Technischer Artikel

Benutzerverwaltung mit EUS, OUD und MS AD

Stefan Oehrli
Solution Manager
31. Mai 2017

Sicherheit ist heutzutage eine der zentralen Herausforderungen für On-Premises und Cloud basierte Datenbanken. Mit der Umsetzung von Sicherheitskonzepten für Datenbanken werden diese Herausforderungen gemeistert. Doch viele dieser Bestrebungen sind nur sinnvoll, wenn bereits die Authentifizierung und Autorisierung mit entsprechender Sorgfalt umgesetzt werden. Anstelle der dezentralen Verwaltung der Benutzer, Rechte und Rollen in jeder Datenbank ist es übersichtlicher und vor allem sicherer, diese zentral zu verwalten. In diesem Artikel wird aufgezeigt, wie die Benutzerverwaltung mit Oracle Enterprise User Security und Oracle Unified Directory verwaltet und mit MS Active Directory integriert werden kann.

Ausgangslage für die zentrale Benutzerverwaltung

In der Regel wird für die Authentifizierung vom Oracle Datenbankbenutzer die lokale Authentifizierung in der Datenbank mit Benutzername und Password verwendet. Mit einem entsprechend sicheren Password ist diese Methode für viele Umgebungen weiterhin eine akzeptable Authentifizierungsmethode. Dies entspricht aber nicht mehr den aktuellen Sicherheitsempfehlungen. Je mehr Benutzer und Datenbanken vorhanden sind, desto unübersichtlicher und somit unsicherer wird die Benutzeradministration. Wo hat welcher Benutzer Zugriff? Wer hat wo welche Rechte? Werden bei Funktions- oder Rollenwechsel keine Rechte vergessen?

Viele dieser Fragen lassen sich bei einer dezentralen Benutzerverwaltung nicht einfach beantworten. Die verzeichnisbasierte Authentifizierung respektive Oracle Enterprise User Security (EUS) bietet hier eine alternative Methode zur Authentifizierung von Datenbankbenutzern. Im Gegensatz zur lokalen Datenbankauthentifizierung geht EUS über die reine Authentifizierung hinaus. In einem Oracle Verzeichnis können Benutzer, Gruppen und verschieden Rollen verwaltet werden; also auch ein Teil der Autorisierung. Die effektiven Objekte und System Privilegien werden dann in der jeweiligen Datenbank entsprechenden Schemas oder Rollen zugewiesen. Diese werden wiederum mit den Enterprise Usern oder Enterprise Rollen verknüpft. Der wesentliche Vorteil dieser Lösung ist die zentrale Verwaltung. Es gibt nur eine Stelle, wo Benutzer erstellt und Berechtigungen zugewiesen werden. So ist es z.B. nicht mehr nötig, dass der Datenbankadministrator in jeder seiner Datenbanken Benutzer anlegt oder löscht.

Oracle EUS setzt auf die Oracle Identity Management-Infrastruktur, welche wiederum einen LDAP kompatiblen Verzeichnisdienst verwendet, um Benutzer zentral zu speichern und zu verwalten. Dabei werden folgende Verzeichnisdienste unterstützt:

- **OID Oracle Internet Directory:** ein LDAP v3 konformes Verzeichnis. Es basiert auf einer Oracle Datenbank und ist vollständig in Oracle Fusion Middleware und Oracle Applikation integriert.
- **OUD Oracle Unified Directory:** ein Java basiertes Verzeichnis. Es ist eine all-in-one Lösung mit Storage, Proxy, Synchronisation- und Virtualisierungsfähigkeiten.

Die eigentliche Authentifizierung wird bei EUS je nach Konfiguration entweder durch Passwort, Kerberos oder SSL Authentifizierung gemacht. Die Benutzer profitieren dabei von Single Sign-On (SSO) oder Single Passwortauthentifizierung.

