

EUS mit Oracle Unified Directory

Ein Überblick


Stefan Oehrli

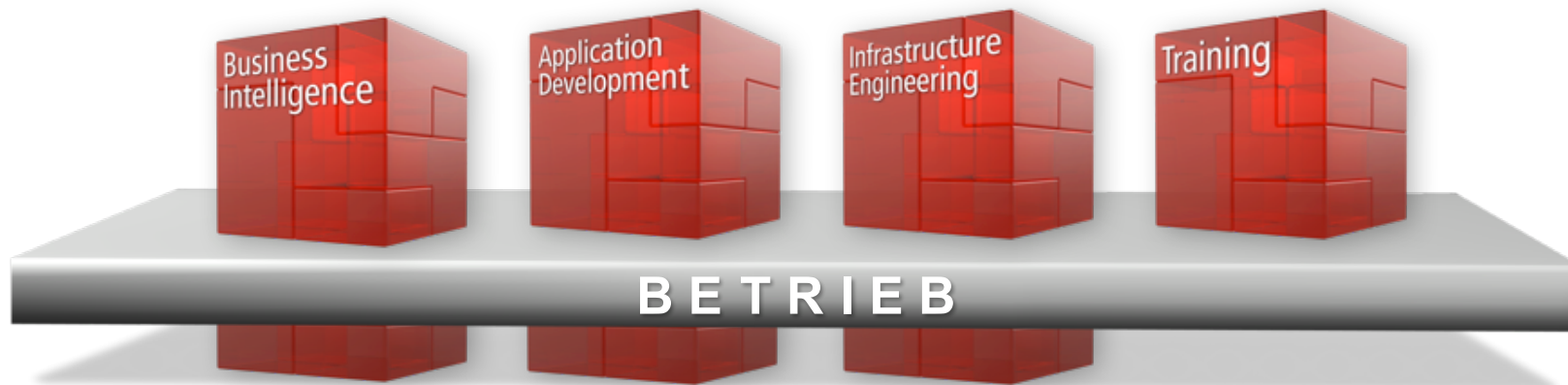


BASEL ▪ BERN ▪ BRUGG ▪ DÜSSELDORF ▪ FRANKFURT A.M. ▪ FREIBURG I.BR. ▪ GENÈVE
HAMBURG ▪ KOPENHAGEN ▪ LAUSANNE ▪ MÜNCHEN ▪ STUTTGART ▪ WIEN ▪ ZÜRICH

trivadis
makes IT easier. ■ ■ ■

■ Unser Unternehmen.

Trivadis ist **führend bei der IT-Beratung, der Systemintegration, dem Solution Engineering** und der Erbringung von **IT-Services** mit Fokussierung auf **ORACLE®** - und  **Microsoft** -Technologien in der Schweiz, Deutschland, Österreich und Dänemark. Trivadis erbringt ihre Leistungen aus den strategischen Geschäftsfeldern:



Trivadis Services übernimmt den korrespondierenden Betrieb Ihrer IT Systeme.

■ Mit über 600 IT- und Fachexperten bei Ihnen vor Ort.



- 14 Trivadis Niederlassungen mit über 600 Mitarbeitenden.
- Über 200 Service Level Agreements.
- Mehr als 4'000 Trainingsteilnehmer.
- Forschungs- und Entwicklungsbudget: CHF 5.0 Mio.
- Finanziell unabhängig und nachhaltig profitabel.
- Erfahrung aus mehr als 1'900 Projekten pro Jahr bei über 800 Kunden.

trivadis
makes IT easier. ■ ■ ■

Technik allein bringt Sie nicht weiter. Man muss wissen, wie man sie richtig nutzt.



■ Stefan Oehrli



Solution Manager BDS SEC

- Seit 1997 IT-Bereich tätig
- Seit 2008 bei der Trivadis AG
- Seit 2010 Disziplin Manager SEC INFR
- Seit 2014 Solution Manager BDS Security

IT Erfahrung

- DB Administration und DB Security Lösungen
- Administration komplexer, heterogenen Umgebungen
- Datenbank Teamleiter

Spezialgebiet

- Datenbank Sicherheit Security und Betrieb
- Security Konzepte
- Security Reviews
- Oracle Backup & Recovery

