Der lange Weg vom SSO-Server zu SAML und Identity Federation

Marc Brenkmann
SüdLeasing GmbH
Mannheim

Dr. Joachim Reising
PROMATIS software GmbH
Ettlingen

Schlüsselworte:

Oracle Fusion Middleware 11*g*, Identity Management, Oracle Identity Federation, Oracle Access Manager, SAML, Single Sign-On

Einleitung

Single Sign-On ermöglicht Anwendern nicht nur ein einfacheres Arbeiten, sondern bietet auch ein erhöhtes Maß an Sicherheit, da die Anzahl der notwendigen Kennwörter erheblich reduziert wird. Aus Anwendersicht ist in den heutigen Portal-Landschaften diese Möglichkeit der einmaligen Authentifizierung nahezu unabdingbare Voraussetzung.
Beim Upgrade von Oracle 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. Allerdings werden bei diesem verschiedene Features, wie die sogenannten „external Applications“, nicht mehr angeboten. Diese boten unter 10*g* die Möglichkeit, „externe“ Web-Anwendungen mit eigener Benutzerverwaltung durch Speicherung der Benutzer-Informationen in die Single Sign-On Umgebung zu integrieren. Um auch nach dem Upgrade weiterhin die automatische Anmeldung zu ermöglichen, sollte am Beispiel einer Dokuwiki-Anwendung ein adäquater Ersatz gefunden und evaluiert werden.

Das Problem

Bei den Vorbereitungen zum Upgrade der diversen Application Server 10*g*-Umgebungen, wurde beim Studium des Upgrade Guides für Oracle Identity Management 11*g* der Hinweis gefunden, dass die sogenannten „external Applications“ nicht in den Oracle Access Manager 11*g* übernommen werden. Die entsprechende Rückfrage bei Oracle Support bestätigte diese Tatsache und so stellte sich die Frage, in welcher Form für die betroffenen Anwendungen eine automatische Authentifizierung zur Verfügung gestellt werden kann.
Bei den „external Applications“ werden die Login-Daten für die entsprechende Anwendung bei der erstmaligen Eingabe in einer Datenbank-Tabelle gespeichert, wobei neben Benutzername und Passwort auch noch weitere Parameter hinterlegt werden können. Bei weiteren Verbindungsversuchen verwendet der SSO-Server diese Informationen, um die Anmeldung automatisch durchzuführen und somit dem Anwender die Notwendigkeit der manuellen Eingabe zu ersparen.
Da aber keine der Komponenten von Oracle Identity Management 11*g* eine analoge Funktionalität bietet, wurden auch alle weiteren Möglichkeiten untersucht und auf ihre Machbarkeit im Zusammenhang mit einer Dokuwiki-Anwendung hin überprüft, wobei schon recht schnell der Begriff „simpleSAMLphp“ in den Fokus der Untersuchungen trat.

Die Werkzeuge

Bei simpleSAMLphp handelt es sich um eine PHP-Anwendung basierend auf „SAML“ (Security Assertion Markup Language), einem XML-Framework zum Austausch von Authentifizierungs- und Autorisierungsinformationen. SAML wurde unter anderem für Single Sign-On und Autorisierungsdienste entwickelt und besteht aus SAML-Assertions, dem SAML-Protokoll, SAML-Bindings und Profilen. Die SAML-Assertions werden dabei von einem Identity Provider (IdP) zum Service Provider (SP) übertragen, die dieser verwendet, um über das Zulassen eines Zugriffs zu entscheiden.
Um den IdP auf Seiten des Oracle Identity Managements zur Verfügung zu stellen, kann Oracle Identity Federation (OIF) verwendet werden, während der Service Provider in simpleSAMLphp selbst konfiguriert wird.
Als weitere OIM-Komponente kommt schließlich der Oracle Access Manager (OAM) zum Einsatz, der nicht nur für diese Anwendung die Authentifizierung übernehmen soll, sowie eine WebGate-Installation für den WebServer von OIF.
Zunächst werden die einzelnen Installationen durchgeführt: für die Oracle-Software ist auf einem separaten Middle-Tier-Server der WebLogic-Server und eine Domain durch das bereits im Vorfeld erfolgte Upgrade des OID vorhanden. Nach der Software-Installation wird diese Domain um die Konfiguration der beiden Komponenten Oracle Identity Federation mit Webtier und Oracle Access Manager erweitert. Auf dem zweiten Server, auf dem auch die Dokuwiki-Anwendung ausgeführt wird, wird simpleSAMLphp installiert. Hierzu müssen lediglich die notwendigen Software-Packages installiert und dann das entsprechende tar-Archiv entpackt werden.
Um eine Anmeldung mit gültigen Benutzerdaten zu erreichen wird in OIF zunächst das bestehende OID für das LDAP-Directory als Standard-Authentifizierungs-Engine definiert.