Trotz den Vorteilen einer zentralen Benutzerverwaltung wird bei vielen Unternehmen die Authentifizierung und Autorisierung weiterhin dezentral in den Oracle Datenbanken gelöst. Die Gründe dafür sind vielfältig. Ohne weiter im Detail auf diese einzugehen, lässt sich mit Sicherheit sagen, dass viele Unternehmen nicht die nötigen Ressourcen aufbringen können, um einen weiteren mehr oder weniger komplexen Verzeichnisdienst zu betreiben. Obwohl Benutzer und Gruppeninformationen bereits zentral in einem MS Active Directory oder LDAP Verzeichnis verwaltet werden, lassen sich diese nicht direkt für EUS verwenden. Es braucht zwingend immer ein Oracle Verzeichnis wie OID oder OUD. Das bedeutet, dass neben einem weiteren Verzeichnis auch eine Synchronisation aufgebaut und betrieben werden muss. Dies führt zu einer redundanten Datenhaltung, komplexeren Architektur und birgt das Risiko erhöhter Fehleranfälligkeit, was schlussendlich nicht im Interesse des Kunden ist.

Oracle Unified Directory AD Proxy Server

Im Gegensatz zu OID kann OUD aber nicht nur als reiner Verzeichnisserver, sondern auch als Proxy Server betrieben werden. Dabei nutzt OUD die Benutzer- und Gruppeninformationen im bestehenden Verzeichnis und ruft diese direkt mit LDAP Abfragen ab. EUS spezifische Informationen wie DB Registrierungsinformationen, Benutzer- und Rollenzuordnungen sowie weiteren EUS spezifische Metadaten werden lokal im OUD gespeichert. Auf diese Weise arbeitet OUD als Echtzeit-Interpreter für die Oracle Datenbanken. Anfragen nach Benutzerinformationen werden transparent beantwortet, unabhängig davon, ob die Informationen lokal im OUD abgelegt sind oder aus einem zentralen Verzeichnis abgerufen werden. Somit müssen die Daten nicht synchronisiert oder redundant abgelegt werden, was wiederum die Gesamtbetriebskosten reduziert.

Abbildung 1 zeigt den schematischen Aufbau einer EUS Datenbank mit einem OUD AD Proxy und MS Active Directory als zentralen Verzeichnisserver. Der Verbindungsaufbau vom Benutzer Scott und damit die Authentifizierung und Autorisierung ist mit den Pfeilen dargestellt.

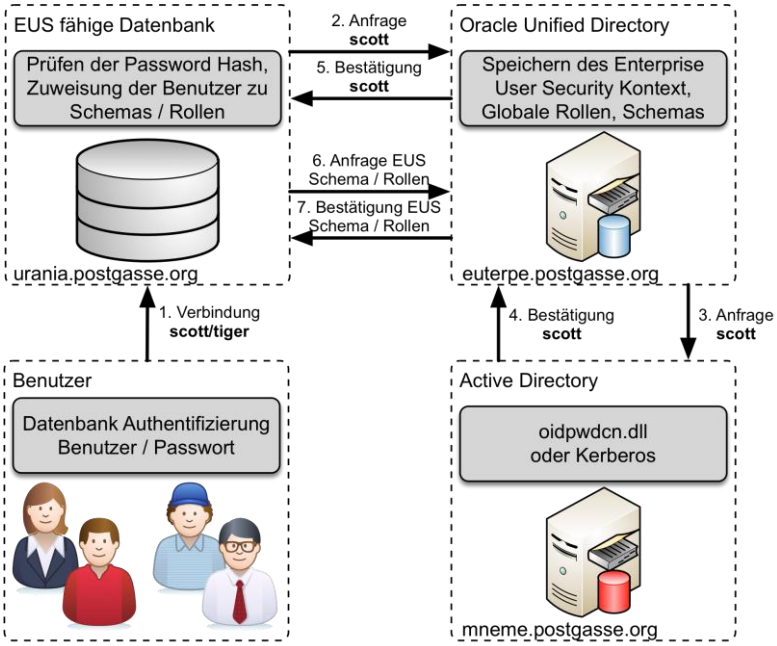

Abbildung 1 Enterprise User Security mit Active Directory Integration

Authentifizierung

Je nach Konfiguration stehen Passwort, Kerberos oder SSL Authentifizierung zur Verfügung. Am einfachsten ist dabei sicher die Passwort Authentifizierung, bei welcher sich der Datenbankbenutzer mit seinem Windows Passwort an der Datenbank anmeldet. Auch diese kann nicht ganz ohne Hürden umgesetzt werden. Der von Microsoft verwendete Passwort-Hashes ist nicht direkt mit Oracle Datenbanken kompatibel. Daher muss auf jedem Active Directory Domain Controller das Oracle Password Change Notification Plug-In (`oidpwdcn.dll`) installiert werden. Dazu gehört auch eine Active Directory Schemaerweiterung, damit das Plug-In den Oracle spezifischen Hashwert abspeichern kann.

