

# INTRODUCTION TO ORACLE WEB SERVICES MANAGER

*Dan Norris, dnorris(at)itconvergence.com, IT Convergence*

## INTRODUCTION AND OVERVIEW

A web service is a program that provides access to information or performs a function using standard protocols. Web services may employ many standards such as: SOAP, UDDI, XML, and WSDL. As web services have begun providing access to more sensitive information like bank account balances, credit reports, and other personal information, security for web services has become an issue. While some of the web services standards do offer authentication methods, performing complex authorization checks and policy management is difficult.

Oracle Web Services Manager (WSM) integrates tightly with the application server, and it provides an easy interface used to manage both web services and access to those web services. Access control is commonly handled by implementing a web services gateway that can provide authentication, logging, and selective notifications so that web service developers can focus on programming application functionality instead of security infrastructure.

## ORACLE WEB SERVICES MANAGER TERMS

With any new product, there are some unfamiliar terms used to describe various components. Here are some definitions to a few of the most common terms used when discussing WSM.

**Policy:** A policy is a rule that must be met in order to access the requested web service. There can be multiple policies defined for a given web service. Some policies may simply require a log entry to be created while others may require further authentication of a particular form (i.e. password or certificates).

**Policy Pipeline:** A policy pipeline is an ordered collection of policies that are applied to a web service access request before granting access to the request.

**Lightweight Directory Access Protocol (LDAP):** LDAP defines a network protocol for interacting with servers that follow the LDAP standard. LDAP is commonly used as a source for authenticating users in an WSM deployment.

**Enforcement Point:** An enforcement point is where a policy is applied to a web services request.

## ORACLE WEB SERVICES MANAGER ARCHITECTURE

There are many deployment options for WSM. This section will detail the most common deployment.

The diagram below depicts a basic deployment and its components.

