Zentraler Identity Repository Zugriff für Oracle BPM Suite mit Oracle Virtual Directory

Abdi Mohammadi/Kersten Mebus
Oracle
Hamburg

Schlüsselworte
Oracle, Identity Repository, Oracle Business Process Management , Oracle BPM, SOA, OPSS, Security, Virtual Directory, Directory, Application Roles, Role Management, BMP Studio, LDAP Groups, Users, Authentication, Authorization

Einleitung

Die Authentisierung und Autorisierung von Benutzern innerhalb der Oracle BPM Suite bzw. der Oracle Business Workspace Applikation basiert auf Zugriffe eines Directory Servers. Ein Directory Server muss natürlich als Authentication Provider des Woblogic Domains konfiguriert worden sein. Der Weblogic Server verwendet standardmässig einen integrierten LDAP Server als „DefaultAuthenticator“ und speichert die User und Gruppen darin.

Der integrierte LDAP Server im Weblogic Server ist zwar für einige wenige lokale Users oder Gruppen geeignet, für Produktionsumgebungen möchte man jedoch auf unternehmensweite Directories zugreifen.

Die zentralen Directory Servers (Corporate Directory) in einem Unternehmen enthalten im Allgemeinen User-Einträge für alle Mitarbeiter und Partners eines Unternehmens. Üblicherweise werden Corporate Directories zentral verwaltet und enthalten meist keine applikationsspezifischen Daten und Attribute . So kann es sein, dass zwar alle Benutzer einer Applikation in dem zentralen Directory Server enthalten sind, aber keine spezielle applikationsspezifische Attribute oder Gruppen zu finden sind.

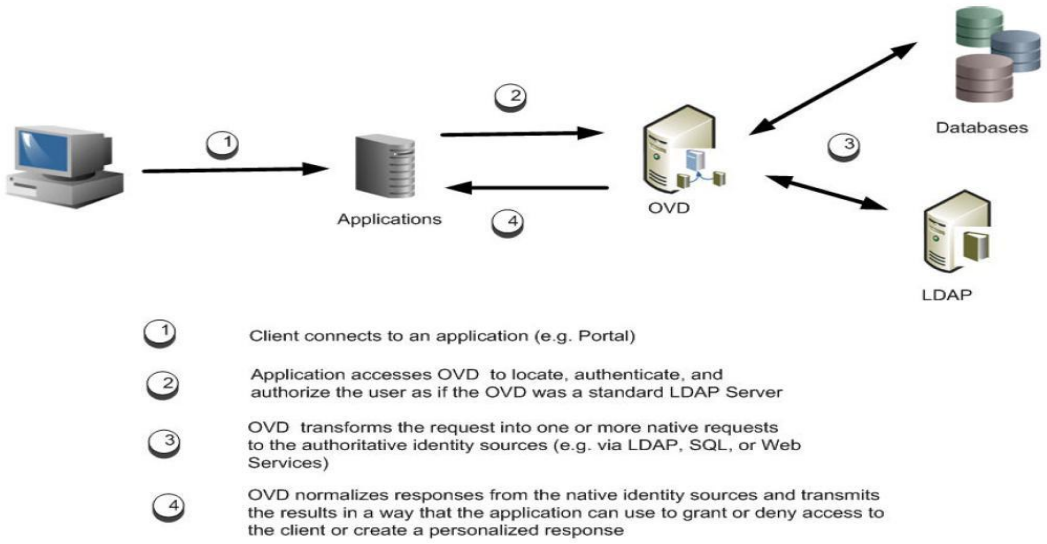

Abb. 1: OVD und JoinView

Um den zentralen Directory Server als Authentisierungs- Server zu benutzen und die fehlenden Attribute oder Gruppen aus einem anderen Directory Server zu erhalten, kann auf die Funktionalität des Oracle Virtual Directory zugegriffen werden. Während die Authentisierung des Users über OVD direkt an den zentralen Directory Server durchgereicht wird, können andere Attribute und Gruppenmitgliedschaften aus anderen Quellen geholt werden. Join Views in OVD können zur Aggregation von User Attributen aus unterschiedlichen Datenquellen (LDAP und JDBC) verwendet werden. Darüber hinaus können mittels Filter und Plugins von OVD dynamische Datentransformation für Daten durchgeführt werden. Z.B. kann ein virtuelles Attribut „Mail“ aus der Kombination vom Vornamen und Nachnmen eines Benutzers und den Domainnamen gewonnen werden. Auch statische Gruppen können dynamisch und virtuell erzeugt werden.

