trivadis

Trivadis triCast

Demo Oracle Centrally Managed User 18c/19c

28 Mai 2019, Version 1

Trivadis AG
Sägereistrasse 29
8152 Glattbrugg

info@trivadis.com
+41 58 459 55 55

Contents

1 Einleitung Oracle Centrally Managed User 18c/19c **3**

2 Centrally Managed User 18c **4**

2.1 Active Directory Konfiguration 4

2.2 Server und Datenbank Konfiguration 7

2.3 Benutzer und Rollen 10

2.4 Rollen und Admininistratoren 11

3 Kerberos Authentifizierung **12**

3.1 Service Principle und Keytab Datei 13

3.2 SQLNet Konfiguration 14

3.3 Kerberos Authentifizierung 15

3.4 Kerberos Authentifizierung für weitere CMU Benutzer 16

4 Demo- und Lab Umgebung **17**

4.1 Architektur 17

4.2 Oracle Datenbank Server 18

4.3 Oracle Unified Directory Server 20

4.4 MS Active Directory Server 22

5 Links und Referenzen **24**

5.1 OUD EUS Workshop 24

5.2 Oracle Dokumentation 25

5.3 My Oracle Support Notes 25

5.4 Software und Tools 25

1 Einleitung Oracle Centrally Managed User 18c/19c

Mit der Live-Demo Oracle Centrally Managed User 18c/19c wird die Active Directory Integration am Beispiel der Trivadis Lab Umgebung aufgezeigt. Die Live-Demo wird im Rahmen des Trivadis triCast durchgeführt. Die vorliegende Dokumentation ist eine kurze nicht abschliessende Zusammenfassung der Live-Demo und der Testumgebung. Die Testumgebung besteht, wie man in der folgenden Abbildung sehen kann, jeweils aus drei virtuellen Systemen.

- DB Server mit Oracle 18c
- Windows Server 2016 mit MS Active Directory
- OUD Server mit OUD 12.2.1.3.0 für die LDAP Namensauflösung

Optional können für weitere Tests zusätzliche VM's mit Oracle 19c, 12c oder 11g genutzt werden.

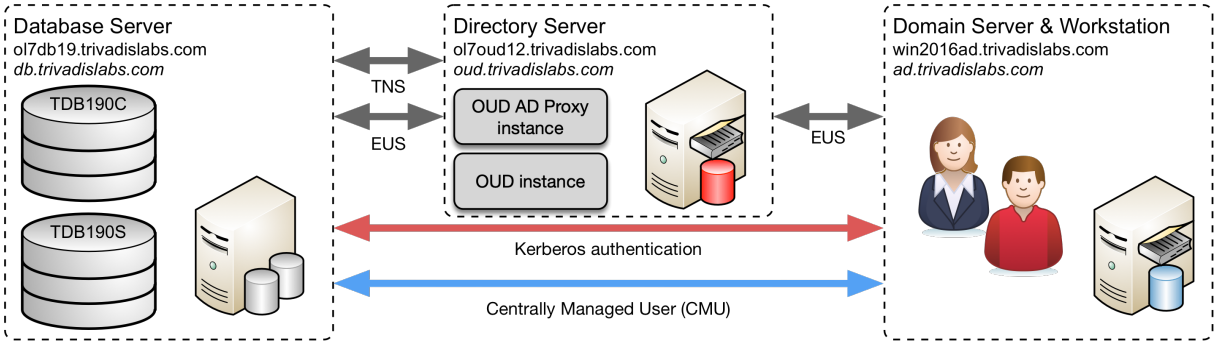

Abb. 1: Architektur Lab Umgebung

Wichtigsten Login Informationen im Überblick:

- Datenbank Server (Linux VM) Oracle 19c
  - Host Name : ol7db19.trivadislabs.com
  - Interne IP Adresse : 10.0.0.19
- Datenbank Server (Linux VM) Oracle 18c
  - Host Name : ol7db19.trivadislabs.com
  - Host Alias: db.trivadislabs.com
  - Interne IP Adresse : 10.0.0.18
- Directory Server (Linux VM)
  - Host Name : ol7oud12.trivadislabs.com
  - Host Alias: oud.trivadislabs.com
  - Interne IP Adresse : 10.0.0.5
- Active Directory Server (Windows VM)
  - Host Name : win2016ad.trivadislabs.com
  - Host Alias: ad.trivadislabs.com
  - Interne IP Adresse : 10.0.0.4
- 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

Das Login erfolgt jeweils via vagrant respektive ssh. Alternativ kann man auch direkt mit SSH oder Putty auf den weitergeleiteten Port zugreifen.

```
vagrant ssh
sudo su - oracle
```

Im Kapitel Demo- und Lab Umgebung wird die Testumgebung etwas ausführlicher beschrieben. Zusätzlich besteht die Möglichkeit, selber eine eingene Testumgebung aufzubauen. Hierzu gibt es ein GitHub Repository oehrlis/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 Centrally Managed User 18c

Ziele: Konfiguration von Centrally Managed Users für die Datenbank TDB180S. Erweitern des Active Directory Schemas inklusive der Installation des Password Filter Plugins. Erstellen von Mappings für Benutzer und Rollen sowie erfolgreichem Login mit Passwort Authentifizierung.