Wird dagegen Kerberos als Authentifizierungsmethode verwendet, wird das Plug-In und die Schemaerweiterung nicht benötigt. Dafür kann mit Kerberos zusätzlich Single Sign On (SSO) erreicht werden.

Voraussetzungen

Für den Aufbau der in der Abbildung 1 vorgestellten Architektur sind folgende Voraussetzungen zu erfüllen:

- Oracle Enterprise Edition 12c Datenbank (12.1.0.2) mit LDAP Client Patch 19285025 und einer Datenbank, welche für Enterprise User Security konfiguriert wird
- Oracle Unified Directory 11.1.2.3.0 mit aktuellem Bundle Patch 25383162
- MS Active Directory Domain Controller auf Windows 2012 R2
- Oracle Enterprise Manager Cloud Control 13c R2 für die Konfiguration von Enterprise User Security. Alternativ kann hier auch eine ältere OEM Version oder das EUSM Command Line Utility verwendet werden. Siehe hierzu auch MOS Note 1085065.1 *EUSM, Command Line Tool for EUS Administration and Some EUS Good to Knows*

Konfiguration Active Directory

Damit die EUS Password Authentifizierung auch mit Active Directory funktioniert, ist ein OUD Password Synchronisations Plug-In sowie eine Schema Erweiterung nötig. OUD liefert die entsprechende Java Klasse, um das Attribut *orclCommonAttribute* zu erstellen. Die Schema Erweiterung wird mit dem Aufruf der Java Klasse direkt aus dem OUD Home Verzeichnis `$OUD_HOME/OUD1/config/EUS/ActiveDirectory` erstellt.

```
java ExtendAD -h mneme.postgasse.org -p 389 \
  -D cn=administrator,cn=users,dc=postgasse,dc=org \
  -w <pwd> -AD dc=postgasse,dc=org -commonattr
```

Das OUD Password Synchronisation Plug-In `oidpwdcn.dll` ist im selben Verzeichnis und steht als 32Bit oder 64Bit Version zur Verfügung. Die DLL Datei muss für die Installation auf dem Active Directory Server in das Verzeichnis `C:\Windows\system32` kopiert werden. Damit die DLL Datei verwendet wird, muss in der Registry zusätzlich der Registry Key

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Notification` mit `oidpwdcn` erweitert werden. Mit dem Restart des Active Directory Servers ist die Installation abgeschlossen. Sind mehrere Active Directory Server vorhanden, muss das Plug-In analog auf jedem Server installiert werden. Wie weiter oben angemerkt, sind diese Anpassungen nicht nötig, wenn ausschliesslich Kerberos zur Authentifizierung verwendet wird.

Aufbau der OUD Proxy Instanz

Für das Erstellen der verschiedenen OUD Instanzen liefert Oracle entsprechende Setup Programme, welche im OUD Installations- respektive OUD Home Verzeichnis bereitstehen. Je nach Bedarf können die Programme mit einer grafischen Oberfläche, als Command Line Installation oder auch als Silent Installation ausgeführt werden. Die Silent Installation ist vorwiegend hilfreich, wenn mehrere Instanzen mit einem Skript automatisiert aufgebaut werden sollen.

Die OUD Proxy Instanz selbst wird mit `oud-proxy-setup` erstellt. Ohne Angabe eines Parameters wird direkt die grafische Oberfläche für die Eingabe der Server-und Instanz Konfiguration gestartet. Für EUS und die MS AD Integration muss dabei zwingend LDAPS aktiviert werden. Entweder wird ein kundenspezifisches SSL Zertifikat verwendet oder wie beim Aufbau der Testumgebung (siehe Abbildung 2) ein selbstsigniertes Zertifikat. Für Produktionsumgebungen wird empfohlen, jeweils nur korrekt signierte Zertifikate zu verwenden.

