Fusion Applications 11g Shared Identity Management

Olaf Heimburger
Oracle Deutschland B.V. & Co KG
Berlin

Schlüsselworte
Sicherheit, Identity und Access Management, Single Sign On, Fusion Applications

Einleitung
Die Fusion Applications Infrastruktur verwendet den gesamten Identity und Access Management Stack der Fusion Middleware. Wenn dieser Stack quasi zum Nulltarif installiert wird, was hindert uns daran diesen gleich global einzusetzen? Oder, wie können wir bereits vorhandene Komponenten nutzen um diese mit Fusion Applucations und dessen IDM Stack zu verwenden? Wie sind Herausforderungen mit vorhandenen Elementen wie Active Directory, CA SiteMinder aber auch einfachen Lösungen wie Oracle SSO zu meistern?

Die Herausforderung
Jede neue Anwendung trifft auf bestehende Infrastruktur. Besonders vorhandene Sicherheitsarchitekturen und -mechnismen müssen berücksichtigt oder integriert werden können.

Windows Native Authentication (WNA)
In einem Unternehmensnetzwerk mit Windows Domain Servern, in der Regel mit Microsoft Active Directory implementiert, haben wir es hier mit einer verbreitenden Lösung zu tun. Im wesentlichen meldet man sich an seinem Arbeitsplatz an und kann entsprechend konfigurierte Anwendungen wie Outlook ohne weitere Anmeldung verwenden. Der Einsatz von Web-Anwendungen kann durch geeignete Konfiguration, besonders einfach mit dem Microsoft Internet Information Server, der gleiche Effekt erzielt werden.

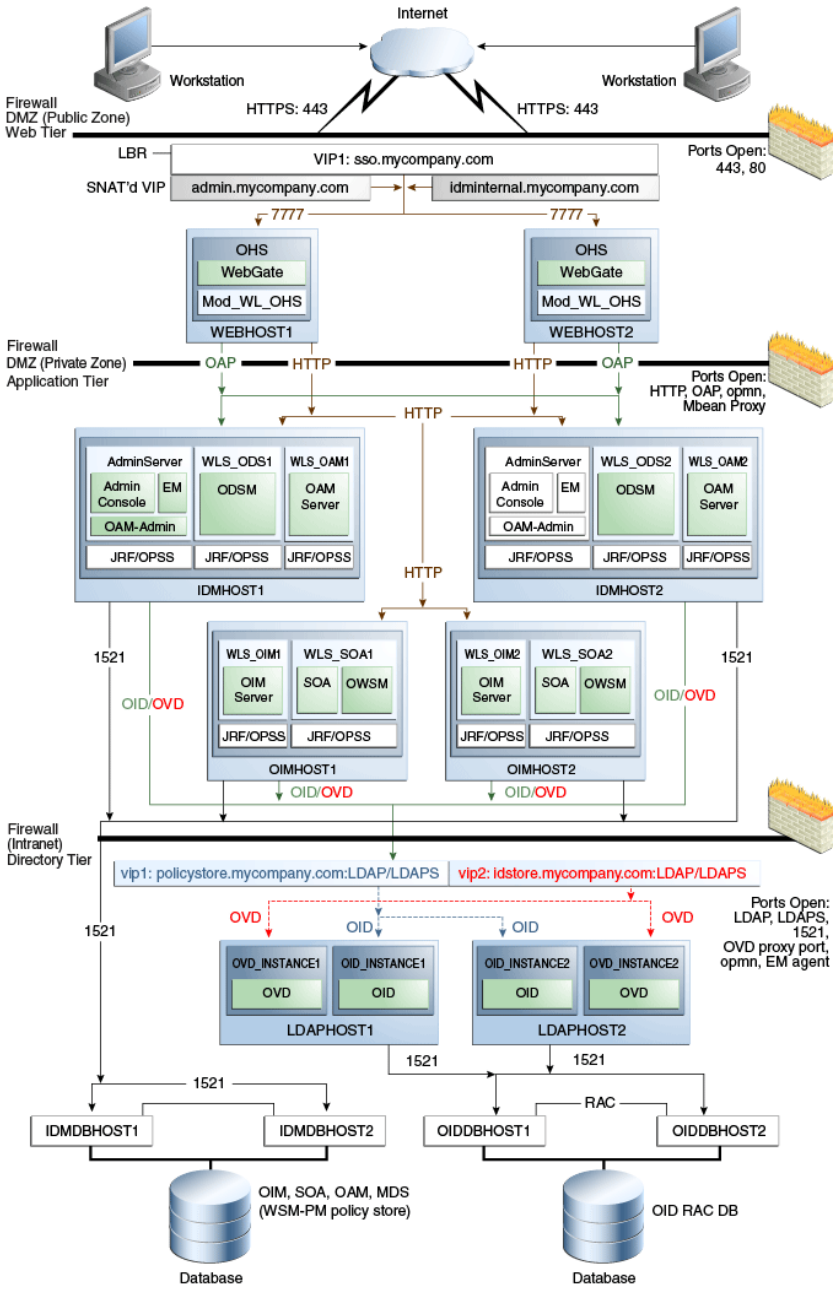
Kerberos/SPNEGO
Mit Kerberos steht eine vom MIT entwickelte, plattformunabhängige Single Sign-on Lösung zur Verfügung. Nahezu jede verfügbare Plattform ist mit der entsprechenden Implementierungen ausgestattet und kann durch gezielte Konfiguration für diesen Dienst eingerichtet werden („kerberized“). Heute übliche Implementierungen sind in Windows Umgebungen mit dem Einsatz von Active Directory.

