Oracle Platform Security Services & Authorization Policy Manager

Vinay Shukla
July 2010
The following 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.
Agenda

• Application Security Challenges
• Oracle Platform Security Services
• Powering the Next Generation of Applications
• OPSS as IDM Integration platform
• Authorization Policy Manager
• Benefits
• Summary
• Resources
How do Applications Deal with Security Today?

Business applications need many aspects of security:

- Provisioning
- Authorization
- Authentication
- Identity Data
- Federation
- Audit
How do Applications Deal with Security Today?

Application developers end up building & embedding security…

- User tables
- LDAP Schemas
- Role repository
- Policy repository
- Registration processes
- Administration functionality
- Profile management
- Security & business policy enforcement
- …
The Result..

- Complexity
- Lack of agility
- Cost

CxO’s Nightmare
Challenge : Complexity

- Application security is fragmented
- App developers are required to understand and implement security
- Multiple apps with security holes leads to increased risk of breaches
- Lack of visibility and manageability of security and compliance
Challenge: Lack of Agility

- Integration requires custom point-to-point hardwiring
- Changes lead to redeployment & testing
- Bolt-on solutions lead to vendor lock-in
Challenge: Cost

• Time-to-Market Delays
• Integration Costs
• Administrative Costs
• Lower IT Agility
• Slower Innovation
What is needed of Security
Service Oriented & Application Centric Security

- Externalized & loosely coupled
- Application centric - supports application life cycle
- Provides re-usable security services
- Integrates with IdM
- Standards based & Comprehensive
- Security for the cloud ready enterprise
Oracle Platform Security Services

Introducing OPSS

- The security platform for Oracle Fusion Middleware and Applications
- Declarative, Enterprise-grade Security Framework
- Standards-based services exposed through pluggable abstraction layers
Oracle Platform Security Services

Key Features

**Authentication & Identity Services**
- JAAS Login Modules
- LDAP server integration
- SAML, Kerberos, SPNEGO token support
- Identity profiles via Identity Governance Framework

**Authorization Services**
- JAAS Permissions
- Role Based Access Control (RBAC)
- Declarative support through ADF and JDeveloper

**Audit Framework**
- Common Audit Framework (CAF)
- Centralized Audit Policy Mgmt & storage
- Pre-built BI Audit reports
- E2E tracing through ECID

**Credentials and Cryptography**
- Secure storage of credentials
- Oracle Security Developers Toolkit (OSDT)
- Based on Java Cryptography Extensions (JCE)
- Supports XML-Sig, XML-Enc, SAML
Application Centric Security
Supports all phases of application life cycle

Oracle Fusion Middleware

Oracle Platform Security Services

Identity Store, Credential Store, and Policy Store Providers

LDAP Directories  File  Databases

Copyright © 2010, Oracle. All rights reserved
Oracle Platform Security Services
IDM enablement platform for Applications & Middleware

Oracle Platform Security Services
AuthN
AuthZ
Creds & Keys
Audit
ID Profile
Trust
XML Security Crypto, SSL

Security Service Providers
OAM
OES
OAAM*
OID, OVD ODSEE
OIM*
STS
OWSM

Identity, Policy, Credential Store Providers

File LDAP Database

Copyright © 2010, Oracle. All rights reserved
Oracle Platform Security Services

Example: Authentication & Identity Profiles

Design Time

**Develop : JDeveloper**
- Declarative Development
- Security Wizards

**Test : Integrated WLS**
- login()
- logout()
- getUserProfile()
- getUserGroups()
- etc....

**Authentication**
- Form Based Authn

**ID Store**
- WLS Embedded LDAP
Oracle Platform Security Services
Example: Authentication & Identity Profiles

Design Time

Develop: JDeveloper
- Declarative Development
- Security Wizards

Test: Integrated WLS
- login()
- logout()
- getUserProfile()
- getUserGroups()
- etc...

Authentication
- Form Based Authn

ID Store
- WLS Embedded LDAP

Production

Deploy & Config: EM
- Deploy & Config Wizards
- Runtime Monitoring

Runtime: WLS, WAS, JBoss
- login()
- logout()
- getUserProfile()
- getUserGroups()
- etc...