In den nächsten Schritten wird als Proxy Konfiguration *Configure EUS* festgelegt und MS Active Directory als Datenquelle mit dem entsprechenden EUS Namenskontext ausgewählt. Die Abbildung 2 zeigt zusammenfassend alle Einstellungen. Durch die Bestätigung mit dem Button *Finish* wird anschliessend eine OUD Proxy Instanz erzeugt. Als Standard wird dabei immer eine Instanz mit dem Namen *ASINST*_1 im OUD Home Verzeichnis erstellt.

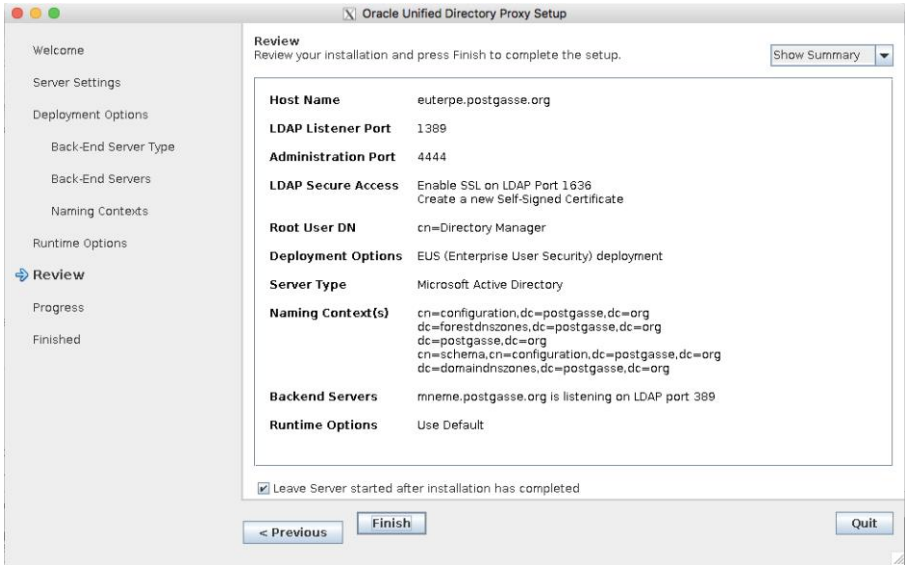

Abbildung 2 Zusammenfassung OUD Proxy Setup

Grundsätzlich wird empfohlen, die OUD Instanz explizit zu benennen und in einem anderen Verzeichnis respektive auf einem anderen Filesystem als die OUD Software anzulegen. Ähnlich wie bei OFA (Oracle Flexible Architecture) wird so sichergestellt, dass Daten und Konfiguration getrennt von der Software verwaltet werden. Um eine OUD Instanz explizit zu benennen, muss der Instanz Name vor dem Aufruf von `oud-proxy-setup` via Umgebungsvariable *INSTANCE_NAME* festgelegt werden. Der Instanz Name wird dabei als Pfad relative zum OUD Home Verzeichnis angegeben. Für die EUS Test Umgebung wurde als Instanz Name *oud_ad_proxy* gewählt. Die folgende Tabelle zeigt die verschiedenen Verzeichnisse und Umgebungsvariablen:

Umgebungsvariable	**Pfad**
ORACLE_BASE	`/u00/app/oracle`
OUD_HOME	`/u00/app/oracle/product/oud11.1.2.3`
ORACLE_HOME	`/u00/app/oracle/product/oud11.1.2.3/OUD1`
Verzeichnis für die OUD Instanzen	`/u00/app/oracle/instances`
INSTANCE_NAME	`../../instances/oud_ad_proxy`