Die Oracle BPM Suite benutzt den „Authentication Provider“ vom Weblogic Server, um den Benutzer zu authentisieren und um Applikationsrollen für die Authorisierung der Prozeßaktivitäten festzulegen. Das Mapping zu den Applikationsrollen erfolgt aus den LDAP Gruppen und den einzelnen Benutzerinformationen.

Das untere Bild zeigt das Mapping von Users und Gruppen von LDAP auf BPM Rollen, was entweder in BPM Studio oder in der BPM Workspace Applikation definiert werden kann:

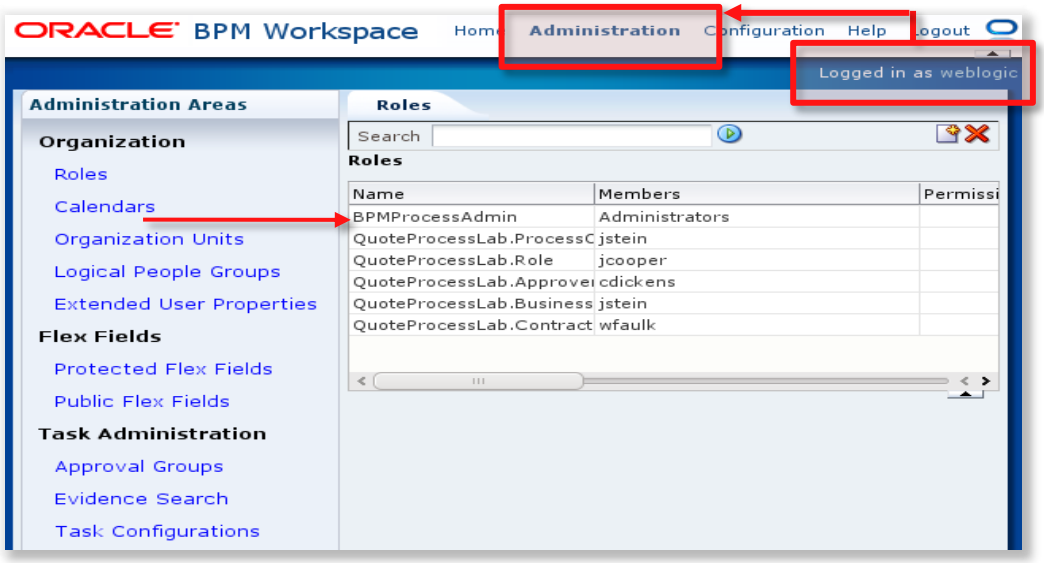

Abb. 2: Mapping von BPM Roles zu LDAP Users undGruppen

In dieser Session werden aus zwei PoCs mit Novell’s eDirectory und Oracle Datenbank sowie Siemens DirX über die Architektur und Hürden der Implementierung berichtet.

Beim ersten PoC wurde durch die Aggregation von Standard-Userdaten aus eDirectory und die zugehörigen Felder einer Datenbanktabelle (JoinView) ein virtueller Eintrag des Benutzers mit allen notwendigen Attributen zusammengestellt. Die BPM Suite kann nun anhand des Wertes des aggregierten Attributes eine Authorisierungs-Entscheidung fällen und dem Benutzer eine bestimmten Rolle zuweisen.

Beim zweiten PoC hatte man ca. 400k Users im zentralen DirX Directory. Der Kunde wollte jedoch seine Berechtigungen durchs Mapping von Applikationsrollen auf LDAP Gruppen realisieren. In DirX wurden jedoch keine Gruppen gepflegt. Darüber hinaus sollten sich nur bestimmte Benutzer aus DirX

in der BPM Workspace Applikation einloggen dürfen. Auch in diesem Fall wurde OVD eingesetzt, der einerseits mit geeignetem Filter nur bestimmte Benutzer aus DirX ausgwählt hat, um anschliessend mittels OVD Plugins eine oder mehrere statischen Gruppen dynamisch zu erzeugen. Auch hier sollten die Rollen des Benutzers durch Virtualisierung einer Datenbank-Tabelle mittels DynamicGroup Plugin von OVD realisiert werden.

Sicherheit in BPM

Hohe Anforderungen für Sicherheit sind beim Design der Sicherheitsaspekte der BPM Suite definiert. Die wichtigsten sind hier aufgelistet:

- Sicherheit / Zugriffskontrolle
  - Integration der vorhandenen User Repositories
  - Single Sign On
  - Hierachische Berechtigungen
    - Pages
    - Resources
  - Fein granulare Authorisierung

Um diesen Anforderungen gerecht zu werden, setzt Oracle BPM auf die „Oracle Plattform Security Services“ (OPSS). Diese Schnittstelle wird mittlerweile von allen Oracle Fusion Middleware Produkten (WLS, SOA, WebCenter, ADF, Entitlement Server, Access Manager) verwendet und vereinfacht die feine Integration unterschiedlichen Produkten in einer Architektur.

