# Oracle Centrally Managed Users 18/19c

Live Demo zu CMU

Stefan Oehrli

@stefanoehrli

www.oradba.ch

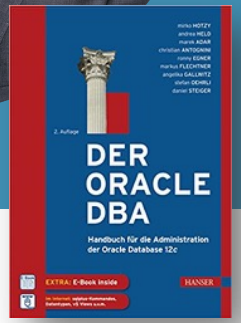
# Stefan Oehrli

Solution Manager, Trainer und Partner bei Trivadis
- Seit 1997 in verschiedenen IT-Bereichen tätig
- Seit 2008 bei der Trivadis AG
- Mehr als 20 Jahre Erfahrung im Umgang

Fokus: Daten schützen und Datenbanken sicher betreiben
- Security Assessments und Reviews
- Datenbank Sicherheitskonzepte und deren Umsetzung
- Oracle Backup & Recovery Konzepte und Troubleshooting
- Oracle Enterprise User Security, Advanced Security, Database Vault, …
- Oracle Directory Services

Co-Autor des Buches Der Oracle DBA (Hanser, 2016/07)

@stefanoehrli




ORACLE ACE

# Trivadis – Unsere wichtigsten Kennzahlen.

- Gründung: 1994
- 16 Trivadis Niederlassungen mit über 650 Mitarbeitenden
- Umsatz CHF 111 Mio. (EUR 96 Mio.)
- Über 250 Service Level Agreements
- Mehr als 4'000 Trainingsteilnehmer
- Forschungs- und Entwicklungsbudget: CHF 5.0 Mio.
- Mehr als 1'900 Projekte pro Jahr bei über 800 Kunden
- Finanziell unabhängig und nachhaltig profitabel

# Agenda

trivadis

- Einleitung Oracle Centrally Managed User 18/19c
- Live Demo
  - MS Active Directory Konfiguration
  - SQLNet Konfiguration
  - Datenbank Konfiguration
  - Authentifizierung und Autorisierung
  - Weitere Use Cases
  - Kerberos Konfiguration
- Überblick Trivadis LAB
- Fazit

