SharePoint-Integration von OBIEE

Frank Weyher und Dr. Götz Gleitsmann, ORBIT Gesellschaft für Applikations- und Informationssysteme mbH

Oracle Business Intelligence (OBI) lässt sich in Microsoft SharePoint integrieren. Dies erfordert Anpassungen in mehreren System-Komponenten. Dieser Artikel zeigt Schritt für Schritt, wie man dieses Ziel erreichen kann.

Für eine möglichst nahtlose Integration von OBIEE in SharePoint ist Single sign-on (SSO) erforderlich. Dazu muss die Nutzer- und Rollenverwaltung ausgelagert werden. Da SharePoint stets in einer Windows-Infrastruktur genutzt wird, ist ein Active Directory (AD) erforderlich. Als ersten Schritt übergibt man die Verwaltung der Benutzer und Rollen an das AD. Bevor die eigentliche Umstellung des OBIEE-Servers erfolgt, sind dort einige User und Gruppen anzulegen.

Konfiguration des AD-Servers

Der OBIEE-Server muss nicht Mitglied der Domäne des AD sein. Es reicht auch, wenn die beiden Server miteinander kommunizieren können. Zuerst wird ein Benutzer (kein Computerkonto) angelegt, den der OBIEE-Server zur internen Kommunikation mit seinen Komponenten benötigt. Er sollte „OBIEESystemUser" heißen, benötigt keine weiteren Rechte und entspricht dem standardmäßigen User „BISystemUser".

Darüber hinaus wird ein User benötigt, mit dem sich der OBIEE-Server beim AD authentifiziert. Er sollte „srv_bi" („sAMAccountName") heißen und sein Common-Name (cn) lautet „Service Account BI". Das „cn"-Attribut wird später bei der Eigenschaft „Principal" benötigt, siehe Abschnitt „Konfiguration des WebLogic Servers". Zusätzlich benötigt man Gruppen, die den Applikationsrollen des OBIEE-Servers entsprechen. Dies sind zunächst die Standardrollen *(siehe Tabelle 1)*.

Existieren bereits weitere Rollen, so sind dazu korrespondierende AD-Gruppen erforderlich. Die AD-Benutzer, die nun auf den OBIEE-Server zugreifen dürfen, werden den neu angelegten Gruppen zugeordnet.

Applikationsrolle	AD-Gruppe
BIAdministrator	OBIEEAdmin
BIAuthor	OBIEEAuthor
BIConsumer	OBIEEConsumer

Tabelle 1: Applikationsrollen und AD-Gruppen-Zuordnung

Parameter	Bedeutung/Beispiel
Host	DEV-DC2.orbit.test
Port	389 *
Principal	CN=Service Account BI, OU=Dienstkonten, OU=Benutzer, OU=ORBITTEST, DC=orbit, DC=test
Credential	Das Passwort, das bei der Anlage des Users verwendet wurde
User Base DN	OU=Benutzer,OU=ORBITTEST,DC=orbit,DC=test
User From Name Filter	(&(sAMAccountName=%u)(objectclass=user))
User Name Attribute	sAMAccountName
Group Base DN	OU=Gruppen,OU=ORBITTEST,DC=orbit,DC=test
Optional, wenn das Gruppen-Attribut nicht cn, sondern sAMAccountName ist	
Static Group Name Attribute	sAMAccountName
Group From Name Filter	(&(sAMAccountName=%g)(objectclass=group))

*Tabelle 2: Authentication-Provider-Parameter, * Standardwert*

Konfigurationen im Enterprise Manager

Als Erstes wird im linken Baum auf „WebLogic Domain" („bifoundation_domain") der interne User angepasst („User Name = OBIEESystemUser", gleiches Passwort wie im AD). Dort erfolgt auch die Zuordnung zur Rolle „BI System Role". Die weiteren bestehenden Rollen werden den AD-Gruppen nach demselben Muster zugeordnet. In der Regel wird man die Berechtigungen immer über Rollen erteilen. Normalerweise verwendet das AD den Inhalt des Feldes „sAMAccountName" als Usernamen, deshalb muss dort „sAMAccountName" statt „cn" verwendet werden. Dies erfordert allerdings eine Anpassung der „Identity Store Configuration". So muss im Abschnitt „Identity Store Provider" der „bifoundation_domain" ein neuer Eintrag mit „Property Name = user.login.attr" und „Value = sAMAccountName" hinzugefügt werden.