2.1 Active Directory Konfiguration

Arbeitsumgebung:

- Server: win2016ad.trivadislabs.com
- Benutzer: Administrator

Die folgenden Arbeiten werden in der Regel in Zusammenarbeit mit dem Windows respektive Active Directory Administrator durchgeführt. Je nach Unternehmensgrösse sind allenfalls noch weiter IT Bereich mit involviert.

Für das Oracle Wallet wird das Root Zertifikat vom Active Directory Server benötigt. Diesen kann in der LAB Umgebung einfach via Commandline exportiert werden. Dazu öffnet man ein Command Prompt (`cmd.exe`) und exportieren das Root Zertifikat. Das exportiert Root Zertifikat muss anschliessend mit WinSCP auf den Datenbank Server in das Verzeichnis `/u00/app/oracle/network/admin` kopiert werden. Alternativ kann man das unten aufgeführte Putty SCP Kommando verwenden.

```
certutil -ca.cert c:\vagrant_common\config\tnsadmin\RootCA_trivadislabs.
    com.cer

"C:\Program Files\PuTTY\pscp.exe" c:\vagrant_common\config\tnsadmin\
    RootCA_trivadislabs.com.cer ol7db18.trivadislabs.com:/u00/app/oracle/
    network/admin
```

In der Vagrant VM Umgebung ist zudem das Verzeichnis `c:\vagrant_common\` auf allen Systemen verfügbar. Somit lässt sich die Datei einfach auf dem Datenbank Server nutzen.

```
cp /vagrant_common/config/tnsadmin/RootCA_trivadislabs.com.cer /u00/app/
    oracle/network/admin
```

Um Oracle CMU mit Passwort Authentifizierung verwenden zu können, muss Active Directory entsprechend angepasst werden. Dazu muss mit WinSCP die Datei `opwdintg.exe` auf den Active Directory Server kopiert werden. Auf dem Datenbank Server liegt die Datei im Oracle Home `$ORACLE_HOME/bin/opwdintg.exe`. Alternativ man das unten aufgeführte Putty SCP Kommando verwenden.

```
"C:\Program Files\PuTTY\pscp.exe" ol7db18.trivadislabs.com:/u00/app/
    oracle/product/18.0.0.0/bin/opwdintg.exe c:\vagrant_common\config\
    tnsadmin\
```

In der Vagrant VM Umgebung ist zudem das Verzeichnis `c:\vagrant_common\` auf allen Systemen verfügbar. Somit lässt sich die Datei einfach auf dem Datenbank Server kopieren.

```
ls -alh $ORACLE_HOME/bin/opwdintg.exe
cp $ORACLE_HOME/bin/opwdintg.exe /vagrant_common/config/tnsadmin
```

Anschliessend muss die Datei auf dem Active Directory ausgeführt werden, um das AD Schema zu erweitern und das Passwort Filter Plugin zu installieren. Dazu wird `opwdintg.exe` direkt in einem Command Shell (`cmd.exe`) ausgeführt.

```
c:\vagrant_common\config\tnsadmin\opwdintg.exe
```

Bei der Installstion sind folgende Fragen mit Ja respektive Yes zu beantworten:

- Do you want to extend AD schema? [Yes/No]:
- Schema extension for this domain will be permanent. Continue? [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]:

Nachdem der Active Directory Server neu gestartet wurde, müssen zum Abschluss die neu erstellten Gruppen für die Passwort Verifier entsprechend vergeben werden. Entsprechende Benutzer, welche sich an der Datenbank anmelden, müssen dazu ein Oracle Password Hash haben. Dieser wird vom Password Filter bei allen Benutzer erstellt, welche in der Gruppe *ORA_VFR_11G* respektive *ORA_VFR_12C* sind. Zudem müssen diese Benutzer ihr Passwort neu setzten, damit das Passwort Filter Plugin auch effektive das Attribut *orclCommonAttribute* setzt.

Variante 1: Anpassen der Gruppe *Trivadislabs Users* und manuelles hinzufügen von *ORA_VFR_11G* respektive *ORA_VFR_12C* zu MemberOf.

- Starten von *Active Directory Users and Computers*.
- Auswahl der Gruppe *Trivadislabs Users* im Container Groups.
- Öffnen der *Properties* mit rechtem Mausklick.
- Im Tab *Member Of Add...* auswählen.
- Hinzufügen der Gruppe *ORA_VFR_11G* respektive *ORA_VFR_12C*.
- Schliessen der Dialoge mit *Ok*.

Anschliessend manuelles Anpassen der Passwörter für die gewünschten Benutzer. Dazu muss man in *Active Directory Users and Computers* jeweils den Benutzer auswählen und mit rechtem Mausklick *Reset Password...* starten, um ein neues Passwort zu setzten.

Variante 2: Öffnen eines PowerShell Fenster und ausführen des Scripts `c:\aoug\lab\04_cmu\reset_ad_users.ps1`. Das Script passt sowohl die Gruppe an und ändert die Passwörter aller Benutzer.

```
C:\vagrant\scripts\reset_ad_users.ps1
```

Kontrolle ob das Attribut *orclCommonAttribute* gesetzt ist. Die folgende Abbildung zeigt die Properties vom Benutzer King und das Attribut *orclCommonAttribute*.

