Oracle Platform Security Service in Ihrer Umgebung

DOAG 2012

Andreas Chatziantoniou

Foxglove-IT

BIO

- Andreas Chatziantoniou
- Freelance Oracle Fusion Middleware Consultant
- 14 Jahre Oracle Erfahrung/24 Jahre IT (Unix/C)
- 50% Deutscher/50% Grieche/50% Holländer
  - Arbeitet sehr viel, zahlt keine Steuern und hat ein Auto mit Anhängerkupplung aber keinen Wohnwagen ;-)
- Oracle ACE
- andreas@foxglove-it.nl

Agenda

- **OPSS Grundlagen**
- Security im Oracle Technology Stack
- JAZN/JPS/OPSS - eine Übersicht
- OPSS und Authentifizierung im WLS
- OPSS und Single Sign On
- OPSS und Autorisierung
- OPSS und Auditing
- Rolle von OPSS bei ADF Projekten
- Roadmap zur Einführung von OPSS in Organisationen

OPSS Grundlagen

- Oracle Platform Security Services ist ein Framework um Enterprise Anwendungen sicher zu entwickeln und zu Betreiben
  - Standardbasiert:
    - J2EE, JAAS (JAZN), RBAC

OPSS Grundlagen

- OPSS bietet Security-relevante Dienste für J2EE (SE und EE)
  - Authentifikation
  - Authorisation
  - Application Policy Management
  - Auditing
  - Security Administration
  - etc

OPSS Grundlagen

- Architektur von OPSS
  - OPSS lebt zwischen den Fusion Middleware Komponenten und den Security Providern

OPSS Grundlagen

"Selbstbau" Anwendungen

Fusion Apps

Nicht-Oracle Anwendungen

SOA | WebCenter | IDM | BI | RDBMS

OPSS

Authori-sation | Authentifi-kation | Auditing | Credential Mgmt. | Kryptografie SSL, etc.

Security Service Providers

OAM | OAAM | OID, OVD | OIM | OWSM | OES

Identity Store | Credential Store | Policy Store

Nutzen von OPSS

- OPSS extrahiert Security Policies aus der Anwendung
  - Entwickler müssen sich nicht mehr um Die Absicherung des Systems kümmern
  - Security wird den Experten überlassen (Security Architekt, Betrieb)
- Änderungen der Securityregeln erfordern keine Anpassung der Software

Nutzen von OPSS

- OPSS sorgt für eine einheitliche Implementierung von Security über die Produktgrenzen hinweg
  - Hierdurch wird der Betrieb verschiedener Anwendungen einfacher
- WebLogic Server und ADF bauen auf OPSS auf
- Integration mit verschiedenen Security Providern erleichtert die Einbettung in existierenden Enterprise Umgebungen

Agenda

- OPSS Grundlagen
- **Security im Oracle Technology Stack**
- JAZN/JPS/OPSS - eine Übersicht
- OPSS und Authentifizierung im WLS
- OPSS und Single Sign On
- OPSS und Autorisierung
- OPSS und Auditing
- Rolle von OPSS bei ADF Projekten
- Roadmap zur Einführung von OPSS in Organisationen

Security im Oracle Technology Stack (früher)

- Obwohl Security immer schon wichtig war gab es immer Probleme wenn mehrere (Oracle) Produkte miteinander integriert werden mussten
  - DB Security != Enterprise Security
  - Unterschiedliche Lösungen per Produkt, Fokus auf unabhängigen Einsatz der Einzelprodukte

Security im Oracle Technology Stack (Application Server)

- Diese Probleme wurden mit dem Einsatz des Oracle Application Server deutlich und die ersten Ansätze einer konsolidierten und integralen Lösung wurden sichtbar
  - Weg vom Client/Server, hin zu Enterprise IDM
  - Einsatz des OID für IDM
  - Portal Partner Applications
  - Single Sign On
- Integration war nicht trivial
  - Kaum Unterstützung durch Tools

Security im Oracle Technology Stack (OPSS)

- Die treibende Kraft hinter OPSS ist wohl Oracle Fusion Apps
  - Der gesamte Fusion Middleware Stack muss installiert werden
  - Hiervon ist ca. 60% IDM
  - (die meisten) Produkte unterstützen OPSS
- Enterprise Manager (GC/CC) unterstützen Management der FMW Produkte
  - Eindeutige Behandlung über die Breite der FMW Produkte

Agenda

- OPSS Grundlagen
- Security im Oracle Technology Stack
- **JAZN/JPS/OPSS - eine Übersicht**
- OPSS und Authentifizierung im WLS
- OPSS und Single Sign On
- OPSS und Autorisierung
- OPSS und Auditing
- Rolle von OPSS bei ADF Projekten
- Roadmap zur Einführung von OPSS in Organisationen