Normalerweise ist für die AD-Gruppen keine Anpassung nötig, weil das „cn"-Attribut zum Einsatz kommt. Sollte man hier ebenfalls auf „sAMAccountName" ausweichen, sind die analogen Anpassungen beim WebLogic Server durchzuführen *(siehe den optionalen Teil in Tabelle 2)*.

Konfiguration des WebLogic Servers

In der Administrations-Konsole des WebLogic Servers werden zunächst ein neu-

Anpassung der Group Policies

1. Die Group-Policy-Management-Console öffnen
2. Zu Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options navigieren
3. Die Option „Network security: Configure encryption types allowed for Kerberos“ anklicken
4. Die Option „Define these policy settings“ und alle (sechs) Verschlüsselungstypen anklicken
5. OK anklicken

er Authentication Provider erstellt sowie unter „Domain Structure“ und „Security Realms“ die Domäne (etwa „myrealms“) angepasst. Der neue Provider heißt „ADAuthenticator“. Er ist vom Typ „ActiveDirectoryAuthenticator”. Nach dem Speichern ist der neue Eintrag nochmals anzuklicken, um „Control Flag = SUFFICIENT“ zu setzen. Im Register „Provider Specific“ sind die in *Tabelle 2* gezeigten Informationen einzutragen. Durch Klick der Schaltfläche „Reorder“ wird der Provider „ADAuthenticator“ von ganz unten nach ganz oben bewegt. Nun muss noch im Provider „DefaultAuthenticator“ ebenfalls das „Control Flag“ von „REQUIRED“ auf „SUFFICIENT“ umgestellt werden. Anschließend können die Änderungen gespeichert und freigegeben werden.

Da im Enterprise Manager der „BI-SystemUser“ angepasst wurde, muss in der Domäne überprüft werden, ob der User beziehungsweise die Administrationsrollen der Admin-Rolle entsprechen. In der Spalte „Role Policy“ der „Predicate List“ wird mit „Add Condition“ eine Bedingung hinzugefügt, nämlich „User Argument Name = OBIEESystemUser“. Wichtig ist die Vorwahl der ODER-Bedingung, da man sich ansonsten aussperrt. Jetzt sind alle Voraussetzungen getroffen, um die Benutzer und Rollen im AD zu verwalten. Das gesamte BI-System ist neu zu starten.

Konfiguration für SSO

Die Konfiguration von SSO erfordert Eingriffe an folgenden Stellen:

- AD-Server
- OS des BI-Servers
- WebLogic Server
- Analytics-Applikation
- Enterprise-Manager
- Browser-Konfiguration der Clients

Als Authentifizierungsmechanismus wird Kerberos genutzt, der sowohl vom AD als auch vom BI-Server unterstützt wird. In den nun folgenden Beschreibungen ist insbesondere auf die Groß- und Kleinschreibung zu achten. Andernfalls funktioniert das Verfahren nicht.

Der AD-Server fungiert als Kerberos Key Distribution Center (KDC) für Kerberos-basierte Clients. Jeder dort angemeldete Benutzer wird auch als valider Nutzer (Principal) eines sogenannten „Kerberos Realm“ erachtet. Im Allgemeinen ist also eine AD-Domäne einem Kerberos Realm gleichzusetzen. Sie ist normalerweise die in Großbuchstaben geschriebene DNS-Domäne, in unserem Beispiel also „ORBIT.TEST“. Zunächst muss sichergestellt sein, dass der AD als KDC agieren kann. Für Windows 2008 R2 und Windows 7 ist zunächst die DES-Verschlüsselung zu aktivieren. Damit die Clients DES ebenfalls unterstützen, müssen die Group-Policies angepasst werden *(siehe Kasten)*.