trivadis

# Oracle Centrally Managed User 18/19c

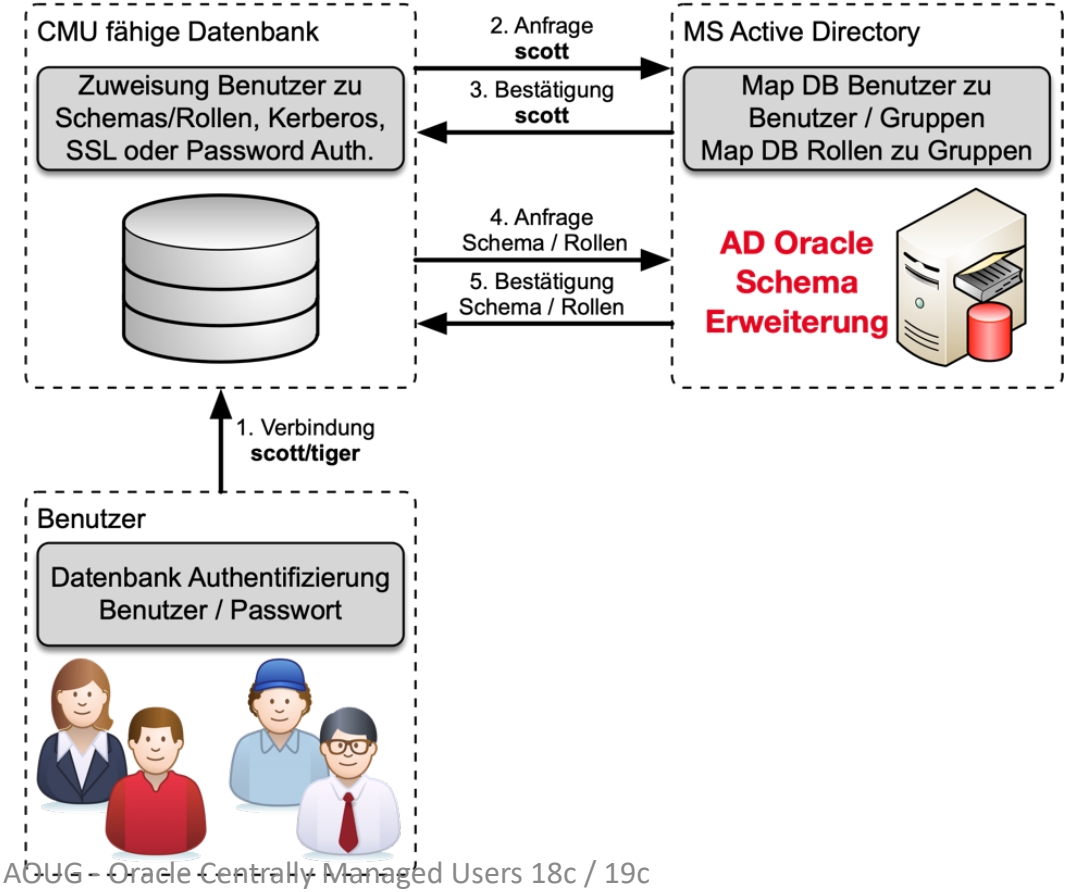
# Integration von MS Active Directory

trivadis

- Neues Security Feature von Oracle Database Relase 18c
- Centrally Managed User CMU…
  - …benötigt kein zusätzliches Oracle Verzeichnis
  - …ermöglicht die Verwaltung der Benutzer im direkt im MS Active Directory
  - …benötig keine zusätzliche Lizenz aber
  - …wird nur von Oracle Enterprise oder Express Edition unterstützt ☺
  - …wird nicht in Oracle Standard Edition unterstützt ☹
- Unterstützt gängige Authentifizierungsmethoden
  - Password- , Kerberos- und PKI / SSL Authentifizierung
- Erfordert einen Passwortfilter und eine AD-Schema-Erweiterung für die Password Authentifizierung
- Erfordert ein AD-Service Account
- Perfekt für kleine und mittlere Unternehmen

# Beispiel Integration mit CMU

trivadis



# Centrally Managed User mit MS AD

trivadis

- 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

trivadis

# Live Demo

# Live Demo

trivadis

- MS Active Directory Konfiguration
- SQLNet Konfiguration
- Datenbank Konfiguration
- Authentifizierung und Autorisierung
- Kerberos Konfiguration
- Weitere Use Cases

# MS Active Directory Konfiguration

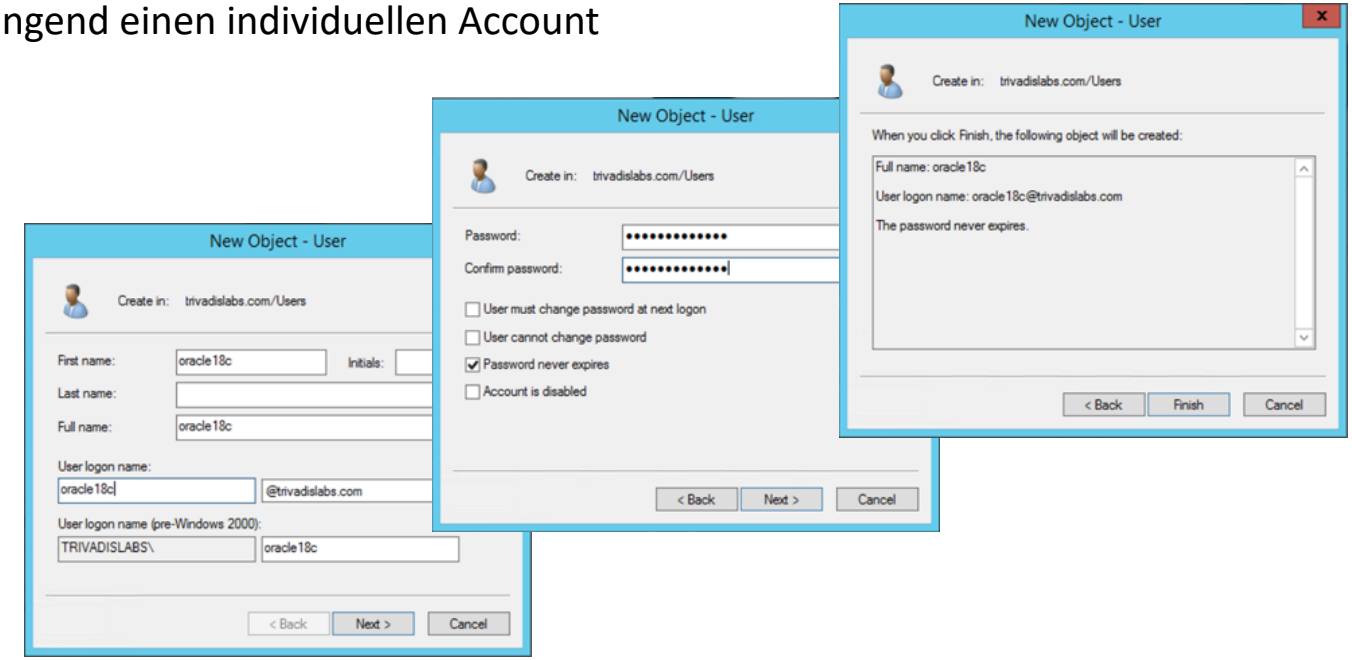
trivadis

- Die Datenbank benötigt Zugriff auf MS Active Directory
  - Leserechte für die Suchen von User / Gruppen
  - Schreibrechte für das Aktualisieren von Logininformationen
- Anlegen eines Oracle Service Account
  - MS Active Directory Domain Architektur gibt vor, wo der Oracle Service Account anzulegen ist
- Bei komplexen AD Domains im Root Verzeichnis
  - Oracle Service Account muss alle Gruppen/Benutzer “sehen”
- Service Account in der Windows Active Directory Root Domain, wenn
  - …die AD-Benutzer sich in verschiedenen Domänen befinden
  - …Active Directory mehrere Windows-Domänen hat, welche von CMU unterstütz werden sollen

