Web Services Manager in Action: zentrale Sicherheitsplattform für Web Services

Kersten Mebus
ORACLE Deutschland B.V. & Co.KG
Düsseldorf

Schlüsselworte:

SOA / BPM Security, Web Services Manager, OWSM, WS-Security, SAML, Oracle Enterprise Gateway (OEG)

Einleitung

Heutzutage werden Anwendungen nicht mehr isoliert entwickelt und später über aufwändig implementierte Schnittstellen miteinander verknüpft, sondern es werden Funktionsbausteine von zu entwickelnden Applikationen als Services gekapselt und zu Anwendungen oder weiteren Diensten zusammengesetzt. Auf dem Weg dorthin, gibt es viele Herausforderungen, von denen das Thema Sicherheit ein wichtiger Bestandteil ist. Der Oracle Web Services Manager (OWSM) bietet Werkzeuge für die Erstellung, Verwaltung, Anwendung und Durchsetzung von wiederverwendbaren Sicherheitsregeln (Security Policies) für Authentifizierung, Autorisierung, Verschlüsselung, Signaturen, Identitätspropagierung und eigenentwickelten Sicherheitsregeln für Web Services an.

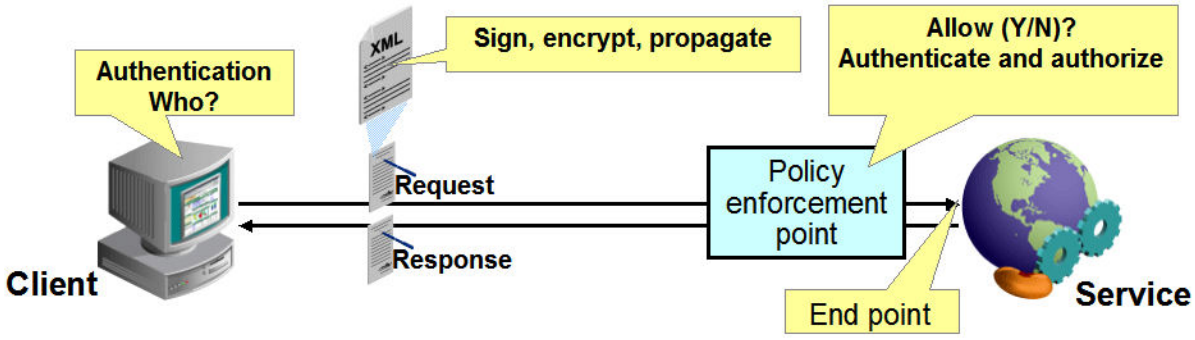

Abbildung 1: Web Services Sicherheitsanforderungen

Unterstützte Standards sind beispielsweise WS-Security, WS-Policy, WS-I Basic Security Profile, X509 Zertifikate, SAML, Kerberos und vieles mehr. Durch die Verwendunng des Oracle Web Services Managers ergeben sich deutliche Vorteile, da durch einen regelbasierten Ansatz

- Sicherheitsregeln durchgängig umgesetzt werden
- eine einfachere Überwachung solcher Sicherheitsregeln möglich wird und
- Sicherheitsregeln zentral definiert und nicht für jede Applikation spezifisch implementiert werden müssen.

Der Oracle Web Services Manager erlaubt es somit Web Services abzusichern, die auf einem JEE Server verteilt worden sind. Damit ist es möglich eine Ende-zu-Ende-Sicherheitsarchitektur zu

etablieren. Sollten Dienste abgesichert werden, die nicht auf einem von Oracle unterstützten JEE Server laufen oder Funktionen einer XML-Firewall und XML-Beschleunigungen abgebildet werden beziehungsweise die Sicherheitsarchitektur soll in einer DMZ liegen, so empfiehlt sich der Einsatz des neuen Oracle Produktes, Oracle Enterprise Gateway (OEG), das ebenfalls über o.g. Sicherheitsaspekte verfügt. Beim OEG muss berücksichtigt werden, dass die erste sowie letzte Meile zu den Services unsicher ist, d.h. diese muss mit anderen Mitteln wie z.B. OWSM oder SSL, etc. abgesichert werden. Liegen beispielsweise Services im Intranet und das Intranet wird als sicher erachtet, könnte die letzte Meilenabsicherung entfallen. Ähnliches gilt für die DMZ.

