Oracle Web Services Manager (WSM)

Marc Chanliau
Director, Product Management
Outline

• Introduction
• Product Overview
• Typical Use-Case Scenarios
• Roadmap
• Q & A
Introduction
Oracle Fusion Middleware

**User Interaction**
- Portals, Content, Search, Desktop, Mobile, VoIP

**Business Intelligence**
- ETL, Q&A, OLAP, Reports, Alerts, Real Time

**Integration & Process Management**
- Messaging, ESB, BPM, B2B, BAM, MDM

**Application Server**
- J2EE, WS-*+, Events, Rules

**Grid Infrastructure**
- Clusters, Metadata, Registry, Security

**Development Tools**
- SOA Tools & Framework

**Systems Management**
- System Application Services

**Identity Management**
- SSO, Access Control, Id Admin, Provisioning, Directory Services
Oracle Identity Management

- Access Manager
  - Web Access Control/Single Sign-On
- Web Services Manager
  - SOA Security
- eSSO Suite
  - Desktop/Legacy Single Sign-On
- Identity Federation
  - Cross Domain Single Sign-On
- Identity Manager
  - Enterprise User Provisioning
- Directory Services
  - Identity Virtualization, Synch & Storage

Auditing & Reporting
- Compliance & Attestation

Systems Mgmt
- Monitoring & Management
Oracle SOA Suite

**BPA Suite**
- Analyst Tools

**JDeveloper**
- App Dev Framework

**BAM**
- Events
- Business Monitoring

**BI**
- Analytics

**Enterprise Manager**
- System Monitoring

**Web Services Manager**
- Management
- Security

**Enterprise Service Bus**
- Multi Protocol
- XSLT Transform
- Routing
- Adapters
- ODI
- B2B Partners
- SES RFID

**BPEL Process Manager**
- Native BPEL
- Human Workflow
- Business Rules

**GOVERNANCE**
- Events
- Analytics
- Business Monitoring
- System Monitoring

**MANAGEMENT & MONITORING**
- Analyst Tools
- JDeveloper
- BPEL Process Manager
- Enterprise Service Bus
- BAM
- BI
- Enterprise Manager
- Web Services Manager
- Registry
- Discovery Policies

**Reporting**
- BAM
- BI

**J2EE Application Server**
- Oracle AS, JBoss, WebLogic, WebSphere
Intersecting Identity Management and SOA

Third-Party Environments
- Identity management infrastructures
- LDAP directories
- UDDI registries
- XML acceleration

Oracle Internet Directory
Oracle Access Manager

OWSM

Oracle BPEL Process Mgr
Oracle Ent. Service Bus

OC4J / UDDI Registry / OLite
Web Services Security & Mgt Concerns

Service Providers
- How do I control who can access my services?
- How do I define and monitor SLAs?
- How do I manage QoS (reliability, prioritization, load balancing)?
- How do I manage auditing?
- How do I upgrade to new web services versions without disrupting customers?
- How do I handle failures in services my application depends upon?
- How do I do root-cause analysis and identify the services causing performance/availability issues for my application?
- How do I log service requests for auditing purposes? (How much do I think I should be billed?)
- How do I handle the disparity in security mechanisms across different back-end services?
- How do I switch to new providers, without changing my calling application?

Service consumers
- SOA implemented for loosely-coupled approach for business-logic, but operational issues are deeply buried into applications
- Business parameters are hard-coded within every connection (SLAs, security certificates, connection type)
- Security is buried in applications
- Verifying compliance with policy guidelines is difficult
- Education and training on new standards and technologies requires significant investment
- Very difficult to deal with changing policies
- Integrations and software upgrades are costly

Enterprise IT
Web Services Security & Mgt Benefits

• Externalizing web services security
  • No web services security “silos”
• Focusing on domain expertise
  • Developers focus on business logic
  • Security architects and administrators focus on security and management
• Meeting governance requirements
  • Centralized corporate rules are applied
  • Security policies are defined in a single point of control
• Lowering costs of administration
  • Security policy changes are handled centrally, not in each web service
  • Security audits / reports are run across all web services from a single point of administration
  • Web services security and management environment is easier to deploy, maintain, and upgrade
Product Overview
Introducing Oracle WSM

• Standalone platform for securing and managing access to web services
  • Used by a developer, deployer, or security administrator
  • Does not require developers to modify applications or services (no programmatic security necessary)
  • Executes security policies in real time
  • Monitors all access-control events (graphical reports)
  • Provides tools for defining and monitoring service-level agreements (SLA)
  • Leverages backend identity management infrastructures such as Oracle Access Manager for authentication and authorization
Support For Key Security Standards