# Oracle Service Account

trivadis

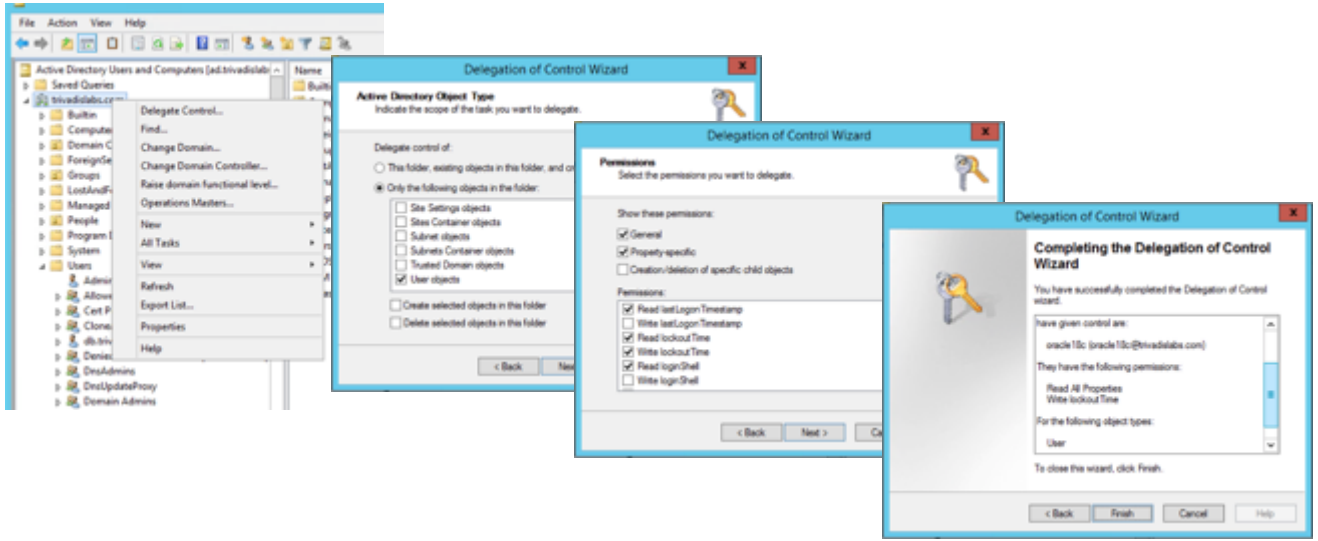
- Ein Oracle Service Account für mehrere CMU Datenbanken
  - Nicht jede Datenbank mit CMU benötigt zwingend einen individuellen Account



# Oracle Service Account

trivadis

- Oracle Service Account benötigt zusätzlich folgende Rechte
  - Read Properties von Active Directory Benutzern
  - Write LockoutTme von Active Directory Benutzern



# Passwort Authentifizierung

trivadis

- MS Active Directory Anpassung für Passwort Authentifizierung nötig
  - Standardmässig funktioniert die Datenbank- respektive Passwort Authentifizierung mit MS Active Directory nicht.
- Erweiterung des MS Active Directory Schema
  - Ergänzt das Schema mit dem Attribut **orclCommonAttribute**
  - Ermöglicht die Oracle Database Passwort Authentifizierung
- Die AD Gruppen ORA_VFR_MD5, ORA_VFR_11G und ORA_VFR_12C werden erstellt
  - Werden vom Passwort Filter benötigt um die Hashes zu generieren
- **Achtung** Backup vor der Schema Anpassung erstellen
  - AD Schemaerweiterung kann sonst **nicht** rückgängig gemacht werden

# Passwort Authentifizierung

trivadis

- Installation Password Filter auf dem Active Directory Server
  - Legt Passwörter zusätzlich in einem Oracle spezifischen Hash ab
  - Ggf. auf allen beteiligten Domain Kontrollern installieren
  - Umgebungssprache muss bei der Installation Englisch sein
- Oracle stellt das Tool **opwdintg.exe** zur Verfügung
  - Jeweils **$ORACLE_HOME/bin** abgelegt
  - Auf Linux Installationen die einzige EXE Datei im ORACLE_HOME ☺
- Fehler falls Schemaerweiterung / Passwort Filter bereits installiert
- Reboot vom Active Directory Server ist nötig
- Analoge Anpassungen für Enterprise User Security mit AD Integration
  - Oder auch andere Tools / IDM Lösungen, die auf AD zugreifen
- Anpassung wird für Kerberos Authentifizierung **nicht** benötigt!

