Sicherung der Kommunikation zwischen OAM und WebGate: Erstellung, Konfiguration, Diagnostic und Troubleshooting

Mohammad Esad-Djou
OPITZ CONSULTING Deutschland GmbH

Schlüsselwörter

Oracle Fusion Middleware, WebLogic Server, Sicherung der Kommunikation zwischen OAM und WebGate, SSL, Verschlüsselung

Einleitung

Wie können wir durch die verschlüsselte Kommunikation zwischen Oracle Access Management und Webtier (durch WebGate) einen besseren Sicherheitsstandard in der IT-Landschaft erreichen?

In diesem Vortrag werden die OAM-Konfigurationsmöglichkeiten sowie verschiedene Sicherheitsstufen bzgl. WebGate präsentiert.

Themen wie die Erstellung von WebGate Artefakten und Zertifikaten, Verschlüsselungsstandards, Anwendungsfälle für OAM- und WebGate Konfigurationen oder OAM Troubleshooting sind betroffen. Nach einer kurzen Einführung in die Sicherheitsproblematik werden verschiedene Lösungsansätze vorgestellt. Ein besonderer Fokus wird dabei auf Sicherheitszertifikate, deren Erstellung und Anwendungsbeispiele gelegt. Danach werden die Möglichkeiten von OAM für Diagnostic, Test und Troubleshooting dargestellt.

Kommunikation zwischen OAM und WebGate im Überblick

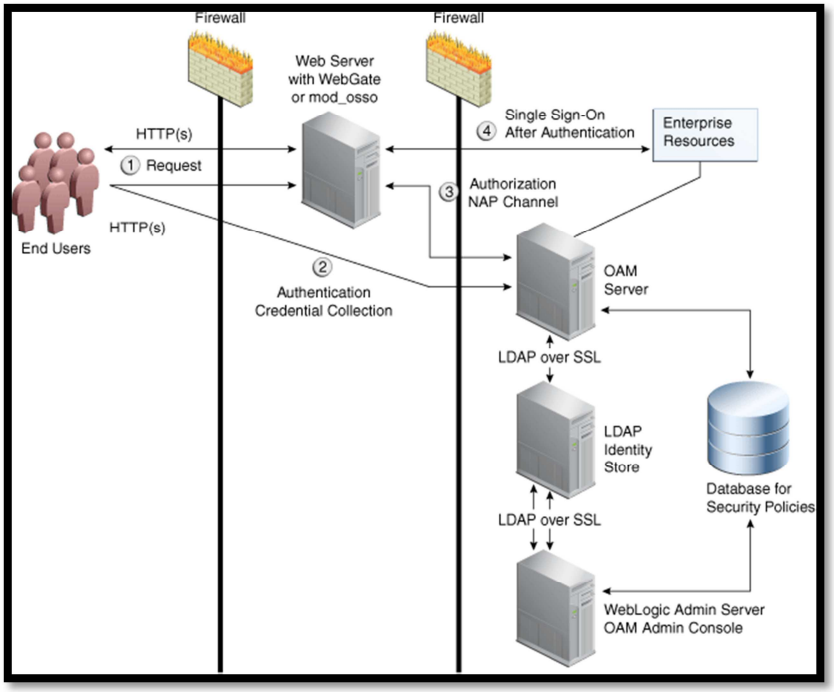
Oracle bietet eine Sicherheitslösung für die Sicherung von Anwendungen, Daten, Web-Services und Cloud-basierten Diensten. Die Oracle Access Management Komponente bietet eine Lösung für die Authentifizierung, Single Sign-On (SSO), Autorisierung, Federation, Mobile und Social Sign-On. Die Abbildung zeigt die Kommunikation zwischen einem WebGate und dem OAM-Server[1].

Der Prozessablauf wird wie folgt durchgeführt (vereinfacht):

1- Endbenutzer schickt eine Anfrage an der geschützte Webseite (https)
2- Authentication-Phase[2]: OAM Server bekommt Credential Information vom Endbenutzer, z. B. User/Password.
3- Authorization-Phase[3]: OAM-Server überprüft auf Basis der Identität des Benutzers, ob der Benutzer die notwendigen Rechte für den Zugriff auf Ressourcen und Applikationen hat. (NAP - NetPoint Access Protocol in OAM 10g oder Oracle Access Protocol - OAP in OAM11g: ermöglichen die Kommunikation zwischen OAM Komponenten während Authentication- und Autorisation-Prozessen)
4- Single Sign-On (SSO): Benutzer melden sich einmalig an einer zentralen Stelle (Enterprise Resources) an und müssen sich nur ein Passwort merken.