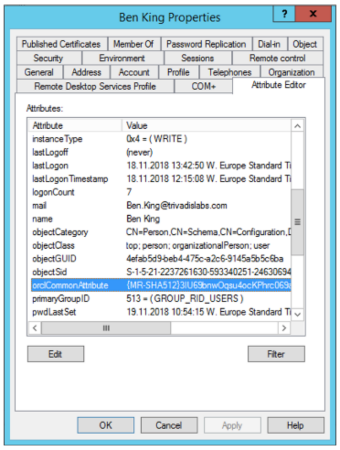

Figure 1: "Benutzereigenschaften Benutzer King"

Benutzer `oracle` für die CMU intergration

2.2 Server und Datenbank Konfiguration

Arbeitsumgebung für diesen Abschnitt:

- Server: ol7db18.trivadislabs.com
- Benutzer: oracle
- Datenbank: TDB180S

CMU benötigt in allen Oracle 18c Versionen einen Patch. Siehe auch Oracle MOS Note 2462012.1 *How To Configure Authentication For The Centrally Managed Users In An 18c Database* und Oracle Support Bug OUD 12C: DIGEST-MD5 SASL AUTHENTICATION FAILS IF ORACLECONTEXT ENTRY AND LDAPS 29034231. Bevor CMU genutzt werden kann ist zu prüfen ob der Patch installiert ist.

```
$cdh/OPatch/opatch lsinventory

$cdh/OPatch/opatch lsinventory |grep -i 28994890
```

Erstellen der SQLNet Konfigurationsdatei `dsi.ora` mit den folgenden Informationen zum Aktive Directory Server. Eine Beispiel Konfigurationsdatei ist im Verzeichnis `$cdl/aoug/lab` vorhanden.

```
cp $cdl/aoug/lab/dsi.ora $cdn/admin/dsi.ora
vi $cdn/admin/dsi.ora
```

```
DSI_DIRECTORY_SERVERS = (win2016ad.trivadislabs.com:389:636)
DSI_DEFAULT_ADMIN_CONTEXT = "dc=trivadislabs,dc=com"
DSI_DIRECTORY_SERVER_TYPE = AD
```

Erstellen eines neuen Oracle Wallet für die Datenbank TDB180S.

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

Hinzufügen der Einträge für den Benutzername, Passwort und den Distinguished Name.

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

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

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

Copy/Paste Variante für die Live Demo

```
echo LAB01schulung|mkstore -wrl $ORACLE_BASE/admin/$ORACLE_SID/wallet -
   createEntry ORACLE.SECURITY.USERNAME oracle@trivadislabs.com

echo LAB01schulung|mkstore -wrl $ORACLE_BASE/admin/$ORACLE_SID/wallet -
   createEntry ORACLE.SECURITY.DN CN=oracle,CN=Users,DC=trivadislabs,DC=
   com

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

Laden des Root Zertifikat vom Active Directory Server in das Wallet.

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

Mit folgenden Befehlen läst sich prüfen, wass nun effektiv im Wallet steht.

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

Oracle PKI Tool Release 18.0.0.0.0 - Production
Version 18.1.0.0.0
```

```
Copyright (c) 2004, 2017, Oracle and/or its affiliates. All rights
   reserved.

Requested Certificates:
User Certificates:
Oracle Secret Store entries:
ORACLE.SECURITY.DN
ORACLE.SECURITY.PASSWORD
ORACLE.SECURITY.USERNAME
Trusted Certificates:
Subject:        CN=Trivadislabs Enterprise Root CA,DC=trivadislabs,DC=com
```

Oder der Inhalt vom Wallet mit mkstore

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

```
echo LAB01schulung|mkstore -wrl $ORACLE_BASE/admin/$ORACLE_SID/wallet -
   list
echo LAB01schulung|mkstore -wrl $ORACLE_BASE/admin/$ORACLE_SID/wallet -
   viewEntry ORACLE.SECURITY.DN
echo LAB01schulung|mkstore -wrl $ORACLE_BASE/admin/$ORACLE_SID/wallet -
   viewEntry ORACLE.SECURITY.PASSWORD
echo LAB01schulung|mkstore -wrl $ORACLE_BASE/admin/$ORACLE_SID/wallet -
   viewEntry ORACLE.SECURITY.USERNAME
```

Mit dem LDAP Search Befehl läst sich zudem Prüfen, ob der Zugriff auf das Active Directory mit dem Wallet funktioniert. Der folgende Befehl sucht nach einem *sAMAccountName=blo*. Achtung! Die Passwörter für den Benutzer oracle18c sowie das Wallet Passwort werden hier auf dem Commandline angegeben.

```
ldapsearch -h win2016ad.trivadislabs.com -p 389 \
    -D "CN=oracle,CN=Users,DC=trivadislabs,DC=com" \
    -w LAB01schulung -U 2 \
    -W "file:/u00/app/oracle/admin/$ORACLE_SID/wallet" \
    -P LAB01schulung -b "OU=People,DC=trivadislabs,DC=com" \
    -s sub "(sAMAccountName=blo*)" dn orclCommonAttribute
```