Tabelle 1 Umgebungsvariablen und Instanz Verzeichnisse

Bevor die neu erstellte OUD Proxy Instanz nun für EUS verwendet werden kann, braucht es noch kleinere Anpassungen. Als erstes wird das Proxy Workflow Element angepasst und die Remote Bind Anmeldeinformationen festgelegt. Im Folgenden wird dabei der AD Benutzer *OUD Admin* verwendet. Grundsätzlich kann dies aber ein beliebiger AD Benutzer sein, welcher vollen Lesezugriff auf Benutzer- und Gruppeninformationen hat. Zusätzlich wird auch der Client Connection Mode auf *use-specific-identity* gesetzt. Diese Einstellung ist nötig, wenn das externe Verzeichnis keine anonymen Bind Anfragen zulässt. Die Anpassungen werden mit dem OUD Command Line Admin Tool *dsconfig* ausgeführt:

```
dsconfig set-workflow-element-prop --element-name proxy-we1 \
  --add exclude-list:cn=directory\ manager \
  --add exclude-list:cn=oraclecontext,dc=postgasse,dc=org \
  --set remote-root-dn:"cn=OUD Admin,cn=users,dc=postgasse,dc=org" \
  --set remote-root-password:<PASSWORT> \
  --set remote-ldap-server-bind-dn:"cn=OUD Admin,cn=users,dc=postgasse,dc=org" \
  --set remote-ldap-server-bind-password:<PASSWORT> \
  --set ldap-server-extension:proxy1 \
  --set client-cred-mode:use-specific-identity \
  --hostname euterpe.postgasse.org --port 4444 --trustAll \
  --bindDN "cn=Directory Manager" --bindPasswordFile $etc/oud_ad_proxy.pwd \
  --no-prompt
```

Damit EUS die Benutzer- und Gruppeninformationen findet, müssen die entsprechenden Einträge im EUS Kontext ebenfalls angepasst werden. Oracle liefert hierzu im Verzeichnis `$OUD_HOME/OUD1/config/EUS` eine LDIF Template Datei `modifyRealm.ldif`, welche wie folgt angepasst werden muss:

- Ersetzen von `dc=example,dc=com` mit dem korrekten Namenskontext
- Ersetzen von `ou=people` und `ou=groups` mit dem entsprechenden Ort für die Benutzer- respektive Gruppeninformationen

Das angepasste LDIF Template wird anschliessend mit `ldapmodify` geladen:

```
ldapmodify --hostname euterpe.postgasse.org --port 1389 \
  --bindDN "cn=Directory Manager" --bindPassword <PASSWORT> \
  --filename modifyRealm.ldif
```

Grundsätzlich ist die OUD Proxy Instanz nun bereit für EUS. Oracle 11g Datenbanken können direkt in OUD registriert und für EUS konfiguriert werden. Für Oracle 12c respektive EUSM 12c und Oracle Cloud Control 12c / 13c braucht es hingegen noch eine weitere Anpassung. Die aktuellen Versionen der Oracle Datenbank und Oracle Cloud Control verwenden den SASL Mechanismus, um sich mit der OUD Instanz zu verbinden. Allerdings funktioniert dies in OUD standardmässig nicht. Das Admin Passwort vom EUS User muss zusätzlich zwingend mit einem reversiblen Algorithmus abgespeichert werden. Dazu ist das Root Passwort Profile zu erweitert, so dass neue Passwörter auch mit dem AES Algorithmus abgespeichert werden.

```
dsconfig set-password-policy-prop \
  --policy-name "Root Password Policy" \
  --add default-password-storage-scheme:"AES"
  --hostname euterpe.postgasse.org --port 4444 --trustAll \
  --bindDN "cn=Directory Manager" --bindPasswordFile $etc/oud_ad_proxy.pwd \
  --no-prompt
```

Mit einem expliziten Neusetzten des Passwortes wird sichergestellt, dass auch das neue Passwort Storage Schema verwendet wird.

```
ldappasswordmodify --hostname euterpe.postgasse.org --port 4444 \
  --bindDN "cn=Directory Manager" --bindPasswordFile $etc/oud_ad_proxy.pwd \
  --useSSL --trustAll \
  --currentPassword <PASSWORT> --newPassword <PASSWORT>
```

```
ldapsearch --hostname euterpe.postgasse.org --port 4444 \
  --bindDN "cn=Directory Manager" --bindPasswordFile $etc/oud_ad_proxy.pwd \
  --useSSL --trustAll \
  -- baseDN "cn=Directory Manager,cn=Root DNs,cn=config" \
  --searchScope base objectclass=* userpassword

dn: cn=Directory Manager,cn=Root DNs,cn=config
userpassword: {AES}AfLk8S3k8k3ekXLV6qaP+mFUe/DStQ4ngUAdo6P5EjOKOMm4AN27Xw==
userpassword: {SSHA512}YSI4tlv3gO4z0czFU9EdTOGnfmGhQqOtbWUopV7xgcPDlYS/Eea3ydQUt
 YT5Qog/ngZ8w4M3EHNf4/MObnPC8M+lblEIKivf
```

Für Produktionsumgebungen ist es sinnvoll, dass anstelle des Root Passwort Profils ein dezidiertes Passwort Profile für EUS sowie entsprechende EUS Admin Benutzer erstellt werden.

