Configure EUS with OUD, AD and DB12c

How to configure Oracle Enterprise User Security (EUS) using current version of the Oracle Database (12.1), Oracle Unified Directory (OUD) and Microsoft Server 2012 Active Directory (AD) with Kerberos authentication

EUS can be used to authenticate Enterprise Users and Roles for the Oracle Database. The goal of this setup is that Active Directory users can log in to a connected Oracle Database using Kerberos without a database administrator having to create a local database user account for each individual user. Oracle Unified Directory (OUD) is used to store the OracleContext and configured to be an LDAP proxy to AD.

The setup has some nasty surprises before you are rewarded with a working installation.

Oracle Unified Directory installation

Check Linux server requirements

These packages are necessary according to documentation (for Oracle Enterprise Linux 6 (UL1+)):

- binutils-2.20.51.0.2-5.28.el6
- compat-libcap1-1.10-1
- compat-libstdc++-33-3.2.3-69.el6 for x86_64
- compat-libstdc++-33-3.2.3-69.el6 for i686
- gcc-4.4.4-13.el6
- gcc-c++-4.4.4-13.el6
- glibc-2.12-1.7.el6 for x86_64
- glibc-2.12-1.7.el6 for i686
- glibc-devel-2.12-1.7.el6 for i686
- libaio-0.3.107-10.el6
- libaio-devel-0.3.107-10.el6
- libgcc-4.4.4-13.el6
- libstdc++-4.4.4-13.el6 for x86_64
- libstdc++-4.4.4-13.el6 for i686
- libstdc++-devel-4.4.4-13.el6
- libXext for i686
- libXtst for i686
- libXext for x86_64
- libXtst for x86_64
- openmotif-2.2.3 for x86_64
- openmotif22-2.2.3 for x86_64
- redhat-lsb-core-4.0-7.el6 for x86_64

- sysstat-9.0.4-11.el6
- xorg-x11-utils*
- xorg-x11-apps*
- xorg-x11-xinit*
- xorg-x11-server-Xorg*
- xterm

Additional packages required for OUD:

- binutils-2.20.51.0.2-5.11.el6-x86_64
- compat-libcap1-1.10-1-x86_64
- **compat-libstdc++-33-3.2.3-69.el6-x86_64**
- **compat-libstdc++-33-3.2.3-69.el6-i686**
- **ibgcc-4.4.4-13.el6-i686**
- libgcc-4.4.4-13.el6-x86_64
- libstdc+-4.4.4-13.el6-x86_64
- **libstdc++-4.4.4-13.el6-i686**
- libstdc+-devel-4.4.4-13.el6-x86_64
- sysstat-9.0.4-11.el6-x86_64
- gcc-4.4.4-13.el6-x86_64
- gcc-c+-4.4.4-13.el6-x86_64
- **glibc-2.12-1.7.el6-i686**
- glibc-2.12-1.7.el6-x86_64
- glibc-devel-2.12-1.7.el6-x86_64
- glibc-devel-2.12-1.7.el6
- libaio-0.3.107-10.el6-x86_64
- libaio-devel-0.3.107-10.el6-x86_64

Name Resolution using DNS has to be available and correct between alle machines involved.

Download of necessary software

- wls1036_generic.jar
- ofm_oud_generic_11.1.2.3.0_disk1_1of1.zip (und ggf. aktuelle Patches)
- jdk-8u65-linux-x64.rpm
- ofm_appdev_generic_11.1.1.7.0_disk1_1of1.zip

Installation

Java 8

- rpm -ivh /u01/Software/jdk-8u65-linux-x64.rpm

Linux user & environment

- useradd -c "OUD Software Owner" -m oud
- vi .bash_profile

```
JAVA_HOME=/usr/java/jdk1.8.0_65 INSTANCE_NAME=oud-proxy OUD_HOME=/u01/Middleware/Oracle_OUD1 PATH=$PATH:$HOME
/bin:.:/usr/kerberos/bin:/usr/local/bin:/usr/bin:/bin:/usr/X11R6/bin:/home/oud/bin:$JAVA_HOME/bin:/u01/Middleware
/Oracle_OUD1/binexport PATH JAVA_HOME INSTANCE_NAME OUD_HOME
```

Oracle Unified Directory (OUD)

- Unpack software archive
- Run installer:
  - ./runInstaller -jreLoc /usr/java/jdk1.8.0_65/jre
  - OUD Base Location: /u01/Middleware
  - everything else: default

WebLogic Server 11g (WLS)

WLS 10.3.6 (11g) is used for ODSM (Oracle LDAP GUI in Weblogic). You could also use an Open Source product like Apache Directory Studio.

- Check available disk space in /tmp before installation
- /usr/java/jdk1.8.0_65/bin/java -Djava.io.tmpdir=/var/tmp -jar wls1036_generic.jar
- Create a new Middleware Home in /u01/Middleware
- Ignore a warning message regarding the non-empty middleware directory
- Custom Installation, without Coherence
- Do not run QuickStart at the end of installation

Application Developerment Framework(ADF)

- Unpack software archive
- ./runInstaller -jreLoc /usr/java/jdk1.8.0_65/jre

Configuration

Deploy ODSM

- [oud@ioaotow03 Middleware]$ oracle_common/common/bin/config.sh
- Create new WebLogic Domain "odsm"
- Select component "Oracle Directory Services Manager" (Oracle JRF is automatically selected)
- Username (weblogic) / passwort for WebLogic Domain
- Setup-type is "Production"

Provide the web logic password:

```
[~]$ cd /u01/Middleware/user_projects/domains/odsm/servers/AdminServer/

[AdminServer]$ mkdir security

[AdminServer]$ cd security

[security]$ vi boot.properties
username=weblogic password=...
```

At weblogic startup, the password is automatically encrypted in the file boot.properties, so you do not have to provide it any more.

