Konfiguration von WNA in Oracle Access Manager 11*g*

Dr. Joachim Reising
PROMATIS software GmbH
Ettlingen

Marc Brenkmann
SüdLeasing GmbH
Stuttgart

Schlüsselworte:
Oracle Fusion Middleware 11*g*, Identity Management, Oracle Access Manager, Windows Native Authentication (WNA), Single Sign-On

Einleitung

In heutigen Software-Landschaften ist es nahezu unabdingbar, den Anwendern durch Single Sign-On eine möglichst einfache Authentifizierung zu bieten ohne dabei die Sicherheit zu vernachlässigen. Über Windows Native Authentication (WNA) ist es sogar möglich, die Windows Benutzerkennung über den Browser an entsprechend konfigurierte Web-Anwendungen weiterzugeben. Schon mit dem Oracle Identity Directory (OID) des Application Server 10*g* konnte so eine zusätzliche Benutzerverwaltung umgangen werden. Stattdessen werden die Benutzerinformationen aus dem Active Directory ins OID synchronisiert, und die Authentifizierung am Single Sign-On Server erfolgt mittels WNA. Bei dem nun notwendig gewordenen Upgrade von Application Server 10*g* nach Fusion Middleware 11*g* gibt es für den Oracle Single Sign-On Server keinen direkten Nachfolger. Stattdessen erfolgt hierbei ein Wechsel auf den Oracle Access Manager. Einige Features werden bei der Migration nun allerdings nicht übernommen, darunter auch die WNA-Konfiguration. Diese muss komplett neu durchgeführt werden, wobei auch hier wieder OID als Basis für die Benutzer-Informationen konfiguriert werden soll.

Installation der Software

Doch zunächst gilt es, die neue Software zur Verfügung zu stellen, denn mit dem Wechsel zu WebLogic und Fusion Middleware müssen alle Komponenten komplett neu installiert werden. Dies ist allerdings auch ein Vorteil, denn so kann die WebLogic-Umgebung parallel zu den bestehenden Application Server-Instanzen aufgebaut werden. In unserem Fall handelt es sich sogar um eine hochverfügbare Installation, was insofern von Vorteil ist, als dass die einzelnen Instanzen nach und nach auf die neue Version gebracht werden können und sich somit die Downtime der Umgebung auf ein Minimum reduziert.

Als erstes ist, wie für alle WebLogic-Installationen, neben der notwendigen Java-Umgebung, die zur Fusion Middleware passende Version auszuwählen und zu installieren. Somit ergibt sich für die zum Installationszeitpunkt aktuellste Identity Management Version 11.1.1.5 der WebLogic Server 10.3.5 und als Java-Umgebung wurde JRockit gewählt.

Die Installation der WebLogic-Komponenten gestaltet sich wie gewohnt als einfach und wenig zeitintensiv, so dass wir uns nach kurzer Zeit schon Gedanken über die Konfiguration der Domäne machen müssen. Um zukünftig verschiedene Anwendungen strikt voneinander trennen zu können, wird auch das Identity Management auf die zugehörigen Server verteilt, womit sich die Domänen bzw. Cluster über jeweils zwei physikalische Rechner erstrecken sollen.

Zusätzlich zur Identity Management Software benötigt man für den Access Manager ein Datenbank-Repository, womit dessen einmalige Einrichtung mittels dem „Repository Creation Utility“ notwendig wird.

Zusätzlich zur Identity Management Software wird noch eine WebTier-Umgebung zur Verfügung gestellt, um zu gewährleisten, dass Komponenten des SSO Server10*g* (u.a. OIDDAS) auch in der neuen Umgebung weiter verwendet werden können. Im Gegensatz zur IM-Software kann hier die

Zielversion nicht direkt installiert werden, sondern es muss zunächst die Version 11.1.1.2 installiert und anschließend der Patch 11.1.1.5 eingespielt werden.

Die Konfiguration

Nach der Installation der Fusion Middleware Software für Oracle Access Manager 11.1.1.5 kann die notwendige Domäne über den mitgelieferten Konfigurations-Manager erstellt werden. Ein Wizard leitet recht intuitiv durch die notwendigen Schritte und richtet auch die notwendige Datenbankverbindung zum zuvor erstellten Repository ein, sodass die „IDMDomain“ mit zwei Managed Servern „oam_server1/2“ schon nach kurzer Zeit verfügbar ist.

Bei der Konfiguration der WebTier-Komponenten wird als OHS-Port der Port der aktuellen 10*g*-SSO Server-Installation angegeben, was für den jeweils zu installierenden Server ein Stoppen der entsprechenden 10*g*-Komponenten bedeutet. In unserer HA-Umgebung erfordert dies allerdings nicht unbedingt eine Downtime. Dennoch ist zu beachten, dass der Knoten nicht über den Load Balancer angesprochen wird, da eventuelle Requests natürlich noch nicht korrekt abgearbeitet werden können.

