

Enterprise User Security

Eine Einführung

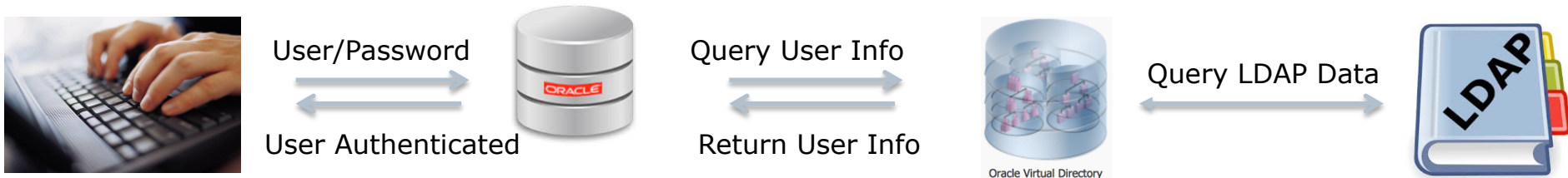
DOAG Regionaltreffen München
18. September 2014

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

- ❑ 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

- ❑ 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)



☐ 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)

- ❑ 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

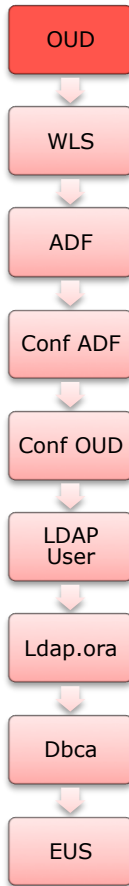
- ☐ Installation JDK 1.7
- ☐ Installation OUD 11.1.2.2.0
- ☐ Installation Oracle Weblogic 10.3.6
- ☐ Installation Oracle ADF 11.1.1.7.0
- ☐ Configure ODSM mit ADF für OUD
- ☐ Configure OUD
- ☐ LDAP User anlegen
- ☐ Configure ldap.ora
- ☐ DBCA: Register Database
- ☐ Configure Schema Mapping, Enterprise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

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

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



Oracle Fusion Middleware 11g Installation

Specify Inventory directory

ORACLE 11g FUSION MIDDLEWARE

You are starting your first installation on this host. As part of this install, you need to specify a directory for installer files. This is called the "inventory directory". Within the inventory directory, the installer automatically sets up subdirectories for each product to contain inventory data and will consume typically 150 Kilobytes per product.

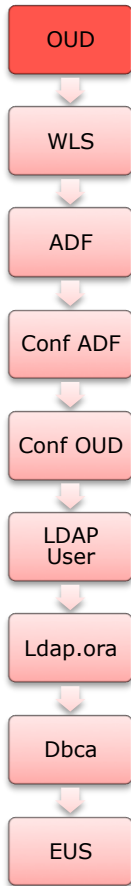
Enter the full path of the inventory directory.
You can specify an Operating System group that has write permissions to the above directory

Inventory Directory:

Operating System Group name:

Implementierung OUD

OUD:



The screenshot shows the 'Specify Installation Location' window for Oracle Unified Directory (OUD) installation. The window title is 'Oracle Unified Directory Installation - Step 4 of 7'. The Oracle 11g Fusion Middleware logo is in the top right. On the left, a navigation pane lists the installation steps: Welcome, Skip Software Updates, Prerequisite Checks, **Installation Location** (selected), Installation Summary, Installation Progress, and Installation Complete. The main area contains two input fields: 'OUD Base Location Home' with a dropdown menu showing '/u01/app/oracle/mw' and a 'Browse' button, and 'Oracle Home Directory' with a text box containing 'Oracle_OUD1'. Below these fields is a message box that says 'Provide a valid Unified Directory Base location'. At the bottom, there are buttons for 'Help', '< Back', 'Next >', 'Finish', and 'Cancel'. The 'Elapsed Time: 6m 29s' is displayed in the bottom right corner.

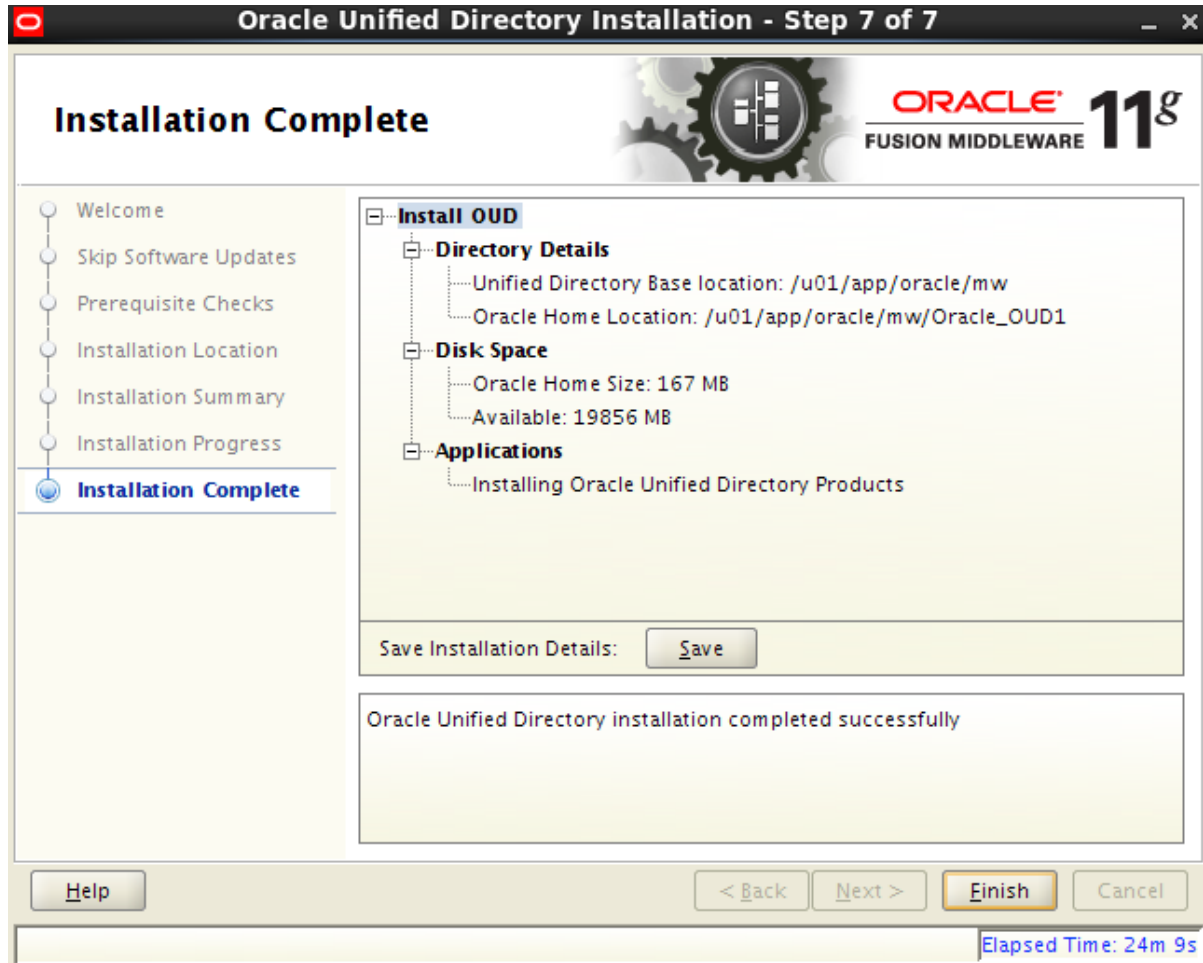
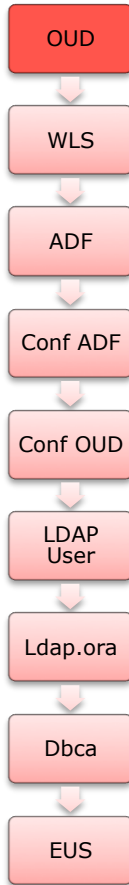
Implementierung OUD

ORA-SOLUTIONS.NET

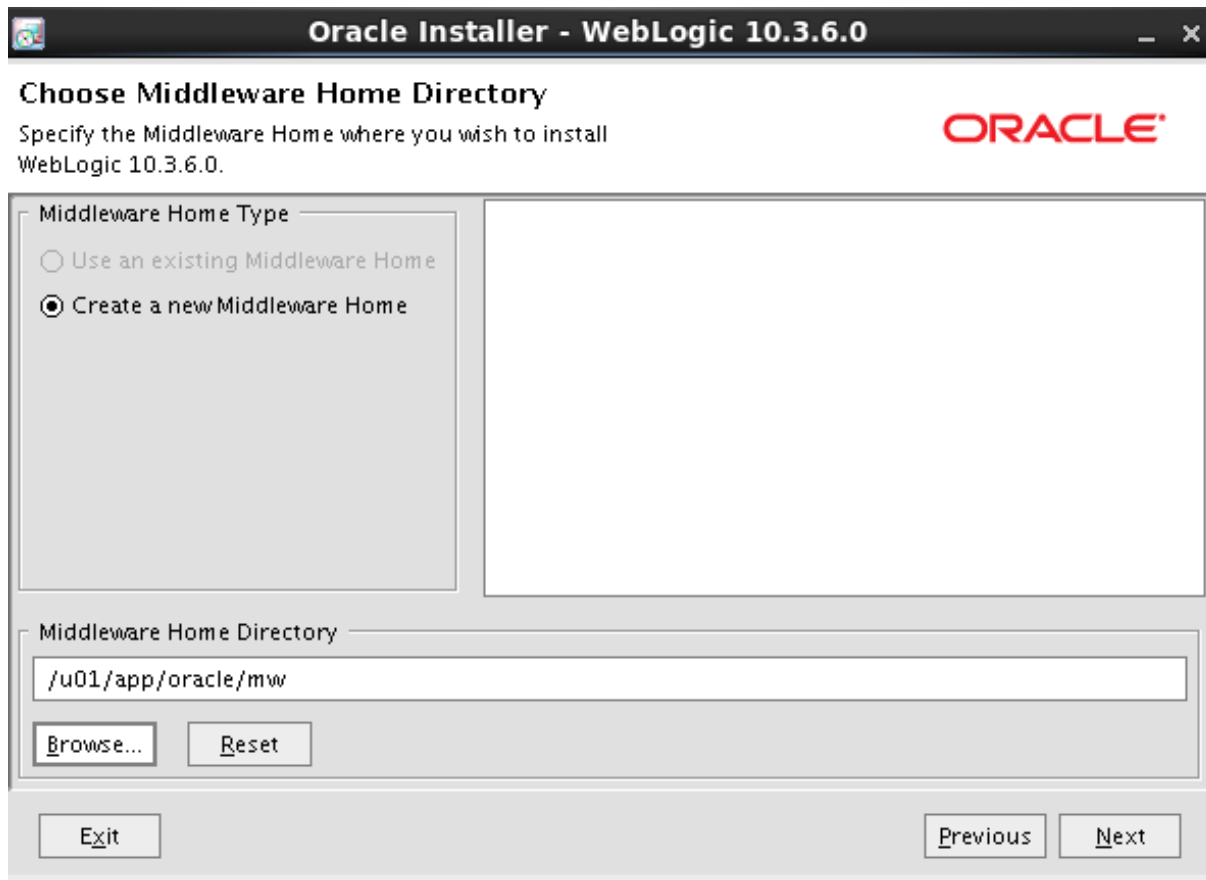
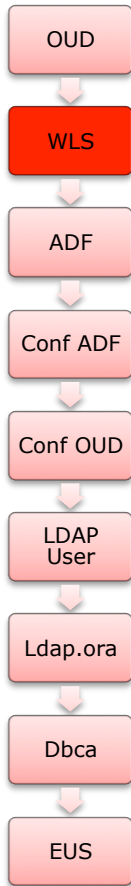
Mastering Oracle Performance, High Availability, Manageability

Martin Decker

OUD:



Weblogic: `java -d64 -jar wlsversion_generic.jar`



Implementierung OUD

Weblogic: (Custom, De-Select Coherence)

The diagram illustrates the installation sequence for OUD (Oracle Universal Installer) and the Oracle WebLogic 10.3.6.0 installer windows.

