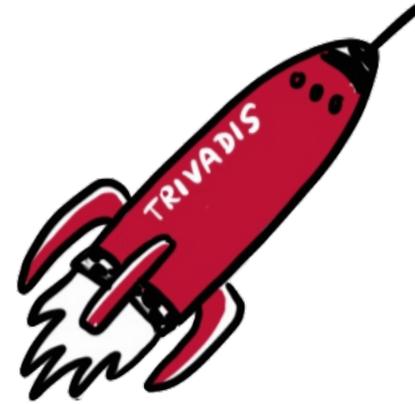
Oracle Enterprise User Security

- Requires an additional directory
  - Increased effort regarding administration, integration, operation, ...
  - Additional License (ODSP)

+ Independence in terms of basic directory structure, schema, authentication

+ name resolution

+ Support of different directories

+ Extensive Enterprise Features
  - Enterprise Roles / Users / Groups
  - Proxy and Admin User

Oracle Centrally Managed Users

- No name resolution

- Only with MS Active Directory
  - Dependency MS AD Structure

- Password Filter / Schema Extension for Password Authentication

- Limited Features
  - No proxy user, enterprise roles, etc. yet

+ No additional license costs

+ No additional directory

+ Simple and easy for simpler environments

Agenda

- Overview Authentication and Authorization
- Variants for central user administration of Oracle databases
- Integration of Oracle Database 18c/19c with Active Directory
- CMU Configuration Live Demo
- Troubleshooting
- Distinction Oracle EUS / CMU
- **Overview Trivadis LAB**
- Summary

Trivadis LAB
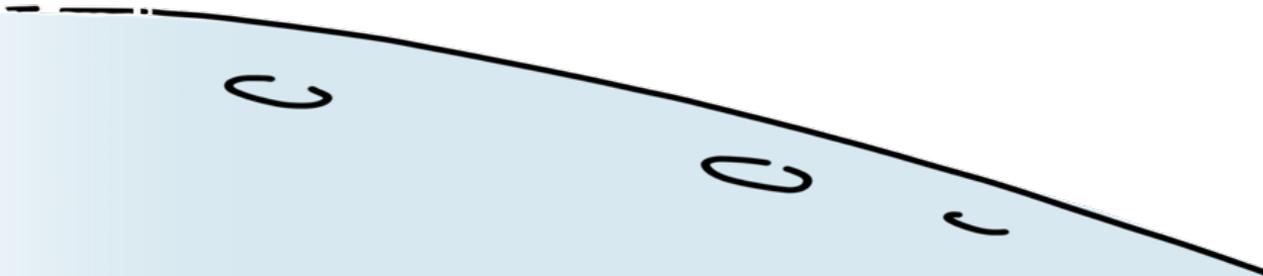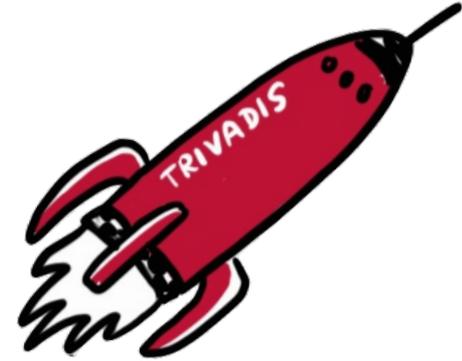
- Virtualbox based test and engineering environment

- Infrastructure as Code with Vagrant
  - Vagrant Scripts available in GitHub Repository https://github.com/oehrlis/trivadislabs.com

- Requires Vagrant, Virtualbox and the various images, software etc.
  - HashiCorp Vagrant https://www.vagrantup.com
  - Oracle VM Virtualbox https://www.virtualbox.org/wiki/Downloads

- Different VM for different applications
  - *win2016ad.trivadislabs.com*   Windows 2016 Active Directory
  - *ol7db18.trivadislabs.com*   Oracle DB Server with 18c (TDB180C and TDB180S)
  - *ol7db19.trivadislabs.com*   Oracle DB Server with 19c (TDB190C and TDB190S)
  - *ol7oud12.trivadislabs.com*   Oracle Unified Directory Server 12c