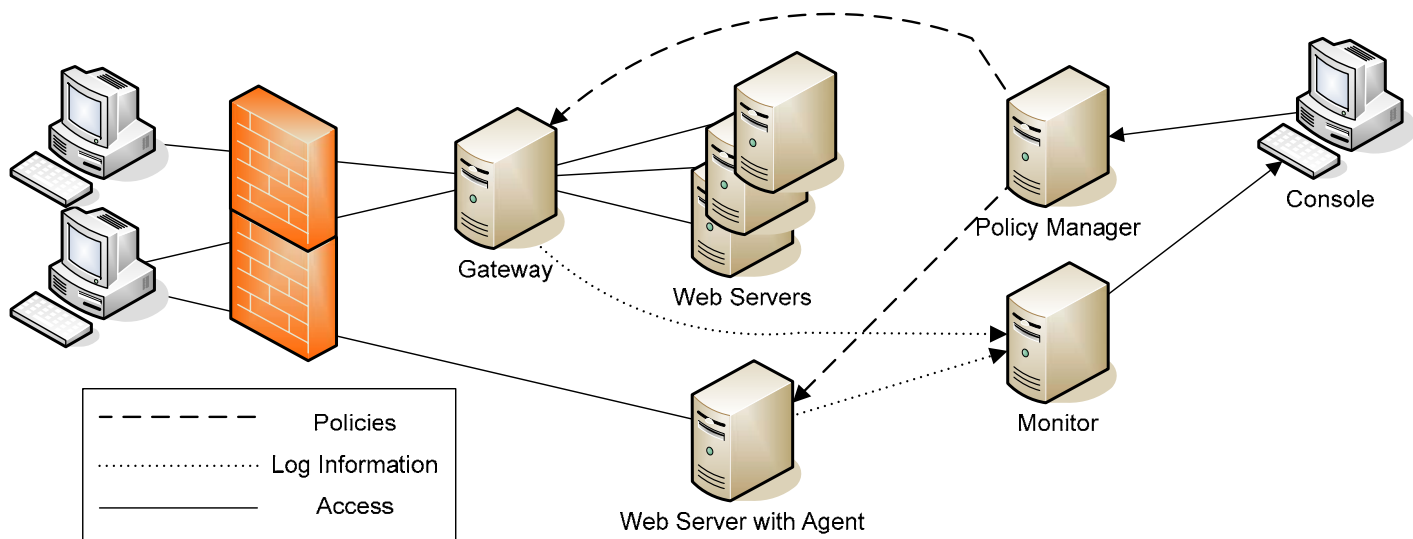


Figure 1: Basic WSM Deployment

## **ORACLE WSM COMPONENT TYPES AND FUNCTIONS**

There are several components that cooperate to provide the WSM features. The diagram in the section above depicts the major components and the purpose of each component.

### **WEB SERVICES POLICY MANAGER**

The Web Services Policy Manager component provides the primary management interface, and it is responsible for sending all policy pipelines to the enforcement points. The browser-based interface is used to create, modify, and version security policies for the entire WSM environment. Web services can be managed individually or in groups when similar policies must be applied to many services.

The Policy Manager is the first component to configure in a basic deployment. All other services interact with the Policy Manager or depend on it in some way.

### **WEB SERVICES MANAGEMENT GATEWAY**

The Web Services Management Gateway (or "Gateway") is an enforcement point for WSM. A Gateway acts as a proxy to keep the location and configuration of the data source secure. Like many proxies, the Gateway is also capable of transforming the protocol used to request service. For example, it may take an incoming HTTP request with an XML payload and transform that into a JMS message to a back-end web service. Gateways can also route messages to the proper service provider based on the content in the request. When combined with the proper policy pipeline, this message routing functionality makes Gateways very powerful tools for combining multiple back-end web services into a single logical service for presentation to users. The Policy Manager periodically sends updated policy pipelines to the Gateway.

### **WEB SERVICES MANAGEMENT AGENT**

A Web Services Management Agent (or "Agent") is also an enforcement point for WSM. An Agent is deployed in the same memory space as the web server hosting the service. This deployment allows for end-to-end encryption for the request data which may be important for sensitive data such as credit history or medical record data. Due to the deployment location, Agent enforcement points are unable to route requests to different back-end services. As with the Gateway, the Policy Manager sends updated policy pipelines to the Agent.

### **WEB SERVICES MONITOR**

The Web Services Monitor receives statistical information from Gateways and Agents as they service requests. The Monitor provides this information to the management console via the Policy Manager. These statistics can be used to measure response time, availability, and compliance with service level agreements.

## WEB SERVICES REGISTRY DATABASE(S)

The Oracle WSM environment requires at least one database to store information related to WSM components, policies, statistical data, and other administrative metadata. The quick install procedure includes an installation of Oracle Lite to serve as the repository for all WSM registry data.

## ORACLE WSM ADMINISTRATIVE INTERFACE

The main management interface for WSM is the browser-based Policy Manager. It is through this interface that you'll perform all enforcement point, policy, policy pipeline, and service configuration. Upon login, the console offers the interface shown below:

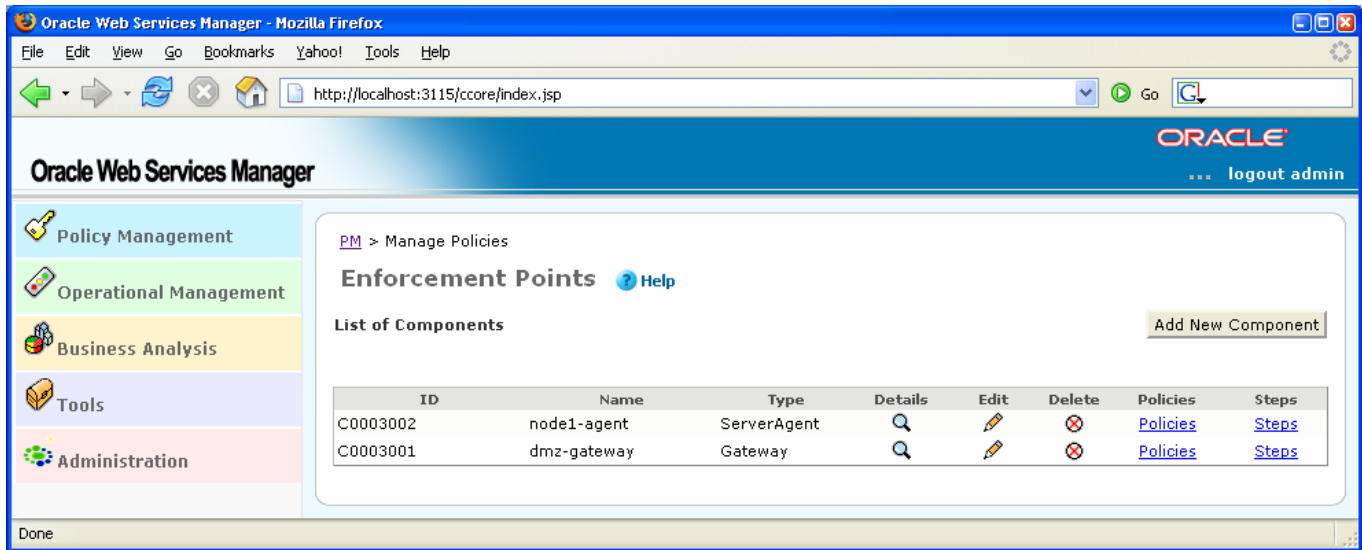


Figure 2: Oracle WSM Console

The left-hand navigation menu includes:

**Policy Management:** In this section, the administrator can add enforcement points, manage services for each gateway, and manage pipeline templates.

**Operational Management:** Here is where the statistics regarding response time, failure rates, and alarms are reported. There are multiple reporting options for time period, services included, and which enforcement point is being reported.

**Business Analysis:** Graphs and charts are two types of reporting that can be generated from the business analysis section of the Policy Manager interface. This is also where rules can be created to trigger alerts for key business-sensitive or important operations.

**Tools:** In the tools section, test harnesses can be created and stored to simulate client accesses for testing purposes. There is also a tool to ping the server to confirm that it is operational.

**Administration:** Oracle WSM supports multiple administrators with varying levels of privilege. This section of the Policy Manager is where privileges can be assigned to users.

## EXAMPLES OF WSM DEPLOYMENTS AND USES

### LOGGING OR AUDITING

Some policy pipelines may only require that an access be logged. The powerful log policy can be adjusted to record any of the following information from the request: envelope, body, header, or all.

All log entries are centralized to the Policy Manager and can be summarized for reporting purposes.

Below is what a very simple prerequisite logging pipeline may look like.