Datenbank Konfiguration

Damit die Datenbanken nun im OUD registriert werden können, wird im Netzwerk Verzeichnis der Datenbank die Datei `ldap.ora` angepasst. Dazu wird der OUD Server und der Default Kontext angegeben. Im Folgenden ist als Beispiel die Datei `ldap.ora` aufgeführt, wie sie bei der in Abbildung 1 beschrieben Testumgebung verwendet wird. Als Directory Server Typ muss auch bei OUD OID angegeben werden.

```
DIRECTORY_SERVERS= (euterpe.postgasse.org:1389:1636)
DEFAULT_ADMIN_CONTEXT = "dc=postgasse,dc=org"
DIRECTORY_SERVER_TYPE = OID
```

In `sqlnet.ora` wird die Namesauflösung angepasst und neu LDAP als zusätzliche Quelle angegeben. Anbei ein Auszug aus der Datei `sqlnet.ora`.

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

Die eigentliche Registrierung der Datenbank in OUD erfolgt mit dem *dbca* interaktiv wie in Abbildung 3 oder Silent via Command Line. Für die Registrierung wird die Anmeldeinformation des EUS Admins benötig. Als Standard Database CN wird der DB Unique Name verwendet, optional lässt sich dieser aber auch anpassen. Ist für diese Datenbank noch kein Oracle Wallet vorhanden, legt der *dbca* ein neues Wallet im Admin Verzeichnis der Datenbank an und speichert darin die OUD DB Credentials.

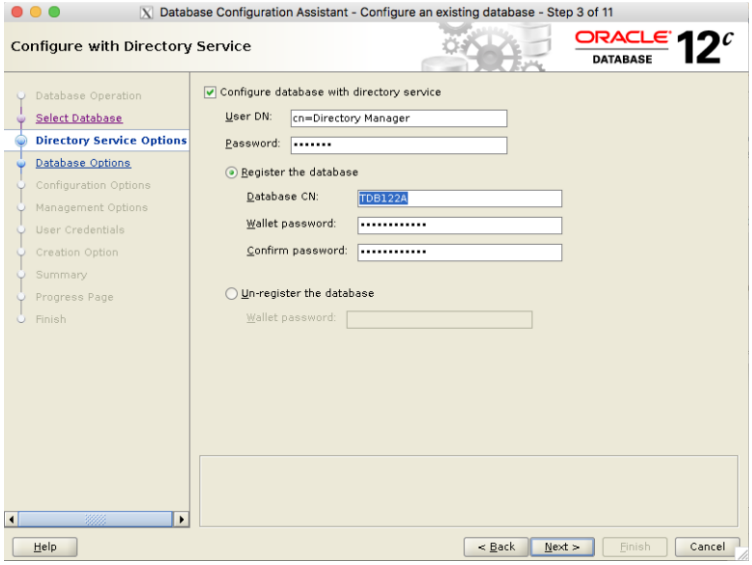

Abbildung 3 DB Registrierung mit dem dbca

Neben der OUD Registrierung und dem Wallet passt der *dbca* zusätzlich auch die Datenbank Parameter *ldap_directory_access* sowie *ldap_directory_sysauth* entsprechend an.

Die Basis für EUS ist nun sichergestellt. Was noch fehlt, sind entsprechende EUS Rollen respektive Datenbank Benutzer und Rollen sowie die Zuweisung zu den verschiedene EUS Datenbanken. Als einfaches Beispiel wird mit SQL*Plus ein globales shared Schema erstellt, welches die lokalen Rollen *connect* erhält:

```
CREATE USER global_shared IDENTIFIED GLOBALLY;

GRANT connect TO global_shared;
```