Authentication
- OAM or 3rd Party SSO

ID Store
- Oracle or 3rd Party LDAP
Oracle Platform Security Services
Example: Authentication & Identity Profiles

**Design Time**
- **Develop**: JDeveloper
  - Declarative Development
  - Security Wizards
- **Test**: Integrated WLS
  - login()
  - logout()
  - getUserProfile()
  - getUserGroups()
  - etc...
- **OPSS**
- **Authentication**
- **ID Store**
- **WLS Embedded LDAP**

**Production**
- **Deploy & Config**: EM
  - Deploy & Config Wizards
  - Runtime Monitoring
- **Runtime**: WLS, WAS, JBoss
  - login()
  - logout()
  - getUserProfile()
  - getUserGroups()
  - etc...
- **OPSS**
- **Authentication**
- **ID Store**
- **OAM or 3rd Party SSO**
- **Oracle or 3rd Party LDAP**

*No Code Changes!*
# Oracle Products using OPSS

**Used by over 50 Products in FMW, Apps & GBU**

<table>
<thead>
<tr>
<th>Product</th>
<th>What it does</th>
<th>How it uses OPSS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle ADF &amp; WebCenter</td>
<td>ADF is the framework used to develop WebCenter applications (portlets, etc.)</td>
<td>Authentication, Authorization, Audit, Policy management, Credential store framework, Identity Profile</td>
</tr>
<tr>
<td>Oracle SOA Suite</td>
<td>Provides applications designed to deploy SOA environments (BPEL, ESB, etc.)</td>
<td>Authentication, Authorization, Audit, Identity Profile, Credential Store Framework</td>
</tr>
<tr>
<td>Oracle Entitlements Service (OES)</td>
<td>Provides externalized fine-grained authorization</td>
<td>Authentication, Identity assertion, Authorization, Role mapping, Credential mapping, Cert. lookup, Audit.</td>
</tr>
<tr>
<td>WebLogic Server (WLS) Container</td>
<td>Java EE server / container</td>
<td>Authentication, identity assertion, authorization, role mapping, credential mapping, Cert. lookup, Audit, SSO, SSPI framework for third-party integration</td>
</tr>
<tr>
<td>Oracle Access Manager</td>
<td>Enterprise Single Sign On</td>
<td>Identity Assertion</td>
</tr>
<tr>
<td>Oracle Web Services Manager (OWSM)</td>
<td>Provides SOA and web services security</td>
<td>Authentication, Authorization, Key store service, Credential store framework and Audit</td>
</tr>
<tr>
<td>Fusion Applications</td>
<td>Next Gen Packaged Applications</td>
<td>All services</td>
</tr>
</tbody>
</table>
Fusion Applications Security
One Integrated Security Solution

• Rationalized, Centralized, and Externalized
  – Authorization policies & decisions
  – Authentication policies & services
  – User provisioning & administration

• Standards based

• Natively built into our core technologies

• Benefits
  – Integrated & understood across all components / tiers
  – Reduce # of points of failure, modules with potential security holes
  – Simplify administration experience & reduce cost
  – Improved developer experience & productivity
  – Enforce security regardless of entry point
  – Allow customers and auditors to setup, and review policies centrally
  – Single integration point to Oracle & 3rd party solutions
Fusion Applications
Security Architecture

Access Manager
- Single Sign-On

Authz Policy Manager
- Authz policy & App Role Mgmt

Identity Manager
- Identity & Enterprise Role Mgmt

Authentication

Authorization

OES Policy Store

OID ID Store

User & Role Profile

Data security, Apps transaction data

Oracle RDBMS

Fusion Applications
- ADF, SOA, BI, WebCenter
- OWSM
- SPML
- OPSS

Copyright © 2010, Oracle. All rights reserved
Authorization Policy Manager

Overview

- UI console for administration of OPSS based authorization policies
  - Rich desktop like UI with drag ‘n drop capabilities
  - Delegated Administration
  - Extensible

- Standards based
  - JAAS Permissions & Enterprise RBAC
  - Identity Store access through IGF / ArisID

- For customers relying on
  - Oracle ADF security for in house built ADF applications
  - Oracle’s next generation Fusion Applications
OPSS/APM

Benefits

Better Business Agility

- An adaptable security service infrastructure that more closely models your business
- Respond faster to changing corporate, regulatory, market requirements
- Reduce time-to-market

Enhanced Security and Compliance

- Manage security from a single place
- Provides finer control over the protection of all resources
- Separates security decisions from application logic
- Offers robust auditing of events

Increased IT Efficiency

- Centralizes security policy management
- Enables reuse and sharing of security services
- Frees developers up to focus on value-added business logic
- Integrates easily with identity and access management
Summary

- Externalize security to get business agility, cost saving & compliance
- Oracle’s vision for Service-Oriented Security will enable the creation of an Identity Infrastructure that manages identity across both on-premise and cloud environments
- OPSS is the next generation security framework providing development teams with a standards-based, portable, integrated, enterprise-grade security framework for Java EE and Java SE applications
- APM is the Authorization policy management GUI for OPSS based applications
Resources

• **OPSS @ OTN** for
  • OPSS Whitepaper
  • OPSS FAQ
  • APM Datasheet
  • Help Forum
  • Documentation on OPSS & APM
  • Sample App
  • Blog
For More Information

search.oracle.com

Oracle Platform Security