ORA-SOLUTIONS.NET
Mastering Oracle Performance, High Availability, Manageability

Enterprise User Security

Eine Einführung

DOAG Regionaltreffen München
18. September 2014

Agenda

- Vorstellung
- Benutzerverwaltung – Problemstellung
- Lösung: Enterprise User Security
- Implementierung
- EUS Use-Cases
  - Schema Mapping
  - Enterprise Roles
  - Proxy Permissions

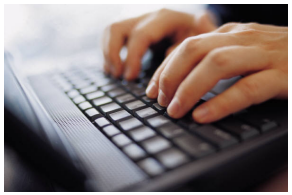
Wer bin ich?

- 10 Jahre Oracle Datenbank Erfahrung
- Seit 6 Jahren unabhängiger Oracle Consultant in D/A/CH
- Spezialisierung auf:
  - Performance Management (Instance / SQL)
  - Hochverfügbarkeit (MAA, RAC, DataGuard)
  - Manageability (OEM)
  - Unix (Linux, Solaris, HP-UX)
- Oracle Certified Master 10g & 11g
- Website & Blog: ora-solutions.net

- dutzende DB Accounts lokal in einer Vielzahl von verschiedenen Datenbanken mit möglicherweise unterschiedlichen Passworten
- Password Policy (Expiry) erzwingt regelmäßige Passwort-Änderung in allen Datenbanken
- Entfernung von Benutzer-Accounts bei Verlassen des Unternehmens
- hoher Administrationsaufwand
- Oracles Lösung für diese Problemstellung: **Enterprise User Security**

EUS - Einführung

- Teil von Oracle Database Enterprise Edition
- Authentifizierung nicht gegenüber SYS.USER$ Tabelle, sondern gegenüber LDAP Directory
- Directory Services Plus License (min 2000 User á 12 USD)
- Benötigt spezielles Directory (lizenzpflichtig)
  - Oracle Virtual Directory (OVD) -> 3rd Party LDAP Backend/AD
  - Oracle Internet Directory (OID) -> 3rd Party LDAP Backend/AD
  - Oracle Unified Directory (OUD)



EUS – Begriffe

- Komponenten:
  - In Datenbank: („GLOBAL“)
    - Global User:
      ```
      CREATE USER <username> IDENTIFIED EXTERNALLY;
      ```
    - Global Role:
      ```
      CREATE ROLE <role> IDENTIFIED EXTERNALLY;
      ```
  - In LDAP: („ENTERPRISE“)
    - Enterprise Domain (Container für DBs)
    - Enterprise Users (LDAP User-Eintrag)
    - Enterprise Roles (Mapping zw. Enterprise Users und Global Roles)
    - Proxy Permissions (Mapping zw. Enterprise Users und Proxy Users)

Implementierung OVD

- Installation LDAP Directory (z.B. ODSEE)
- Installation Oracle Weblogic 10.3.6
- Installation Oracle Identity Management 11.1.1.2.0
- Upgrade auf Oracle Identity Management 11.1.1.7.0
- Configuration Oracle Virtual Directory
- Create LDAP Suffix
- OracleContext / Schema Configuration
- Configure ldap.ora
- DBCA: Register Database
- Configure Schema Mapping, Enterprise Roles, Proxy Permissions

Implementierung OUD

- Installation JDK 1.7
- Installation OUD 11.1.2.2.0
- Installation Oracle Weblogic 10.3.6
- Installation Oracle ADF 11.1.1.7.0
- Configure ODSM mit ADF für OUD
- Configure OUD
- LDAP User anlegen
- Configure ldap.ora
- DBCA: Register Database
- Configure Schema Mapping, Enterprise Roles, Proxy Permissions

Implementierung OUD

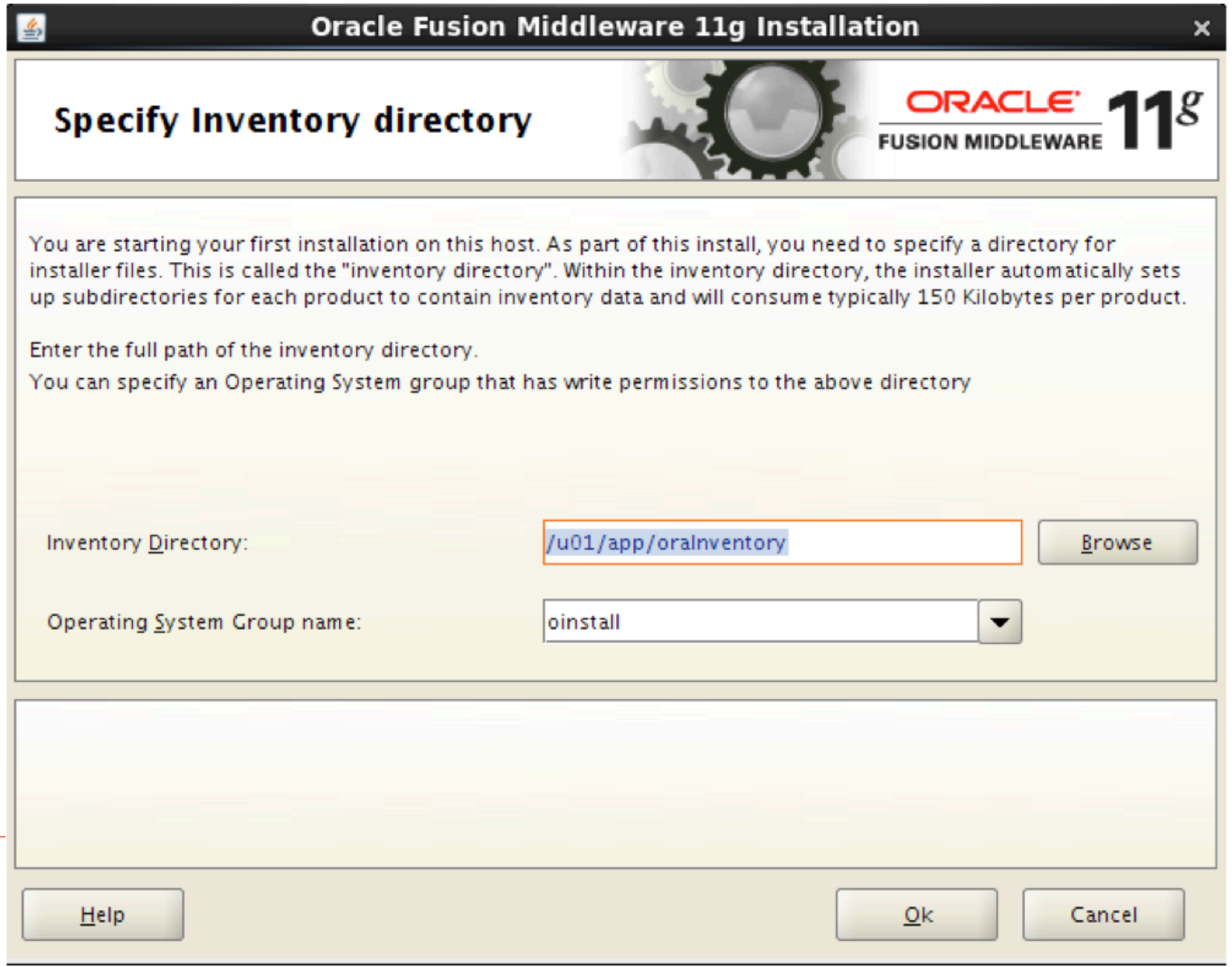
Download Files:

- jdk-7u55-linux-x64.tar.gz
- ofm_oud_generic_11.1.2.2.0_disk1_1of1.zip
- wls1036_generic.jar
- ofm_appdev_generic_11.1.1.7.0_disk1_1of1.zip

Implementierung OUD

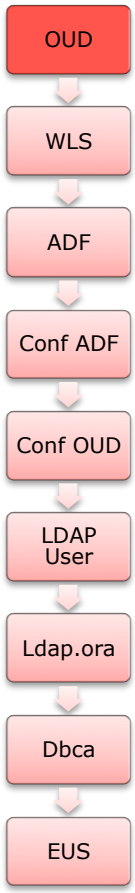
OUD: (JDK Installiert nach /u01/app/jdk)
./runInstaller -jreLoc /u01/app/jdk/jre

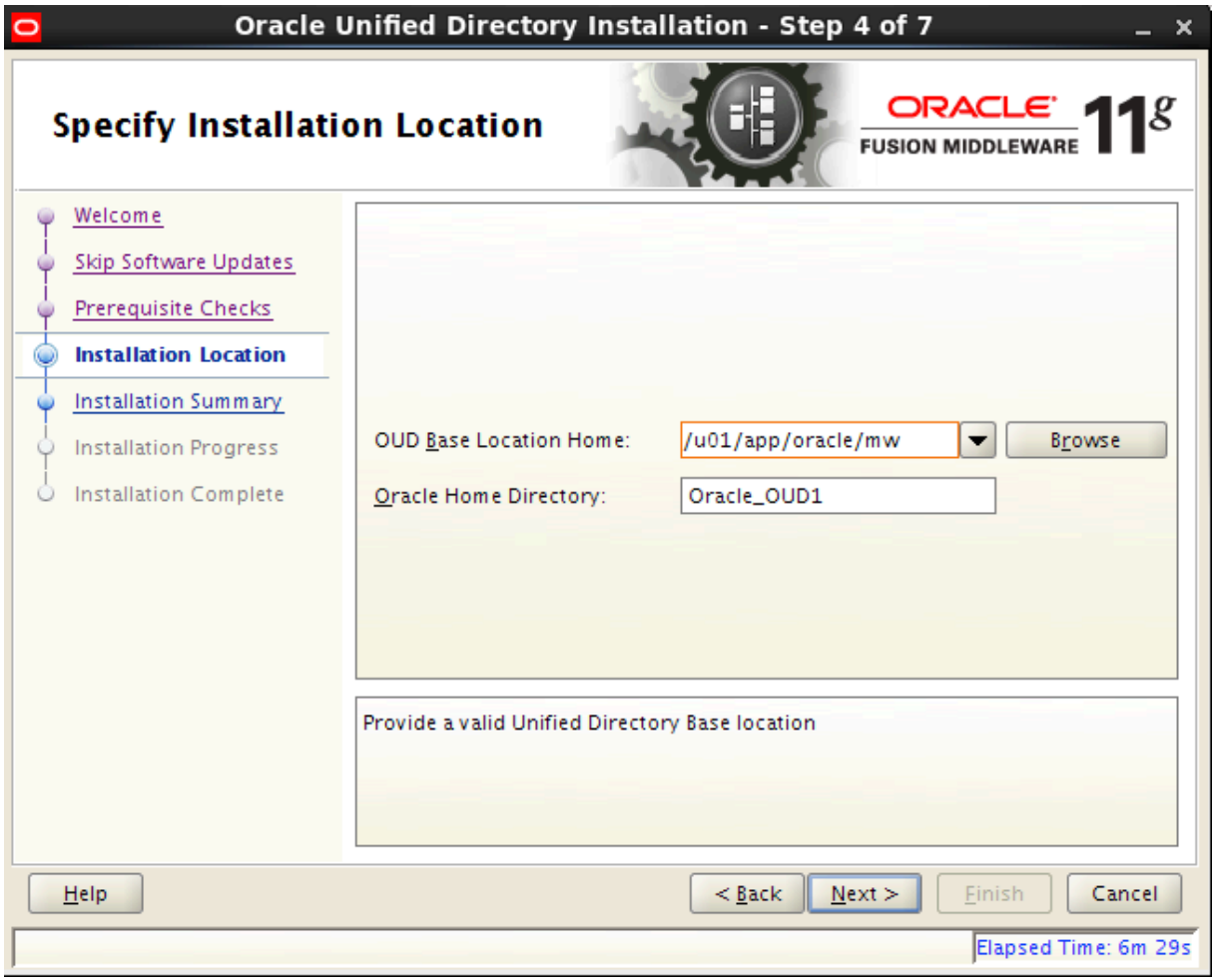
- OUD
- WLS
- ADF
- Conf ADF
- Conf OUD
- LDAP User
- Ldap.ora
- Dbca
- EUS



Implementierung OUD

OUD:

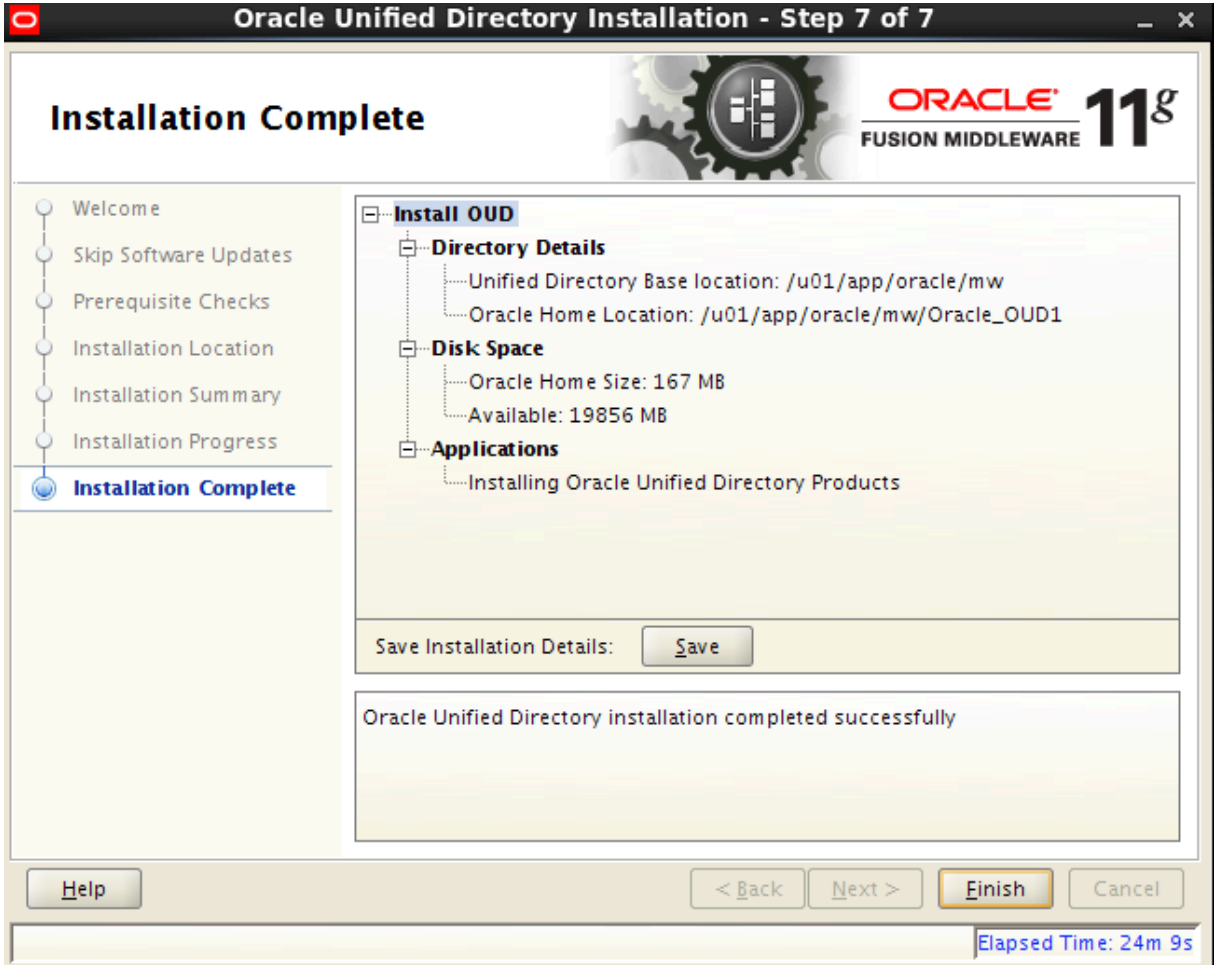




Implementierung OUD

OUD:

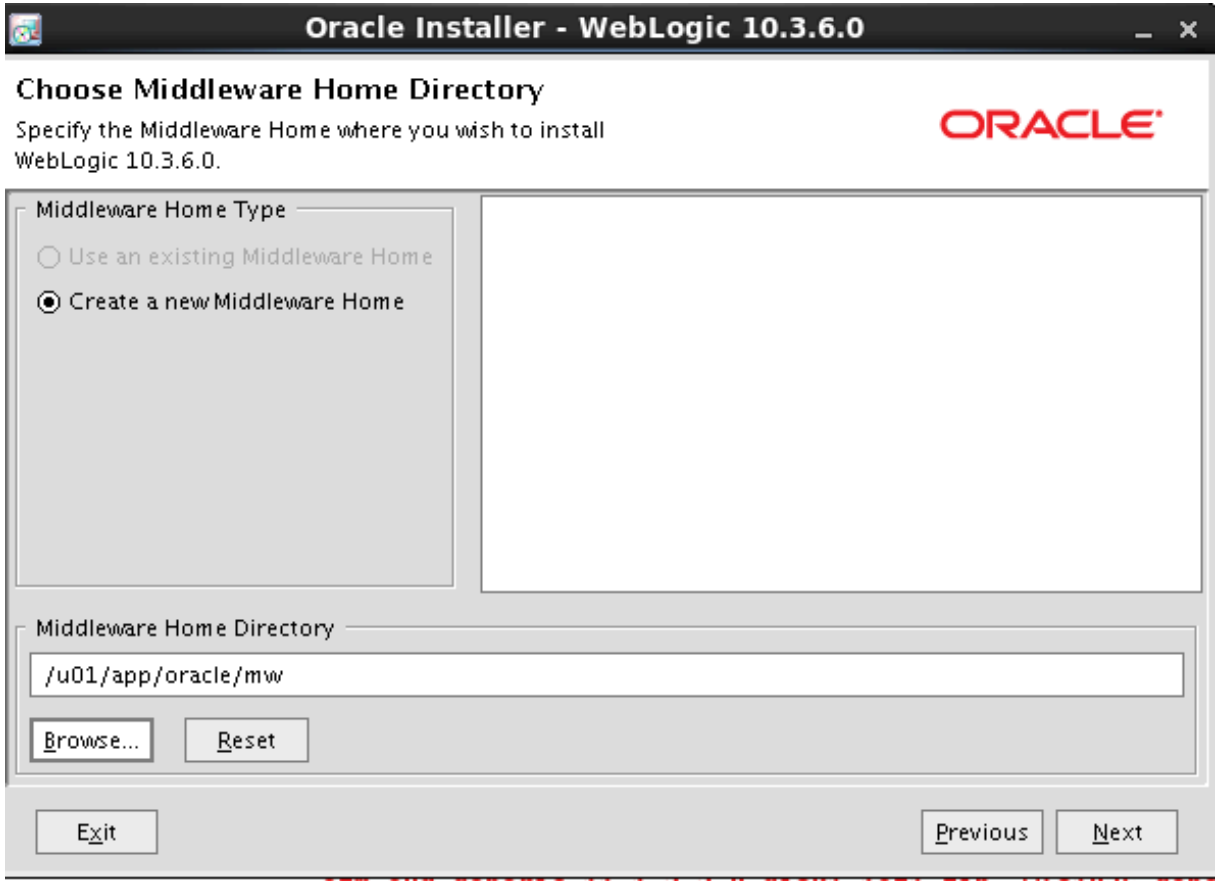
- OUD
- WLS
- ADF
- Conf ADF
- Conf OUD
- LDAP User
- Ldap.ora
- Dbca
- EUS