2.3 Benutzer und Rollen

Arbeitsumgebung für die Übung:

- Server: ol7db18.trivadislabs.com
- Benutzer: oracle
- Datenbank: TDB180S

Als letzter Konfigurationspunkt für Centrally Managed User müssen neben dem Mapping entsprechende init.ora Parameter angepasst werden. Starten Sie ein sqlplus als SYSDBA und setzen Sie die beiden Parameter *ldap_directory_access* und *ldap_directory_sysauth*.

```
ALTER SYSTEM SET ldap_directory_access = 'PASSWORD';
ALTER SYSTEM SET ldap_directory_sysauth = YES SCOPE=SPFILE;
STARTUP FORCE;
```

Erstellen Sie einen gobalen shared Benutzer *tvd_global_users*, der für alle Mitarbeiter gilt. Also für alle Benutzer in der Gruppe *cn=Trivadislabs Users,ou=Groups,dc=trivadislabs,dc=com*. Zudem sollen sich alle Benutzer verbinden können.

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

Verbinden Sie sich als Benutzer Blofeld mit dem Windows Domain und prüfen Sie die detail Informationen zu dieser Session wie Authentifizierung, Identity etc.

```
connect "blofeld@TRIVADISLABS.COM"@TDB180S

show user
@sousrinf
```

Alternative Verbindung wie üblich mit Usernamen und Passwort.

```
connect blofeld@TDB180S

show user
@sousrinf
```

Nun können sich alle AD Benutzer der Gruppe *Trivadislabs Users* mit der Datenbank TDB180A verbinden. Sie erhalten dabei die basis Rechte, welche wir zuvor dem Datenbank Account *tvd_global_users* gegeben haben. Interessant wird es, wenn die Benutzer aus den verschiedenen Abteilungen unterschiedliche

Rechte oder Rollen erhalten. Dazu erstellen wir entsprechende Rollen mit einem Mapping auf die Active Directory Gruppe oder Organisation Unit.

```
CONNECT / AS SYSDBA

CREATE ROLE mgmt_role IDENTIFIED GLOBALLY AS
'CN=Trivadislabs Management,OU=Groups,DC=trivadislabs,DC=com';

CREATE ROLE rd_role IDENTIFIED GLOBALLY AS
'CN=Trivadislabs Developers,OU=Groups,DC=trivadislabs,DC=com';
```

Prüfen Sie nun die verschiedenen Rechte / Rollen der einzelnen Mitarbeitern aus diesem Abteilungen.

```
CONNECT "moneypenny@TRIVADISLABS.COM"/LAB01schulung@TDB180S
SELECT * FROM session_roles;

CONNECT "smith@TRIVADISLABS.COM"/LAB01schulung@TDB180S
SELECT * FROM session_roles;

CONNECT "blofeld@TRIVADISLABS.COM"/LAB01schulung@TDB180S
SELECT * FROM session_roles;
```

2.4 Rollen und Admininistratoren

Erstellen eines global private Schema für den Benutzer Adams.

```
CONNECT / AS SYSDBA

CREATE USER adams IDENTIFIED GLOBALLY AS 'CN=Douglas Adams,OU=Research,OU
   =People,DC=trivadislabs,DC=com';
GRANT create session TO adams ;
GRANT SELECT ON v_$session TO adams ;

connect "adams@TRIVADISLABS.COM"/LAB01schulung@TDB180S
SELECT * FROM session_roles;
show user
@sousrinf
```

Erstellen des Mapping für die DBA's, welche sich auch als SYSDBA anmelden sollen. Prüfen Sie dazu als erstest das Format der Oracle Password Datei. Voraussetzung für das Mapping von Administratoren ist die Passwort Datei Version 12.2.

```
orapwd describe file=$cdh/dbs/orapwTDB180S
```

Migrieren Sie die aktuelle Passwort Datei in das Format 12.2. Alternativ können Sie die Passwort Datei auch neu anlegen.

```
mv $cdh/dbs/orapwTDB180S $cdh/dbs/orapwTDB180S_format12
orapwd format=12.2 input_file=$cdh/dbs/orapwTDB180S_format12 file=$cdh/
    dbs/orapwTDB180S
orapwd describe file=$cdh/dbs/orapwTDB180S
```

Erstellen Sie ein Mapping für den DBA Ian Fleming *CN=Ian Fleming,OU=Information Technology,OU=People,DC=trivadislabs,DC=com*

```
CREATE USER fleming IDENTIFIED GLOBALLY AS
'CN=Ian Fleming,OU=Information Technology,OU=People,DC=trivadislabs,DC=
    com';
GRANT SYSDBA TO fleming;
GRANT connect TO fleming;
GRANT SELECT ON v_$session TO fleming;
```

Verbinden Sie sich mit und ohne SYSDB als Ian Fleming. Was für Rechte sowie Authentifizerungsinformationen finden Sie?

```
CONNECT "fleming@TRIVADISLABS.COM"/LAB01schulung@TDB180S
SELECT * FROM session_roles;
show user
@sousrinf
```

```
CONNECT "fleming@TRIVADISLABS.COM"/LAB01schulung@ol7db18.trivadislabs.com
    :1521/TDB180S as sysdba
CONNECT fleming/LAB01schulung@TDB180S as sysdba
SELECT * FROM session_roles;
show user
@sousrinf
```

3 Kerberos Authentifizierung

Ziele: Konfiguration der Kerberos Authentifizierung für die Datenbanken TDB180S und TDB190S. Erstellen eines Benutzers mit Kerberos Authentifizierung sowie erfolgreichem Login lokal (Linux VM) und remote (Windows VM).

