



DOAG Schulungstag 2018

Übungen zum Workshop Oracle EUS mit OUD und AD Integration

15 November 2018, Version 0.5

*Trivadis AG
Sägereistrasse 29
8152 Glattbrugg
info@trivadis.com
+41 58 459 55 55*

Inhalt

1	Einleitung DOAG Schulungstag 2018	3
2	Datenbank Authentifizierung und Password Verifier	3
3	Kerberos Authentifizierung	3
4	Centrally Managed User 18c	5
5	Oracle Unified Directory	5
5.1	Einführung in Oracle Unified Directory	5
5.2	OOD Directroy Server und AD Proxy	5
5.3	Oracle Unified Directory, Hochverfügbarkeit und Backup & Recovery	5
6	Oracle Enterprise User Security	5
6.1	Übungen Oracle Enterprise User Security Teil 1	5
6.2	Übungen Oracle Enterprise User Security Teil 2	5
6.3	Troubleshooting Enterprise User Security	5
7	Zusammenfassung und Abschluss	6
7.1	Architektur	6
7.2	Oracle Datenbank Server	6
7.2.1	Trivadis BasEnv	7
7.2.2	Übungschema TVD_HR	8
7.3	Oracle Unified Directory Server	9
7.3.1	Trivadis OUD Base	9
7.4	MS Active Directory Server	9
7.4.1	AD Domain TRIVADISLAB	9
8	Links und Referenzen	9
8.1	OOD EUS Workshop	9
8.2	Oracle Dokumentation	10
8.3	Software und Tools	10
8.3.1	Betriebssystem und Virtualisierung	10
8.3.2	Oracle Datenbank Binaries	10
8.3.3	Oracle Unified Directory Binaries	11
8.3.4	Tools Active Directory Server	11

1 Einleitung DOAG Schulungstag 2018

Lorum larum lipsum

2 Datenbank Authentifizierung und Password Verifier

DB authentifizierung ist wichtig. . .

3 Kerberos Authentifizierung

- Einrichten keytab file
- DB user erstellen
- okinit auf db server
- kerkberos login auf DB server
- User informationen
- kerberos login remote vom AD domain
- bestehendne benutzer anpassen
- Kerberos mit Proxy kombinieren

Kurs Agenda Einleitung DB Authentifizierung und Password Verifier Einführung Übungsumgebung - wie ist die Umgebung aufgebaut (Architektur, Software, Zugriff) - TRIVADISLAB Domain - Firma Born Inc. - passwörter - Zugriff via ssh / putty - Zugriff via Remote Desktop - Trivadis Basenv und OUD Base Übungen Password Verifier Kerberos Authentifizierung Übungen Kerberos Authentifizierung

User anlegen

krb5 file auf dem server anlegen #####krb5.conf DB Server

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

[realms]
TRIVADISLABS.COM = {
    kdc = ad.trivadislabs.com
    admin_server = ad.trivadislabs.com
```

```
}

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

sqlnet.ora file

```
#####
# Kerberos Configuration
#####
SQLNET.AUTHENTICATION_SERVICES = (BEQ,KERBEROS5)
SQLNET.FALLBACK_AUTHENTICATION = TRUE
SQLNET.KERBEROS5_KEYTAB = /u00/app/oracle/network/admin/db.trivadislabs.
    com.keytab
SQLNET.KERBEROS5_REALMS = /u00/app/oracle/network/admin/krb.realms
SQLNET.KERBEROS5_CC_NAME = /u00/app/oracle/network/admin/krb5cache
SQLNET.KERBEROS5_CONF = /u00/app/oracle/network/admin/krb5.conf
SQLNET.KERBEROS5_CONF_MIT=TRUE
SQLNET.AUTHENTICATION_KERBEROS5_SERVICE = oracle
```