Implementierung OUD

Weblogic: java -d64 -jar wlsversion_generic.jar

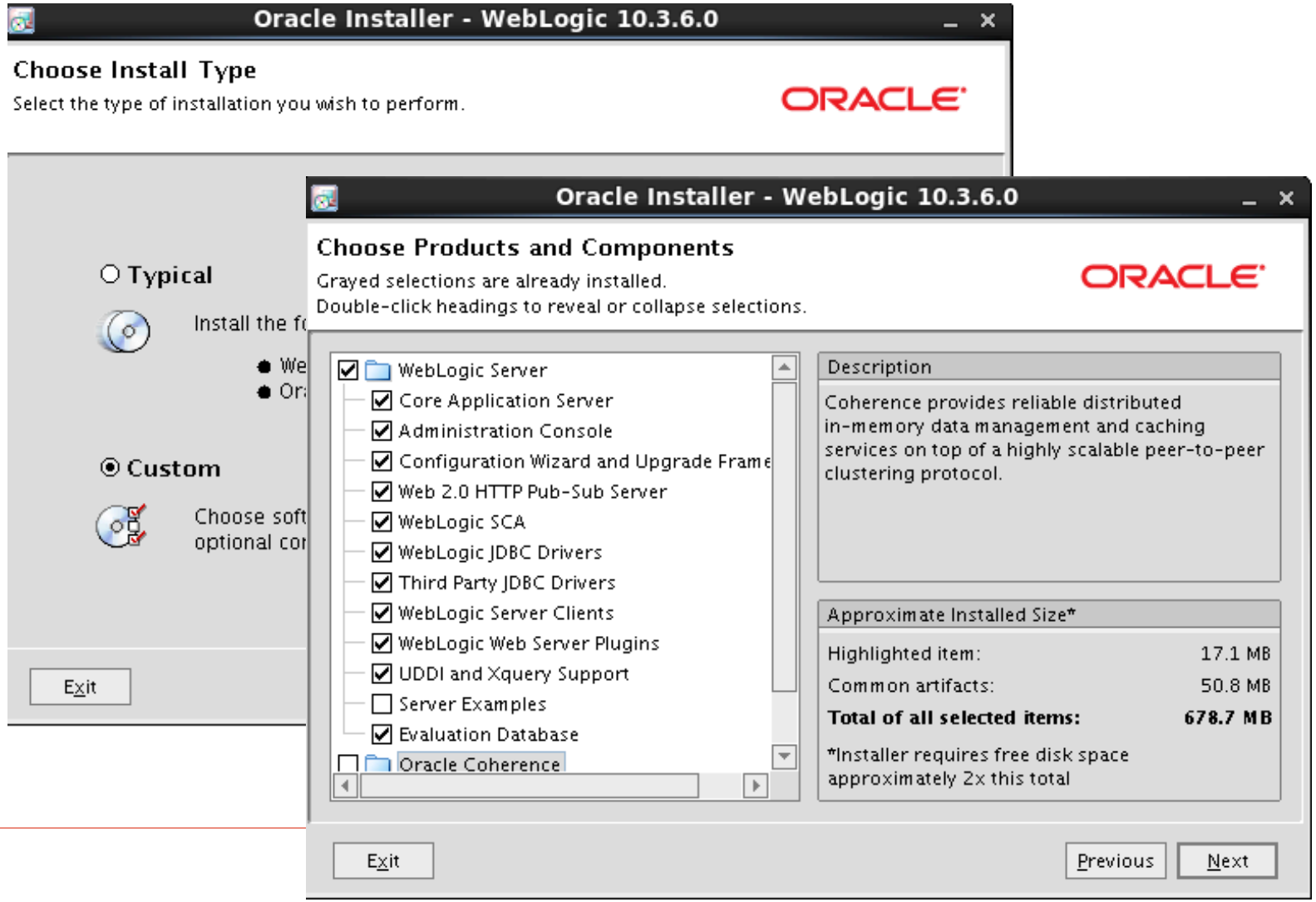
- OUD
- **WLS**
- ADF
- Conf ADF
- Conf OUD
- LDAP User
- Ldap.ora
- Dbca
- EUS



Implementierung OUD

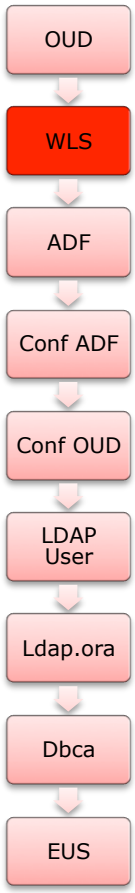
Weblogic: (Custom, De-Select Coherence)

- OUD
- WLS
- ADF
- Conf ADF
- Conf OUD
- LDAP User
- Ldap.ora
- Dbca
- EUS



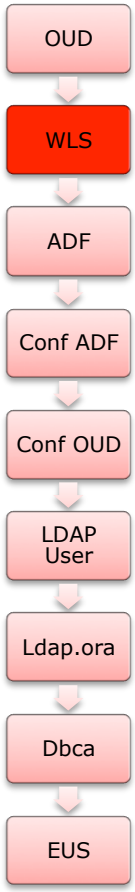
Implementierung OUD

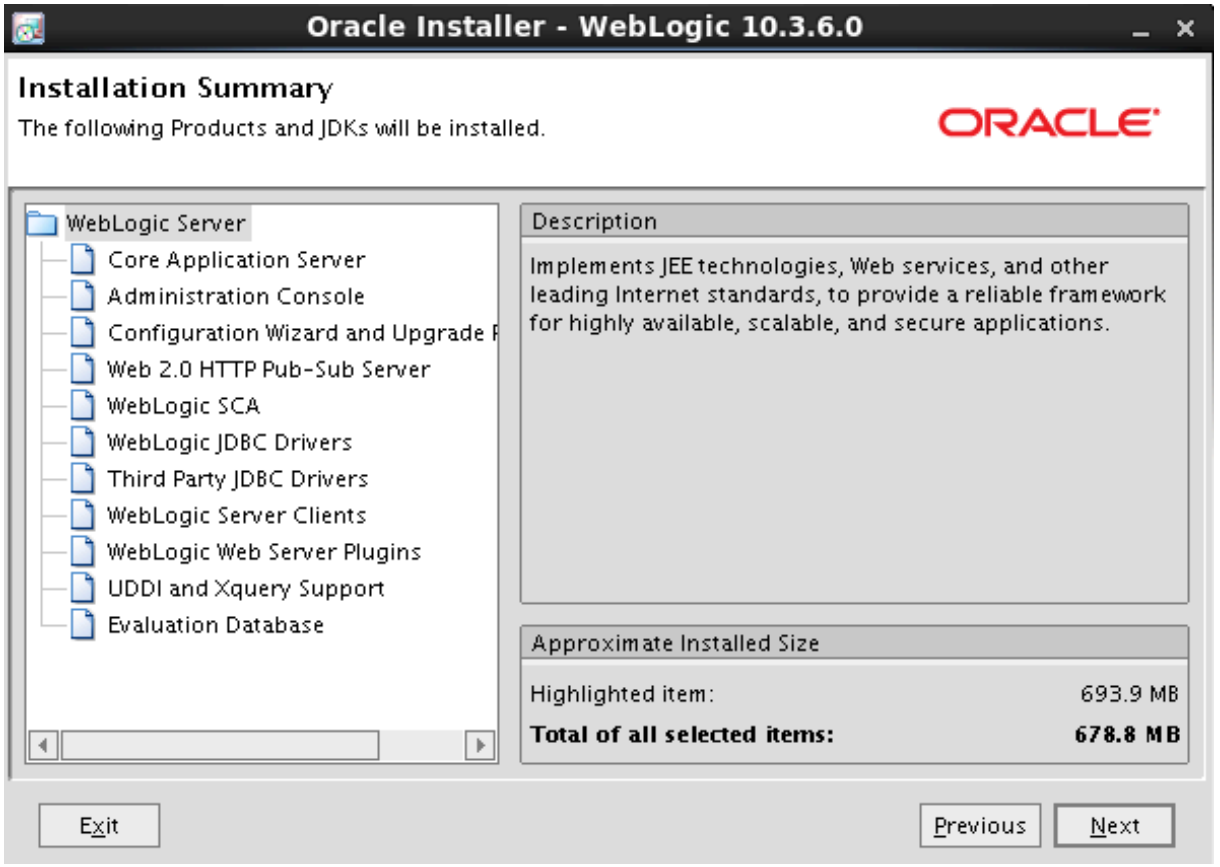
Weblogic:



Implementierung OUD

Weblogic:

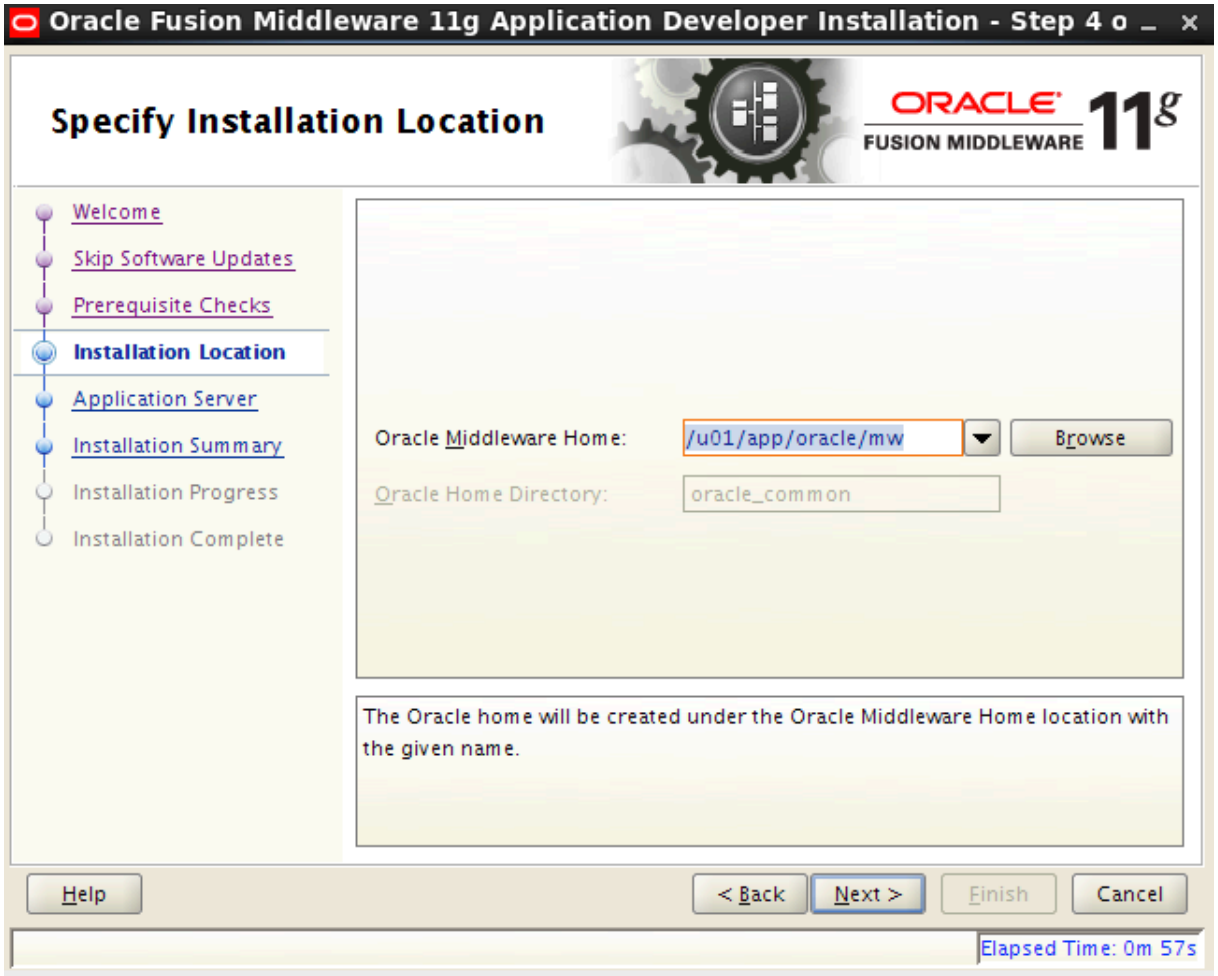




Implementierung OUD

ADF: ./runInstaller -jreLoc $JAVA_HOME/jre

- OUD
- WLS
- **ADF**
- Conf ADF
- Conf OUD
- LDAP User
- Ldap.ora
- Dbca
- EUS



Implementierung OUD

ADF:

- OUD
- WLS
- ADF
- Conf ADF
- Conf OUD
- LDAP User
- Ldap.ora
- Dbca
- EUS

Implementierung OUD

ADF:

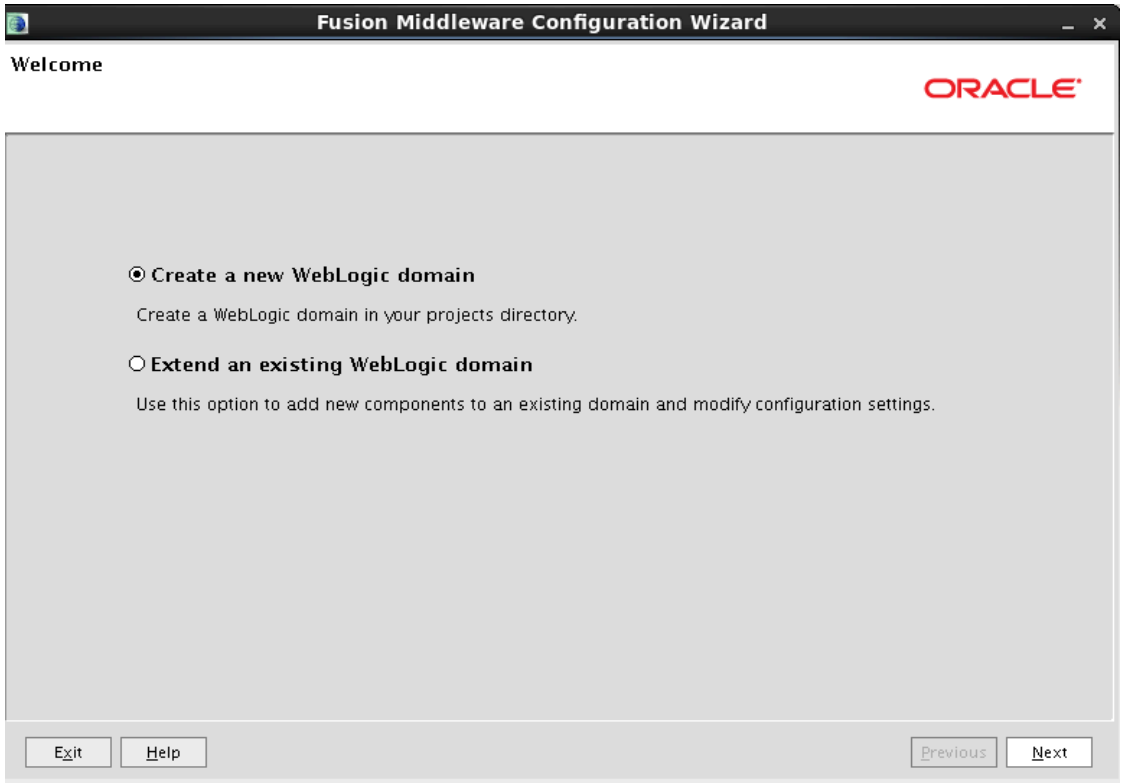
- OUD
- WLS
- ADF
- Conf ADF
- Conf OUD
- LDAP User
- Ldap.ora
- Dbca
- EUS

Implementierung OUD

Configure OSDM with ADF for OUD:

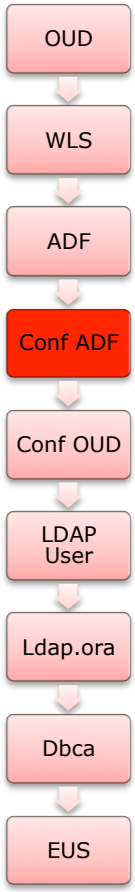
- OUD
- WLS
- ADF
- Conf ADF
- Conf OUD
- LDAP User
- Ldap.ora
- Dbca
- EUS