3.1 Service Principle und Keytab Datei

Arbeitsumgebung für die Übung

- Server: win2016ad.trivadislabs.com
- Benutzer: Administrator

Für die Kerberos Authentifizierung wird ein Service Principle benötigt. Der Entsprechende Benutzer Account wurde vorbereitet. Kontrollieren Sie in auf dem Server *win2016ad.trivadislabs.com* mit dem Tool *Active Directory User and Computers* ob der Benutzer *ol7db18.trivadislabs.com.keytab* existiert. Falls ja, was hat der Benutzer für Einstellungen bezüglich Login Name und Account optionen? Passen Sie ggf noch die Account Optionen an uns setzen *Kerberos AES 128* und *Kerberos AES 256*. Die folgende Abbildung zeigt ein Beispiel. Optional können Sie den Benutzer auch löschen und neu anlegen.

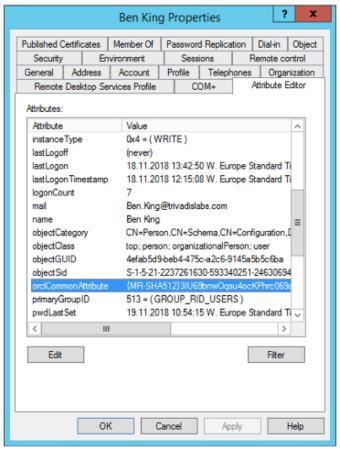

Figure 2: "Benutzereigenschaften"

Nachdem die Account Optionen angepasst wurden, ist für diesen Benutzer eine Keytab Datei zu erstellen. Öffnen Sie dazu ein Command Prompt (`cmd.exe`) und führen `ktpass.exe` aus.

```
ktpass.exe -princ oracle/ol7db18.trivadislabs.com.keytab@TRIVADISLABS.COM
    -mapuser ol7db18.trivadislabs.com.keytab -pass LAB01schulung -crypto
   ALL -ptype KRB5_NT_PRINCIPAL  -out C:\u00\app\oracle\network\admin\
   ol7db18.trivadislabs.com.keytab
```

Überprüfen Sie anschliessend den Service Principle Names (SPN) mit `setspn`

```
setspn -L ol7db18.trivadislabs.com.keytab
```

Kopieren Sie die Keytab Datei mit WinSCP auf den Datenbank Sever in das Verzeichnis `$cdn/admin` . Achten Sie darauf, dass die Datei als Binärdatei kopiert wird. Alternativ können Sie auch das unten aufgeführte Putty SCP Kommando verwenden.

```
"C:\Program Files\PuTTY\pscp.exe" C:\u00\app\oracle\network\admin\ol7db18
    .trivadislabs.com.keytab ol7db18.trivadislabs.com.keytab:/u00/app/
    oracle/network/admin
```

3.2 SQLNet Konfiguration

Arbeitsumgebung für die Übung:

- Server: ol7db18.trivadislabs.com.keytab
- Benutzer: oracle

Ergänzen Sie die `sqlnet.ora` Datei mit folgenden Parametern.

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

# Kerberos Configuration
#
    ######################################################################

SQLNET.AUTHENTICATION_SERVICES = (BEQ,KERBEROS5)
SQLNET.FALLBACK_AUTHENTICATION = TRUE
SQLNET.KERBEROS5_KEYTAB = /u00/app/oracle/network/admin/ol7db18.
    trivadislabs.com.keytab
SQLNET.KERBEROS5_REALMS = /u00/app/oracle/network/admin/krb.realms
SQLNET.KERBEROS5_CC_NAME = /u00/app/oracle/network/admin/krbcache
SQLNET.KERBEROS5_CONF = /u00/app/oracle/network/admin/krb5.conf
SQLNET.KERBEROS5_CONF_MIT=TRUE
SQLNET.AUTHENTICATION_KERBEROS5_SERVICE = oracle
```

Erstellen Sie die Kerberos Konfigurationsdatei `krb5.conf` mit folgendem Inhalt.

```
vi $cdn/admin/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
```

Nachdem die Keytab Datei auf dem Datenbank Server kopiert worden ist, kann mit `oklist` überprüft werden was die Datei für Crypto Algorithmen untersützt. Somit wird zudem indirekt geprüft ob die Keytab Datei verwendet werden kann.

```
oklist -e -k $cdn/admin/ol7db18.trivadislabs.com.keytab
```

Kontrollieren Sie ob die Namensauflösung wie gewünscht funktioniert.

```
nslookup win2016ad.trivadislabs.com
nslookup 10.0.0.4
nslookup ol7db18.trivadislabs.com
nslookup 10.0.0.5
```

Erstellen Sie anschliessend mit`okinit` manuell ein Session Ticket.