# Installation Password Filter

trivadis

- **opwdintg.exe** auf den Active Directory Server kopieren
- Backup der Active Directory Domain erstellen
- Installation starten und die Fragen entsprechend beantworten
  - Do you want to extend AD schema? [Yes/No]:
  - Schema extension for this domain will be permanent. Continue? [Yes/No]:
  - Found password filter installed already. Do you want to deinstall? [Yes/No]:
  - Do you want to install Oracle password filter? [Yes/No]:
  - The change requires machine reboot. Do you want to reboot now? [Yes/No]:
- Sicherstellen, dass **opwdintg.exe** in einem normalen **cmd.exe** Fenster gestartet wird
  - Schema Erweiterung funktioniert mit BasEnv, PowerShell etc nicht.

# Installation Password Filter

trivadis

- Beispiel Ausgabe von **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...
```

# Abschluss Installation Passwort Filter

trivadis

- Entsprechende Gruppen / Benutzer müssen angepasst werden
- Zuweisung der neuen Gruppen
  - ORA_VFR_MD5 wird für Oracle Datenbank WebDAV Clients benutzt
  - ORA_VFR_11G ermöglicht die Nutzung des Oracle 11g Passwort Verifiers
  - ORA_VFR_12C ermöglicht die Nutzung des Oracle 12c Password Verifiers
- Anpassen der Passwörter bzw. Passwort Reset nötig
  - **orclCommonAttribute** wird erst gesetzt wenn Passwort neu gesetzt
  - Prüfen ob das Attribut **orclCommonAttribute** gesetzt wird

# SQLNet Konfiguration

trivadis

- Die SQLNet Konfiguration für CMU in **dsi.ora** oder **ldap.ora**
  - Enthält Informationen zum Active Directory Server, Ports und Admin Kontext
- Oracle sucht die Datei **dsi.ora** in folgender Reihenfolge
  - In der WALLET_LOCATION falls diese in *sqlnet.ora* angegeben
  - In der Standard WALLET_LOCATION falls nicht in *sqlnet.ora* konfiguriert
- Im Anschluss werden die Verzeichnisse analog für **ldap.ora** durchsucht
  - *$LDAP_ADMIN* Umgebungsvariable
  - *$ORACLE_HOME/ldap/admin* Verzeichnis
  - *$TNS_ADMIN* Umgebungsvariable
  - *$ORACLE_HOME/network/admin* Verzeichnis
- Falls **dsi.ora** sowie **ldap.ora** definiert sind, hat **dsi.ora** Vorrang

# SQLNet Konfiguration

trivadis

- Kombination mit bestehender Namensauflösung möglich
  - **dsi.ora** für Centrally Managed Users
  - **ldap.ora** für die Namensauflösung mit Oracle Names, OID oder OUD
- Individuelle Konfiguration von **dsi.ora** bei Multitenant Datenbanken
  - Generell für die CDBs und alle PDBs
  - Nur für die CDB
  - Für jede PDB individuell
- Beispiel dsi.ora

```
DSI_DIRECTORY_SERVERS = (ad.trivadislabs.com:389:636)
DSI_DEFAULT_ADMIN_CONTEXT = "dc=trivadislabs,dc=com"
DSI_DIRECTORY_SERVER_TYPE = AD
```

# Setup Oracle Wallet

trivadis

- Root Zertifikat vom Active Directory Server auf den DB Server kopieren
- Ein Wallet für die Anmeldeinformationen vom AD Server erstellen

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

- Den Oracle Service Account Name hinzufügen

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

- Den distinguished Name DN Oracle Service Account Name hinzufügen

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

# Setup Oracle Wallet

trivadis

- Passwort für den Oracle Service Account hinzufügen

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

- MS Active Directory Server Root Zertifikat erfassen

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

- Inhalt vom Wallet mit mkstore oder orapki verifizieren

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

# Datenbank Konfiguration

trivadis

- Für den Zugriff auf den Active Directory Server müssen noch Datenbank Parameter gesetzt werden
- Manuelles setzen der Parameter

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

- Alternativ kann dazu auch der **dbca** im CLI oder GUI Mode verwendet werden
  - Der **dbca** benötigt aber unbedingt ein **ldap.ora, dsi.ora** kennt er nicht ☺
- MOS Note 2462012.1 beschreibt die CMU Konfiguration

# Authentifizierung und Autorisierung

trivadis

- Zuordnen eines AD Benutzers zu einem globalen DB Benutzer
  - Entspricht einem global private Schema in EUS
  - Jeder Benutzer hat sein eigenes Datenbank 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;
```

