Oracle Centrally Managed User 18c/19c

28. Mai 2019, 16:00 bis 16:45 Uhr

Speaker

Fabian Karsch
Senior Marketing Specialist

fabian.karsch@trivadis.com

Stefan Oehrli
Senior Platform Architect

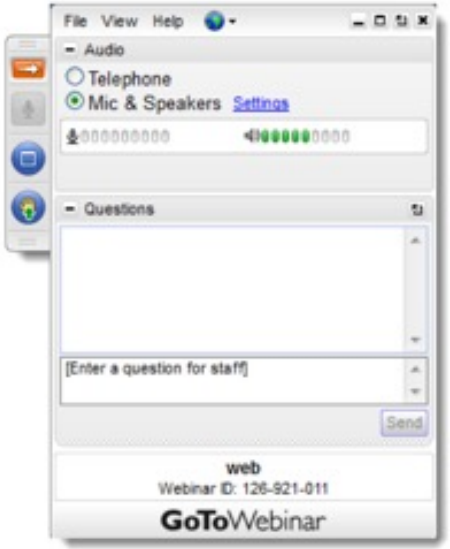
stefan.oehrli@trivadis.com

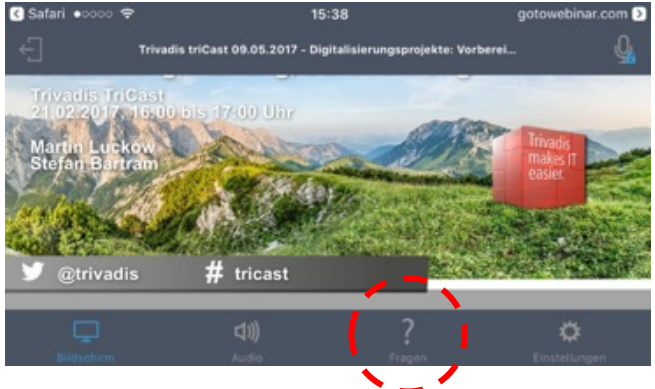
@stefanoehrli

Trivadis triCast Format

trivadis

- Dienstags um 16:00 Uhr
- Vortrag, Fragen & Antworten
- Aktuelle IT-Themen, Trivadis Sichtweise
- WebCast wird aufgezeichnet
- Kurze Umfragen
- Möglichkeit für Fragen mittels Fragen-Menü





Mit über 600 IT- und Fachexperten bei Dir vor Ort

trivadis

- 16 Trivadis Niederlassungen mit über 600 Mitarbeitenden.
- Über 200 Service Level Agreements.
- Mehr als 4'000 Trainingsteilnehmer.
- Forschungs- und Entwicklungs-budget: CHF 5.0 Mio. / EUR 4.0 Mio.
- Finanziell unabhängig und nachhaltig profitabel.
- Erfahrung aus mehr als 1'900 Projekten pro Jahr bei über 800 Kunden.

Oracle Centrally Managed Users 18/19c

Varianten zur zentraler Benutzerverwaltung von Oracle Datenbanken

Stefan Oehrli

@stefanoehrli

www.oradba.ch

Stefan Oehrli

Plattform Architekt, 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

www.oradba.ch

ORACLE ACE

Agenda

trivadis

- Übersicht Authentifizierung und Autorisierung
- Variante zur zentralen Benutzerverwaltung von Oracle Datenbanken
- Integration von Oracle Datenbanken 18c mit Active Directory
- CMU Konfiguration Live Demo
- Troubleshooting
- Abgrenzung Oracle EUS / CMU
- Überblick Trivadis LAB
- Fazit