```
okinit king@TRIVADISLABS.COM

oklist
```

3.3 Kerberos Authentifizierung

Arbeitsumgebung für die Übung:

- Server: ol7db18.trivadislabs.com
- Benutzer: oracle

Passen Sie den init.ora Parameter OS Prefix an. Für die Kerberos Authentifizierung muss dieser leer sein.

```
sqh
Show parameter os_authent_prefix
ALTER SYSTEM SET os_authent_prefix='' SCOPE=spfile;
STARTUP FORCE;
```

Erstellen Sie einen Kerberos Benutzers für den Mitarbeiter King. Verwenden Sie dazu die Variante mit dem Kerberos Principal Name.

```
CREATE USER king IDENTIFIED EXTERNALLY AS 'king@TRIVADISLABS.COM';
GRANT CONNECT TO king;
GRANT SELECT ON v_$session TO king;
```

Login als Benutzer King mit dem zuvor generierten Session Ticket und anzeigen der Informationen zur aktuellen Session.

```

connect /@TDB180S

show user

@sousrinf

SELECT sys_context('USERENV','AUTHENTICATION_TYPE') FROM DUAL;
SELECT sys_context('USERENV','AUTHENTICATION_METHOD') FROM DUAL;
SELECT sys_context('USERENV','AUTHENTICATED_IDENTITY') FROM DUAL;
```

3.4 Kerberos Authentifizierung für weitere CMU Benutzer

Wie ist das jetzt mit Kerberos? Wenn Sie die Übung zu Kerberos erfolgreich abgeschlossen haben, können sich die Benutzer nun auch mit Kerberos Authentifizieren. Ein Versuch mit dem Benutzer *Bond* schaft hier klarheit. Generieren sie zuerst manuell ein Ticket Granting Ticket mit `okinit`. Die Passwortabfrage umgehen wir bei diesem Beispiel einfach indem wir das Passwort mit einem `echo |` via STDIN an `okinit` schicken. Mit dem Skript `sousrinf.sql` sehen wir anschliessend detailierte Informationen zur Authentifizierung.

Kerberos Cache für den Benutzer *bond* erstellen und einloggen

```
sqh
host echo LAB01schulung|okinit bond
connect /@TDB180S
SELECT * FROM session_roles;

show user
@sousrinf.sql
```

Kerberos Cache für den Benutzer *fleming* erstellen und einloggen. Geht auch als *SYSDBA*.

```
sqh
```

```
host echo LAB01schulung|okinit fleming
connect /@TDB180S
SELECT * FROM session_roles;

