OBIEE 11g Integration mit Oracle Access Manager & MS Active Directory

Rico Haupt
Robotron Datenbank-Software GmbH
Dresden

Schlüsselworte
Oracle Fusion Middleware 11g, Identity- und Access-Management, Oracle Business Intelligence 11g, Oracle Access Manager, SSO

Einleitung
Die Durchsetzung von Sicherheitsrichtlinien für IT-Systeme in Unternehmen und Organisationen gewinnt weiterhin an Bedeutung, um Datenschutz und Compliance sicherzustellen. Ein integraler Bestandteil ist dabei das Identity- und Access-Management. Dabei geht es um die effektive Verwaltung von Benutzern und die Durchführung einer Zugriffskontrolle mit dem Ziel, dass nur berechtigte Personen Zugriff auf Anwendungen und Daten haben.
Der Vortrag handelt von einem Projekt zur Integration von Oracle Business Intelligence 11g Enterprise Edition in ein zentrales Identity- und Access-Management System bestehend aus Active Directory, Oracle Access Manager und Oracle Internet Directory inklusive Durchführung von Single Sign-on.

Vorstellung der beteiligten Oracle Komponenten
Oracle Business Intelligence (OBIEE) 11g:
Ist ein komfortables Reportingtool zur Erstellung von Analysen, Dashboards, Ad-hoc Abfragen, Scorecards und Nutzung von OLAP-Funktionalität.

Als zentraler Bestandteil ist wie bei Oracle Fusion Middleware 11g üblich der WebLogic Server. Er wird für die Bereitstellung der OBIEE-Webkomponenten und Security-Services genutzt. Dazu kommen weitere Komponenten wie der Bi Server und der BI Presentation Server, die außerhalb des WebLogic Server als C++ Prozesse bereitgestellt sind.

Oracle Internet Directory (OID):
Ist ein LDAP V3-konformer Directory-Server von Oracle. Er wird genutzt, um Benutzer- und Gruppeninformationen zu verwalten und bietet zusätzlich die Möglichkeit Daten mit anderen Verzeichnisdiensten zu synchronisieren. Es kann dabei sowohl die Quelle als auch das Ziel darstellen.

Oracle Access Manager (OAM):
Das strategische Oracle Produkt für das Access-Management erlaubt die Durchführung zentraler Zugriffskontrolle, Authentifizierung und Single Sign-on. Abbildung 1 zeigt die Komponenten, die der OAM umfasst.

Benutzer und Gruppeninformationen, die für die Zugriffskontrolle herangezogen werden, sind außerhalb in einem Verzeichnisdienst abgelegt. Für die Authentifizierung bietet er verschiedene Mechanismen wie z.B. Benutzername/Passwort, Kerberos, SSL. Für alle integrierten Web-Anwendungen bietet er Single Sign-on an.

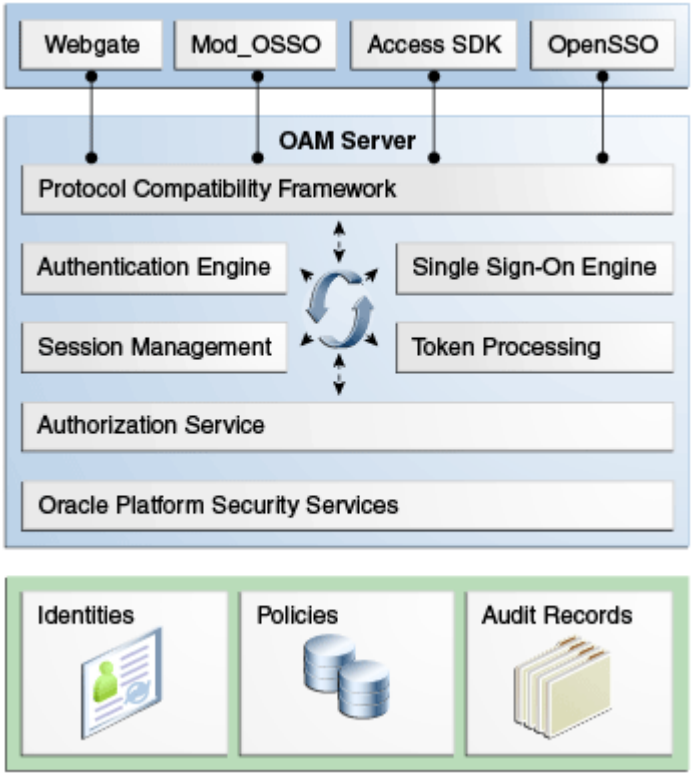


Abb. 1: Oracle Access Manager Komponenten und Dienste (Quelle: Oracle)