Skills

- Backup & Recovery
- Oracle Advanced Security
- Oracle AVDF und DB Vault
- Oracle Directory Services
- Team / Projekt Management

■ Agenda

1. Enterprise User Security in a Nutshell
2. Überblick über Oracle Unified Directory
3. Aufbau der Infrastruktur
4. Konfiguration von OUD, AD, DB und EUS
5. Fallstricke und Problembehandlung
6. Schlussfolgerungen

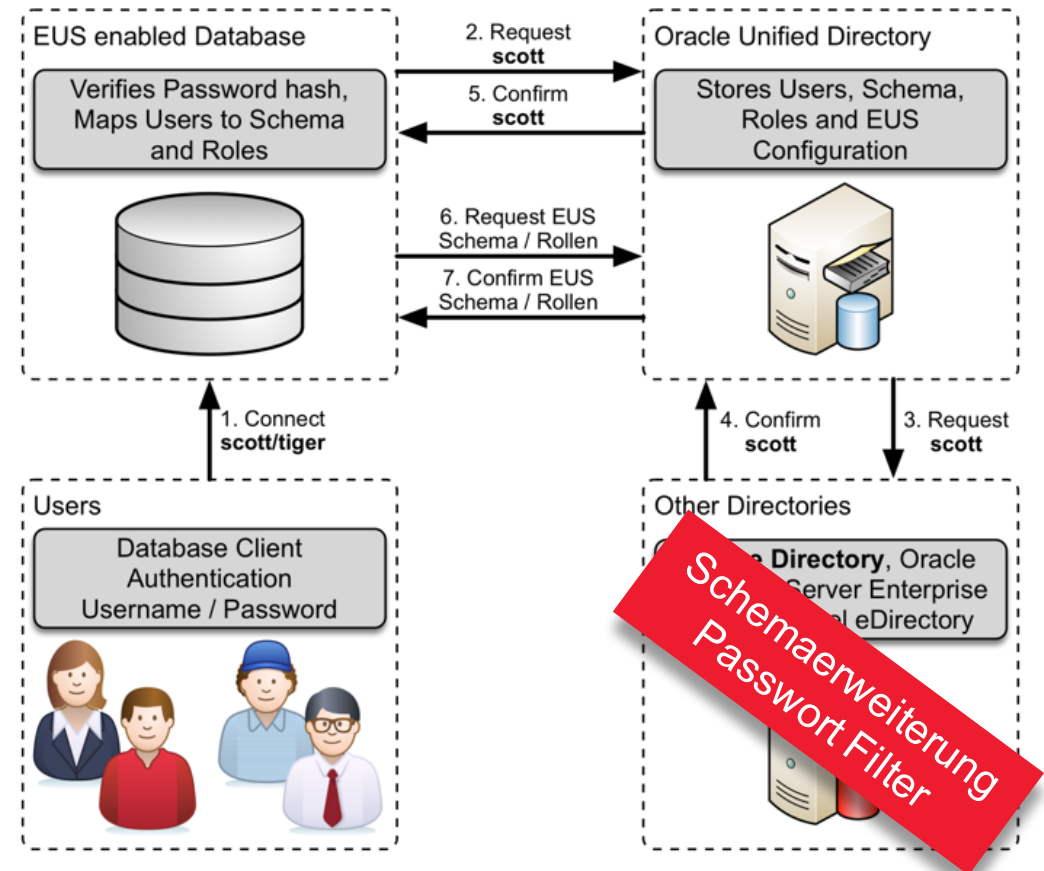
Enterprise User Security in a Nutshell

■ Enterprise User Security

- Zentrales Verzeichnis der Datenbanken, Benutzer und Berechtigungen
 - LDAP-kompatibles Verzeichnis
- Vereinfachte Administration durch Zentralisierung
 - Ein Ort zum Verwalten der Benutzern, Gruppen, Rollen und Berechtigungen. D.h. Änderung des Aufgabenbereichs von Benutzer X erfordert nur eine Anpassung der Benutzerrolle im Verzeichnis
 - Single point of authentication
- Oracle Database Enterprise Edition Feature
 - Zusätzliche Lizenz für das Oracle Verzeichnis ist erforderlich