JAZN Konzept

- JAZN ist die Oracle Implementierung von Java Authentication and Authorization Service
- Zwei Files:
  - jazn.xml
    - Beschreibt den JAAS Provider (LDAP/OID oder XML)
  - jazn-data.xml
    - XML JAAS Provider
    - Speichert Benutzer, Rollen und Policies

OPSS Konzept

- OPSS basiert auf den folgenden Konzepten:
- User (Benutzer)
  - Person die eine Anwendung benutzen will
- Group (Gruppe)
  - User mit gemeinsamen Merkmalen, Hierarchie, Organisation
- Application Role (Anwendungsrolle)
  - Beschreibung eines Users in einer Anwendung, bestimmt die Zugriffsrechte

OPSS Konzept

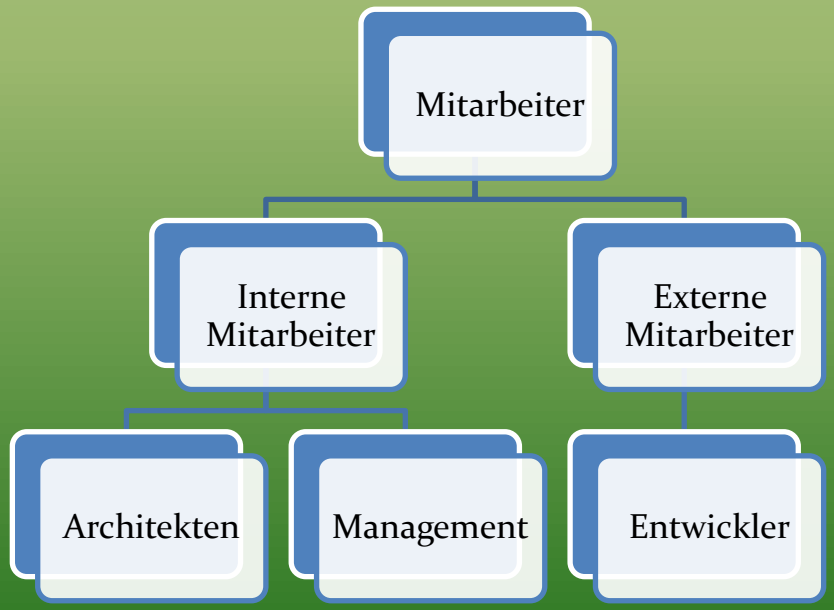
- Identity Store (Identitätsspeicher)
  - Enthält Benutzer und Gruppen
  - Benutzer authentifizieren sich hier
  - LDAP
- Credential Store („Password-Speicher“)
  - Speichert Passwords und andere Zugangsdaten (z.B. Zertifikate)

OPSS Konzept

- Policy Store („Zugangsberechtigungen“)
  - Enthält System- und Anwendungszugangsberechtigungen
- Application Roles werden im Policy Store abgelegt
- Policies funktionieren mit Benutzern, Gruppen oder Rollen

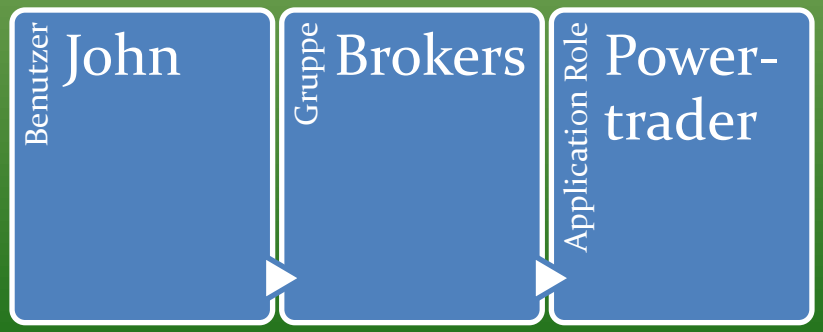
OPSS Konzept

- Benutzer und Gruppen sind im allgemeinen in einer Hierarchie aufgenommen
  - Vererbung von Rechten von oben nach unten



OPSS Konzept

- Application Roles
  - Application Roles sind statisch definiert und orientieren sich an Benutzern oder Gruppen
- Benutzer oder Gruppen werden Application Roles zugeordnet
- Application Roles sind keine J2EE oder WLS Rollen



OPSS Konzept

- Application Roles kommen aus den Anwendungen
- Application Roles werden im OPSS Policy Store abgelegt
- Anwendungen können J2EE Deployment Descriptors benutzen (z.B. web.xml) und diese auf Benutzer und Gruppen im Identity Store abbilden
- Application Roles benutzen dann diese Abbildungen