Die Konfiguration
Während bei den vorangegangen Installationsschritten nur wenige kleinere Hürden genommen werden mussten, gestaltet sich die Konfiguration der einzelnen Komponenten bedeutend schwieriger, zumal nicht immer ausreichend Informationen zur Verfügung standen oder erst durch längere Suche wenigstens ansatzweise gefunden werden konnten.

simpleSAMLphp

Eine ausführliche Anleitung findet sich auf der simpleSAMLphp-WebSite „simplesamlphp.org“. So ist zunächst der WebServer der Dokuwiki-Anwendung anzupassen und dessen Konfiguration um einen „Alias“ und ein Directory-Direktive zu erweitern, die den Zugriff auf die notwendigen Dateien gewährleisten. Ferner sind in der Datei `config.php` von simpleSAMLphp selbst einige globale sowie sicherheitstechnische Einstellungen durchzuführen.
Nun wird in der Datei `config/authsources.php` der Service Provider (SP) konfiguriert, für den zusätzlich mittels „openssl“ ein „self-signed“ Zertifikat erstellt wird. Hier wird neben der EntityID vor allem der zugehörige Identity Provider (IdP) eingetragen. Für diese IdP müssen allerdings noch die Metadaten in der dafür vorgesehenen Konfigurationsdatei (`metadata/saml20-idp-remote.php`) eingetragen werden. Im Falle von OIF als IdP erhält man die notwendigen Metadaten über den Enterprise Manager als XML-Datei, die jedoch noch in das simpleSAMLphp-Format konvertiert werden muss. Die mitgelieferte Web-Anwendung hält für diese Konvertierung eine eigene Seite bereit, über die man schließlich die Metadaten umwandeln kann.
Über eine weitere Seite dieser Web-Anwendung kann man die gerade konfigurierte Authentifizierungsquelle sogar testen. Allerdings erhält man zum jetzigen Zeitpunkt „`Error 500 – Internal Server Error`“. Der Blick in die entsprechende Log-Datei auf Seiten von OIF liefert die fast schon erwartete Information „`Unknown Provider`“, denn simpleSAMLphp kennt zwar bereits den konfigurierten IdP, aber für OIF ist der Service Provider noch völlig unbekannt.

Oracle Identity Federation

Somit benötigt man wiederum Metadaten, diesmal jedoch vom SP. Auch diese können einfach über die Web-Anwendung von simpleSAMLphp bereitgestellt werden. Mit den erhaltenen Daten kann über den Oracle Enterprise Manager der Service Provider in Oracle Identity Federation als „Trusted Provider“ eingetragen werden. Doch auch nach dieser Eintragung kommt es beim Test noch zu einem Fehler, der im Logfile als „`InvalidNameID`“ ausgegeben wird. So ist im OIF für die SAML2.0-Assertion Settings das NameID-Format auf „`Kerberos Principal Name`“ zu ändern und „`UID`“ als Mapping einzutragen. Anschließend werden auf der Test-Statusseite von simpleSAMLphp die übertragenen Attribute angezeigt, die initiale Konfiguration des Zusammenspiels von OIF und simpleSAMLphp war erfolgreich.