- Bestehende Benutzer anpassen und auf CMU umstellen

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

# Authentifizierung und Autorisierung

trivadis

- Zuordnen einer AD Gruppe zu einem shared globalen DB Benutzer
  - Entspricht einem global shared Schema in EUS
  - Die AD Benutzer „teilen“ sich das Datenbank 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 ;
```

- Zuordnung einer AD Gruppe zu einer globalen Rolle

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

- Alle Mitglieder der Gruppe *Trivadis LAB Management* erhalten die Rolle **management**

# Verbindung zur Datenbank

trivadis

- Verbinden mit dem User Principal Name (UPN) …

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

Enter password:

Connected.
```

- … oder mit DOMAIN\Benutzer

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

Enter password:

Connected.
```

- Wird etwas viel mit „“, @ und \ insbesondere in Kombination mit EZCONNECT und Passwörtern

# Komplexe Gruppen / Rollen

trivadis

- Zudem ist die Objekt Klasse beim Mapping entscheidend
  - 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"
```

- Wer in welcher Gruppe / Rolle ist, ist entscheidend für das Mapping
- Doppelte Gruppenzugehörigkeit führt zu Problemen

# Administrative Benutzer

trivadis

- Format 12.2 erzwingt Benutzerprofile für das SYS Passwort
  - Passwortlänge, Case Sensitiv und Sonderzeichen
- Festlegen ob Passwort, Extern oder Globale Authentifizierung

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

- CMU unterstützt administrative Benutzer wie SYSDBA, SYSOPER etc.
- Konfigurieren von administrativen Benutzern mit…
  - Shared Global Schema, Zuweisung via Gruppe → einfaches Management
  - Private global Schema, 1:1 Zuweisung zu einem DB Benutzer
- **Voraussetzung** Passwort Datei **orapwd** muss im Format 12.2 sein
  - Default, wenn ein neue Passwort Datei unter 18c erstellt wird
  - Ansonsten neu erstellen oder migrieren

# Administrative Benutzer mit Shared Global Schema

trivadis

- Verbindung als SYSDBA aufbauen

```
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;
```

- Im AD muss eine entsprechende Gruppe vorhanden sein
- Erstellen eines Shared Global Schema

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

- Alle Benutzer der Gruppe Trivadis LAB DB Admins können sich als SYSDBA anmelden
- Arbeiten als SYSDBA mit zentraler Benutzerverwaltung möglich

# Administrative Benutzer mit Private Global Schema

trivadis

- Verbindung als SYSDBA aufbauen

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

- Im AD muss ein entsprechender Benutzer vorhanden sein
- Erstellen eines Private Global Schema

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

- Im Vergleich zu Global Shared Schema müssen hier die Benutzer in den Datenbanken individuell gewartet werden  Mehraufwand

# Informationen zu CMU Benutzer

trivadis

- Detaillierte Informationen im Session Kontext USERENV
  - Abfragen mit der Funktion SYS_CONTEXT
  - 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;
```

- Grundsätzlich wie bei bestehenden Benutzern mit **SHOW USER** oder SESSION_ROLES.

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

# Proxy Benutzer und CMU

trivadis

- Proxy mit Kerberos Authentifizierung funktioniert

```
connect tvd_hr["bond@TRIVADISLABS.COM"]@TDB180S
```

- Ja aber…
  - Connection Syntax wird mit zusätzlichen [ ] Klammern nicht einfacher
  - Wird in der Dokumentation nicht explizit erwähnt
  - Proxy mit Passwort Authentifizierung funktioniert nicht
  - Proxy mit CMU unterstützt / nicht unterstützt?

```
ALTER USER tvd_hr GRANT CONNECT THROUGH king
AUTHENTICATED USING DISTINGUISHED NAME;

connect [tvd_hr]/@TDB180S
```

# Active Directory Konto-Richtlinien

trivadis

- Integration der Active Directory Sicherheitsrichtlinien für Benutzer
- Oracle Database erzwingt die AD Richtlinien beim Einloggen
- Service Account für CMU benötigt entsprechende Rechte auf dem AD
  - Account Properties zu lesen
  - Gewisse Properties wie *lockout time* zu schreiben
- Oracle verhindert das Einloggen für AD Benutzer mit Kontostatus
  - Passwort abgelaufen
  - Passwort muss geändert werden
  - Konto gesperrt
  - Konto deaktiviert

# Kerberos - Keytab Datei

trivadis

- Die Keytab Datei wird mit dem Tool *ktpass.exe* auf dem Active Directory Server erstellt