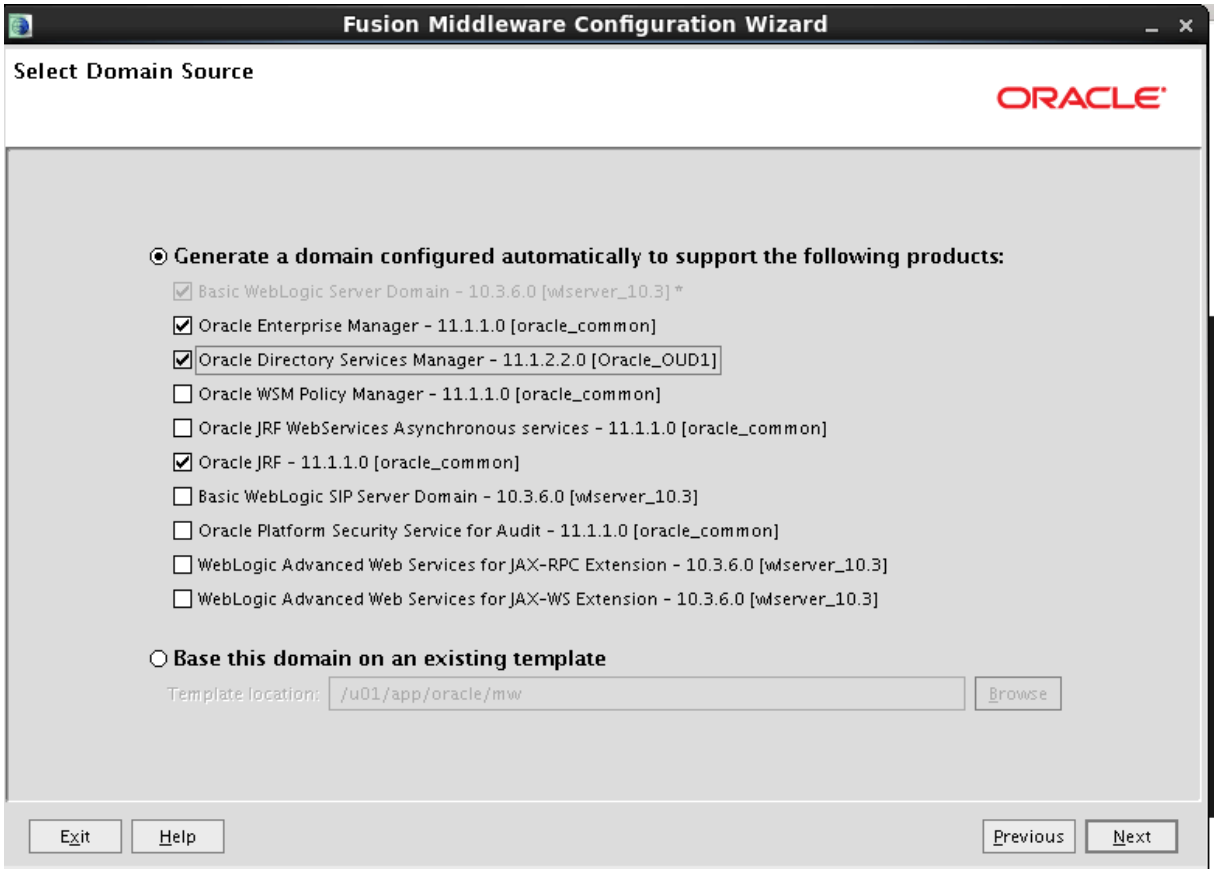
```
[oracle@oud1 Disk1]$ cd /u01/app/oracle/mw/oracle_common/common/bin/
[oracle@oud1 bin]$ ./config.sh
```



Implementierung OUD

Configure OSDM with ADF for OUD:

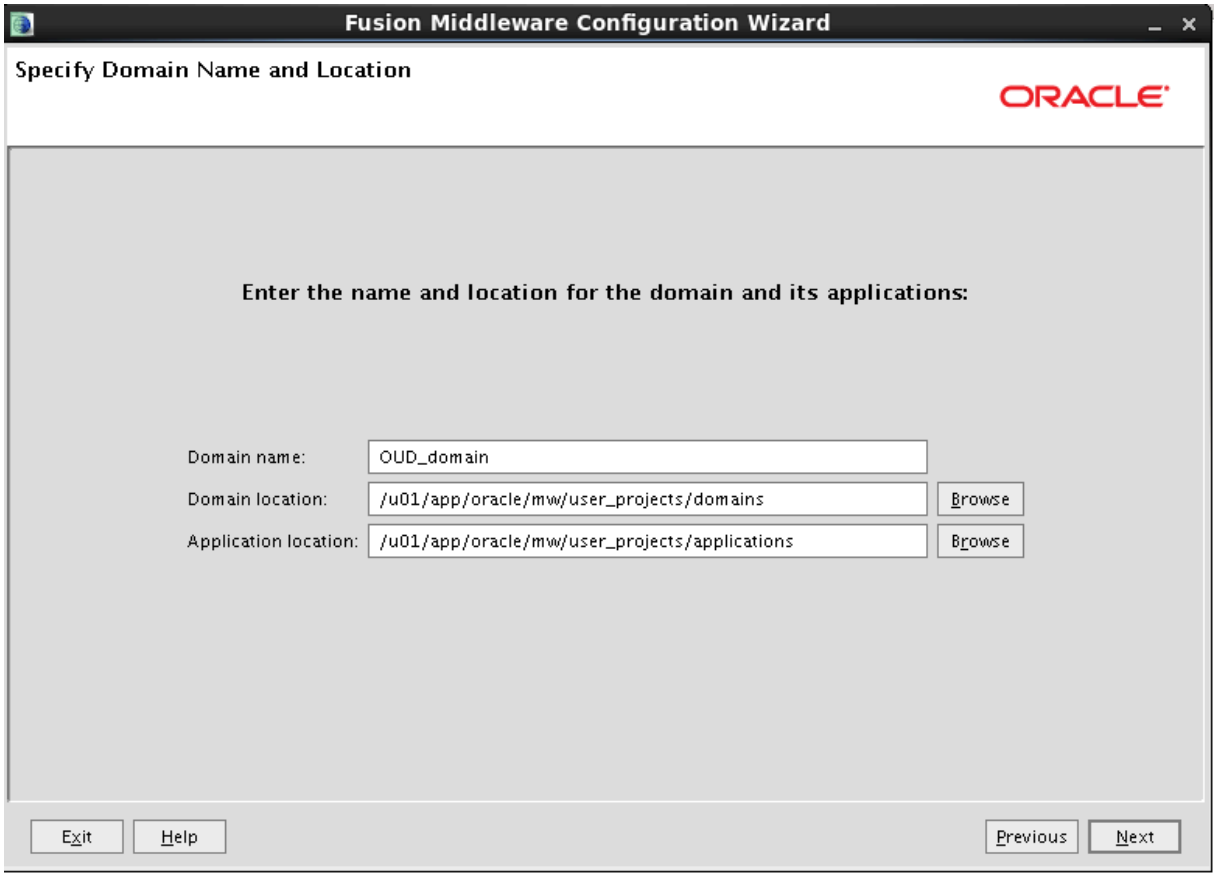




Implementierung OUD

Configure OSDM with ADF for OUD:

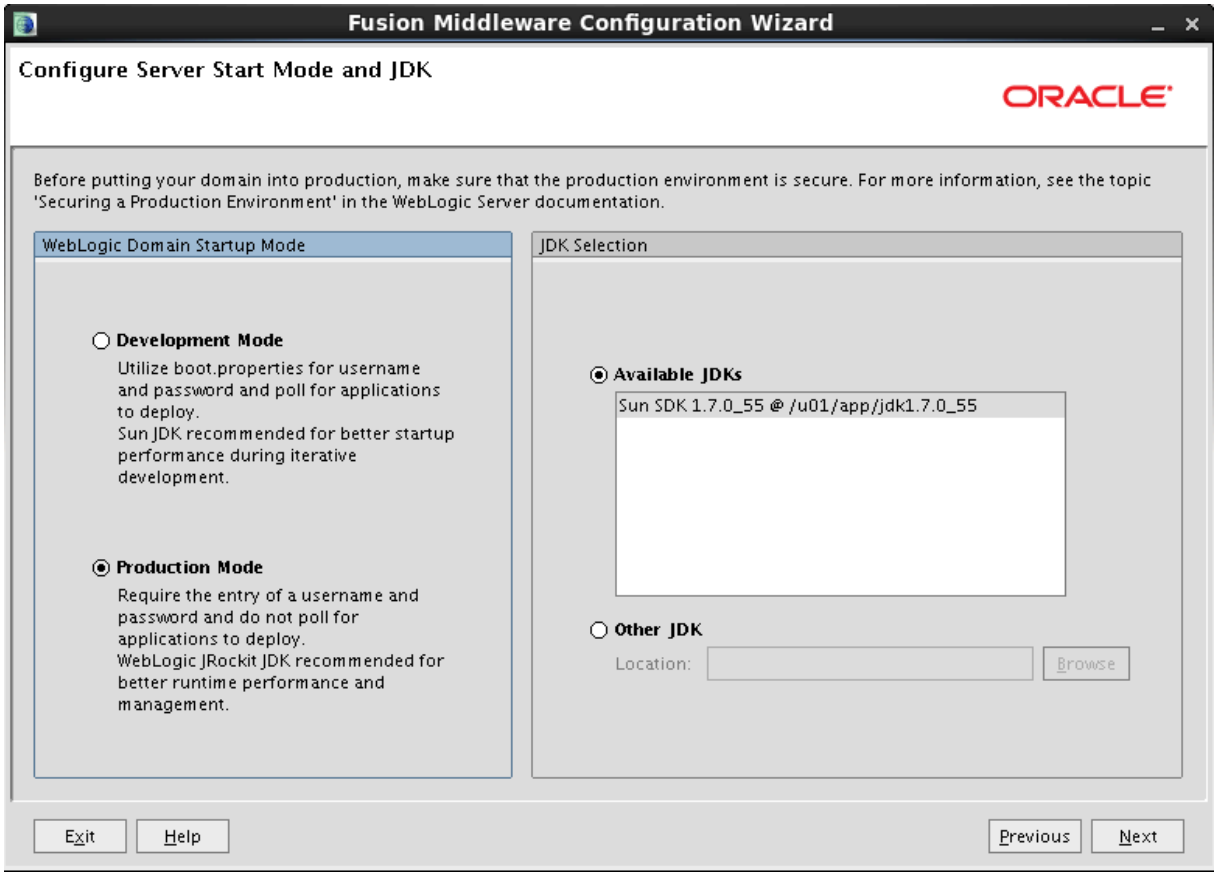
- OUD
- WLS
- ADF
- **Conf ADF**
- Conf OUD
- LDAP User
- Ldap.ora
- Dbca
- EUS



Implementierung OUD

Configure OSDM with ADF for OUD:

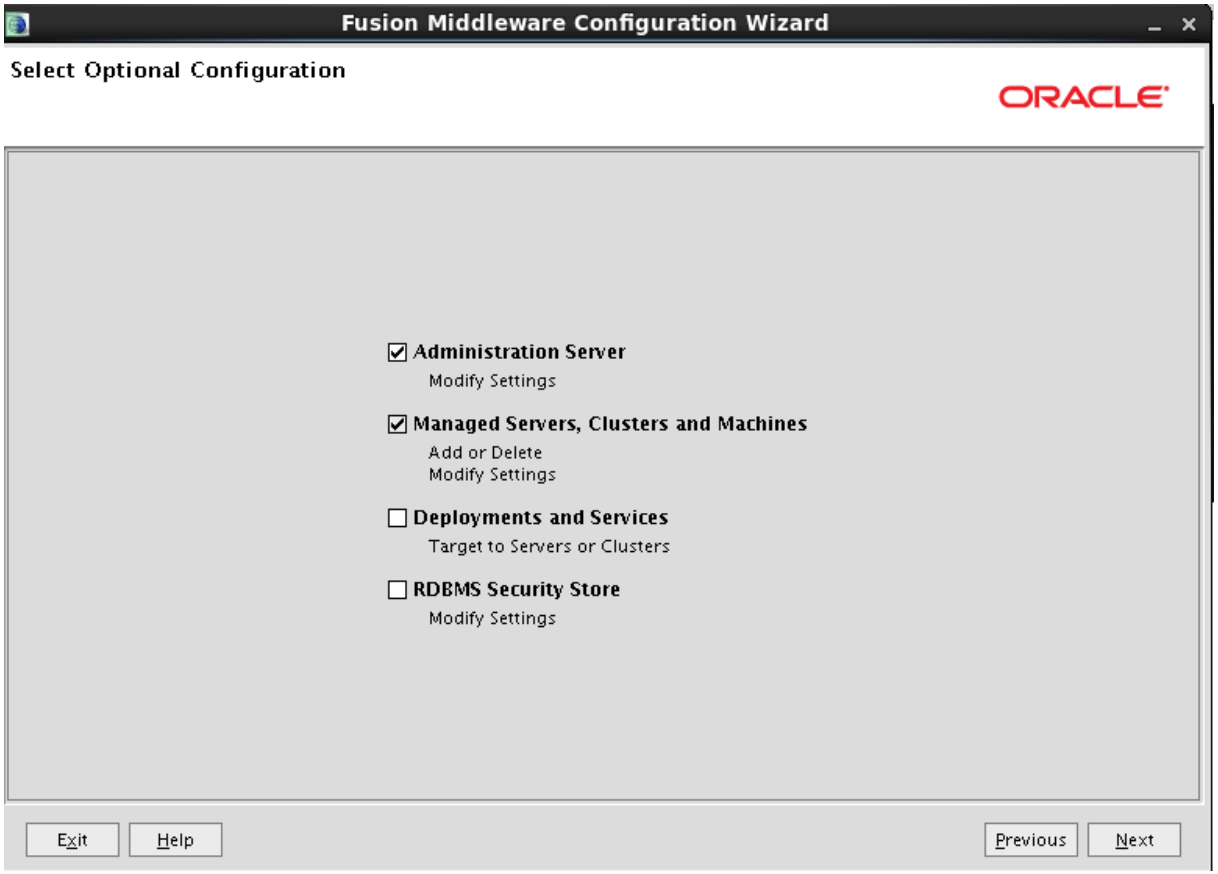
- OUD
- WLS
- ADF
- Conf ADF
- Conf OUD
- LDAP User
- Ldap.ora
- Dbca
- EUS



Implementierung OUD

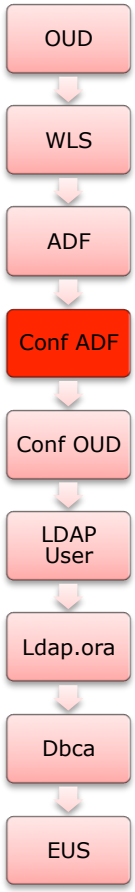
Configure OSDM with ADF for OUD:

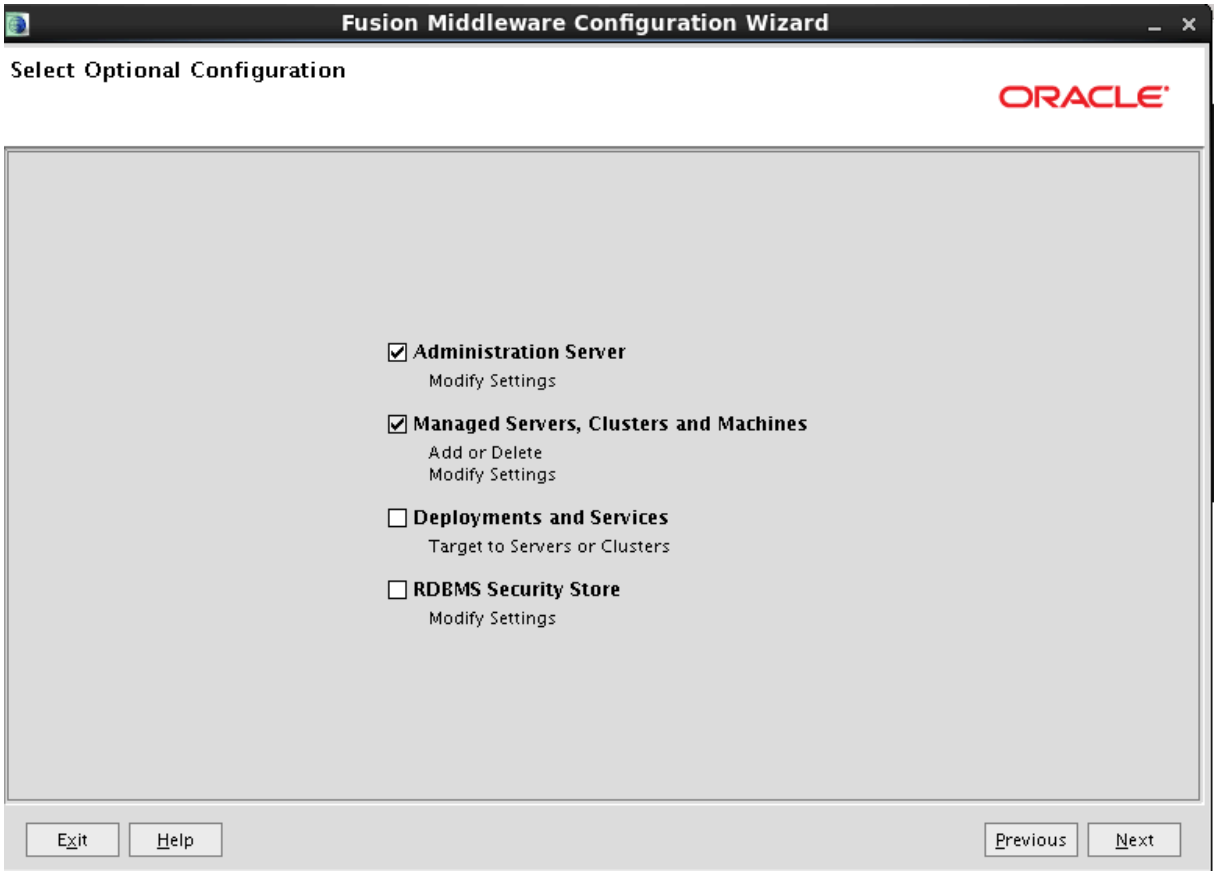
- OUD
- WLS
- ADF
- **Conf ADF**
- Conf OUD
- LDAP User
- Ldap.ora
- Dbca
- EUS



Implementierung OUD

Configure OSDM with ADF for OUD:





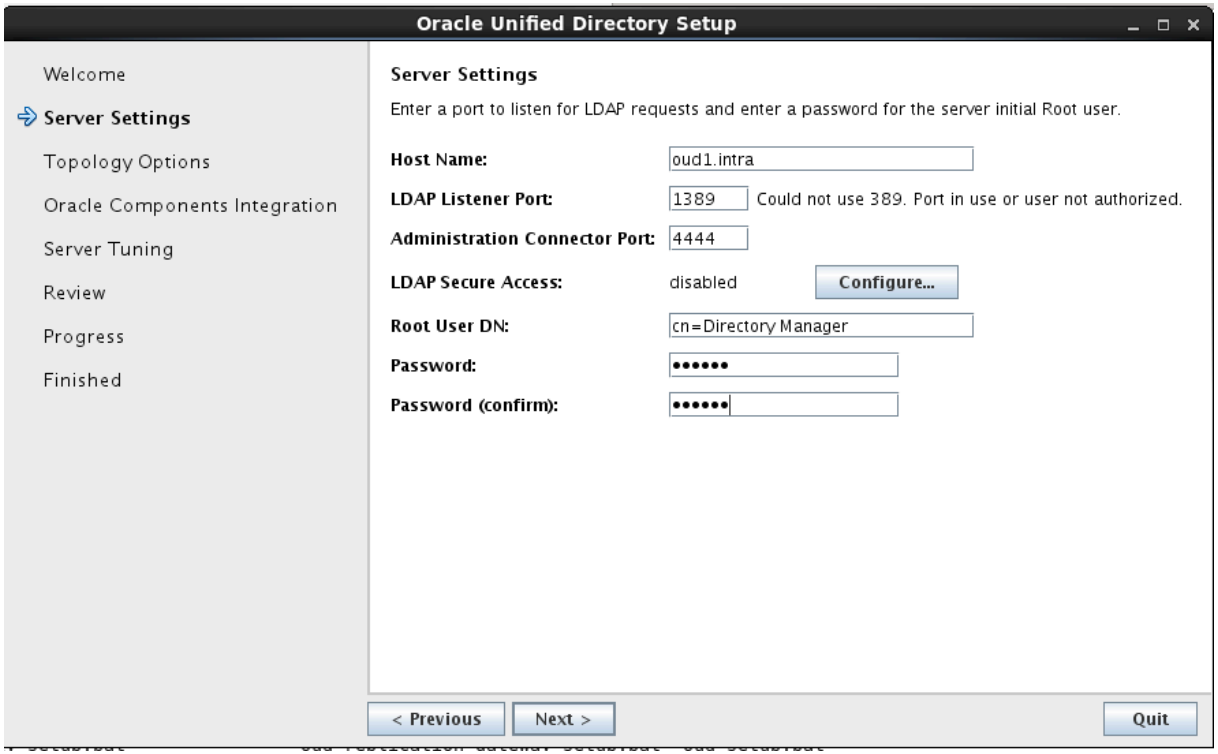
OSDM: https://oud1.intra:7002/odsm/
WLS Admin Server Console: https://oud1.intra:7002/console/

Implementierung OUD

Configure OUD:

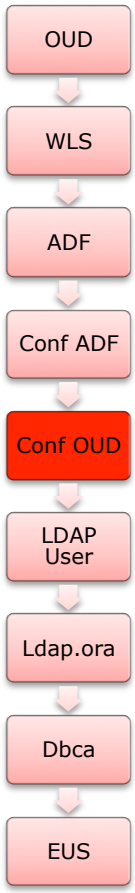
- OUD
- WLS
- ADF
- Conf ADF
- **Conf OUD**
- LDAP User
- Ldap.ora
- Dbca
- EUS

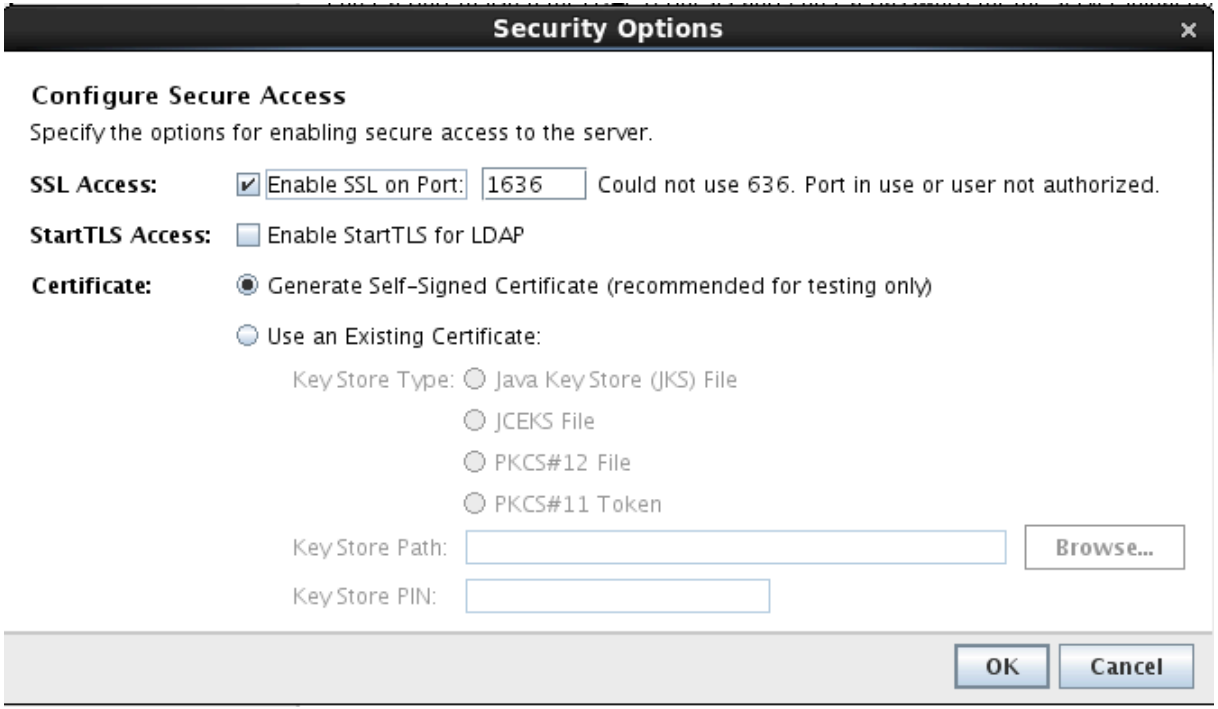
```
[oracle@oud1 bin]$ export ORACLE_INSTANCE=/u01/app/oracle/mw/Oracle_OUD1
[oracle@oud1 bin]$ export PATH=/u01/app/jdk/jre/bin:$PATH
[oracle@oud1 bin]$ cd $ORACLE_INSTANCE
[oracle@oud1 Oracle_OUD1]$ ./oud-setup
```



Implementierung OUD

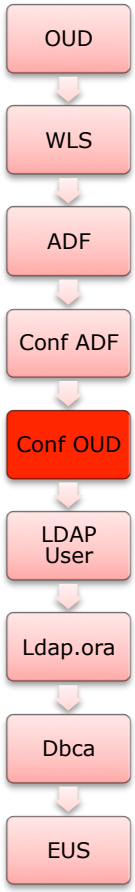
Configure OUD:

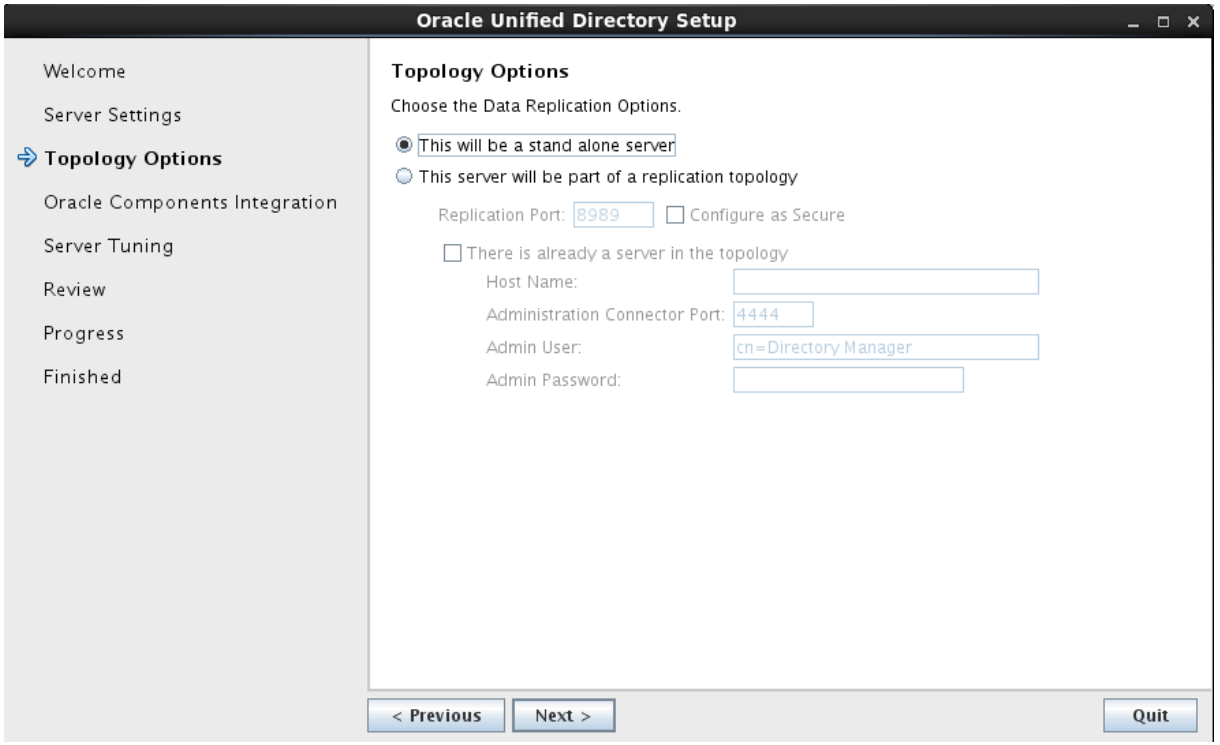




Implementierung OUD

Configure OUD:

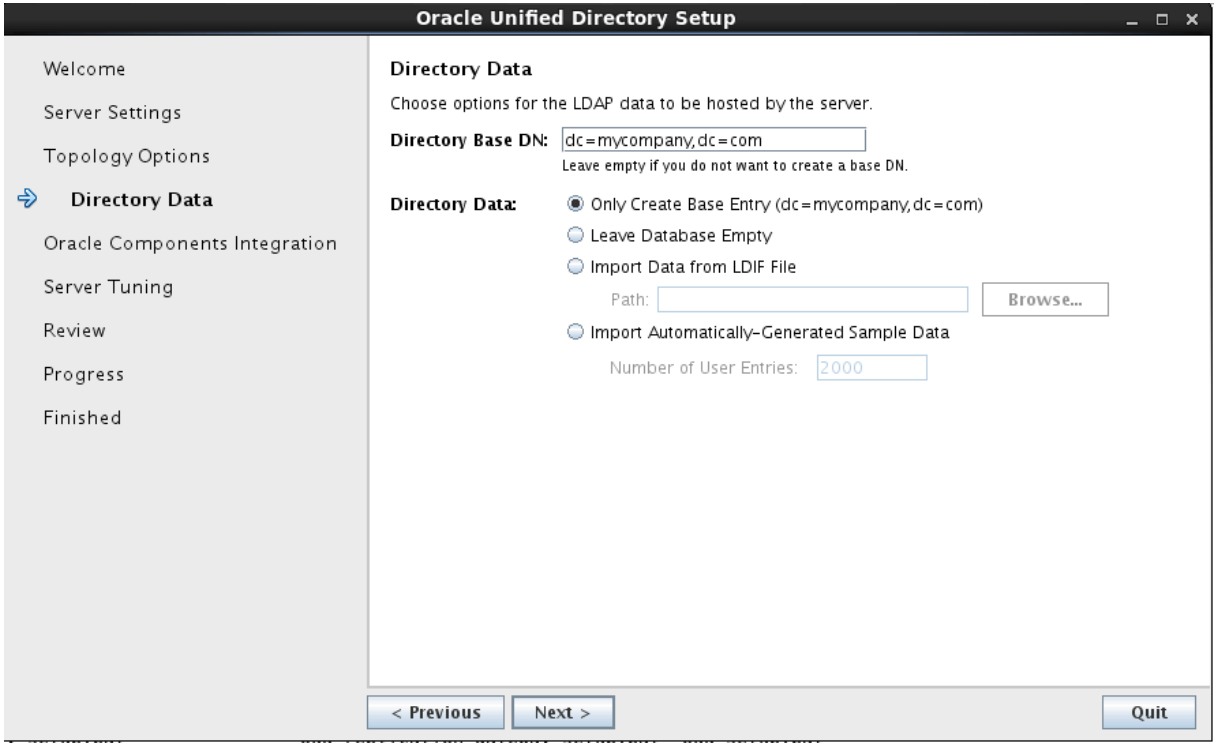




Implementierung OUD

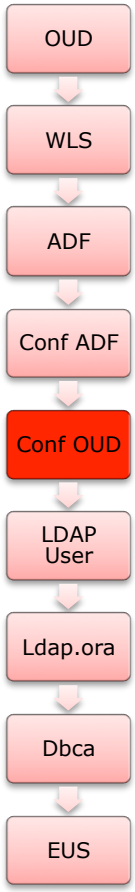
Configure OUD:

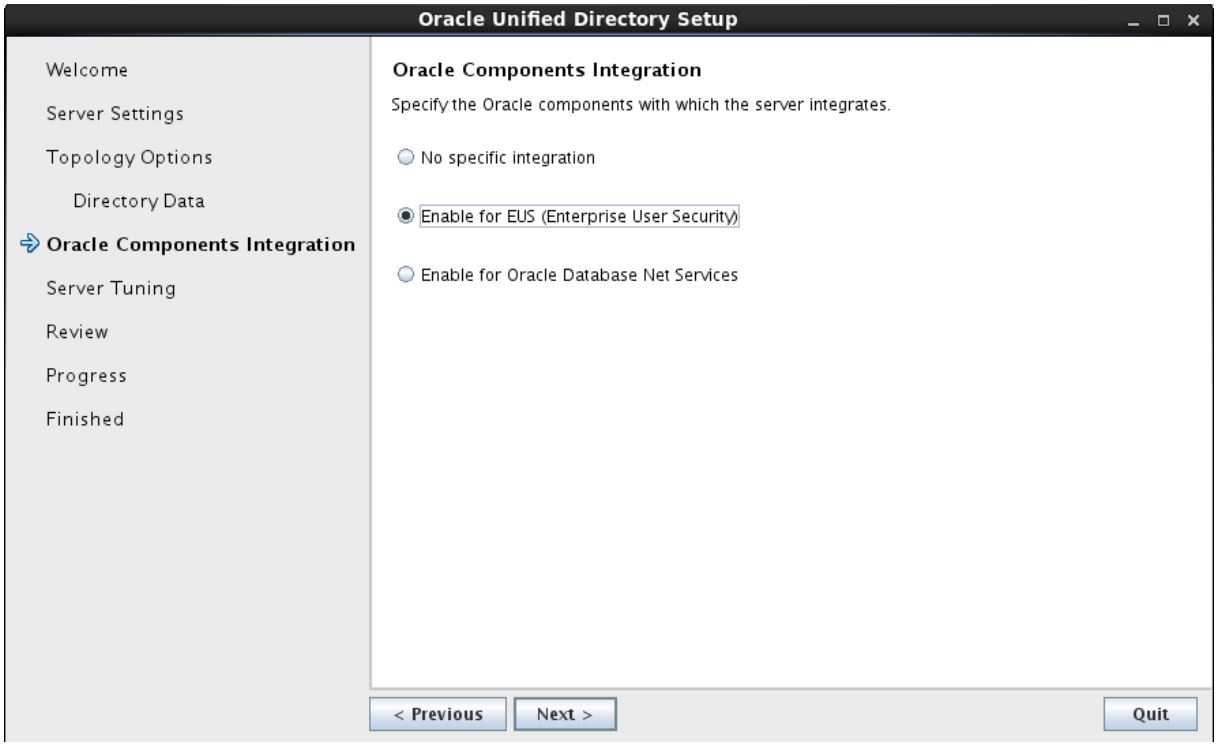
- OUD
- WLS
- ADF
- Conf ADF
- **Conf OUD**
- LDAP User
- Ldap.ora
- Dbca
- EUS



Implementierung OUD

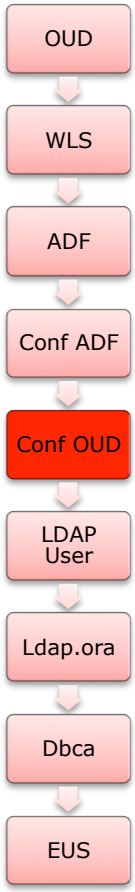
Configure OUD:

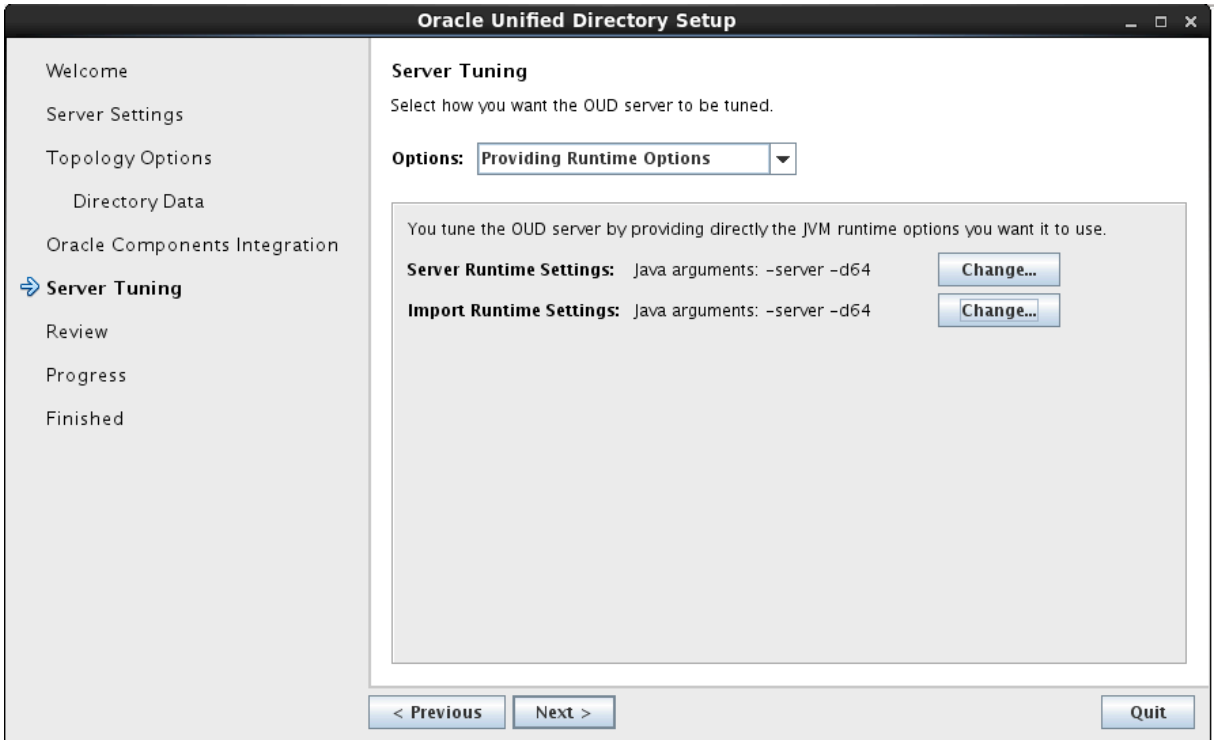




Implementierung OUD

Configure OUD:

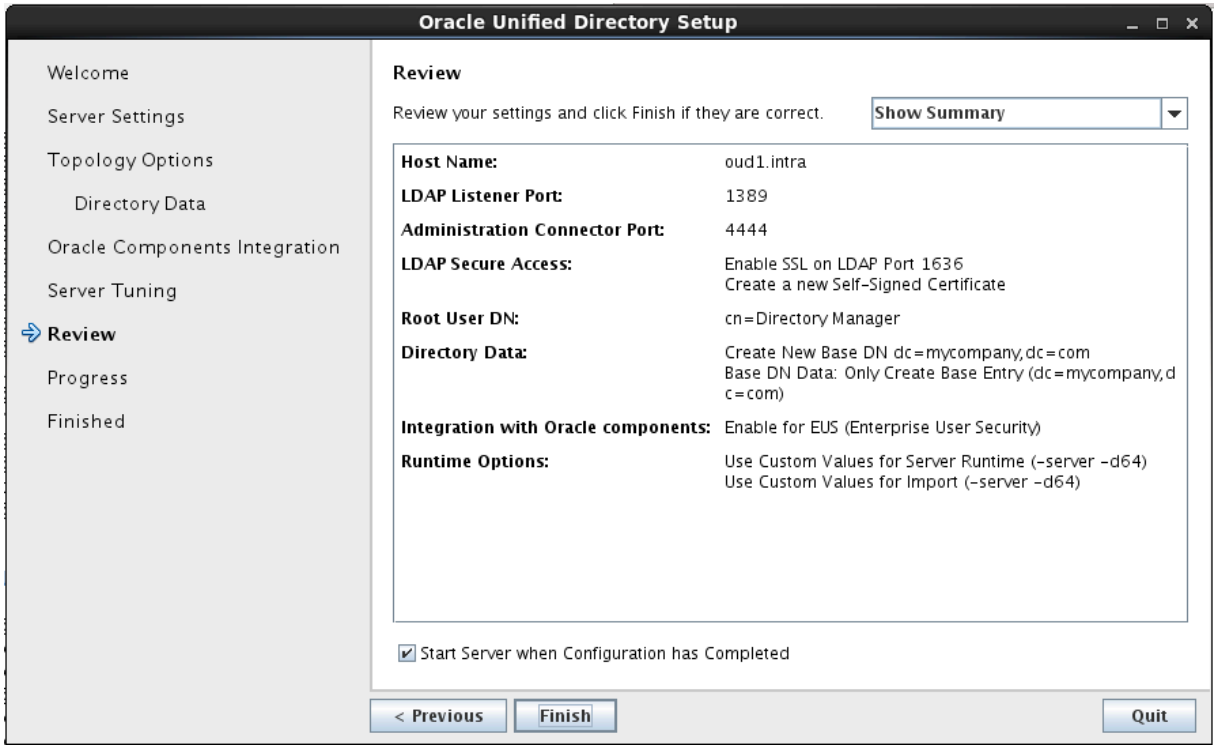




Implementierung OUD

Configure OUD:

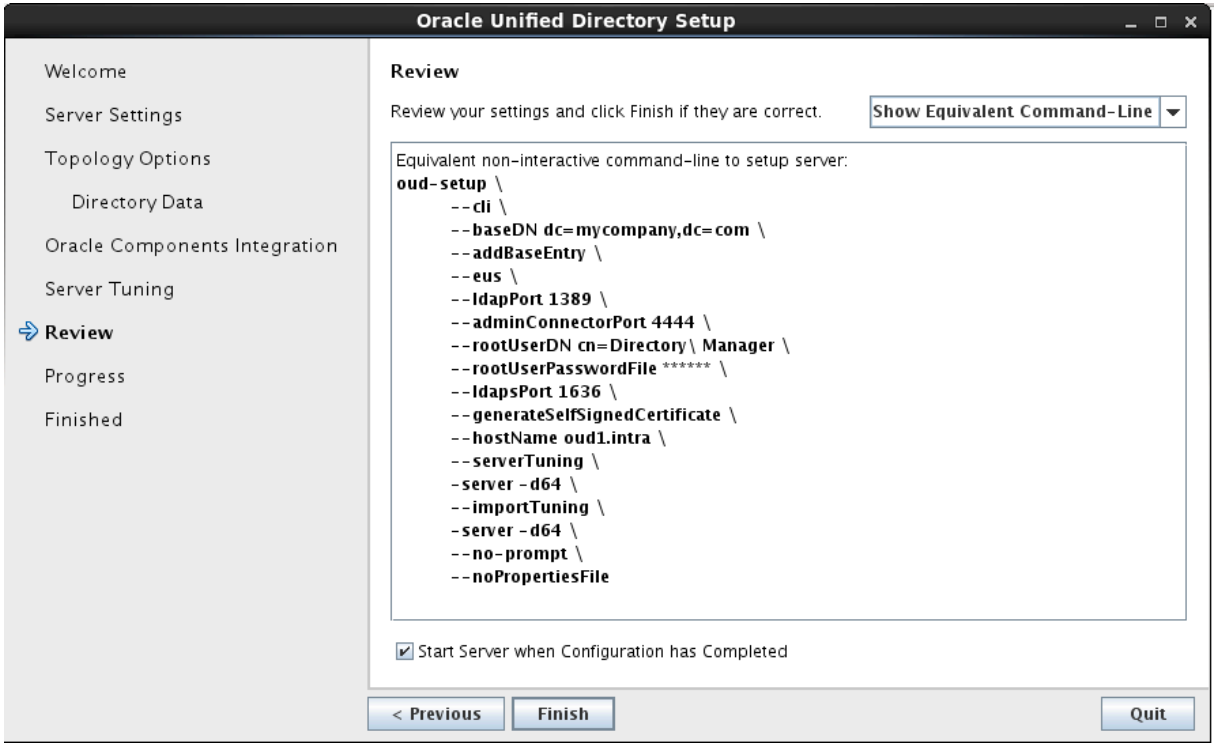
- OUD
- WLS
- ADF
- Conf ADF
- **Conf OUD**
- LDAP User
- Ldap.ora
- Dbca
- EUS



Implementierung OUD

Configure OUD:

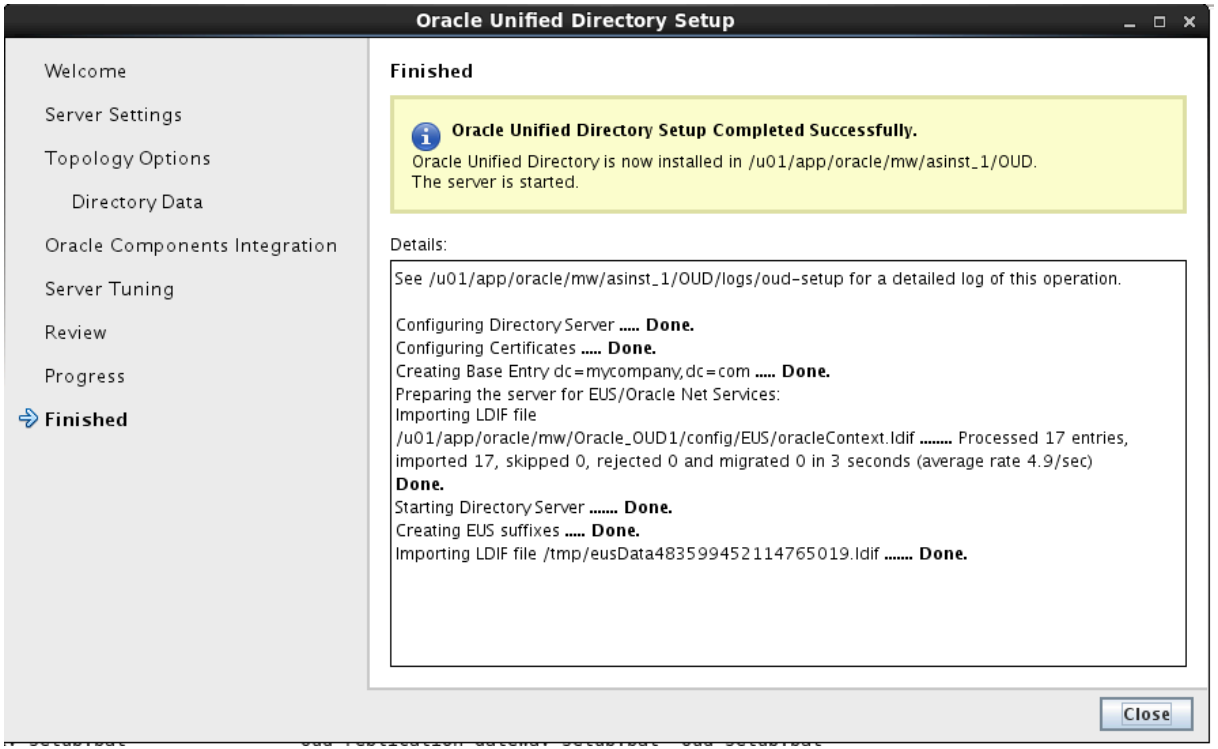
- OUD
- WLS
- ADF
- Conf ADF
- **Conf OUD**
- LDAP User
- Ldap.ora
- Dbca
- EUS



Implementierung OUD

Configure OUD:

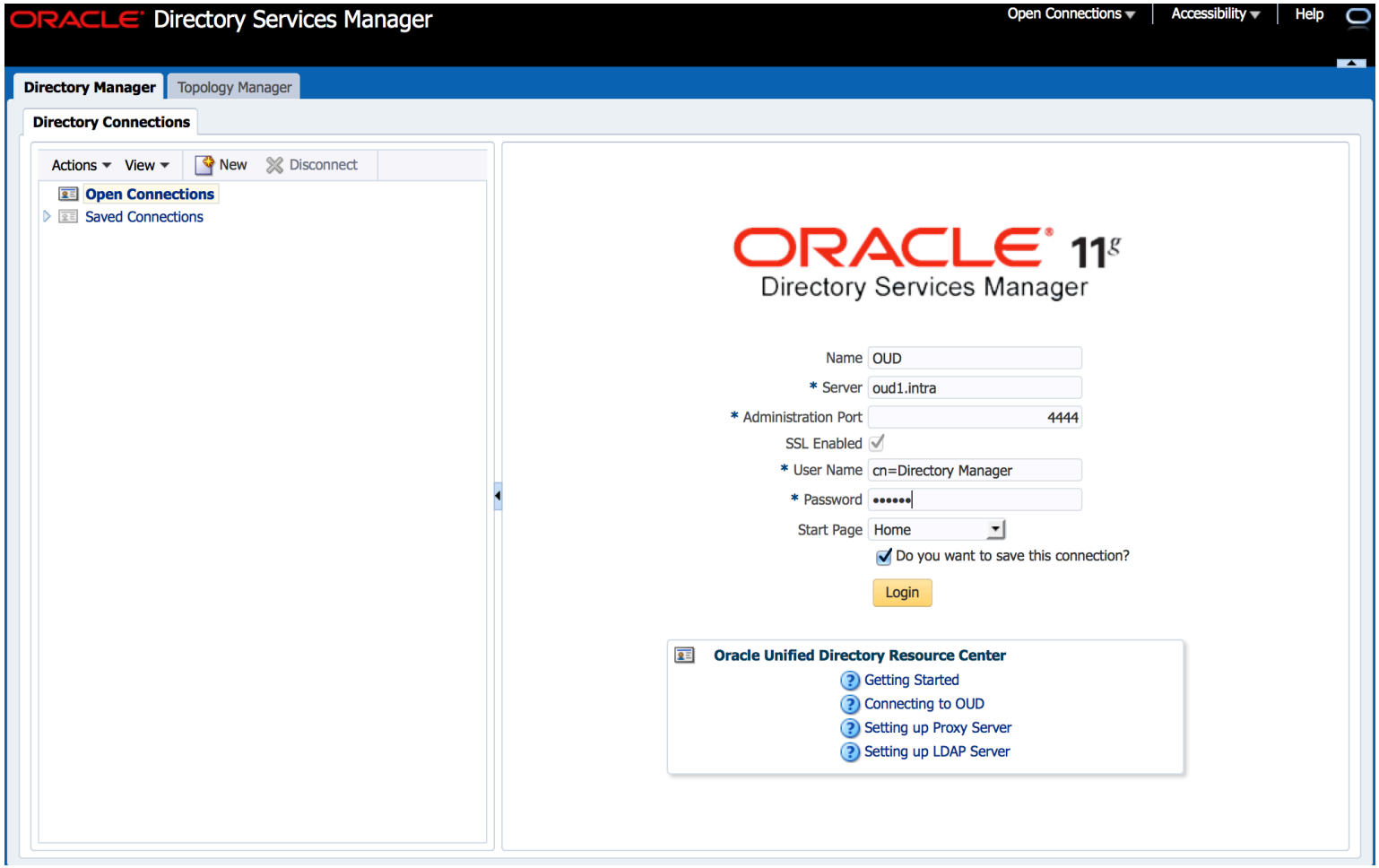
- OUD
- WLS
- ADF
- Conf ADF
- **Conf OUD**
- LDAP User
- Ldap.ora
- Dbca
- EUS



Implementierung OUD

Create LDAP Users & Groups: https://oud1.intra:7002/odsm/

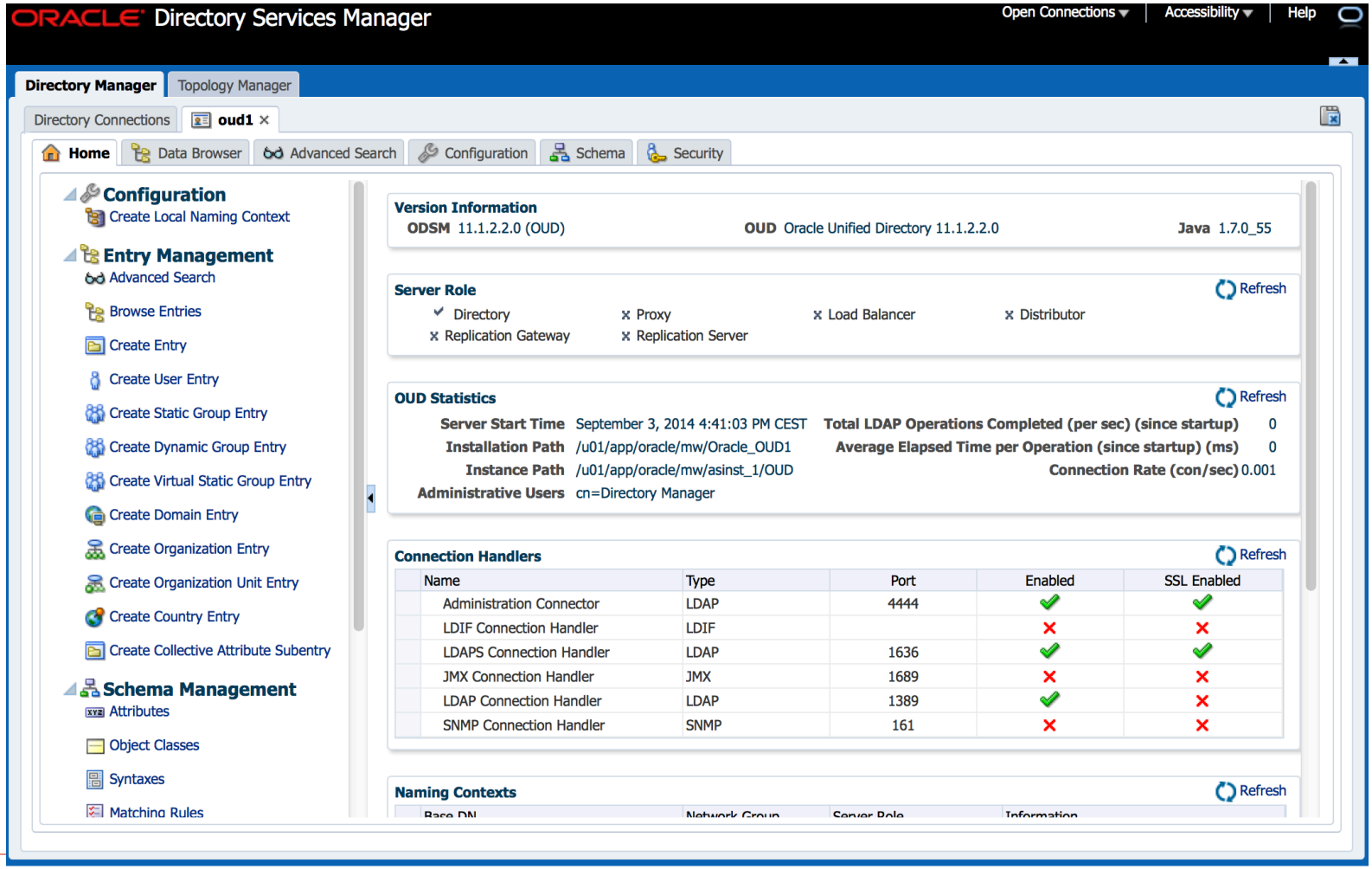
- OUD
- WLS
- ADF
- Conf ADF
- Conf OUD
- **LDAP User**
- Ldap.ora
- Dbca
- EUS



Implementierung OUD

Create LDAP Users & Groups:

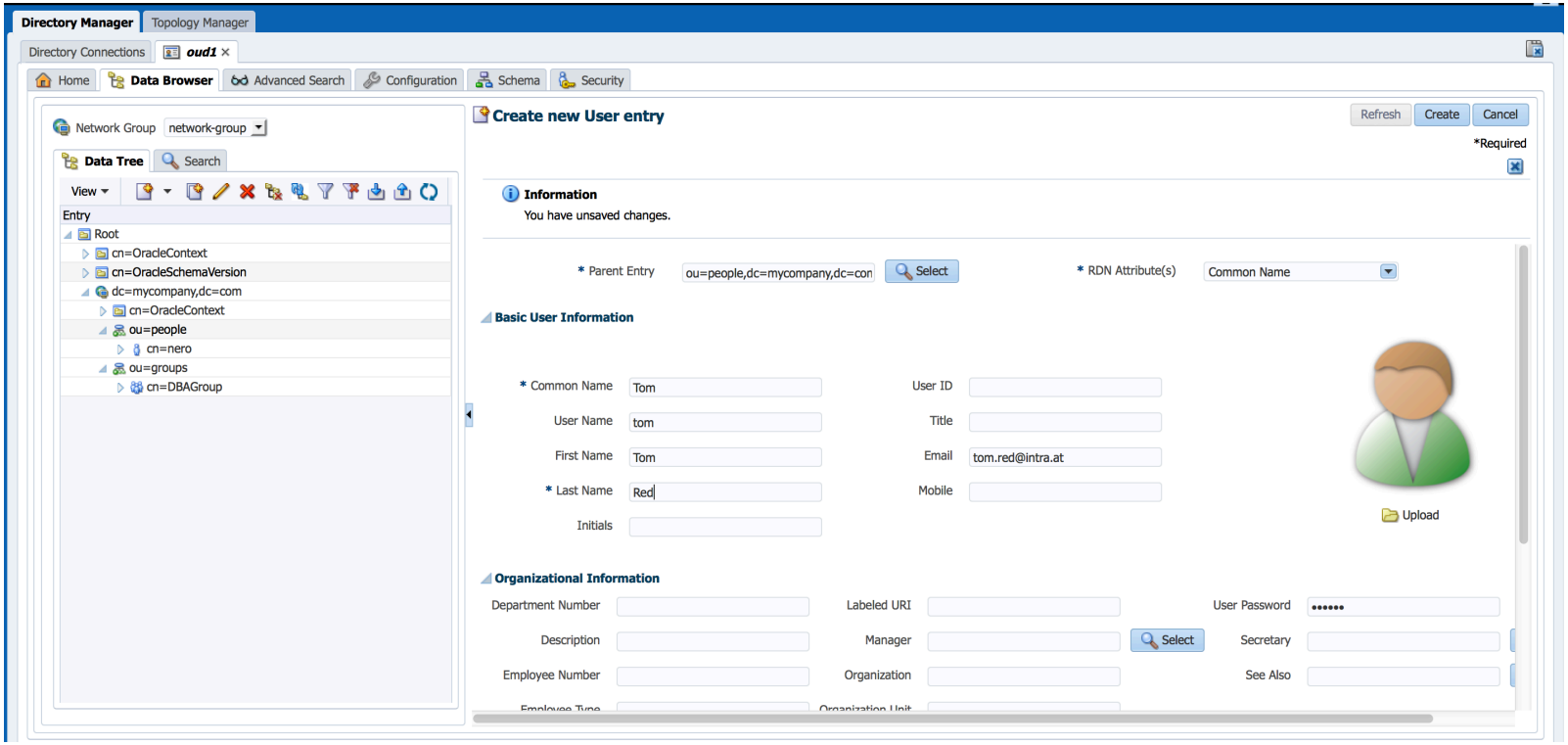
- OUD
- WLS
- ADF
- Conf ADF
- Conf OUD
- LDAP User
- Ldap.ora
- Dbca
- EUS



Implementierung OUD

Create LDAP Users & Groups:
-> Data Browser
-> ou=people
-> Create User Entry

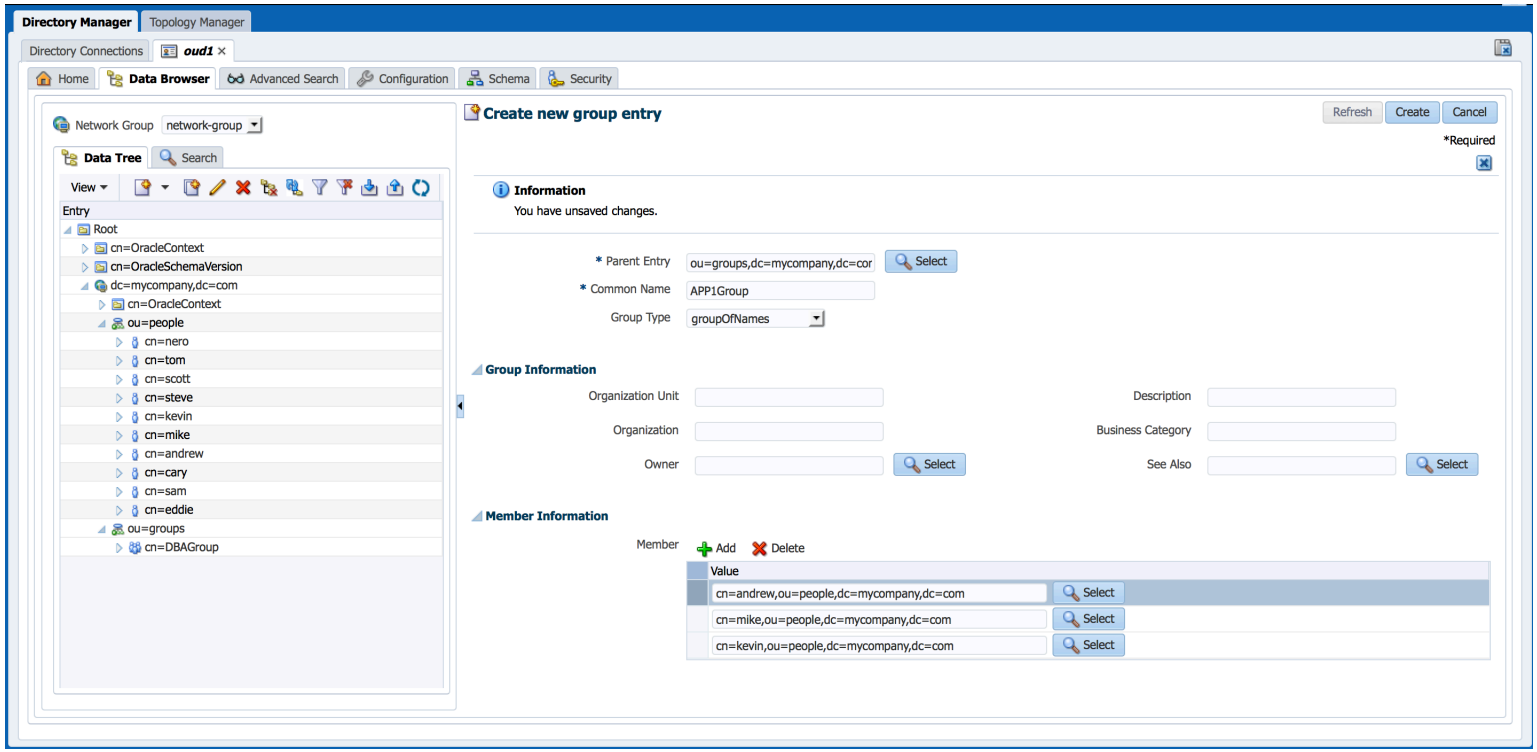
- OUD
- WLS
- ADF
- Conf ADF
- Conf OUD
- **LDAP User**
- Ldap.ora
- Dbca
- EUS



Implementierung OUD

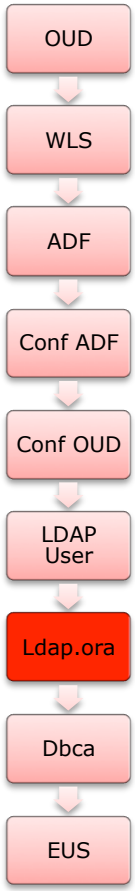
Create LDAP Users & Groups:
-> Data Browser
-> ou=group
-> Create Group Entry -> Static Group

- OUD
- WLS
- ADF
- Conf ADF
- Conf OUD
- LDAP User
- Ldap.ora
- Dbca
- EUS



Implementierung OUD

Configuration:



ldap.ora

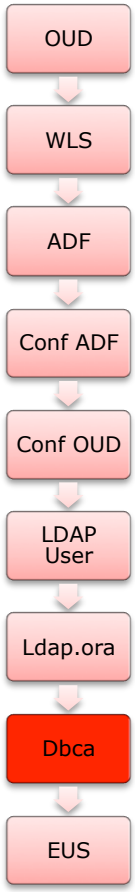
```
DIRECTORY_SERVERS=(oud1.intra:1389:1636)
DEFAULT_ADMIN_CONTEXT = "dc=mycompany,dc=com"
DIRECTORY_SERVER_TYPE = OID
```

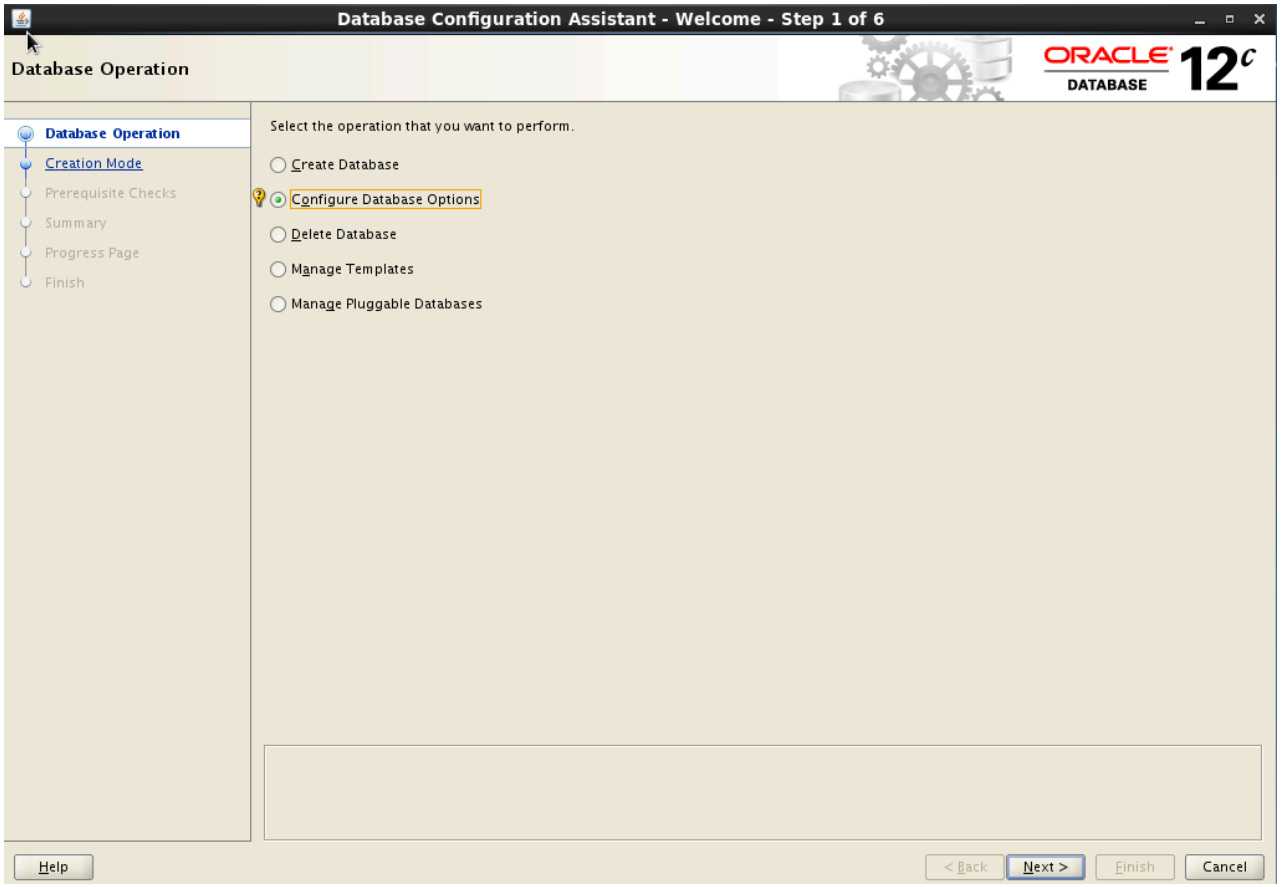
Optional: sqlnet.ora:

```
NAMES.DIRECTORY_PATH= (LDAP, TNSNAMES)
```

Implementierung OUD

DBCA: register Database in directory (GUI)



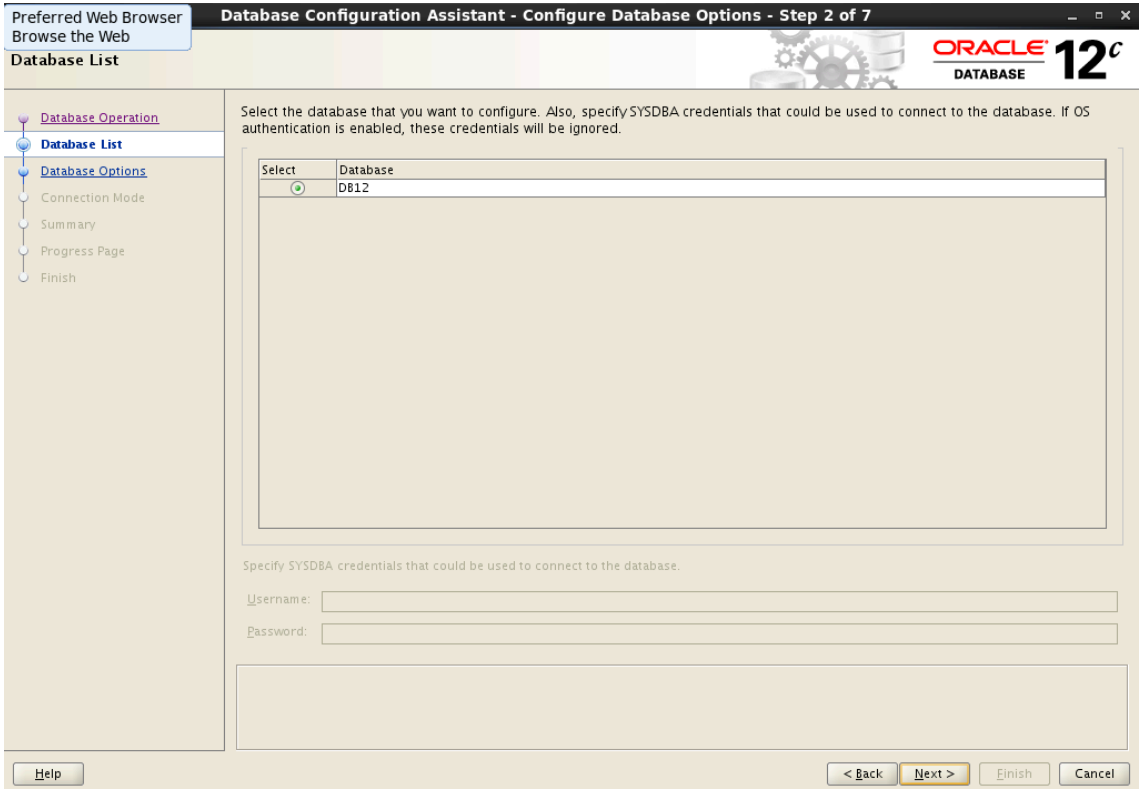


ACHTUNG: dbca silent funktioniert nicht, wegen Whitespace in „cn=directory manager"

Implementierung OUD

DBCA: register Database in directory (GUI)

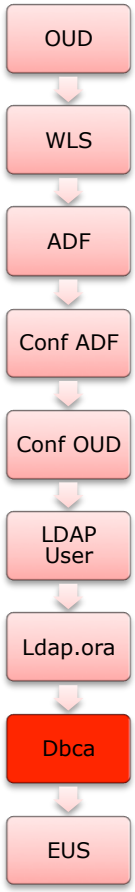
- OUD
- WLS
- ADF
- Conf ADF
- Conf OUD
- LDAP User
- Ldap.ora
- **Dbca**
- EUS

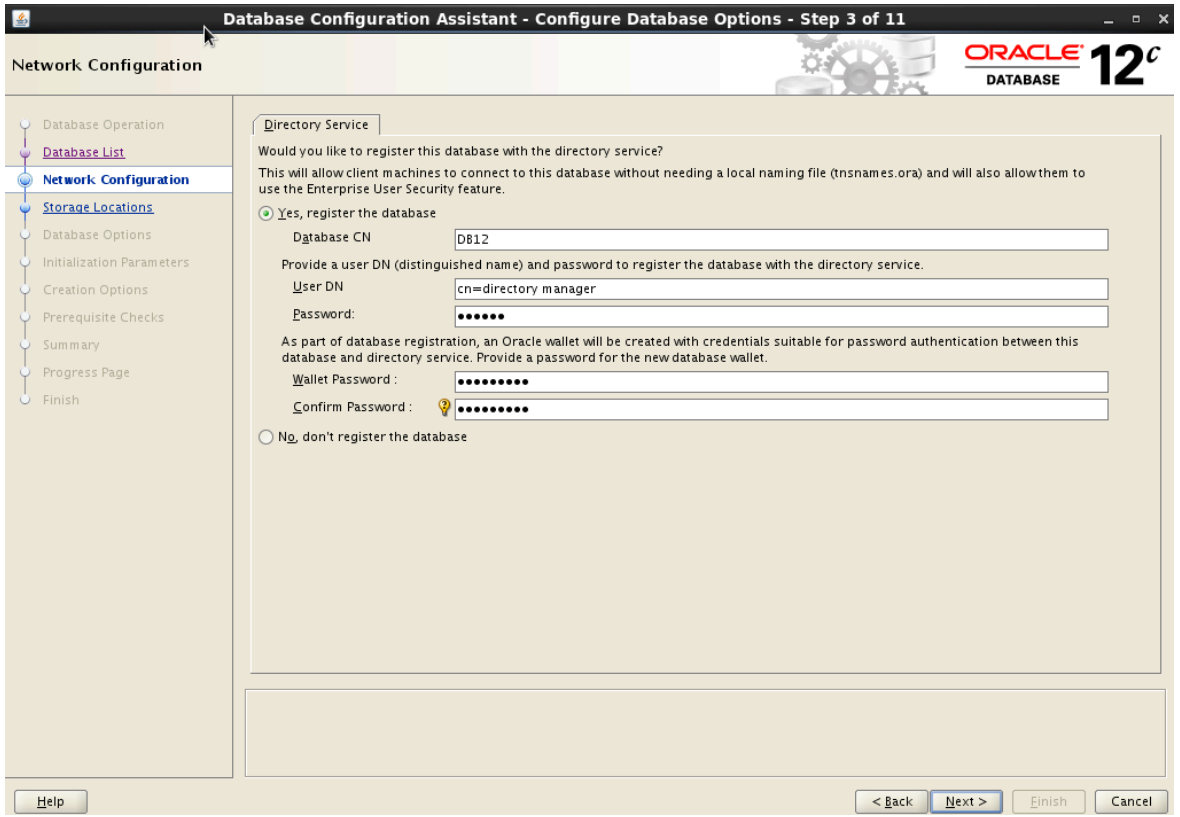


ACHTUNG: dbca silent funktioniert nicht, wegen Whitespace in „cn=directory manager"