Einen WebLogic-Account anlegen

Der WebLogic Server muss nicht zur AD-Domäne gehören, sich aber beim KDC authentifizieren. Dazu erstellt man das AD-Konto (Personenkonto) „wl_ora01d“, das einem KDC-Principal entspricht. Es dürfen

```
ktpass.exe
   -princ HTTP/bn-ora01d.orbit.test@ORBIT.TEST
   -mapuser wl_ora01d -pass <Passwort des>
   -crypto all -ptype KRB5_NT_PRINCIPAL
   -out C:\bn-ora01d.keytab
```

Listing 1

```
[libdefaults]
default_realm = ORBIT.TEST
default_tkt_enctypes = arcfour-hmac-md5 des-cbc-crc des-cbc-md5
default_tgs_enctypes = arcfour-hmac-md5 des-cbc-crc des-cbc-md5
ticket_lifetime = 600
allow_weak_crypto = true

[realms]
ORBIT.TEST = {
kdc = 172.18.2.80 *
admin_server = DEV-DC2.orbit.test
default_domain = ORBIT.TEST
}

[domain_realm]
.orbit.test = ORBIT.TEST

[appdefaults]
autologin = true
forward = true
forwardable = true
encrypt = true

[logging]
kdc = FILE:/var/log/krb5/krb5kdc.log
admin_server = FILE:/var/log/krb5/kadmind.log
default = SYSLOG:NOTICE:DAEMON
WebLogic-Konfiguration
```

*Listing 2, * IP-Adresse des AD-Servers*

keine Passwort-Optionen selektiert sein. Zur Kontrolle der Verschlüsselungs-Einstellungen muss man den Nutzer im AD-Baum suchen und im Account-Tab kontrollieren, ob die Checkbox „Use DES encryption types for this account“ selektiert und die Option „Do not require Kerberos pre-authentication“ nicht selektiert ist. Zum Ausschluss unerwünschter Änderungen sollte das Passwort neu gesetzt werden.

Ein Service Principal Name (SPN) ist ein eindeutiger Name, der den AD-User mit dem User verbindet, den der WebLogic Server zur Authentifizierung bei Kerberos verwendet. Für den SPN gibt es verschiedene Varianten, die mit dem Kommandozeilenprogramm „setspn“ registriert werden:

- setspn -A HTTP/bn-ora01d.orbit.test wl_ora01d
- setspn -A HTTP/bn-ora01d wl_ora01d

Ein „setspn -L wl_ora01d“ zeigt die dem Nutzer „wl_ora01d“ zugeordneten SPNs. Die Schlüssel-Tabelle wird vom WebLogic Server zur Authentifizierung beim Kerberos KDC verwendet *(siehe Listing 1)*. Dieses Kommando erstellt die Datei „bn-ora01d.keytab“, die auf den BI-Server kopiert wird, siehe auch Abschnitt „Anpassungen im Dateisystem“. Zusätzlich wird mit dem Aufruf von „ktpass“ der weitere SPN „HTTP/bn-ora01d.orbit.test@ORBIT.TEST“ erstellt.

Konfiguration des BI-Server OS

Der BI-Server läuft auf einem SUSE Enterprise Linux, bei dem Kerberos mit der Konfigurationsdatei „/etc/krb5.conf“ konfiguriert ist *(siehe Listing 2)*. Zur Anpassung im Dateisystem muss die Datei „bn-ora01d.keytab“ nach „${FMW_HOME}/user_projects/domains/bifoundation_domain“ kopiert werden. Dort erstellt man auch die Datei „krb5Login.conf“ *(Inhalt siehe Listing 3)*. Diese Datei konfiguriert das JAAS-Kerberos-Login-Modul.

Beim Start des WebLogic Servers müssen nun einige Parameter zur Konfigurierung von Kerberos mitgegeben werden. Diese Einstellungen werden in der Datei „setDomainEnv.sh“ vorgenommen, die im Verzeichnis „${FMW_HOME}/user_projects/domains/bifoundation_domain/bin“ zu finden ist. Dazu wird eine Zeile mit zusätzlichen Java-Properties nach dem letzten Setzen der Variablen EXTRA_JAVA_PROPERTIES erstellt *(siehe Listing 4)*.

Anpassungen des Presentation-Servers

Der OBI Presentation Server befindet sich als Applikation im WebLogic Server. Die zugrunde liegende EAR-Datei „analytics.ear“ steht im Verzeichnis „${FMW_HOME}/Oracle_BI1/bifoundation/jee“ und ist zunächst mit „jar -xvzf analytics.ear“ zu entpacken, ebenso die darin enthaltene „.war“-Datei. Anschließend werden folgende Schritte ausgeführt:

- In der Datei „META-INF/MANIFEST.MF“ muss die Zeile „WebLogic-Application-Version“ angepasst beziehungsweise hinzugefügt und mit dem Wert „11.1.1.sso“ versehen werden.
- In der Datei „analytics.war/WEB-INF/weblogic.xml“ sind die im BI-Server verwendeten Rollen zu konfigurieren. Dazu