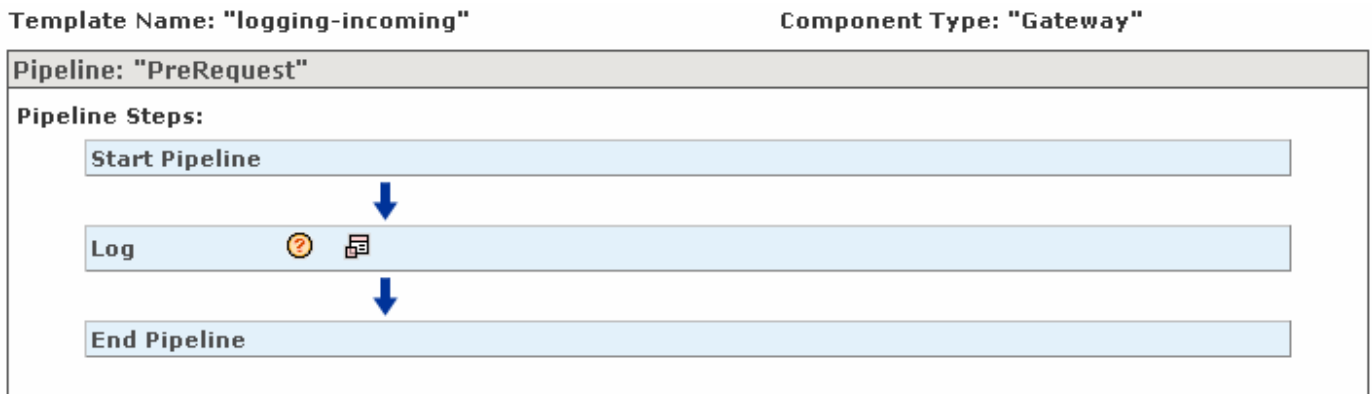


Figure 3: Basic Logging Pipeline

### ADDITIONAL AUTHENTICATION

Certain web service requests may require authentication. For these cases, Oracle WSM offers the capability to authenticate against several different types of external sources: COREid Identity and Access, Netegrity SiteMinder, Microsoft Active Directory, and standard LDAPv3 directories. Credentials for authentication are typically passed along in the request and defined in the WSDL for the web service. They can also be provided in other parts of the request and the Extract Credentials step can be used to pull out the credentials to be passed to later policies in the policy pipeline.