■ Enterprise User Security – Verzeichnisse

- Unterstützte Verzeichnisse für die EUS-Implementierungen
 - **Oracle Internet Directory (OID)**
 - **Oracle Unified Directory (OUD)**
 - *Oracle Virtual Directory (OVD)*
- Integration bestehender Verzeichnisse durch DIP, Proxys, Virtualisierung etc.
 - Microsoft Active Directory
 - Novell eDirectory
 - Oracle Server Enterprise Edition



■ Enterprise User Security – Authentifizierungsmethoden

■ Password Authentifizierung

- Benutzer behält aktuelle Authentifizierungsmethode
- Erfordert die gesonderte Authentifizierung für jede Datenbankverbindung
- Oracle Password Filter DLL für Active Directory

■ SSL Authentifizierung

- Starke Authentifizierung über SSL
- Unterstützt SSO mit SSL erfordert dafür eine PKI Infrastruktur

■ Kerberos Authentifizierung

- Starke Authentifizierung durch Kerberos Tickets (Version 5)
- Unterstützt SSO mit Kerberos

■ Enterprise User Security – Database Schemas

■ Globales privates Schema

- 1:1 Schema Zuweisung im Verzeichnis
- Jeder Benutzer hat sein eigenes Schema in der Datenbank

```
CREATE USER soe IDENTIFIED GLOBALLY AS 'cn=soe,cn=Users,dc=tvb,dc=ch
```

■ Globales Shared Schema

- Gemeinsames Schema in der Datenbank
- Verzeichnis Benutzer werden einem globalen shared Schema zugewiesen

```
CREATE USER employees IDENTIFIED GLOBALLY;
```

