Oracle Application Server 10g Security

An Oracle White Paper
April 2006

ORACLE

Oracle Application Server 10g Security

INTRODUCTION

Businesses must address security concerns in several different categories, as more business is online and outsourced. Patch management, reducing email spam, eliminating spyware and virus control are being quickly transformed into table stakes in business operations. Platform and Application security however, address an entirely different set of security concerns related to applications that companies deploy both internally and externally across their lines of business. Application Security includes thinking through and standardizing on authentication, authorization, integrity, confidentiality, and access control mechanisms across the enterprise. The application server that powers and secures these applications has critical legal and business implications for companies, their corporate brands and their relationships with customers, employees and partners.

This paper discusses the business drivers that drive security features in application server and a high level description of the new security products and features in Oracle Application Server 10g Release 3. It is organized into two sections consisting of product level security features followed by deployment specific configuration options.

The product security feature section includes discussion on the Application Platform Suite Security, SSL Connectivity and key security features offered by some of the key components including Oracle Http Server, Oracle Web Cache and Oracle Containers for Java. Oracle Identity Management is a security offering within the Application Platform suite and this paper includes a brief discussion about its benefits. The deployment security section summarizes typical implementation concerns and offers solutions.

SECURITY DRIVERS IN AN ENTERPRISE

As more business is online, there is greater sensitivity to applying security to portals and applications that have grown over the years. The key aspects of security are the ability to

- Apply consistent security policies across all applications
- Ensure that the applications are protected with the appropriate level of security (user authentication and access control)
- Provide integration with existing security systems

- Simplify user management
- Provide privacy and confidentiality for all communications and transactions, and
- Support identity driven security in all applications

Decisions about single sign on for application aggregation and reducing the administrative complexities of identities across the enterprise are the front burner projects that are driving security.

An organization's business strategy is easily aligned with its security goals by selecting the right Application Server platform. Some of the major business initiatives are focused on content aggregation and deploying portals to address collaboration needs and easy information access. As a result, decisions about single sign on (a deployment aspect) and content aggregation (an administrative aspect) to simplify user experience and reduce administrative overhead are front burner projects driving security. This quickly cascades to decisions about:

- Managing identities (Identity Management) in a distributed environment
- Securing transactions over HTTPS protocol for security and privacy

ORACLE APPLICATION SERVER 10G – PRODUCT SECURITY

Oracle Application Server 10g is an integrated, standards-based software platform that allows organizations of all sizes to be more responsive to changing business requirements. It is a platform that provides an enterprise the ability to develop, deploy and manage middleware services in an efficient and cost effective manner. Managing security in an environment that consists of personalized portals, allows access from wired and wireless devices to business applications and dealing with application integration is serious business.

In order to achieve this, Oracle Application Server 10g provides security features in a number of components including

- Application Platform Suite (APS)
- SSL Connectivity
- Oracle HTTP Server
- Oracle Web Cache
- Oracle Identity Management

These components and features make Oracle Application Server uniquely able to provide the combination of flexibility and security across a broad range of enterprise applications and infrastructure.

Oracle Application Server 10g provides the platform to enable Identity Driven Security in your enterprise. It is unique in that it is the only application server platform that includes an Identity Management solution in its product offering. Oracle Application Server 10g components also provide security features such as the ability to communicate over SSL/TLS for over the wire encryption and several other PKI integration capabilities. Many of the components integrate with an

existing authentication infrastructure investment such as Kerberos, PKI or RADIUS, to aid a secure deployment.

Oracle Application Server 10g provides an Application Platform Suite (APS) that allows customers and system integrators to design and develop business solutions in an open, modular fashion that integrate with legacy and new applications with ease. Application Platform Suite is a comprehensive and integrated enterprise application infrastructure based on service-oriented architecture (SOA). The APS framework is designed to meet the following two key business goals of any enterprise:

Oracle Application Server 10g provides standards based solutions with Security and Interoperability as the key differentiators.