OPSS ist auf Standards basiert und portabel sowie in den Oracle Produkten integriert. Es bietet ein Security Framework. Diese abstrakte Sicherheits-Schnittstelle (APIs) entkoppelt die Applikationen von der verwendeten Sicherheits-Infrastruktur.

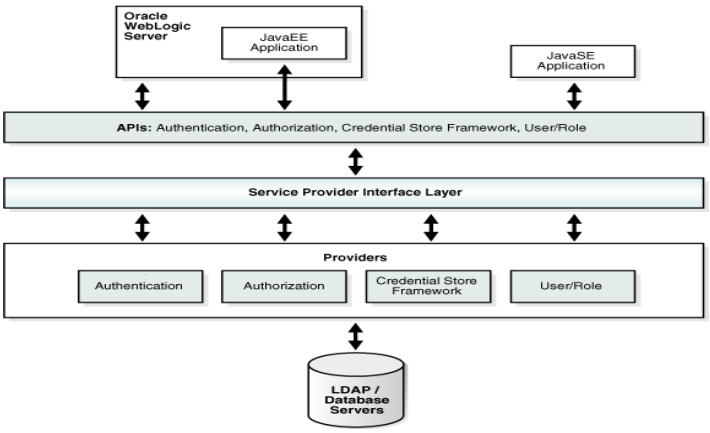

Abb. 3: OPSS Architecture Overview

Eine Untermenge der Funktionalität von OVD sind über die sogenannte „libOVD“ in OPSS integriert. Es ermöglicht, dass mehrere LDAP Provider virtualisiert werden. Im Gegensatz zu OVD können hier leider keine „nicht-LDAP“ Provider über OPSS integriert werden, auch wenn sie im Weblogic Server zu sehen sind. Die Konfiguration wird in dem Directory fmwconfig/ovd eines Weblogic Domains hinterlegt.

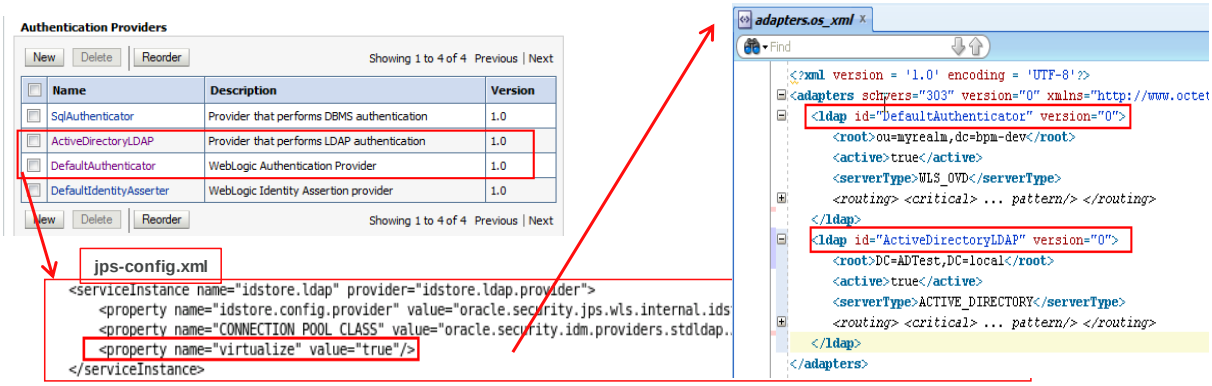

Abb. 4: OPSS Konfiguration / jps-config.xml und adapters.os_xml

Das Property “virtualize” in jps-config.xml schaltet die libOVD Funktionalität ein.

OVD

Das Oracle Virtual Directory kann selbst als ein Authentication Provider in Security Realms des Weblogic Servers angegeben werden. OVD anstatt libOVD ermöglicht, die volle Funktionalität von OVD zu nutzen. Damit ist es möglich sowohl auf Directory Server als auch auf Datenbanktabellen oder gar WebServices zuzugreifen und deren Daten zu aggregieren. Der LDAP- Client (in diesem Fall Weblogic Server bzw. BPM Suite) bekommt die aggregierten Daten eines Benutzers bzw. die dynamisch erzeugte Mitgliederliste einer oder mehrerer statischen Gruppen zu sehen.