Start Weblogic server

- [oud@ioaotow03 Middleware]$ user_projects/domains/odsm/bin/startWebLogic.sh
- You can reach WebLogic server at (in our example): http://ioaotow03.tested.lcl:7001/odsm/+

Create Active Directory access user

We need an AD user for OUD to connect to AD to obtain the information it shall proxy to the database. This AD user has to have read access privileges on AD users and groups.
Username: **CN=oud-proxy,OU=AO,OU=IT-Department,DC=tested,DC=lcl**

Proxy-Configuration

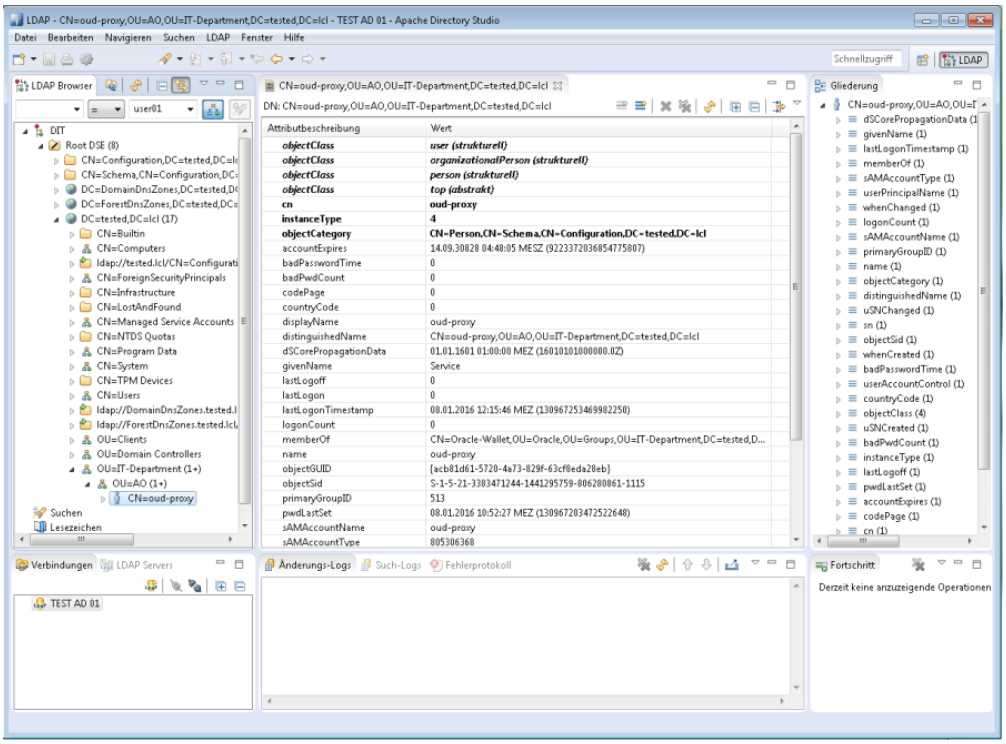
Environment

Set $INSTANCE_NAME: $ echo $INSTANCE_NAME

AD directory tree

We have to check AD access using the proxy used created in previous step.

We can use Apache Directory Studio.



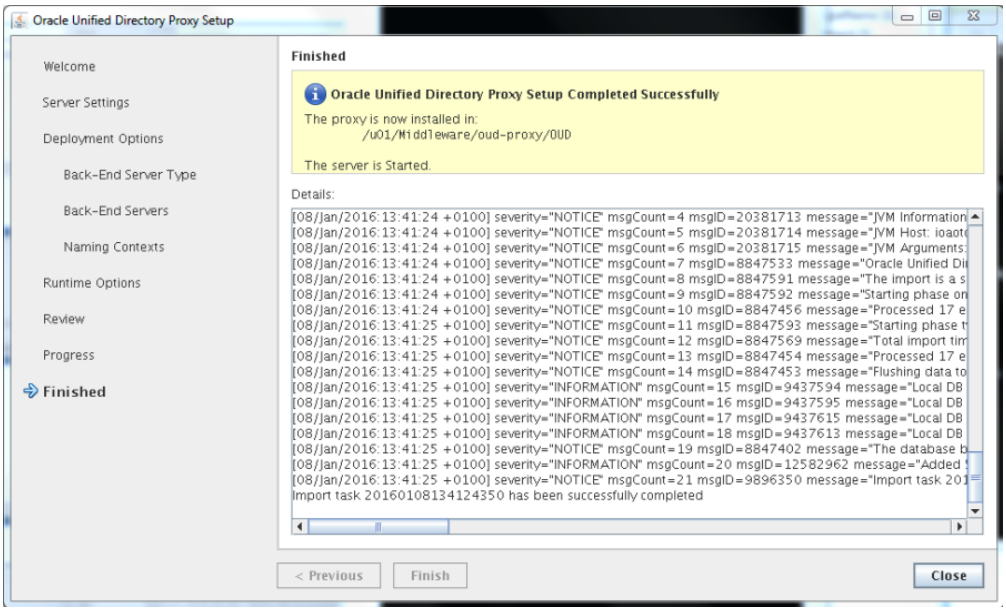
OUD proxy setup

Actual configuration of the OUD proxy is done by the script "oud-proxy-setup":

```
[oud@ioaotow03 Oracle_OUD1]$ ./oud-proxy-setup
```

Secure Access has to be enabled für EUS. The OUD server has to be entered as proxy server. LDAP ports are *1389* and LDAPS *1636*. AdminPort ODSM access is 4444. Root user of OUD is cn=Directory Manager.

