Die wichtigsten Punkte der Single Sign-On Konfiguration mit Oracle Access Manager

Alexander Bertman
Jon Erik de Linde
PITSS GmbH
Stuttgart

Schlüsselworte
Single-Sign-On, SSO, Oracle Access Manager, OAM, WebLogic Server,

Einleitung
Wie schön könnte doch die Welt sein. Ein Logon und schon kann man alle zugeteilten Ressourcen nutzen. Schließlich habe ich doch nur eine Identität! Doch nicht nur diese Gedanken treiben viele Unternehmen in die Single Sign-On Arme. Themen wie zentrale Benutzerverwaltung sind oft die Treiber solcher Projekte. Klare Kosteneinsparungen für Support, Wartung und Management sind dann der Lohn für solche nicht ganz einfachen Vorhaben. Zusätzlich können wir so noch eine höhere Sicherheit und eine bessere Benutzbarkeit erreichen. Doch was ist überhaupt Single Sign-On? Wie kann ich dies in meiner konkreten Oracle-Umgebung umsetzen?

Sicherheitsprobleme entstehen meist aufgrund komplizierter, breitverteilter und heterogener Umgebungen. Die Schwachstelle bei den Authentisierungsmethoden ist meistens das Passwort. Probleme bereitet hauptsächlich das Passwort wählen, benutzen, speichern, ändern, versenden, verwalten und löschen.

Heutige Unternehmen unterhalten eine Vielzahl von Applikationen und transparent nutzbarer Dienste wie zum Beispiel Mail, HR-Applikationen, Zeiterfassung, Webanwendungen, Netzwerkressourcen, Foren usw. Gleichzeitig erwarten sie vom „einfachen“ Benutzer, mehrere unterschiedliche und sichere Passworte zu wählen und zu merken (Sicher heißt beim Passwort: kompliziert und lang). Was daraus entsteht liegt vielfach auf der Hand:

- Einfache Passwörter werden gewählt
- Sichere Passwörter sind schwierig zum merken und werden „irgendwo“ aufgeschrieben
- Sichere Passwörter verursachen viele Anfragen beim Helpdesk (Passworte vergessen)

Single Sign-On kann da Abhilfe schaffen. EIN „sicheres“ Passwort sollte sich jeder merken können.

Single Sign-On: Vorteile

Für die Benutzer:
- Einfache Authentifikation:
  - Nur ein Passwort merken
  - Ein sicheres Passwort kann gewählt werden
  - Authentifizierungsdaten können auf einem Hardware-Token gespeichert werden
- Effizientes Arbeiten
  - Zugriff zu allen berechtigten Systemen ist automatisch vorhanden
  - Einfache Zusammenarbeit zwischen einzelnen Applikationen
- Zertifikatsverwaltung
  - Automatische Überprüfung der CRL (Certificate Revocation List)
  - Automatische Schlüssel- und Zertifikatserneuerung

Für die Administration:
- Reduzierung der administrativen Kosten:
  - Die Benutzerverwaltung ist einheitlich und zentral gelöst
  - Weniger Supportanfragen wegen vergessenen Passwörtern
- Höherer Sicherheitslevel
  - Verwendung von starken Passwörtern für Netzwerk-Zugriffe
  - Das Sperren von Usern im Directory hat auf allen Systemen sofortige Wirkung
  - Verschlüsselte Verbindungen zu allen Ressourcen

Die wichtigsten Punkte der Single Sign-On Konfiguration mit Oracle Access Manager

Eine mögliche Single-Sing-On Lösung für Oracle Forms bietet seit der Version Forms 11g R2 die Verwendung vom Oracle Access Manager. Um eine betriebsfähigen Umgebung zu erhalten gehören mehreren Produkte und Konfigurationen welche zusammenspielen müssen.

Als Betriebssystem für unsere Beispiel wählen wir Red Hat Linux 5.5 64-bit.

Wichtig:

- Wir prüfen zuerst, dass diese Betriebssystem und alle Paketen für die Installation verfügbar sind (überprüfen sie die Oracle Voraussetzungen).
- Firewall ausschalten. Nach der Installation können wir die Firewall wiedereinschalten und alle Ports, die wir verwenden, in Ausnahme hinzufügen.
- Die IP-Adresse muss statisch sein.