Konzept
Das OBIEE Security Konzept basiert auf Benutzern und Gruppen, die durch den WebLogic Server bereitgestellt werden. Standardmäßig basiert die Authentifizierung auf den Benutzern und Gruppen, die im WebLogic Server integrierten LDAP-Verzeichnis abgelegt sind.

Damit andere Mechanismen für die Benutzerauthentifizierung und Benutzeridentifizierung eingebunden werden können gibt es Authentication Provider.

Dabei lassen sich zwei Arten unterscheiden: Authentication Provider und Identity Asserter. Authentication Provider ermöglichen es transparent andere Systeme, wie Verzeichnisdienste oder Datenbanken, als Quellen für Benutzer und Gruppen einzubinden und darauf basierend die Authentifizierung durchzuführen.

Identity Asserter dienen dazu aus übergebenen Security Token die Benutzeridentität zu ermitteln. Die Authentifizierung wurde dabei von dritter Seite durchgeführt.

Ziel ist es die Benutzerbasis des Active Directory zu integrieren. Bei den vorhandenen Oracle Installationen wird bereits das OID eingesetzt. Das OID bietet die Möglichkeit Daten mit dem Active Directory zu synchronisieren. Dadurch sind die Benutzer zwar in zwei Verzeichnissen gespeichert, die Pflege erfolgt aber ausschließlich im Active Directory. Der Vorteil dabei ist, dass man Bedürfnisse von Oracle Anwendungen unabhängig vom Active Directory sicherstellen kann.

Für das Projekt bedeutet das schließlich:

Im OID muss die Synchronisation mit dem Active Directory eingerichtet werden. Die Integration mit der OBIEE-Instanz wird durch Anlegen eines OID Authentication Providers realisiert.

Das Access Manager WebGate stellt den Policy Enforcement Point dar, wird im Oracle HTTP Server (WLS Proxy) als Modul installiert und verhindert, dass nicht autorisierte Aufrufe an die Anwendungen weitergeleitet werden. Authentifiziert werden die Benutzer durch den Authentifizierungsmechanismus des Access Server.
Die Integration mit dem Oracle Access Manager erfolgt durch Nutzung des „Oracle Access Manager Identity Asserter“. Er basiert auf der Auswertung eines Security Tokens, dass durch den OAM Server erstellt wird und vom WebGate an dahinterliegende Komponenten weitergereicht wird.

Der schematische Ablauf beim Zugriff auf den WebLogic Server sieht dann wie folgt aus (siehe Abb. 2).