OPSS Konzept

- Application Roles sind nicht mit Gruppen gleichzusetzen
  - Konzepte sind ähnlich, aber der Moment der Auswertung ist unterschiedlich

JPS Konzept

- Das File jps-config.xml ist die Referenz für OPSS Services:
  - Login Module
  - Authentication provider
  - Authorization Policy provider
  - Credential stores
  - Auditing services
- Wenn eine OPSS Anwendung einen Security Service benötigt wird ein JPSContext Objekt eingesetzt, dass die Konfiguration für alle notwendigen Services enthält

JPS Konzept

- In ADF Anwendungen wird jps-config.xml erzeugt wenn die ADF Security eingesetzt wird
  - Hiermit kann im Jdeveloper getestet werden (unit tests)
- Das jps-config.xml wird in ADF Anwendungen NICHT mehr benutzt (selbst wenn es im Deployment mitgeliefert wird) sobald es im WLS aktiv ist
  - Hier gibt es ein jps-config.xml in <domain-home>/config/fmwconfig für die WLS Domain
  - Es existiert kein JPS Konzept auf dem Anwendungsniveau (server level)

Agenda

- OPSS Grundlagen
- Security im Oracle Technology Stack
- JAZN/JPS/OPSS - eine Übersicht
- **OPSS und Authentifizierung im WLS**
- OPSS und Single Sign On
- OPSS und Autorisierung
- OPSS und Auditing
- Rolle von OPSS bei ADF Projekten
- Roadmap zur Einführung von OPSS in Organisationen

OPSS und Authentifizierung

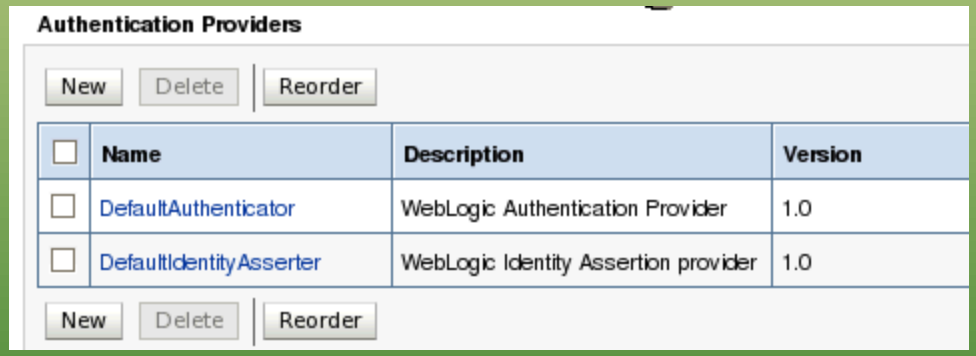
- Die Authentifizierung ist im Allgemeinen zum WLS und den konfigurierten Authentication Provideren delegiert
- Für J2SE Anwendungen ist die Entwicklung von Authentifizierung notwendig

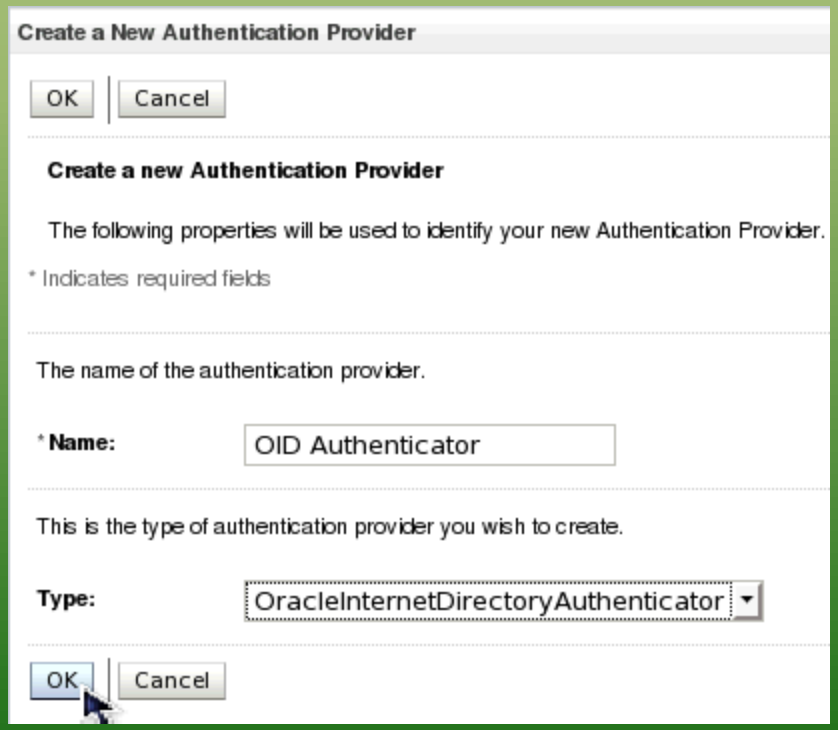
OPSS und Authentifizierung

- J2SE Anwendungen benutzen vorher definierte Login Module
  - Diese werden in jps-config-jse.xml konfiguriert
- OPSS APIs verfügt über den oracle.security.jps.service.login.LoginService um ein Login Module einzusetzen
- OPSS unterstützt den Identity Store von JavaSE Anwendungen

