Cloud Control , Single Sign On in Active Directory Umfeld

Abdi Mohammadi
ORACLE Deutschland B.V. & Co. KG
Hamburg

Schlüsselworte
Cloud Control, SSO, SPNEGO, Kerberos, Enterprise User Security, Web SSO, Oracle Access Manager, Oracle Unified Directory, Active Directory

Einleitung

Oracle Enterprise Manager Cloud Control (EMCC) wird bei Enterprises mit Oracle Lösungen sehr gern als das zentrale Monitoring und Management System eingesetzt. Mit der Software werden vor allem aber nicht nur Oracle Datenbanken, Application Servers und sonstige Systeme überwacht bzw. Administriert. Auf die zu überwachenden Target Systeme werden die sogenannten Enterprise Manager Agents installiert, um Systemparameters und Status an den zentralen Server zu senden.

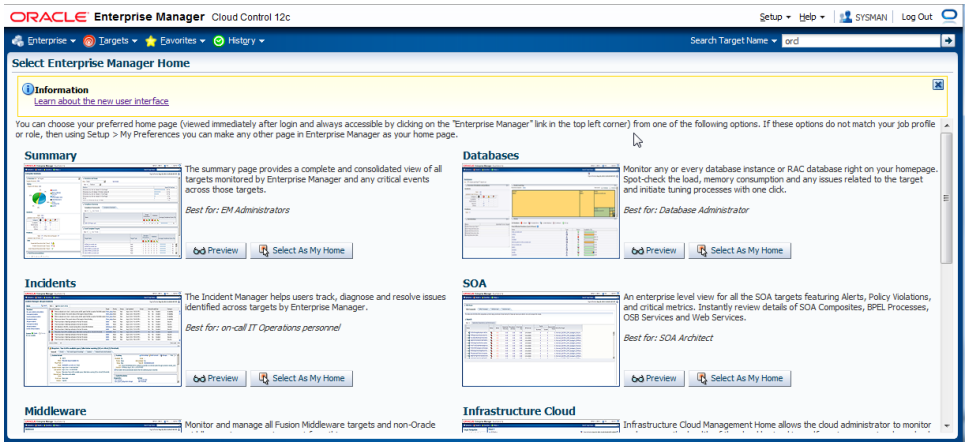

Abb. 1:EMCC Console

Die Administrationsoberfläche von EMCC wird über die üblichen Browser erreicht. EMCC verfügt über eine eigene Benutzerverwaltung. So können Systemadministratoren mit unterschiedlichen Privilegien erstellt werden. Diese Benutzer können sich dann an der EMCC Oberfläche authentisieren und je nach vordefinierten Autorisierung (Rollen und Privilegien) Target Systeme überwachen oder aber auch administrieren.
Während die Authorisierungs-Regeln von EMCC selbst überprüft werden, kann das Authentisieren der Benutzer extern erfolgen.

```
[oracle@em12c bin] $ ./emcli create_user -name=abdi  -type=EXTERNAL_USER
```

Dieses Kommando erzeugt einen User in dn der View SYSMAN.GC_USERS der Datenbank Instanz „EMREP“. Die EMCC Rollen sind dann in der View SYSMAN.GC_USER_ROLES definiert.

Dabei vertraut EMCC auf die im Weblogic Server konfigurierten Authentication/Assertion Providers. Auch der eigene Authentication Provider von EMCC „EM Repos Authentication Provider“ wird bei der Installation der Software in Weblogic Server eingebaut.

Dieser Provider verwendet den eingebetteten „libOVD“ um zwei LDAP Teilbäume über den JDBC Adapter von libOVD bereitzustellen.
Während SYSMAN.GC_USERS mittels ObjectClass „inetOrgPerson“ unter cn=emusers,dc=oracle,dc=com zur Verfügung steht, wird SYSMAN.GC_USER_ROLES mittels ObjectClass „GroupOfUniqueNames“ unter cn=emroles,dc=oracle,dc=com dargestellt.