Installation Sequence:

- OAD
- WLS (highlighted in red)
- ADF
- Conf ADF
- Conf OUD
- LDAP User
- Ldap.ora
- Dbca
- EUS

Oracle Installer - WebLogic 10.3.6.0 - Choose Install Type

Select the type of installation you wish to perform.

Options:

- ☐ Typical
- ☒ Custom

Oracle Installer - WebLogic 10.3.6.0 - Choose Products and Components

Grayed selections are already installed. Double-click headings to reveal or collapse selections.

Selected Components:

- ☒ WebLogic Server
 - ☒ Core Application Server
 - ☒ Administration Console
 - ☒ Configuration Wizard and Upgrade Framework
 - ☒ Web 2.0 HTTP Pub-Sub Server
 - ☒ WebLogic SCA
 - ☒ WebLogic JDBC Drivers
 - ☒ Third Party JDBC Drivers
 - ☒ WebLogic Server Clients
 - ☒ WebLogic Web Server Plugins
 - ☒ UDDI and Xquery Support
 - ☐ Server Examples
 - ☒ Evaluation Database
- ☐ Oracle Coherence

Description:

Coherence provides reliable distributed in-memory data management and caching services on top of a highly scalable peer-to-peer clustering protocol.

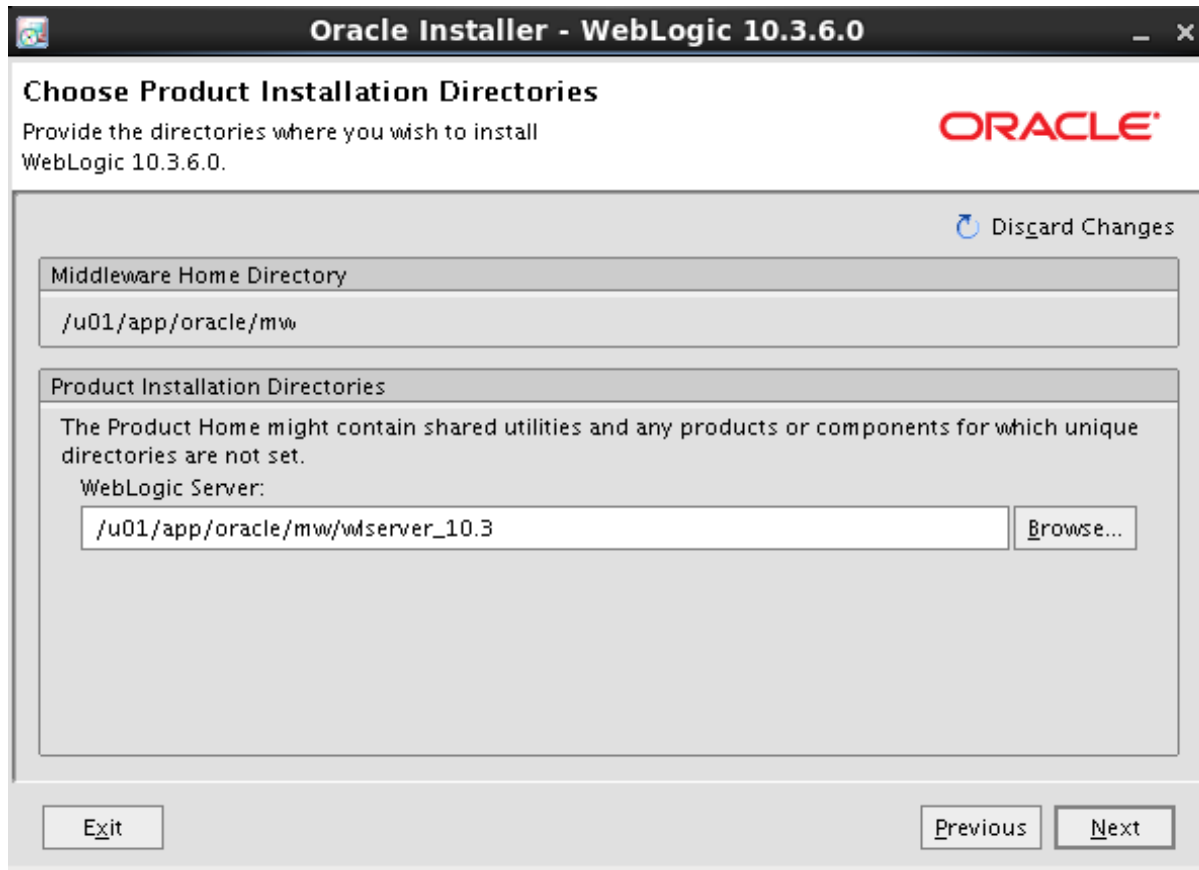
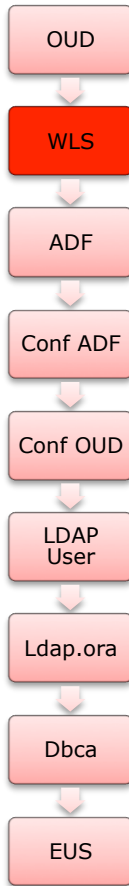
Approximate Installed Size*

Approximate Installed Size*	
Highlighted item:	17.1 MB
Common artifacts:	50.8 MB
Total of all selected items:	678.7 MB

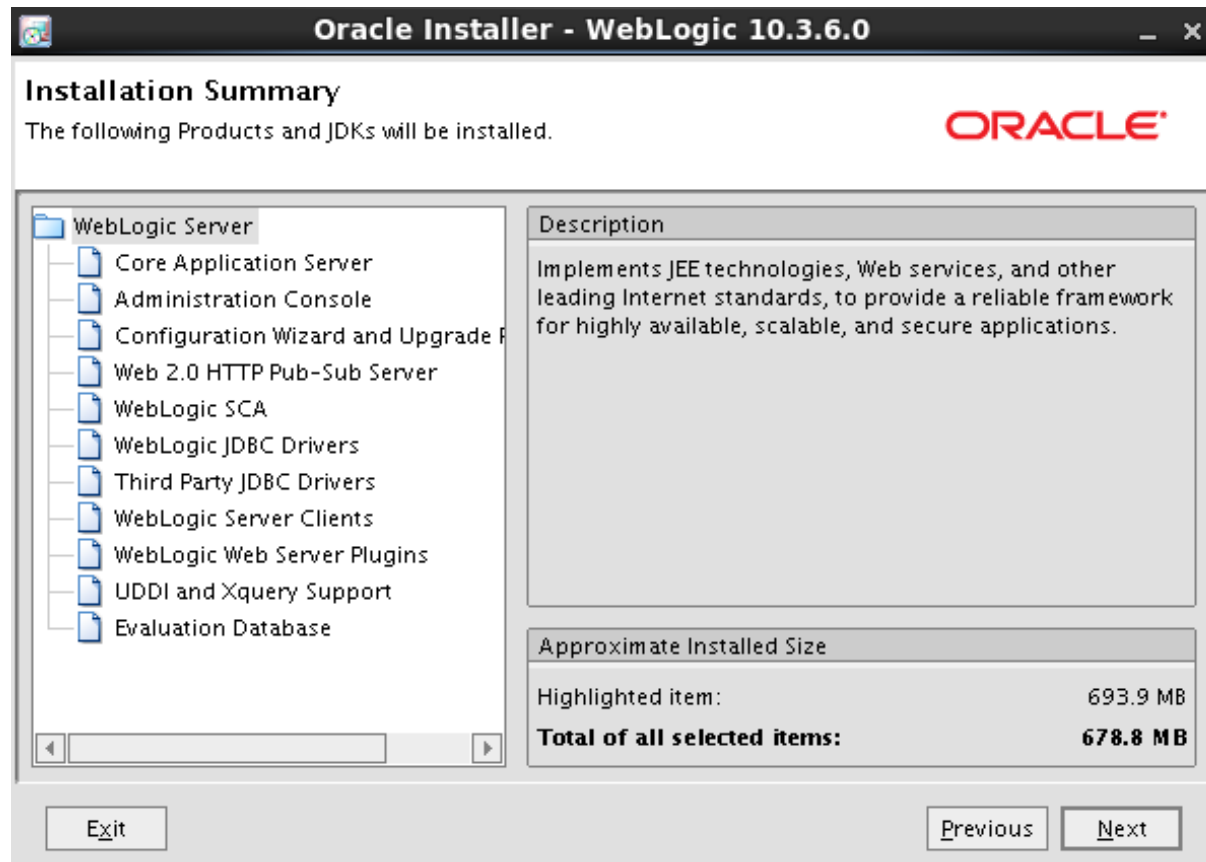
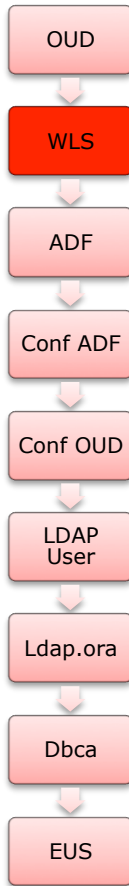
*Installer requires free disk space approximately 2x this total

Buttons: Exit, Previous, Next

Weblogic:

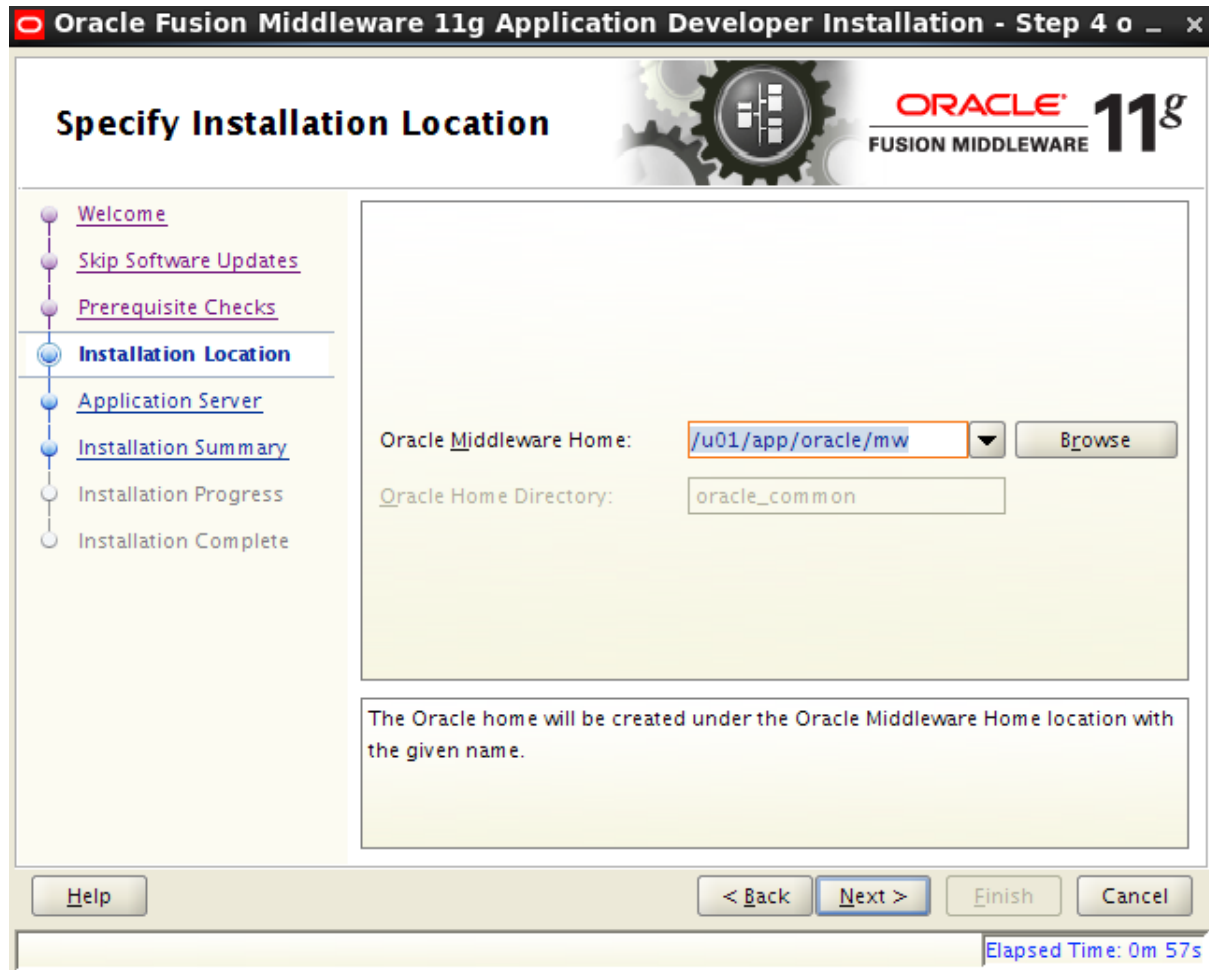
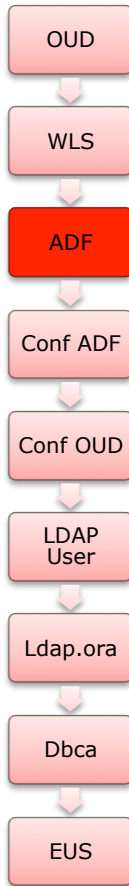


Weblogic:



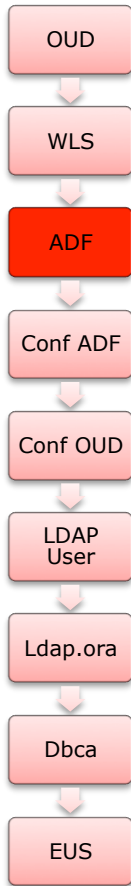
Implementierung OUD

ADF: `./runInstaller -jreLoc $JAVA_HOME/jre`



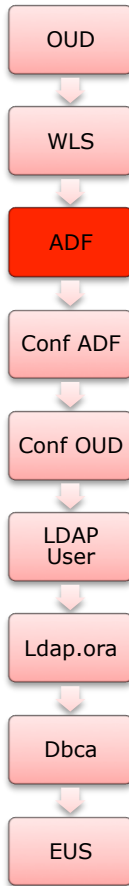
Implementierung OUD

ADF:



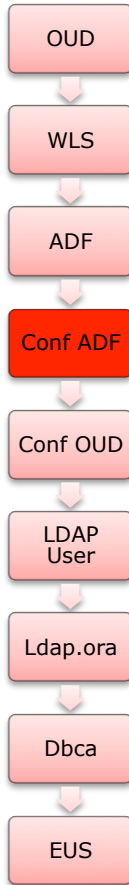
Implementierung OUD

ADF:

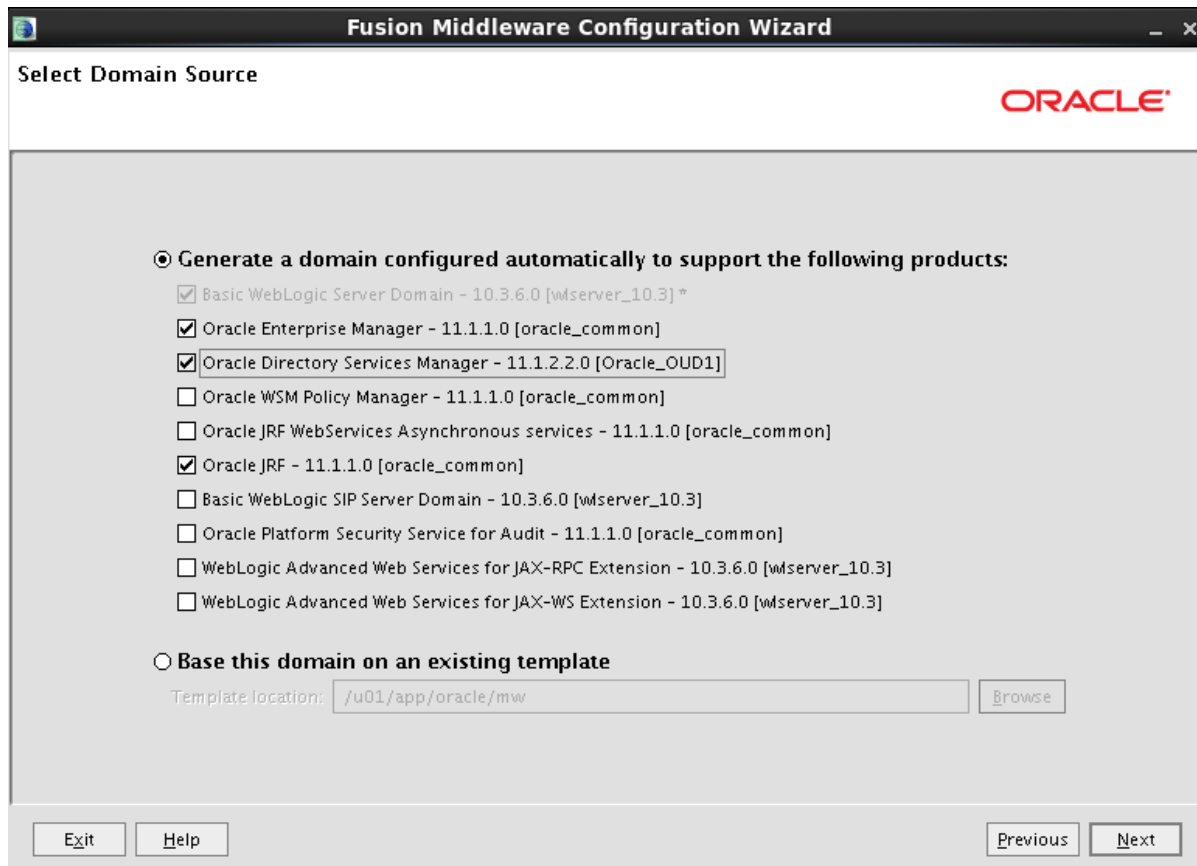
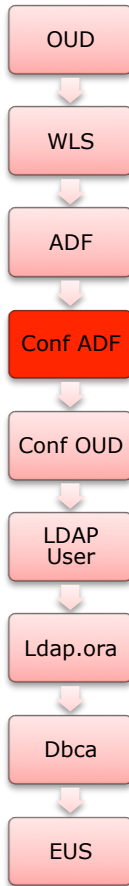


Configure OSDM with ADF for OUD:

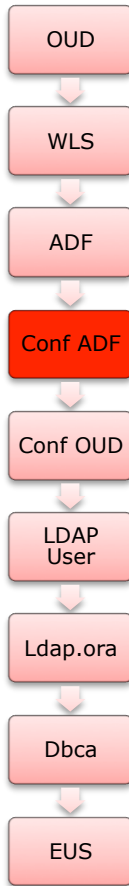
```
[oracle@oud1 Disk1]$ cd /u01/app/oracle/mw/oracle_common/common/bin/  
[oracle@oud1 bin]$ ./config.sh
```



Configure OSDM with ADF for OUD:



Configure OSDM with ADF for OUD:



Fusion Middleware Configuration Wizard

Specify Domain Name and Location

ORACLE

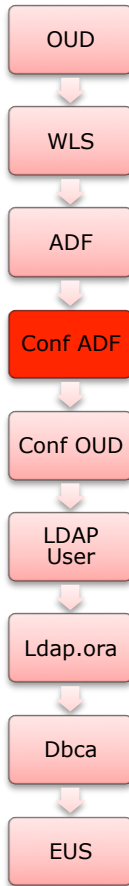
Enter the name and location for the domain and its applications:

Domain name:

Domain location:

Application location:

Configure OSDM with ADF for OUD:



Fusion Middleware Configuration Wizard

Configure Server Start Mode and JDK

ORACLE

Before putting your domain into production, make sure that the production environment is secure. For more information, see the topic 'Securing a Production Environment' in the WebLogic Server documentation.

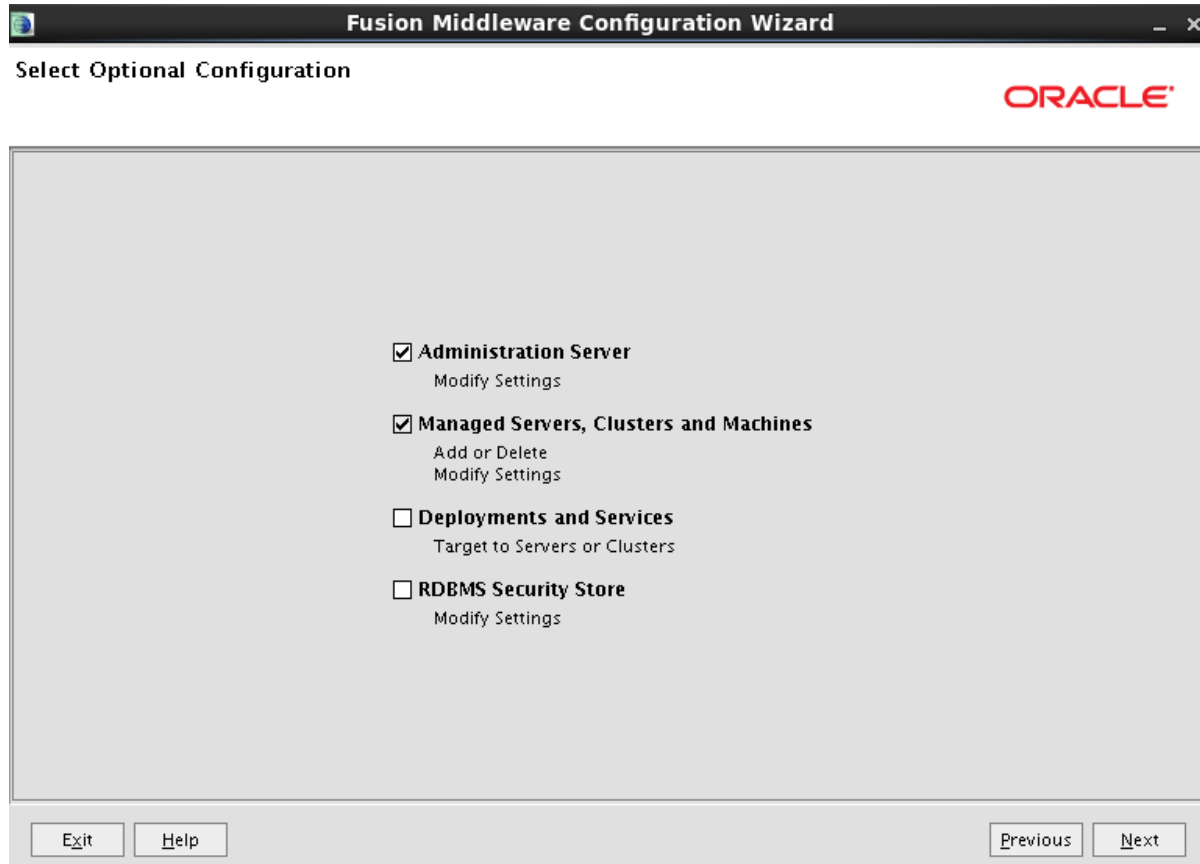
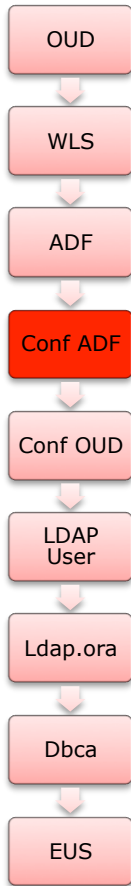
WebLogic Domain Startup Mode