OPSS und Authentifizierung

- Im FMW Control kann ein Authentication Provider konfiguriert oder hinzugefügt werden





Agenda

- OPSS Grundlagen
- Security im Oracle Technology Stack
- JAZN/JPS/OPSS - eine Übersicht
- OPSS und Authentifizierung im WLS
- **OPSS und Single Sign On**
- OPSS und Autorisierung
- OPSS und Auditing
- Rolle von OPSS bei ADF Projekten
- Roadmap zur Einführung von OPSS in Organisationen

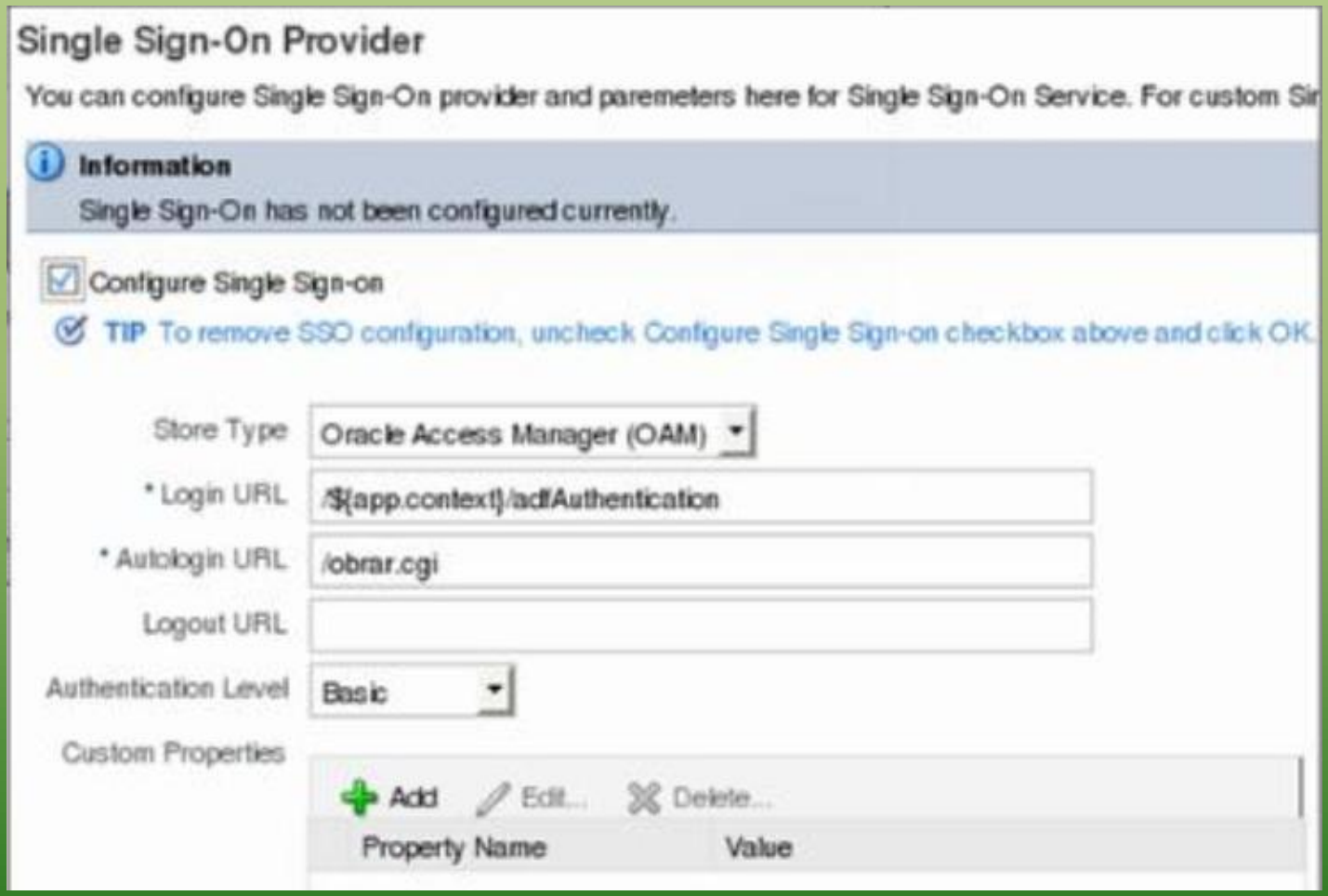
OPSS und Single Sign On

- OPSS hat Möglichkeiten um Anwendungen einer Domain mit SSO zu verbinden
  - API's für login, logout und auto login
- Nach der erfolgreichen Anmeldung leitet der SSO Service den Benutzer zum angefragten URL weiter
- Ein SSO Provider muss einen Credential Mapping Service haben