Überblick über Oracle Unified Directory

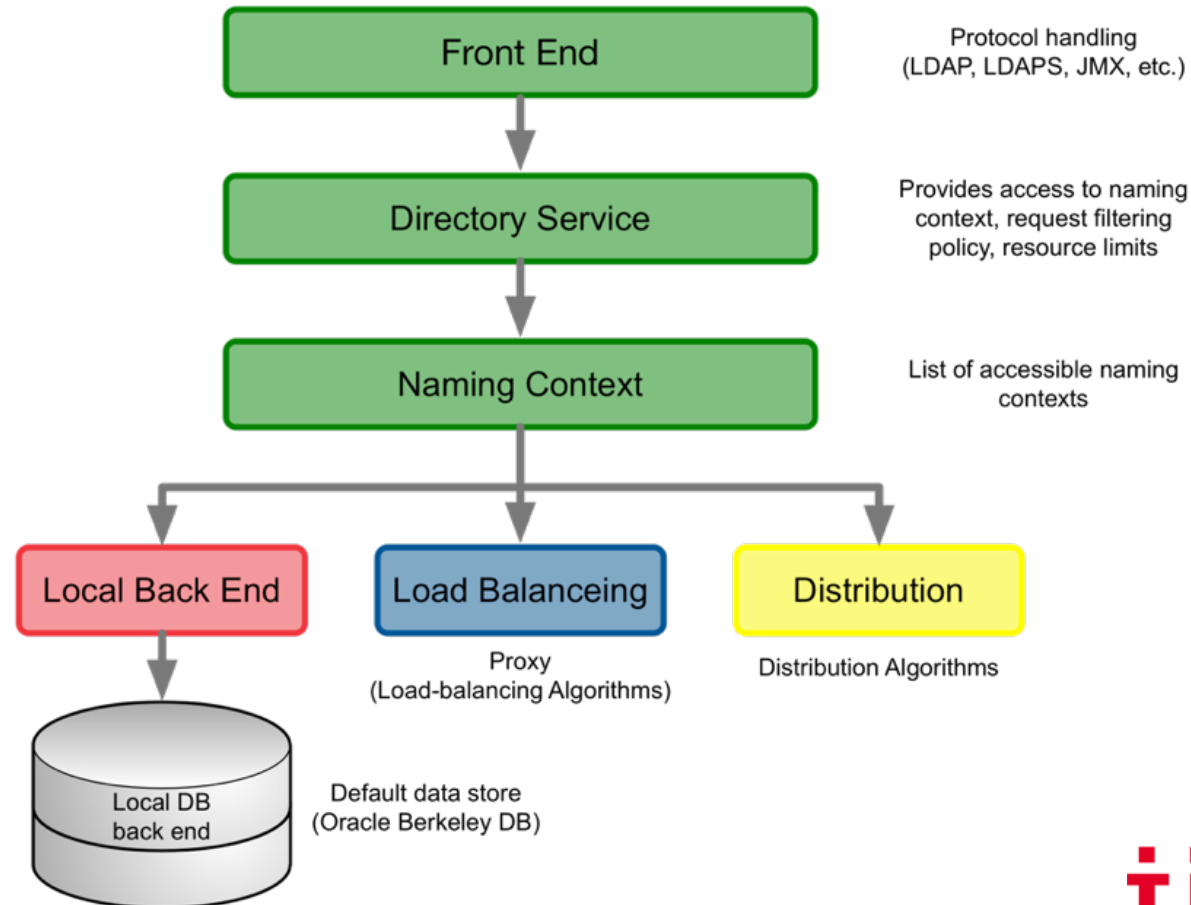
■ Oracle Unified Directory

- Das Andere Oracle Directory ...☺
- OUD ist das neuste der drei Oracle LDAP Verzeichnisse und basiert auf OpenDS
 - Voll LDAPv3 konformer Verzeichnis Server
 - Proxy Server e.g. Integration von OUD und MS Active Directory
 - Replication Server
- Java basiertes Verzeichnis
 - in Java und dadurch Unterstützung für verschiedene Plattformen
- Performant sowie effiziente Datenspeicherung
 - Embedded Berkley DB

■ Oracle Unified Directory

- Horizontale Skalierung im Vergleich zu monolithischen Skalierbarkeit für OID
 - hinzufügen von weiteren Instanzen mit add more instances mit Datenpartition und globalen Indizes für Performance und Skalierbarkeit auf Standard-Hardware
- Oracle Unified Directory ist Teil der Oracle Directory Service Plus Lizenz
 - **ODU** Oracle Unified Directory
 - **ODSEE** Oracle Directory Server Enterprise Edition (formerly Sun Directory Server Enterprise Edition)
 - **OID** Oracle Internet Directory
 - **OVD** Oracle Virtual Directory

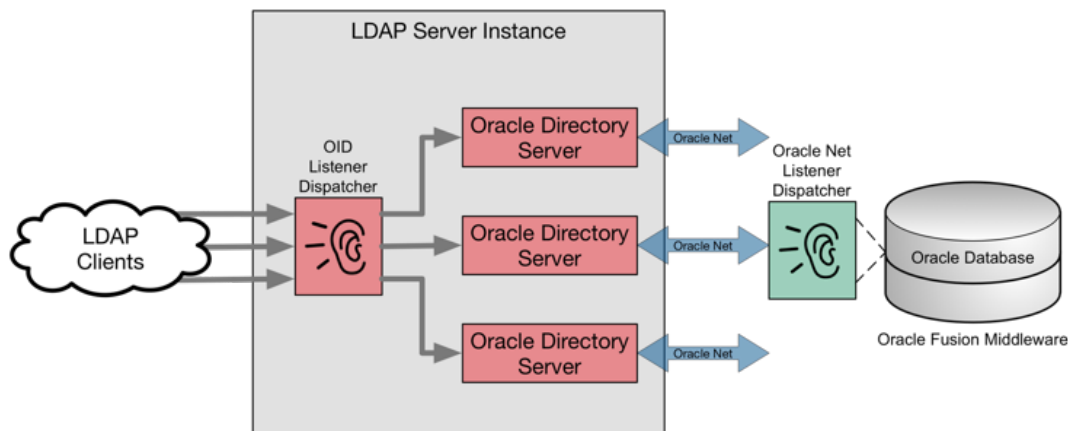
■ OUD Architecture



■ OUD und OID, die Unterschiede...

OID

- Vertikale Skalierbarkeit
- Benötigt eine Oracle Datenbank
- Teilweise in PL/SQL, Java und C
- Lizenzfrei für Oracle Names



OUD

- Keine separate Datenbank
 - Installation, nur der OUD Binaries
 - Einfache Dimensionierung
- Horizontale und Vertikale Skalierbarkeit
- All-Java Solution
- Berkeley Java DB zur Datenspeicherung
- Benötigt immer die Oracle Directory Server Plus Lizenz