```
C:\> ktpass.exe -princ oracle/db.trivadislabs.com@TRIVADISLABS.COM
-mapuser db.trivadislabs.com -crypto all -pass LAB01schulung -out
C:\u00\app\oracle\network\admin\db.trivadislabs.com.keytab
```

- Kontrolle des SPN

```
C:\> setspn -L db.trivadislabs.com
Registered ServicePrincipalNames for
CN=db.trivadislabs.com,CN=Users,DC=trivadislabs,DC=com:
        oracle/db.trivadislabs.com
```

# Kerberos - Server Konfiguration

trivadis

- Anpassen der *krb5.conf*

```
[libdefaults]
 default_realm = TRIVADISLABS.COM
 clockskew=300
 ticket_lifetime = 24h
 renew_lifetime = 7d
 forwardable = true

[realms]
 TRIVADISLABS.COM = {
   kdc = win2016ad.trivadislabs.com
   admin_server = win2016ad.trivadislabs.com
}

[domain_realm]
.trivadislabs.com = TRIVADISLABS.COM
trivadislabs.com = TRIVADISLABS.COM
```

# Kerberos - Datenbank Konfiguration

trivadis

- Zuweisen der benötigen Rechte und Rollen z.B CREATE SESSION
- Anpassen eines bestehenden Benutzers

```
CREATE USER "KING@TRIVADISLABS.COM" IDENTIFIED EXTERNALLY;
CREATE USER king IDENTIFIED EXTERNALLY AS 'king@TRIVADISLABS.COM';
```

- Erstellen eines Datenbank Benutzers für die Nutzung mit Kerberos
  - Gross / Kleinschreibung des UPN (User Principle Name) beachten!

```
ALTER USER king IDENTIFIED EXTERNALLY AS 'king@TRIVADISLABS.COM’;
ALTER USER "KING@TRIVADISLABS.COM" IDENTIFIED EXTERNALLY;
```

- Falls der Kerberos Principal Name länger als 30 Zeichen ist, muss zwingend IDENTIFIED EXTERNALLY AS verwendet werden
  - Somit sind Kerberos Principal Namen bis 1024 Zeichen möglich

# Manuelles Ticket Granting Ticket

trivadis

- Manuell ein Ticket Granting Ticket mit okinit generieren

```
oracle@db:~/ [TDB184A] okinit king@TRIVADISLABS.COM

Kerberos Utilities for Linux: Version 18.0.0.0.0 - Production on 07-NOV-2018 14:18:18

Copyright (c) 1996, 2017 Oracle.  All rights reserved.

Configuration file : /u00/app/oracle/network/admin/krb5.conf.
Password for king@TRIVADISLABS.COM:
```

- Login mit SQLPlus

```
oracle@db:~/ [TDB184A] sqlplus /@TDB122A
...
SQL> SELECT sys_context('userenv','authentication_method') FROM dual;

SYS_CONTEXT('USERENV','AUTHENTICATION_METHOD')
----------------------------------------------------------
KERBEROS
```

trivadis

# One More Thing

# Troubleshooting mit CMU

trivadis

- Hier hilft neben der Kontrolle der Anmeldeinformationen nur ein Trace
  - War das Passwort wirklich richtig? Siehe MOS Note 352389.1

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

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

- Troubleshooting ist wie bei Kerberos und EUS schwierig
  - ORA-01017 in allen möglichen und unmöglichen Situationen

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

- Allenfalls stimmen aber auch andere Punkte nicht z.B.
- UPN ist falsch oder passt nicht zur DB => User@REALM

# Troubleshooting mit CMU

trivadis

- Es gibt auch Fehler, die sind „offensichtlicher“
  - Manchmal aber auch nicht
- ORA-28276: Invalid ORACLE password attribute
  - Das Attribut *orclCommonAttribute* wurde nicht korrekt gesetzt
  - Prüfen, ob und was in *orclCommonAttribute* gesetzt ist
- ORA-28030: Server encountered problems accessing LDAP directory
  - Prüfen der LDAP Anmeldeinformationen
- ORA-28043: invalid bind credentials for DB-OID connection
  - Prüfen der LDAP Anmeldeinformationen
- Bei den Fehlern ORA-28030 und ORA-28043 kann es aber auch einfach ein Bug wie der Bug 28880433 sein

# Kontrolle der Anmelde Informationen

trivadis

- Ausführen eines LDAP bind oder LDAP Search
  - Hier am Beispiel mit LDAP Search nach sAMAccountName=blo*

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

- Kontrolle was im Wallet ist
  - -list zeigt alle Einträge
  - -viewEntry zeigt den entsprechenden Wert an