Wenn wir eine Umgebung mit OSSO (basierte auf 11g Versionen) auf Linux 64-bit aufbauen möchten, werden folgende Softwarekomponenten benötigt:

1. JDK (1.6.0_24 oder höher).
2. Datenbank (11.2.0.1 oder höher)
3. RCU (Repository Creation Utility 11.1.1.5.0)
4. Web Logic Server (10.3.5)
5. Oracle Internet Directory
   Oracle Identity Management (11.1.1.2.0 + Patch 12395123)
6. Oracle Business Intelligence 11g 11.1.1.5.0 (muss sein, wegen Oracle Identity and Access Management).
7. Oracle Identity and Access Management (11.1.1.5.0)
8. Oracle Web Tier Utilities 11g (11.1.1.2.0 + Update (11.1.1.5.0))
9. Oracle Access Manager OHS 11g Webgates (11.1.1.5.0)
10. Oracle Application Server (Forms & Reports) 11.1.2.0.0 + OHS Patch 12632886

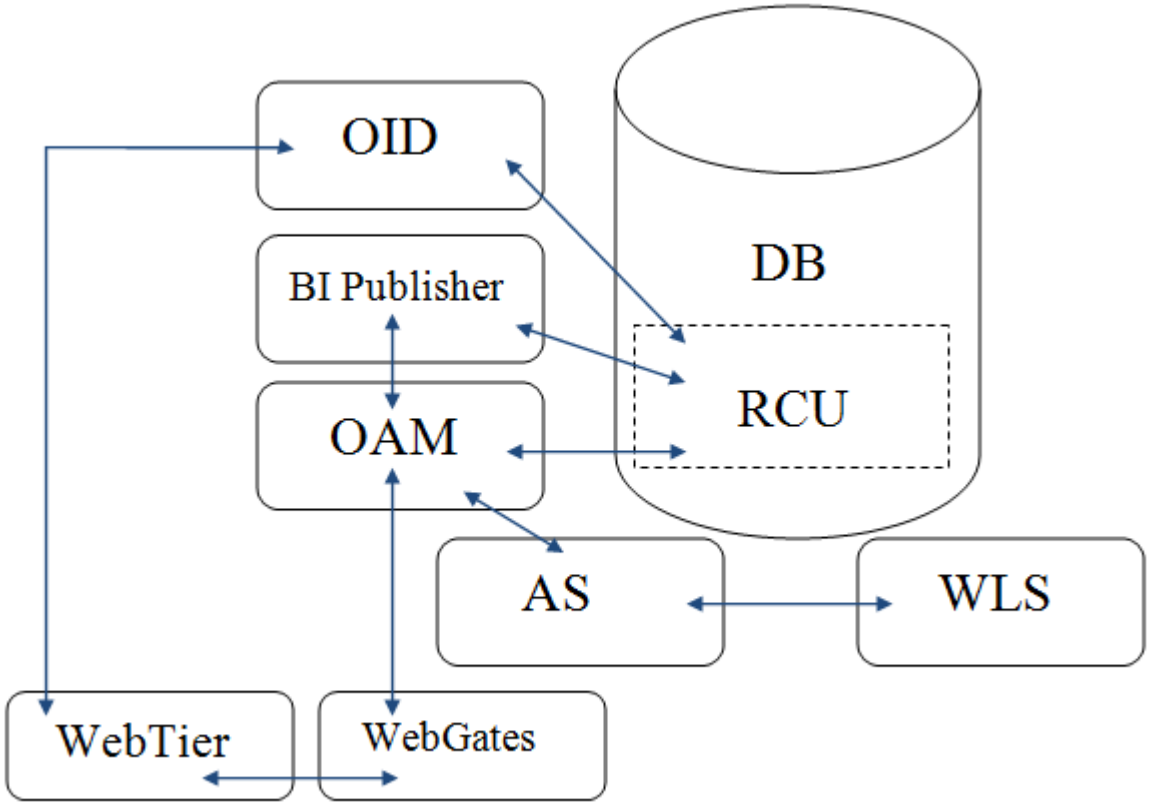

Abb. 5: Unser OSSO-Model

Wichtige Punkten in der Installation
Wir installieren alle benötigten RPM-Paketen, die Sie in Oracle Voraussetzungen Dateien finden könnten.
Wenn das Betriebssystem auf Fremdsprache ist, die wir nicht wissen, dann sollen wir den Parameter NLS_ENABLE=TRUE mit NLS_ENABLE=FALSE in der Datei oraparam.ini ersetzen.
Wenn die Sprache des Betriebssystems japanische ist und wir wissen diese Sprache nicht, dann sollen wir den Parameter NLS_ENABLE=TRUE mit NLS_ENABLE=FALSE in der Datei oraparam.ini ersetzen. Im diesen Fall nehmen wir statt der Sprache des Betriebssystems die Standardeinstellungssparache (Englisch).

Für die Installation wählen wir Java Developer Kit (JDK) 1.6.0_29 64-bit.