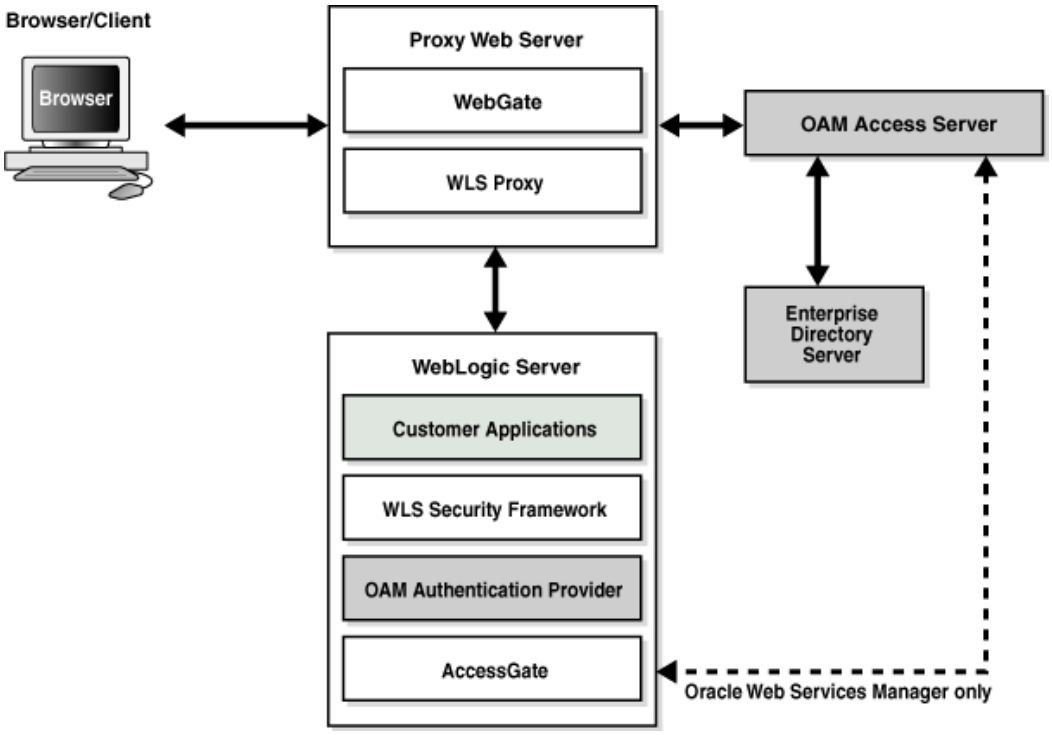


Abb. 2: Oracle Access Manager SSO für Web-Anwendungen (Quelle: Oracle)

Bereitstellung und Konfiguration von OBIEE
Die Software-Installation wird wie bei Fusion Middleware 11g üblich durchgeführt. Installiert werden folgende Komponenten:

- Oracle WebLogic Server 10.3.6
- Oracle Business Intelligence Enterprise Edition 11.1.1.7

Die Metadatenschemas werden in der vorhandenen Metadatendatenbank vom OID erstellt. Aus dem OBIEE Oracle Home heraus wird eine Instanz erstellt. Die Instanz nutzt nach der Erstellung ihren eigenen Authentifizierungsmechanismus auf Basis von Nutzername/Passwort. Als Identity Store dient das WebLogic-eigene LDAP-Verzeichnis.

Damit zusätzlich das Oracle Internet Directory als Identity Store verwendet werden kann, wird ein Authentication Provider mit folgenden WLST-Script angelegt.

```
DOMAIN_NAME='rdsbi_bifoundation_domain'

USERNAME='weblogic'

PASSWORD='password'

ADMIN_SERVER_URL='t3://localhost:7001'

REALM='myrealm'

PROVIDER_NAME='RDS_TESTOID_PROVIDER'

HOST='localhost'

PORT='7001'

USER_DN='cn=search,cn=users,dc=robotron,dc=de'

USER_PWD='password'

GROUP_BASE_DN='cn=rdsbi_bifoundation_domain,cn=groups,dc=robotron,dc=de'

connect(USERNAME,PASSWORD,ADMIN_SERVER_URL)

try:

        edit()

        startEdit()

        cd('/SecurityConfiguration/' + DOMAIN_NAME + '/Realms/' + REALM)

        cmo.createAuthenticationProvider(PROVIDER_NAME,
'weblogic.security.providers.authentication.OracleInternetDirectoryAuthenticator')

        cd('/SecurityConfiguration/' + DOMAIN_NAME + '/Realms/' + REALM +
'/AuthenticationProviders/' + PROVIDER_NAME)

        cmo.setControlFlag('SUFFICIENT')

        cmo.setUserNameAttribute('uid')

        cmo.setPrincipal(USER_DN)

        cmo.setCredential(USER_PWD)

        cmo.setHost(HOST)
```

```
        cmo.setGroupBaseDN(GROUP_BASE_DN)

        cmo.setUserBaseDN('cn=Users,dc=robotron,dc=de')

        cmo.setAllUsersFilter('(&(uid=*)(objectclass=person))')

cmo.setAllGroupsFilter('(&(cn=*)(|(objectclass=groupofUniqueNames)(objectclass=orclgroup)))')

cmo.setGroupFromNameFilter('(|(&(cn=%g)(objectclass=groupofUniqueNames))(&(cn=%g)(objectclass=
orclgroup)))')

        cmo.setUserFromNameFilter('(&(uid=%u)(objectclass=person))')

        save()

        activate()

except:

        undo('true','y')

        stopEdit('y')
```

Abbildung 3 zeigt das Anlegen des OAM Identity Asserter zur Verarbeitung der OAM Security Token mit der WebLogic Admin Console.