```
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
```

trivadis

# Trivadis LAB

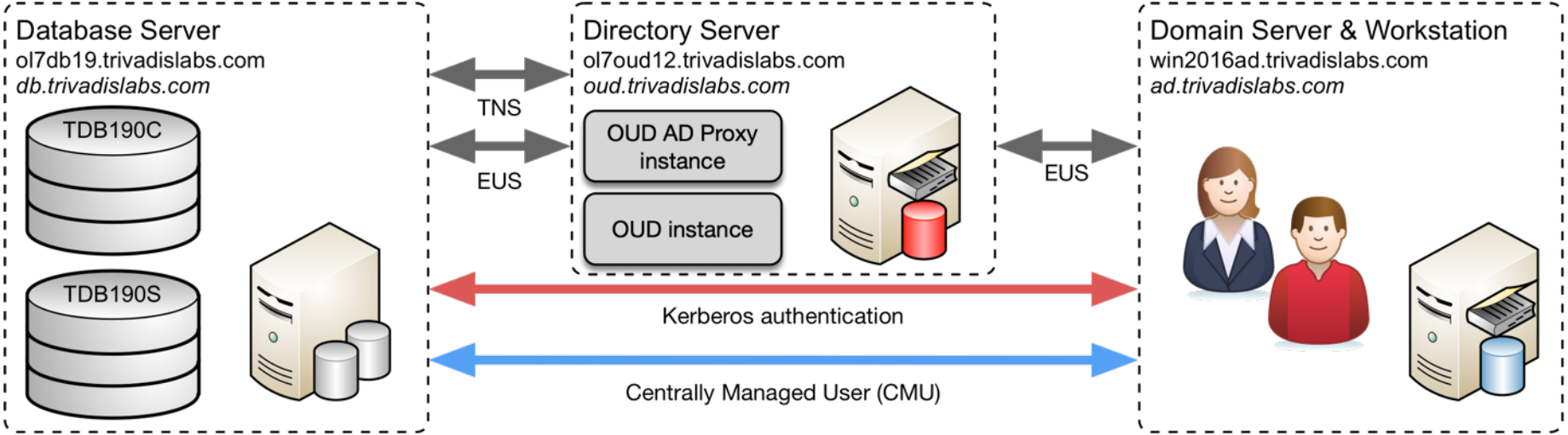
# Trivadis LAB

trivadis

- Virtualbox basierte Test und Engineering Umgebung
- Infrastruktur as Code mit Vagrant
  - Vagrant Scripts verfügbar im GitHub Repository https://github.com/oehrlis/trivadislabs.com
- Benötigt Vagrant, Virtualbox sowie die verschiedenen Images, Software etc
  - HashiCorp Vagrant
    https://www.vagrantup.com
  - Oracle VM Virtualbox
    https://www.virtualbox.org/wiki/Downloads
- Verschiedene VM für unterschiedliche Anwendungsfälle
  - *win2016ad.trivadislabs.com* Windows 2016 Active Directory
  - *ol7db18.trivadislabs.com* Oracle DB Server mit 18c (TDB180C und TDB180S)
  - *ol7db19.trivadislabs.com* Oracle DB Server mit 19c (TDB190C und TDB190S)
  - *ol7oud12.trivadislabs.com* Oracle Unified Directory Server 12c

# Trivadis LAB Demo Umgebung

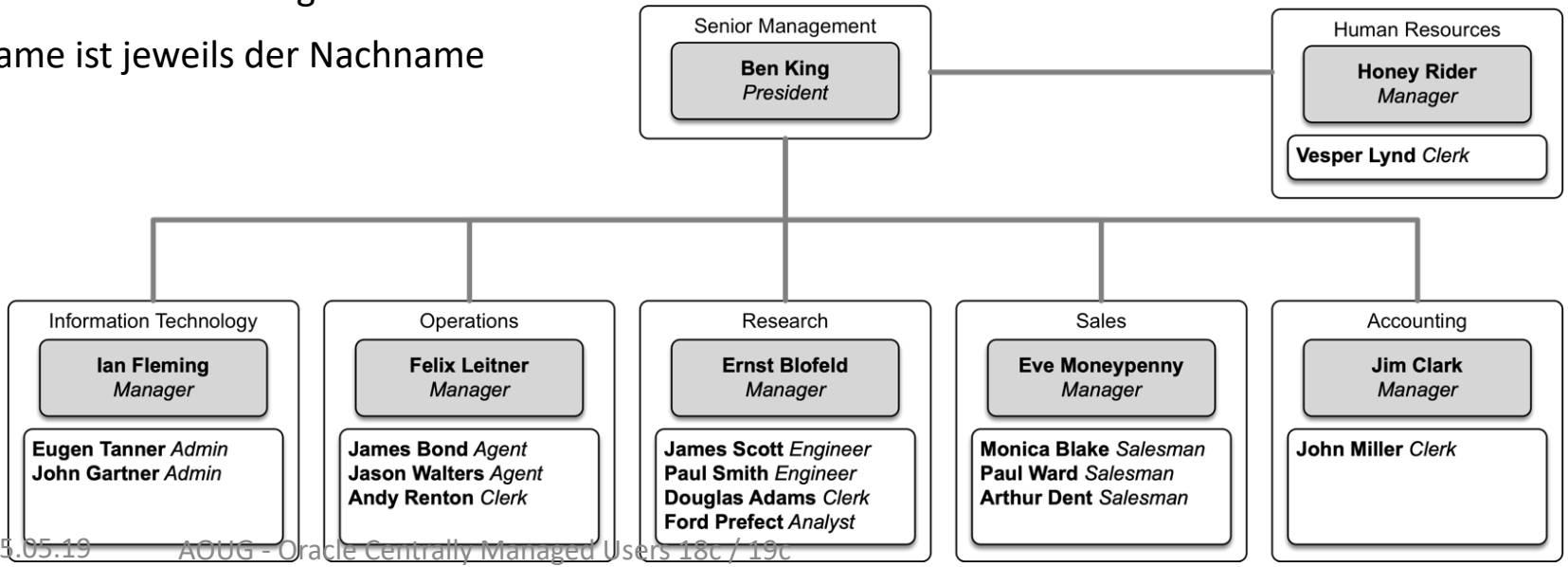
trivadis



# Trivadis LAB Company

trivadis

- Fiktives Unternehmen ***Trivadis Lab*** mit Benutzer, Abteilungen, etc.
- Der Active Directory Server ist gleichzeitig auch DNS Server
- MS Active Directory Domain ist TRIVADISLABS
- Alle Benutzer haben die gleichen Passwörter
- Username ist jeweils der Nachname



# Vagrant in a Nutshell

trivadis

- Git Repository clonen

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

- Entsprechende Oracle Software in die ../software Verzeichnisse kopieren
- Initiales Starten und Provisionieren der VM (win2016ad, ol7db18, ol7db19 ol7oud12

