Oracle Platform Security Services (OPSS) in Ihrem Environment

Andreas Chatziantoniou
Foxglove-IT
Utrecht - Niederlande

Schlüsselworte

OPSS, Security

Einleitung

Security ist seit jeher ein wichtige Bestandteil von Oracle Systemen. Oft werden Ideen der Systemsicherheit nur teilweise umgesetzt. Oracle Platform Security Services (OPSS) sorgen für eine konsistente Umsetzung der Sicherheitsmechanismen in Anwendungen und Infrastrukturkomponenten.

Dieses Dokument und die dazugehörende Präsentation gehen auf den Aufbau und die Benutzung von OPSS ein und zeigen wie OPSS in Ihrem Environment eingesetzt werden kann.

OPSS - Einführung

Was ist OPSS? OPSS bietet eine Standard API die Sicherheitsthemen als extra Abstraktionslage zugänglicher macht. Hierdurch soll gleichzeitig der Entwickler von den technischen Details von Systemkomponenten (Identity Management, Single Sign On, Auditing, etc.) abgeschirmt werden und gleichzeitig Möglichkeiten im Source Code einbauen, die einem Systemadministrator erlauben um spezifische Einstellungen zu konfigurieren und zu überwachen.

Hierdurch können Entwickler sich auf die Funktionalen Anforderungen konzentrieren während die Produkte in mit denselben Sicherheitsmerkmalen in der IT Infrastruktur eingebettet werden können.

OPSS Themen der Präsentation

In der Präsentation werden die folgenden Themen behandelt:

- Isolation von Security Lösungen im herkömmlichen Oracle Technology Stack
- JAZN/JPS/OPSS - eine Übersicht
- OPSS und Authentifizierung im WLS
- OPSS und Single Sign On
- OPSS und Autorisierung
- OPSS und Auditing
- Konfiguration von Security (OPSS) im Enterprise Manager

Weiterhin wird auf die Rolle von OPSS bei ADF Projekten eingegangen. Zum Schluss wird eine Roadmap definiert wie OPSS in Organisationen eingeführt werden kann.

Eine besondere Rolle werden die verschiedenen Oracle Fusion Middleware (FMW) Produkte und deren Beziehung zum OPSS spielen. Per Hauptkomponente der FMW wird gezeigt wie und wo die verschiedenen OPSS Aspekte zum Tragen kommen.

Isolation von Security Lösungen im herkömmlichen Oracle Technology Stack

Bisher waren die verschiedenen Oracle Technologiekomponenten so ausgelegt, dass sie Themen wie Security selber implementiert hatten.
So gab es in jedem Produkt die Möglichkeit der Definition von Benutzern, spezielle Rechte und Rollenkonzepte und produktspezifische Managementtools bzw. -möglichkeiten um diese zu konfigurieren und zu überwachen. Oft wurde hierfür die Oracle Datenbank als "Repository" eingesetzt, selten waren diese Bemühungen jedoch soweit integriert, dass es eine eindeutige Vorgehensweise gab die über die Produktgrenzen hinaus sichtbar war.

Dies ist nachvollziehbar, denn einerseits kamen diese Produkte aus verschiedenen Bereichen (teilweise sogar von aufgekauften Firmen), andererseits war es lange die Absicht um diese Produkte unabhängig voneinander zu implementieren. Hierdurch kam es in großen Projekten immer wieder zu der Situation, dass ein Teil der Implementierungsaktivitäten zur Konsolidierung von Security Themen benutzt wurden.

Die Architektur der Fusion Apps setzt jedoch eine vollständige Implementierung der FMW voraus. Dies erklärt (wenigstens teilweise) die Wahl eines eindeutigen und umfassenden Security Konzeptes wie OPSS es bietet. Die oben benannten Vorteile der Integration des Security Managements mit den System Management Komponenten des Oracle Enterprise Manager machen auch deutlich, dass die bisherige zersplitterte Vorgehensweise nicht länger als akzeptabel eingeschätzt wird.

Besonders deutlich wurde dies bei den Produkten der Oracle Application Server. Obwohl Entwicklungen von Oracle Portal (der L/SQL Version) schon das Konzept von Partner und External Applications kannten, war es schwierig um die Security eindeutig zu benutzen.