Dokuwiki

Zunächst ist die Datei `simplesamlphp.class.php` in das „`inc/auth`“-Verzeichnis des Dokuwiki zu kopieren. Neben verschiedenen Eintragungen in der `init.php`-Datei des Dokuwikis, die davon abhängig sind, ob der PHP- oder der MemCache-SessionHandler verwendet wird, muss vor allem in der Konfigurationsdatei `local.php` der Authentifizierungstyp auf „`simpleSAMLphp`“ umgestellt und die dazugehörigen Attribute eingetragen werden. Nach diesen Schritten wird versucht die Dokuwiki-Anwendung zum einen über den „normalen“ Wiki-URL bzw. über den entsprechenden OIF-URL aufzurufen. Bei beiden Versuchen erscheint nach erfolgreicher Anmeldung jedoch eine „weiße“ Seite mit der Meldung „`no attribute "eduPersonPrincipalName" provided by IDP`“. Sucht man in den Konfigurationsdateien nach diesem Attributsnamen findet man den zugehörigen Eintrag in der Datei `simplesamlphp.class.php`, wo dies als User-Attribut definiert ist. Auch eine Änderung auf „`UID`“ als Attribut analog dem Mapping in OIF bringt nur eine Änderung in der Fehlermeldung.
Offensichtlich sind noch weitere Anpassungen in der Konfiguration von Identity Federation durchzuführen.

Oracle Identity Federation

Der in der Oracle-Dokumentation gefundene Ansatz, OIF als „`Attribute Responder`“ zu aktivieren führt nicht zum gewünschten Ergebnis, stattdessen liefert nach weiterer Suche die Dokumentation doch noch die Lösung, nämlich die Einstellungen des Service Providers im OIF zu ändern. Dort müssen „`Attribute Mappings`“ mit dem Flag „`Send with SSO assertion`“ definiert und für den SP die Checkbox „`Enable Attributes in Single Sign-On (SSO)`“ aktiviert werden.
Nun werden diese übergebenen Attribute, die auch bestehende Gruppenzugehörigkeiten enthalten einerseits auf der simpleSAMLphp-Testseite ausgegeben und außerdem zum Aufruf des Dokuwiki für die Berechtigungsprüfung verwendet.

Oracle Access Manager

Als letzter Schritt muss noch der Oracle Access Manager als generelle Authentifizierungskomponente eingebunden werden. Zunächst wird das OID als neuer „`User Identity Store`“ erstellt und dieser dann als `primär` definiert, womit nun alle Anmeldungen am OAM über den OID und somit die bestehenden Benutzerdaten erfolgen. Als nächstes müssen die Webseiten von OIF geschützt werden, damit auch für diese eine Anmeldung am OAM erforderlich wird. Hierzu wird eine WebGate-Installation durchgeführt, bei der schon die Suche nach den korrekten gcc-Libraries eine kleine

Herausforderung ist. Um die WebGate-Instanz mit der Webtier von OIF zu verknüpfen sind anschließend noch einige Post-Installations-Schritte durchzuführen. Nun kann über die OAM-Konsole der WebGate-Agent registriert werden, wobei im OAM auch automatisch die notwendige `Application Domain` mit den zugehörigen `Resourcen` sowie den `Authentication` und `Authorization Policies` erstellt wird.
Nachdem schließlich noch der Oracle Access Manager als Standard-Authentifzierungs-Engine von OIF eingerichtet wird, kommt beim nächsten Versuch das Dokuwiki aufzurufen wie erwartet die OAM-Login-Seite als Anmeldemaske. Nach erfolgreichem Anmelden erscheint aber erneut eine bekannte Fehlermeldung: „`no attribute "UID" provided by IDP`“.
Aber auch dies kann letztendlich behoben werden, indem in der `Authorization Policy` sogenannte „`Responses`“ definiert werden. Die Online-Hilfe des OAM liefert hierbei den entscheidenden Hinweis, welcher Wert hier übergeben werden muss und dass der entsprechende Namespace vorangestellt werden muss, nämlich „`$user.userid`“.
So kann schließlich die Anmeldung an der Dokuwiki-Anwendung über Oracle Access Manager, Identity Federation und simpleSAMLphp erfolgreich durchgeführt werden. Über entsprechende Gruppenzugehörigkeiten sind zudem die Berechtigungen für einzelne Bereiche innerhalb des Wikis einstellbar.

Kontaktadressen:

Marc Brenkmann
Technischer Projektleiter
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 Strasse 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