■ OUD Best Practice

■ Dimensionierung abhängig vom Anwendungsfall und der Verzeichnisdaten

- Dedizierter Sizing Guide für OUD Servers mit +5Mio Einträge

■ Mehrere CPU's bei hoher Last wird empfohlen

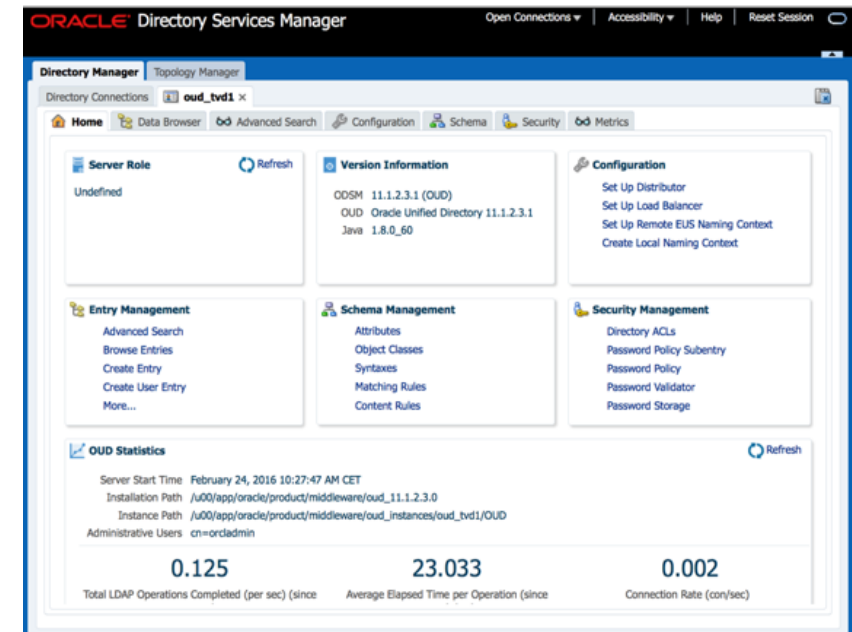
■ Installation nach OFA Standard

- Middleware Home / OUD Binaries
- OUD Instance Home, nicht nur AINST1

■ ODSM zur Überwachung und Administration

- Benötigt WLS Installation

■ Überwachung mit **cn=Monitor** oder OEM Plug-In



Aufbau der Infrastruktur

■ Aufbau der Infrastruktur – Software

- System Anforderungen *Oracle Fusion Middleware Supported System Configurations*
<http://www.oracle.com/technetwork/middleware/ias/downloads/fusion-certification-100350.html>
- Bezug der Software von OTN
 - Oracle Unified Directory 11g Release 2 (11.1.2.3.0)
 - Oracle WebLogic Server 11g Release 1 (10.3.6)
 - Oracle Application Development Framework 11g Release 1 (11.1.1.9.0)
 - Aktuelle PSU's für OUD und WLS
- Installation mit GUI oder CLI und Response Dateien
- Test Installation auf einer Virtualbox mit 256M für die OUD Instanz

■ Aufbau der Infrastruktur – Installation Verzeichnisse

Umgebungsvariablen	Verzeichnisse
ORACLE_BASE	/u00/app/oracle
MIDDLEWARE_BASE	\$ORACLE_BASE/product/middleware
JAVA_BASE	\$ORACLE_BASE/product/java
JAVA_HOME	\$JAVA_BASE/jdk1.7.0_79
OUT_ORACLE_HOME	\$MIDDLEWARE_BASE/oud_11.1.2.3.0
INSTANCE_NAME	oud_instances/oud_eus_ad
ORACLE_HOME	\$MIDDLEWARE_BASE/\$INSTANCE_NAME/OUT

■ Aufbau der Infrastruktur – Installation

- Follow OUD Dokumentation
 - [Installing Oracle Unified Directory](#)
- Java Installation
 - Dediziertes Java für OUD
- OUD Software Installation

```
runInstaller -jreLoc $JAVA_HOME
```

- Installation des aktuellen OUD PSU 22675286 vom April 2016

■ Aufbau der Infrastruktur – Installation ODSM

■ Weblogic Installation

```
java -d64 -Xmx1024M -jar wls1036_generic.jar
```

■ Installation des aktuellen WLS PSU 22505423 vom April 2016

■ ADF Installation

```
runInstaller -jreLoc $JAVA_HOME
```

■ ODSM Configuration

```
$MIDDLEWARE_BASE/oracle_common/common/bin/config.sh
```

