Fun with OUD (Oracle Unified Directory)

Manfred Hoppe
Talanx Systeme AG
Hannover

Schlüsselworte

OUD, Oracle Unified Directory, Directory Service, LDAP, LDAPS, EUS, Enterprise User Security, Identity- und Access Management

Einleitung

In den heutigen Cloud-Infrastrukturen ist ein Identity- und Access Management (IAM) unverzichtbar. Als Basis dafür dienen Directory Service Systeme. Das Oracle Unified Directory (OUD) ist ein sehr effizienter und schlanker Directory Service. Das Motto ‚Fun with OUD' soll vermitteln, dass es Spaß macht einen Directory Service aufzubauen.

Oft wird das OUD im Rahmen der Oracle Datenbank mit dem Enterprise User Security (EUS) in Verbindung gebracht. Die Einsatzmöglichkeiten sind erheblich höher, wobei EUS nur ein kleiner Teilaspekt ist.

Basierend auf einem OUD-Projekt im Rahmen von Oracle Net Service werden Best Practice, zusätzliche Vorgehensweisen beim Aufbau sowie Hochverfügbarkeit vorgestellt. Darüber hinaus wird neben Tuningmaßnahmen auch eine Kopplung z. B. zum Active Directory präsentiert. Es wird auf Backupstrategien, Monitoring und die Administration im täglichen Betrieb eingegangen. Speziell werden Security, wie Verschlüsselung und dedizierte Zugriffe, erläutert. Einige Hinweise auf Fallstricke bei der Konfiguration vom OUD werden dargestellt. Auch das Thema Lasttests soll nicht zu kurz kommen.

Fun with OUD

Beim OUD handelt es sich um einen integrierten und auf Java basierten Directory Service. Das OUD basiert auf den den openDS der Firma Sun, dass sehr stark verbreitet ist.. Durch Übernahme der Firma Sun durch die Firma Oracle wurde das openDS übernommen und zum jetzigen OUD weiterentwickelt. Mittlerweile ist das OUD ein strategisches Produkt und etliche andere Produkte sind bzw. werden im OUD integriert.

Der Directory Server erfüllt den Full LDAPv3 compliance (RFC 4510-4519) Standard. Ebenfalls beinhaltet der Directory Server einen Replikations-Mechanismus. Mit der Replikation kann eine hohe Verfügbarkeit vom OUD erreicht werden.

Im OUD ist eine Datenbank vom Type Oracle Berkeley Database Java Edition eingebettet. Die Installation und der Administrationsaufwand sind niedrig. Für die Administration kann das Oracle Directory Service Manager (ODSM) eingesetzt werden.

Die Hauptkomponenten sind:

- Directory Server
- Proxy Server
- Replication Gateway Server

Der Proxy Server speichert keine Daten, sondern kann zum Routen von Client- Request zum Directory Server oder anderen LDAPv3 Compliant Server benutzt werden. Darüber hinaus kann mit dem Proxy Server auch Load Balancing oder Daten Verteilung durchgeführt werden. Ferner können andere LDAP v3-compliant Directory Server eingebunden werden. Außerdem kann mit dem Proxy auch eine Virtualisierung vorgenommen werden.

Das Replication Gateway wird zu Replikation zur Oracle Directory Server Enterprise Edition (ODSEE) benutzt.

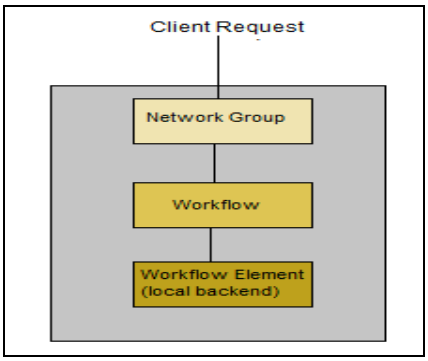
Ein wichtiger Aspekt ist der interne Aufbau der Komponenten vom OUD und aus der Erfahrung heraus ist dies eine wichtige Grundvorrausetzung, um die Wirkungsweise vom OUD zu verstehen.

Die Komponenten sind:

- Network Group
- Workflow
- Workflow Element

Die Komponenten haben bestimmte Aufgaben und außerdem gibt es Abhängigkeiten unter den Komponenten. Durch die Abhängigkeiten der Komponenten muss beim Aufbau der Komponenten eine gewisse Reihenfolge eingehalten werden. Die Network Group ist der Einstiegspunkt aller Client Request zum OUD. Die Network Groups können aus einer oder mehreren Network Groups bestehen. Die Aufgabe sind z. B. Filterung, Ressourcen Limitierungen usw. Eine Network Group kann aus einem oder mehreren Workflows bestehen. Der Workflow hat die Aufgabe den Naming Context (BaseDN) zu definieren und den dazugehörigen Workflow Element mit Zugriffsberechtigungsgruppen (access control group) und deren ACI (access control instructions) zu steuern. Von den Workgroup Elementen gibt es verschiedene Elementtypen, die bestimmte Aufgaben haben. Die Aufgaben können verschieden sein, z.B. das Leaf Workflow Element beinhaltet das Local Backend, welches im Directory Server vorhanden ist.