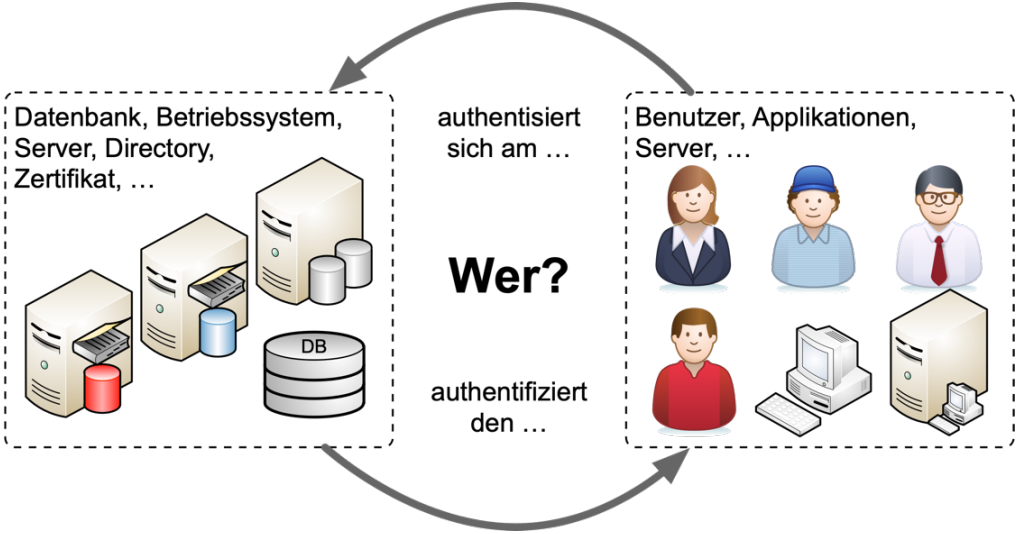
trivadis

Übersicht Authentifizierung und Autorisierung

Authentifizierung

trivadis

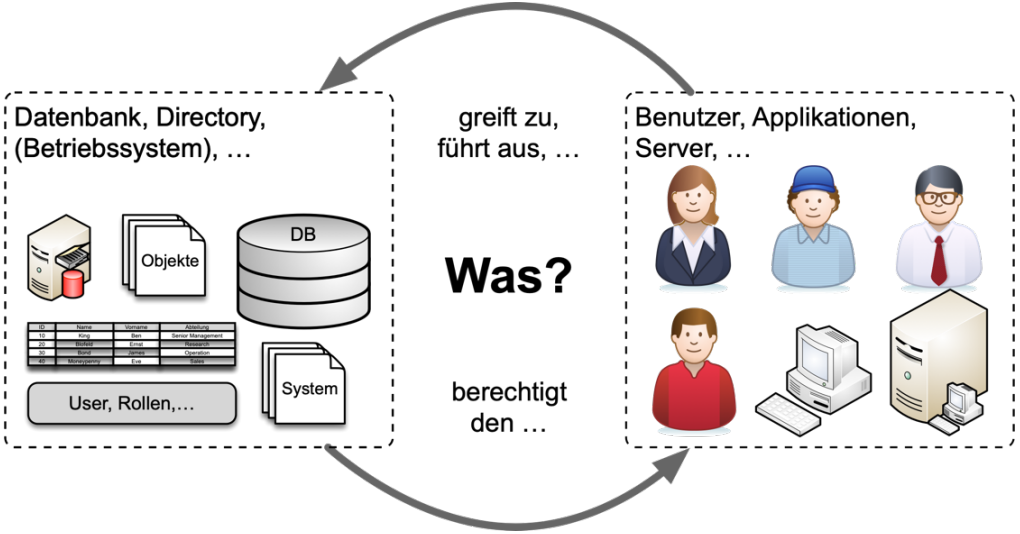
- Überprüfung der Identität einer Person, die auf Daten, Ressourcen oder Anwendungen zugreifen möchte.
- Person kann dabei ein Benutzer, ein Gerät oder eine Einheit sein.
- Die Validierung dieser Identität schafft eine Vertrauensbeziehung für weitere Interaktionen.



Autorisierung

trivadis

- Im weitesten Sinne eine Zustimmung oder Erlaubnis respektive die Einräumung von Rechten gegenüber einer Person.
- Die Zuweisung von Privilegien an Benutzer bzw. Benutzergruppen.
- Oracle kann Berechtigungen auf unterschiedlichen Ebenen erteilen.



Authentifizierungsmethoden

trivadis

- Datenbank Authentifizierung
  - Authentifizierung an der Datenbank mit Benutzername / Passworte
  - Datenbank prüft Password Hashes
  - je nach Version unterschiedliche Hashes und Protokoll Versionen.
- Datenbank Administratoren Authentifizierung
  - Authentifizierung SYSDBA, SYSOPER, SYSBACKUP, SYSRAC, SYSDG, SYSKM und SYSASM
  - Basiert auf OS Gruppen (lokal) oder Passwortdatei (remote)
  - Erlaubt administrative Tätigkeiten sowie die Authentifizierung bei gestoppter Datenbank
- Betriebssystem Authentifizierung
  - Authentifizierung anhand des Betriebssystem Benutzers
  - Abgabe der Verantwortung an das Betriebssystem

Authentifizierungsmethoden

trivadis

- Netzwerk / Starke Authentifizierung
  - Nutzung eines Netzwerkservices zu Authentifizierung von Benutzern
  - **Kerberos** Authentifizierung
  - **RADIUS** Authentifizierung
  - **SSL** respektive Zertifikatsbasierte Authentifizierung
- Verzeichnis basierte Authentifizierung
  - Verwaltung der Benutzer und Rollen / Gruppen in einem externen Verzeichnisdienst
  - Zwingend mit einem Oracle Directory
  - Oracle Enterprise User Security (EUS)
  - Oracle Centrally Managed User 18c (CMU)
  - Kombination mit Password-, Kerberos- oder SSL Authentifizierung

Spezielle Authentifizierungsmethoden

trivadis

- Proxy Authentifizierung
  - Authentifizierung mit alternativen Anmeldeinformationen
  - Benutzer X verbindet als Benutzer Y authentifiziert sich aber mit X
- NO Authentifizierung
  - mit Oracle 18c eingeführt
  - *Schema only* Accounts
  - Keine Authentifizierung und somit kein Logon möglich
  - Für Applikationsschemas
- Claim basierte Authentifizierung wie **SAML**, **OAuth**, etc. sowie **Two-Factor** Authentifizierung sind mit Oracle Datenbanken direkt nicht möglich.