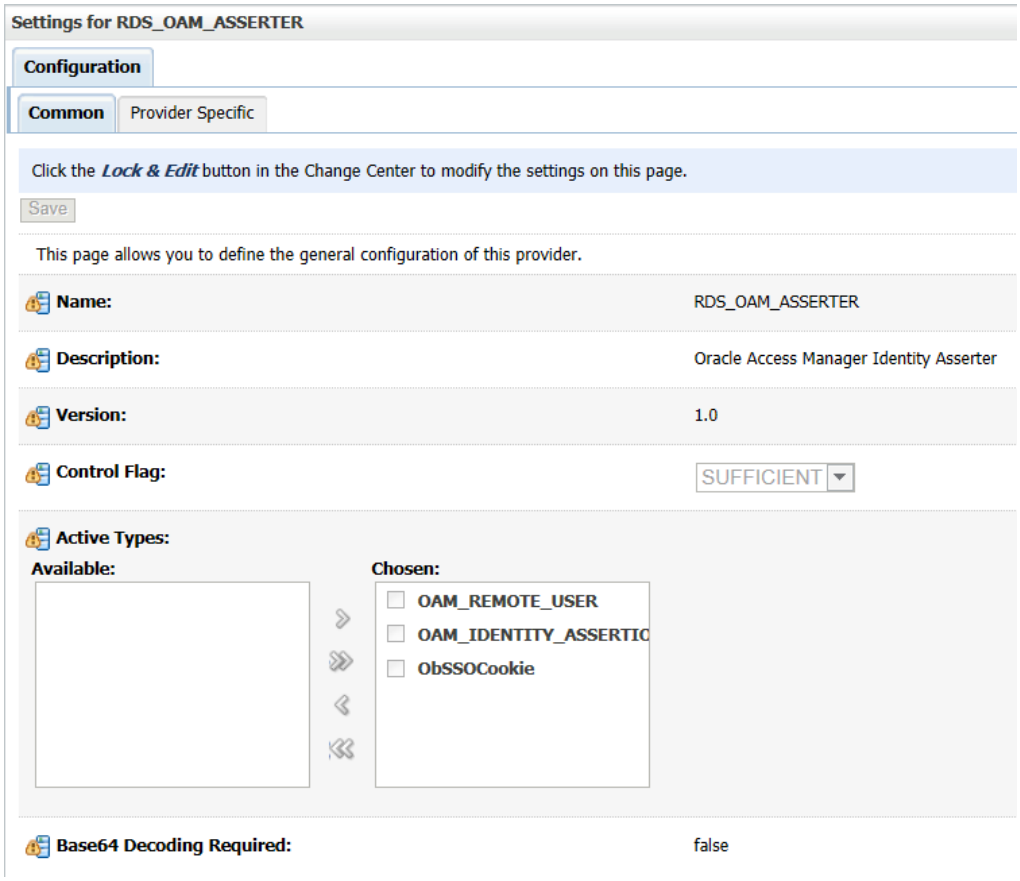


Abb. 3: Konfiguration des OAM Identity Asserter

Anschließend wird die richtige Abarbeitungsreihenfolge für die Provider festgelegt (Abb. 4). Die beiden standardmäßig eingerichteten „DefaultAuthenticator“ und „DefaultIdentityAsserter“ bleiben erhalten. Darüber werden die Benutzer für den Betrieb des Systems bereitgestellt, sodass auch ohne verfügbares OID die Instanz gestartet und verwaltet werden kann.