Ein Beispiel eines vereinfachten Aufbaus eines Local Backend



Bevor man jedoch eine OUD Installation beginnt, muss eine Integration vom OUD in der IT-Gesamtarchitektur genau abgestimmt sein. Diese Abstimmung hat wesentliche Auswirkung über den Einsatz vom OUD. Es hat auch entscheidende Auswirkungen für die Installation und Konfiguration vom OUD. Auch die beschriebenen OUD Komponenten spielen hier eine wichtige Rolle.

Die eigentliche Installation vom OUD ist per GUI relativ simple. Dort kann per Oracle Installer (runInstaller) der OUD aufgebaut werden. Hier der Hinweis, dass sämtliche Installationen im OUD-Kontext sich streng an die Vorgaben des Installation Guide zu halten haben.

Der eigentliche Kern vom OUD ist die sogenannte OUD Instance. Die OUD Instance beinhaltet den eigentlichen Directory Server bzw. den Proxy Server. Die Installation führt bei einfachen Umgebungen zu schnellen Ergebnissen. Mit der Installation der OUD Instance kann auch gleichzeitig eine Replikation mit aufgebaut werden. Aus der Praxis sollten besonders auch bei komplexem Aufbau, einer manuellen bzw. eine Skriptvariante den Vorzug gegeben werden. Hier noch der Hinweis, dass viele OUD- Kommandos im interaktiven Modus oder als Kommandozeile ausgeführt werden können. Für den Aufbau einer OUD-Instance wird das Kommando oud-setup benutzt.

Ein Tipp beim Aufbau einer OUD-Instance ist, möglichst eine zentrale Verzeichnisstruktur für Passwörter und für Zertifikate anzulegen. Der Hintergrund ist, dass viele OUD-Kommandos mit Password-Files arbeiten und durch diese Eigenschaft wird das Ausführen der Kommandos bzw. Skripts sehr stark vereinfacht.

Ein Ausschnitt vom Kommando oud-setup zum manuellen Anlegen eine OUD-Instance:

```
# Set Variable

. /home1/oracle11/tools/create/Install_new/env

echo " ... Setup OUD Instance $HOST1 ...."

$MW_HOME/Oracle_OUD1/oud-setup \

--cli \

--baseDN ${DOMAIN1} \

--addBaseEntry \

--adminConnectorPort $ADMINP \

--ldapPort $LDAP \

--rootUserDN "$DIRMAN" \

--rootUserPasswordFile ${PW3} \

……
```

Nach der Installation der OUD-Instance beginnen einige Konfigurationsschritte. Wenn eine Replikation vorhanden ist, sollte die Replikation bei der Installationsstrategie zur Installationserleichterung eingesetzt werden. Die Replikation hilft dabei, die zukünftigen Konfigurationsschritte auf anderer OUD-Instance zu verteilen.

Eine Konfiguration kann auch über den ODSM erfolgen, jedoch mit dem Nachteil der Nachvollziehbarkeit der Konfiguration. Mit ODSM lassen sich Ad hoc Änderungen bzw. Einstellungen überprüfen und damit ist es sehr leicht möglich, sich einen Überblick über das System zu verschaffen.

Ein anderer Vorteil zu Beginn mit OUD-Kommandos zu arbeiten ist, ein Grundverständnis der Kommandos zu bekommen, bevor man sich mit dem GUI-basierten Administrationswerkzeug ODSM beschäftigt.

In der folgenden Übersicht sind einige wichtige Kommandos vom OUD aufgelistet:

Kommando	Beschreibung
start-ds	Starten der OUD-Instance
stop-ds	Stoppen der OUD-Instance
dsconfig	Konfigurationswerkzeug, wichtig für alle OUD-Komponenten
manage_suffix	Strukturen mit einen Backend anlegen.
dsreplication	Überprüfung und Konfiguration von Replikationseinstellungen
startWebLogic.sh	Startet die Weblogic-Instance(ODSM Umgebung)
backup	OUD Backup bzw. Backup der OUD-Backends
restore	OUD Restore bzw. restore der OUD-Backends
ldapmodify	LDAP Daten ändern
ldapsearch	LDAP Daten suchen
ldapdelete	LDAP Daten löschen
status	Überprüfung des OUD-Status
dstune	Tuning Utility

Das Kommando dsconfig ist eines der wichtigsten Kommandos. Mit dsconfig können sich sämtliche Konfigurationen, wie z. B. eine Kopplung mit dem Active Directory (Mircosoft), bewerkstelligen lassen. Somit kann aus einem Mix von verschiedenen Kommandos ein automatisiertes Anlegen von einer OUD-Instance erreicht werden.

Kontaktadresse:
Manfred Hoppe
Talanx Systeme AG
Pobielskistr, 396
D-30659 Hannover

Telefon: +49 (0) 511-645 5160
Fax: +49 (0) 511-645 1152480
E-Mail manfred.hoppe@talanx.com
Internet: www.talanx.com