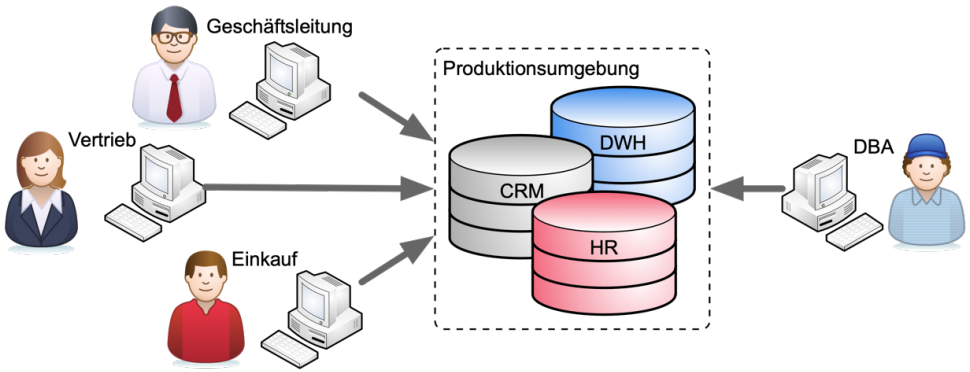
trivadis

Variante zur zentralen Benutzerverwaltung von Oracle Datenbanken

Herausforderung Benutzerverwaltung

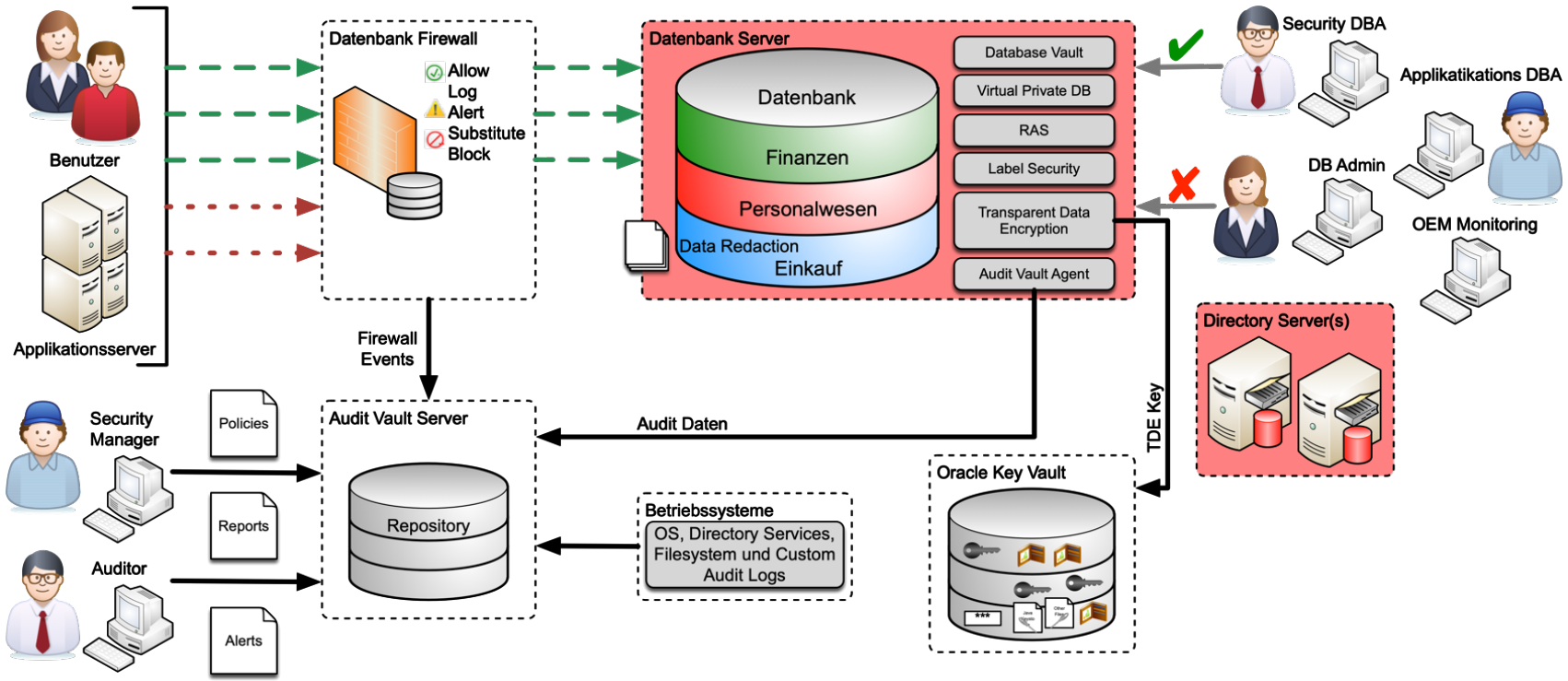
trivadis

- Wer greift wo auf welche Daten / Datenbank zu?
  - Authentifizierung und Autorisierung
  - Produktions-, Test und Entwicklungsumgebungen
- Wie werden die Berechtigungen verwaltet?
  - Individuell / dezentral durch Administratoren
  - Was passiert bei Mutationen (Funktionswechsel, Kündigungen etc.)
- Besteht ein Rollen Konzept?
  - Wird es auch umgesetzt?
- Redundanzen
- Integration mit Oracle Feature