Oracle Web Services Manager: zentrale Sicherheitsplattform für Web Services

Mit Hilfe des OWSM werden Sicherheitsregeln nicht in der Applikation codiert, sondern deklarativ durch vordefinierte Regelwerke den Services zugeordnet. Die drei wichtigsten Operationen, auf denen der OWSM beruht, sind:

- die zentrale Definition von Sicherheitsregeln und die Zuordnung dieser Policies zu den zu schützenden Web Services, die
- Verteilung der Sicherheitsregeln an sogenannte Policy Enforcement Points (hier: Agenten), die die Durchführung der Regeln zur Laufzeit, bevor der Web Service ausgeführt wird, erzwingen sowie das
- Monitoring von Sicherheits- und Managementereignissen, die zur Laufzeit eintreten, wie z.B. Sicherheitsfehler für Authentifizierung, Autorisierung, Vertraulichkeit und Integrität, etc.

Abbildung 2 zeigt die Applikationen / Dienste, die durch den OWSM abgesichert werden können. Diese Services laufen genauso, wie der OWSM selber, auf dem gleichen WebLogic Server.

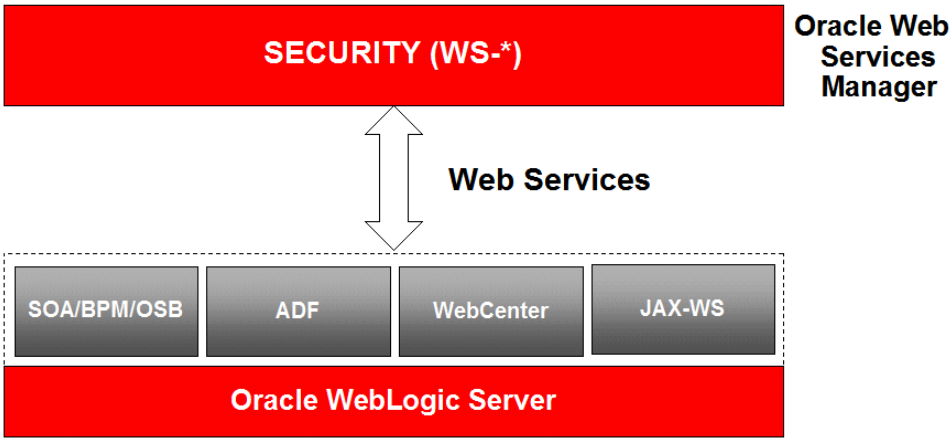

Abbildung 2: Applikationen / Dienste, die der OWSM absichern kann

Es gibt eine Reihe von vordefinierten Sicherheitsregeln, die zur Designzeit im JDeveloper aber auch zur Laufzeit mittels Enterprise Manager (Fusion Middleware Control) den Services zugeordnet werden können (Policy Attachment). Web Services, die keine solche lokalen Sicherheitszuordnung bekommen haben, können während des Deployments globalen Policies automatisch zugeordent werden. Die Sicherheitsregeln werden in einem zentralen Repository (Policy Store) abgelegt und über den Policy Manager an die Agenten verteilt. Somit ist gewährleistet, dass diese Regelwerke zuerst ausgeführt werden bevor der eigentliche WS zum Ablauf gebracht wird. Abbildung 3 verdeutlicht diesen Sachverhalt.