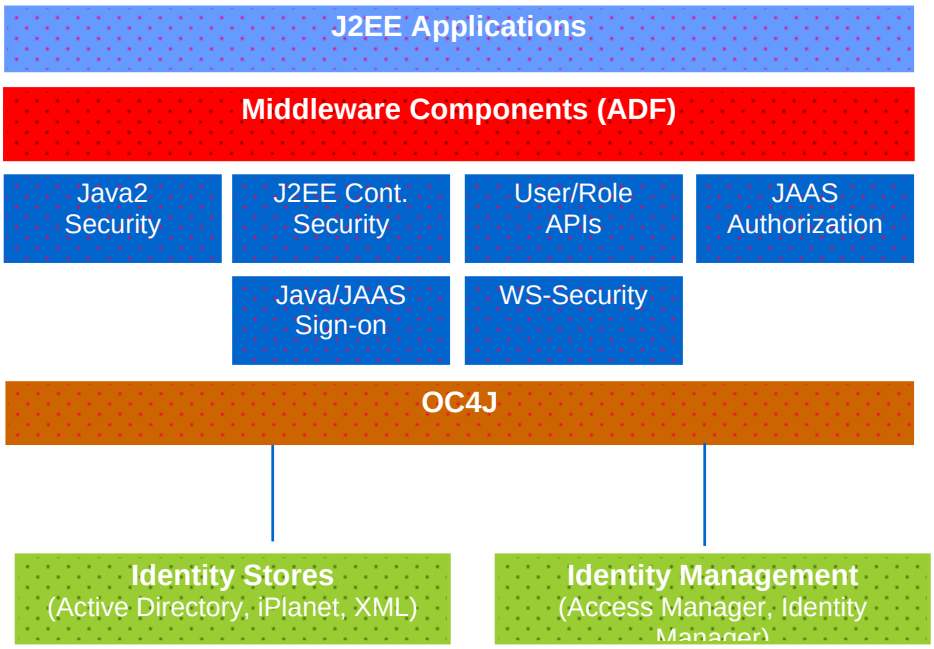
- *Standards based Interoperability with Security as primary driver.* As a Java platform, there is comprehensive compatibility with the Java Security Model in the APS components. This includes supporting standalone deployments of OC4J applications with Oracle Http Server that does not use an enterprise Identity Management deployment. Ability to deploy solution based on Liberty and WS-Security and SAML standards is a key purchasing criterion for many businesses. Usage of SSL /TLS is ubiquitous in the Application Server world and the encryption and strong authentication capabilities provided by Oracle Application Server 10g uses industry standard algorithms.
- *Integration with existing security infrastructure such as an Enterprise Identity Management solution.* APS provides tight integration with Oracle Identity Management. Oracle Identity Management is a key component of the Oracle Application Server 10g and provides the infrastructure to centrally manage user and application identities, their authorizations and other policy decision points. This component serves as the provisioning and/or synchronizing hub to facilitate Oracle applications or components integration with the chosen enterprise Identity Management system.

Application Platform Suite Security

As a standard Java platform, Application Platform Suite (APS) offers the standard Java Security Model services for authentication, authorization and accountability. APS delivers user management and administration APIs that enable consistent enterprise deployments. Oracle Application Server 10g components rely on the APS framework for delivering their security interfaces to their end users.

APS uses standard Java Authentication and Authorization Service (JAAS) to provide pluggable authentication and permissions based authorization for all Oracle Application Server components. Application Platform Suite provides the infrastructure to enable one or more authentication mechanisms for the container. These authentication mechanisms can include passwords, Kerberos credentials or digital certificates (for PKI).

Figure: Application Platform Suite Security



The JAAS model is also used to implement the fine-grained access control security aware applications whose security requirements are not handled by the runtime J2EE security. The access control lists are also referred to as security policies. These are permissions to access specific resources, which are aggregated in a policy store. When an OC4J container is configured to rely on the security policy store, multiple OC4J applications or EJBs deployed in that instance now share a common security authorization policy. The choice of a standard XML file or an LDAP repository as the policy store can be deferred to deployment time as APS provides the flexibility to choose and move between both transparently.

In Oracle Application Server 10g, OC4J security can be configured to redirect authentication to Identity Management solutions such as Oracle Access Manager and Oracle Single Sign-on. This works well for J2EE applications such as Oracle Portal. For standalone OC4J deployments, APS provides the flexibility to use any user repository (user store) such as any 3rd party LDAP server for enterprise deployment or, simple XML files and have custom login modules for departmental application deployment.

Java Security

J2EE applications in general have the ability to use either XML or an LDAP based repository for user, role and security policy administration. As one might expect, integration with JAAS provides a greater degree of freedom to security aware applications. Oracle Application Server's components such as Portal, Business Intelligence, Forms and Reports rely on the Application Platform Suite security to integrate with any deployment environment.