Konfiguration von OUD, AD, DB und EUS

■ Konfiguration – Active Directory (1)

- Schemaerweiterung für das Password Filter Plugin (OIDPWDCN.DLL)

```
cd $OUD_ORACLE_HOME/config/EUS/ActiveDirectory  
$JAVA_HOME/bin/java ExtendAD -h <AD Server> -D <AD Admin> \  
-w <PWD> -AD "dc=postgasse,dc=org" -commonattr
```

- Kopieren des Password Filter Plugin auf dem AD Server
- Anpassen der Registry mit Regedit und Neustart von Active Directory

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Notification
```


■ Konfiguration – Active Directory (2)

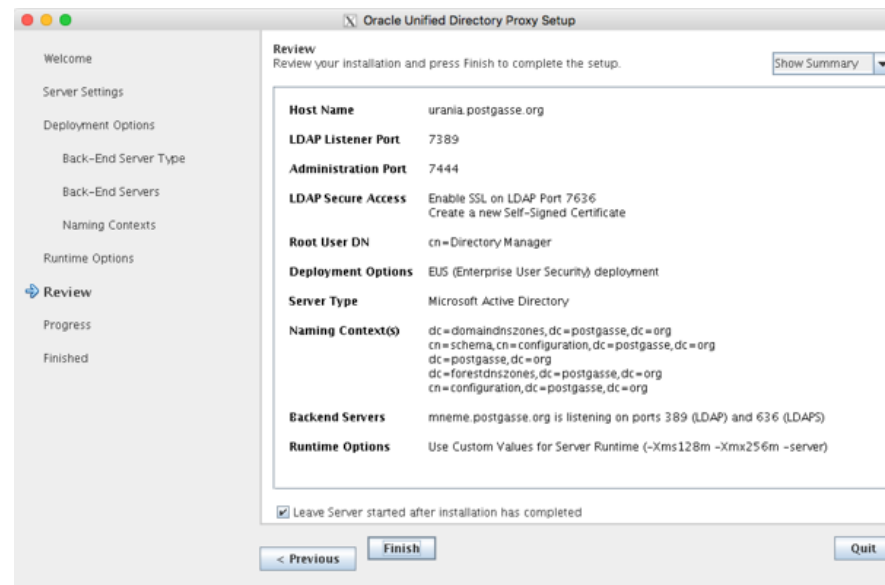
- Anonymous Bind auf dem Active Directory Server zulassen
- Passwort eines AD Benutzers ändern und mit LDAP Search Plug-In prüfen

```
ldapsearch -h <AD Server> -D <AD User> -w <PWD> \  
-b cn=users,dc=postgasse,dc=org "cn=Stefan Oehrli" orclCommonAttribute  
dn: CN=Stefan Oehrli,CN=Users,DC=postgasse,DC=org  
orclCommonAttribute: {SHA}opzeovd4xPkv8sUADE11XnvmUfQ=
```

■ Konfiguration – OUD Proxy Setup

■ Erstellen des OUD AD Proxys

```
export INSTANCE_NAME=oud_instances/oud_eus_ad  
$OUD_ORACLE_HOME/oud-proxy-setup
```



■ Konfiguration – OUD Workflow Elemente

■ Erstellen eines Workflow Elementes für den Zugriff auf AD

```
dsconfig set-workflow-element-prop --element-name proxy-we1 \  
--set remote-root-dn:cn=oudproxy,cn=users,dc=postgasse,dc=org -j ./pwd.txt \  
--set remote-root-password:<PWD> -h <OUD Host> -p 7444 -D <OUD Admin> -X -n
```

■ Erstellen von Exclude Regeln im Workflow

```
dsconfig set-workflow-element-prop --element-name proxy-we1 -h <OUD Host> -p 7444 \  
--add exclude-list:cn=<OUD Admin> -D <OUD Admin> \  
--add exclude-list:cn=oraclecontext,dc=postgasse,dc=org \  
--set remote-ldap-server-bind-dn:cn=oudproxy,cn=users,dc=postgasse,dc=org \  
--set remote-ldap-server-bind-password:TVD04manager -j ./pwd.txt -X -n \
```

■ Zusätzliches Storage Schema mit einem reversiblen Algorithmus z.B AES

■ Konfiguration – Datenbank (1)

- Festlegen des LDAP Verzeichnisse mit **netca** oder direkt in `ldap.ora`