```
cd win2016ad
vagrant up
```

- Zugriff via vagrant ssh / rdp

```
vagrant ssh
sudo su - oracle

vagrant rdp
```

trivadis

# Fazit

# Herausforderungen mit CMU

trivadis

- Centrally Managed Users ist ein „junges“ DB Security Feature
  - Diverse Kinderkrankheiten sind vorhanden, siehe MOS Note 2462012.1
  - Relativ gute Chancen, selber ein Issue zu finden ☺
- Wird noch nicht häufig eingesetzt
  - Verfügbares Know-How und Erfahrung in der Community ist bescheiden
- Centrally Managed Users für Oracle Enterprise und Express Edition
  - Weiterhin keine Lösung für Oracle Standard Edition
  - Braucht es hier etwas?
- Die Connect Strings sind etwas gewöhnungsbedürftig
  - Wie werden diese von den Tools und Applikationen unterstütz?

# Herausforderungen mit CMU

trivadis

- Herausforderungen bei..
  - komplexen Active Directory Strukturen mit mehreren Forest / Domain
  - komplexen Gruppen / Rollen Strukturen
- Auch für Centrally Managed Users (CMU) braucht es zwingend…
  - … ein Sicherheitskonzept für die Oracle Datenbanken
  - … ein Benutzer und Rollen Konzept
  - … personenbezogene Benutzer
  - … entsprechender Support von den Anwendungen

# Quicklinks

trivadis

- http://url.oradba.ch/AOUG19

oehrlis / AOUG19_summary.md Secret

Last active May 15, 2019

Star 0 Fork 0

Code Revisions 5

Embed <script src="https://gi: Download ZIP

Quicklinks AOUG 2019 Conference

AOUG19_summary.md Raw

All links sources etc. summarised in one place.

## AOUG Live Demo

- AOUG 2019 Oracle Centrally Managed Users 18/19c pdf
- AOUG 2019 Live Demo documentation pdf
- AOUG 2019 Live Demo git repository oehrlis/aoug
- Trivadis LAB enviromnent git repository oehrlis/aoug

# Question and answers...

**Stefan Oehrli**

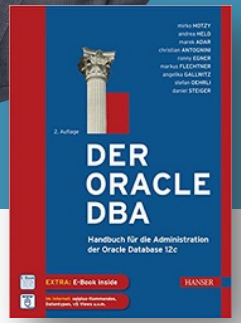
**Solution Manager / Trivadis Partner**

Tel.: +41 58 459 55 55

stefan.oehrli@trivadis.com

@stefanoehrli

www.oradba.ch




ORACLE ACE

Eine WELT ermöglichen,
in der intelligente IT
LEBEN und ARBEITEN
völlig selbstverständlich
erleichtert.