Naming Context is in our example: **OU=AO,OU=IT-Department,DC=tested,DC=lcl**



Proxy post installation steps

Konfigurieren der Workflow-Elemente

Remote Credentials for the AD access user are stored in a Workflow Element of the proxy.

First, we write the password to a temporary file:

```
[oud ~]$ touch /tmp/password.txt [oud ~]$ vi /tmp/password.txt ...
```

Now, we setup the necessary workflow elements with "dsconfig":

```
dsconfig set-workflow-element-prop \
--element-name proxy-we1 \
--set remote-root-dn:CN=oud-proxy,OU=AO,OU=IT-Department,DC=tested,DC=lcl \
--set remote-root-password:XXX \
--hostname ioaotow03.tested.lcl \
--port 4444 \
--trustAll \
--bindDN cn=Directory\ Manager \
--bindPasswordFile /tmp/password.txt \
--no-prompt

dsconfig set-workflow-element-prop \
--element-name proxy-we1 \
--add exclude-list:cn=Directory\ Manager \
--add exclude-list:cn=oraclecontext,OU=AO,OU=IT-Department,DC=tested,DC=lcl \
--set remote-ldap-server-bind-dn:CN=oud-proxy,OU=AO,OU=IT-Department,DC=tested,DC=lcl \
--set remote-ldap-server-bind-password:XXX \
--hostname ioaotow03.tested.lcl \
--port 4444 \
--trustAll \
--bindDN cn=Directory\ Manager \
--bindPasswordFile /tmp/password.txt \
--no-prompt
```

"XXX" is the Active Directory access user password.

Initial loading of the OracleContext

OUD is now configured to access the AD directory for the user and group data and OUD for the OracleContext. Now we have to fill in the necessary startup information into the OracleContext. The file /u01/Middleware/Oracle_OUD1/config/EUS/modifyRealm.ldif can be modified and used:

```
[oud@ioaotow03 ~]$ ldapmodify -h ioaotow03 -p 1389 -D "cn=Directory Manager"  -j /tmp/password.txt -v -f
EOS_modifyRealm.ldif
```

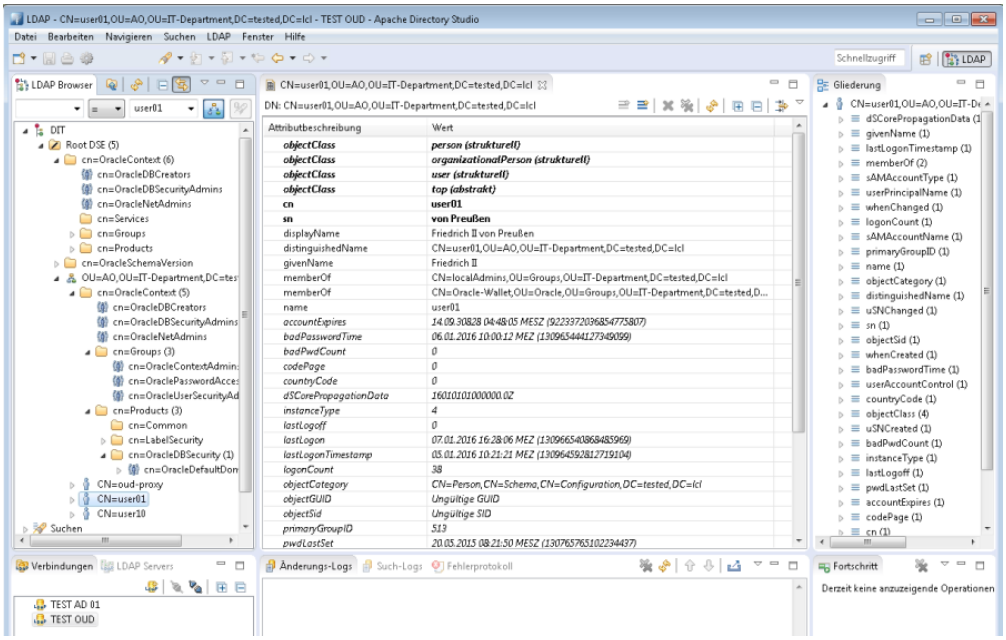
In the next step we provide the Kerberos settings for the OracleContext:

```
[oud@ioaotow03 ~]$ ldapmodify -h ioaotow03 -p 1389 -D "cn=Directory Manager" -j /tmp/password.txt -v -f
NickNameAttribute.ldif
```

```
[oud@ioaotow03 ~]$ ldapmodify -h ioaotow03 -p 1389 -D "cn=Directory Manager" -j /tmp/password.txt -v -f
KerberosPrincipal.ldif [oud@ioaotow03 ~]$ rm /tmp/password.txt
```