Oracle Application Server 10g J2EE platform supports the declarative security model while retaining its ability to provide security APIs to the security developers in your organization. The declarative security model respects the distinction between a development and deployment environment making it easy for developers to develop, test and deploy applications relying on the framework for the security expertise. Security is expressed in a Deployment Descriptor file to express security roles, access control, and authentication requirements. The programmatic security model provides finer control over user and role information to the J2EE applications. Using programmatic security along with declarative security provides J2EE applications with the ability to be flexible and secure at the same time.

Authentication and Authorization for OC4J applications

Java platform supports three distinct authentication modes

- When relying on Oracle Identity Management system, it supports integration with Oracle AS Single Sign-on.
- When relying on Oracle Access Manager, it supports authentication and authorization through the policies and authentication form factors supported by this product.
- When relying on JAAS framework, it supports pluggable authentication module using its custom LoginModule.
- An out-of-the-box RealmLoginModule support for non-SSO environments

J2EE container (OC4J) integration with JAAS provides distinct advantages in terms of providing integration with Single Sign On for usability. J2EE security provides identity propagation between servlets or EJBs, fine grained access control with permissions and secure storage of passwords with keystore implementations. Furthermore, OC4J security provides hierarchical role support with role-based access control, provides comprehensive support for Java2 Permission model.

Web Services Security

Service-Oriented Architecture is a methodology that enables loose coupling between interacting processes. The success of this architecture depends on its ability to interface amongst these processes with consistent interfaces. A critical aspect of SOA is that the security context that is established at the producer end is passed on to the consumer. Oracle Application Server 10g provides transport level security to deploy Web Services.

Identity Propagation

Identities can be propagated between an application and an EJB deployed within an OC4J instance as there is a trust relationship established within the instance. The target receives the propagated identity and performs authorization checks alone.

OC4J also supports identity propagation in ORMI (OC4J Remote Method Invocation) as well as CSI v2.

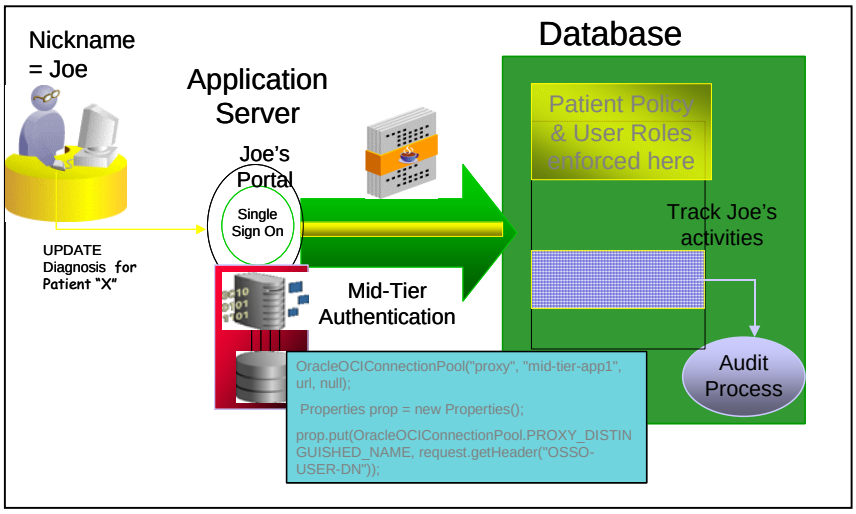
Integration with Database Security

Oracle Application Server 10g is the only platform that is capable of providing a variety of identity propagation mechanisms across all tiers.

Database security features including database roles, VPD and Label Security policies can be enabled if the application's user repository is the Oracle Identity Management system. By configuring the Enterprise User Security feature of the Oracle Database Enterprise Edition, the database participates in the "Identity Driven" enterprise and the applications can in turn enjoy the benefits of strong database security.

Typically, mid-tier applications set up a connection pool for managing database access requests. When a Single Sign On User makes a request to access a database resource, the mid-tier application can proxy the user's identity by his Distinguished Name (DN), username/password or just the username. This feature provides a way to drive the compliance architecture in any enterprise as the user's identity can be preserved right up to the data tier so that his/her transactions can be audited. An example of this request is in the figure below.