Create the keytab file

```
ktpass.exe -princ oracle/db.trivadislabs.com@TRIVADISLABS.COM \
    -mapuser db.trivadislabs.com -pass manager \
    -crypto ALL -ptype KRB5_NT_PRINCIPAL \
    -out C:\u00\app\oracle\network\db.trivadislabs.com.keytab
```

```
ktpass.exe -princ oracle/db.trivadislabs.com@TRIVADISLABS.COM -mapuser db.
    trivadislabs.com -pass manager -crypto ALL -ptype KRB5_NT_PRINCIPAL -
    out C:\u00\app\oracle\network\db.trivadislabs.com.keytab
```

Kaffeepause Vormittag Kerberos Troubleshooting - was gibts so für Probleme - Namesauflösung und DNS Probleme - Zeit Differenzen - Keytab File falsch z.B. falscher Algorithmus, vno Nummer etc - - welche Möglichkeiten für die Problemanalyse stehen zur Verfügung - SQLNet Trace - Wireshark - TRACE File

4 Centrally Managed User 18c

Generell verschiedenens

Übung Centrally Managed User 18c

Was neues in 18c

5 Oracle Unified Directory

5.1 Einführung in Oracle Unified Directory

OUD ist super

5.2 OUD Directroy Server und AD Proxy

gibt beides DS und Proxy

5.3 Oracle Unified Directory, Hochverfügbarkeit und Backup & Recovery

halt wichtig

6 Oracle Enterprise User Security

Allgemein

6.1 Übungen Oracle Enterprise User Security Teil 1

Kaffeepause Nachmittag

6.2 Übungen Oracle Enterprise User Security Teil 2

Oracle Unified Directory, Hochverfügbarkeit und Backup & Recovery

6.3 Troubleshooting Enterprise User Security

fehler gibt es immer

7 Zusammenfassung und Abschluss

Das war's mit Tricks und Gägs, tschouzäme # Demo und Übungsumgebung

7.1 Architektur

Für die praktischen Arbeiten im Rahmen des DOAG 2018 Schulungstages, steht pro zweiter Team eine einfach Testumgebung zur Verfügung. Die Umgebung läuft für die Dauer der Schulung in der [Oracle Ravello Cloud](#) und besteht, wie in Abbildung 1 ersichtlich aus folgenden Servern respektive VMs:

- **db.trivadislabs.com** Oracle Datenbank Server mit Oracle 12c R2 sowie 18c
- **oud.trivadislabs.com** Oracle Directory Server mit Oracle Unified Directory 12c
- **ad.trivadislabs.com** MS Windows Server 2012 R2 mit Active Directory

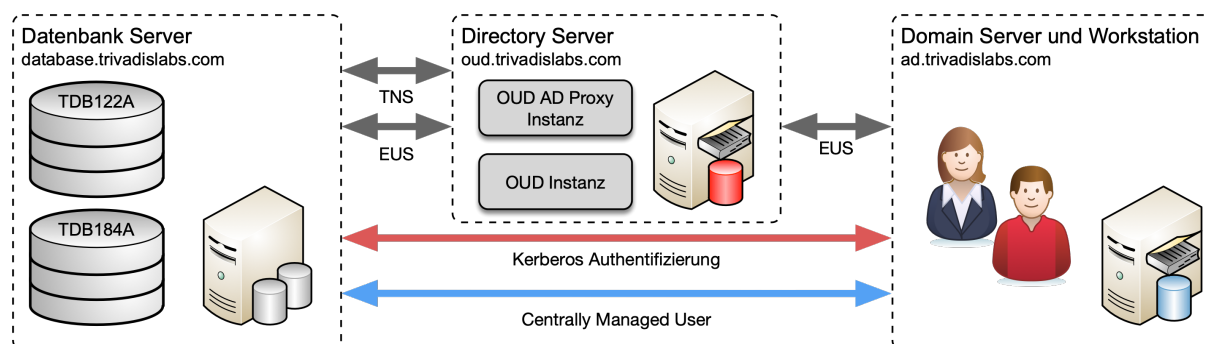


Abb. 1: Architektur Schulungsumgebung

Die Umgebung ist soweit vorbereitet, dass direkt mit den Übungen gestartet werden kann.