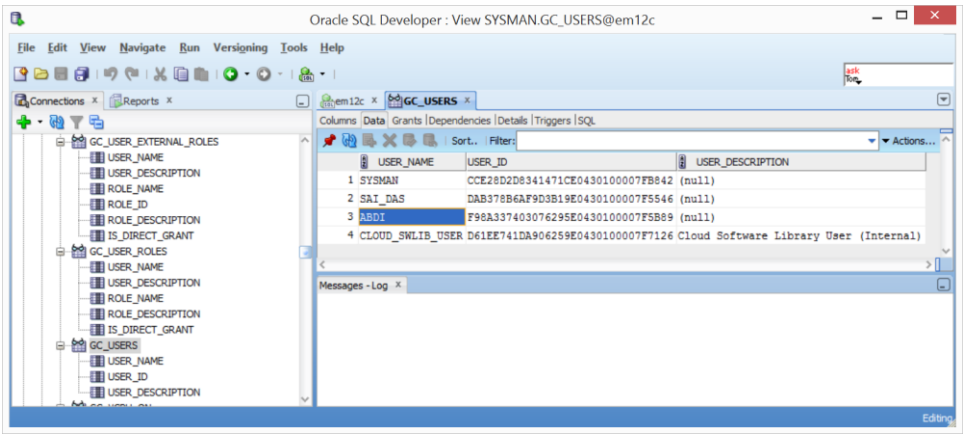

Abb. 2 EMCC Create User

Somit ist es kein Problem andere von Weblogic Server offiziell unterstützten aber auch Custom Authentication Providers einzusetzen. Das sind in der Regel zentrale Directory Servers, Access Management sowie Kerberos oder Federation Lösungen.

In Enterprises mit Windows Clients ist Active Directory als zentrales Identitiy Store vorhanden.
Mit SPNEGO (Simple and Protected GSSAPI Negotiation Mechanism) wird ein Verfahren eingesetzt, um bei Zugriff auf Web Applikationen ein automatische Single Sign On zu erreichen. So kann der bei Active Directory angemeldete User mittels Browsers auf Applikationen zugreifen, ohne erneut nach Password gefragt zu werden. Die Voraussetzung ist, dass die Applikation WNA (Windows native Authentication) basiert auf SPNGEO unterstützt und der Browser für NWA konfiguriert ist. Hier das Beispiel für Firefox:

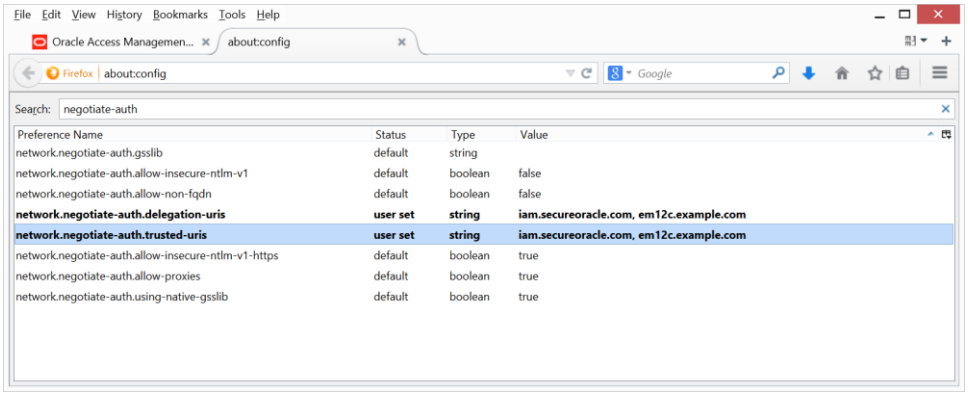

Abb. 3: Firefox Configuration for NWA

Weblogic Server und Oracle Access Manager beide unterstützen WNA und können daher in Verbindung mit EMCC eingesetzt werden.

Zwecks Authentisierens unterstützt EMCC grundsätzlich drei unterschiedliche Methoden:

1. User/Password von EMCC eigener Benutzerverwaltung (EM Repos Authentication Provider)
2. User/Password von einem externen Directory Server (z.B. Oracle Unified Directory)
3. Single Sign On über Identity Asserter (z.B. Oracle Access Manager SSO Token, oder Weblogic Server Kerberos Token).

EMCC unterstützt entweder Web Single Sign On über externe Identity Asserter oder Single Sign On zwischen EMCC und den Target Databases mit Hilfe von Enterprise User Security (EUS). Leider ist es nicht möglich, die beiden Methoden zu kombinieren.
Im Falle von WebSSO reicht es aus, wenn der jeweilige Identity Asserter von Weblogic Server (z.B. Oracle Access Manager oder NegotiateIdentityAsserter) den UserNamen an EMCC weiterleitet und der entsprechende User in einem der verwendeten Identity Provider (User in Directory Server) referenziert werden kann. In den weiteren Abschnitten wird erklärt, wie dies in Verbindung mit WNA über Oracle Access Manager oder Weblogic Server alleine erreicht werden kann.