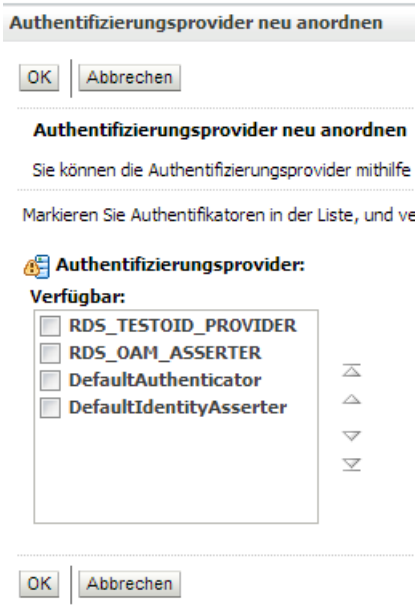
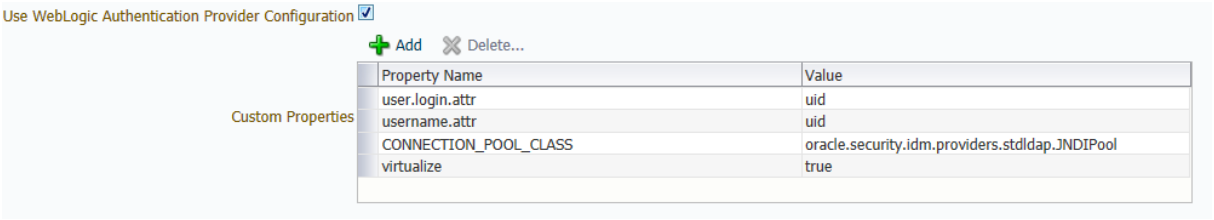


Abb. 4: Authentication Provider Reihenfolge

Damit OBIEE zusätzlich mit dem OID Identity Provider arbeiten kann, wird im Fusion Middleware Control die Identity Provider Konfiguration wie folgt vorgenommen werden.



Zur Aktivierung von SSO mit dem OAM für OBIEE muss noch folgendes aktiviert werden (Abb. 5).

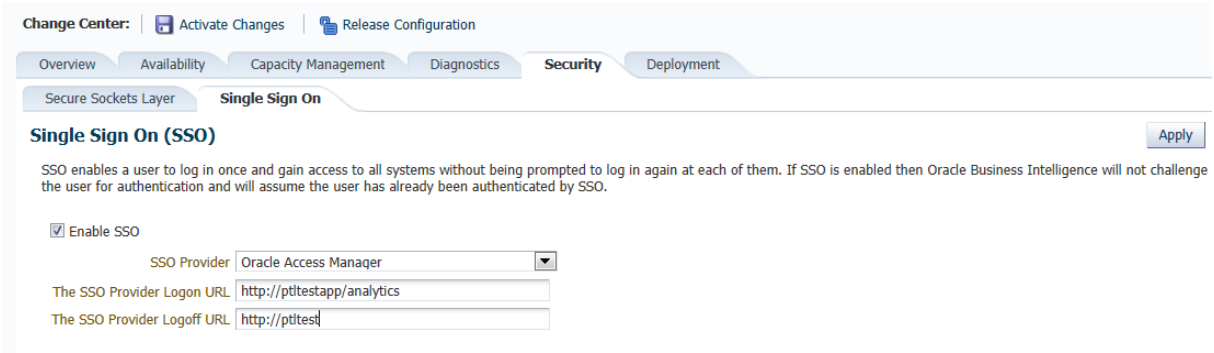


Abb. 5: OBIEE SSO Konfiguration

Bereitstellung von Oracle HTTP Server und OAM WebGate
Das WebGate, die Verbindung zum Access Manager und Policy Enforcement Point, wird im Oracle HTTP Server 11g bereitgestellt. Installiert wurde dafür Oracle Web Tier 11.1.1.7 in einem separaten Middleware Home. Davon wurde eine HTTP Server Instanz erstellt.

Der nächste Schritt ist die Installation des OAM WebGates in dieses Middleware Home.

Das WebGate wird in der OAM Console konfiguriert . Die Policy Domain soll für jeden Context Path gelten. Für die OHS-Instanz wird das WebGate dann wie folgt auf der Kommandozeile eingerichtet:

```
export MW_HOME=/opt/oracle/middleware_wt

export ORACLE_INSTANCE=$MW_HOME/user_projects/instances/rdsohs

export ORACLE_HOME=$MW_HOME/Oracle_OAMWebGate1

cd $MW_HOME/Oracle_OAMWebGate1/webgate/ohs/tools/deployWebGate/

./deployWebGateInstance.sh -w $ORACLE_INSTANCE/config/OHS/ohs1 -
oh $ORACLE_HOME

./EditHttpConf -w $ORACLE_INSTANCE/config/OHS/ohs1
```