Die zentrale Benutzerverwaltung mit *Oracle Centrally Managed Users* oder *Oracle Enterprise User Security* sind komplexe Themen, welche nicht abschliessend am Schulungstag diskutiert werden können. Aus diesem Grund gibt es für das Selbststudium die Möglichkeit, eine Testumgebung analog dem Schulungstag aufzubauen. Diese Umgebung wird Skript gestützt mit [Vagrant](#) auf [Virtualbox](#) aufgebaut. Man benötigt lediglich die entsprechenden Software Images für die Oracle Datenbank 12c R2 + 18c, Oracle Unified Directory sowie die Umgebungsskripte. Anschliessend lässt sich die Umgebung nahezu voll automatisch aufbauen. Eine entsprechende Anleitung für den Aufbau der Trivadis LAB Umgebung sowie die dazugehörigen *Vagrant Files*, *Skripte* etc. findet man im GitHub Repository [oehrli/trivadislabs.com](https://github.com/oehrli/trivadislabs.com).

7.2 Oracle Datenbank Server

Der Oracle Datenbank Server ist wie folgt konfiguriert:

- **Betriebssystem** : Oracle Enterprise Linux Server Release 7.5

- **Oracle Datenbank Software :**
 - Oracle 12c Release 2 Enterprise Edition (12.2.0.1) mit Release Update vom Oktober 2018
 - Oracle 18c Enterprise Edition (18.4.0.0) mit Release Update vom Oktober 2018
- **Oracle Datenbanken :**
 - **TDB122A** Oracle 12cR2 Enterprise Edition Single Instance für die Übungen mit EUS
 - **TDB184A** Oracle 18c Enterprise Edition Single Instance für die Übungen mit CMU
- **Betriebssystem Benutzer :**
 - oracle / TW4,36BAK3
 - root / 27.2VNCN4z
- **Datenbank Benutzer :**
 - sys / manager
 - system / manager
 - scott / tiger
 - tvd_hr / tvd_hr

7.2.1 Trivadis BasEnv

Das Trivadis Base Environment (TVD-Basenv™) ermöglicht einfaches Navigieren in der Directory Struktur und zwischen den verschiedenen Datenbanken. In der folgenden Tabelle sind die Aliases für den OS Benutzer *oracle* aufgelistet, welche am häufigsten verwendet werden.

Alias Name	Beschreibung
TDB122A	setzt die Umgebung im Terminal für die Datenbank TDB122A
TDB184A	setzt die Umgebung im Terminal für die Datenbank TDB184A
cda	zum Admin Verzeichnis der aktuell gesetzten Datenbank
cdob	zum Oracle Base
cdh	zum Oracle Home
cdt	zum TNS_ADMIN
sqh	startet SQLPlus mit „sqlplus / as sysdba“ inklusive Befehlshistory
u	Statusanzeige für alle Oracle Datenbanken und Listener (z.B. open, mount)
sta	Statusanzeige für die aktuell gesetzte Datenbank
via	öffnet das Alertlog der aktuell gesetzten Datenbank in vi
taa	öffnet das Alertlog der aktuell gesetzten Datenbank mit <code>tail -f</code>

Die Installation ist nach dem OFA (Optimal Flexible Architecture) Standard vorgenommen worden – Beispiel für die Installation auf der Datenbank-VM für die Datenbank - TDB122A:

Mount Point / Directory	Beschreibung
<code>/u00/app/oracle/admin/TDB122A/adump</code>	Oracle Audit Files
<code>/u00/app/oracle/admin/TDB122A/backup</code>	Oracle Backup
<code>/u00/app/oracle/admin/TDB122A/dpdump</code>	Data Pump Dateien
<code>/u00/app/oracle/admin/TDB122A/etc</code>	Oracle Backup Konfig Dateien
<code>/u00/app/oracle/admin/TDB122A/log</code>	Log Dateien (z.B. Backup, Export, etc.)
<code>/u00/app/oracle/admin/TDB122A/pfile</code>	Parameter- und Password-Datei
<code>/u00/app/oracle/admin/TDB122A/wallet</code>	Oracle Wallet
<code>/u00/app/oracle/etc</code>	oratab und diverse Konfigurationsdateien
<code>/u00/app/oracle/local/dba</code>	Environment Tools (TVD-Basenv)
<code>/u00/app/oracle/network/admin</code>	Oracle Net Konfigurationsdateien
<code>/u00/app/oracle/product/12.2.0.1</code>	Oracle 12.2.0.1 Home
<code>/u00/app/oracle/product/18.4.0.0</code>	Oracle 18.4.0.0 Home
<code>/u01/oradata/TDB122A</code>	Datenbank Dateien, Redo Log Files, CTL
<code>/u02/oradata/TDB122A</code>	Redo Log Files, CTL
<code>/u02/fast_recovery_area/TDB122A</code>	Fast Recovery Area

7.2.2 Übungschema TVD_HR

In den Datenbanken ist neben dem Scott Demo Schema zusätzlich das Beispiel Schema *TVD_HR*. Das Schema *TVD_HR* basiert auf dem bekannten Oracle *HR* Beispiel Schema. Der wesentliche Unterschied zum regulären *HR* Schema ist, dass die Abteilungen sowie Mitarbeiter den Mitarbeitern im Active Directory entspricht.

Erklärung zu den Tabellen basierend auf den Kommentaren vom *HR* Schema:

- **REGIONS** Tabelle, welche Regionsnummern und -namen enthält. Verweise auf die Tabelle *LOCATION*.
- **LOCATIONS** Tabelle, die die spezifische Adresse eines bestimmten Büros, Lagers und/oder Produktionsstandortes eines Unternehmens enthält. Speichert keine Adressen von Kundenstandorten.

- **DEPARTMENTS** Tabelle, die Details zu den Abteilungen zeigt, in denen die Mitarbeiter arbeiten. Verweise auf Standorte, Mitarbeiter und Job History Tabellen.
- **JOB_HISTORY** Tabelle, in der die Beschäftigungshistorie der Mitarbeiter gespeichert ist. Wenn ein Mitarbeiter innerhalb der Stelle die Abteilung wechselt oder die Stelle innerhalb der Abteilung wechselt, werden neue Zeilen in diese Tabelle mit alten Stelleninformationen des Mitarbeiters eingefügt. Verweise auf Tabellen mit Jobs, Mitarbeitern und Abteilungen.
- **COUNTRIES** Tabelle. Verweise mit der Tabelle der Standorte.
- **JOBS** Tabelle mit Jobbezeichnungen und Gehaltsgruppen. Verweise auf Mitarbeiter und Job History Tabelle.
- **EMPLOYEES** Tabelle. Verweise mit Abteilungen, Jobs, Job History Tabellen. Enthält einen Eigenbezug.

7.3 Oracle Unified Directory Server

Generell wichtig

7.3.1 Trivadis OUD Base

Wie wo was ist basenv

7.4 MS Active Directory Server

AD VM ist hier

```
TRIVADISLABS\Administrator  
: qp8F+82Pe9
```

7.4.1 AD Domain TRIVADISLAB

Die Domain

8 Links und Referenzen

8.1 OUD EUS Workshop

Unterlagen und Skripte zum Workshop

- Übungsskripte zum DOAG Schulungstag [doag2018](#)
- Vagrant Setup zum Aufbau der Trivadis LAB Umgebung [oehrlis/trivadislabs.com](#)
- Setup Skripte für die Konfiguration der Umgebung (Cloud, Vagrant, Docker) [oehrlis/oradba_init](#)
- OUD Base Umgebungsskripte für Oracle Unified Directory [oehrlis/oudbase](#)