Trivadis LAB Demo Environment
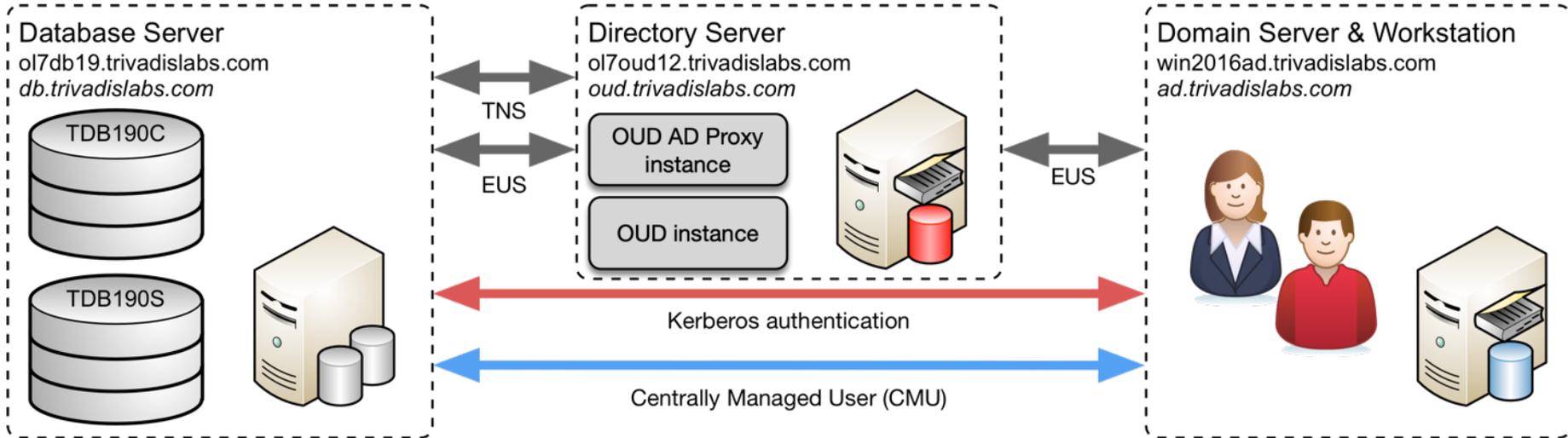
Trivadis LAB Demo Environment
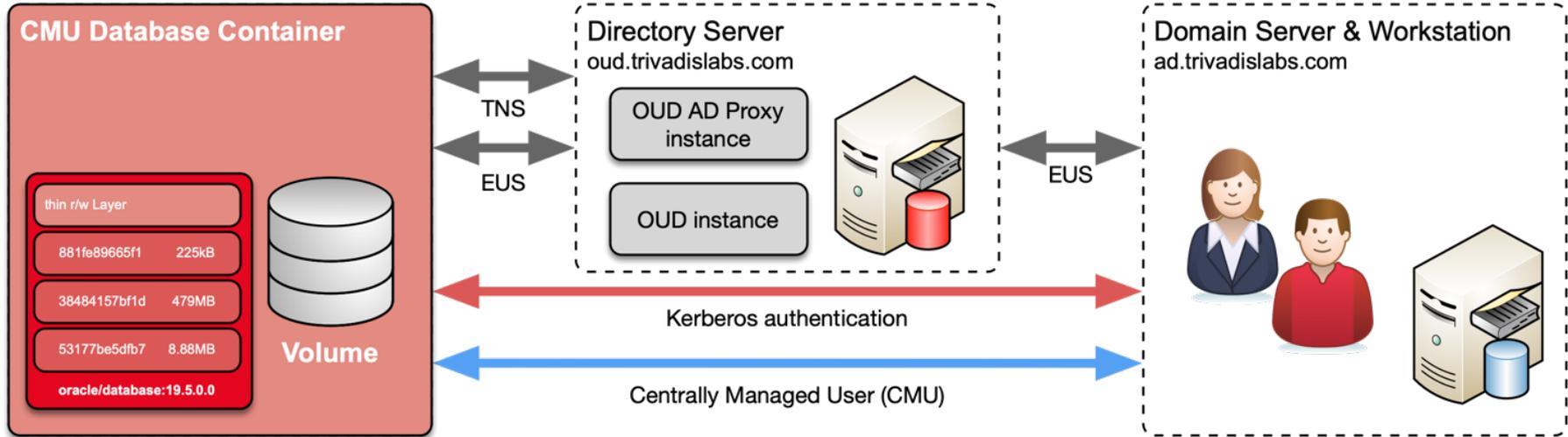
Trivadis LAB Company

- Fictitious company Trivadis Lab with users, departments, etc.

- The Active Directory Server is also a DNS server.