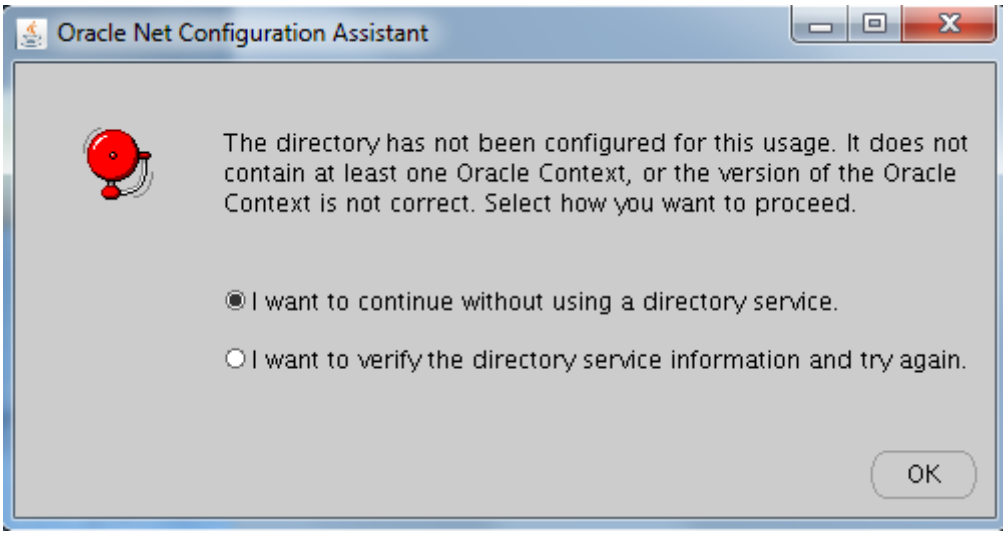
LDAP proxy server check

We can now browse the OracleContext and the AD user data in the OUD LDAP directory using an LDAP browser.



Configure LDAP access for the database

Usually, with Oracle Internet Directory (OID), this step would be done using Network Creation Assistant. With OUD and AD backend, NetCA pops up this error message when used to configure LDAP settings:



The console reads:

```
ConfigException: Could not get a list of Oracle Contexts: oracle.net.config.ConfigException: TNS-04409: Directory
service error   caused by: oracle.net.config.DirectoryServiceException: TNS-04405: General error   caused
by: oracle.net.ldap.NNFLException
```

OUD logfile reads:

```
[27/Jan/2016:19:12:29 +0100] SEARCH PROXY_RES conn=21 op=2 msgID=3 result=1 nentries=0 Message="000004DC:
LdapErr: DSID-0C09072B, comment: In order to perform this operation a successful bind must be completed on the
connection., data 0, v2580" etime=1 authzDN= s_conn=2 s_msgid=8
```

NetCA wants to perform an anonymous LDAP bind to the AD server, which is prohibited there.

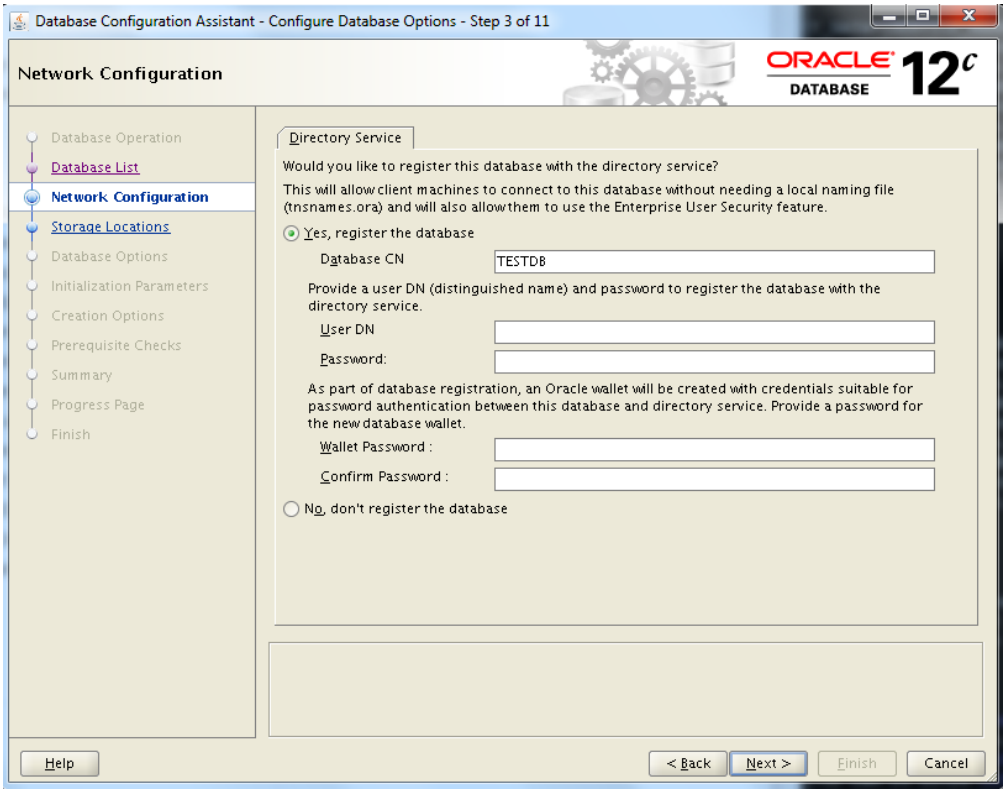
Oracle Support MOS Doc ID 1571196.1 states: "*If your organization is concerned about anonymous access to AD: you can enable the anonymous access to AD, run NETCA, then disable the anonymous access to AD, or you can create the ldap.ora manually, instead of using NETCA to create this configuration file*" 😉

But it is just sufficient to create the LDAP configuration manually:

```
DIRECTORY_SERVERS= (ioaotow03.tested.lcl:1389:1636)
DEFAULT_ADMIN_CONTEXT = "OU=AO,OU=IT-Department,DC=tested,DC=lcl"
DIRECTORY_SERVER_TYPE = OID
```

Register database with directory

This step is done using Database Configuration Assistant (DBCA).