Implementierung OUD

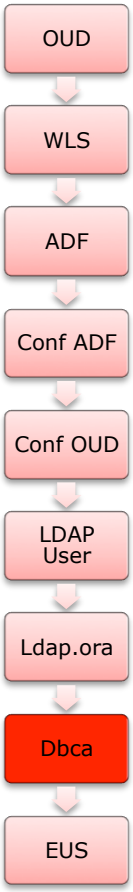
DBCA: register Database in directory (GUI)

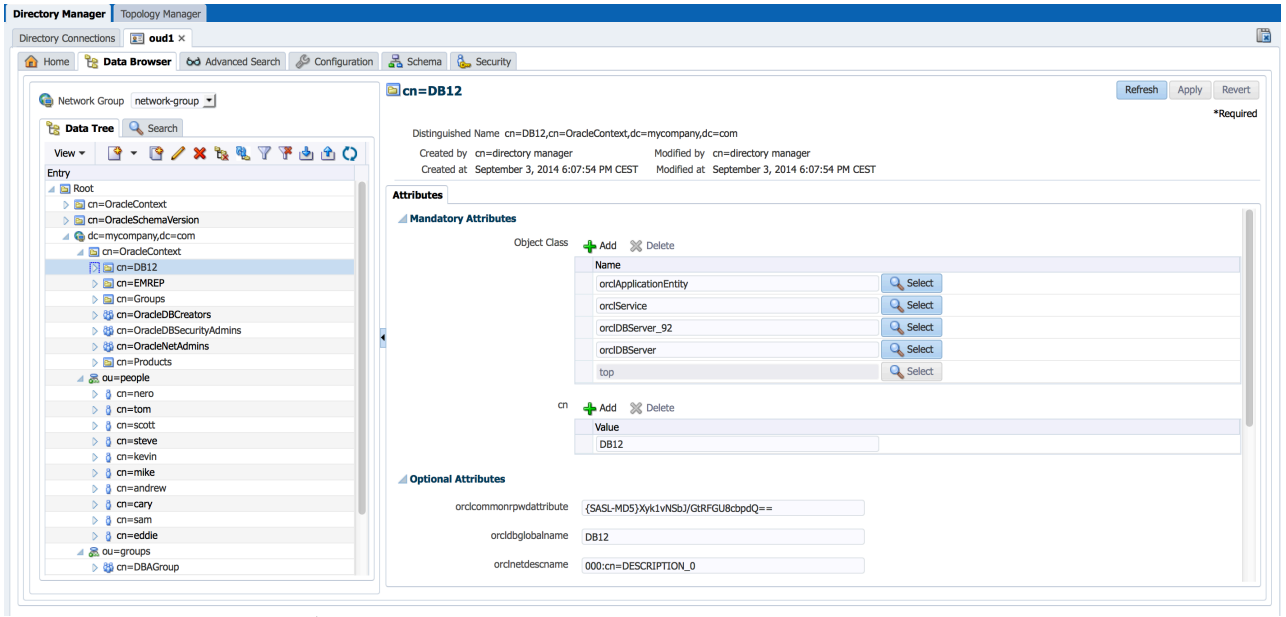




ACHTUNG: dbca silent funktioniert nicht, wegen Whitespace in „cn=directory manager"

DBCA: register Database in directory (GUI)

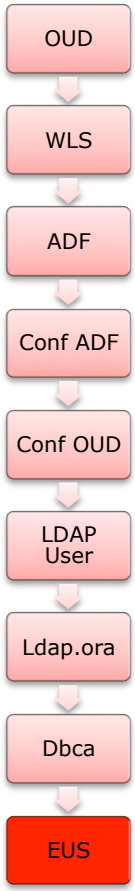





```
[oracle@db12oel6 admin]$ tnsping DB12

TNS Ping Utility for Linux: Version 12.1.0.2.0 - Production on 03-SEP-2014 18:16:58

Copyright (c) 1997, 2014, Oracle.  All rights reserved.

Used parameter files:
/u01/app/oracle/product/12.1.0.2/dbhome_1/network/admin/sqlnet.ora

Used LDAP adapter to resolve the alias
Attempting to contact (DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=db12oel6.intra)(PORT=1521))
(CONNECT_DATA=(SERVICE_NAME=DB12)))
OK (10 msec)
```

EUS Use Cases

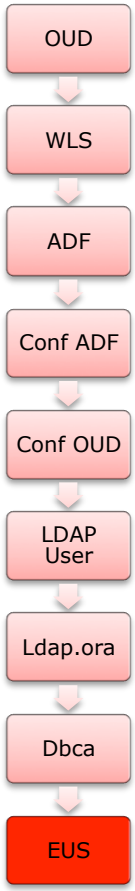
3 Use Cases:



- DBA Accounts:
  - 3 DBAs: TOM / BOB / STEVE
  - Zugriff auf Global User GU_DBA
  - Enterprise Role ER_DBA, Global Role GR_DBA
- Application Admins:
  - 3 APPAdmins: KEVIN / MIKE / ANDREW
  - Zugriff auf Schema APP1 über Proxy-Permission
- Application Admins:
  - 3 APPAdmins: CARY / SAM / EDDIE
  - Zugriff auf Schema APP2 über Proxy-Permission mittels LDAP Group

EUS Use Cases

Vorbereitung auf Target-Database:




```
CREATE USER GU_DBA IDENTIFIED EXTERNALLY;
CREATE USER GU_APP1 IDENTIFIED EXTERNALLY;
CREATE USER GU_APP2 IDENTIFIED EXTERNALLY;
CREATE ROLE GR_DBA IDENTIFIED EXTERNALLY;

GRANT DBA TO GR_DBA;

ALTER USER APP1 GRANT CONNECT THROUGH
ENTERPRISE USERS;

ALTER USER APP2 GRANT CONNECT THROUGH
ENTERPRISE USERS;
```

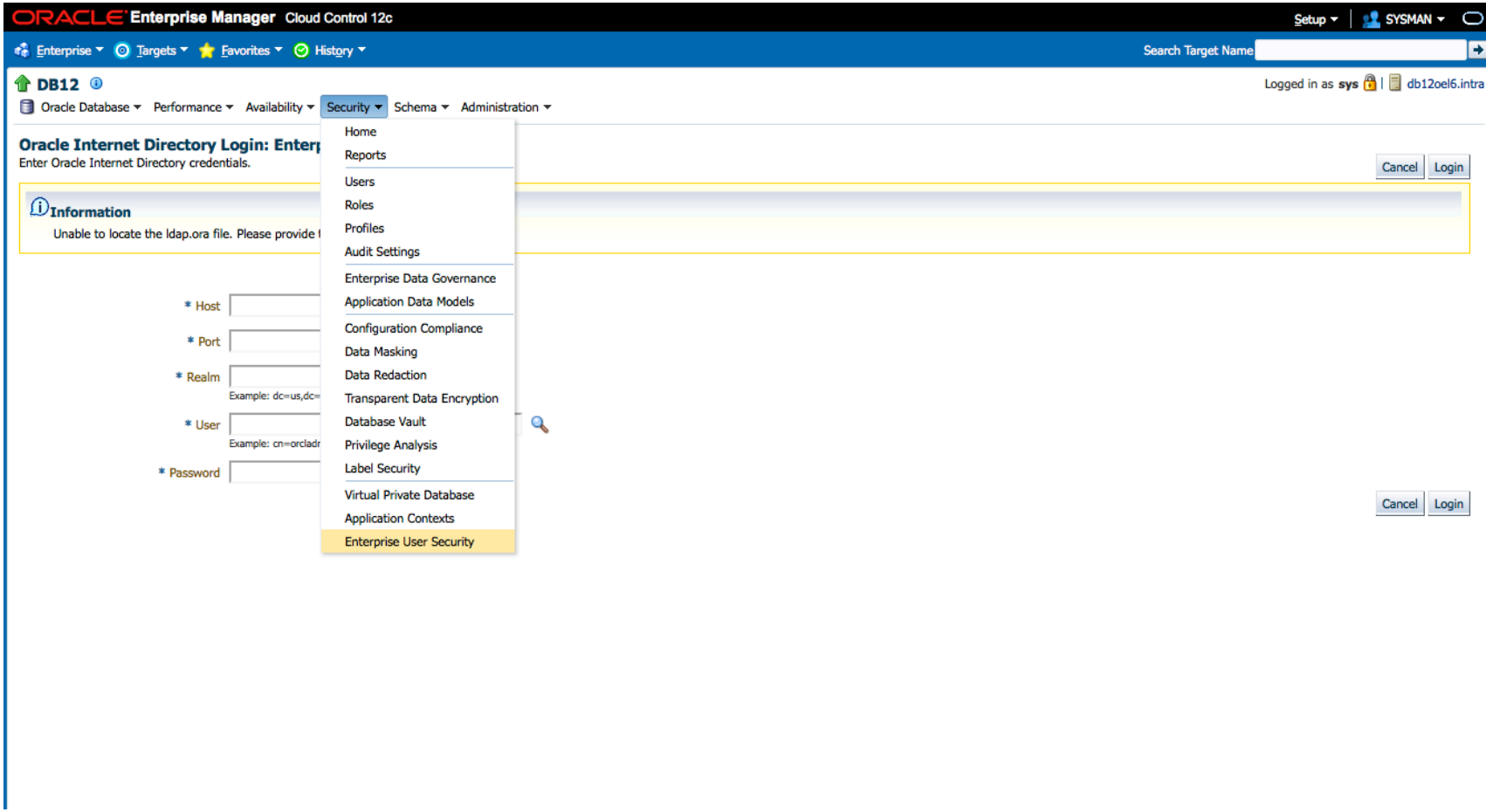
Tracing:

```
alter system set events '28033 trace name
context forever, level 9';
```

EUS Use Cases

EUS: Configuration

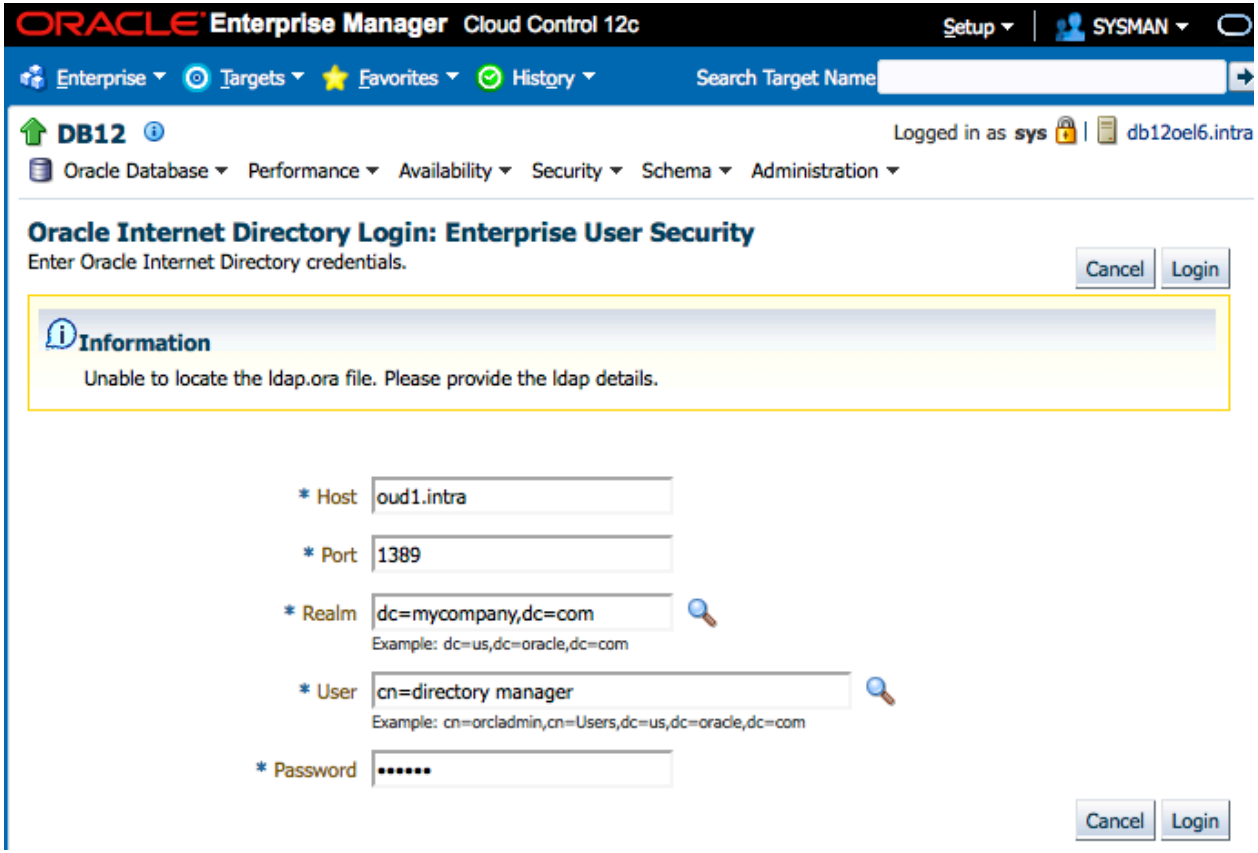
- OUD
- WLS
- ADF
- Conf ADF
- Conf OUD
- LDAP User
- Ldap.ora
- Dbca
- EUS



EUS Use Cases

EUS: Configuration

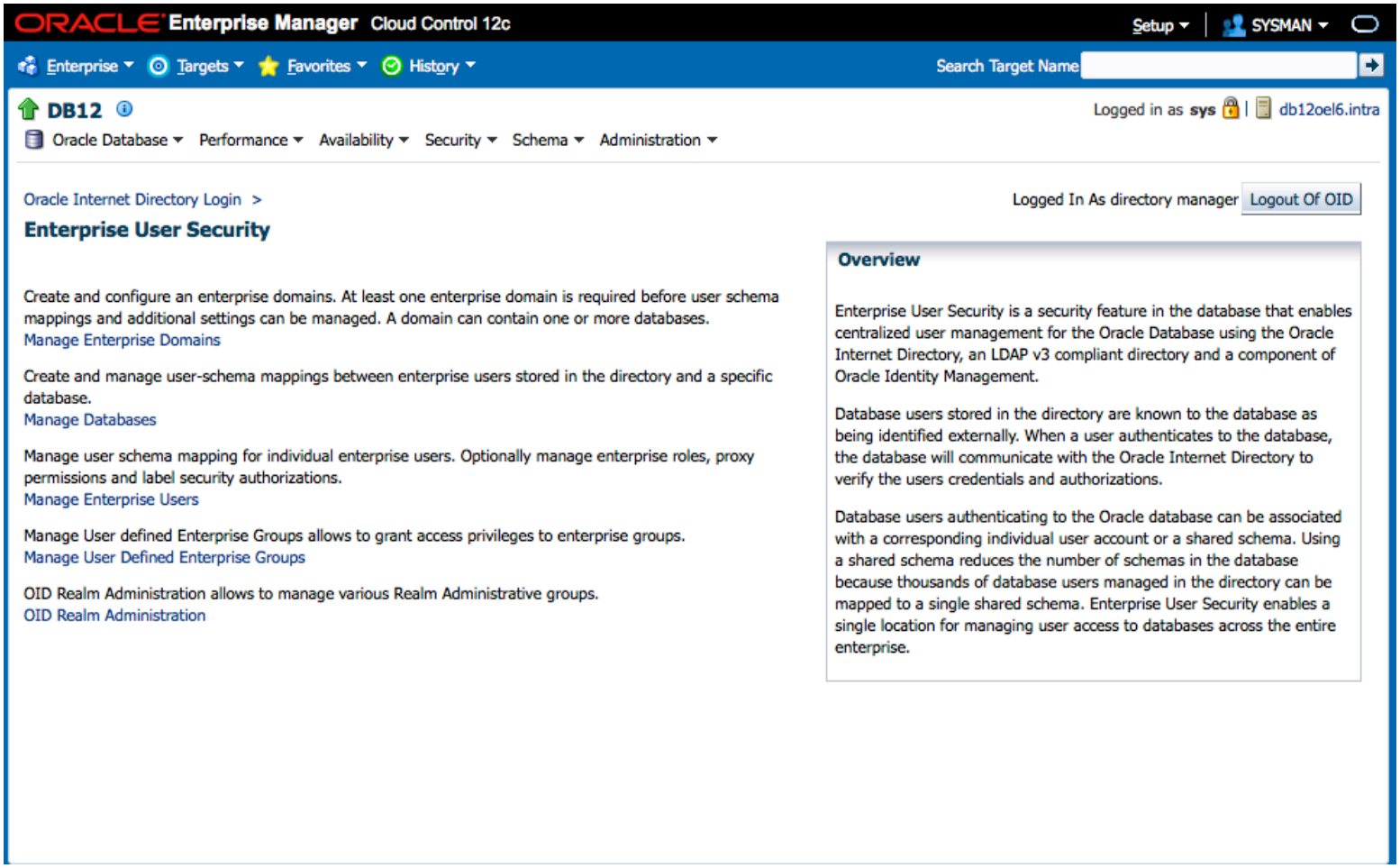
- OUD
- WLS
- ADF
- Conf ADF
- Conf OUD
- LDAP User
- Ldap.ora
- Dbca
- EUS



EUS Use Cases

EUS: Configuration

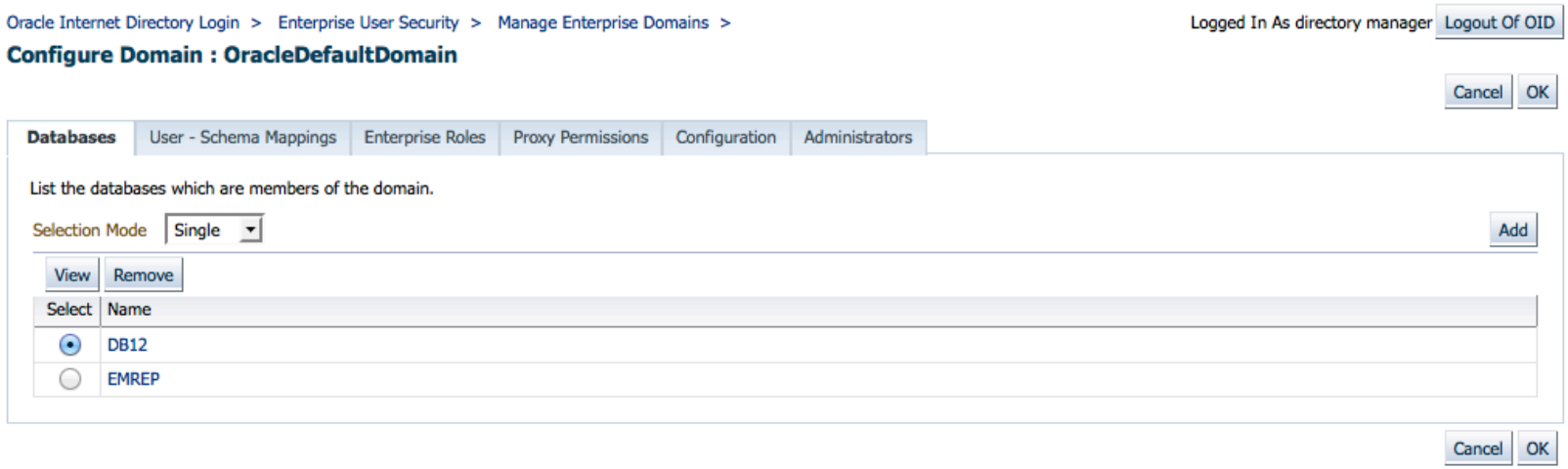
- OUD
- WLS
- ADF
- Conf ADF
- Conf OUD
- LDAP User
- Ldap.ora
- Dbca
- EUS



EUS Use Cases

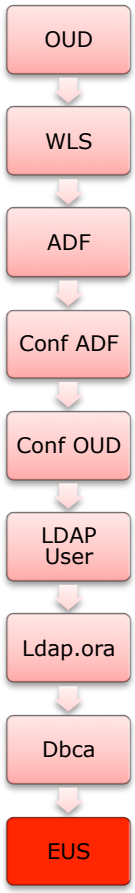
EUS: Configuration - Target DB

- OUD
- WLS
- ADF
- Conf ADF
- Conf OUD
- LDAP User
- Ldap.ora
- Dbca
- EUS



EUS Use Cases

EUS: Configuration – User Schema Mapping



Oracle Internet Directory Login > Enterprise User Security > Manage Enterprise Domains >

Logged In As directory manager | Logout Of OID

Configure Domain : OracleDefaultDomain

Cancel | OK

Databases | **User - Schema Mappings** | Enterprise Roles | Proxy Permissions | Configuration | Administrators

A user-schema mapping binds a single enterprise user (entry level mapping) or sub tree of enterprise users (sub tree level mapping) to a database schema.