- ☐ **Development Mode**
Utilize boot.properties for username and password and poll for applications to deploy.
Sun JDK recommended for better startup performance during iterative development.
- ☒ **Production Mode**
Require the entry of a username and password and do not poll for applications to deploy.
WebLogic JRockit JDK recommended for better runtime performance and management.

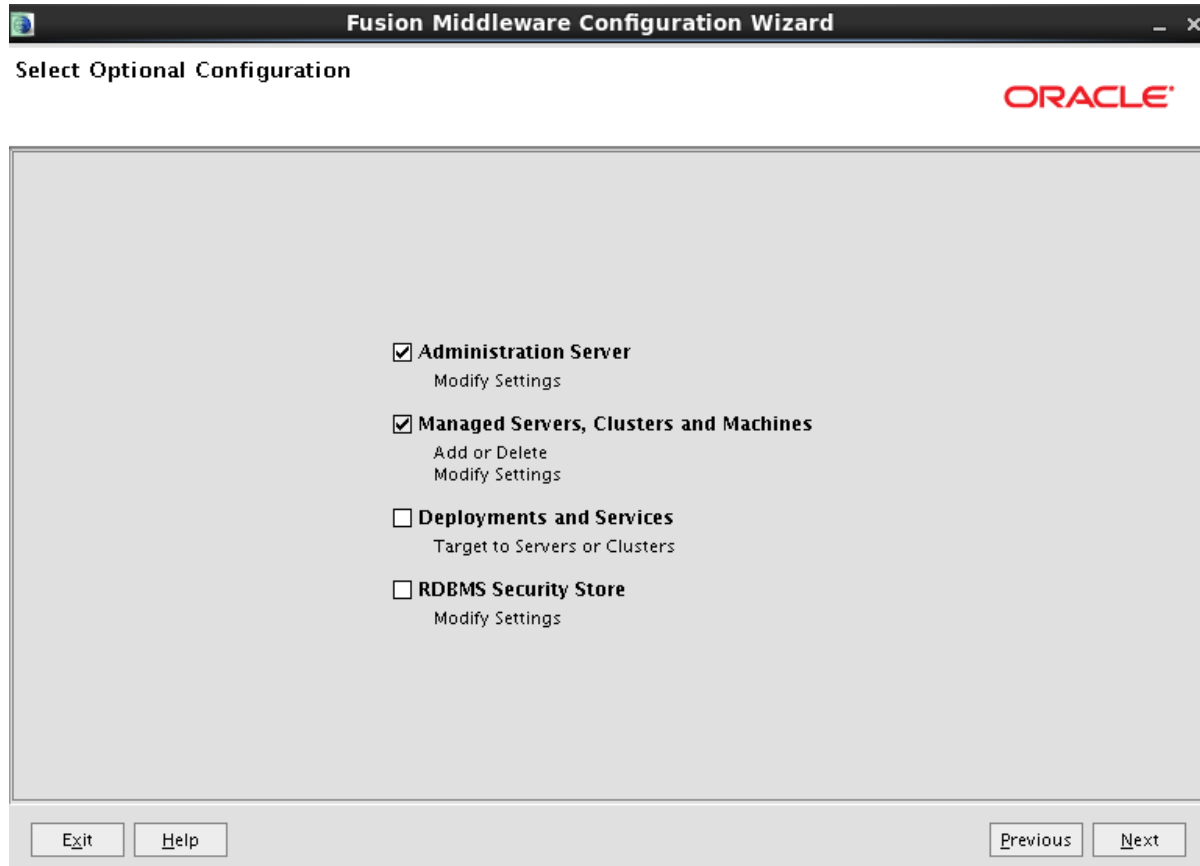
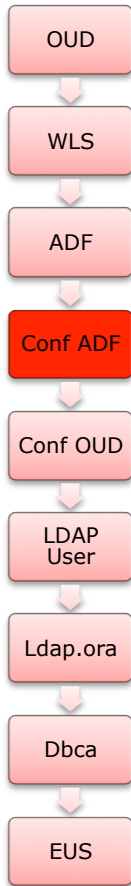
JDK Selection

- ☒ **Available JDKs**
Sun SDK 1.7.0_55 @ /u01/app/jdk1.7.0_55
- ☐ **Other JDK**
Location:

Configure OSDM with ADF for OUD:



Configure OSDM with ADF for OUD:

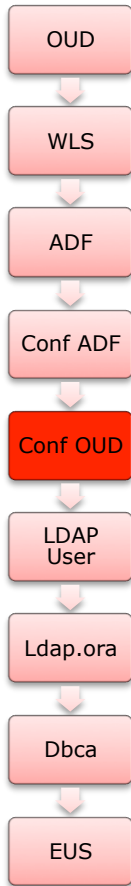


OSDM: <https://oud1.intra:7002/odsm/>

WLS Admin Server Console: <https://oud1.intra:7002/console/>

Configure OUD:

```
[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
```



Oracle Unified Directory Setup

Welcome

➔ **Server Settings**

Topology Options

Oracle Components Integration

Server Tuning

Review

Progress

Finished

Server Settings

Enter a port to listen for LDAP requests and enter a password for the server initial Root user.

Host Name:

LDAP Listener Port: Could not use 389. Port in use or user not authorized.

Administration Connector Port:

LDAP Secure Access: disabled

Root User DN:

Password:

Password (confirm):

< Previous Next > Quit

Configure OUD:



Security Options

Configure Secure Access
Specify the options for enabling secure access to the server.

SSL Access: ☒ Enable SSL on Port: Could not use 636. Port in use or user not authorized.

StartTLS Access: ☐ Enable StartTLS for LDAP

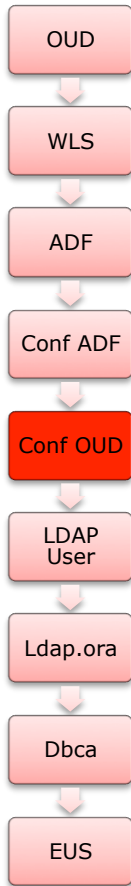
Certificate: ☒ Generate Self-Signed Certificate (recommended for testing only)
☐ Use an Existing Certificate:

Key Store Type: ☐ Java Key Store (JKS) File
☐ JCEKS File
☐ PKCS#12 File
☐ PKCS#11 Token

Key Store Path:

Key Store PIN:

Configure OUD:



Oracle Unified Directory Setup

Welcome

Server Settings

Topology Options

Oracle Components Integration

Server Tuning

Review

Progress

Finished

Topology Options

Choose the Data Replication Options.

☒ This will be a stand alone server

☐ This server will be part of a replication topology

Replication Port: 8989 ☐ Configure as Secure

☐ There is already a server in the topology

Host Name:

Administration Connector Port: 4444

Admin User: cn=Directory Manager

Admin Password:

< Previous Next > Quit

Configure OUD:

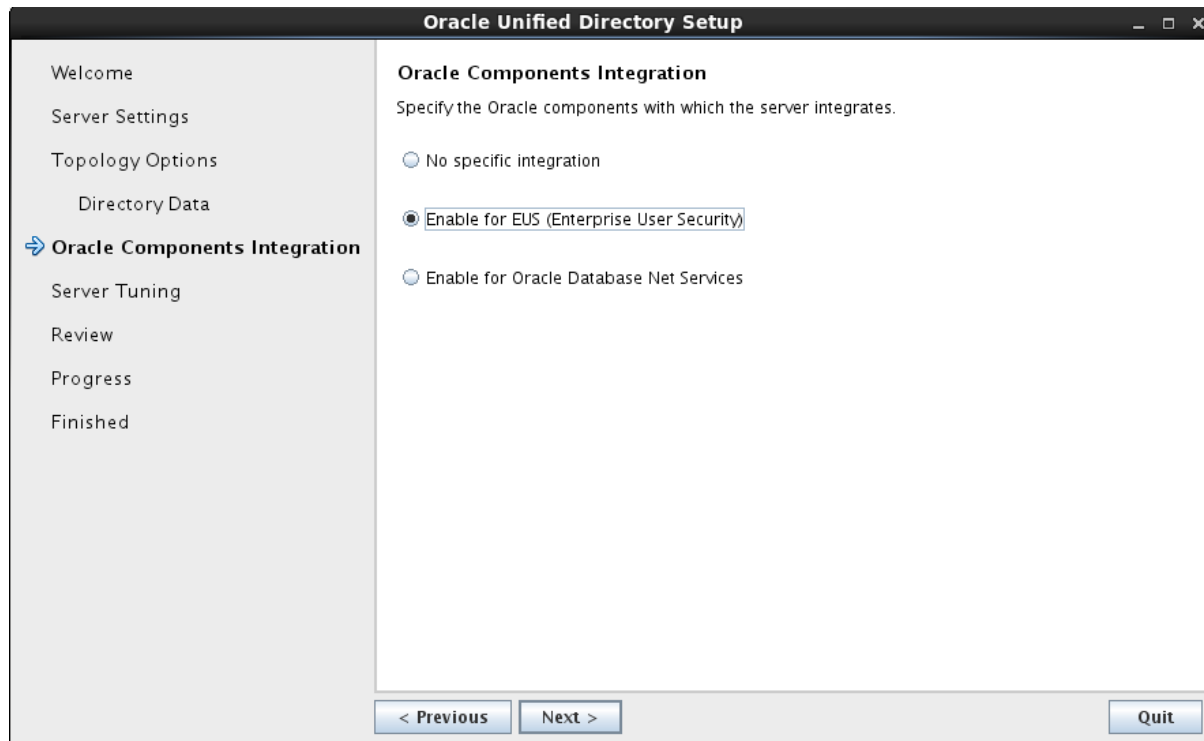
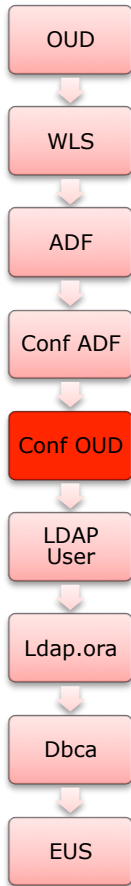