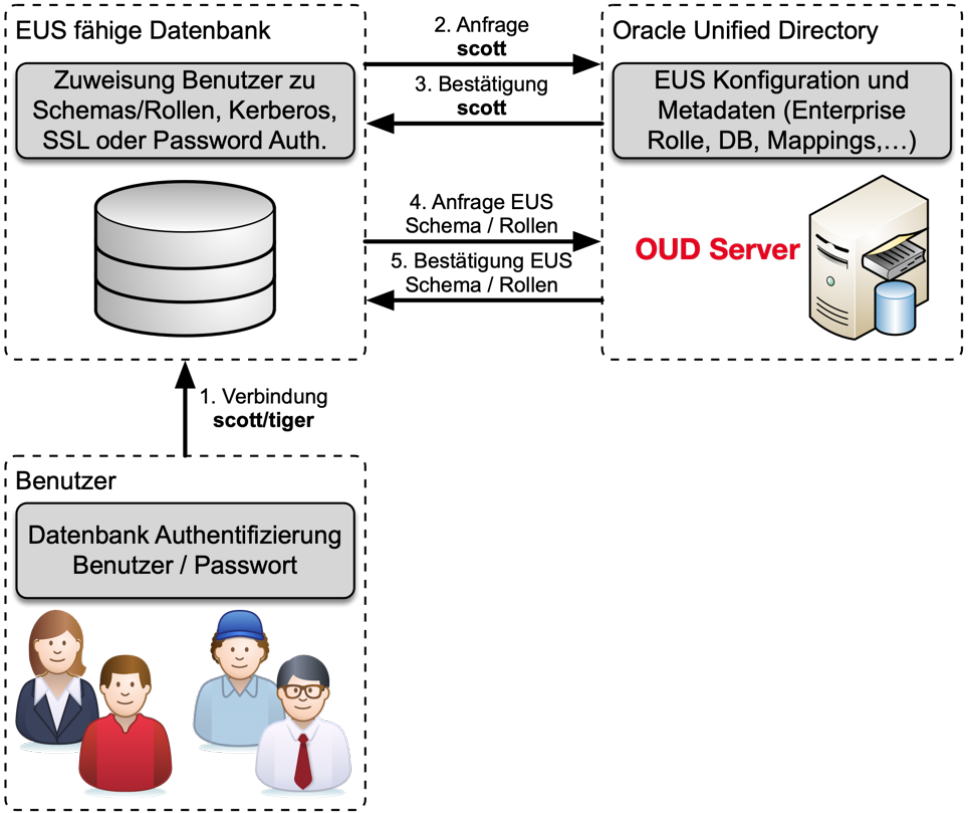
Maximum Data Security Architekture

trivadis



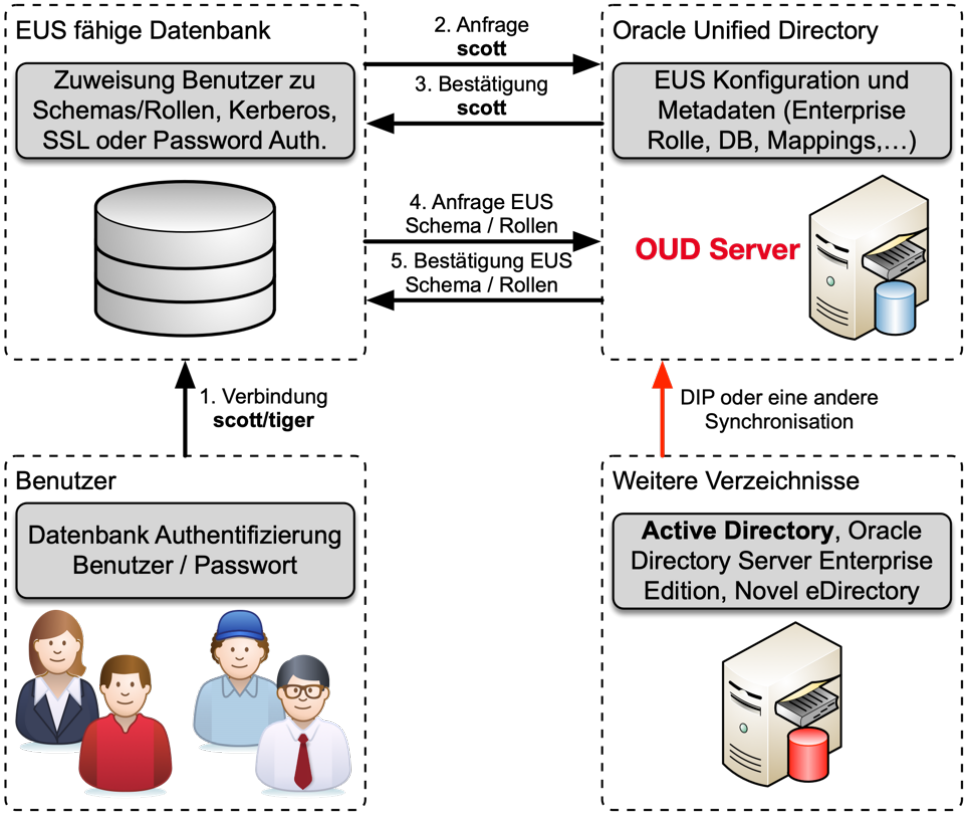
EUS mit Standalone Verzeichnis

trivadis



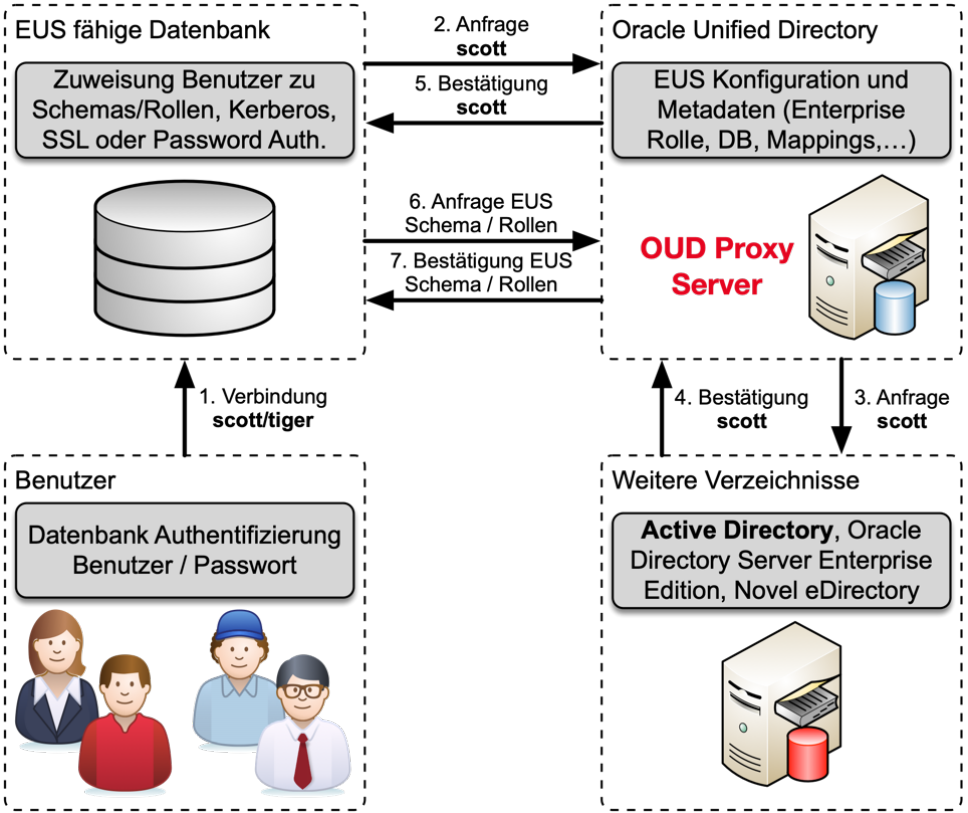
EUS mit DIP Integration

trivadis

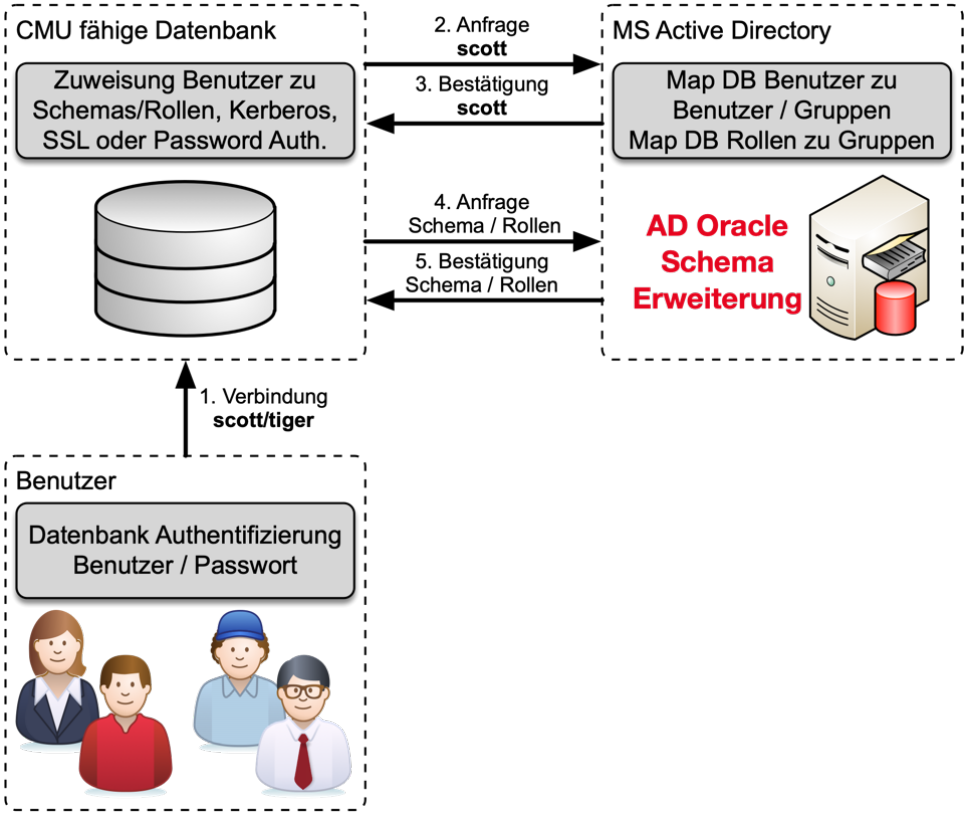


EUS mit Proxy Integration

trivadis



Integration mit CMU



trivadis

Integration von Oracle Datenbanken 18c mit AD

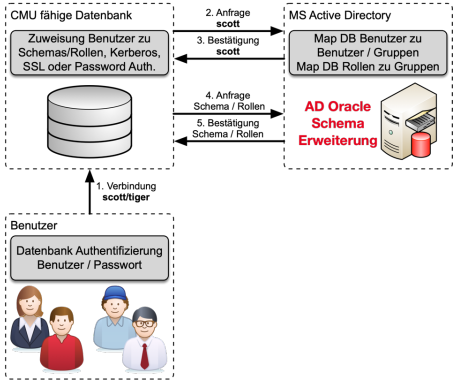
Integration von MS Active Directory

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

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