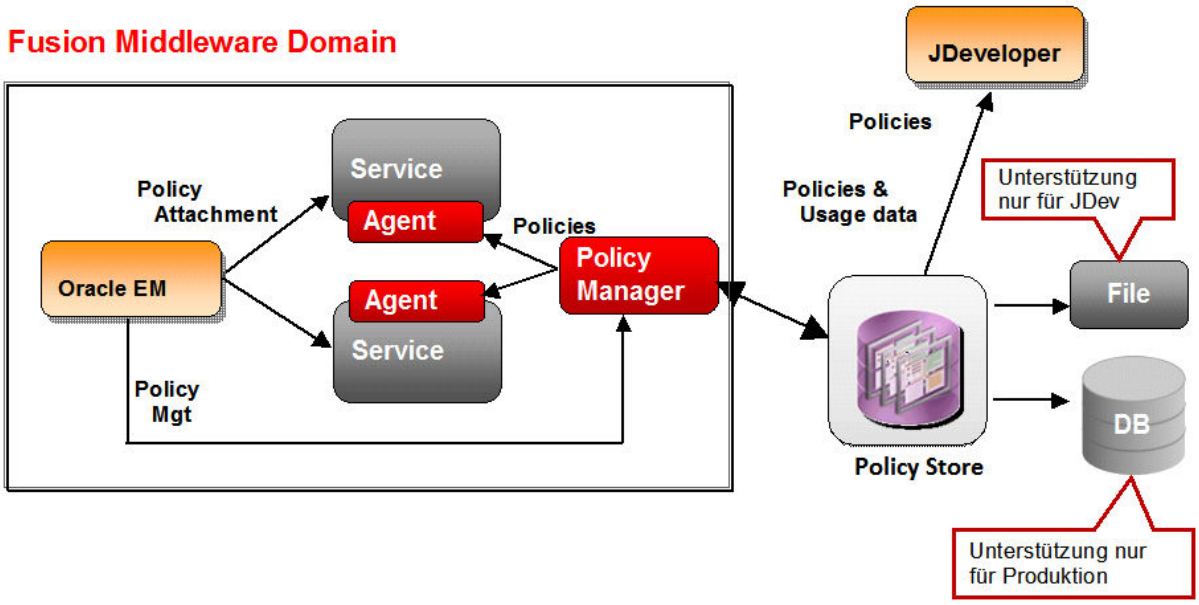

Abbildung 3: OWSM Deployment Architektur

Vordefinierte Sicherheitsregeln können mit dem Enterprise Manager geändert, gelöscht oder neu erzeugt (create like) werden. Policies werden entweder einem Clientaufruf oder einem Service per Zuordnung zugewiesen. Nachfolgende Aufzählung zeigt ein paar Beispiele vordefinierter Sicherheitsregeln:

- oracle/wss_username_token_service_policy
- oracle/wss10_saml_token_client_policy
- oracle/wss11_message_protection_service_policy
- oracle/wss11_username_token_with_message_protection_service_policy
- oracle/wss11_saml20_token_with_message_protection_service_policy
- oracle/wss11_kerberos_token_with_message_protection_client_policy
- ...

Dabei bezeichnet das erste Wort vor dem Querstrich, das es sich um eine Regeldefinition von Oracle handelt. Nachdem Slash steht die verwendete WS Security Version. So bedeutet wss11, dass es sich um den WS Security 1.1 Standard handelt. Die letzten beiden Wörter stehen jeweils für den Client bzw. Service Aufruf. So bedeutet service_policy, dass diese Regel einem Service hinzugefügt wird, der abgesichert werden soll. Analoges gilt für die client_policy. Hier werden dem Client entsprechende Sicherheitsregeln hinzugeführt. Die Wörter nach dem verwendeten WSS Standard beschreiben die Art der Sicherheitsregel. Wichtig dabei ist, ob es sich um eine client_policy oder service_policy handelt. Je nachdem hat diese Sicherheitsregel dann eine andere Bedeutung. So beschreibt beispielhaft username_token_with_message_protection_*service_policy*, dass zuerst das Username-Token verifiziert und der SOAP Request anschließend einer Nachrichtenüberprüfung unterzogen wird, d.h. die Nachricht wird entschlüsselt und es findet eine Signaturprüfung statt. Würde service_police ersetzt durch client_policy, dann würde dem SOAP Request im WSS Header das entsprechende Username-Token gesetzt und der Request würde verschlüsselt und mit einer Signatur versehen.

Sollten die vordefinierten WSS Standardregeln nicht ausreichen, so können in Java neue Policies implementiert und dem OWSM bekanntgemacht werden. Diese neu entwickelten Sicherheitsregeln können somit ebenfalls, wie die vordefinierten Policies, den Web Services zugeordent werden.

In der DOAG Session wird gezeigt wie

- JAX WS,
- SOA / BPM Services und die zugehörigen
- Clientaufrufen
    - Java Clients / JAX WS Clients
    - ADF Web Clients

mit Sicherheitsregeln versehen werden, einschliesslich der notwendigen Konfigurationen.

Fazit:

Der Oracle Web Service Manager ist eine Sicherheitsplattform für die Zugriffssicherung und -verwaltung von Web Services. Mit dem OWSM kann eine Ende-zu-Ende-Sicherheitsarchitektur für diese Dienste aufgebaut werden. Dabei werden Clients und die zugehörigen Web Services deklarativ mit standardisierten Sicherheitsinformationen für Authentifizierung, Autorisierung, Verschlüsselung, Signaturen und Identitätspropagierung versehen. Sicherheitsregeln werden daher durchgängig umgesetzt und müssen nicht für jeden Dienst / Applikation spezifisch implementiert werden.

Kontaktadresse:

Kersten Mebus
ORACLE Deutschland B.V. & Co. KG
Hamborner Str. 51
40472 Düsseldorf

E-Mail: kersten.mebus@oracle.com