Bevor wir DB Installation starten, müssen wir die Umgebungsvariablen erstellen:
- ORACLE_HOME
- ORACLE_SID
- PATH
- SHLIB_PATH
- LIBPATH
- LD_LIBRARY_PATH
- DISPLAY
- TMP

- TMPDIR
- TNS_ADMIN

Wir installieren RCU (Repository Creation Utility 11.1.1.5.0) und WebLogic Installation (10.3.5) Danach starten wir die Installation Oracle Identity Management (Oracle Internet Directory). Am Anfang installieren wir 11.1.1.2.0 ohne Konfiguration und dann starten wir die Installation des Patches 12395123. Danach können wir Konfiguration ausführen. Wenn Installation und Konfiguration erfolgreich abgeschlossen wurden, sollen wir den Port des Admin Server OID ändern. Das müssen wir machen, wenn wir unsere Anwendung mit Enterprise Manager, Console im Zukunft verwalten wollen. Dann sollen wir das Skript inspre11.pl mit Parameter -op1 ausführen. Dieses Skript wird anonyme Verbindung in Oracle Internet Directory (OID) aktivieren und Oracle Application Server Metadata Repository Creation Assistant (OracleAS RepCA) erlauben, ein Schema in DB für Oracle Single Sign-On and Oracle Delegated Administration Services zu laden

Nächster Schritt ist die Installation des Oracle Business Intelligence 11g 11.1.1.5.0. Diese Software müssen wir wegen "Oracle Identity and Access Management" installieren. Bei Konfiguration Schritt wählen wir nur "BI Publisher" für die Installation.

Dann können wir die Installation "Oracle Identity and Access Management (11.1.1.5.0)" anfangen. Normalerweise starten wir die Installation in Linux mit `./runInstaller`, aber in dieser Situation sollen wir noch einen Parameter hinzufügen (`./runInstaller -jreLoc $JAVA_HOME`). Der Konfigurationsprozess des OIAM starten wir mit `../Oracle_IDM1/common/bin/config.sh`.

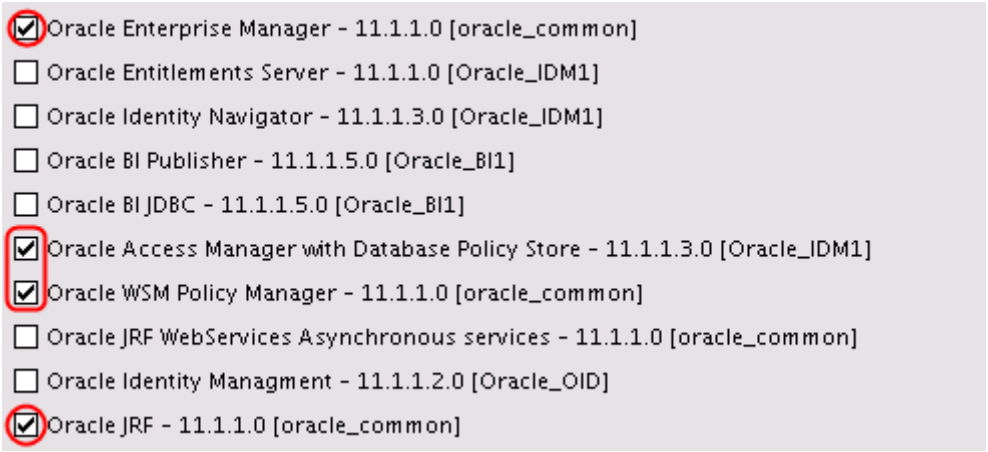

Abb. 6: Konfiguration des OIAM

Mit der Domain des OIAM Erstellung wählen wir die folgende Produkten:

- Oracle Access Manager with Database Policy Store - 11.1.1.3.0 [Oracle_IDM1]
- Oracle Enterprise Manager - 11.1.1.0 [oracle_common],
- Oracle WSM Policy Manager - 11.1.1.0 [oracle_common]
- Oracle JRF - 11.1.1.0 [oracle_common]

Wir wollen OSSO mit OAM und OID konfigurieren, deswegen wählen wir nur Oracle Access Manager ohne Oracle Identity Manager.

Wir installieren "Oracle Web Tier Utilities 11g (11.1.1.2.0)" mit dem Update (11.1.1.5.0). Die Installationsschritte sind fast gleiche so wie für OID. Wir starten zweimal die Installation ohne

Konfiguration und danach konfigurieren die Komponenten. Wir assoziieren Web Tier mit WebLogic Domain des OID.

