



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	Übungen: Datenbank Authentifizierung und Password Verifier	4
2.1	Überprüfung der aktuellen Password Verifier	4
2.2	Anpassen der Password Verifier	6
2.3	Zusatz Aufgaben	8
3	Übungen: Kerberos Authentifizierung	8
3.1	Service Principle und Keytab Datei	9
3.2	SQLNet Konfiguration	9
3.3	Kerberos Authentifizierung	9
3.4	Zusatz Aufgaben	9
4	Übungen: Centrally Managed User 18c	10
5	Übungen: Oracle Unified Directory	11
5.1	Einführung in Oracle Unified Directory	11
5.2	OID Directroy Server und AD Proxy	11
5.3	Oracle Unified Directory, Hochverfügbarkeit und Backup & Recovery	11
6	Übungen: Oracle Enterprise User Security	11
6.1	Übungen Oracle Enterprise User Security Teil 1	11
6.2	Übungen Oracle Enterprise User Security Teil 2	11
6.3	Troubleshooting Enterprise User Security	11
7	Zusammenfassung und Abschluss	11
8	Demo- und Workshopumgebung	12
8.1	Architektur	12
8.2	Oracle Datenbank Server	12
8.3	Oracle Unified Directory Server	15
8.4	MS Active Directory Server	17
9	Links und Referenzen	19
9.1	OID EUS Workshop	19
9.2	Oracle Dokumentation	19
9.3	Software und Tools	20

1 Einleitung DOAG Schulungstag 2018

Im Rahmen des Workshop besteht die Gelegenheit verschiedene Themen am praktischen Beispiel zu vertiefen. Dazu gibt es zu jedem Kapitel Aufgaben, welche nach Anleitung oder individuell auf einer Testumgebung umgesetzt werden können. Die Testumgebung besteht, wie man in der folgenden Abbildung sehen kann, jeweils aus drei virtuellen Systemen. Pro zweier Team steht jeweils eine entsprechende Testumgebung zur Verfügung.

Eine Umgebung besteht jeweils aus 3 VM's * DB Server mit Oracle 12.2 und 18c * OUD Server mit OUD 12.1.2.3 * Windows Server 2012 R2 mit MS Active Directory

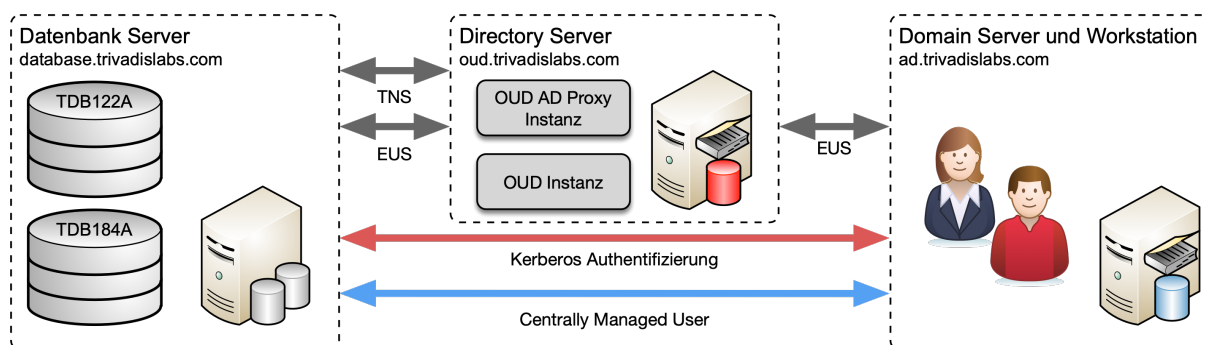


Abb. 1: Architektur Schulungsumgebung

Für die Zeitdauer des DOAG Schulungstages wurden diese Testumgebungen in der Oracle Ravello Cloud aufgebaut. Der Zugriff erfolgt direkt mit SSH (Linux VM's) oder Remote Desktop (Windows VM) vom eigenen Laptop. Zuweisung der Testumgebung erfolgt durch den Referenten.