The screenshot shows the 'Oracle Unified Directory Setup' window, specifically the 'Directory Data' step. The left sidebar lists the setup stages: Welcome, Server Settings, Topology Options, **Directory Data** (selected), Oracle Components Integration, Server Tuning, Review, Progress, and Finished. The main area contains the following options:

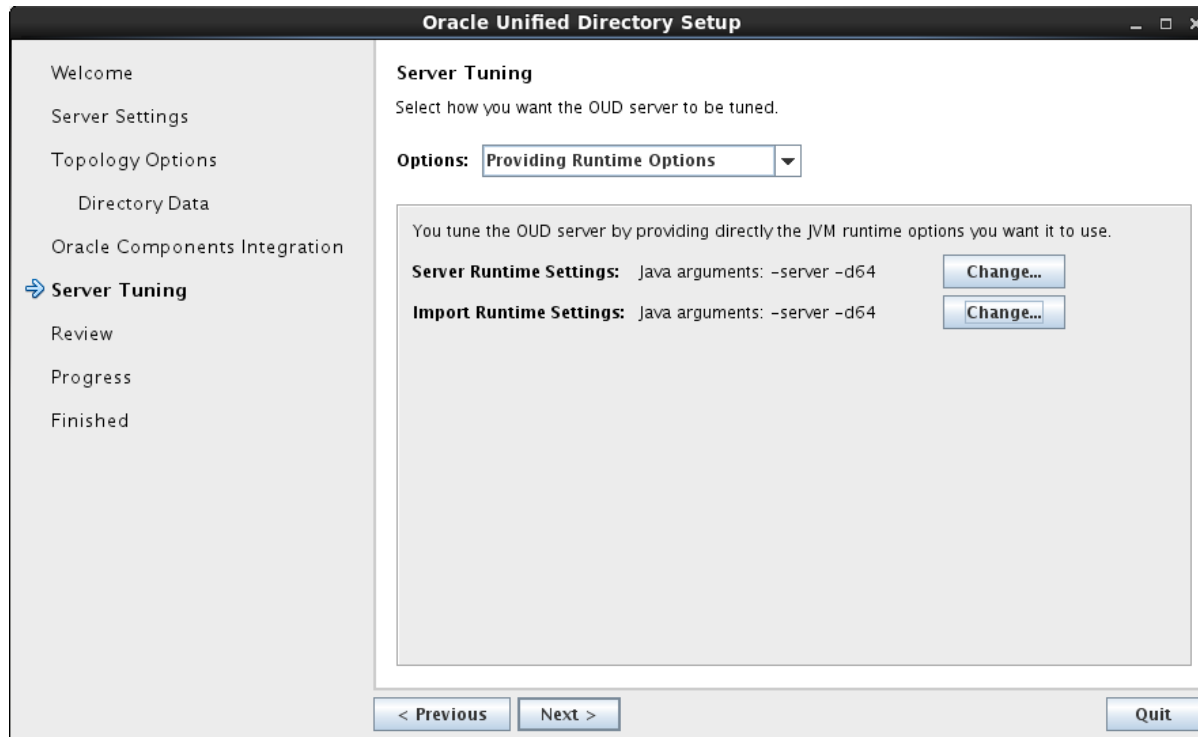
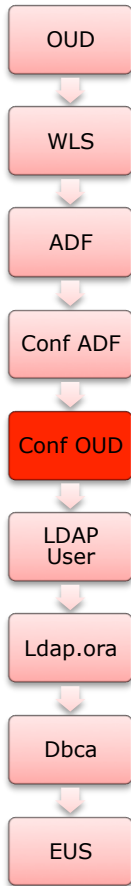
- Directory Base DN:** (Note: Leave empty if you do not want to create a base DN.)
- Directory Data:**
 - ☒ Only Create Base Entry (dc=mycompany,dc=com)
 - ☐ Leave Database Empty
 - ☐ Import Data from LDIF File
 - Path:
 - ☐ Import Automatically-Generated Sample Data
 - Number of User Entries:

Navigation buttons at the bottom: '< Previous', 'Next >', and 'Quit'.

Configure OUD:



Configure OUD:



Configure OUD:

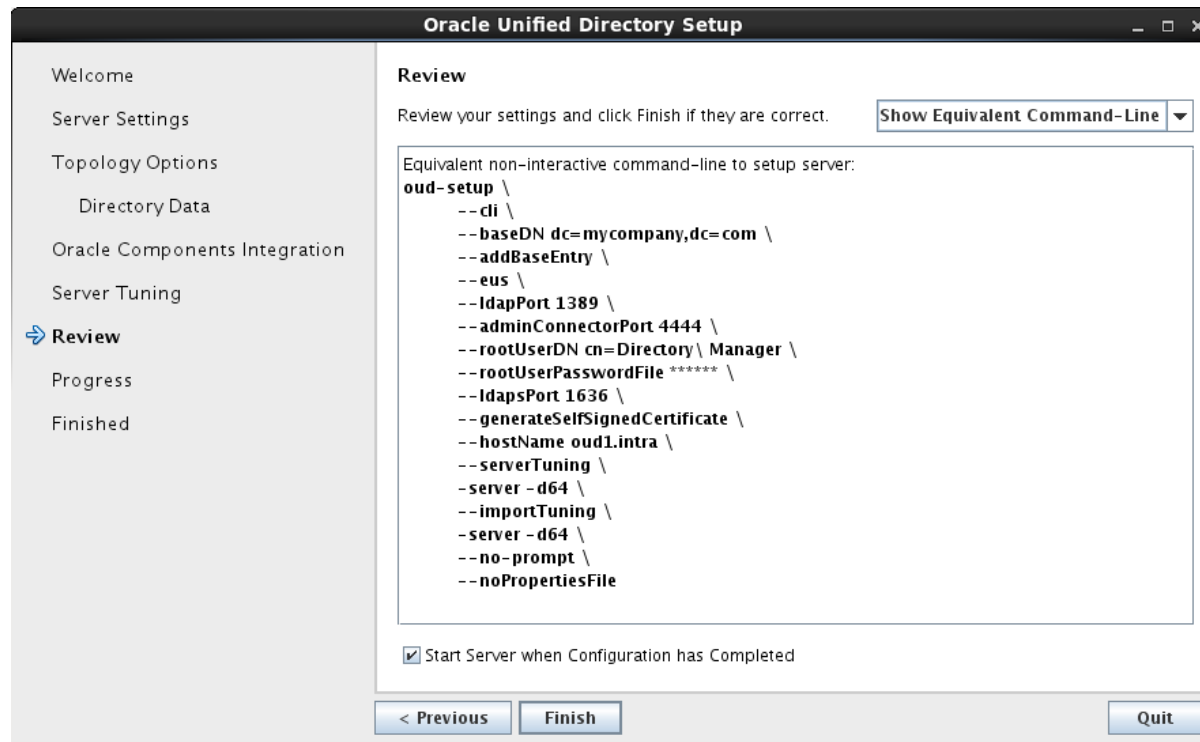


The screenshot shows the 'Oracle Unified Directory Setup' window, specifically the 'Review' step. The left sidebar lists the setup stages: Welcome, Server Settings, Topology Options, Directory Data, Oracle Components Integration, Server Tuning, Review (selected), Progress, and Finished. The main area displays the configuration details for review.

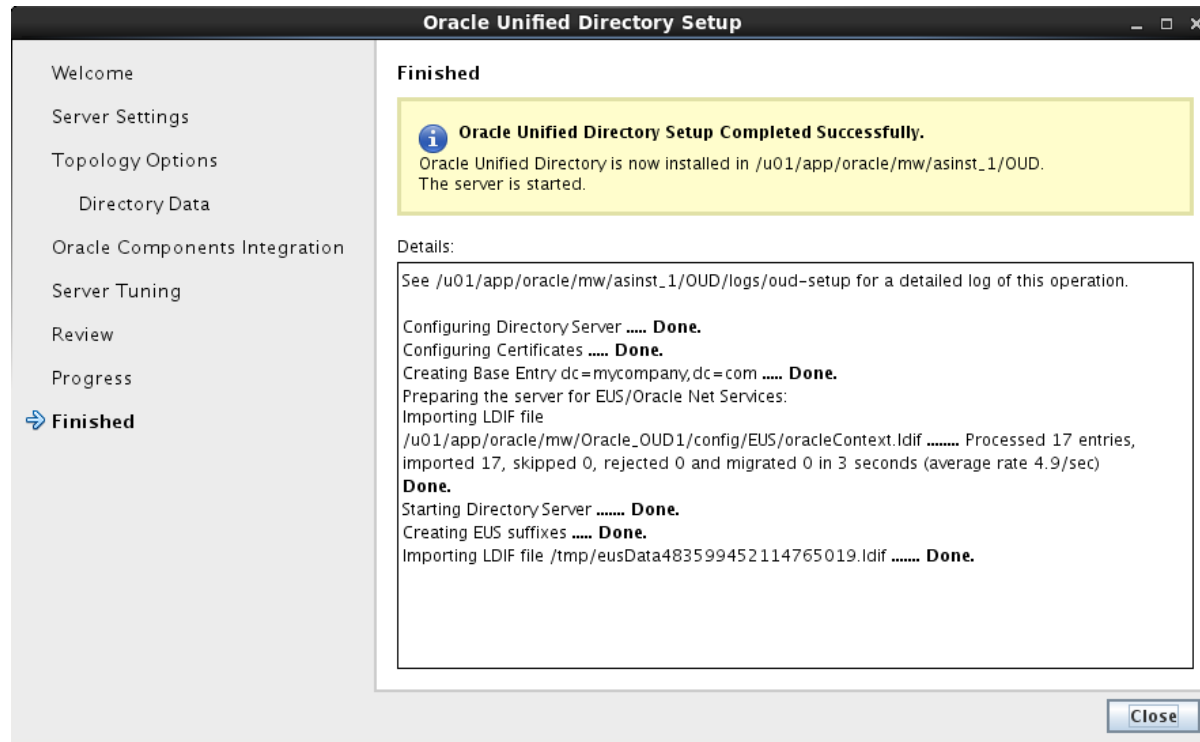
Property	Value
Host Name:	oud1.intra
LDAP Listener Port:	1389
Administration Connector Port:	4444
LDAP Secure Access:	Enable SSL on LDAP Port 1636 Create a new Self-Signed Certificate
Root User DN:	cn=Directory Manager
Directory Data:	Create New Base DN dc=mycompany,dc=com Base DN Data: Only Create Base Entry (dc=mycompany,d c=com)
Integration with Oracle components:	Enable for EUS (Enterprise User Security)
Runtime Options:	Use Custom Values for Server Runtime (-server -d64) Use Custom Values for Import (-server -d64)

At the bottom, there is a checkbox labeled 'Start Server when Configuration has Completed' which is checked. Navigation buttons at the bottom include '< Previous', 'Finish', and 'Quit'. A 'Show Summary' button is also present in the top right of the review area.