8.2 Oracle Dokumentation

- Oracle Online Dokumentation 18c <https://docs.oracle.com/en/database/oracle/oracle-database/18/books.html>
- Oracle Enterprise User Security <https://docs.oracle.com/en/database/oracle/oracle-database/18/dbimi/index.html>
- Oracle Centrally Managed User https://docs.oracle.com/en/database/oracle/oracle-database/18/dbseg/integrating_mads_with_oracle_database.html
- Oracle EUSM Utility <https://docs.oracle.com/en/database/oracle/oracle-database/18/dbimi/enterprise-user-security-manager-eusm-command-summary.html>

8.3 Software und Tools

8.3.1 Betriebssystem und Virtualisierung

- Oracle VM Virtualbox [virtualbox](#)
- HashiCorp Vagrant [vagrant](#)
- Oracle Enterprise Linux 7.5
 - Oracle Vagrant Boxes [vagrant image](#). Predefined Image von Oracle für die Nutzung mit Virtualbox und Vagrant. Das Vagrant Image wird bei einem [vagrant up](#) falls nicht vorhanden direkt herunter geladen.
 - Oracle Software Delivery Cloud [iso](#). Basis Setup iso File, falls individuell ein Oracle Linux Server installiert werden soll.
- Microsoft Windows Server 2016
 - Vagrant Box [StefanScherer/windows_2016](#). Vagrant Image aus der Vagrant Cloud. Erstellt von Stefan Scherer für die Nutzung mit Virtualbox und Vagrant. Das Vagrant Image wird bei einem [vagrant up](#) falls nicht vorhanden direkt herunter geladen.
 - Evaluation 2016 [iso](#). Basis Setup iso File, falls individuell ein Windows Server installiert werden soll.
- Trivadis BasEnv Test [basenv-18.05.final.b.zip](#)

8.3.2 Oracle Datenbank Binaries

- Oracle Base Releases 12c Release 2 und 18c [Oracle Technology Network](#)

- Oktober Critical Patch Update Oracle Database 18c
 - DATABASE RELEASE UPDATE 18.4.0.0.0 [28655784](#)
 - OJVM RELEASE UPDATE: 18.4.0.0.181016 [28502229](#)
- Oktober Critical Patch Update Oracle Database 12c Release 2
 - DATABASE OCT 2018 RELEASE UPDATE 12.2.0.1.181016 [28662603](#)
 - OJVM RELEASE UPDATE 12.2.0.1.181016 [28440725](#)
- Oracle OPatch Utility 12.2.0.1.13 for DB 12.2.0.x and DB 18.x [6880880](#)

8.3.3 Oracle Unified Directory Binaries

- Java Server 1.8 u192 [28414856](#)
- Oracle Fusion Middleware 12.2.1.3.0 Oracle Unified Directory [26270957](#)
- OUD BUNDLE PATCH 12.2.1.3.0(ID:180829.0419) [28569189](#)
- Oracle Fusion Middleware 12.2.1.3.0 Fusion Middleware Infrastructure [26269885](#)
- WLS PATCH SET UPDATE 12.2.1.3.181016 Oracle WLS 12.2.1.3.0 [28298734](#)
- OPatch Utility für WLS [28186730](#)
- OUD Base Umgebungsskripte für Oracle Unified Directory [oehrlis/oudbase](#)

8.3.4 Tools Active Directory Server

- Oracle Clients
 - Oracle Clients [Oracle Technology Network](#)
 - Oracle Instant Clients [Oracle Technology Network](#)
- Apache Directory Studio LDAP Browser [Home](#)
- Putty SSH Utility [Putty Home](#)
- WinSCP SFTP client und FTP Client für Microsoft Windows [WinSCP Home](#)