CMU Konfiguration
Live Demo

Live Demo

trivadis

- MS Active Directory Konfiguration
- SQLNet Konfiguration
- Datenbank Konfiguration
- Authentifizierung und Autorisierung

MS Active Directory Konfiguration

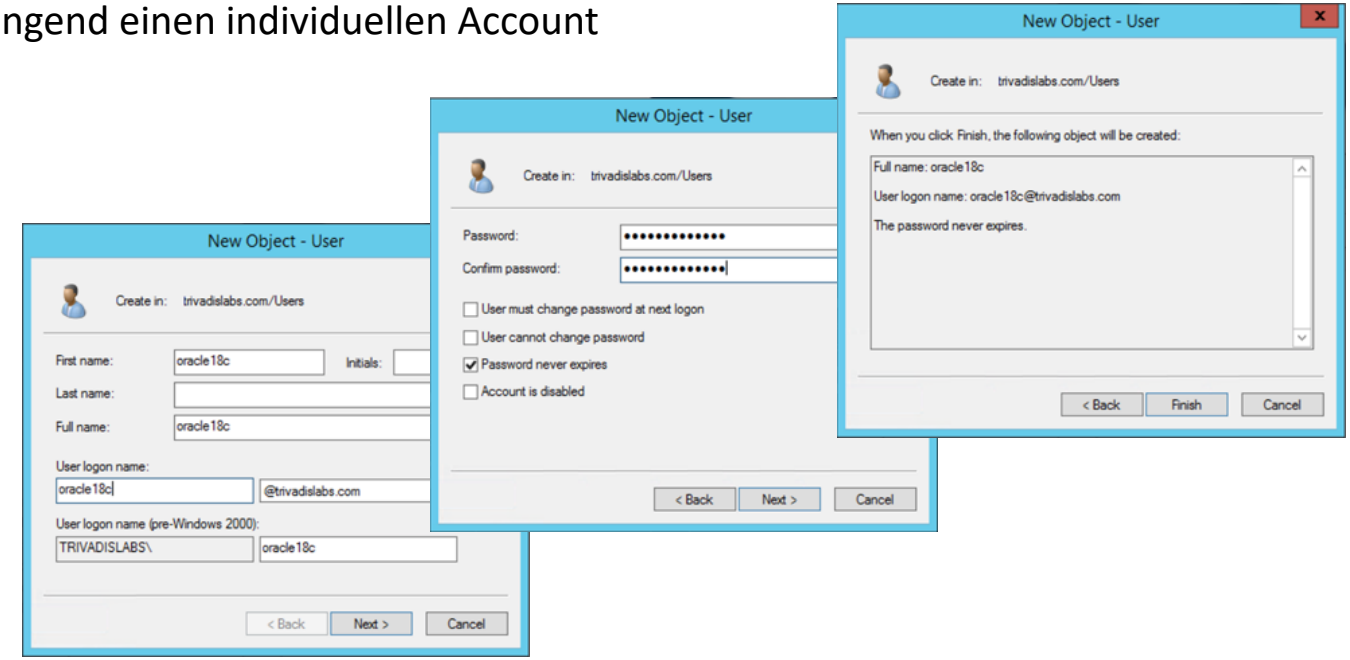
trivadis

- Die Datenbank benötigt Zugriff auf MS Active Directory
  - Leserechte für die Suchen von User / Gruppen
  - Schreibrechte für das Aktualisieren von Login Informationen
- 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



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

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
- Geht in der Zwischenzeit mit **regulärem** Connect String

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
- Abhängigkeit von der AD Struktur / Gruppen / Rollenkonzept

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
```

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

trivadis

Troubleshooting

Troubleshooting mit CMU

trivadis

- Hier hilft neben der Kontrolle der Anmeldeinformationen nur ein Trace
  - War das Passwort wirklich richtig?
  - MOS Note 352389.1 *Finding the source of failed login attempts*