OPSS und Single Sign On

- Die Konfiguration von Single Sign On mit OPSS wird wie folgt eingestellt:
  - Im FMW Control wird der Security Provider geöffnet
    - Domain → Security →Security Provider Configuration
  - Hier ist der Single-Sign-On Provider aufgeführt
    - Oracle Access Manager (OAM)
    - Oracle Single Sign On (OSSO)
    - Custom SSO

OPSS und Single Sign On



Agenda

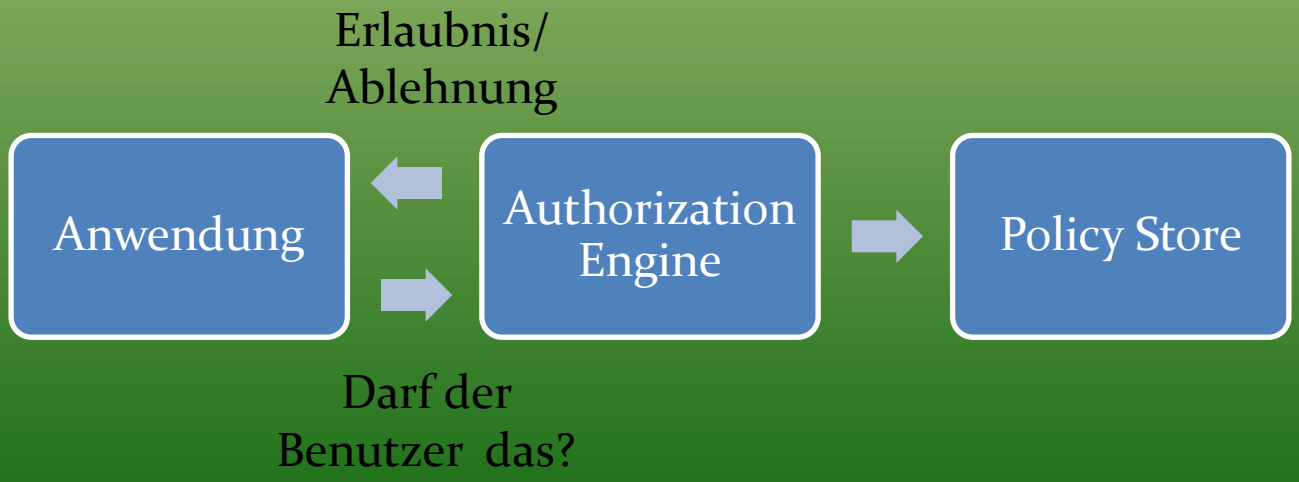
- OPSS Grundlagen
- Security im Oracle Technology Stack
- JAZN/JPS/OPSS - eine Übersicht
- OPSS und Authentifizierung im WLS
- OPSS und Single Sign On
- **OPSS und Autorisierung**
- OPSS und Auditing
- Rolle von OPSS bei ADF Projekten
- Roadmap zur Einführung von OPSS in Organisationen

OPSS und Autorisierung

- Autorisierung beschreibt was ein Benutzer in einer Anwendung darf
  - Ausführen von Aktivitäten
  - Zugang zu Daten
- OPSS beschreibt in Application Policies die Autorisierung der Anwender (Benutzer, gruppen)

OPSS und Autorisierung

- Die Entscheidung um den Zugang zu erlauben wird durch die Authorization Engine getroffen
  - Vergleich Rechte des Users mit den Authorization Policies im Policy Store