Figure: Identity Propagation with Enterprise User Security



SSL Connectivity for Application Server Components

Oracle Application Server 10g components can communicate with one another over secure sockets layer. Users accessing applications can communicate over the https protocol. This functionality is mature and has now been available for several releases.

Oracle Cryptographic Libraries for SSL (Release 9.0.4) have received Federal Information Processing Standards (FIPS) 140-2 evaluation.

The Oracle Application Server has the capability to use the new industry SSL protocol standard, TLS 1.0. While TLS 1.0 is based on SSL 3.0, the more tangible benefits for Oracle users using TLS 1.0 are

- Relatively improved efficiencies for CPU intensive cryptographic operations resulting in increased SSL based throughput
- Improved TLS Handshake Protocol that provides increased privacy and integrity for peer-to-peer communication

Oracle Wallet Manager continues to be the tool to use for certificate requests and other certificate management tasks for the end user. Additional command line utilities that assist in managing Certificate Revocation Lists (CRLs) and other Oracle Wallet operations are also available in this release. Certification Revocation Lists published to an LDAP server, a file system or a URL is supported by Oracle's SSL infrastructure.

PKCS#11 Support, Smart Cards/Hardware Security Modules

An Oracle Wallet is a software container that holds the private key and other trust points of the certificate. Oracle's SSL libraries support PKCS#11 industry standard. This allows the private keys that were previously stored on the file system to be created and stored in secure devices such as Hardware Security Modules or Smart Cards that are available in the market.

Interoperability with PKI Vendors

As Oracle SSL libraries are industry standards compliant, certificates issued by many of the leading PKI vendors including Oracle Certificate Authority can be used in an Oracle environment. The certificate request when originating from Oracle Wallet Manager must be followed up by a certificate import when issued by the appropriate Certificate Authority. If the certificate is provisioned by other means (external to Oracle Wallet Manager), converting it into a PKCS#12 format will allow interoperability with an Oracle Environment.

Oracle Http Server Security

Oracle Application Server 10g HTTP Server (OHS) provides a web server to create dynamic applications. Based on the proven Apache 1.3.28 Infrastructure, Oracle HTTP Server adds significant enhancements including Dynamic Monitoring Service (DMS), Perl (via mod_perl, cgi), C (via CGI, and FastCGI), C++ (FastCGI), PHP and PLSQL for tighter integration with Oracle Database. OHS can also be configured as a forward or reverse proxy server.

Oracle Http Server provides strong security solutions by enforcing transport level security, certificate based authentication. It also supports hardware acceleration and integration with modsecurity plug in to eliminate unwanted requests.

The Web Server component of Oracle HTTP Server (OHS) provides the standard web server security features including Encryption, Authentication and Authorization. Using standard SSLv3 and TLS Oracle Http Server is able to provide network encryption using the more recent NIST approved AES Cipher suites. The web server can be configured to rely on Oracle Single Sign On Server for authentication. As a result an application developer can truly be agnostic to the deployment choice for authentication.

Oracle Http Server Integration with Oracle Identity Management

This integration is achieved via a standard Apache mode called "mod_osso" (Mod for Oracle Single Sign On). This integration allows an organization to leverage their investment in an enterprise directory and rely on the directory experts to manage users and authorization. The example below illustrates the integration.

1. Customer requests the page http://www.foo.com/subscribe/content

2. OHS recognizes that the customer has not logged in, and redirects him to Oracle Single Sign On Server (SSO).

3. The customer logs in and is redirected by SSO server to their requested page. The SSO Server sets an encrypted cookie that its partner applications - such as mod_osso - can decrypt.

4. When OHS receives the request (again), it detects the existence of the encrypted login cookie and serves up the page.

5. The Single Sign On Server has the ability to time out a login cookie. During the time the cookie is valid, the end user will experience single sign on to other partner applications to the Oracle Single Sign On Server.

Oracle Http Server support for SSL Renegotiation

Oracle Http Server provides groups based authorization schemes for both static and dynamic applications.

The SSL renegotiation capability allows an individual directory to be protected by encryption algorithms of varying strength. A common application is to have a directory that allows access when a client is authenticated only with a specific strength certificate (2048 bit key size as opposed to 512 bit key size). An SSL request from the browser to access this directory is redirected to get the client certificate for computing the authorization.