We provide the login data to access OUD (CN=Directory Manager). During DBCA configuration, a new wallet is created for SSL communication between database and OUD:

```
[oracle@ioaotow01 ~]$ ls -lhrt /oracle/admin/TESTDB/wallet
total 8.0K
rw-rw-rw 1 oracle oinstall   0 Jan 15 15:45 ewallet.p12.lck
rw------ 1 oracle oinstall 456 Jan 15 15:45 ewallet.p12
rw-rw-rw 1 oracle oinstall   0 Jan 15 15:45 cwallet.sso.lck
rw------ 1 oracle oinstall 501 Jan 15 15:45 cwallet.sso
```

Configuration of EUS

Create Test accounts:

```
SQL> create user global_ident identified globally;
User created.
SQL> grant connect to global_ident;
Grant succeeded.
```

Mapping between local and global users

The necessary mappings can be created and administered with Enterprise Manager or the CLI tool "eusm".

List current mappings:

```
eusm listMappings realm_dn="OU=AO,OU=IT-Department,DC=tested,DC=lcl" ldap_port=1389 ldap_host=ioaotow03.tested.
lcl ldap_user_dn="cn=Directory Manager" ldap_user_password=welcome1 database_name=testdb
javax.naming.AuthenticationException: [LDAP: error code 49 - Invalid Credentials]
```

This is caused by Bug 21678564:

> *A quick workaround is to remove all the whitespaces and have all the characters written in lower case*

You may be tempted to install patch 21678564/20851192 after reading MOS information. Do not do that, or it will look like:

```
[oracle@ioaotow01 ~]$ eusm listMappings realm_dn="OU=AO,OU=IT-Department,DC=tested,DC=lcl" ldap_port=1389
ldap_host=ioaotow03.tested.lcl  ldap_user_dn="cn=Directory Manager" ldap_user_password=welcome1
database_name=testdb

Exception in thread "main" java.lang.NoClassDefFoundError: oracle/ldap/util/Util

 at oracle.security.eus.esm.EUSLogin.initOIDContext(EUSLogin.java:165)

 at oracle.security.eus.util.ESMdriver.main(ESMdriver.java:105)

 Caused by: java.lang.ClassNotFoundException: oracle.ldap.util.Util

 at java.net.URLClassLoader$1.run(URLClassLoader.java:202)

 at java.security.AccessController.doPrivileged(Native Method)

 at java.net.URLClassLoader.findClass(URLClassLoader.java:190)

 at java.lang.ClassLoader.loadClass(ClassLoader.java:306)

 at sun.misc.Launcher$AppClassLoader.loadClass(Launcher.java:301)

 at java.lang.ClassLoader.loadClass(ClassLoader.java:247)

 ... 2 more
```

A better solution can be found after consulting the OUD log files in the WebLogic directory (Middleware/oud-proxy/OUD/logs):

```
[oud@ioaotow03 logs]$ tail -f access
[27/Jan/2016:11:14:49 +0100] BIND RES conn=156 op=1 msgID=2 result=49 authFailureID=1310929 authFailureReason="
SASL DIGEST-MD5 protocol error: SaslException(DIGEST-MD5: digest response format violation. Mismatched URI: ldap
/ioaotow03.tested.lcl; expecting: ldap/ioaotow03)" etime=0
```

Use caution to provide the hostname in the exactly matching form. After fixing this error, on the database site it still looks like:

```
eusm listMappings realm_dn="OU=AO,OU=IT-Department,DC=tested,DC=lcl" ldap_port=1389 ldap_host=ioaotow03
ldap_user_dn="cn=Directory Manager" ldap_user_password=welcome1 database_name="testdb"
javax.naming.AuthenticationException: [LDAP: error code 49 - Invalid Credentials]
```

The logfile states:

```
[27/Jan/2016:11:22:34 +0100] BIND REQ conn=160 op=1 msgID=2 type=SASL mechanism=DIGEST-MD5 dn="" version=3
[27/Jan/2016:11:22:34 +0100] BIND RES conn=160 op=1 msgID=2 result=49 authFailureID=1245385 authFailureReason="
The server was not able to find any user entries for the provided username of CN=Directory Manager" etime=7
```

The solution is a current Oracle Bug: 20529805 - SUPPORT FOR EUSM 12C AUTHENTICATION SCHEME IN OUD IS MISSING:

> *As of now OUD SASL implementation assumes that a DN identity is prefixed by the dn: prefix as defined in RFC 2829 ({+}http://www.ietf.org/rfc/rfc2829.txt+). EUSM does not uses the dn: prefix, so default identity mapping in OUD is applied and EUS SASL authentication will fail.*

See: MOS Doc ID 2093460.1

Solution: Install patch **20529805**. OUD has to be stopped for the patch installation.