- MS Active Directory Domain is TRIVADISLABS

- All users have the same passwords

- Username is always the last name

Senior Management

Ben King
President

Human Resources

Honey Rider
Manager

Vesper Lynd *Clerk*

Information Technology

Ian Fleming
Manager

Eugen Tanner *Admin*
John Gartner *Admin*

Operations

Felix Leitner
Manager

James Bond *Agent*
Jason Walters *Agent*
Andy Renton *Clerk*

Research

Ernst Blofeld
Manager

James Scott *Engineer*
Paul Smith *Engineer*
Douglas Adams *Clerk*
Ford Prefect *Analyst*

Sales

Eve Moneypenny
Manager

Monica Blake *Salesman*
Paul Ward *Salesman*
Arthur Dent *Salesman*

Accounting

Jim Clark
Manager

John Miller *Clerk*

Vagrant in a Nutshell

trivadis

- Git Repository clonen

```
git clone https://github.com/oehrlis/trivadislabs.com.git
```

- Copy the corresponding Oracle software into the ../software directories.

- Initial starting and provisioning of the VM (win2016ad, ol7db18, ol7db19 ol7oud12

```
cd win2016ad
vagrant up
```

- Access via vagrant ssh / rdp

```
vagrant ssh
sudo su – oracle

vagrant rdp
```

Agenda

- Overview Authentication and Authorization

- Variants for central user administration of Oracle databases

- Integration of Oracle Database 18c/19c with Active Directory

- CMU Configuration Live Demo

- Troubleshooting

- Distinction Oracle EUS / CMU

- Overview Trivadis LAB

- **Summary**

Challenges with CMU

trivadis
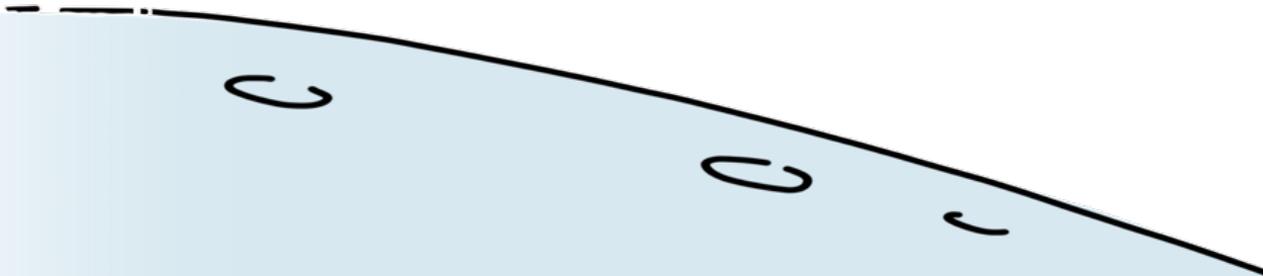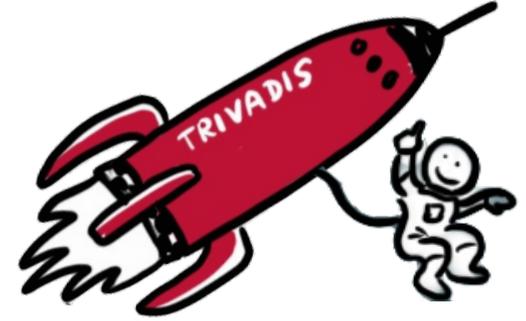
- Centrally Managed Users is a "young" DB Security Feature
    - Various childhood illnesses are present, see MOS note 2462012.1
    - Relatively good chances of finding an issue yourself ☺
    - Bug and patches depending on release

- Not yet widely used
    - Available know-how and experience in the community is modest

- Use of different authentication methods possible and combinable
    - Password authentication perfect for integration into existing applications
    - With Kerberos or SSL authentication SSO possible, no customizations AD

- Biggest challenge is the Active Directory
    - Active Directory structure e.g. multiple domains, forests etc.
    - Password Plugin vs. Kerberos….

Challenges with CMU

- Challenges with...
  - complex Active Directory structures with several Forest / Domain
  - complex groups / role structures
- Centrally Managed Users also need the following …
  - … a security concept for databases
  - … a user and roles concept
  - … personal users
  - … corresponding support from the applications

Quicklinks

trivadis

- https://url.oradba.ch/techfest19

Making a **WORLD** possible in which **intelligent IT** facilitates **LIFE** and **WORK** as a **matter** of **course.**