Wichtigsten Login Informationen im Überblick:

- Datenbank Server (Linux VM)
 - **Host Name** : db.trivadislabs.com
 - **Interne IP Adresse** : 10.0.0.3
 - **Externe IP Adresse** : gemäss Liste
- Directory Server (Linux VM)
 - **Host Name** : oud.trivadislabs.com
 - **Interne IP Adresse** : 10.0.0.5
 - **Externe IP Adresse** : gemäss Liste
- Active Directory Server (Windows VM)
 - **Host Name** : ad.trivadislabs.com
 - **Interne IP Adresse** : 10.0.0.4
 - **Externe IP Adresse** : gemäss Liste
- Benutzer und Passwörter
 - root / gemäss Referent oder SSH Key

- oracle / gemäss Referent oder SSH Key
- sys / manager
- system / manager
- TRIVADISLABS\Administrator / gemäss Referent
- Allgemein AD User ist Nachname/LAB01schulung

Im Kapitel [Demo und Übungsumgebung](#) wird die Testumgebung etwas ausführlicher beschrieben. Zusätzlich besteht die Möglichkeit, selber eine eingene Testumgebung aufzubauen. Hierzu gibt es ein GitHub Repository [oehrli/trivadislabs.com](https://github.com/oehrli/trivadislabs.com) mit entsprechender Dokumentation, Scripts, Vagrant Files etc. um die Trivadis LAB Umgebung basierend auf Oracle [Virtualbox](#) und [vagrant](#) nahezu vollautomatisch lokal aufzubauen.

2 Übungen: Datenbank Authentifizierung und Password Verifier

Übungsziele: Kennenlernen der Übungsumgebung, BasEnv sowie der Datenbanken. Festigen der Kenntnisse im Bereich Passwort Authentifizierung und Password Hashes.

Arbeitsumgebung für die Übung * **Server:** db.trivadislabs.com * **DB:** TDB122A oder TDB184A

Die folgenden Aufgaben und Beispiele werden auf der DB TDB184A durchgeführt. Grundsätzlich können diese aber auch auf TDB122A ausgeführt werden.

2.1 Überprüfung der aktuellen Password Verifier

1. Prüfen was aktuell für Passwort Hashes in der Datenbank vorhanden sind. Welche Hashes gibt es? Wieso sind bei gewissen Benutzer keine Angaben in *password_versions*?

```
set linesize 120 pagesize 200
col USERNAME for a25
SELECT username, password_versions FROM dba_users;
```

2. Prüfen wie die VIEW *dba_users* auf die Information zu *password_versions* kommt. Im Code zum View *dba_users* findet man entsprechende *decode* Funktionen wo auf die Spalten *u.password* und *u.spare4* zugegriffen wird.

```
set linesize 120 pagesize 200
set long 200000
SELECT text FROM dba_views WHERE view_name='DBA_USERS';
```

3. Was für Passwort Hashes hat der Benutzer SCOTT effektiv?

```
set linesize 120 pagesize 200
col password for a16
col spare4 for a40
SELECT password, spare4 FROM user$ WHERE name='SCOTT';
```

4. Kontrolle was in der Datei `sqlnet.ora` für die Parameter `*ALLOWED_LOGON_VERSION_*` definiert wurde. Verwenden sie alternative `cat`, `less`, `more` oder `vi` um den Inhalt von `sqlnet.ora` anzuzeigen.

```
less $cdn/admin/sqlnet.ora

cat $cdn/admin/sqlnet.ora|grep -i ALLOWED_LOGON_VERSION
```