- Encryption algorithms: AES-128, AES-256, 3-DES
- Message digests: MD5, SHA-1
- Message structure: XML / SOAP / WS-Security1.0
  - Security token profiles: Username, X.509, SAML
- Message integrity: XML Signature,
- Message confidentiality: XML Encryption
- PKI
  - Key encryption: RSA OAEP-MGF1P, RSA V1.5
  - Signature algorithms: RSA (PKCS #1) (1024-, 2048-bit keys), DSA
  - Credentials store, wallets: PKCS#12
Oracle WSM Security Principles

BUILD Policies
Policy Manager

ENFORCE and EXECUTE Policies
Web Services Clients
Gateway
Agents
Applications or Web Services

MONITOR Policies
Monitor
Oracle WSM Management Console

![Oracle WSM Management Console](image)

### Enforcement Points

<table>
<thead>
<tr>
<th>Id</th>
<th>Name</th>
<th>Type</th>
<th>Details</th>
<th>Edit</th>
<th>Delete</th>
<th>Policies</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>C0003001</td>
<td>MyGateway</td>
<td>Gateway</td>
<td></td>
<td></td>
<td>⌚️</td>
<td>Policies</td>
<td>Steps</td>
</tr>
<tr>
<td>C0003002</td>
<td>anotherGateway</td>
<td>Gateway</td>
<td></td>
<td></td>
<td>⌚️</td>
<td>Policies</td>
<td>Steps</td>
</tr>
</tbody>
</table>
Oracle WSM Components

Clients

Web services

Policy Enforcement Points (PEP)

Oracle WSM server components

Gateway

Policy manager

Monitor

Management Console

Database
Oracle WSM Components

Clients

Policy Enforcement Points (PEP)

Oracle WSM server components

Agent

Agent

Agent

Agent

Agent

Policy manager

Monitor

Management Console

Web services

Database
Deploying a Server Agent to the Oracle Application Server

- Register the server agent and define security policies using the Oracle WSM console
- Deploy the server agent to the Oracle Application Server using the `wsmadmin` tool
# Comparing Gateways and Agents

<table>
<thead>
<tr>
<th>Features</th>
<th>Gateways</th>
<th>Agents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administration</td>
<td>Provides a central location</td>
<td>No new component to administer</td>
</tr>
<tr>
<td>Protocol Support</td>
<td>Can perform protocols translation</td>
<td>Leverages existing platforms and existing protocol support</td>
</tr>
<tr>
<td>Securing Services</td>
<td>Cannot guarantee endpoint-level security</td>
<td>Provides endpoint-level security</td>
</tr>
<tr>
<td></td>
<td>Single enforcement points to administer</td>
<td>Several enforcement points to administer</td>
</tr>
<tr>
<td>Impact on Clients</td>
<td>Need to point the client to the Gateway</td>
<td>No need to make changes in the client or the UDDI registry</td>
</tr>
</tbody>
</table>
Monitoring:
Snapshot of all Activities
Monitoring: Authentication & Authorization Events

Oracle Enterprise Manager 10g
Web Services Manager Control

Access Control

Access Control Display Criteria
Component: MyGateway
Service: ALL SERVICES
Time Range: Last hour

Access Control
Component: MyGateway
Service: ALL SERVICES
Start: Tuesday, August 15, 2006 04:59:00 PM
End: Tuesday, August 15, 2006 05:59:00 PM

Access Violation Of All Services:
- Access granted
- Access denied: Authentication failure
- Access Denied: Authorization Failure

Access Violation Per Service:

Click on bars to drill down into details, move your mouse over the graph to see more information.
Monitoring:
Traffic Analysis
Monitoring:
SLA Compliance

SLA Compliance Display Criteria

SLA Compliance

Component: MyGateway  Service: TimeService  Time Range: Last day

Display

SLA Compliance

Component: MyGateway  Service: TimeService  Start: Monday, August 14, 2006 08:21:00 PM  End: Tuesday, August 15, 2006 08:21:00 PM

Overall Availability: 80%  Availability SLA: Max Failure Rate: 5%

Latency SLA: Assured Latency: 5%

Overall Execution Summary:

Move your mouse over the pie wedges to see more information.
Use Cases
Protecting Access To Web Services Using Gateway