Über den Upgrade-Assistenten der WebTier-Installation kann man zudem die Konfiguration der entsprechenden 10*g*-Installation auf die neue Fusion Middleware 11*g*-WebTier übertragen.

Während der Konfiguration wird der Web Server bereits an der zuvor erstellten Domäne registriert, muss aber nun noch so konfiguriert werden, dass eingehende Anfragen an den zugehörigen WebLogic Server weitergeleitet werden. Um den Oracle Access Manager mit dem OHS 11g und dessen virtuellen Hosteintrag zu verknüpfen, sind noch einige Konfigurationsdateien (mod_wl_ohs.conf, oam.conf und oam_config,xml) sowie Einstellungen der WebLogic Server (Admin- und Managed Server) anzupassen.

Verwendung von 10*g*-Komponenten

Wie schon erwähnt, ist es möglich mit Identity Management 11*g* auch Komponenten aus der ursprünglichen 10*g*-Installation weiter zu verwenden. Das ist vor allem dann nötig, wenn z.B. OIDDAS verwendet wird, um Benutzer- bzw. Gruppen-Berechtigungen zu verwalten, wie es beispielsweise für Oracle Portal der Fall ist. Da wir in der neuen Umgebung die Port-Einstellungen der 10*g*-Installation verwenden, muss zunächst der Listen-Port des HTTP-Server 10*g* geändert werden und dieser dann am Oracle Access Manager als Partner-Anwendung registriert werden. Dies geschieht durch Erstellen eines neuen OSSO Agents über die OAM Konsole, wobei eine entsprechende `osso.conf`-Datei erstellt wird, die anschließend in das Konfigurationsverzeichnis des OHS 10*g* kopiert werden muss.

Damit die Requests nun auch an den „alten“ WebServer weitergeleitet werden, ist die Konfiguration des 11*g*-WebServers durch Eintragen diverser ProxyPass-Direktiven anzupassen.

Upgrade der Umgebung

Das eigentliche Upgrade des SSO Servers 10*g* nach Oracle Access Manager 11*g* ist wenig spektakulär und erfolgt wie gewohnt über einen entsprechenden Wizard. Nach Eingabe der Quell-Konfiguration des SSO Servers und Verbindungsdaten zur SSO Datenbank und dem zugehörigen OID Server, werden die notwendigen Daten an den Access Manager übertragen.

Je nachdem, ob Host und Port des SSO Servers für den Access Manager übernommen werden oder nicht, werden auch automatisch neue `osso.conf`-Dateien für jede gefundene Partner-Anwendung erstellt und in einem speziellen Verzeichnis zur Verfügung gestellt. Auch wird für den OID ein neuer sogenannter Speicher für Benutzeridentitäten mit dem Namen „MigratedUserIdentityStore“ erstellt.

Konfiguration OAM

Nun muss der OID noch als Benutzer-Speicher für die OAM Konsole selbst und auch für die Partner-Anwendungen eingerichtet werden.

Zunächst wird im OID eine neue Gruppe „Administrators“ erstellt, in die alle gewünschten Benutzer-Accounts als Mitglieder eingestellt werden. Diese Gruppe wird benötigt, um die notwendigen Administrationsrechte in der OAM Konsole zu haben.
Über die Systemkonfiguration in der OAM Konsole wird nun der Benutzeridentitätsspeicher „MigratedUserIdentityStore“ als Standard- und Systemspeicher definiert und die neu erstellte Gruppe „Administrators“ als Zugriffssystemadministratoren angegeben.
Weiterhin wird ein neues Authentifizierungsmodul „LDAP-OID11*g*“ erstellt, für das als Benutzeridentitätsspeicher ebenfalls der migrierte OID-Speicher „MigratedUserIdentityStore“ definiert wird. Dieses neue Authentifizierungsmodul, das nun der OID-Verbindung des SSO Servers 10*g* entspricht, wird nun für das Authentifizierungsschema „OAMAdminConsoleScheme“ verwendet, womit zukünftig die Authentifizierung an der OAM Konsole über den OID Server erfolgen muss.
Für die Konfiguration der Partner-Anwendungen wird nun in der Policy-Konfiguration ein neues Authentifizierungsschema als Kopie des bestehenden „LDAPScheme“ erstellt und für das neue „OIDScheme“ das zuvor erstellte Authentifizierungsmodul „LDAP-OID11*g*“ definiert. Weiterhin wird dieses neue Schema als Standard festgelegt und außerdem in der „Protected Resource Policy“ der migrierten Anwendungsdomäne „migratedSSOPartners“, die alle vom SSO Server 10*g* übernommene Partner-Anwendungen beinhaltet, als Authentifizierungsschema ausgewählt. In der Host-ID-Definition dieser „migratedSSOPartners“ sind nun noch alle virtuellen Hosts anzugeben, über die die zugehörigen WebServer angesprochen werden und in der Folge erfolgt die Anmeldung über die Standard-Loginseite des OID Servers.