5. Prüfen was von SQLNet effektiv verwendet wird.

- Einschalten des SQLNet Tracing auf der Client Seite. Setzen von `DIAG_ADR_ENABLED` und `TRACE_LEVEL_CLIENT`. Anbei manuell mit `vi` oder alternativ direkt mit `sed` ersetzen lassen.

```
vi $cdn/admin/sqlnet.ora
DIAG_ADR_ENABLED=OFF
TRACE_LEVEL_CLIENT=SUPPORT
```

```
sed -i "s|DIAG_ADR_ENABLED.*|DIAG_ADR_ENABLED=OFF|" $cdn/admin/sqlnet.ora
sed -i "s|TRACE_LEVEL_CLIENT.*|TRACE_LEVEL_CLIENT=SUPPORT|" $cdn/admin/
sqlnet.ora
```

- Löschen allfälliger alten Trace files.

```
rm $cdn/trc/sqlnet_client_*.trc
```

- Verbinden als Benutzer Scott

```
sqlplus scott/tiger
```

```
show user
```

- Kontrolle des Trace Files. Was ist für ALLOWED_LOGON_VERSION gesetzt? Falls nichts gesetzt ist, was für ein Wert gilt?

```
ls -rtl $cdn/trc
```

```
less $cdn/trc/sqlnet_client_*.trc
```

```
grep -i ALLOWED_LOGON_VERSION $cdn/trc/sqlnet_client_*.trc
```

- Tracing wieder ausschalten.

```
vi $cdn/admin/sqlnet.ora
```

```
DIAG_ADR_ENABLED=ON
```

```
TRACE_LEVEL_CLIENT=OFF
```

```
sed -i "s|DIAG_ADR_ENABLED.*|DIAG_ADR_ENABLED=ON|" $cdn/admin/sqlnet.ora
```

```
sed -i "s|TRACE_LEVEL_CLIENT.*|TRACE_LEVEL_CLIENT=OFF|" $cdn/admin/sqlnet.ora
```

2.2 Anpassen der Password Verifier

1. Löschen des Oracle 12c Password Hash vom Benutzer Scott. Respektive explizites setzen des 11g Hashes.

```
SELECT spare4 FROM user$ WHERE name='SCOTT';
```

```
set linesize 170
```

```
col 11G_HASH for a62
```

```
SELECT
```

```
    REGEXP_SUBSTR(spare4,'(S:[[:alnum:]]+)') "11G_HASH"
```

```
FROM user$ WHERE name='SCOTT';
```

```
col 12C_HASH for a162
SELECT
    REGEXP_SUBSTR(spare4,'(T:[[:alnum:]]+)') "12C_HASH"
FROM user$ WHERE name='SCOTT';

ALTER USER scott IDENTIFIED BY VALUES 'S:54
A0B23AE639D4E0E22963A65A380DD496B8FCB65D1A5F9CC910EE625D8C';
```

2. Kontrolle der *password_versions* vom Benutzer *SCOTT*.

```
col username for a30
SELECT username,password_versions FROM dba_users WHERE username='SCOTT';
```

3. Anpassen des SQLNet Parameter *ALLOWED_LOGON_VERSION_SERVER* uns setzen des 12a Authentifizierungsprotokolls.

```
sed -i "s|#SQLNET.ALLOWED_LOGON_VERSION_SERVER.*|SQLNET.
ALLOWED_LOGON_VERSION_SERVER=12a|" $cdn/admin/sqlnet.ora
sed -i "s|#SQLNET.ALLOWED_LOGON_VERSION_SERVER.*|SQLNET.
ALLOWED_LOGON_VERSION_SERVER=12a|" $cdn/admin/sqlnet.ora
```

4. Als User Scott verbinden. Kann man sich überhaupt verbinden?

```
sqlplus scott/tiger

show user
```

5. Anpassen des SQLNet Parameter *ALLOWED_LOGON_VERSION_CLIENT* uns setzen des 11 Authentifizierungsprotokolls.

```
sed -i "s|#ALLOWED_LOGON_VERSION_CLIENT.*|SQLNET.
ALLOWED_LOGON_VERSION_CLIENT=11|" $cdn/admin/sqlnet.ora
sed -i "s|#SQLNET.ALLOWED_LOGON_VERSION_CLIENT.*|SQLNET.
ALLOWED_LOGON_VERSION_CLIENT=11|" $cdn/admin/sqlnet.ora
```