---

[1] Mehr siehe: https://docs.oracle.com/cd/E40329_01/admin.1112/e27239/keytool.htm#AIAAG2091
[2] Siehe auch: IT-Security (Part 4): WebLogic Server and Authentication: http://modj.org/wordpress/?p=28
[3] Siehe auch: IT-Security (Part 6): WebLogic Server and Authorization: http://modj.org/wordpress/?p=46



Sicherung der Kommunikation zwischen OAM Servern und WebGate

Es gibt für die Kommunikation zwischen OAM Server und Clients (WebGate) drei Sicherheitsstufen:

- Open: verwendet unverschlüsselte Kommunikation
- Simple: verwendet verschlüsselte Kommunikation (SSL) mit einem Public Key ausgeliefert von Oracle
- Cert: verwendet verschlüsselte Kommunikation (SSL) mit einem Public Key ausgeliefert von einer sogenannten `certificate authority (CA)`

In diesem Vortrag wird die Verschlüsselung der OAM WebGate-Kommunikation an praktischen Beispielen demonstriert:

1- Konfiguration und Anpassung von WebGate
2- Erstellung das Zertifikate (`Self-Signed certificate`)
3- Konfiguration und Anpassung des OAM-Servers
4- Verschlüsselung der OAM-Client-Kommunikation
5- Test und Troubleshooting: Tipps und Tricks

Unterschiede zwischen OAM 11g und OAM 10g

Bevor wir mit OAM 11g starten können, macht es Sinn die Unterschiede zwischen OAM 10g und 11g berücksichtigen[4]. Die Unterschiede werden im Vortrag geklärt und diskutiert.

	OAM 11g	OAM 10g	OSSO 10g
Server-side components	OAM Server (installed on a WebLogic Managed Sever) Oracle Security Token Service runs on OAM Server Oracle Access Manager Console (installed on WebLogic Administration Server)	Access Server Policy Manager	OracleAS SSO server (OSSO server)
Cryptographic keys	One per agent secret key shared between Webgate and OAM Server, generated during Agent registration		One key per partner shared between mod_osso and OSSO server
The protocols used to secure information exchange on the Internet.	One OAM Server key, generated during Server registration	One global shared secret key per Webgate	OSSO server's own key One global key per OSSO setup for the GITO domain cookie
Keys storage	Agent side: A per agent key is stored locally in the Oracle Secret Store in a wallet file OAM 11g server side: A per agent key, and server key, are stored in the credential store on the server side Oracle Security Token Service	Global shared secret stored in the directory server only (not accessible to Webgate)	mod_osso side: partner keys and GITO global key stored locally in obfuscated configuration file OSSO server side: partner keys, GITO global key, and server key are all stored in the directory server

[4] http://docs.oracle.com/cd/E25178_01/doc.1111/e15478/servers.htm

OAM: Diagnostic, Test und Troubleshooting

Oracle Access Management ist ein unternehmenskritisches System. Deshalb muss man Probleme in innerhalb kurzer Zeit analysieren und beheben. In diesem Abschnitt wird über die OAM-Systemanalyse und Problemszenarien diskutiert. Oracle unterteilt die Probleme in zwei Basis-Kategorien:

- Cascading catastrophic failure
- Gradual breakdown in performance

Ursachen für `Cascading catastrophic failure` können folgende Probleme sein:

- LDAP-Server ist belastet und reagiert nicht mehr
- Spitzenlast am Beginn der Geschäftszeit oder Woche
- Webgate Issues

`Gradual breakdown in performance` könnte im Laufe der Zeit auftreten, wenn z.B. OAM für 10.000 User und 500 Gruppe bereitgestellt wurde und sich die Anzahl der Benutzer und Gruppen im Laufe eines Jahres signifikant erhöht (z. B. auf bis zu 50.000 Benutzer und 2500Gruppen) [5]

Zusätzlich werden Werkzeuge wie `Diagnostic Tool` und `Access Tester` vorgestellt und anhand der Beispiele präsentiert.

Demo

Der Vortrag wird mit praktischen Beispielen angereichert.

Fazit

Oracle Access Management übernimmt eine zentrale Rolle beim Single Sign-on (SSO) für das gesamte Unternehmen. Wir können durch die verschlüsselte Kommunikation zwischen Oracle Access Management und Clients, einen besseren Sicherheitsstandard in der IT-Landschaft erreichen.

Im vorliegenden Vortrag wird zunächst die Verschlüsselung der OAM WebGate Kommunikation präsentiert und danach die Möglichkeiten des OAM für Diagnostic, Test und Troubleshooting diskutiert.

[5] Siehe: http://docs.oracle.com/cd/E27559_01/admin.1112/e27239/trouble.htm#AIAAG5111

Kontaktadresse:

Mohammad Esad-Djou

OPITZ CONSULTING Deutschland GmbH

Kirchstraße 6

D-51647 Gummersbach

Telefon:	+49 (0) 2261-6001 0
Mobil:	+49 (0) 173-7279576
E-Mail	mohammad.esad-djou@opitz-consulting.com
Internet:	www.opitz-consulting.com