Beim Einsatz von EUS jedoch muss sich ein Directory User mit User/Password in EMCC's Administrationsoberfläche anmelden. Beim Zugriff auf die Target Databases wird ein automatisches SSO realisiert. Die Voraussetzung dazu ist, dass sämtliche Target Databases inklusive von EMREP (Database Instance von EMCC selbst) für EUS konfiguriert sind.

Web Single Sign On mit Active Directory und anderen Web-Applikationen

Oracle Access Manager ist eine Komplettlösung, um die Zugriffe auf geschützten Applikationen zentral zu steuern. Die Applikationen werden durch die sogenannten Webgates geschützt. Die nachfolgende Abbildung zeigt den Informationsfluss und die Abläufe bei einem Zugriff:

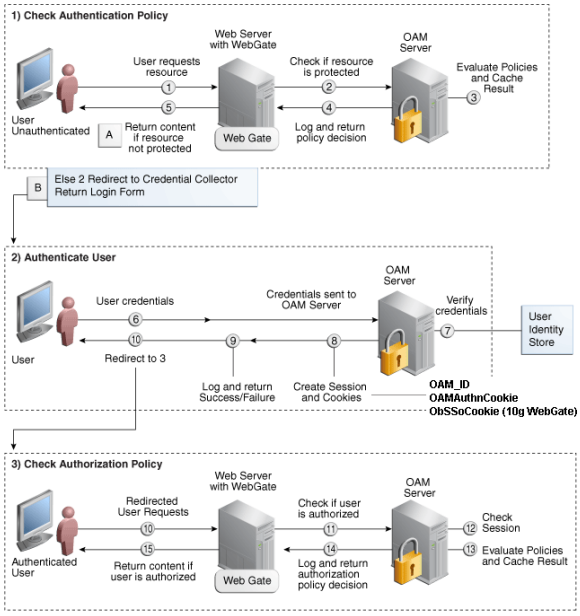

Abb. 4: Request Flow

Beim ersten Zugriff des Benutzers checkt das Webgate, ob die Ressource geschützt ist. Falls nicht, dann wird die Seite dem Benutzer gezeigt.

Wenn die Ressource als geschützt deklariert ist, wird der Benutzer zwecks Authentisierung auf die Login-Seite des Access Managers umgeleitet. Die Verifikation des Benutzer Passwords übernimmt das jeweilige konfigurierte Authentication Modul gegen eine User Store wie z.B. Active Directory.

Nach der erfolgreichen Authentisierung wird eine Session generiert und die entsprechende Security Tokens ausgestellt, die über Cookies an den Benutzer geschickt werden.
Der Benutzer wird dann auf die geschützte Seite bzw. Webgate zurückgeschickt. Diese erkennt anhand des Security Tokens, dass der Benutzer authentisiert ist und prüft nun, ob die angeforderte Ressource für diesen Benutzer freigeschaltet ist (Autorisierung). Falls ja, wird der Zugriff auf die Ressource erlaubt. Dabei kann das Webgate bestimmte User-Profil Informationen in der Form von HTTP_HEADER, Session Attribute oder Cookies an die Applikation weiterleiten.

Um OAM in einer Windows Umgebung effektive einzusetzen, wird der Kerberos Authentication Module (Das Modul für SPNEGO/Kerberos) eingesetzt.
So wird einem Browser die Möglichkeit gegeben, anstatt User/Password das Kerberos Ticket des angemeldeten Windows User in ein SPNGEO Mantel an den OAM Server zu schicken.