Selection Mode: Single — Create

Edit | Delete

Select	From Enterprise User(s)	Mapping Type	To Schema
◉	tom	USER	GU_DBA
○	bob	USER	GU_DBA
○	steve	USER	GU_DBA
○	nero	USER	EUS_DBA
○	kevin	USER	GU_APP1
○	mike	USER	GU_APP1
○	andrew	USER	GU_APP1
○	cary	USER	GU_APP2
○	sam	USER	GU_APP2
○	eddie	USER	GU_APP2

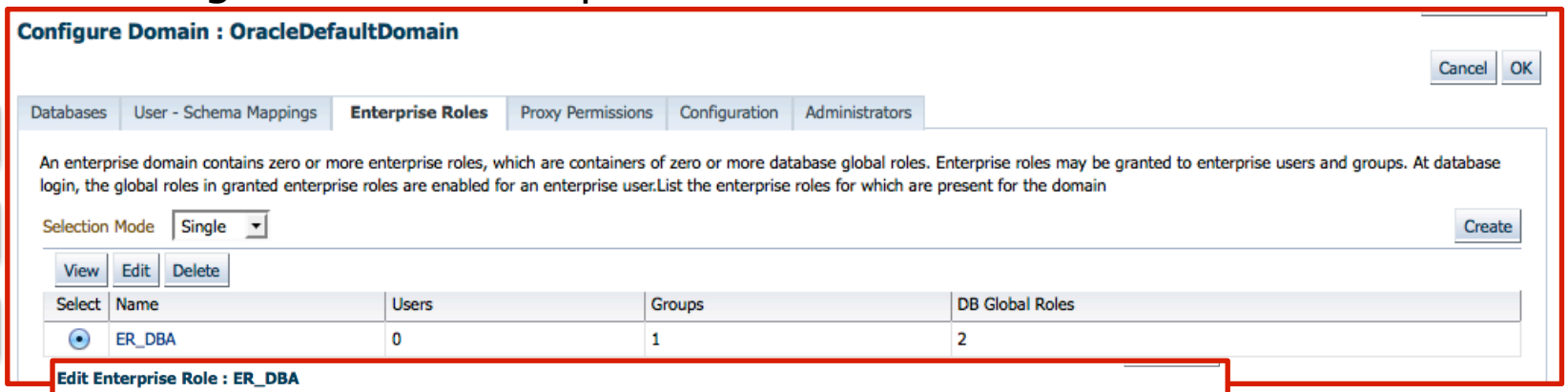
Edit | Delete

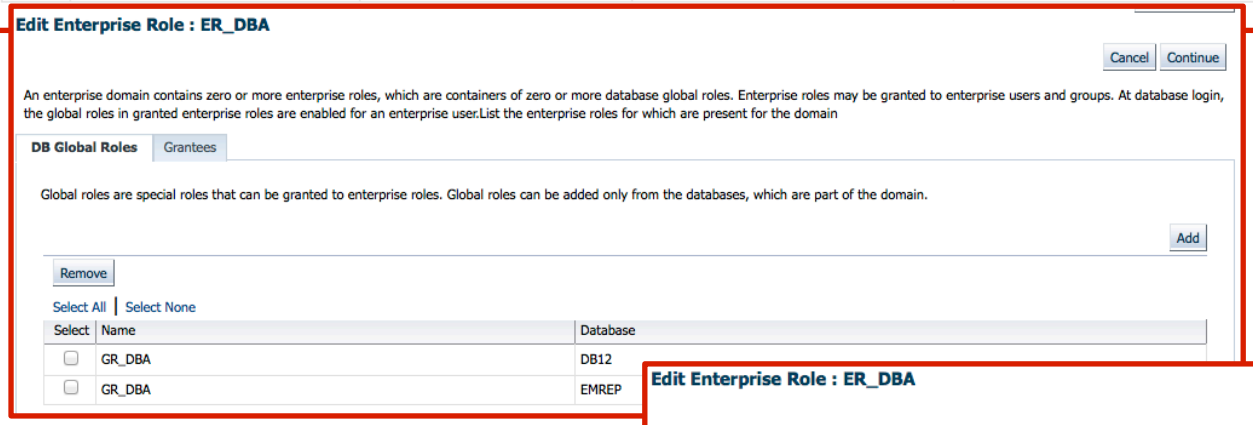
Cancel | OK

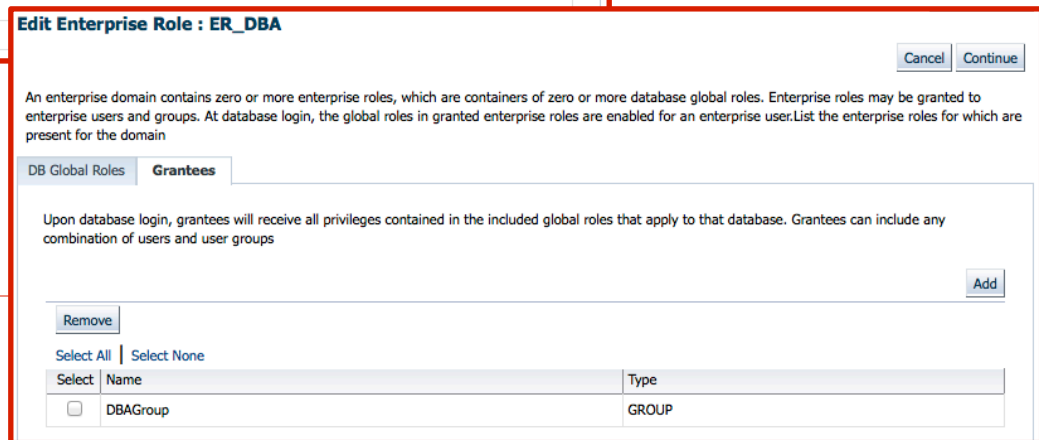
EUS Use Cases

EUS: Configuration – Enterprise Role

- OUD
- WLS
- ADF
- Conf ADF
- Conf OUD
- LDAP User
- Ldap.ora
- Dbca
- EUS



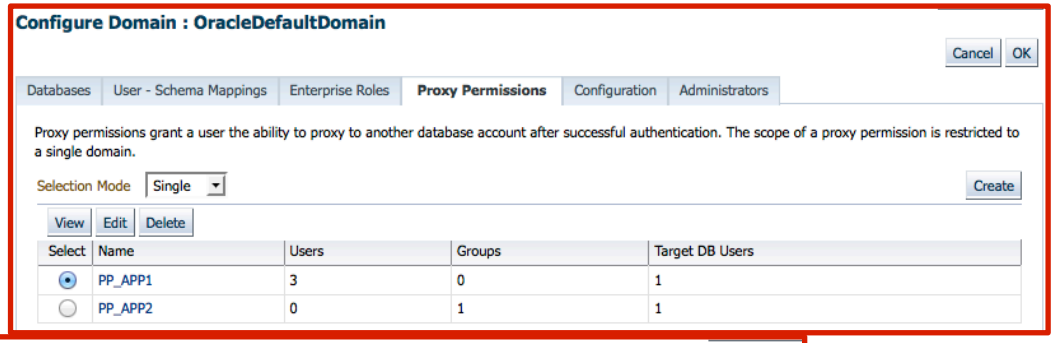


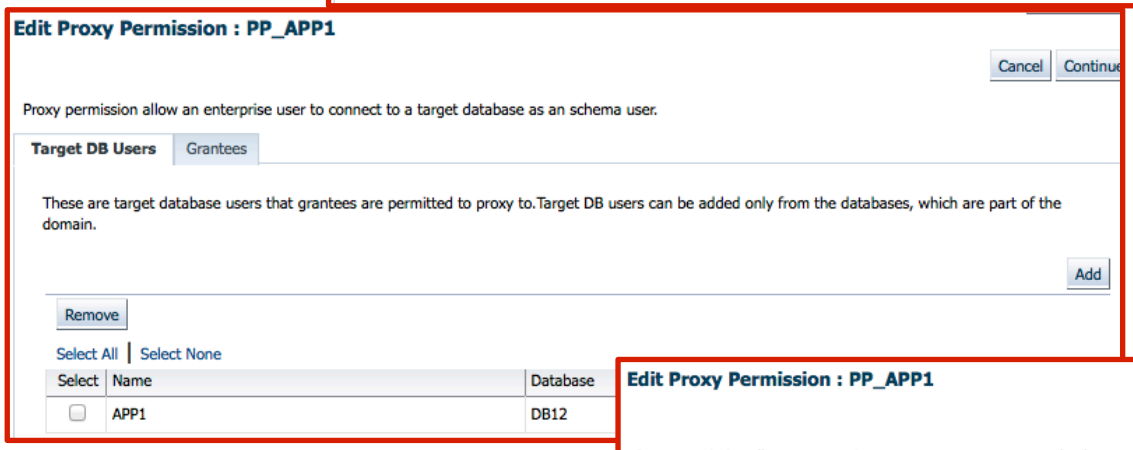


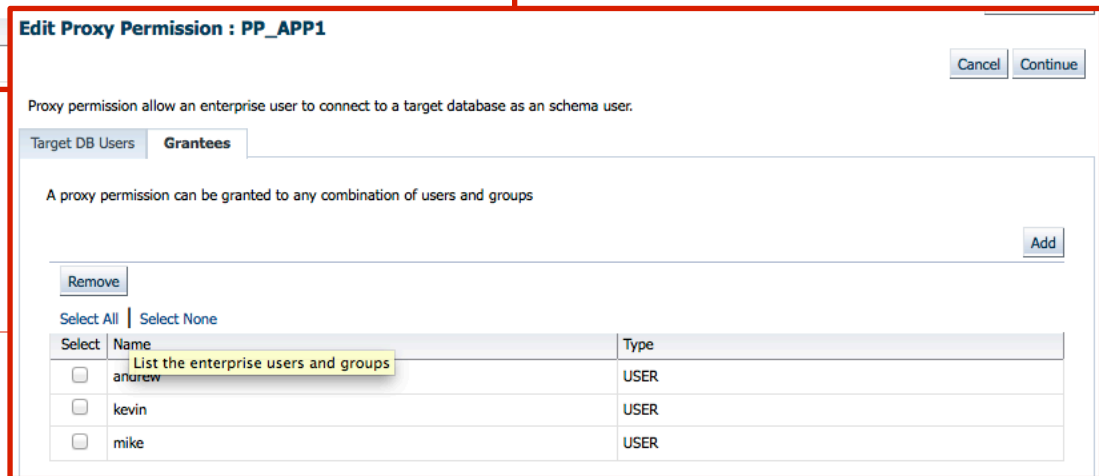
EUS Use Cases

EUS: Configuration – Proxy Permissions

- OUD
- WLS
- ADF
- Conf ADF
- Conf OUD
- LDAP User
- Ldap.ora
- Dbca
- EUS

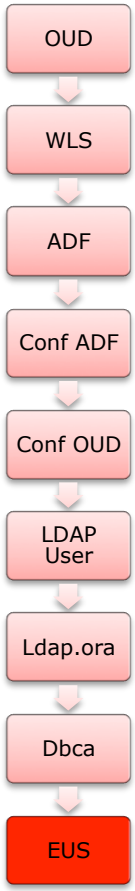






EUS Use Cases

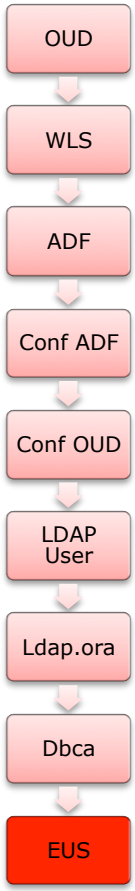
EUS: Enterprise Role




```
SQL> connect tom/pw4tom@DB12
Connected.
SQL> show user
USER is "GU_DBA"
SQL> select * from session_roles;

ROLE
--------------------------------------------------------------------------------------------------------------------------------
--------------------------
DBA
SELECT_CATALOG_ROLE
EXECUTE_CATALOG_ROLE
DELETE_CATALOG_ROLE
CAPTURE_ADMIN
EXP_FULL_DATABASE
IMP_FULL_DATABASE
DATAPUMP_EXP_FULL_DATABASE
DATAPUMP_IMP_FULL_DATABASE
XS_RESOURCE
GATHER_SYSTEM_STATISTICS
OPTIMIZER_PROCESSING_RATE
EM_EXPRESS_BASIC
EM_EXPRESS_ALL
SCHEDULER_ADMIN
HS_ADMIN_SELECT_ROLE
HS_ADMIN_EXECUTE_ROLE
XDBADMIN
XDB_SET_INVOKER
WM_ADMIN_ROLE
JAVA_ADMIN
JAVA_DEPLOY
OLAP_XS_ADMIN
OLAP_DBA
GR_DBA

25 rows selected.

SQL> select sys_context('userenv','current_user') current_user,
       sys_context('userenv','authenticated_identity') authenticated_identity,
                 sys_context('userenv','enterprise_identity') enterprise_identity from dual;  2    3

CURRENT_US AUTHENTICA ENTERPRISE_IDENTITY
---------- ---------- --------------------------------------------------
GU_DBA     TOM        cn=tom,ou=people,dc=mycompany,dc=com
```

EUS Use Cases

EUS: Proxy-Perms




```
SQL> connect mike[app1]/pw4mike@DB12
Connected.
SQL> select * from session_roles;

ROLE
--------------------------------------------------------------------------------
--------------------------
RESOURCE

SQL> show user
USER is "APP1"
SQL> col proxy_enterprise_identity format a50

select sys_context('userenv','current_user') current_user,
       sys_context('userenv','authenticated_identity') authenticated_identity,
       sys_context('userenv','PROXY_ENTERPRISE_IDENTITY') proxy_enterprise_identity from dual;

CURRENT_US AUTHENTICA PROXY_ENTERPRISE_IDENTITY
---------- ---------- --------------------------------------------------
APP1       APP1       cn=mike,ou=people,dc=mycompany,dc=com
```

```
SQL> connect sam[APP2]/pw4sam@DB12
Connected.
SQL> show user
USER is "APP2"
SQL> select * from session_roles;

ROLE
--------------------------------------------------------------------------------
--------------------------
RESOURCE

SQL> select sys_context('userenv','current_user') current_user,
       sys_context('userenv','authenticated_identity') authenticated_identity,
       sys_context('userenv','PROXY_ENTERPRISE_IDENTITY') proxy_enterprise_identity from dual;

CURRENT_US AUTHENTICA PROXY_ENTERPRISE_IDENTITY
---------- ---------- --------------------------------------------------
APP2       APP2       cn=sam,ou=people,dc=mycompany,dc=com
```

Referenzen

- DB Documentation: **Oracle® Database Enterprise User Security Administrator's Guide /** http://docs.oracle.com/database/121/DBIMI/toc.htm

- OUD Documentation: **Fusion Middleware Unified Directory 11g Release 2 (11.1.2.2)** http://docs.oracle.com/cd/E49437_01/index.htm

- Oracle Virtual Directory / **Oracle® Fusion Middleware Administrator's Guide for Oracle Virtual Directory 11*g* Release 1 (11.1.1)** http://docs.oracle.com/cd/E28280_01/admin.1111/e10046/toc.htm

Fazit

- interessante Technologie
- Randprodukt mit wenig Kunden
- viele Bugs, aber keine Showstopper
- Oracle Support problematisch (SR älter als 9 Monate), da Team-übergreifend (OVD, OUD, EUS)
- keine neuen Features mit 12c, außer Pluggable DB Unterstützung

Q & A

Martin Decker
ora-solutions.net

ORACLE 10g Certified Master

ORACLE Certified Master
Oracle Database 11g Administrator

E-Mail: martin.decker@ora-solutions.net
Internet: http://www.ora-solutions.net
Blog: http://www.ora-solutions.net/web/blog/