Configure OUD:

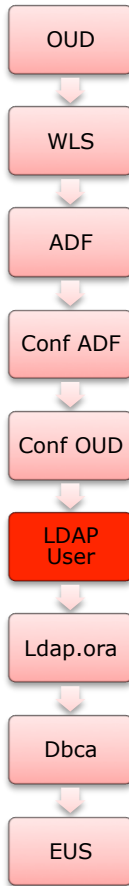


Configure OUD:



Implementierung OUD

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



The screenshot shows the Oracle Directory Services Manager (ODSM) web interface. The top navigation bar includes "Open Connections", "Accessibility", and "Help". The main content area is titled "Directory Manager" and "Topology Manager". The "Directory Connections" section is active, showing a list of connections on the left and a configuration form on the right. The form is for a connection named "OUD" with the following details:

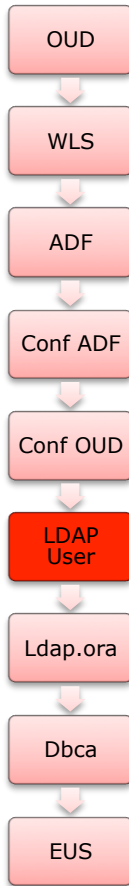
- Name: OUD
- * Server: oud1.intra
- * Administration Port: 4444
- SSL Enabled: ☒
- * User Name: cn=Directory Manager
- * Password:
- Start Page: Home
- ☒ Do you want to save this connection?
- Login button

Below the form, there is a section titled "Oracle Unified Directory Resource Center" with links to:

- ? Getting Started
- ? Connecting to OUD
- ? Setting up Proxy Server
- ? Setting up LDAP Server

Implementierung OUD

Create LDAP Users & Groups:



ORACLE Directory Services Manager

Open Connections ▾ Accessibility ▾ Help

Directory Manager Topology Manager

Directory Connections oud1 x

Home Data Browser Advanced Search Configuration Schema Security

Configuration

- Create Local Naming Context

Entry Management

- Advanced Search
- Browse Entries
- Create Entry
- Create User Entry
- Create Static Group Entry
- Create Dynamic Group Entry
- Create Virtual Static Group Entry
- Create Domain Entry
- Create Organization Entry
- Create Organization Unit Entry
- Create Country Entry
- Create Collective Attribute Subentry

Schema Management

- Attributes
- Object Classes
- Syntaxes
- Matching Rules

Version Information

ODSM 11.1.2.2.0 (OUD) OUD Oracle Unified Directory 11.1.2.2.0 Java 1.7.0_55

Server Role

Directory Proxy Load Balancer Distributor
Replication Gateway Replication Server

Refresh

OUD Statistics

Server Start Time September 3, 2014 4:41:03 PM CEST Total LDAP Operations Completed (per sec) (since startup) 0
Installation Path /u01/app/oracle/mw/Oracle_OUD1 Average Elapsed Time per Operation (since startup) (ms) 0
Instance Path /u01/app/oracle/mw/asinst_1/OUD Connection Rate (con/sec) 0.001
Administrative Users cn=Directory Manager

Refresh

Connection Handlers

Name	Type	Port	Enabled	SSL Enabled
Administration Connector	LDAP	4444	✓	✓
LDIF Connection Handler	LDIF		✗	✗
LDAPS Connection Handler	LDAP	1636	✓	✓
JMX Connection Handler	JMX	1689	✗	✗
LDAP Connection Handler	LDAP	1389	✓	✗
SNMP Connection Handler	SNMP	161	✗	✗

Refresh

Naming Contexts

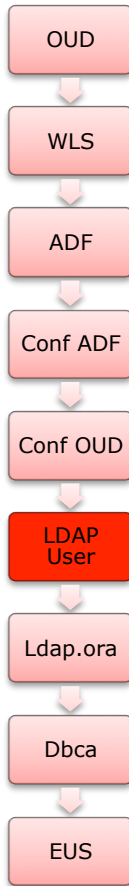
Base DN	Network Group	Server Role	Information
---------	---------------	-------------	-------------

Refresh

Implementierung OUD

Create LDAP Users & Groups:

- > Data Browser
- > ou=people
- > Create User Entry



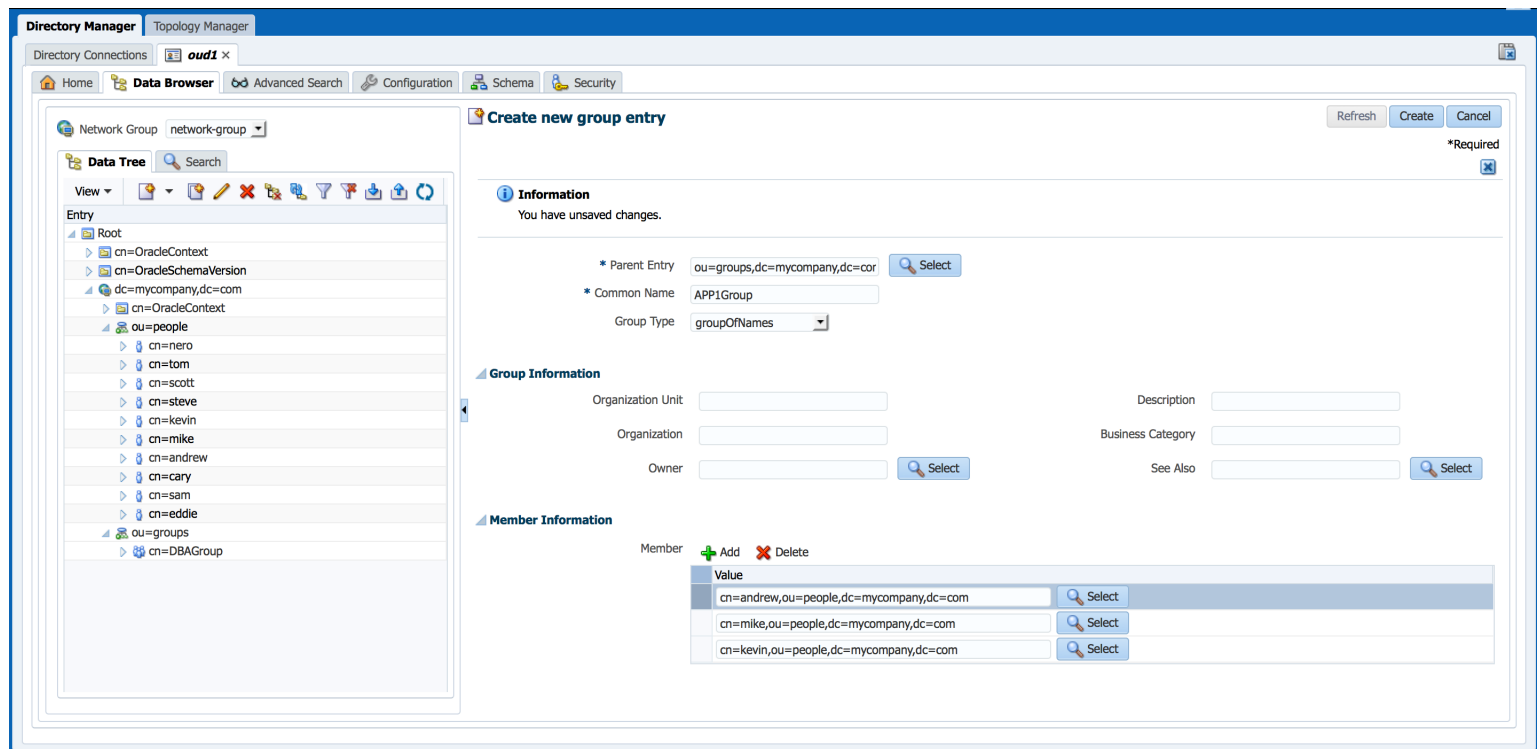
The screenshot shows the Oracle Directory Manager interface. On the left, the 'Data Tree' pane displays a hierarchy under 'network-group' with entries like 'cn=OracleContext', 'dc=mycompany,dc=com', 'ou=people', and 'ou=groups'. The 'ou=people' entry is selected. The main pane is titled 'Create new User entry' and contains several sections: 'Information' (Parent Entry: ou=people,dc=mycompany,dc=com), 'Basic User Information' (Common Name: Tom, User Name: tom, First Name: Tom, Last Name: Red), and 'Organizational Information' (Department Number, Description, Employee Number, etc.). The 'User Password' field is masked with dots. A user profile icon is visible on the right side of the form.

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

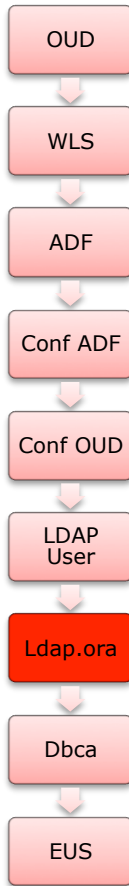
Martin Decker

-> Data Browser

-> Create Group Entry -> Static Group



Configuration:



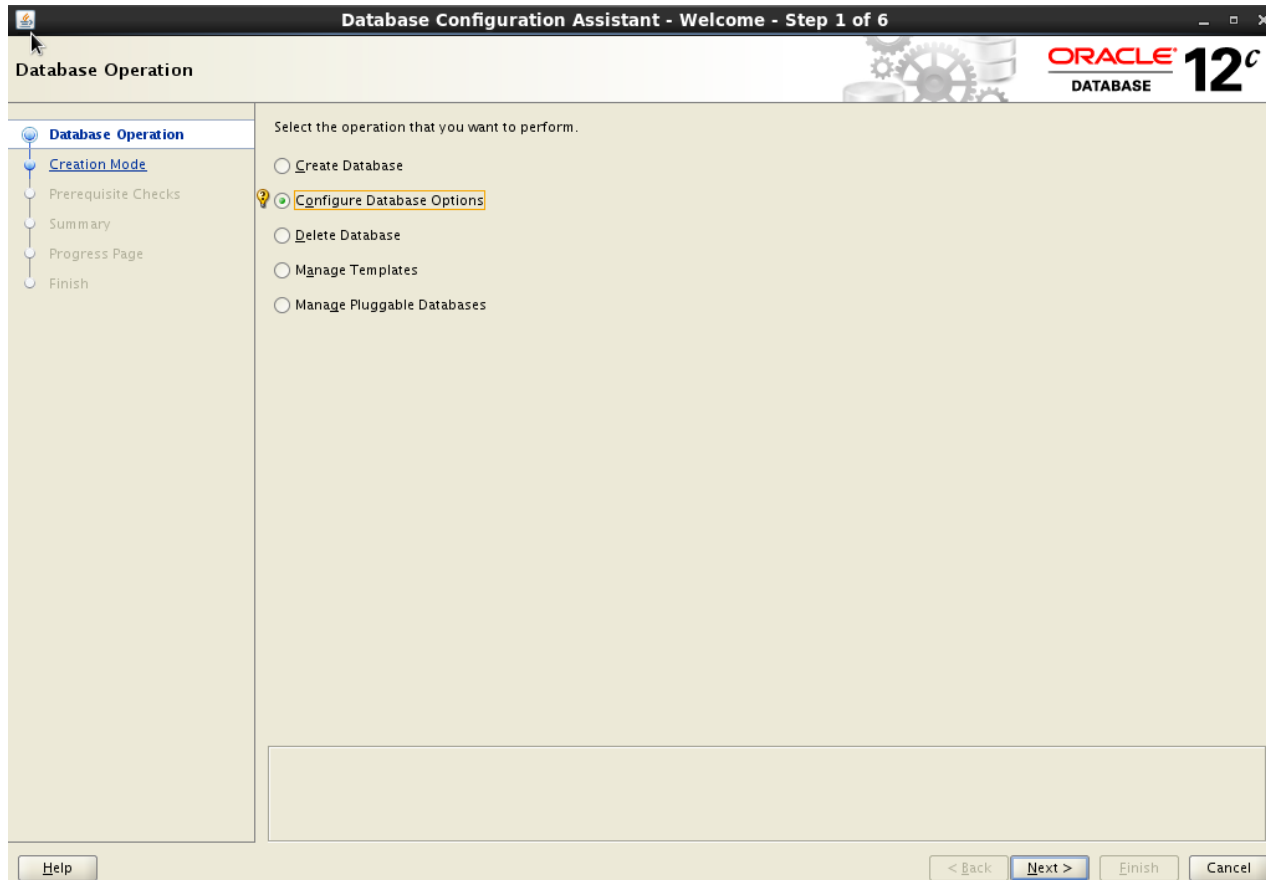
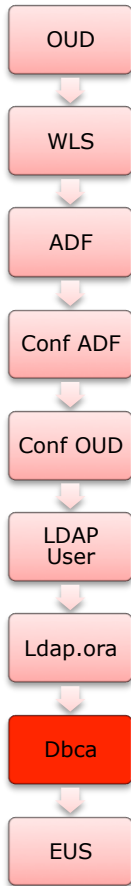
ldap.ora