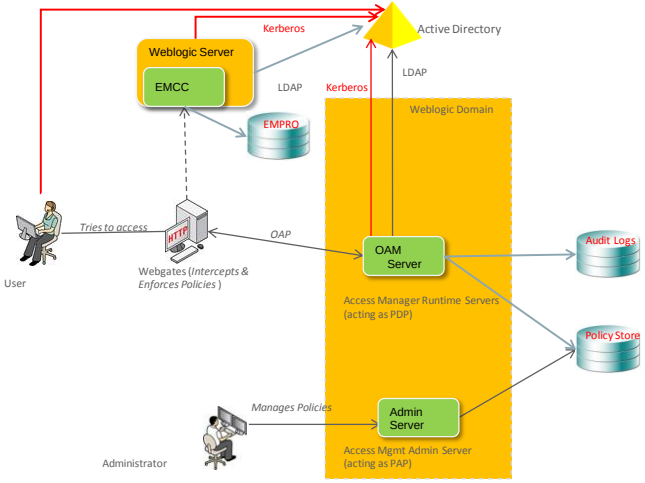

Abb. 5: SPNEGO with Oracle Access Manager

OAM verifiziert das Kerberos Ticket, extrahiert daraus den UserPrincipal, sucht sich den entsprechenden User im Identity Store und erzeugt ein User Session. Ein SSO Token wird erzeugt und an den Browser zurückgeschickt. Das SSO Token wird vom „Oracle Access Manager Identity Asserter“ des Weblogic Servers (Container für EMCC Server) verifiziert und daraus der UserPrincipal extrahiert und an EMCC weitergegeben. EMCC verifiziert diesen User gegen seine interne User Repository bzw. Externe Directory Server, die als Authentication Provider in Weblogic Server konfiguriert sind.
Die entsprechende Konfiguration der Authentication/Assertion Providers auf dem Weblogic Servers von EMCC sieht dann wie folgt aus:

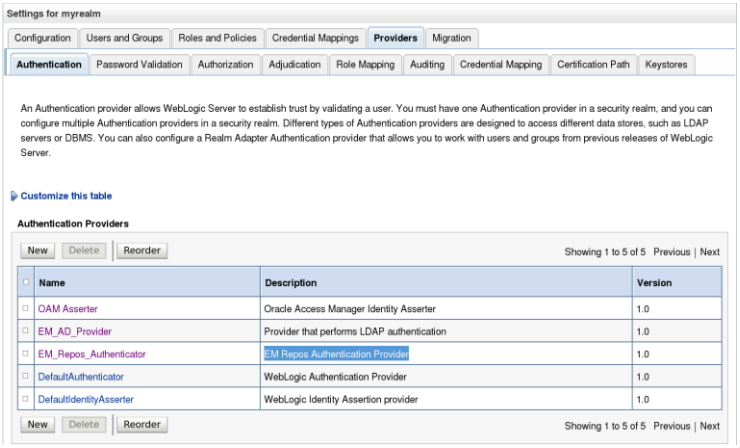

Abb. 6: Weblogic Server Authentication/Assertion Providers

Als eine Alternative zu der obigen Lösung kann eine einfache Single Sign On mit Active Directory auch ohne Oracle Access Manager erreicht werden. Hierzu muss man anstatt „Oracle Access Manager Identity Asserter“ den in Weblogic Server vorhandenen „NegotiateIdentityAsserter“ einsetzen. Die Architektur ohne den OAM Server und das Webgate sieht dann viel einfacher aus.

Dabei verzichtet man aber auf allen Vorteilen eines zentral Access Management Systems wie Session Management und Policy Store.

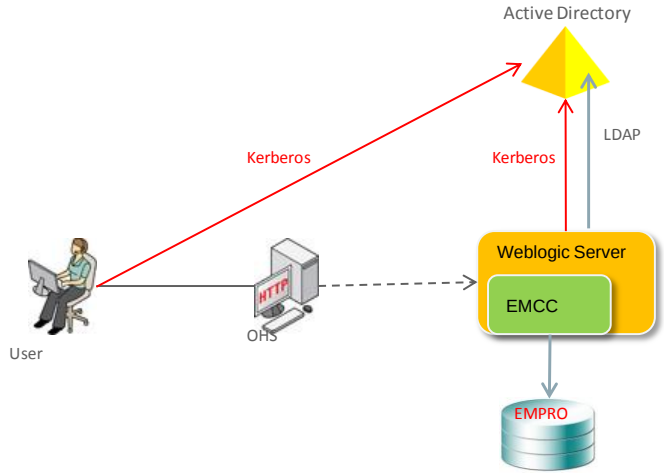

Abb. 7: Single Sign On between EMCC and Active Directory

Die entsprechende Provider Konfiguration auf dem Weblogic Server sieht dann so aus:

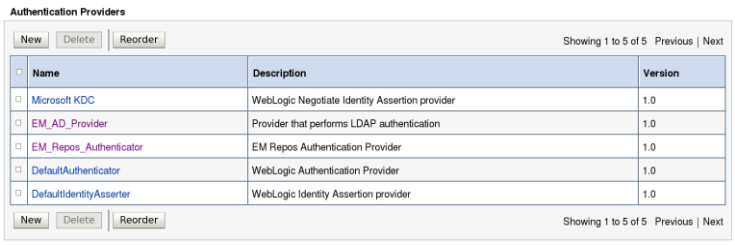

Abb. 8: Weblogic Server Authentication/Assertion Providers

Die detailierte Konfiguration der beiden Alternativen wird in dem Vortrag ausführlich behandelt.