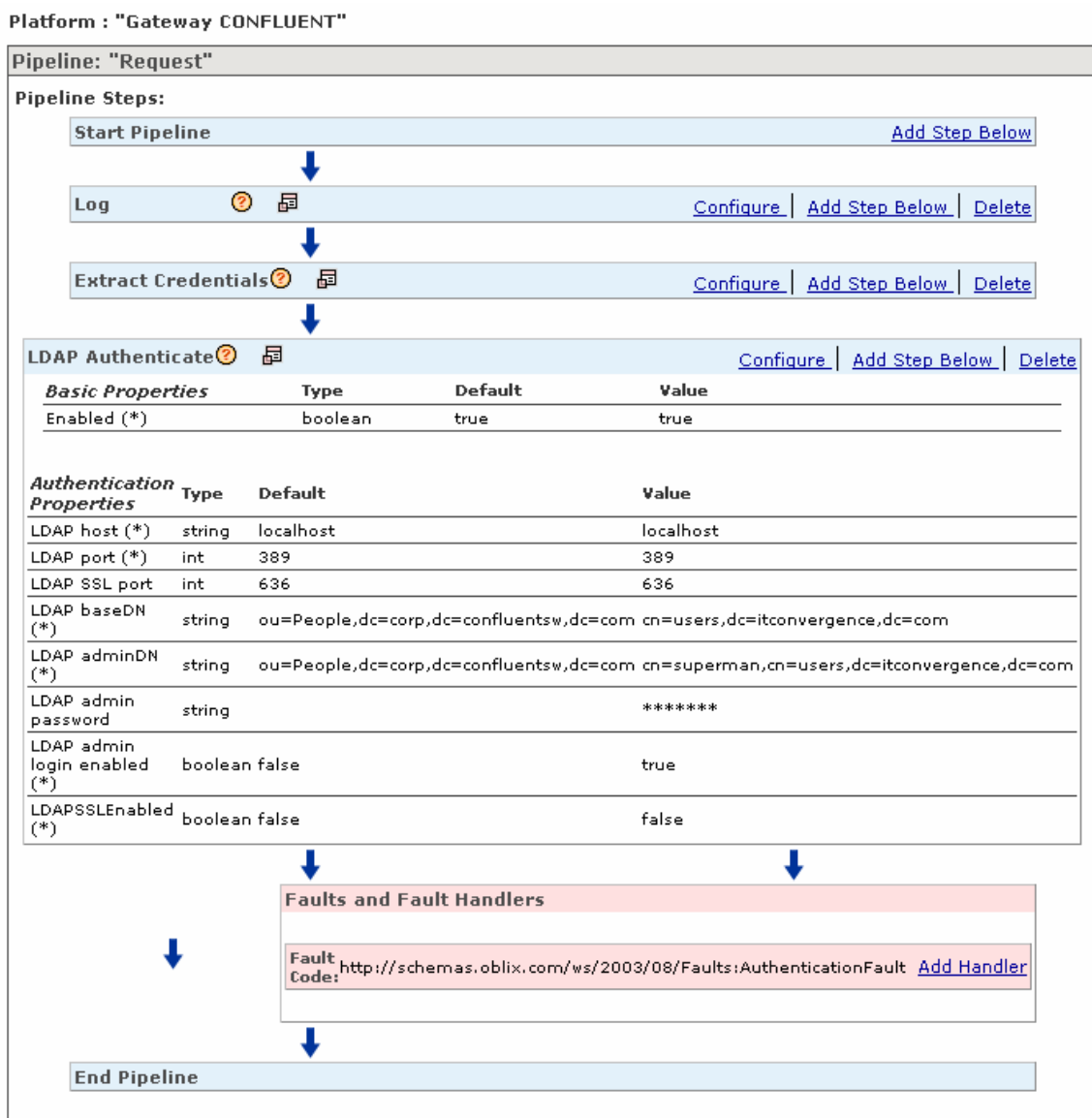


Figure 4: Additional Authentication Pipeline

**INTEGRATION POINTS WITH OTHER ORACLE AND NON-ORACLE PRODUCTS**

Oracle WSM Gateways don't require integration with the application at all. The Gateway is employed as a network device positioned as a proxy that does not interfere or integrate with the application directly. Gateways can be used with any application server and any application from any vendor. Gateway deployment is easy and designed to require little change in application behavior.

Oracle WSM Agents are deployed directly with the application and require tight integration with the application server platform. WSM Server Agents provide the ability to decrypt messages in the same address space where the application runs. WSM Agent deployments come in two varieties: server agents and client agents. Server agents are SOAP interceptors or servlet filters that are deployed with the web service application. For applications that require end-to-end encryption, Server Agents may be the best deployment option.

Client Agents are SOAP interceptors that must be deployed where the web service calls originate. This type of deployment may be used in many scenarios, but is commonly used with a logging-only deployment of an external web service for which you are a consumer. A Client Agent in this case would allow you to capture all outbound calls to the web service without having to add auditing capabilities to the application.

WSM provides server agents for selected application servers including Oracle OC4J, Apache Tomcat, BEA WebLogic, IBM WebSphere, TIBCO BW, and Microsoft .NET. Supported versions and platforms for each application server are listed in the installation guide. There are separate sections in the documentation related to TIBCO BW and Microsoft .NET deployments due to the special considerations when using these application environments.

Given the deployment method for Agents, integration for any of the supported application server environments is very similar and results in a supported configuration.

### **PACKAGING AND LICENSING OVERVIEW**

Oracle WSM is a part of the Oracle Application Server product family and it can be licensed by named user or on a per processor basis. According to the price list dated January 6, 2006, WSM licenses cost \$800 per named user or \$40,000 per processor. There may be prerequisites required to license WSM and minimums may also apply. WSM may be purchased separately or as part of the Identity Management Suite. The Identity Management Suite is licensed on a per user basis at \$80 per employee user and \$10 per non-employee (external) user.

You can also download WSM via Oracle Technology Network at <http://www.oracle.com/technology/software/products/ias/htdocs/101202.html> (subject to OTN license agreement).

### **REFERENCES**

- Oracle Web Services Manager Installation and Deployment Guide, 10g Release 2 (10.1.2), August 2005
- An Introduction to Oracle Web Services Manager; An Oracle White Paper, May 2005, [http://www.oracle.com/technology/products/webservices\\_manager/pdf/oracle\\_wsm\\_402\\_wp.pdf](http://www.oracle.com/technology/products/webservices_manager/pdf/oracle_wsm_402_wp.pdf)
- Oracle Web Services Manager 4.0.3 online help
- Oracle US Commercial Price List dated January 6, 2006, <http://www.oracle.com/corporate/pricing/pricelists.html>

### **FROM THE LAWYERS**

The information contained herein should be deemed reliable but not guaranteed. The author has made every attempt to provide current and accurate information. If you have any comments or suggestions, please contact the author at [dnorris@itconvergence.com](mailto:dnorris@itconvergence.com).