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

Optional: sqlnet.ora:

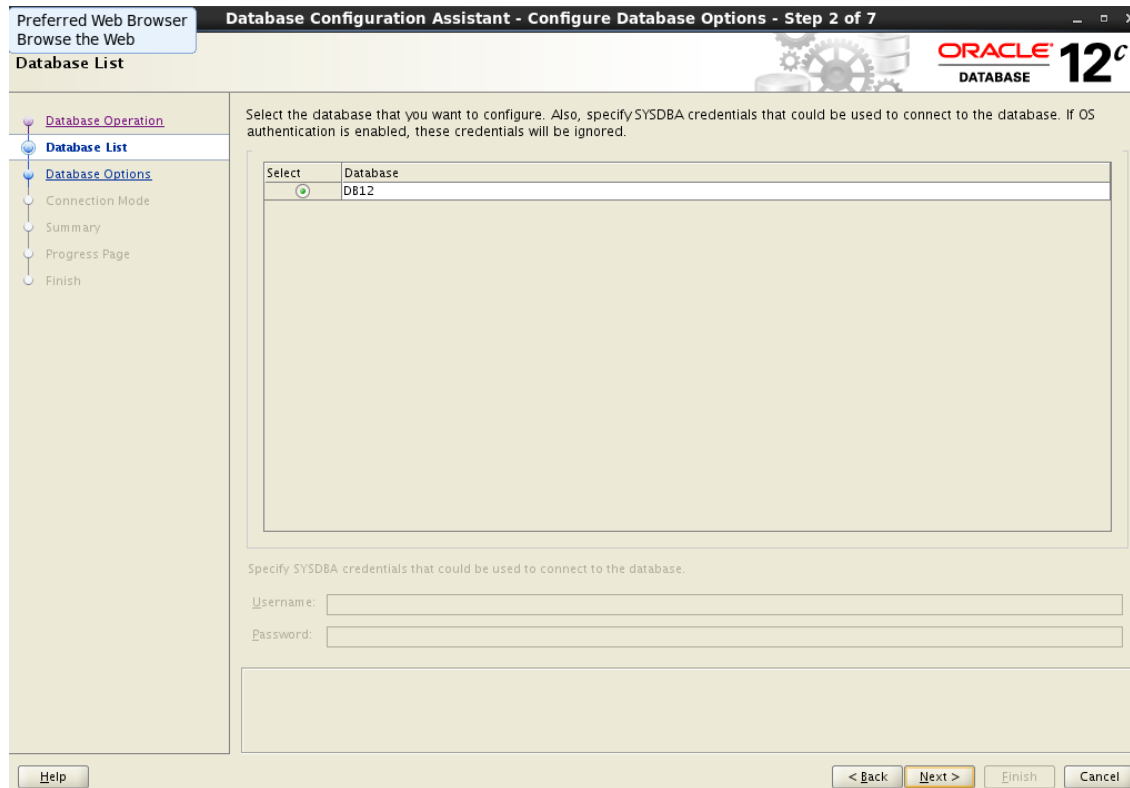
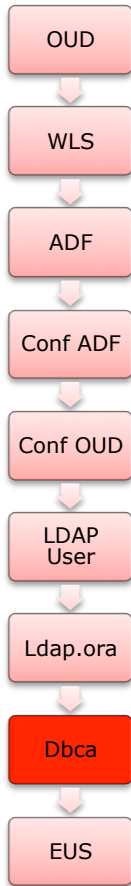
```
NAMES.DIRECTORY_PATH= (LDAP, TNSNAMES)
```

DBCA: register Database in directory (GUI)



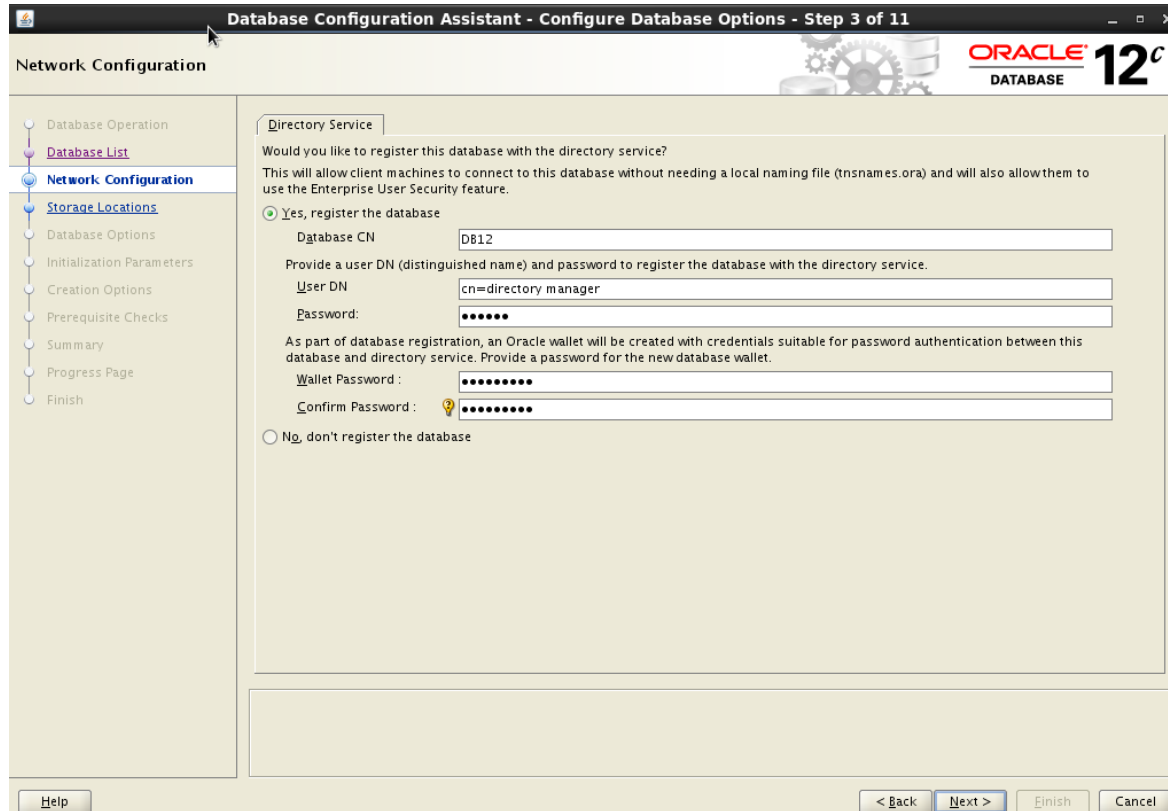
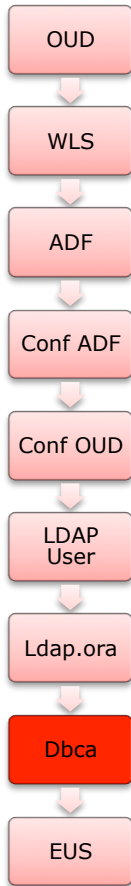
ACHTUNG: dbca silent funktioniert nicht, wegen Whitespace in „cn=directory manager“

DBCA: register Database in directory (GUI)



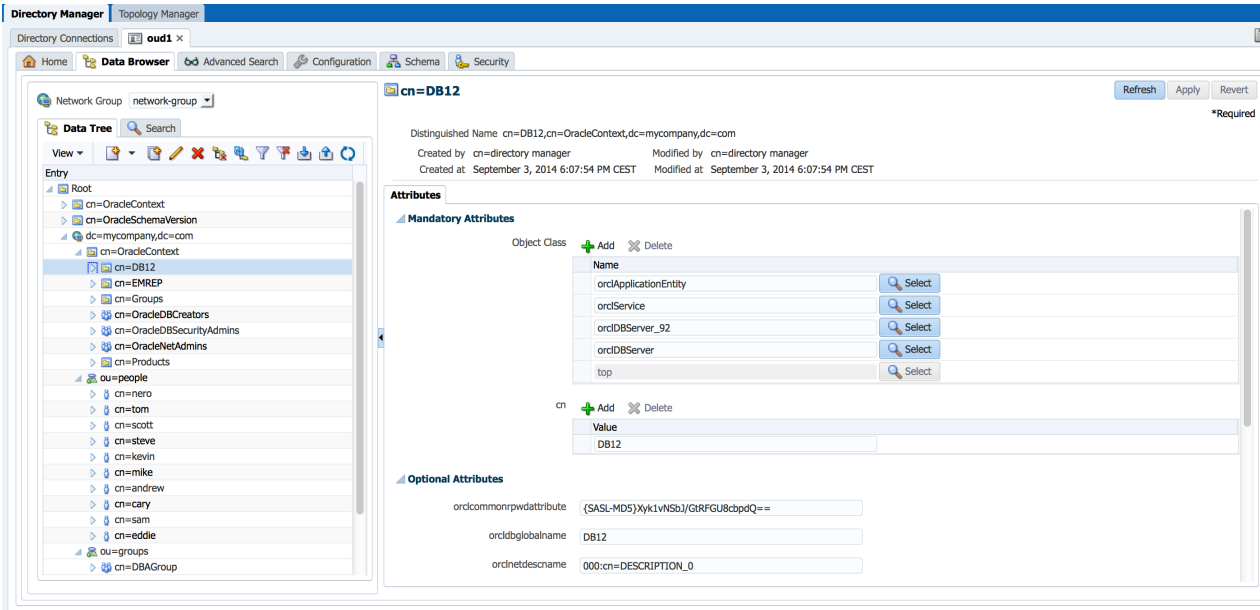
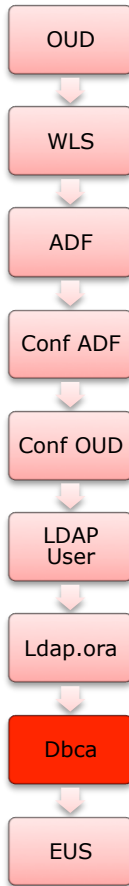
ACHTUNG: dbca silent funktioniert nicht, wegen Whitespace in „cn=directory manager“

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.