Konfiguration WNA
Als letzter Schritt steht nun noch die Konfiguration der Windows Native Authentication an, für die initial eine `keytab`-Datei vom AD-Server erstellt werden muss, wozu ein spezieller AD-Account notwendig ist, über den dann das Mapping bei der Kerberos-Authentifizierung erfolgt. Diese Datei „`sso.keytab`“ wird nun auf jedem Server, auf dem der Oracle Access Manager installiert ist, zur Verfügung gestellt.
In der Systemkonfiguration der OAM Konsole muss nun in den Access Manager-Einstellungen die Definition für das Kerberos-Authentifizierungsmodul angepasst werden. Hier ist einzutragen, wo sich die Keytab- und die KRB-Konfigurationsdatei (i.d.R. `/etc/krb5.conf`) bzw. wie der Principal heißt. In unserem Fall: „HTTP/sso.suedleasing.de@SUEDLEASING.COM“.
Die gleichen Informationen sind ein zweites Mal, ebenfalls über die OAM Konsole, für das Plugin „KerberosTokenAuthenticator“ einzutragen.
Die Information die der OAM/WNA aus dem Kerberos-Ticket holt ist nun zwar „user@Domain“, allerdings wird in der Version 11.1.1.5 offensichtlich die Domain „abgeschnitten“. Außerdem soll ja nicht das Active Directory als UserIdentityStore verwendet werden, sondern OID, was auch prinzipiell gut funktioniert. Das Problem ist allerdings, dass OAM/WNA mit dem abgeschnittenen SamAccountName versucht sich gegen den OID zu authentifizieren, was mit dem „Standard“-KerberosScheme im OAM nicht funktioniert, da kein analoger Wert ins OID synchronisiert wird. Auch funktionieren beispielsweise die APEX-Anwendungen nicht mehr, da dort eine zusätzliche Autorisierung mit dem übergebenen Benutzernamen eingebaut wurde.
Aus diesen Gründen müssen für das Benutzerdefinierte Authentifizierungsmodul „KerberosPlugin“ im Schritt „stepUIF“ die Plug-In-Parameter KEY_LDAP_FILTER, KEY_IDENTITY_STORE_REF und KEY_SEARCH_BASE_URL eingetragen werden, wobei für den KEY_LDAP_FILTER an den Wert {KEY_USERNAME} nun explizit wieder die verwendete Domäne (also @SUEDLEASING.COM) angehängt werden muss.
Weiterhin ist in der Definition des „MigratedUserIdentityStore“ das Benutzernamenattribut auf „uid“ zu ändern, damit es eine Übereinstimmung mit dem nun übergebenen Benutzernamen geben kann.

Als letzte Schritte sind im Authentifizierungsschema „KerberosScheme“ als Authentifizierungsmodul „KerberosPlugin“ einzutragen und für die Protected Resource Policy der migratedSSOPartners als Authentifizierungsschema auf „KerberosScheme“ zu wechseln.
Damit sich nun die sogenannten „Seeded Users“ (z.B. orcladmin, oc4jadmin) trotz WNA anmelden können, müssen in der Domäne noch zusätzliche Authentifizierungs-Provider eingerichtet werden. Dies kann in der Admin-Konsole über „Sicherheits-Realms - myRealm“ durchgeführt werden. Hier werden der „OIDAuthenticator“ mit Verbindungsinformationen zum OID-Server sowie der „OAMIDAsserter“ erstellt und der Realm anschließend so konfiguriert, dass die Authentifizierung an einem der Provider ausreicht. Somit wird nun auch eine eventuelle mehrmalige Anmeldung an verschiedenen Providern verhindert.

Kontaktadressen:

Marc Brenkmann
Dipl.-Wirtschaftsinformatiker (DH)
SüdLeasing GmbH
Pariser Platz 7
70155 Stuttgart

Telefon: +49(0)621 4281-1185
Fax: +49(0)621 428651-1185
E-Mail: marc.brenkmann@suedleasing.com
Internet: www.suedleasing.com

Dr. Joachim Reising
Division Manager
PROMATIS software GmbH
Pforzheimer Str. 160
76275 Ettlingen

Telefon: +49(0)7243 2179-0
Fax: +49(0)7243 2179-99
E-Mail: joachim.reising@promatis.de
Internet: www.promatis.de