SSL Hardware Accelerator support

Since SSL authentication is resource intensive, SSL hardware accelerators provide a way to offload the mathematical computations to the accelerator. This new feature supports the nCipher hardware accelerator card and improves performance.

Mod_Security Plug In

Oracle Http Server 10g bundles mod_security plug in for Apache. This provides a non-invasive method to define filters to detect anomalies (such as SQL injections) and prescribe appropriate actions. ModSecurity is an open source intrusion detection and prevention engine for web applications. Audit logs of the POST payload analysis and request filtering is available for further analysis. For more information, please visit http://modsecurity.org.

Oracle Web Cache Security

OracleAS Web Cache can be configured to cache pages for https protocol requests. Oracle AS Web Cache relies on the Oracle SSL libraries for its SSL services and as a result it supports TLS and AES cipher suites and provides hardware acceleration support. Oracle AS WebCache integration with Oracle Identity Management provides it the ability to support client and server authentication with digital certificates.

Oracle Identity Management

Identity Management provides common security and management infrastructure for Web and enterprise applications that can be applied across all application tiers. Oracle Identity Management provides the solutions to enable secure management of business transactions in a networked enterprise.

Oracle Identity Management solution provides provisioning and centralized user and access management solution that operates in a heterogeneous environment.

Oracle Identity Management includes the following components:

Oracle Internet Directory

The central component of Oracle Identity Management, Oracle Internet Directory is a robust LDAP v3 compliant directory service. Oracle Internet Directory acts as a central point of integration for Oracle applications, as well as third party directories/applications. Oracle Internet Directory is deployed on the Oracle 10g database.

Oracle Directory Integration Platform

Oracle Directory Integration Platform enables synchronization between Oracle Internet Directory and other directories. The service supports third party directories, such as Microsoft's Active Directory and SunONE Directory Server, as well as Oracle HR.

Oracle Provisioning Integration Service

This service enables automated provisioning functionality throughout the Oracle application environment, as well as for third party applications.

Oracle Delegated Administration Service

Delegated Administration Service is an administration console that provides administrators with extensive Oracle Internet Directory management tools. Administrators can manage users or groups, or delegate administrative

responsibilities to individual departments. Delegated Administration Service also includes a customizable end user self-provisioning service, including password reset.

Oracle 10g Single Sign-On

Oracle 10g Single Sign-On provides web browsers require based single sign-on capabilities for Oracle partner and non-partner applications and provides integration with external Single Sign-On solutions such as *Entrust, Netegrity, RSA*, and federated systems. Oracle 10g Single Sign-On is standards-based, with support for HTTP(s), cookies, and X.509 certificates. By combining multilevel authentication functionality with Single Sign On capability, it delivers security with usability.

Oracle 10g Certificate Authority

Oracle 10g Certificate Authority enables corporations to provision users and servers with digital certificates for authentication and encryption. The Certificate Authority's integration with Oracle 10g Single Sign-On Server and Oracle 10g Oracle Internet Directory provides a unique certificate provisioning capability for Single Sign On Users.

Oracle Secure Federation Services

New in Oracle Identity Management 10g is the Oracle Secure Federation Services functionality. With support for SAML (Security Assertion Mark-up Language), Liberty Alliance and WS-Federation (Web Services Federation Language), Oracle Secure Federation in Services can synchronize with external applications, and enable Single Sign-On functionality.

Oracle Identity Management provides solutions that assist in achieving regulatory compliance. For example, consistent password policies can be define and enabled in Oracle Internet Directory. These centralized policies can constrain the password values and/or the password state. The Oracle Database and the Single Sign On Server can enforce these value and state based policies. Delegated administration is a powerful concept that helps in enabling separation of duties by using the system of least privilege.

ORACLE APPLICATION SERVER 10G - DEPLOYMENT SECURITY

In a typical enterprise deployment, security is of utmost concern considering the increasing classes of threats on the Internet including Encryption, Strong Authentication or multi level authentication for different applications, Flexible administration for multi-application deployments, Super user accountability.

Encryption

Oracle Application Server 10g provides standard SSL and Transport Layer Security (TLS) for wire level security. In order to secure back end communication between

the application server and the database, you have a choice of using SSL or other native encryption algorithms offered by Oracle Advanced Security, an Oracle Database Enterprise Edition option.

Single Sign On – Authentication

Oracle Application Server 10g components can participate in enterprise's Single Sign On initiatives using Oracle Identity Management as the security infrastructure. Oracle Identity Management serves as the gateway to integrate with the existing Enterprise Directory infrastructure.