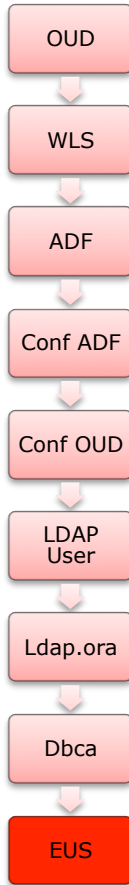
Used parameter files:

```
/u01/app/oracle/product/12.1.0.2/dbhome_1/network/admin/sqlnet.ora
```

Used LDAP adapter to resolve the alias

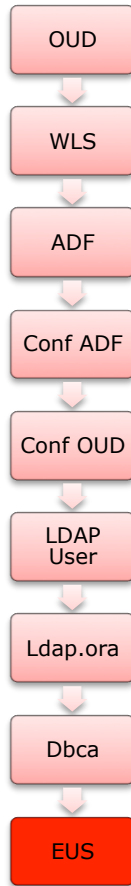
```
Attempting to contact (DESCRIPTION=(ADDRESS=(PROTOCOL=TCP) (HOST=db12oel6.intra) (PORT=1521))
(CONNECT_DATA=(SERVICE_NAME=DB12)))
OK (10 msec)
```

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

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

Oracle Enterprise Manager Cloud Control 12c

Enterprise Targets Favorites History Search Target Name

DB12 Oracle Database Performance Availability Security Schema Administration

Oracle Internet Directory Login: Enter Oracle Internet Directory credentials.

Enter Oracle Internet Directory credentials.

Information
Unable to locate the ldap.ora file. Please provide the file path.

* Host
* Port
* Realm
Example: dc=us,dc=com
* User
Example: cn=orcladm
* Password

Home
Reports
Users
Roles
Profiles
Audit Settings
Enterprise Data Governance
Application Data Models
Configuration Compliance
Data Masking
Data Redaction
Transparent Data Encryption
Database Vault
Privilege Analysis
Label Security
Virtual Private Database
Application Contexts
Enterprise User Security

Cancel Login

Cancel Login

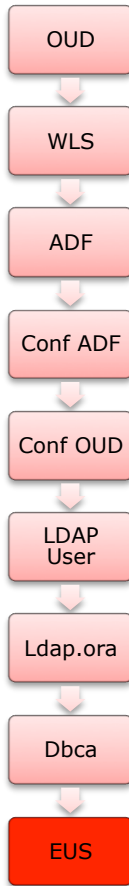
LDAP User

Ldap.ora

Dbca

EUS

EUS: Configuration



ORACLE Enterprise Manager Cloud Control 12c

Setup | SYSMAN

Enterprise Targets Favorites History Search Target Name

DB12

Logged in as sys db12oel6.intra

Oracle Database Performance Availability Security Schema Administration

Oracle Internet Directory Login: Enterprise User Security

Enter Oracle Internet Directory credentials.

Cancel Login

Information

Unable to locate the ldap.ora file. Please provide the ldap details.

* Host

* Port

* Realm

Example: dc=us,dc=oracle,dc=com

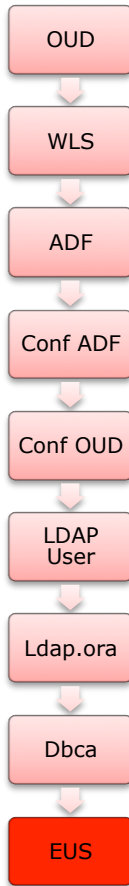
* User

Example: cn=orcladmin,cn=Users,dc=us,dc=oracle,dc=com

* Password

Cancel Login

EUS: Configuration



The screenshot displays the Oracle Enterprise Manager Cloud Control 12c interface. The top navigation bar includes 'Setup', 'SYSMAN', and a search bar. The main content area is titled 'Enterprise User Security' and provides an overview of the feature. The interface is logged in as 'sys' for the target 'db12oel6.intra'.

Oracle Enterprise Manager Cloud Control 12c

Setup | SYSMAN

Enterprise Targets Favorites History Search Target Name

DB12

Oracle Database Performance Availability Security Schema Administration

Oracle Internet Directory Login >

Enterprise User Security

Logged In As directory manager Logout Of OID

Overview

Enterprise User Security is a security feature in the database that enables centralized user management for the Oracle Database using the Oracle Internet Directory, an LDAP v3 compliant directory and a component of Oracle Identity Management.

Database users stored in the directory are known to the database as being identified externally. When a user authenticates to the database, the database will communicate with the Oracle Internet Directory to verify the users credentials and authorizations.

Database users authenticating to the Oracle database can be associated with a corresponding individual user account or a shared schema. Using a shared schema reduces the number of schemas in the database because thousands of database users managed in the directory can be mapped to a single shared schema. Enterprise User Security enables a single location for managing user access to databases across the entire enterprise.

Create and configure an enterprise domains. At least one enterprise domain is required before user schema mappings and additional settings can be managed. A domain can contain one or more databases.
[Manage Enterprise Domains](#)

Create and manage user-schema mappings between enterprise users stored in the directory and a specific database.
[Manage Databases](#)

Manage user schema mapping for individual enterprise users. Optionally manage enterprise roles, proxy permissions and label security authorizations.
[Manage Enterprise Users](#)

Manage User defined Enterprise Groups allows to grant access privileges to enterprise groups.
[Manage User Defined Enterprise Groups](#)

OID Realm Administration allows to manage various Realm Administrative groups.
[OID Realm Administration](#)

EUS: Configuration - Target DB

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

Configure Domain : OracleDefaultDomain

Logged In As directory manager Logout Of OID

Cancel OK

Databases User - Schema Mappings Enterprise Roles Proxy Permissions Configuration Administrators

List the databases which are members of the domain.

Selection Mode Single Add

View Remove

Select	Name
☒	DB12
☐	EMREP

Cancel OK

EUS: Configuration – User Schema Mapping

OAD

WLS

ADF

Conf ADF

Conf OUD

LDAP User

Ldap.ora

Dbca

EUS

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

Logged In As directory manager Logout Of OID

Configure Domain : OracleDefaultDomain

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

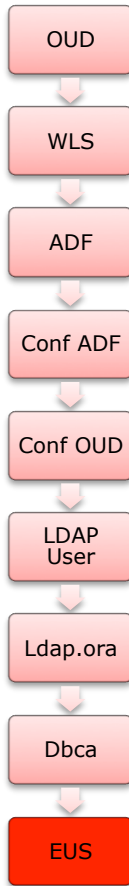
Select	From Enterprise User(s)	Mapping Type	To Schema
☒	tom	USER	GU_DBA
☐	bob	USER	GU_DBA
☐	steve	USER	GU_DBA
☐	nero	USER	EUS_DBA
☐	kevin	USER	GU_APP1
☐	mike	USER	GU_APP1
☐	andrew	USER	GU_APP1
☐	cary	USER	GU_APP2
☐	sam	USER	GU_APP2
☐	eddie	USER	GU_APP2

Edit Delete

Cancel OK

Cancel OK

EUS: Configuration – Enterprise Role



Configure Domain : OracleDefaultDomain

Cancel OK

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

An enterprise domain contains zero or more enterprise roles, which are containers of zero or more database global roles. Enterprise roles may be granted to enterprise users and groups. At database login, the global roles in granted enterprise roles are enabled for an enterprise user. List the enterprise roles for which are present for the domain

Selection Mode Single Create

View Edit Delete

Select	Name	Users	Groups	DB Global Roles
☒	ER_DBA	0	1	2

Edit Enterprise Role : ER_DBA

Cancel Continue

An enterprise domain contains zero or more enterprise roles, which are containers of zero or more database global roles. Enterprise roles may be granted to enterprise users and groups. At database login, the global roles in granted enterprise roles are enabled for an enterprise user. List the enterprise roles for which are present for the domain

DB Global Roles Grantees

Global roles are special roles that can be granted to enterprise roles. Global roles can be added only from the databases, which are part of the domain.

Add

Remove

Select All | Select None

Select	Name	Database
☐	GR_DBA	DB12
☐	GR_DBA	EMREP

Edit Enterprise Role : ER_DBA

Cancel Continue

An enterprise domain contains zero or more enterprise roles, which are containers of zero or more database global roles. Enterprise roles may be granted to enterprise users and groups. At database login, the global roles in granted enterprise roles are enabled for an enterprise user. List the enterprise roles for which are present for the domain

DB Global Roles Grantees

Upon database login, grantees will receive all privileges contained in the included global roles that apply to that database. Grantees can include any combination of users and user groups

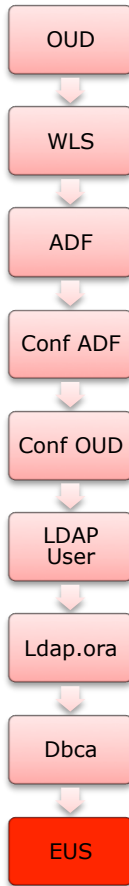
Add

Remove

Select All | Select None

Select	Name	Type
☐	DBAGroup	GROUP

EUS: Configuration – Proxy Permissions



Configure Domain : OracleDefaultDomain

Cancel OK

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

Proxy permissions grant a user the ability to proxy to another database account after successful authentication. The scope of a proxy permission is restricted to a single domain.

Selection Mode Create

View Edit Delete

Select	Name	Users	Groups	Target DB Users
☒	PP_APP1	3	0	1
☐	PP_APP2	0	1	1

Edit Proxy Permission : PP_APP1

Cancel Continue

Proxy permission allow an enterprise user to connect to a target database as an enterprise user.

Target DB Users Grantees

These are target database users that grantees are permitted to proxy to. Target DB users can be added only from the databases, which are part of the domain.

Add

Remove

Select All | Select None

Select	Name	Database
☐	APP1	DB12

Edit Proxy Permission : PP_APP1

Cancel Continue

Proxy permission allow an enterprise user to connect to a target database as an enterprise user.

Target DB Users Grantees

A proxy permission can be granted to any combination of users and groups

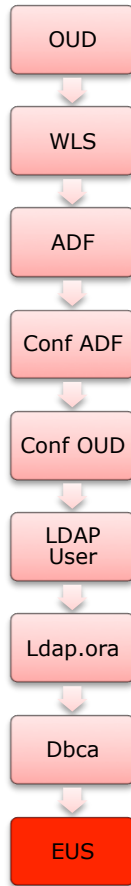
Add

Remove

Select All | Select None

Select	Name	Type
☐	List the enterprise users and groups	USER
☐	andrew	USER
☐	kevin	USER
☐	mike	USER

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
```

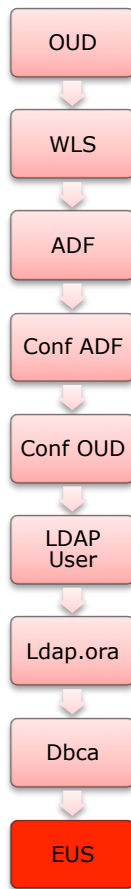
25 rows selected.

```
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: 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
  
```

- ❑ 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 11g Release 1 (11.1.1)**
http://docs.oracle.com/cd/E28280_01/admin.1111/e10046/toc.htm

- ❑ 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/>