6. Als User Scott verbinden. Kann man sich überhaupt verbinden?

```
sqlplus scott/tiger  
  
show user
```

7. Was passiert wenn man als *SYS* das Passwort von *SCOTT* neu setzt? Welcher Passwort Hash hat *SCOTT* nun?

```
connect / as sysdba  
  
ALTER USER scott IDENTIFIED BY tiger;  
  
set linesize 120 pagesize 200  
col USERNAME for a25  
SELECT username, password_versions FROM dba_users WHERE username='SCOTT';
```

2.3 Zusatz Aufgaben

Falls noch Zeit übrig ist, können Sie noch folgende Aufgaben lösen:

- Setzen von *ALLOWED_LOGON_VERSION_CLIENT* und *ALLOWED_LOGON_VERSION_SERVER* auf Werte kleiner 11 z.B 10, 9 oder 8. Was bekommt der Benutzer *SCOTT* für Passwort Hashes wenn man als *SYS* das Passwort mit *ALTER USER* neu setzt?
- Welches Passwort wird beim Login verwendet? Sie können das Prüfen indem sie ein

3 Übungen: Kerberos Authentifizierung

Übungsziele: Konfiguration der Kerberos Authentifizierung für die DB TDB122A und TDB184. Erstellen eines Benutzers mit Kerberos Authentifizierung sowie erfolgreichem Login lokal (Linux VM) und remote (Windows VM).

3.1 Service Principle und Keytab Datei

3.2 SQLNet Konfiguration

3.3 Kerberos Authentifizierung

3.4 Zusatz Aufgaben

- 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 Übungen: Centrally Managed User 18c

Generell verschieden

Übung Centrally Managed User 18c

Was neues in 18c

5 Übungen: Oracle Unified Directory

5.1 Einführung in Oracle Unified Directory

OULD 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 Übungen: 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

8 Demo- und Workshopumgebung

8.1 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 der folgenden Abbildung 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

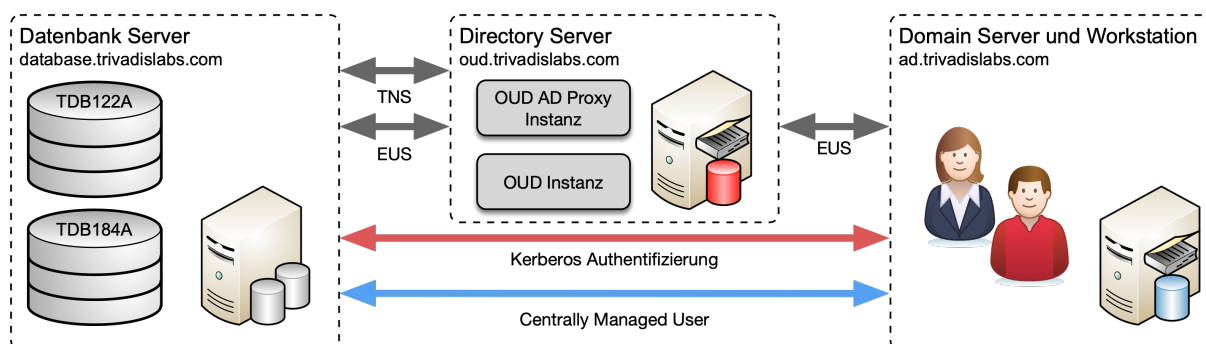


Abb. 2: Architektur Schulungsumgebung

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 Umgebungsscripte. 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).