```
DIRECTORY_SERVERS=urania.postgasse.org:7389:7636  
DEFAULT_ADMIN_CONTEXT = "dc=postgasse,dc=org"  
DIRECTORY_SERVER_TYPE = OID
```

- Registrierung der Datenbank im Verzeichnis mit **dbca** (CLI oder GUI)

- Kann zu Problemen mit nicht Standard Listener Ports führen

- Anpassen der Initialisierungsparameter durch **dbca**

```
ldap_directory_access      string      PASSWORD  
ldap_directory_sysauth     string      NO
```

■ Konfiguration – Datenbank (2)

■ Oracle Wallet für die LDAP Credentials

- **dbca** erstellt ein ein neues Oracle Wallet unter **WALLET_LOCATION**
- **WALLET_LOCATION** wird bei Container Datenbanken nicht unterstützt

```
WALLET_LOCATION =  
(SOURCE =  
  (METHOD = File)  
  (METHOD_DATA = (DIRECTORY = /u00/app/oracle/admin/$ORACLE_SID/wallet)))
```

■ Konfiguration – Enterprise User Security (1)

■ Erstellen eines globalen Benutzers oder Schemas IDENTIFIED GLOBALLY

```
ALTER USER clark IDENTIFIED GLOBALLY  
    AS 'cn=clark,cn=Users,dc=postgasse,dc=org' ;  
CREATE USER employee IDENTIFIED GLOBALLY;
```

■ Festlegen des Schema / Rollen Mapping für EUS

- Enterprise Manager Cloud Control
- **eusm** command line utility MOS Note [1085065.1](#)

■ Konfiguration – Enterprise User Security (2)

■ Mapping zu einem **global shared Schema**

```
eusm createMapping database_name="TDB11A" realm_dn="dc=postgasse,dc=org" \  
  map_type="SUBTREE" map_dn="CN=Users,dc=postgasse,dc=org" \  
  schema="eus_user" ldap_host=<OUD Host> ldap_port=7389 \  
  ldap_user_dn=<OUD Admin> ldap_user_password=<PWD>
```

■ Erstellen einer Enterprise Rolle

```
eusm createRole enterprise_role="Employees" \  
  domain_name="OracleDefaultDomain" realm_dn="dc=postgasse,dc=org" \  
  ldap_host=<OUD Host> ldap_port=7389 \  
  ldap_user_dn=<OUD Admin> ldap_user_password=<PWD>
```

■ Konfiguration – Enterprise User Security (3)

■ Enterprise Rolle einer globale Rolle zuweisen

```
eusm addGlobalRole enterprise_role="Employees" ldap_host=<OUD Host> \  
  ldap_port=7389 domain_name="OracleDefaultDomain" \  
  realm_dn="dc=postgasse,dc=org" database_name="TDB11A" \  
  global_role="employees" dbuser="system" dbuser_password="manager" \  
  dbconnect_string="urania:1521:$ORACLE_SID" \  
  ldap_user_dn=<OUD Admin> ldap_user_password=<PWD>
```

■ Erstellen einer Enterprise Rolle

```
eusm createRole enterprise_role="Employees" ldap_user_dn=<OUD Admin> \  
  domain_name="OracleDefaultDomain" realm_dn="dc=postgasse,dc=org" \  
  ldap_host=<OUD Host> ldap_port=7389 ldap_user_password=<PWD>
```


■ Konfiguration – Enterprise User Security (4)

■ Enterprise Rolle einem Benutzer zuweisen

```
eusm grantRole enterprise_role="Employees" \  
    domain_name="OracleDefaultDomain" realm_dn="dc=postgasse,dc=org" \  
    user_dn="CN=Stefan Oehrli,CN=Users,DC=postgasse,DC=org" \  
    ldap_host=<OUD Host> ldap_port=7389 \  
    ldap_user_dn=<OUD Admin> ldap_user_password=<PWD>
```

■ Weitere Informationen zu **eusm** in der MOS Note [1085065.1](#) oder vom CLI

```
eusm help <option>  
eusm <option> -help
```

■ Konfiguration – Benutzer

■ Information über EUS im **userenv** Context

- Funktion **sys_context**
- Trivadis TVD-BasEnv Script **sousrinf**
- MOS-Note [1447631.1](#) *How to get the name of Enterprise User in V\$SESSION?*