After patch installation, the situation looks the same when calling eusm. But the logfile now reads:

```
[27/Jan/2016:11:48:49 +0100] BIND RES conn=2 op=1 msgID=2 result=49 authFailureID=1245392 authFailureReason="SASL
DIGEST-MD5 authentication is not possible for user cn=Directory Manager,cn=Root DNs,cn=config because none of the
passwords in the user entry are stored in a reversible form" etime=107
```

Well, what kind of hash to we use actually?

```
[oud@ioaotow03 Oracle_OUD1]$ less config/config.ldif
dn: cn=Directory Manager,cn=Root DNs,cn=config
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: ds-cfg-root-dn-user
cn: Directory Manager
givenName: Directory
sn: Manager
userPassword: {SSHA512}l1tXXXXXXXxXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXG9Z
```

Let's see... I think we might have another problem. Let's take a look at MOS Doc ID 2016510.1. Looks like the old-proxy-setup script has missed something:

> *"You need to modify Root Password Policy using dsconfig to add a default-password-storage-scheme (either AES or Base64 or Blowfish or Clear or RC4 or TripleDES, ie one of the reversible storage schemes)"*

Solution:

```
[oud@ioaotow03 ~]$ /u01/Middleware/oud-proxy/OUD/bin/dsconfig -h ioaotow03 -p 4444 -D "cn=Directory Manager" -j
/tmp/pwd.txt --advanced
```

Go to "Change root password policy". This currently is set to:

```
    6)   default-password-storage-scheme            Salted SHA-512
```

Change to:

```
   6)   default-password-storage-scheme            AES, Salted SHA-512
```

We need to set a new password to generate the new hash:

```
[oud@ioaotow03 ~]$ which ldappasswordmodify
/u01/Middleware/oud-proxy/OUD/bin/ldappasswordmodify
[oud@ioaotow03 ~]$ ldappasswordmodify -h ioaotow03 -p 4444 -D "cn=Directory Manager" -j /tmp/pwd.txt --useSSL -c
welcome1 -n secret12
The server is using the following certificate:
    Subject DN:  CN=ioaotow03, O=Administration Connector Self-Signed Certificate
    Issuer DN:  CN=ioaotow03, O=Administration Connector Self-Signed Certificate
    Validity:  Fri Jan 08 13:41:17 CET 2016 through Sun Jan 07 13:41:17 CET 2018
Do you wish to trust this certificate and continue connecting to the server?
Please enter "yes" or "no":yes
The LDAP password modify operation was successful
```

Let's risk a look:

```
[oud@ioaotow03 ~]$ ldapsearch -h ioaotow03 -p 4444 -D "cn=Directory Manager" --useSSL -j /tmp/pwd.txt -b
"cn=Directory Manager,cn=Root DNs,cn=config" -s base objectclass=* userpassword dn: cn=Directory Manager,cn=Root
DNs,cn=config
userpassword: {AES}XXXXXXXXXXXXXXXXXXXXXXM=
userpassword: {SSHA512}XXXXXXXXXXXXXXXXXXXXXXXXXXXXK

[oracle@ioaotow01 ~]$ eusm listMappings realm_dn="OU=AO,OU=IT-Department,DC=tested,DC=lcl" ldap_port=1389
ldap_host=ioaotow03 ldap_user_dn="CN=Directory Manager" ldap_user_password="secret12" database_name="testdb"

LIST OF DATABASE SCHEMA MAPPINGS::
-----------------------------------
```

Finally, we can create some mappings now. This mapping throws all users from the organizational unit AO into the database user GLOBAL_IDENT we created earlier:

```
[oracle@ioaotow01 ~]$ eusm createMapping realm_dn="OU=AO,OU=IT-Department,DC=tested,DC=lcl" ldap_port=1389
ldap_host=ioaotow03  ldap_user_dn="cn=Directory Manager" ldap_user_password="secret12" database_name="testdb"
map_type="SUBTREE" map_dn="U=AO,OU=IT-Department,DC=tested,DC=lcl" schema=GLOBAL_IDENT

[oracle@ioaotow01 ~]$ eusm listMappings realm_dn="OU=AO,OU=IT-Department,DC=tested,DC=lcl" ldap_port=1389
ldap_host=ioaotow03 ldap_user_dn="CN=Directory Manager" ldap_user_password="secret12" database_name="testdb"
LIST OF DATABASE SCHEMA MAPPINGS::
-----------------------------------
Mapping Name:  MAPPING0
Mapping Type:  SUBTREE
Mapping DN:    U=AO,OU=IT-Department,DC=tested,DC=lcl
Mapping schema:GLOBAL_IDENT
Mapping Level :DATABASE
```

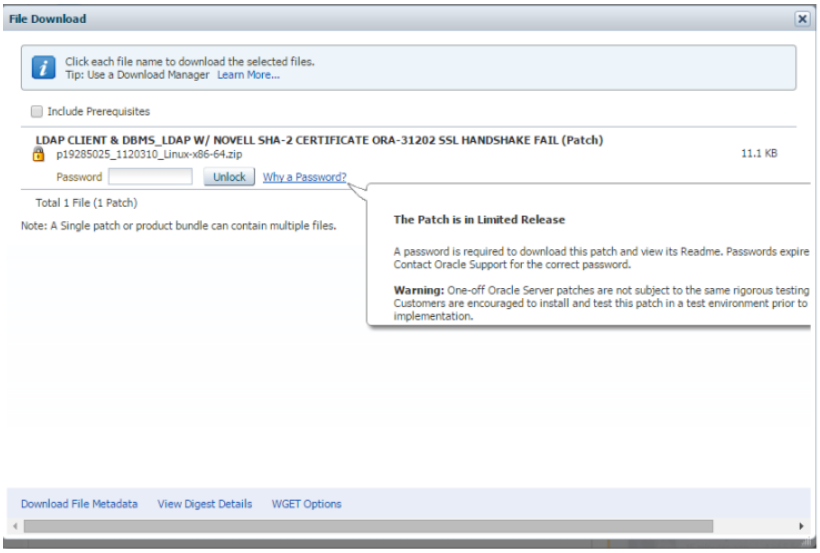
Test database login

```
[oracle@ioaotow01 ~]$ sqlplus user10
SQL*Plus: Release 12.1.0.2.0 Production on Wed Jan 27 18:45:09 2016
Copyright (c) 1982, 2014, Oracle.  All rights reserved.
Enter password:
ERROR: ORA-28030: Server encountered problems accessing LDAP directory service
```