```
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';
```

- Kontrolle der Trace files und suchen nach **kzlg** z.B `grep -i kzlg *.trc`

Troubleshooting mit CMU

trivadis

- ORA-01017 in allen möglichen und unmöglichen Situationen
- Alternativ die üblichen Trace Methoden für EUS, Kerberos etc.
  - MOS Note 783502.1 *EUS Authentication Fails With ORA-28030*
  - MOS Note 2470608.1 *Tracing CMU connection issues*
  - MOS Note 416946.1 *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 ist wie bei Kerberos und EUS schwierig

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

Troubleshooting mit CMU

trivadis

- Es gibt auch Fehler, die sind „offensichtlicher“
  - Manchmal aber auch nicht
- Allenfalls stimmen aber andere Punkte nicht z.B.
  - UPN ist falsch oder passt nicht zur DB => User@REALM
- 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

Abgrenzung Oracle EUS / CMU

Abgrenzung Oracle EUS / CMU

trivadis

Oracle Enterprise User Security

- Benötig eine zusätzliches Directory
  - Erhöhter Aufwand bezüglich Administration, Integration, Betrieb, …
  - Zusätzliche Lizenz (ODSP)

+ Unabhängigkeit im Bezug auf Basis Verzeichnisstruktur, Schema, Authentifizierung
+ Namensauflösung
+ Unterstützung unterschiedlicher Verzeichnisse
+ Umfangreiche Enterprise Features
  - Enterprise Rollen / User / Gruppen
  - Proxy und Admin User

Oracle Centrally Managed Users

- Keine Namensauflösung
- Nur mit MS Active Directory