8.2 Oracle Datenbank Server

8.2.1 Generelle Server Konfiguration

Der Oracle Datenbank Server ist wie folgt konfiguriert:

- **Host Name** : db.trivadislabs.com

- **Interne IP Adresse** : 10.0.0.3
- **Externe IP Adresse** : gemäss Liste
- **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 / PASSWORT
 - root / PASSWORT
- **Datenbank Benutzer** :
 - sys / manager
 - system / manager
 - scott / tiger
 - tvd_hr / tvd_hr

8.2.2 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
cda	zum Admin Verzeichnis der aktuell gesetzten Datenbank
cdh	zum Oracle Home
cdob	zum Oracle Base
cdt	zum TNS_ADMIN
sqh	startet SQLPlus mit „sqlplus / as sysdba“ inklusive Befehlshistory
sta	Statusanzeige für die aktuell gesetzte Datenbank
taa	öffnet das Alertlog der aktuell gesetzten Datenbank mit <code>tail -f</code>
TDB122A	setzt die Umgebung im Terminal für die Datenbank <i>TDB122A</i>
TDB184A	setzt die Umgebung im Terminal für die Datenbank <i>TDB184A</i>
u	Statusanzeige für alle Oracle Datenbanken und Listener (z.B. open, mount)

Alias Name	Beschreibung
------------	--------------

via	öffnet das Alertlog der aktuell gesetzten Datenbank in vi
-----	---

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/fast_recovery_area/TDB122A</code>	Fast Recovery Area
<code>/u02/oradata/TDB122A</code>	Redo Log Files, CTL

8.2.3 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 eine Selbstreferenz.

Zukünftige Versionen von TVD_HR werden zusätzlich entsprechend VPD Policies enthalten.

8.3 Oracle Unified Directory Server

8.3.1 Generelle Server Konfiguration

Der Directory Server ist wie folgt konfiguriert:

- **Host Name** : oud.trivadislabs.com
- **Interne IP Adresse** : 10.0.0.5
- **Externe IP Adresse** : gemäss Liste
- **Betriebssystem** : Oracle Enterprise Linux Server Release 7.5
- **Java** : Oracle JAVA Server JRE 1.8 u192
- **Oracle Fusion Middleware Software** :
 - Oracle Unified Directory (12.2.1.3) mit dem Bundle Patch vom Oktober 2018
 - Oracle Fusion Middleware Infrastructure Directory (12.2.1.3) mit dem Bundle Patch vom Oktober 2018
- **Oracle Home oud12.2.1.3** : Oracle Unified Directory *standalone* Installation.
- **Oracle Home fmw12.2.1.3** : Oracle Unified Directory *collocated* Installation mit Oracle Fusion Middleware Infrastructure.
- **Betriebssystem Benutzer** :
 - oracle / PASSWORT
 - root / PASSWORT

8.3.2 Trivadis OUD Base

Analog zu der Datenbank Umgebung, gibt es auch für Oracle Unified Directory entsprechende Umgebungsscripte. Diese Umgebungsscripte, kurz auch OUD Base genannt, werden unter anderem in [OUD Docker images](#) verwendet. Aus diesem Grund ist OUD Base etwas "leichter" aufgebaut als TVD-Basenv und basiert zu 100% auf Bash. OUD Base ist via GitHub Projekt [oehrlis/oudbase](#) als Open Source verfügbar.

In der folgenden Tabelle sind die Aliases für den OS Benutzer *oracle* aufgelistet, welche am häufigsten verwendet werden.

Alias Name	Beschreibung
cda	zum Admin Verzeichnis der aktuell OUD Instanz
cdh	zum Oracle Home
cdih	zum OUD Instanz Home Verzeichnis
cdil	zum OUD Instanz Log Verzeichnis
cdob	zum Oracle Base
dsc	aufruf von dsconfig inklusive Host Name, <code>\$PORT_ADMIN</code> und <code>\$PWD_FILE</code>
oud_ad	setzt die Umgebung im Terminal für die OUD Instanz <i>oud_ad</i>
taa	öffnet das Access Log der aktuell gesetzten OUD Instanz mit <code>tail -f</code>
u	Statusanzeige für alle OUD Instanz inkl entsprechender Ports
version	Anzeigen der Version von OUD base inklusive geänderten Dateien in <code>\$OUD_LOCAL</code>
vio	öffnet die oudtab Datei. <code>\${ETC_BASE}/oudtab</code>