OUD logfile (/u01/Middleware/asinst_1/OUD/logs/access resp. /u01/Middleware/asinst_1/OUD/logs/server.out) reads:

```
[27/Jan/2016:18:45:10 +0100] DISCONNECT conn=38 reason="I/O Error" msg="Client requested protocol SSLv3 not
enabled or not supported"
```

This is a known Oracle bug. After the poodle attack, Oracle just disabled SSLv3 in Java, but it is still necessary for a database login query. There is a patch for the Oracle Database from 11.2.0.3, but it is not available to the public.



We can re-enable SSLv3 in our Java version to get running for the time being:

```
[oud@ioaotow03 ~]$ java -version
java version "1.8.0_65"
Java(TM) SE Runtime Environment (build 1.8.0_65-b17)
Java HotSpot(TM) 64-Bit Server VM (build 25.65-b01, mixed mode)

[root@ioaotow03 oud]# vi /usr/java/jdk1.8.0_65/jre/lib/security/java.security
old: jdk.tls.disabledAlgorithms=SSLv3, DH keySize < 768

new: jdk.tls.disabledAlgorithms=RC4, DH keySize < 768
```

Restart OUD:

```
[oud@ioaotow03 ~]$ /u01/Middleware/oud-proxy/OUD/bin/stop-ds
[oud@ioaotow03 ~]$ /u01/Middleware/oud-proxy/OUD/bin/start-ds
```

Map AD groups to Oracle roles

Create an Enterprise Role:

```
[oracle@ioaotow01 ~]$ eusm createRole enterprise_role="OUD_DBA" domain_name="OracleDefaultDomain" realm_dn="OU=AO,
OU=IT-Department,DC=tested,DC=lcl" ldap_port=1389 ldap_host=ioaotow03 ldap_user_dn="cn=Directory Manager"
ldap_user_password="secret12"
[oracle@ioaotow01 ~]$ eusm listEnterpriseRoles domain_name="OracleDefaultDomain" realm_dn="OU=AO,OU=IT-Department,
DC=tested,DC=lcl" ldap_port=1389 ldap_host=ioaotow03 ldap_user_dn="cn=Directory Manager" ldap_user_password="
secret12"
LIST OF ENTERPRISE ROLES IN DOMAIN: OracleDefaultDomain
------------------------------------------------
OUD_DBA
```

Create a Global Role in the database:

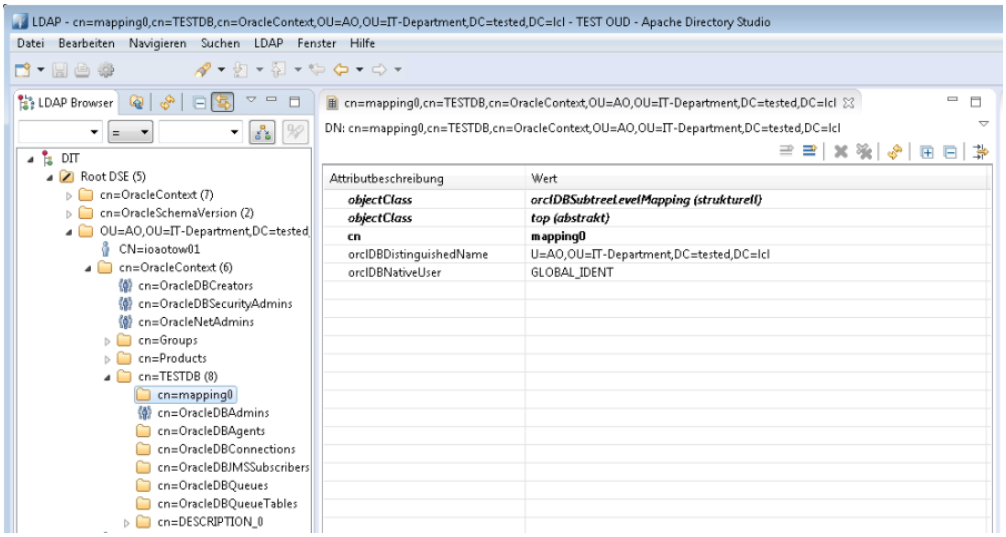
```
SQL> create role GLOBAL_DBA identified globally;
Role created.
SQL> grant DBA to GLOBAL_DBA;
```

Connect the Roles in EUS:

```
[oracle@ioaotow01 ~]$ eusm addGlobalRole enterprise_role="OUD_DBA" domain_name="OracleDefaultDomain" realm_dn="
OU=AO,OU=IT-Department,DC=tested,DC=lcl" database_name="testdb" global_role="GLOBAL_DBA" dbuser="sys as sysdba"
dbuser_password="welcome01" dbconnect_string="ioaotow01:1521:testdb" ldap_host=ioaotow03 ldap_port=1389
ldap_user_dn="cn=Directory Manager" ldap_user_password="secret12"
[oracle@ioaotow01 ~]$ eusm grantrole enterprise_role="OUD_DBA" domain_name="OracleDefaultDomain" realm_dn="OU=AO,
OU=IT-Department,DC=tested,DC=lcl" group_dn="cn=DBA,OU=AO,OU=IT-Department,DC=tested,DC=lcl" ldap_port=1389
ldap_host=ioaotow03  ldap_user_dn="cn=Directory Manager" ldap_user_password="secret12"
```