Aktivierung des SSO im Enterprise Manager

1. Im (linken) Baum den Eintrag „Business Intelligence“ aufklappen und den Eintrag „coreapplication“ anklicken
2. „Lock and Edit Configuration“ anklicken
3. Im Register „Single Sign On“ die Checkbox „Enable SSO“ aktivieren und den „SSO Provider“ auf „Windows Native Authentication“ stellen
4. „Apply“ anklicken
5. „Activate Changes“ anklicken und die Ausführung der Aktion abwarten

```
com.sun.security.jgss.initiate {
   com.sun.security.auth.module.Krb5LoginModule required
   principal="HTTP/wl_ora01d@ORBIT.TEST"
   useKeyTab=true
   keyTab=bn-ora01d.keytab
   storeKey=true
   debug=true;
};

com.sun.security.jgss.krb5.accept {
   com.sun.security.auth.module.Krb5LoginModule required
   principal="HTTP/wl_ora01d@ORBIT.TEST"
   keyTab=bn-ora01d.keytab
   useKeyTab=true
   storeKey=true
   debug=true;
};
```

Listing 3

```
XTRA_JAVA_PROPERTIES="-Djava.security.krb5.conf=/etc/krb5.conf
-Djava.security.auth.login.config=krb5Login.conf
-Djavax.security.auth.useSubjectCredsOnly=false
-DWeblogic.security.enableNegotiate=true
-Dweblogic.debug.DebugSecurityAtn=true ${EXTRA_JAVA_PROPERTIES}"
export EXTRA_JAVA_PROPERTIES
```

Listing 4

```
<security-role-assignment>
   <role-name>SSORole</role-name>
   <principal-name>OBIEEAdmin</principal-name>
   <principal-name>OBIEEAuthor</principal-name>
   <principal-name>OBIEEConsumer</principal-name>
</security-role-assignment>
```

Listing 5

Einstellungen im Internet Explorer

1. Im Register „Sicherheit“ das Icon „Lokales Intranet“ selektieren, „Sites“ anklicken und dort auf die Schaltfläche „Erweitert..“ gehen. Im Dialog den Namen des BI-Servers eintragen
2. Im Register „Sicherheit“ die Schaltfläche „Stufe anpassen..“ anklicken, den Eintrag „Benutzerauthentifizierung“ suchen und „Automatische Anmeldung mit aktuellem Benutzernamen und Kennwort“ auswählen
3. Im Register „Erweitert“ den Eintrag „Integrierte Windows-Authentifizierung aktivieren*“ selektieren.

muss innerhalb des Tags „<weblogic-web-app></weblogic-web-app>“ der in *Listing 5* gezeigte Code eingefügt werden.

- In der Datei „analytics.war/WEB-INF/web.xml“ muss in das Tag „<login-config>...</login-config>“ der Inhalt von Listing 6 eingesetzt werden. Der Eintrag in „<role-name>“ muss mit dem Rollennamen in der Datei „weblogic.xml“ übereinstimmen.
- Abschließend müssen mit „jar –cvf analytics.war *“ die „analytics.war“- und „.ear“-Dateien erzeugt und die „.ear-Datei“ bereitgestellt werden.

Hinweis: Für die Darstellung in SharePoint ist eine weitere Anpassung der Datei „web.xml“ erforderlich, siehe dazu Abschnitt „Konfiguration des BI-Servers“. Die Datei muss nun erneut bereitgestellt werden, siehe Abschnitt „Analytics.ear erneut bereitstellen“.

Parameter	Ausprägung
.allow-proxies	true
.delegation-uris	http://, https://
.gsslib	<leer>
.trusted-uris	http://, https://
.using-native-gsslib	true

Tabelle 3: Firefox SSO-Parameter

```
<security-constraint>
   <web-resource-collection>
       <web-resource-name>BI Analytics</web-resource-name>
       <url-pattern>/*</url-pattern>
   </web-resource-collection>
   <auth-constraint>
       <role-name>SSORole</role-name>
   </auth-constraint>
</security-constraint>

<login-config>
   <auth-method>CLIENT-CERT</auth-method>
</login-config>

<security-role>
   <role-name>SSORole</role-name>
</security-role>
```

Listing 6

```
<context-param>
   <param-name>oracle.adf.view.rich.security.FRAME_BUSTING</param-name>
   <param-value>differentDomain</param-value>
</context-param>
```

Listing 7

Anpassungen in der WebLogic-Konsole

Wie im Abschnitt „Konfiguration des WebLogic Servers“ beschrieben, ist ein neuer Eintrag zu erstellen:

- *Name*
  SPNEGOAsserter
- *Type*
  NegotiateIdentityAsserter

Dieser Eintrag ist für die Behandlung des SPNEGO-/Kerberos-Tickets verantwortlich und unmittelbar hinter „ADAuthenticator“ zu platzieren. Anschließend ist die Datei „Analytics.ear“ erneut bereitzustellen.