Oracle AS Single Sign-On
Mit Oracle AS 9.0.2 wurde eine offene Single Sign-on Lösung für Web-Anwendungen eingeführt. Offen meint hier, dass ein Mechanismus zur Authentifizierung zur Verfügung gestellt wird. Ob dieser Mechanismus genutzt werden soll und wie die Autorisierung der Anwender der registrierten Anwendungen vorgenommen werden soll, bleibt Aufgabe der Anwendung. Natürlich sind mehrere Lösungen mit mehr oder weniger identischen Lösungen, auch im gleichen Unternehmen, die Folge. Vorhandene Systeme wie Oracle Forms oder Oracle E-Business Suite setzen diese Verfahren ein.

SAML
Mit der *Security Assertion Markup Language* (SAML) steht ein Standard zur Verfügung, der unternehmensübergreifende Single Sign-On Lösungen unterstützt. Der sowohl Web-Anwendungen aber auch SOA-Anwendungen unterstützt. Die Kernidee ist die Implementierung zweier Typen von Anbietern (Provider) die entweder Dienste (Service Provider) oder Identitäten (Identity Provider) zur Verfügung stellen. *Service Provider* und *Identity Provider* können zu unterschiedlichen Einheiten

eines Unternehmens oder sogar befreundeten Unternehmen gehören und durch gegenseitiges Vertrauen (Circle of Trust) die passenden Anwendungen für die Anwender authentifizieren und autorisieren. SAML stellt damit einen wesentlichen Standard für moderne SOA-basierte Anwendungen zur Verfügung. Passende Infrastrukturen können u.a. mit Oracle Identity Federation implementiert werden. SAML wird unter anderem im Zusammenhang mit CA Siteminder verwendet.

Oracle Fusion Applications und der Oracle Identity and Access Management Stack
Die Oracle Fusion Applications Software wird mit dem kompletten Oracle Identity and Access Management Stack ausgeliefert und implementiert.



Man hat also bereits einen vollständig funktionsfähigen Stack implementiert. Dieser sollte möglichst mit den vorhandenen Elementen zusammenarbeiten. Welche Möglichkeiten gibt es? Hier einige Beispiele:

Integration Active Directory
Die eingesetzte Architektur des Oracle Identity and Access Management Stack beinhaltet bereits die Komponente Oracle Virtual Directory. Das Oracle Virtual Directory ist bewusst als Integrationskomponente für existierende Benutzerverzeichnisse auf LDAP Basis vorgesehen und eine Intergation mit Active Directory ist vollständig dokumentiert.

Integration Windows Native Authentication
Die Integration von Windows Native Authentication geht meistens einher mit der Integration von Active Directory. Werden beide Verfahren eingesetzt, wird die Komponente Oracle Access Manager entsprechend konfiguriert. Dadurch sind Oracle Fusion Applications in das vorhandene Anmeldeverfahren über das Desktop Login eingebunden.

Integration CA Siteminder
Da CA Siteminder auch SAML unterstützt, liegt hier die Implementierung von Oracle Identity Federation mit dem Oracle Access Manager nahe. Der CA Siteminder wird hierbei als SAML Identity Provider verwendet.

Integration Oracle SSO
Hierbei kommt die Fähigkeit des Oracle Access Manager das Oracle SSO Protokoll zu verstehen zum Tragen. In der Regel reicht die Erstellung eines SSO Agenten im Oracle Access Manager und der Austausch der Datei sso.conf auf dem entsprechenden Server.

Integration E-Business Suite
Für die Integration der E-Business Suite mit dem Oracle Access Manager stehen zwei Möglichkeiten zur Verfügung: Verwendung des Access Gates und Verwendung von Oracle SSO. Beide Verfahren sind in entsprechenden Support Dokumenten beschrieben.

Kontaktadresse:
Olaf Heimburger
Oracle Deutschland B.V. & Co. KG
Schloßstr. 2
D-13507 Berlin
Telefon: +49 (0) 30 435 795-160
Fax: +49 (0) 30 435 795-419
E-Mail: olaf.heimburger@oracle.com
Internet: blogs.oracle.com/olaf