- The Gateway secures access to one or more web services at the web service provider site
  - Step1: The client posts a request to a web service
  - Step2: The Gateway intercepts the request, applies security policies (e.g., decryption, signature verification, authentication, authorization), and forwards the request to the web service
  - Step3: The web service returns a response
  - Step4: The Gateway intercepts the response, applies security policies (e.g., encryption), and forwards the response to the client
**Protecting Access to Web Service(s) Using Server-Side Agent**

- The OWSM Agent protects access to a web service at the web service provider (server-side Agent)
  - Step1: The client posts a request to a web service
  - Step2: The Agent intercepts the request, applies security policies (e.g., decryption, signature verification, authentication, authorization), and passes the request to the web service
  - Step3: The web service returns a response
  - Step4: The Agent intercepts the response, applies security policies (e.g., encryption), and passes the response to the client
Requesting Access To Web Service(s) Using Client-Side Agent

- The OWSM Client-Side Agent enforces web services policies from within the same web application as the service client
  - Step1: The client posts a request to a web service
  - Step2: The Agent intercepts the request, applies security policies (e.g., encryption, etc.), and passes the request to the web service
  - Step3: The web service processes the request and returns a response
  - Step4: The Agent intercepts the response, applies security policies (e.g., decryption), and passes the response to the client
Accessing External Web Services Using Gateway as a Reverse Proxy Server

• The purpose is to allow access to external web services only to specific web service clients making a request from within the corporate intranet
  • Step1: The client (within the corporate intranet’s boundaries) posts a request to an external web service
  • Step2: The Gateway intercepts the request, applies security policies (e.g., authentication, authorization), and forwards the request to the web service
  • Step3: The web service returns a response
  • Step4: The Gateway intercepts the response, applies security policies, and forwards the response to the client
Mapping Credentials Using Gateway and Server-Side Agent

- The web service client and the web service provider don’t support the same type of credentials
  - Step1: The client makes a web service request using basic credentials (“marcc”)
  - Step2: The Gateway intercepts and authenticates the request
  - Step3: Upon successful authentication, the Gateway inserts a SAML assertion in a WS-Security header that it posts to the web service provider as part of a SOAP message
  - Step4: The Agent validates the SAML assertion and passes the request to the web service
  - Step5: The web service returns a response intercepted by the Agent for security
  - Step6: The Agent returns the response to the web service client directly or via the Gateway
Mediating Heterogeneous Protocols Using Gateway

- The web service client and the web service provider don’t support the same protocol
  - In case 1, the Gateway resides within the Intranet and translates an outgoing HTTP request into JMS
  - In case 2, the Gateway resides outside the Intranet and provides access to HTTP-based web services from JMS-based requests
Virtualizing Web Services Using Gateway

Note: For clarity’s sake, responses are not represented in this use case

• The OWSM Gateway provides web services virtualization
  • Actual web services are bound to a virtual service (the Gateway)
  • Users first access the virtual web service and based on their roles, users may access selected actual web services
  • The transport protocol can also be virtualized, for example, all users access a virtual web service through one protocol (e.g., HTTP) and the virtual service can pass the request to an actual web service using a different protocol (e.g., JMS)
  • Users can create multiple versions of a virtual web service and redirect an older version of the virtual web service to a new version

[Diagram depicting the interactions between web service clients, virtual services, and actual web services through a Gateway, with protocols like HTTP and JMS shown.]
Roadmap

• Current Release: Oracle SOA Suite 10.1.3.1 (Available from October 2006)
  • OWSM is a full-fledged component of the Oracle SOA Suite
    • Oracle unified installer
    • OWSM also available as a standalone product
  • Leverages OC4J for high availability and quality of service
  • Globalization (I18N and L12N)
  • WSIL support
  • Oracle Enterprise Management (EM) look and feel
  • Support for additional encryption algorithm
  • Standards update (WS-Security / SAML)
Roadmap (Cont’d)

- **Oracle SOA Suite 11g (2007)**
  - Provide an end-to-end, application-centric SOA solution for the enterprise by fully integrating best-of-breed components
  - Provide a common, standards-based policy / agreement definition and policy attachment environment for the Oracle SOA suite based on OWSM’s Policy Manager (WS-Policy model)
  - Provide a single user interface and common management point across the Oracle SOA Suite based on Oracle Enterprise Management (EM)
  - Provide a consolidated gateway including security, connectivity, routing, and transformation functionality
ORACLE IS THE INFORMATION COMPANY
The preceding is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle’s products remain at the sole discretion of Oracle.