Check the mapping in LDAP OracleContext

The new mappings can be seen in an LDAP browser:



Login as Enterprise User

Test

```
C:\Users\user10>sqlplus /@TESTDB_TNS
SQL*Plus: Release 12.1.0.2.0 Production on Di Feb 9 13:31:16 2016
Copyright (c) 1982, 2014, Oracle.  All rights reserved.
ERROR:
ORA-28030: Server encountered problems accessing LDAP directory service
```

The cause of this error can be seen in the trace file on the database server:

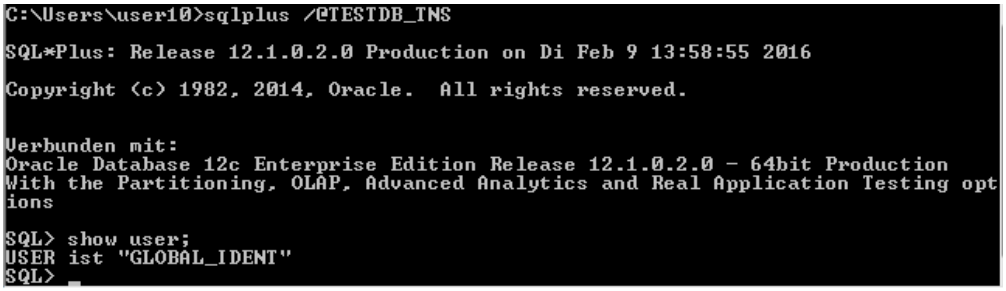
```
$ cat /oracle/diag/rdbms/testdb/TESTDB/trace/TESTDB_ora_811.trc ... kzld_discover received ldaptype: OID
KZLD_ERR: failed to get cred from wallet KZLD_ERR: Failed to bind to LDAP server. Err=28032 KZLD_ERR: 28032 KZLD
is doing LDAP unbind KZLD_ERR: found err from kzldini.
```

DBCA has stored the credentials needed to access OUD via LDAP into the database wallet. But in the meantime, we created a new wallet for SSL. We have to use the correct wallet.

```
[oracle@ioaotow01 ~]$ mkstore -wrl /oracle/admin/TESTDB/wallet -list

Oracle Secret Store entries:
ORACLE.SECURITY.DN
ORACLE.SECURITY.PASSWORD
[oracle@ioaotow01 ~]$ mkstore -wrl /oracle/admin/TESTDB/wallet -viewEntry ORACLE.SECURITY.DN
ORACLE.SECURITY.DN = cn=TESTDB,cn=OracleContext,OU=AO,OU=IT-Department,DC=tested,DC=lcl
```

New attempt:



Connect as Enterprise User with privileges from the DBA role

```
[oracle@ioaotow01 ~]$ eusm createMapping realm_dn="OU=AO,OU=IT-Department,DC=tested,DC=lcl" ldap_port=1389
ldap_host=ioaotow03  ldap_user_dn="cn=Directory Manager" ldap_user_password="secret12" database_name="testdb"
map_type="ENTRY" map_dn="CN=user01,OU=AO,OU=IT-Department,DC=tested,DC=lcl" schema=GLOBAL_ADMIN
[oracle@ioaotow01 ~]$ eusm listMappings realm_dn="OU=AO,OU=IT-Department,DC=tested,DC=lcl" ldap_port=1389
ldap_host=ioaotow03 ldap_user_dn="CN=Directory Manager" ldap_user_password="secret12" database_name="testdb"
LIST OF DATABASE SCHEMA MAPPINGS::
-----------------------------------
Mapping Name:  MAPPING0
Mapping Type:  SUBTREE
Mapping DN:    OU=AO,OU=IT-Department,DC=tested,DC=lcl
Mapping schema:GLOBAL_IDENT
Mapping Level :DATABASE
Mapping Name:  MAPPING1
Mapping Type:  SUBTREE
Mapping DN:    CN=DBA,OU=AO,OU=IT-Department,DC=tested,DC=lcl
Mapping schema:GLOBAL_ADMIN
Mapping Level :DATABASE
Mapping Name:  MAPPING2
Mapping Type:  ENTRY
Mapping DN:    CN=user01,OU=AO,OU=IT-Department,DC=tested,DC=lcl
Mapping schema:GLOBAL_ADMIN
Mapping Level :DATABASE
SQL> drop user user01@tested.lcl
SQL> create user GLOBAL_DBA identified globally;
SQL> grant DBA to GLOBAL_ADMIN;
```

```
C:\Users\user01>sqlplus /@TESTDB_TNS

SQL*Plus: Release 12.1.0.2.0 Production on Di Feb 9 14:45:40 2016

Copyright (c) 1982, 2014, Oracle.  All rights reserved.


Verbunden mit:
Oracle Database 12c Enterprise Edition Release 12.1.0.2.0 - 64bit Production
With the Partitioning, OLAP, Advanced Analytics and Real Application Testing
ions

SQL> show user;
USER ist "GLOBAL_ADMIN"
SQL> desc dba_users;
 Name                                      Null?    Typ
 ----------------------------------------- -------- ----------------------------

 USERNAME                                  NOT NULL VARCHAR2(128)
```

Related articles

- Kreis Stormarn
- ProxMox: VNC-Verbindung zur Konsole ohne WebGUI
- Configure EUS with OUD, AD and DB12c
- Zimbra Anti-Spam Configuration
- How to fix an ORA-28043 error between Oracle database and LDAP directory