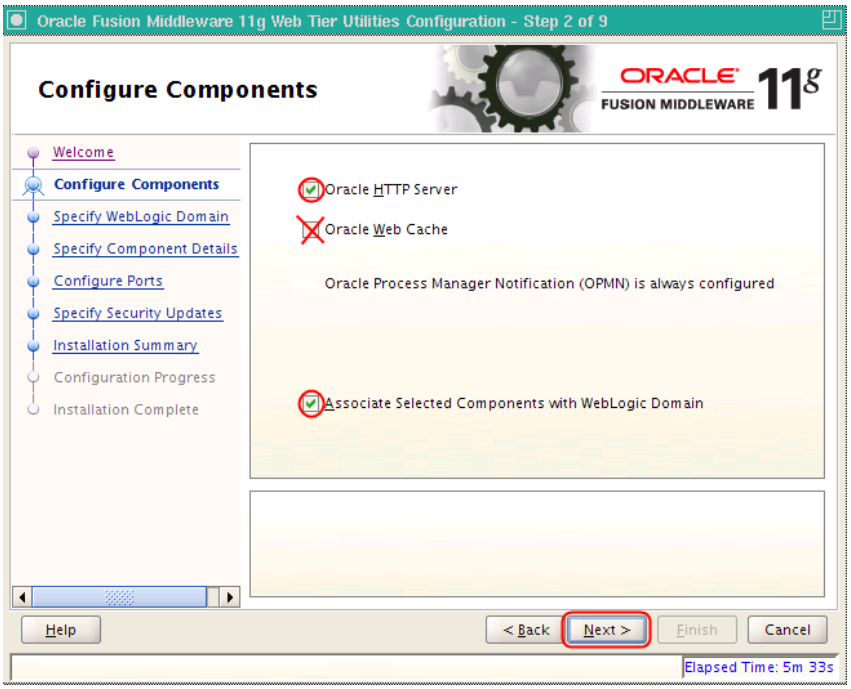

Abb. 7: Konfiguration des Web Tier

Nächster Schritt ist die Installation des Oracle Access Manager OHS 11g Webgates (11.1.1.5.0). Normalerweise starten wir die Installation in Linux mit `./runInstaller`, aber in dieser Situation sollen wir noch einen Parameter hinzufügen (`./runInstaller -jreLoc <WebTier_Home>/jdk`).

Das letzte was wir installieren sollen ist "Oracle Application Server (Forms & Reports) 11.1.2.0.0" mit OHS Patch 12632886.
Am Anfang installieren wir 11.1.2.0.0 ohne Konfiguration und dann führen wir die Konfiguration aus. Bei Konfigurationsphase des AS sollen wir die Verbindungen zwischen AS - OID -OAM einrichten.