Anschliessend wird mit EUSM für die Datenbank TDB121A ein einfaches Mapping für alle Benutzer einer bestimmten Organisation Unit (ou) erstellt. Das Mapping sowie weitere EUS Konfigurationen können, wie weiter oben angemerkt, entweder mit dem EUSM Commandline Tool oder mit Oracle Enterprise Manager Cloud Control erstellt werden. Das folgende Syntax Beispiel zeigt, wie das Mapping mit EUSM erstellt wird:

```
eusm createMapping database_name="TDB121A" realm_dn="dc=postgasse,dc=org"
map_type=SUBTREE map_dn="ou=People,dc=postgasse,dc=org" schema=GLOBAL_SHARED
ldap_host="euterpe.postgasse.org" ldap_port=1389 ldap_user_dn="cn=Directory Manager"
ldap_user_password=<PASSWORT>
```

Etwas einfacher ist es, das Mapping, wie in Abbildung 4 dargestellt, mit OEM Cloud Control 13c R2 zu definieren. Die Benutzer, Gruppe sowie das entsprechend Datenbank Schema können mit einem einfachen Dialog erfasst werden. Für das Erstellen einzelner Mappings ist OEM sicher praktisch. Nichtsdestotrotz lässt sich die EUS Konfiguration mit dem EUSM Tool einfacher in Skripten automatisieren.

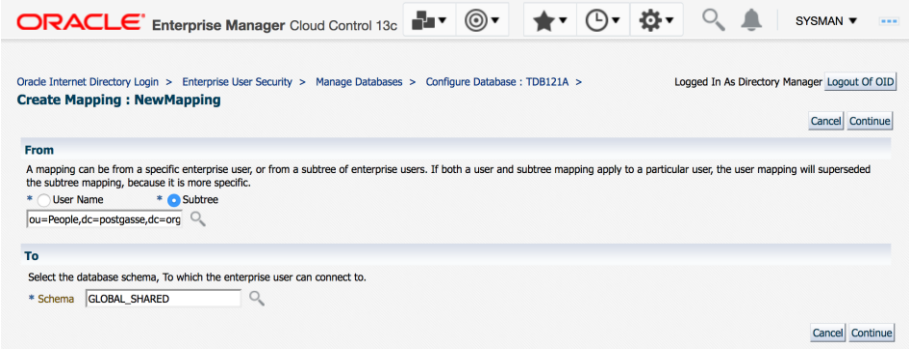

Abbildung 4 EUS Mapping mit OEM 13c R2

Das Mapping wurde als Subtree Mapping auf einen ganzen Baum im Verzeichnis definiert. Somit kann sich nun jeder Benutzer in der OU *ou=People,dc=postgasse,dc=org* in MS AD mit der Datenbank verbinden. Die Abfrage des SYS_CONTEXT gibt entsprechend Auskunft über die Enterprise Identity.

```
SQL> connect oehrli
Enter password:

Connected.

SQL> show user
USER is "GLOBAL_SHARED"

SQL> SELECT
  sys_context('userenv','SESSION_USER') "USER",
  sys_context('userenv','AUTHENTICATED_IDENTITY') "AUTH_IDENTITY",
  sys_context('userenv','ENTERPRISE_IDENTITY') "ENTERPRISE_IDENTITY"
FROM DUAL;

USER            AUTH_IDENTITY  ENTERPRISE_IDENTITY
--------------- -------------- --------------------------------------------------
GLOBAL_SHARED   OEHRLI         cn=Stefan Oehrli,ou=People,dc=postgasse,dc=org
```

Alternativ kann man das Mapping auch für die ganze Domain erstellen. Damit erhalten die Benutzer Zugriff auf alle in dieser Domain registrierten Datenbanken. Die Voraussetzung ist natürlich, dass es lokal jeweils das Schema *GLOBAL_SHARED* gibt.

```
eusm createMapping domain_name="OracleDefaultDomain" realm_dn="dc=postgasse,dc=org"
map_type=SUBTREE map_dn="ou=People,dc=postgasse,dc=org" schema=GLOBAL_SHARED
ldap_host="euterpe.postgasse.org" ldap_port=1389 ldap_user_dn="cn=Directory Manager"
ldap_user_password=<PASSWORT>
```

Das Beispiel zeigt, wie einfach man ein 1:1 Mapping erstellen und sich anschliessend als Enterprise Benutzer an der Datenbank anmelden kann. In der Praxis wird das Mapping komplexer ausfallen. Gewisse EUS Benutzer werden globale private Schemas haben, andere werden dagegen mit globalen shared Schemas und Enterprise Rollen arbeiten. In der Kombination mit Proxy Rechten und Administrativen Privilegien wie SYSDBA lassen sich so umfangreiche und komplexe Benutzer- und Rollenkonzepte umsetzen.