Während der Client über unterschiedliche Protokollle wie LDAP, HTTP oder DSML seine Anfragen an OVD schicken kann, schickt OVD nach Überprüfung der Client-Requests, welche Adapter benutzt werden können, um diese Requests zu bearbeiten. Dabei können Daten (Attribute, Objectklassen und deren Werte) transformiert und durch die Virtualisierung dem Client eine bestimmte Sicht auf die Daten gewährt werden.
Hier ein Ausschnitt für die Konfiguration eines Datenbank-Adapters :

```
<database id=”SHRDB” version=”15”>
      <root>o=db</root>
       <active>true</active>
      <routing>
      ….
       <visible>Yes</visible>
       ….
       <driver>oracle.jdbc.driver.OracleDriver</driver>
       <url>xxxx</url>
       <user>BC_READONLY_TEST</user>
       <password>xxxxxx</password>
       <ignoreObjectClassOnModify>false</ignoreObjectClassOnModify>
       <includeInheritedObjectClasses>true</includeInheritedObjectClasses>
       <maxConnections>10</maxConnections>
      <mapping>
```

```
        ….

       <objectClass name="inetOrgPerson" rdn="uid">
        <attribute ldap="uid" table="SHAREDDATA_TEST_OBJ.AUT_V_GMT_USERS"
       field="U_NAME" type="VARCHAR"/>
        </objectClass>
       <objectClass name="groupOfUniqueNames" rdn="cn">
        <attribute ldap="uniqueMember"
       table="SHAREDDATA_TEST_OBJ.AUT_V_OVD_TEST" field="OVD_GROUP"
       type="VARCHAR"/>
        <attribute ldap="cn" table="SHAREDDATA_TEST_OBJ.AUT_V_OVD_TEST"
       field="OVD_GROUP" type="VARCHAR"/>
        </objectClass>
        </mapping>
        ……
 </dataBase>
```

Hier wird aus einer Datenbanktabelle `SHAREDDATA_TEST_OBJ.AUT_V_GMT_USERS` das Feld als das Attribute „uid“ der ObjectClass „inetOrgPerson“ im hierarchichen LDAP Model dargestellt.

Und hier ein Auszug eines Join-Adapaters:

```
<join id="join1" version="38">
        <root>ou=edir,ou=prod,o=myorg</root>
        <active>true</active>
       <routing>
        ….
        <visible>Yes</visible>
       ….
        </routing>
       ….
        <primary>edir-myorg</primary>
       <bindTo>
        <adapter>edir-myorg</adapter>
        </bindTo>
       <joins>
       <joinrule>
        <jointo>myorgpoc</jointo>
        <type>com.octetstring.vde.join.SimpleJoiner</type>
        <joinon>cn=cn</joinon>
        </joinrule>
       …
 </join>
```

Der Adapter edir-prog wird als Primary-Adapter verwendet. Die Daten aus dem Adapter „myorgproc“ werden aggregiert, wenn die Join Rule wahr ist, in dem der Wert des Attributs „cn“ bei beiden Adaptern identisch ist.

Mit dem enorm flexiblen OVD-Filter und OVD Plugins kann man fast beliebige Logik bei der Datentransformation von den Adaptern zu dem LDAP Client realisiern.

Fazit

Durch die zahlreichen Features von OVD, ist es möglich, in relativ kurzer Zeit die Anforderungen der LDAP Clients wie Weblogic Server bzw. BPM Suite zu erfüllen und Daten aus einem zentralen Unternehmens-Directory mit Daten aus anderen LDAP/JDBC/WebService-Quellen anzureichern und als ein virtueller Eintrag zu präsentieren. Dadurch wird vermieden, das Applikation Schemata in den zentralen Directory Repositories gepflegt werden müssen. Darüber hinaus dient OVD als ein intelligenter LDAP Filter, der aufgrund bestimmter Kriterien jedem LDAP Client eine spezielle Sicht auf bestimmte Teilbäume des gesamten virtuellen Baumes zu zeigen. Dieses erhöht die Sicherheit des Gesamtsystems.

Refernzen

Oracle Business Process Management Overview
http://www.oracle.com/technetwork/middleware/bpm/overview/index.html

Oracle SOA Suite, Business Process Management Suite, and Web Services Documentation
http://docs.oracle.com/cd/E28280_01/soa.htm

Roles and Privileges for Oracle SOA Suite Users in Oracle Enterprise Manager
http://docs.oracle.com/cd/E28280_01/admin.1111/e10226/appx_roles_privs.htm#BABIHDFJ

Oracle Virtual Directory WhitePaper
http://www.oracle.com/technetwork/middleware/id-mgmt/virtual-directory-wp-129468.pdf

Kontaktadresse:

Oracle Deutschland B.V. & Co. KG
Kühnehöfe 5
D- 22761 Hamburg

Telefon:	+49 (0) 40-89091 624
Fax:	+49 (0) 40-89091 250
E-Mail	Abdi.mohammadi@oracle.com
Internet:	www.oracle.com