Die Installation ist an den OFA (Optimal Flexible Architecture) Standard angelegt. Die Software, Konfiguration sowie Instanzen werden explizit von einander getrennt. Beispiel für die Installation auf der OUD-VM für die OUD Instanz - *oud_ad*:

Mount Point / Directory	Beschreibung
<code>/u00/app/oracle/local/oudbase</code>	Environment Tools (OUD Base)
<code>/u00/app/oracle/product/fmw12.2.1.3.0</code>	Oracle Unified Directory 12.2.1.3 Collocated Home
<code>/u00/app/oracle/product/jdk1.8.0_192</code>	Oracle Java 1.8 update 192

Mount Point / Directory	Beschreibung
/u00/app/oracle/product/oud12.2.1.3.0	Oracle Unified Directory 12.2.1.3 Standalone Home
/u01/admin/oud_ad	Instance Admin Verzeichnis
/u01/backup	Standard Backup Verzeichnis
/u01/etc	oudtab und diverse Konfigurationsdateien
/u01/instances/oud_ad/OUUD/config	Instanz Konfigurations Verzeichnis
/u01/instances/oud_ad/OUUD/logs	Instanz Log Verzeichnis
/u01/instances/oud_ad	Instanz Home Verzeichnis

8.4 MS Active Directory Server

8.4.1 Generelle Server Konfiguration

Der Active Directory Server basiert auf einer Windows Server 2012 R2 Umgebung (Windows Server 2016 für on-premises Setup) und ist wie folgt konfiguriert:

- **Host Name** : ad.trivadislabs.com
- **Interne IP Adresse** : 10.0.0.4
- **Externe IP Adresse** : gemäss Liste
- **Betriebssystem** : MS Windows Server 2012 R2
- **Installiere Server Roles** :
 - Active Directory Server
 - DNS Server mit Active Directory Integration
 - Certification Authority
- **Zusatz Software** : nur auf der Cloud VM
 - Putty für SSH Verbindungen mit dem OUD und DB Server
 - MobaXTerm für SSH Verbindungen mit dem OUD und DB Server
 - WinSCP für den File Transfer DB Server <=> AD Server
 - SQL Developer
 - Oracle 12c R2 und 18c Clients
 - MS Visual Studio Code als universellen Texteditor
 - Predefined SSH Keys für den OUD und DB Server
- **Betriebssystem Benutzer** :
 - Administrator / PASSWORT
 - root / PASSWORT

8.4.2 AD Domain TRIVADISLAB

Damit eine mehr oder weniger praxis nahe Anbindung an das Active Directory möglich ist, wurde für die fiktive Firma *Trivadis LAB* eine einfache AD Struktur aufgebaut. Die folgende Abbildung zeigt das Organigramm inklusive Abteilungen und Mitarbeiter für *Trivadis LAB*. Sämtlich aufgeführte Benutzer können als Testbenutzer verwendet werden. Wobei der Loginname jeweils dem klein geschriebenen Nachname entspricht. Passwort ist für alle Benutzer *LAB01schulung*.