JAZN/JPS/OPSS

Besonders deutlich wurden die Probleme bei der Benutzung von JAZN. Obwohl JAZN ein Schritt in die richtige Richtung war, viel schnell auf, dass das Management von großen Benutzergruppen und komplexen Gruppenstrukturen beinahe unmöglich war. Eine Integration mit einem LDAP Server war zwar möglich, machte aber das deutlich, dass es sich hierbei meistens nur um eine Form der Authentifizierung handelte. Kunden sahen jedoch den Mehrwert von Single Sign On Systemen nicht sofort, da die wichtige Frage der Autorisierung meistens nicht beantwortet wurde.

In dieser Hinsicht ist der Oracle Entitlement Server das Produkt mit der richtigen Positionierung. Die einfache Kopplung mit anderen IDM Produkten (OAM, OIM) und der Lösung der Autorisierung innerhalb von Anwendungen spricht Kunden an.
OES kann dann auch als fertige Lösung eines OPSS Vorgehens gesehen werden, bietet aber nicht die Flexibilität und Funktionalität die OPSS liefert. OPSS kann in existierende und neue Anwendungen aufgenommen werden und lässt sich weiterhin mit dem OES integrieren.

Authentifizierung im WLS

Die Präsentation zeigt wie der WLS bei der Authentifizierung OPSS nutzen kann. Anhand von Beispielen werden Themen wie Authentifizierung, LDAP Einbindung, SSO, Credential Storage Framework und andere behandelt. Dies soll deutlich machen, dass OPSS nicht nur eine Lage ist, die Basisfunktionen wie Authentifizierung unterstützt, sondern wie hiermit Enterprise-Ready Systeme

gebaut werden können. Dabei werden auch die parallelen mit einer Container Based Authentication aufgezeigt.

OPSS und SSO

OPSS und SSO treffen besonders dann aufeinander, wenn Anwendungen (z.B. ADF Anwendungen) im WLS deployed werden. Hier spielt die Konfiguration der jps-config.xml eine große Rolle. In der Präsentation wird dann auch der Unterschied der Domain-weiten JPS und der Anwendungs-JPS gezeigt.

OPSS und Autorisierung

Um OPSS für die Autorisierung einzusetzen ist es notwendig um das Konzept der Authentication Providers im WLS zu verstehen. Hier spielt nicht nur die Einbindung eines LDAP eine Rolle, sondern auch die Benutzung eben dieses LDAP's für den Policy Store um die Anwendungs Policies zu speichern. Ein Konfigurationsbeispiel wird dies aufzeigen.

OPSS und Auditing

Auditing von Datenbanken ist ein bekanntes Thema (wenn auch regelmäßig vernachlässigt). Das Auditing von Anwendungen ist dagegen oft noch ein wenig beachteter Punkt in der Entwicklung. Das FMW Common Audit Framework ist ein Service der verschiedene Audit Funktionalitäten anbietet. Hier ist die Integration mit dem OPSS besonders wichtig, da ein Teil der OPSS Konfiguration die Basis des CAF formt.

Enterprise Manager

Die Komplexität vieler verteilter Systeme ist inzwischen so groß, dass eine besondere Beachtung des Themas Betrieb und System Management notwendig ist. OPSS ist in der Lage um innerhalb des Enterprise Managers betrieben zu werden. Hierzu gehört neben der Konfiguration auch die Unterstützung des Betriebs, besonders bei Fragen die ein End-to-end Tracing benötigen. Bei jedem Schritt einer Anwendung ist potentiell ein OPSS relevantes Thema zu entdecken.

ADF und OPSS

Anhand einzelner Beispiele soll auf die Kombination von ADF Security und OPSS hingewiesen werden. Dies soll auch zeigen, dass die Entwicklung für Plattformen wie Webcenter und Fusion Apps auch Berührungspunkte mit OPSS hat.

Roadmap Einführung OPSS

OPSS kann innerhalb eines Projektes gut eingeführt werden, das die verschiedenen Projektphasen unterschiedliche Anforderungen an Security haben. Die Bedeutung dieser Phasen und wie OPSS schrittweise zu mit den verschiedenen Securityinstrumenten einer Organisation verknüpft werden kann, soll es Ihnen erleichtern um OPSS zu einem integralen Bestandteil der Oracle Technologie in ihren Unternehmen zu machen.

Kontaktadresse:
Andreas Chatziantoniou
Foxflove-IT
Texel 18
3524 AP Utrecht
Niederlande

Telefon: +31623259167
E-Mail: andreas@foxglove-it.nl
Internet: www.foxglove-it.nl