show user
@sousrinf.sql

connect /@TDB180S as sysdba
```

4 Demo- und Lab Umgebung

4.1 Architektur

Für die praktischen Arbeiten in den Demos zu Centraly Managed User wird die Trivadis LAB Umgebung genutzt. Wie in der folgenden Abbildung ersichtlich aus folgenden Servern respektive VMs:

- ol7db18.trivadislabs.com.keytab Oracle Datenbank Server mit Oracle 18c
- ol7oud12.trivadislabs.com Oracle Directory Server mit Oracle Unified Directory 12c
- win2016ad.trivadislabs.com MS Windows Server 2012 R2 mit Active Directory

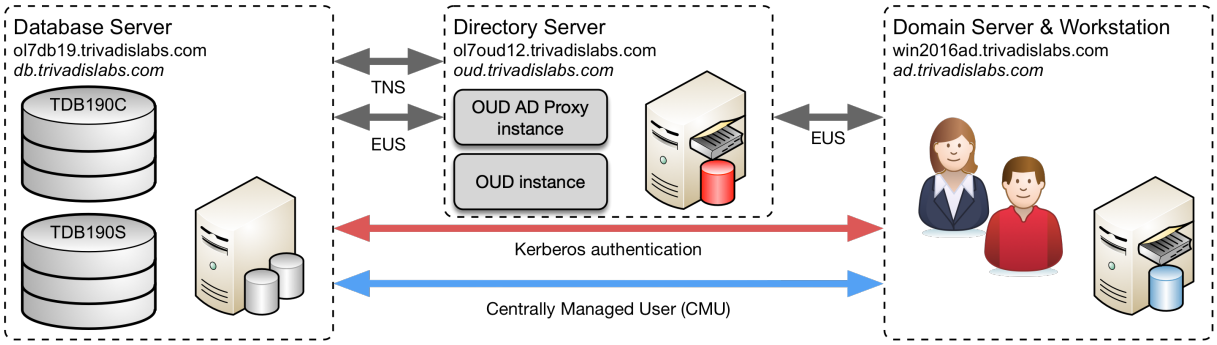

Abb. 2: Architektur Schulungsumgebung

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 oehrlis/trivadislabs.com.

4.2 Oracle Datenbank Server

4.2.1 Generelle Server Konfiguration

Der Oracle Datenbank Server ist wie folgt konfiguriert:

- Host Name : ol7db18.trivadislabs.com.keytab
- Interne IP Adresse : 10.0.0.18
- Externe IP Adresse : gemäss Liste
- Betriebssystem : Oracle Enterprise Linux Server Release 7.6
- Oracle Datenbank Software :
  - Oracle 18c Enterprise Edition (18.6.0.0) mit Release Update vom April 2019
- Oracle Datenbanken :
  - TDB180S Oracle 18c Enterprise Edition Single Instance für die Übungen mit CMU
  - TDB180C Oracle 18c Enterprise Edition Container Database
- Betriebsystem Benutzer :
  - oracle / PASSWORT
  - root / PASSWORT
- Datenbank Benutzer :
  - sys / manager
  - system / manager
  - scott / tiger
  - tvd_hr / tvd_hr

4.2.2 Trivadis BasEnv

Das Trivadis Base Environment (TVD-BasenvTM) 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 `tail -f`

Alias Name	Beschreibung
TDB180S	setzt die Umgebung im Terminal für die Datenbank *TDB180S*
TDB180C	setzt die Umgebung im Terminal für die Datenbank *TDB180C*
u	Statusanzeige für alle Oracle Datenbanken und Listener (z.B. open, mount)
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 - *TDB180S*:

Mount Point / Directory	Beschreibung
`/u00/app/oracle/admin/TDB180S/adump`	Oracle Audit Files
`/u00/app/oracle/admin/TDB180S/backup`	Oracle Backup
`/u00/app/oracle/admin/TDB180S/dpdump`	Data Pump Dateien
`/u00/app/oracle/admin/TDB180S/etc`	Oracle Backup Konfig Dateien
`/u00/app/oracle/admin/TDB180S/log`	Log Dateien (z.B. Backup, Export, etc.)
`/u00/app/oracle/admin/TDB180S/pfile`	Parameter- und Password-Datei
`/u00/app/oracle/admin/TDB180S/wallet`	Oracle Wallet
`/u00/app/oracle/etc`	oratab und diverse Konfigurationsdateien
`/u00/app/oracle/local/dba`	Environment Tools (TVD-Basenv)
`/u00/app/oracle/network/admin`	Oracle Net Konfigurationsdateien
`/u00/app/oracle/product/18.0.0.0`	Oracle 18.6.0.0 Home
`/u01/oradata/TDB180S`	Datenbank Dateien, Redo Log Files, CTL
`/u02/fast_recovery_area/TDB180S`	Fast Recovery Area
`/u02/oradata/TDB180S`	Redo Log Files, CTL

4.2.3 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 Tablle, welche Regionsnummern und -namen enthält. Verweise auf die Tabelle *LOCATION*.
- LOCATIONS Tablle, 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.

4.3 Oracle Unified Directory Server

4.3.1 Generelle Server Konfiguration

Der Directory Server ist wie folgt konfiguriert:

- Host Name : ol7oud12.trivadislabs.com
- Interne IP Adresse : 10.0.0.5
- Externe IP Adresse : gemäss Liste
- Betriebssystem : Oracle Enterprise Linux Server Release 7.6
- Java : Oracle JAVA Server JRE 1.8 u212
- 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.
- Betriebsystem Benutzer :

- oracle / PASSWORT
- root / PASSWORT

4.3.2 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 unteranderem 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, `$PORT_ADMIN` und `$PWD_FILE`
oud_ad	setzt die Umgebung im Terminal für die OUD Instanz *oud_ad*
taa	öffnet das Access Log der aktuell gesetzten OUD Instanz mit `tail -f`
u	Statusanzeige für alle OUD Instanz inkl entsprechender Ports
version	Anzeiden der Version von OUD base inklusive geänderten Dateien in `$OUD_LOCAL`
vio	öffnet die oudtab Datei. `${ETC_BASE}/oudtab`

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
`/u00/app/oracle/local/oudbase`	Environment Tools (OUD Base)

Mount Point / Directory	Beschreibung
/u00/app/oracle/product/fmw12.2.1.3.0	Oracle Unified Directory 12.2.1.3 Collocated Home
/u00/app/oracle/product/jdk1.8.0_212	Oracle Java 1.8 update 212