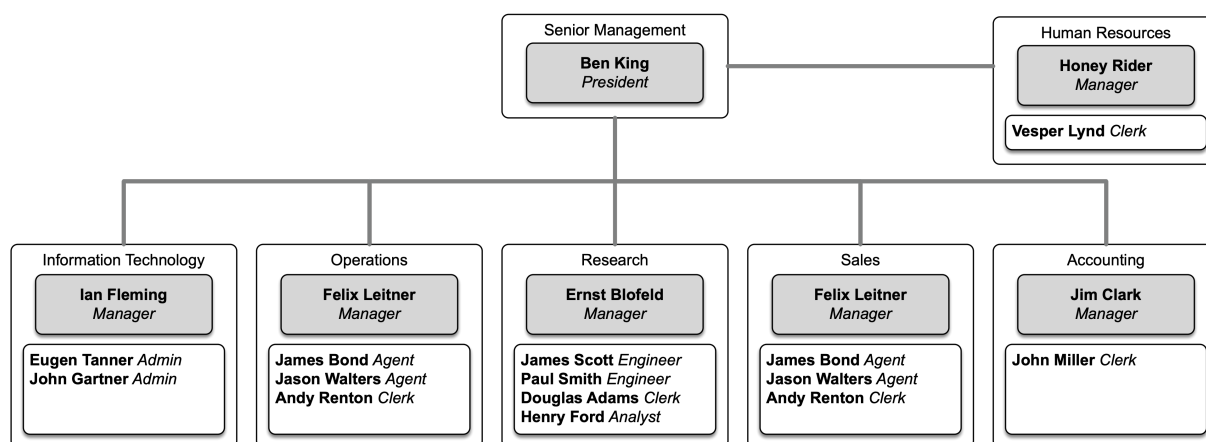


Abb. 3: Organigramm Trivadis LAB Company

Das fiktive Unternehmen hat folgende Abteilungen:

ID	Abteilung	Distinguished Name (DN)	Beschreibung
10	Senior Management	ou=Senior Management,ou=People,dc=trivadislabs,dc=com	Geschäftsleitung
20	Accounting	ou=Accounting,ou=People,dc=trivadislabs,dc=com	Finanzen
30	Research	ou=Research,ou=People,dc=trivadislabs,dc=com	Forschung
40	Sales	ou=Sales,ou=People,dc=trivadislabs,dc=com	Verkauf + Vertrieb
50	Operations	ou=Operations,ou=People,dc=trivadislabs,dc=com	Betriebsabteilung
60	Information Technology	ou=Information Technology,ou=People,dc=trivadislabs,dc=com	IT Abteilung

ID	Abteilung	Distinguished Name (DN)	Beschreibung
70	Human Resources	<code>ou=Human Resources,ou=People,dc=trivadislabs,dc=com</code>	Personalabteilung

Zusätzlich wurden folgende Gruppen definiert:

Gruppe	Distinguished Name (DN)	Beschreibung
Trivadis LAB APP Admins	<code>ou=Trivadis LAB APP Admins,ou=Groups,dc=trivadislabs,dc=com</code>	Applikations Administratoren
Trivadis LAB DB Admins	<code>ou=Trivadis LAB DB Admins,ou=Groups,dc=trivadislabs,dc=com</code>	DB Admins aus der IT Abteilung
Trivadis LAB Developers	<code>ou=Trivadis LAB Developers,ou=Groups,dc=trivadislabs,dc=com</code>	Entwickler aus der Forschungsabteilung
Trivadis LAB Management	<code>ou=Trivadis LAB Management,ou=Groups,dc=trivadislabs,dc=com</code>	Geschäftsleitung und Manager
Trivadis LAB System Admins	<code>ou=Trivadis LAB System Admins,ou=Groups,dc=trivadislabs,dc=com</code>	System Admins aus der IT Abteilung
Trivadis LAB Users	<code>ou=Trivadis LAB Users,ou=Groups,dc=trivadislabs,dc=com</code>	Alle Benutzer

9 Links und Referenzen

9.1 OUD EUS Workshop

Unterlagen und Skripte zum Workshop

- Übungsskripte zum DOAG Schulungstag [doag2018](#)
- Vagrant Setup zum Aufbau der Trivadis LAB Umgebung [oehrlis/trivadislabs.com](https://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](#)

9.2 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>

9.3 Software und Tools

9.3.1 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](#)

9.3.2 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](#)

9.3.3 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](#)

9.3.4 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](#)