Nach den Anpassungen des Presentation-Servers kann das Enterprise Archive bereitgestellt werden. Dazu im Baum „Domain Structure“ auf „Deployments“ klicken, in der Tabelle die Checkbox vor dem Eintrag „analytics“ und dann „Update“ anklicken. Alle Einstellungen, die in den nachfolgenden Seiten angeboten sind, können im Standardfall übernommen werden. Mitunter wird die Version der „.ear“-Datei nicht korrekt erkannt und das Deployment mit einer entsprechenden Fehlermeldung abgelehnt. In diesem Fall löschen wir die Applikation und installieren die „.ear“-Datei unter Verwendung der Standardwerte erneut. Zum Schluss die Änderungen mit „Activate Changes“ aktivieren.

Im Enterprise Manager muss nun das SSO aktiviert werden *(siehe Kasten S. 59)*. Anschließend ist das BI-System neu zu starten.

Anpassung der Windows-Clients

Auch in den Browsern müssen Anpassungen vorgenommen werden. Der Kasten zeigt dies für den Internet Explorer. In Firefox erfolgt die Kontrolle auf der Seite „about:config“. Durch Eingabe von „network.negotiate-auth“ im Such-Feld können die Einstellungen leicht mit den in *Tabelle 3* genannten abgeglichen werden (der vordere „network.negotiate-auth“-Teil ist weggelassen).

Einbindung in SharePoint

Die einfachste Art der Integration ist die Referenzierung eines OBI-Objekts (Dashboard, Bericht) in einem Web Part der Kategorie „Media and Content“ und dem

Part „Page Viewer“. Neben dem Titel benötigt man den URL des OBI-Objekts, der verschiedene Formen haben kann:

- Dashboard mit Dashboard-Menü
  - dashboard&PortalPath=<Pfad >/<Name des Dashboards>:
  - dashboard&PortalPath=/shared/_portal/_portal/Mein Dashboard
- Dashboard-Seite ohne Dashboard-Menü PortalPages&PortalPath=<Pfad >/<Name des Dashboards> &Page=<Seitenname>:
  - PortalPages&PortalPath=/shared/_portal/_portal/Mein Dashboard&Page=Seite 2
- Einzelner Bericht
  - Go&Action=extract&path=<Katalog-Pfad>/<Name des Berichts>:
  - Go&Action=extract&path=/shared/Alle Berichte/Bericht 1

Konfiguration des BI-Servers

Web Parts verwenden IFrames zur Anzeige. Aus Sicherheitsgründen (XSS) ist die Anzeige von Dashboards in IFrames deaktiviert und muss zunächst erlaubt werden. Dazu wird zunächst die Datei „instanceconfig.xml“ in „${FMW_HOME}/instances/instance1/config/OracleBIPresentationServicesComponent/coreapplication_obips1“ angepasst: Dazu im Tag-Paar „<Security>...</Security>“ das Tag „<InIFrameRenderingMode>allow</InIFrameRenderingMode>“ einfügen.

Als Nächstes muss die Datei „web.xml“ im Web-Archive des Enterprise-Archive angepasst werden. Zum Ort, Auspacken und Wieder-neu-Erstellen der „.ear“-Datei siehe Abschnitt „Anpassungen des Presentation-Servers“. Dazu muss man in der Datei eine geeignete Stelle finden, beispielsweise hinter „<servlet-mapping><servlet-name>RelatedContent</servlet-name>...</servlet-mapping>“, und dort den Abschnitt aus *Listing 7* eintragen. Nachdem die EAR-Datei neu erstellt wurde, muss sie wieder bereitgestellt werden.

Frank Weyher
frank.weyher@orbit.de

Dr. Götz Gleitsmann
goetz.gleitsmann@orbit.de