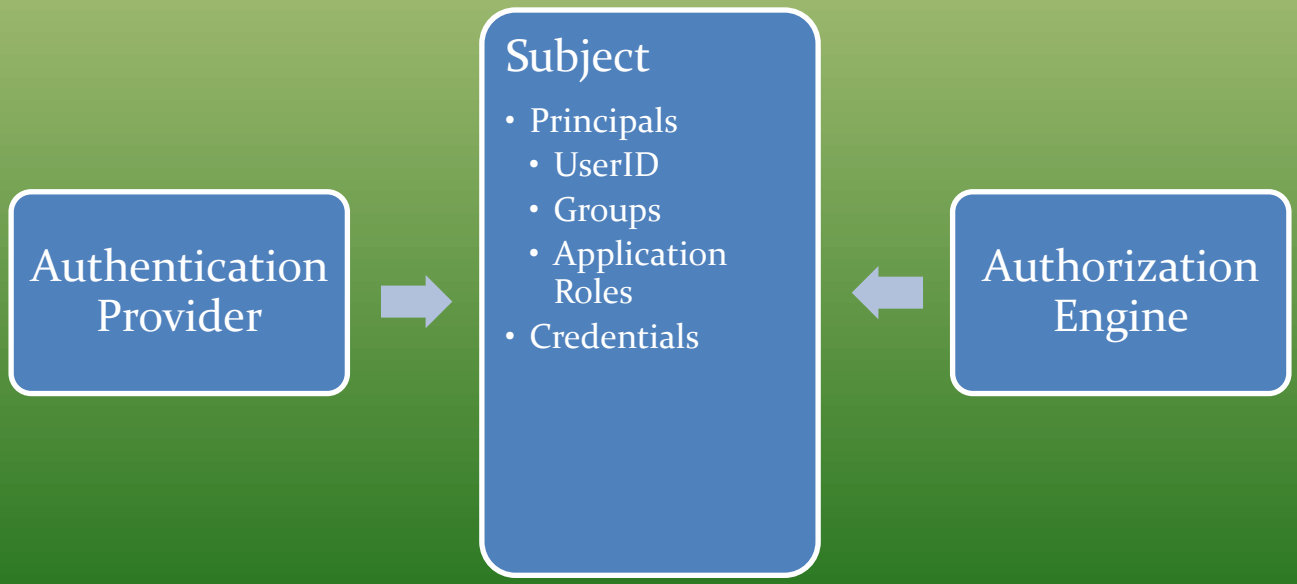


OPSS und Autorisierung

- OPSS kennt den Begriff der ANONYMOUS-ROLE
  - Benutzer ist noch nicht eingeloggt, aber die Authorization Engine stellt fest was der Benutzer darf
  - Nach dem einloggen wird die AUTHENTICATED-ROLE hinzugefügt

OPSS und Autorisierung

- Die Authorization Engine benutzt die Application Roles des PRINCIPAL der wiederum ein Teil des SUBJECT ist