Certificate Based Authentication

Oracle Application Server 10g supports mutual authentication or server authentication with certificates. Users can use certificates that have been provisioned without using Oracle Wallet Manager as long as they are in the standard PKCS#12 format. The private key and/or certificates can reside in a smart card or a hardware security module that speaks the standard PKCS#11 interface. Oracle Corporation has tested the PKCS#11 integration with devices from the following vendors:

- ActivCard
- NCipher, nForce, nShield
- Safenet Inc, Luna SA module
- AET, smart cards

Delegated Administration – Authorization

Oracle Application Server 10g operates using the principles of least privileges delegates only the relevant authorization for installation and administration. The installation privileges are further separated from the administration privileges. As the Oracle Identity Management serves as the security infrastructure for Oracle Application Server components, each of the component administrators can be defined with just the right level of authorizations required to administer the component instead of being a directory administrator or a super user. This separation of privileges is extremely important for secure deployments, as the right to install and /or administer one Application Server component does not automatically grant the privileges to install and/or administer another component.

Self Service for securing end user credentials

A very specific scenario that brings home the power of delegation is self-service for end user password management using Oracle Id Management's Delegated Administrative Services. A very big compliance initiative that organizations are sensitive to in the current regulatory environment is to limit the power of an administrator. An Oracle Identity Management deployment can choose to only provide read and modify rights to the user password only to them selves (self).

Port Tunneling

Oracle Application Server 10g uses AJP protocol for routing communication between Oracle HTTP Server and Oracle Application Server Containers for J2EE (OC4J). By routing requests through a port tunnel process to multiple OC4J instances, the Oracle Http Server requires only limited ports to be opened on the firewall.

Application Security

Oracle Http Server 10g provides mod_security plug in that allows a deployment to define rules to eliminate unexpected requests even before they reach the web server. At a minimum, it provides URL encoding validation, Unicode encoding validation and byte range verification to detect and reject shellcode. It provides the ability to define custom filters that can be used to deny any "ALTER SYSTEM" or "DROP TABLE" commands at the database. For more details on the functionality, please visit http://www.modsecurity.org.

Accountability

Oracle Identity Management that provides the security infrastructure for Oracle Application Server components has the ability to audit

- Super User events across all components
- Authenticated related Events (Deny or Grant)
- Authorization Policy Changes on any directory container

Deployment Configurations

Oracle Application Server 10g components offer several secure deployment alternatives that meet the requirements of several situations. The standard deployment supports a configuration where all incoming network traffic is handled by the load balancer router on a single secure port. The appliance then, routes the traffic to internal IP addresses within the firewall. The components themselves can be grouped as logical entities within the DMZ. The communication between components across the DMZ is restricted by port and protocol.

A typical implementation consists of the

- Web Tier

  An Internet facing service that usually consists of OracleAS Single Sign On, Oracle Http Server, Oracle Web Cache and certain key components of Oracle Delegated Administration Services. The idea is that only port 80 and 443 be open (for Non-SSL and SSL traffic respectively) on the firewall in order to communicate with the corporate servers.

- App Tier

This tier is within the DMZ and hosts the OC4J applications, Portal Applications and any other web based application that can receive on AJP ports. OC4J applications can be deployed as stand alone apps with authorizations being served from local JAZN XML files or they can be deployed as mainstream apps to depend on the Oracle Identity Management framework.

- Data Tier

  This layer holds the key security infrastructure components and is well within the corporate intranet behind another firewall. The remaining Oracle Identity Management components that can be deployed in this layer are the Oracle Internet Directory, Oracle Delegated Administration Service, Oracle Provisioning and Synchronization services.

Please refer to Oracle Application Server Deployment Guide for detailed description of the several deployment scenarios.

Separation of duties, a key deployment choice

The ability to deploy all the components in a manner that preserves the integrity of the enterprise without increasing the business exposure is a compelling purchasing decision driver. Oracle Application Server 10g relies on Oracle Identity Management's Privilege Delegation model to offer a clean distinction between an application installer and an application administrator, or distinguish between a an application developer, a security administrator and a security developer. The role distinction assists in driving the compliance architecture of an organization. For example with Oracle Application Server 10g, a Portal administrator role can be configured to have no privileges to manage the creation of new users for an HR application.