Damit die Weiterleitung der Anfragen an den WLS HTTP-Port der OBIEE-Instanz erfolgen kann, wird die OHS-Konfiguration um folgende Direktiven erweitert.

```
<Location /analytics>

        SetHandler weblogic-handler

        WebLogicCluster    localhost:9704

        DynamicServerList OFF

</Location>

<Location /bicontent>

        SetHandler weblogic-handler

        WebLogicCluster    localhost:9704

        DynamicServerList OFF

</Location>

<Location /biofficeclient>

        SetHandler weblogic-handler

        WebLogicCluster    localhost:9704

        DynamicServerList OFF

</Location>
```

```
<Location /xmlpserver>

        SetHandler weblogic-handler

        WebLogicCluster    localhost:9704

        DynamicServerList OFF

</Location>
```

Synchronisation von Oracle Internet Directory und Active Directory
Die Synchronisation des OID mit dem Active Directory kann durch folgende Kommandozeilentools eingerichtet werden. Alternativ kann auch Fusion Middleware Control genutzt werden.

```
export ORACLE_HOME=/opt/oracle/middleware/oracle_idm1

cd $ORACLE_HOME/bin

./expressSyncSetup -h localhost -p 7005 -D weblogic -pf AD2OID -conDirType
ACTIVEDIRECTORY -conDirUrl AD_HOST:AD_PORT -conDirBindDN AD_USER -
conDirContainer cn=users,dc=robotron,dc=de -enableProfiles  true

./manageSyncProfiles update -h localhost -p 7001 -D WLS_login_ID -pf
AD2OIDImport -params "odip.profile.configfile
$ORACLE_HOME/ldap/odi/conf/activeimp.cfg.master"

./manageSyncProfiles updatechgnum -h localhost -p port -D weblogic -pf
AD2OIDImport
```

Nach Einrichtung des Synchronisationsprofils wird das Bootstrapping durchgeführt, um das OID mit den Benutzerdaten zu füllen. Das Bootstrapping kann wie folgt durchgeführt werden:

```
$ORACLE_HOME/bin/syncProfileBootstrap -host localhost -p 7005 -pf
AD2OIDImport -wlsuser weblogic -f
$ORACLE_HOME/ldap/odi/conf/ldf2ldf.properties
```

Damit bei einem „ldapbind" nicht das Passwort im OID-Benutzereintrag verwendet wird, sondern sein Active Directory Passwort, kann im OID das Externe Authentifizierungsplugin genutzt werden. Das kann mit folgendem Befehl eingerichtet werden.

```
export
CLASSPATH=$ORACLE_HOME/ldap/jlib/oidexcfg.jar:$ORACLE_HOME/ldap/jlib/ldapjc
lnt11.jar:$CLASSPATH
java -classpath $CLASSPATH oracle.ldap.extplg.oidexcfg -h localhost -p 389
-D cn=orcladmin -w password -t ad
```

Fazit
Oracle Business Intelligence Enterprise Edition11g lässt sich effektiv in ein Identity- und Access-Management System bestehend aus Active Directory, Oracle Internet Directory und Oracle Access Manager integrieren. Das Oracle Internet Directory fungiert dabei als Anwendungsbezogener Verzeichnisdienst für die Oracle Produkte. Die Benutzerverwaltung findet nur im Active Directory statt und es werden nur Änderungen mit dem OID synchronisiert.

Durch die Integration wird sichergestellt, dass eine einheitliche Infrastruktur für verschiedene Anwendungen in Unternehmen und Organisationen verwendet wird. Für OBIEE bedeutet das eine einheitliche Benutzerbasis, konsistente Authentisierungsdaten, die Realisierung von Single Sign-on sowie den Zugriff auf Unternehmens- bzw. Organisationsweite Rollen.

Kontaktadresse:
Rico Haupt
Robotron Datenbank-Software GmbH
Stuttgarter Straße 29
D-01189 Dresden

Telefon: +49 (0) 351-25859-2771
Fax: +49 (0) 351-25859-3696
E-Mail rico.haupt@robotron.de
Internet: www.robotron.de