/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/OUD/config	Instanz Konfigurations Verzeichnis
/u01/instances/oud_ad/OUD/logs	Instanz Log Verzeichnis
/u01/instances/oud_ad	Instanz Home Verzeichnis

4.4 MS Active Directory Server

4.4.1 Generelle Server Konfiguration

Der Active Directory Server basiert auf einer Windows Server 2016 Umgebung und ist wie folgt konfiguriert:

- Host Name : win2016ad.trivadislabs.com
- Interne IP Adresse : 10.0.0.4
- Externe IP Adresse : gemäss Liste
- Betriebssystem : MS Windows Server 2016
- Installiere Server Roles :
  - Active Directory Server
  - DNS Server mit Active Directory Integration
  - Certification Autority
- 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
  - MS Visual Studio Code als universellen Texteditor

  - Predefined SSH Keys für den OUD und DB Server
- Betriebsystem Benutzer :
  - Administrator / LAB01schulung
  - root / LAB01schulung
  - Trivadis LAB User / LAB01schulung

4.4.2 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 Organigram 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*.

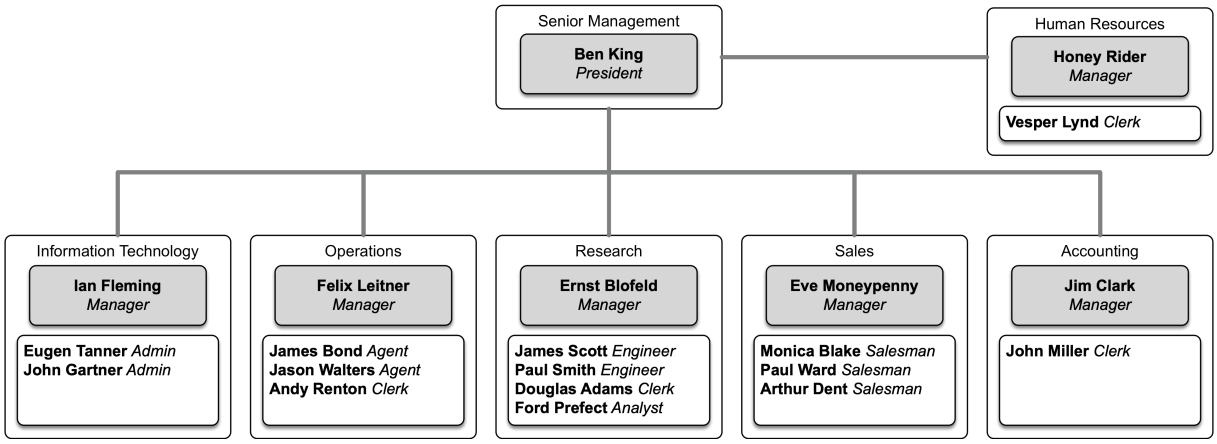

Abb. 3: Organigram Trivadis LAB Company

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

ID	Abteilung	Distinguished Name (DN)	Beschreibung
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
70	Human Resources	`ou=Human Resources,ou=People,dc=trivadislabs,dc=com`	Personalabteilung

Zusätzlich wurden folgende Gruppen definiert:

Gruppe	Distinguished Name (DN)	Beschreibung
Trivadislabs APP Admins	`cn=Trivadislabs APP Admins,ou=Groups,dc=trivadislabs,dc=com`	Applikations Administratoren
Trivadislabs DB Admins	`cn=Trivadislabs DB Admins,ou=Groups,dc=trivadislabs,dc=com`	DB Admins aus der IT Abteilung
Trivadislabs Developers	`cn=Trivadislabs Developers,ou=Groups,dc=trivadislabs,dc=com`	Entwickler aus der Forschungsabteilung
Trivadislabs Management	`cn=Trivadislabs Management,ou=Groups,dc=trivadislabs,dc=com`	Geschäftsleitung und Manager
Trivadislabs System Admins	`cn=Trivadislabs System Admins,ou=Groups,dc=trivadislabs,dc=com`	System Admins aus der IT Abteilung
Trivadislabs Users	`cn=Trivadislabs Users,ou=Groups,dc=trivadislabs,dc=com`	Alle Benutzter

5 Links und Referenzen

5.1 OUD EUS Workshop

Unterlagen und Skripte zum Workshop

- Demo Skript zum Trivadis triCast www.oradba.ch
- 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

5.2 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_m
- Oracle EUSM Utility https://docs.oracle.com/en/database/oracle/oracle-database/18/dbimi/enterprise-user-security-manager-eusm-command-summary.html

5.3 My Oracle Support Notes

- Oracle MOS Note *How To Configure Authentication For The Centrally Managed Users In An 18c Database* 2462012.1
- Oracle MOS Note *Tracing CMU connection issues* 2470608.1
- Oracle Support Bug *OUD 12C: DIGEST-MD5 SASL AUTHENTICATION FAILS IF ORACLECONTEXT ENTRY AND LDAPS* 29034231
- Oracle MOS Note *Centrally Managed User CMU Authentication Fails ORA-28044: unsupported directory type ORA-12638: Credential retrieval failed* 2507340.1
- Oracle MOS Note *CMU Password Authenticated User Login fails With ORA-01017: invalid username/password; logon denied* 2492240.1

5.4 Software und Tools

5.4.1 Betriebsystem und Virtualizierung

- Oracle VM Virtualbox virtualbox
- HashiCorp Vagrant vagrant
- Oracle Enterprise Linux 7.6
  - 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-18.11.final.a.zip

5.4.2 Oracle Datenbank Binaries

- Oracle Base Releases 18c und 19c Oracle Technology Network
- April Critical Patch Update Oracle Database 18c
  - DATABASE RELEASE UPDATE 18.6.0.0.0 29301631
  - OJVM RELEASE UPDATE: 18.6.0.0.190416 29249584
  - CMU-AD: CUMULATIVE FIXES FOR DATABASE 18C 28994890
- OPatch 12.2.0.1.17 for DB 18.x releases (APR 2019) 6880880
- OPatch 12.2.0.1.17 for DB 19.x releases (APR 2019) 6880880

5.4.3 Oracle Unified Directory Binaries

- Oracle SERVER JRE 8 Update 212 29565620
- 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 12.2.1.3.190416 29016089
- OPatch Utility für WLS 28186730
- OUD Base Umgebungsskripte für Oracle Unified Directory oehrlis/oudbase

5.4.4 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