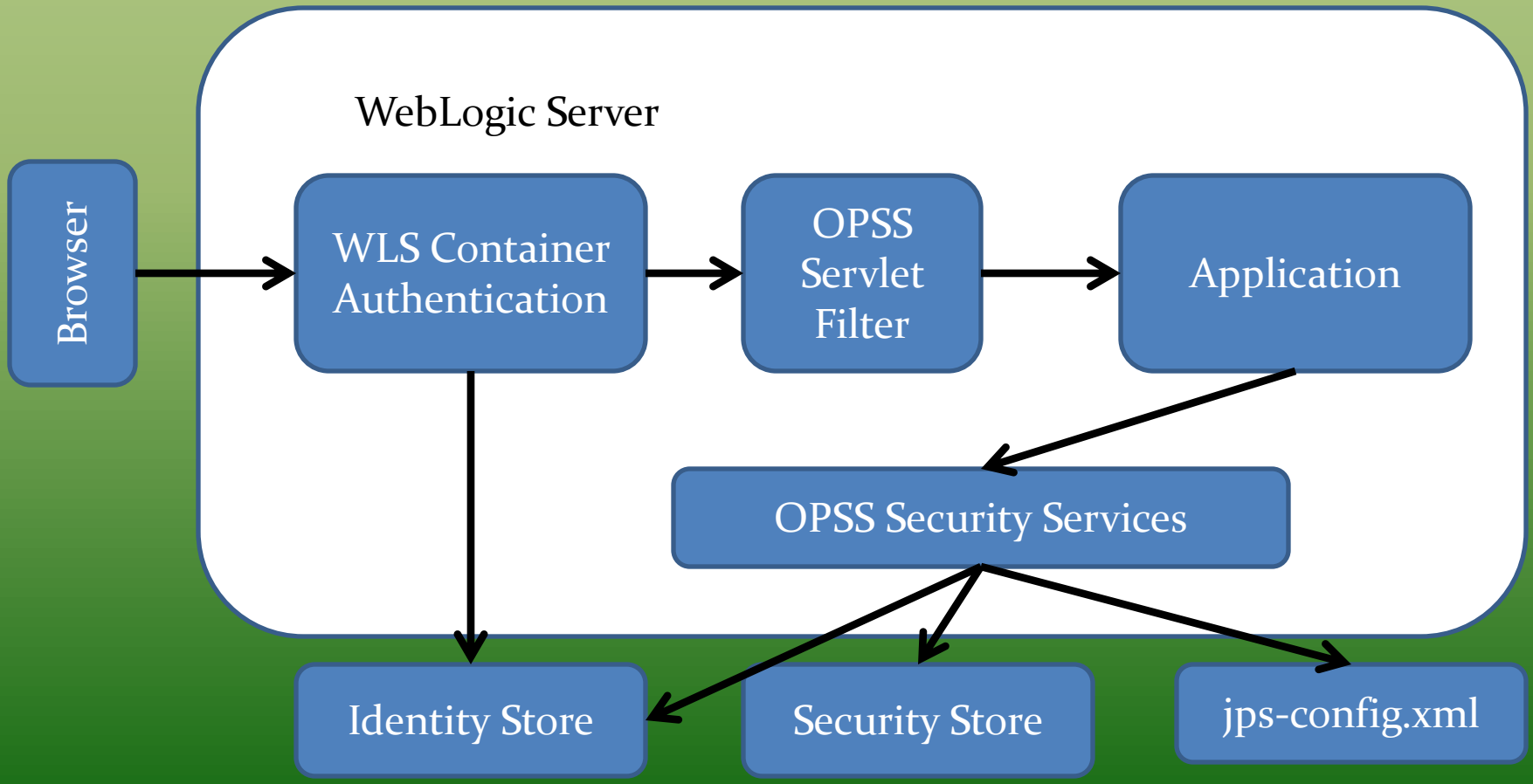


OPSS und Autorisierung

- Festlegen der Autorisierung (Application Roles) ist erst der Anfang
- (OPSS) Administrator legt PERMISSIONS fest und weist diese (GRANT) an die Application Role
  - Beispiel: GET für einen bestimmten URL

OPSS und Autorisierung

- Verarbeitung im WLS



Agenda

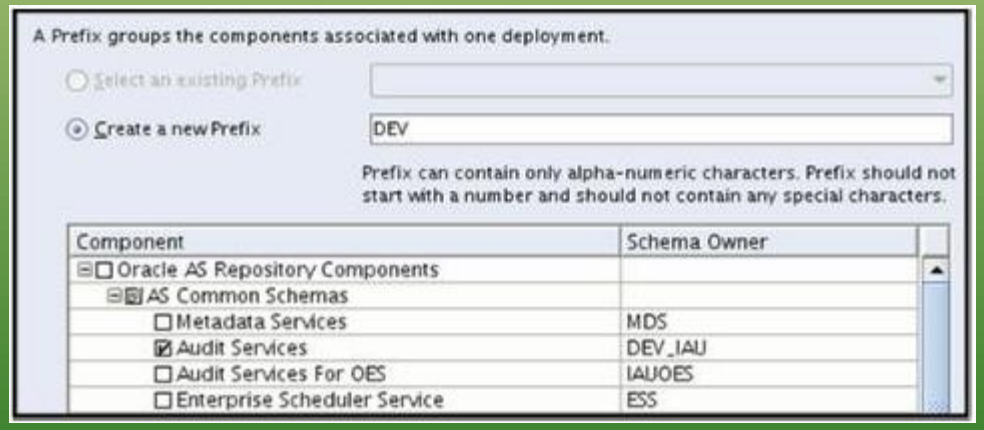
- OPSS Grundlagen
- Security im Oracle Technology Stack
- JAZN/JPS/OPSS - eine Übersicht
- OPSS und Authentifizierung im WLS
- OPSS und Single Sign On
- OPSS und Autorisierung
- **OPSS und Auditing**
- Rolle von OPSS bei ADF Projekten
- Roadmap zur Einführung von OPSS in Organisationen

OPSS und Auditing

- Aufgaben des Auditing
  - Wo werden Audit Daten gespeichert?
  - Auditing Policies erstellen
  - Analyse