Enterprise User Security

Bei den größeren Unternehmen müssen wenige DBAs einige hundert wenn nicht tausende Datenbanken administrieren. Historisch gesehen wird für ein und denselben Administrator in jeder Datenbank entsprechende User samt Password erstellt. Der Administrator muss sich dann für jede Datenbank ein Password merken. Alternativ verwendent man auch den OS Benutzer als einen gemeinsam genutzten Account, der von unterschiedlichen Personen benutzt wird.
Dadurch wird es jedoch schwer genauer nachzuvollziehen, welche Person, was, auf welcher Datenbank gemacht hat. Um einen einfacheren personalisierten Zugang zu Oracle Datenbanken zu ermöglichen wird Enterprise User Security verwendet.

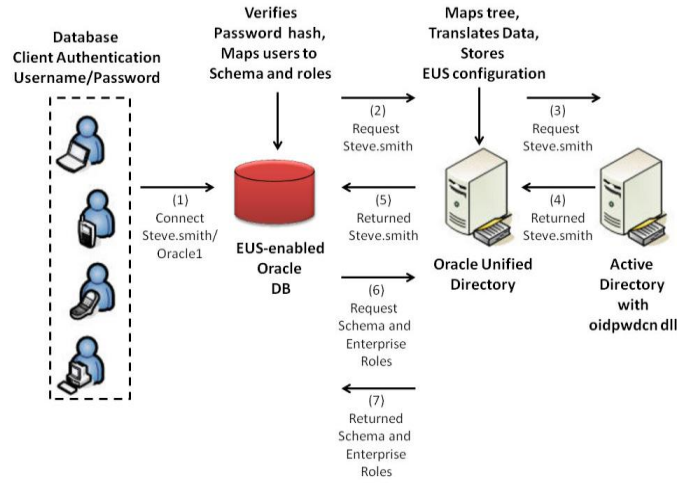

Abb. 9: OUD as Enterprise Security Proxy to Active Directory

Dabei greifen alle Datenbanken auf einen zentralen Server als Identity Store. Jeder DBA kann sich dann mit einem einzigen Directory Server User/Password bei allen ihm zugeteilten Datenbanken anmelden.
EMCC unterstützt EUS, um ein SSO zwischen EMCC und Target Databases zu realisieren. Bei so einer Konfiguration müssen alle als Target bei EMCC registrierten Datenbanken und die EMCC Datenbank selbst (EMREP) für EUS konfiguriert werden. Der DBA loggt sich dann mit seinem User/Password auf EMCC Login Seite und kann dann auf unterschiedliche Target Databases zugreifen und sie administrieren, ohne sich in die Target Databases nochmal einloggen zu müssen.
Um die in Active Directory vorhanden Users für EUS verwenden zu können, muss das Schema auf Active Directory um EUS Schema erweitert werden. Zusätzlich wird eine „Password Change Notification Change DLL“ auf die Domain Controllers installiert, um die Nutzerpasswörter in ein alternatives Attribute in einer gehashten Form (MD5 oder SHA-1) zu speichern. Dieses Attribut wird dann von EUS zur Verifizierung des UserPassword verwendet.
EUS kann nicht direkt auf Active Directory als Directory Server Backend zugreifen. Als ein EUS/Proxy wird der Oracle Unified Directory Server eingesetzt. OUD speichert dann die Enterprise Domain Informationen (Rollen, Administrationsgruppen, Proxy Users, usw.) in seinen lokalen Datenbanken. Lediglich die User-Einträge von DBAs werden aus Active Directory gelesen.

EUS kann auch anstatt über User/Password mit Kerberos Authentisierung verwendet werden, wenn man aus der Windows Umgebung direkt auf die Zieldatenbanken zugreifen möchte.
Ein SSO mit EMCC funktioniert jedoch nur, wenn man sich bei EMCC mit User/Password anmeldet.
In diesem Vortrag wird einen tieferen Überblick über diese Konfigurationsmöglichkeit gegeben.

Kontaktadresse:
Abdi Mohammadi
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.de