Patch, Bug's und weitere Sorgen

Im Zusammenhang mit LDAP, SSL und der Oracle Datenbank gibt es noch einen Bug, welcher zwingend behoben werden muss, damit die Anmeldung so wie oben beschrieben funktioniert. Der Bug 19285025 wurde bis anhin in keinem Base Release oder Patch Set Update behoben. Daher muss der entsprechende Patch 19285025 weiterhin explizit bei allen aktuellen Versionen wie Oracle 11.2.0.4, 12.1.0.2 und leider auch 12.2.0.1 installiert werden. Für die neusten Oracle Version 12.2.0.1 gibt es zudem noch den Bug 26093306, welcher die SASL Authentifizierung am OUD betrifft.

Neben diesem Bug gibt es im SSL und Kerberos Umfeld generell einige Bugs. Diese können mit entsprechenden Workarounds oder Patchs umgangen werden. Trotzdem ist das Troubleshooting nicht immer ganz einfach. Schliesslich ist die Architektur bei der zentralen Benutzerverwaltung komplexer. Neben der Datenbank ist auch OUD und MS AD bei einer Anmeldung an der Datenbank beteiligt. Die effektiven Ursachen von ORA-01017 oder ORA-28030 sind daher häufig nicht direkt identifizierbar. Mit Hilfe des OUD Access Log, SQL Net Tracing oder einem entsprechenden Oracle Event kommt man der effektiven Ursache aber in der Regel schnell auf die Spur.

Deasaster Recovery und Hochverfügbarkeit

Die in Abbildung 1 aufgezeigte Architektur ist für eine Test- und Engineering Umgebung ausreichend. Für den produktiven Betrieb sind jedoch weitere Massnahmen nötig, damit die Hochverfügbarkeit und das Desaster Recovery sichergestellt werden kann. Ansonsten ist eine zentrale Benutzerverwaltung ein Single Point of Failure. Ist sie nicht verfügbar, können sich die Benutzer nicht mehr an den Datenbanken anmelden. OUD bietet verschiedene Möglichkeiten wie z.B. Online Backup und Replikation, um die OUD Instanzen sicher und hochverfügbar zu betreiben. Diese Massnahmen sind in einem entsprechenden OUD Konzept zu planen und entsprechend umzusetzen – und auch zu testen.

Fazit

Mit Oracle Unified Directory und dem AD Proxy wird die Umsetzung einer zentralen Benutzerverwaltung mit Enterprise User Security wesentlich vereinfacht. Ein OUD AD Proxy ist grundsätzlich schnell aufgebaut, so dass man direkt den ersten Nutzen hat. Ungeachtet dessen liegen die Herausforderungen in den Details. So wird die MS AD Integration und Kerberos Konfiguration bei komplexen AD Architekturen um einiges aufwändiger. Zudem braucht es für den unternehmensweiten Einsatz zwingend ein geeignetes Benutzer- und Rollenkonzept. Dafür muss meist mehr Zeit eingeplant werden als für die einfache Konfiguration von OUD. Die verschiedenen Bugs im Kerberos, LDAP bzw. SSL Umfeld erschweren einem das Leben zusätzlich. Sind diese Hürden erst einmal gemeistert, hat man aber ein verlässliches und sicheres System für die zentrale Benutzerverwaltung von Oracle Datenbanken.

Viel Erfolg beim Einsatz von Trivadis-Know-how wünscht Ihnen

Stefan, Oehrli
Solution Manager / Partner

Trivadis AG

Sägereistrasse 29
CH- 8152 Glattbrugg
Telefon: + +41 58 459 55 55
E-Mail: stefan.oehrli@trivadis.com
www.trivadis.com

Weiterführende Informationen, Links…

Trivadis Unternehmenswebseite www.trivadis.com

Trivadis Security Expert Team www.trivadis.com/de/security

Blog Stefan Oehrli www.oradba.ch/category/oud