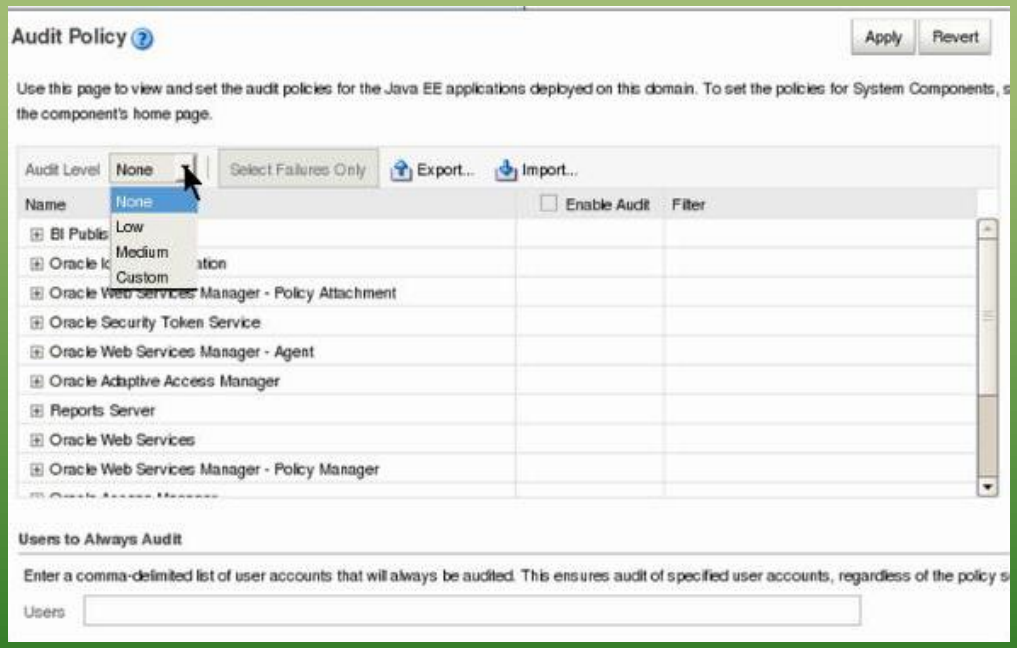
OPSS und Auditing

- Audit Daten können im Filesystem oder in einer Datenbank gespeichert werden
  - Für die Datenbank muss mit dem RCU das Schema angelegt werden



OPSS und Auditing

- Per Komponente der FMW kann eine Audit Policy im FMW Control festgelegt werden
  - Audit Level
  - Anwendung
  - Benutzer



OPSS und Auditing

- Audit is nur dann sinnvoll wenn die daten ausgewertet werden
  - Beste Option ist der Einsatz vom BI Publisher
  - Audit Daten werden in eine Datenbank geladen und von dort durch den BIP ausgelesen

Agenda

- OPSS Grundlagen
- Security im Oracle Technology Stack
- JAZN/JPS/OPSS - eine Übersicht
- OPSS und Authentifizierung im WLS
- OPSS und Single Sign On
- OPSS und Autorisierung
- OPSS und Auditing
- **Rolle von OPSS bei ADF Projekten**
- Roadmap zur Einführung von OPSS in Organisationen

OPSS und ADF

- Oracle ADF Security bietet:
  - Beschreibende Sicherheit (low level)
  - Erstellung von Security Artefacts
  - Hierarchie von Rollen (Zuweisen)
- Integration mit JDeveloper
  - Inkl. Unit Tests

OPSS und ADF

- ADF benutzt implizit OPSS
  - Entwickler braucht keine Security Erfahrung
    - OPSS API kann extra benutzt werden
  - Sicherung der Container Authentication im WLS
- Einbinden von Security Store und Policy Store
  - Benutzen der Application Roles

OPSS und ADF

- Task Flow Security
  - ADF beschützt Task Flows auf der Basis von JAZN/JAAS unabhängig von ADF Bindings
  - Bounded Task Flows werden immer gesichert
- ADF Page Security
  - Page Definitions werden immer gesichert
  - Page-level Security wird innerhalb eines Bounded Task Flows nicht überprüft

Agenda

- OPSS Grundlagen
- Security im Oracle Technology Stack
- JAZN/JPS/OPSS - eine Übersicht
- OPSS und Authentifizierung im WLS
- OPSS und Single Sign On
- OPSS und Autorisierung
- OPSS und Auditing
- Rolle von OPSS bei ADF Projekten
- **Roadmap zur Einführung von OPSS in Organisationen**

Roadmap für OPSS

- Think first!
- Identity Store/Security Store/Policy Store
- Integration Anwendungen
  - Neuentwicklung
  - Existierende Anwendungen

Roadmap für OPSS

- Think first!
  - Was will ich erreichen?
    - Governance
    - Audit
    - andere Form von credentials
    - Etc.
  - Jedes Ziel erfordert eine eigene Planung

Roadmap für OPSS

- Identity Store/Security Store/Policy Store
  - Existierende IDM Infrastruktur so weit wie möglich wieder verwerten
  - Extra Infrastruktur nicht vernachlässigen
  - High Availability?

Roadmap für OPSS

- Integration Anwendungen
  - Neuentwicklung
    - OPSS Lernkurve beachten
    - Proof-of-concept aufbauen
    - Integration mit FMW Control
    - Pentest
  - Existierende Anwendungen
    - Schrittweise extrahieren von Security ist mühsam
    - Integration mit OPSS Application Policies
    - ADF/WLS ready?

Q?

A!