```
SELECT sys_context('userenv','enterprise_identity') FROM dual;
```

```
SYS_CONTEXT('USERENV','ENTERPRISE_IDENTITY')
```

```
-----
```

```
cn=Stefan Oehrli,cn=Users,dc=postgasse,dc=org
```

Fallstricke und Problembehandlung

■ Fallstricke und Problembehandlung (1)

- Security Vulnerabilitäten helfen nicht AD, EUS und OUD zu vereinfachen
- Bug 19285025 LDAP Client und **dbms_ldap**
 - Betrifft Clients, OUD und Datenbank
- Poodle SSL Vulnerability
 - MOS-Note [1935500.1](#) *SSL Poodle Vulnerability (CVE-2014-3566)*
 - MOS-Note [1950331.1](#) *CVE-2014-3566 Instructions to Mitigate the SSL v3.0 Vulnerability (aka "Poodle Attack") in Oracle Unified Directory*
 - MOS-Note [1938502.1](#) *CVE-2014-3566 Poodle Vulnerability and SSL_VERSION Parameter Setting*
- Anpassen von *orclCommonNicknameAttribute* (*uid* versus *samAccountName*)
 - MOS-Note [1570893.1](#) *Active Directory As External Directory Not Working For EUS*

■ Fallstricke und Problembehandlung (2)

■ eusm 12c funktioniert nicht mit OUD

- Bug 21435061 *Storage Schema for Password must be adjusted to support SASL*

■ SSL HANDSHAKE FAIL Fehler erfolgt bei ganz unterschiedlichen Problemen

- Falsches oder fehlendes Oracle Wallet, inkorrekte LDAP Credentials in Wallet

```
mkstore -wrl . -viewEntry ORACLE.SECURITY.DN -viewEntry ORACLE.SECURITY.PASSWORD
Oracle Secret Store Tool : Version 12.1.0.1
Copyright (c) 2004, 2012, Oracle and/or its affiliates. All rights reserved.

Enter wallet password: xxxxxx

ORACLE.SECURITY.DN = cn=TDB12B,cn=OracleContext,dc=trivadistraining,dc=com
ORACLE.SECURITY.PASSWORD = AEOnD@PvNBv0
```

■ Fallstricke und Problembehandlung (3)

■ Anmeldefehler mit ORA-01017 oder ORA-28030

- MOS-Note [783502.1](#) *EUS Authentication Fails With ORA-28030*

```
ALTER SYSTEM SET EVENTS '28033 trace name context forever, level 9';
```

- Fehlerhafte Anmeldung ausführen

```
ALTER SYSTEM SET EVENTS '28033 trace name context off';
```

■ EUS und OUD Troubleshooting Guides

- MOS-Note [191137.1](#) *Troubleshooting Enterprise User Security*
- MOS-Note [398524.1](#) *How to Debug Problems with Enterprise User Security*

■ OUD Log Dateien . . /OUD/logs/...

Schlussfolgerungen

■ Schlussfolgerungen

- EUS mit OUD ist einfacher als gedacht... 😊
- Simple Architektur und einfache Installation für Basiskonfigurationen
 - Keine zusätzliche Oracle Datenbank, nur OUD und WLS für ODSM
- Einfache AD Integration durch OUD Proxy
- Die grosse Herausforderung bleibt das Konzept für die Verzeichnisstruktur
 - Wo liegen die Benutzer, Gruppen, Rollen
- Einfachere Problemsuche als mit OID
- Security Problem im speziellen SSL benötigen je nach Version Patches und zusätzliche Konfigurationsschritte

Links und weitere Informationen



- MOS Note [1376365.1](#) Master Note For Enterprise User Security)
- MOS Note [1401023.1](#) Master Note for Oracle Unified Directory (OUD)
- MOS Note [1592446.1](#) Master Note for OUD-EUS integration
- OUD Documentation https://docs.oracle.com/cd/E52734_01/oud/docs.htm
- OUD Related Blog Posts <http://www.oradba.ch/category/oud/>

Gewinnspiel



Stefan Oehrli
Solution Manager / Trivadis Partner

Tel.: +41 58 459 55 55
stefan.oehrli@trivadis.com

<http://www.trivadis.com/security>
<http://www.oradba.ch>