  - Abhängigkeit MS AD Struktur
- Passwort Filter / Schema Erweiterung für Password Authentifizierung
- Eingeschränkte Features
  - Kein Proxy User, Enterprise Rollen, etc.

+ Keine zusätzliche Lizenzkosten
+ Keine zusätzliches Directory
+ Simple und einfach für einfachere Umgebungen

trivadis

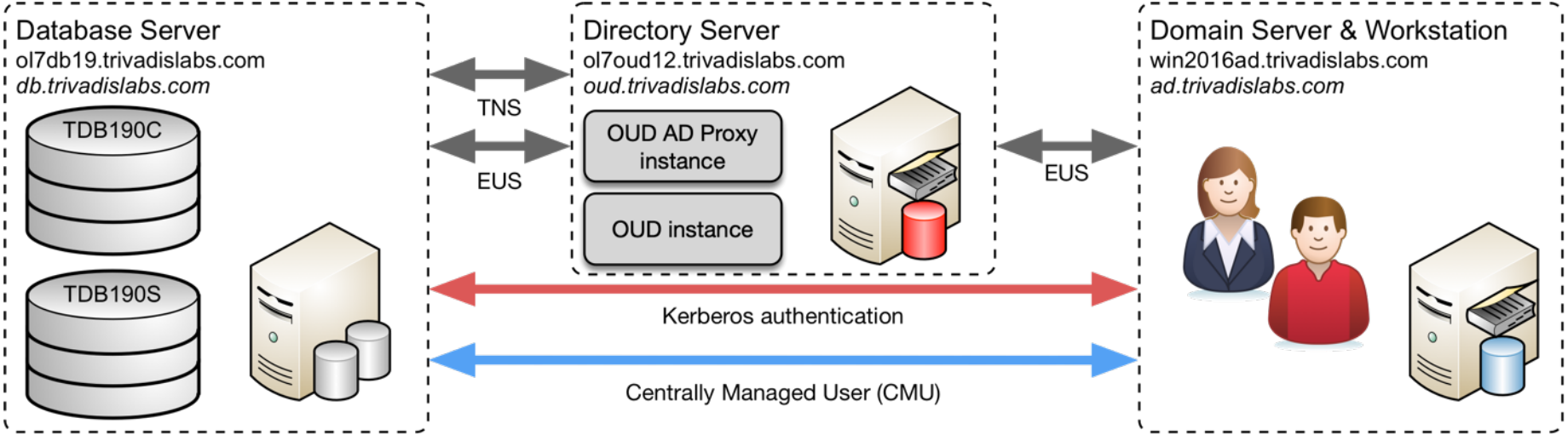
Überblick Trivadis LAB

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

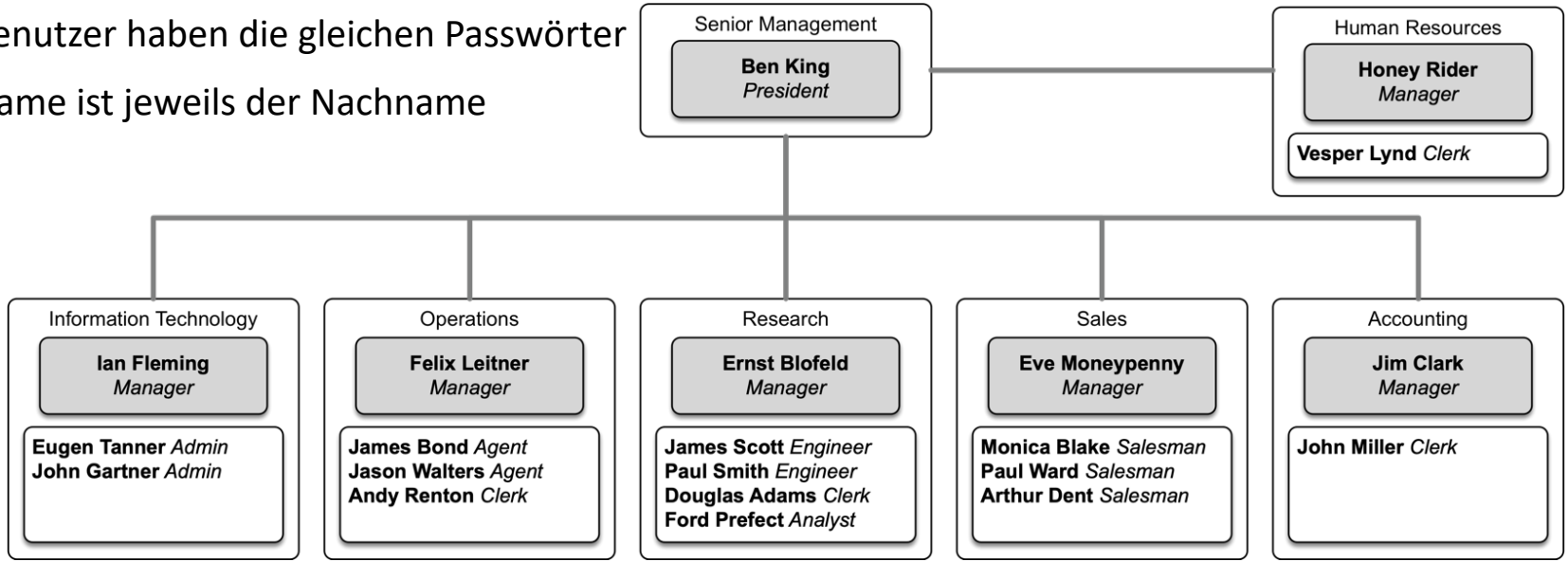
Trivadis LAB Demo Umgebung



Trivadis 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 ☺
  - Bug und Patches abhängig vom Release
- 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?
- Nutzung unterschiedlicher Authentifizierungsmethoden möglich und kombinierbar
  - Password Authentifizierung perfekt für die Integration in bestehende Anwendungen
  - Mit Kerberos oder SSL Authentifizierung SSO möglich, keine Anpassungen AD

Herausforderungen mit CMU

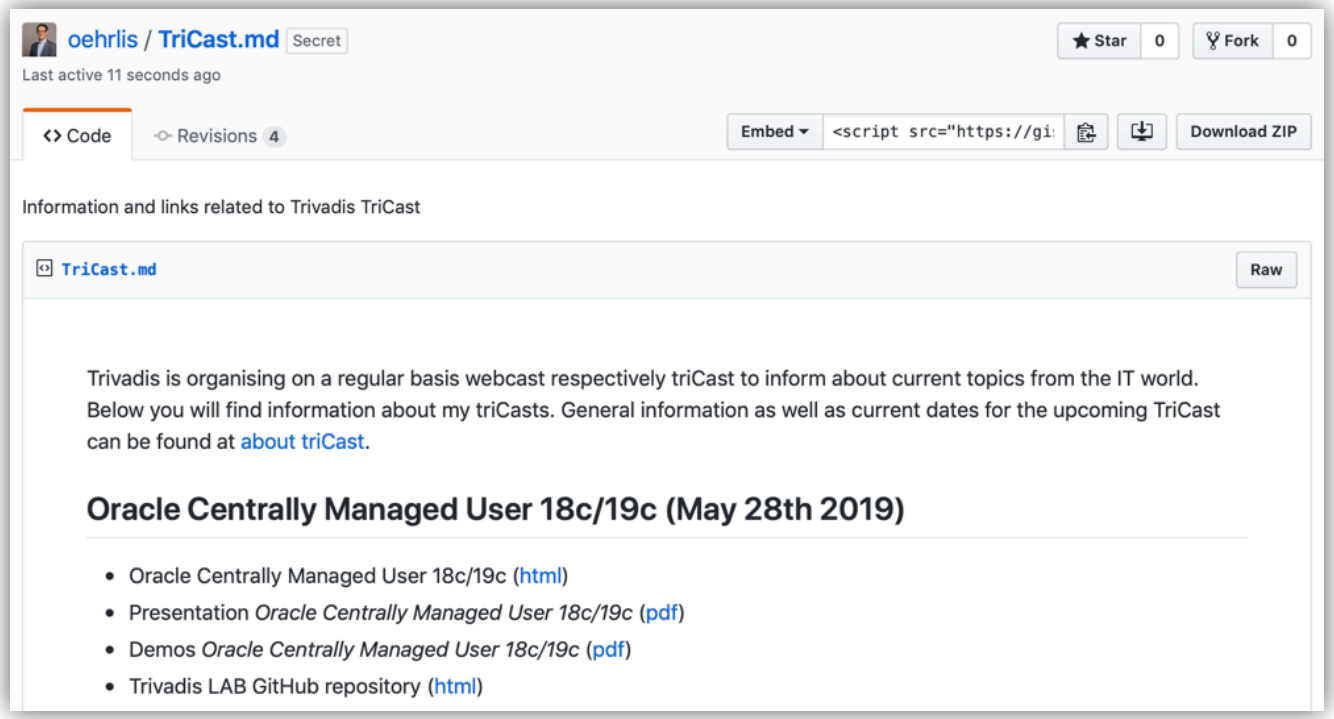
trivadis

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

Quicklinks

trivadis

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



Fragen?

trivadis

Stefan Oehrli
Senior Platform Architect

stefan.oehrli@trivadis.com

Fabian Karsch
Senior Marketing Specialist

fabian.karsch@trivadis.com

Fragen und Antworten...

Stefan Oehrli

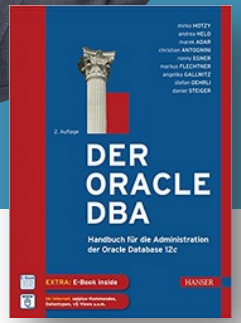
Solution Manager / Trivadis Partner

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.