WEB SERVICES MANAGEMENT AND SECURITY

OWSM Key Features

- Easy to configure and administer using browser-based tools
- Supports multiple and flexible deployment models
- Supports clustering of server components for high availability and scalability
- Extensible standards-based framework
- Allows versioning of policies
- Supports migration of policy development from development to testing, and then on to production
- Enables policy-caching for high-performance.

Oracle Application Server 10g is complemented by Oracle Web Services Manager (OWSM), which consists of three components:

- OWSM Policy Manager
- OWSM Monitor
- OWSM Enforcement Components – Gateways and Agents

OWSM Policy Manager

OWSM Policy Manager has framework for configuring operational rules and security policies and propagating them to its policy enforcement points. At run-time, OWSM's enforcement components intercepts all SOAP requests exchanged between managed Web services, and then apply the right operational rules before any communication occurs.

OWSM Monitor

To provide visibility into these applications interactions, OWSM Monitor receives real-time information from OWSM's enforcement components and instantly reports on the health, performance, security, and compliance of the entire Web services network.

OWSM Enforcement Components – Gateways and Agents

Once the policy pipelines are created with OWSM Policy Manager and propagated to OWSM's enforcement components, agents and gateways. Agents execute in the same process as the application they control, while gateways run on separate processes and possibly on different servers than the applications they control. Also, gateways can manage services from multiple applications while agents control services belonging to the same application.

Agents are SOAP interceptors that enforce Web services policies from within the same Web application as the service client (client-Agents) or the service provider (server- Agents). Gateways are SOAP/XML intermediaries that enforce Web services policies while intermediating Web services traffic between clients and services.

Unique to Gateways is the ability to route service-requests based on their header and content, and to operate on top of different transport protocols. For example, a gateway could receive a SOAP request over HTTP and route it to the target service over JMS or IBM MQ. These capabilities make a gateway suitable for managing interactions among trading partners and with legacy applications.

ORACLE APPLICATION SERVER 10G – DEVELOPER SUPPORT

JDeveloper

Oracle JDeveloper is a Java IDE for writing J2EE applications. It supports ADF security, which simplifies the process of adding security to an application. It also supports adding JAAS authentication and authorization services to enable applications to control access to protected resources. More information on Jdeveloper can be found on oracle.com:

- JDeveloper 10g on Oracle Technical Network

ADF Security

The Oracle ADF security framework is built upon a pluggable architecture that allows applications to be built without needing to understand the specifics of the security service implementation. To do this, the framework implements the Java Authentication and Authorization Service (JAAS) for authentication and authorization, which provides a way to restrict access to the application or parts of the application (called resources) based on the user attempting to access the resource. Authentication provides a way to determine who the current user is.

Authorization provides a way to restrict access to a resource based on the user attempting access.

Oracle ADF Security can authenticate users against data within various resource providers. You can create login pages for both ADF Swing and JSP or JSPX pages, that collect user name and password data. Once that data is verified against the data store, the user is authenticated and the application knows about that user.

Read these topics to learn more about authentication using Oracle ADF Security:

- About Authentication Using Oracle ADF Security Service
- About Creating a JSP Using Oracle ADF Security
- About Creating a Swing Login Page Using Oracle ADF Security
- Implementing Authentication Using Oracle ADF Security

You can set authorization policies against resources and users. For example, you can allow only certain groups of users the ability to view, create or change certain data or invoke certain methods. Or you can prevent components from rendering based on the group a user belongs to. Because the user has been authenticated, the application can determine whether or not that user is allowed to access any object that has an authorization restraint configured against it.

CONCLUSION

Oracle Application Server 10g provides consistency and simplicity in user management and administration of security policies across the Oracle components (including Oracle Database and Oracle Applications). Oracle Identity Management provides the required security infrastructure to deliver this capability.

Oracle Application Server 10g is a Java Platform and allows enterprises to build and deploy pure java applications adhering to the Java Security and J2EE security standards. The platform offers enterprises the flexibility to integrate with one or more security infrastructures. The degrees of freedom in choosing an authentication framework, authorization framework and user stores and policy stores offered by Oracle Application Server 10g suits every unique need of an organization.

Oracle Application Server 10g Security
April 2006
Author: William Bathurst
Contributing Authors: Michael Mesaros, Chris Radkowski, Sudha Iyer

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200
www.oracle.com