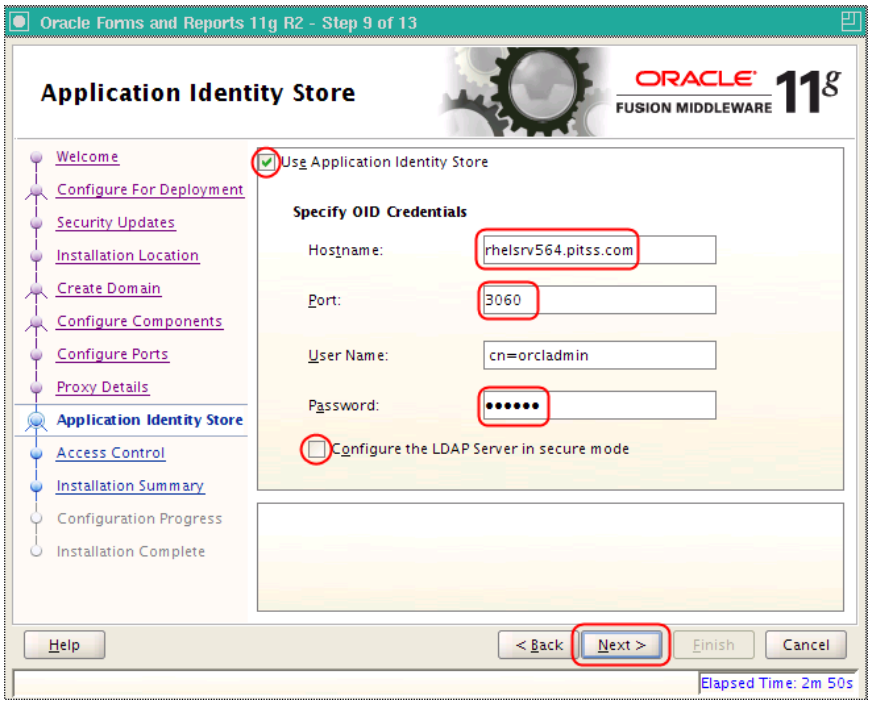

Abb. 9: Konfiguration AS 11gR2: Application Identity Store

Abb. 10: Konfiguration AS 11gR2: Access Control

Oracle Access Manager und OID Einstellungen

Policy Configuration Einstellungen

Wir fügen eine neue Operation ein, so dass die WebGate die Benutzeranmeldung mit OSSO kontrollieren können.
Bei diesem Schritt sollen wir in OAM Konsole anmelden. Standardmäßig können wir den Oracle Forms Hostname und den Port in #####_RREG_OSSO Host Bezeichner finden. Wir kopieren Hostname und löschen den. Danach machen wir einen Doppelklick auf OAM11gHostId Host Bezeichner und fügen den Hostname für unsere Forms Applikation mit dem Port 8888 ein.
Dann konfigurieren wir LDAPSchema (wegen Java Ausnahmen):

```
ssoCookie=disablehttponly
```

Die Application Domains verwalten Authentifizierung und Autorisierung Policies. Um die Antwort hinzuzufügen, klicken wir auf Application Domains -> OAM11g_WebGate -> Authentication Policies -> Protected Ressource Policy und schreiben wir:

```
Name: osso-subscriber-dn
Type: Header
Value: dc=pitss,dc=com
```

Erstellung des Resource Access Descriptors
Zuerst starten das Skript, um den Wert `orclownerguid` zu bekommen.

```
ldapsearch –h oam_server_host_name.domain.com –p 3060 –D cn=orcladmin –w
password_for_cn=orcladmin –b “cn=Extended Properties,cn=OracleContext” –s
one “objectclass=*” dn orclownerguid
```

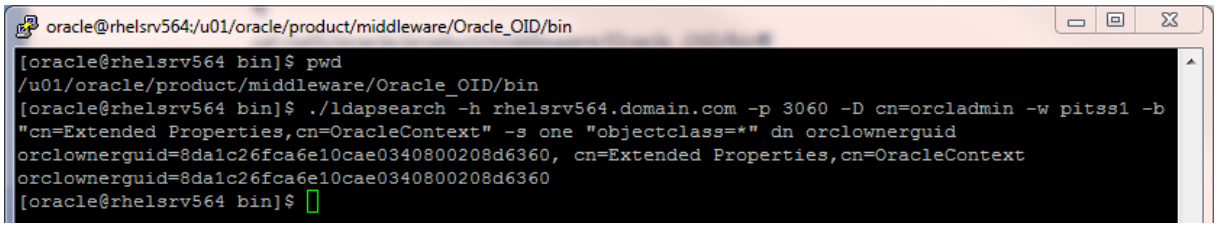

Abb. 11: Resource Access descriptor

Auf dem Forms Server erstellen wir eine LDIF Datei mit bestimmte Werte:

```
dn: orclresourcename=app+orclresourcetypename=OracleDB, cn=Resource Access
Descriptor , orclownerGUID= value_of_orclownerguid, cn=Extended Properties
, cn=oraclecontext, dc=pitss, dc=com
orclresourcetypename: OracleDB
orclflexattribute1: Forms_DB_SID
orcluseridattribute: Forms_username
orclownerguid: value_of_orclownerguid
orclusermodifiable: true
orclpasswordattribute: Forms_password
orclresourcename: app
objectclass: top
objectclass: orclresourcedescriptor
```

Dann starten wir das Skript:

```
ldapadd –h oam_server_hostname.pitss.com –p 3060 –D cn=orcladmin –w
password_for_cn=orcladmin –f test.ldif
```

Nächsten Schritt ist - wir loggen uns zur ODSM Konsole. Dort konfigurieren wir in Data Browser Tab Resource Access Descriptor. Wir klappen eine Baumansicht aus:
`dc=com, dc=domain, cn=OracleContext, cn=Extended Properties, orclownerguid=#######, cn=Resource Access Descriptor`

Das war fast alles über OAM Konfiguration. Es ist selbstverständlich, dass Sie müssen schon konfigurierte OID haben.

Für Test die Anwendung sollen wir so machen:
`http://machine_name:8888/forms/frmservlet?config=app&form=testparam`

Kontaktadresse:
Alexander Bertman
Jon Erik de Linde
PITSS GmbH
Zettachring 2
D-70567 Stuttgart

Telefon:	+49 (0) 711-72 87 5213
	+49 (0) 711-72 87 5205
Fax:	+49 (0) 711-72 87 5201
E-Mail	abertman@pitss.de
	edelinde@pitss.de
Internet:	www.pitss.com