OPITZ CONSULTING

Menschen. Innovationen. Lösungen.

Orchestrierung der IT-Sicherheit

Wie sieht es mit der Oracle Fusion Middleware aus?

DOAG

Mohammad Esad-Djou, Solution Architect
OPITZ CONSULTING Deutschland GmbH

München, 06. März 2014, Regionaltreffen München/Südbayern

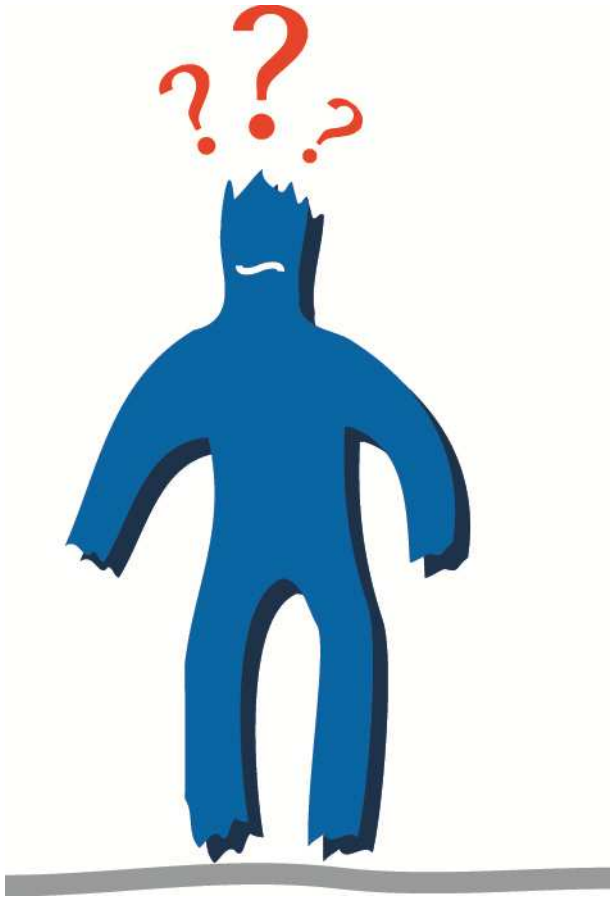
Agenda

1. **Orchestrierung**
   - Rahmenarchitektur für eine Lösung: Orchestrierung
   - Problemstellung: Horizontale-, Vertikale-Komplexität, IT-Strategie, plattformübergreifende Probleme
2. **WebLogic Server und Oracle Platform Security Services (OPSS)**
   - Überblick, Architektur, Funktionalität
3. **Oracle WebLogic Server 11g/12C: Sicherheit**
   - Konzept, Grundlage, Demo via Administration Console

Orchestrierung

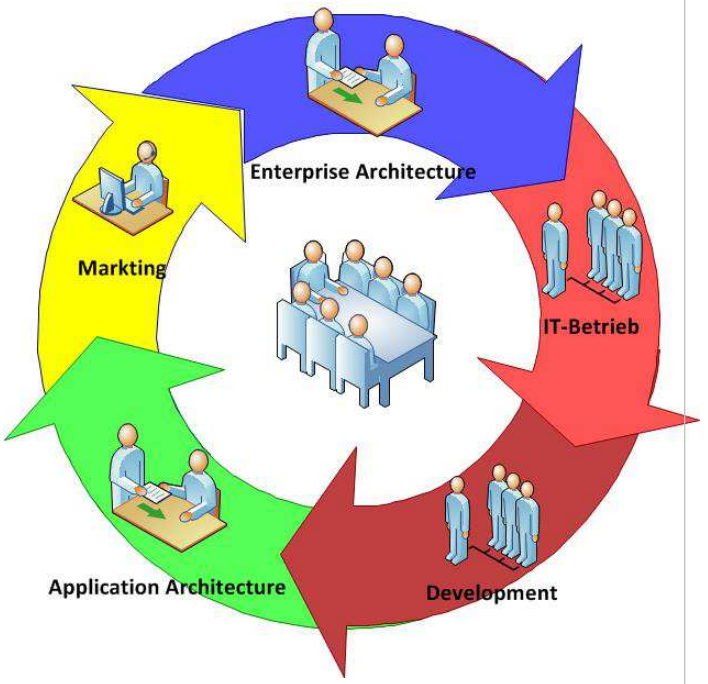
IT-Landschaft wird noch komplexer!

- die klassische Kluft zwischen den Abteilungen
- versteckte Komplexität von Hardware- und Software-Welt
- Neue IT-Strategien und Entwicklungen
- Cloud Computing als verteiltes Echtzeit-System

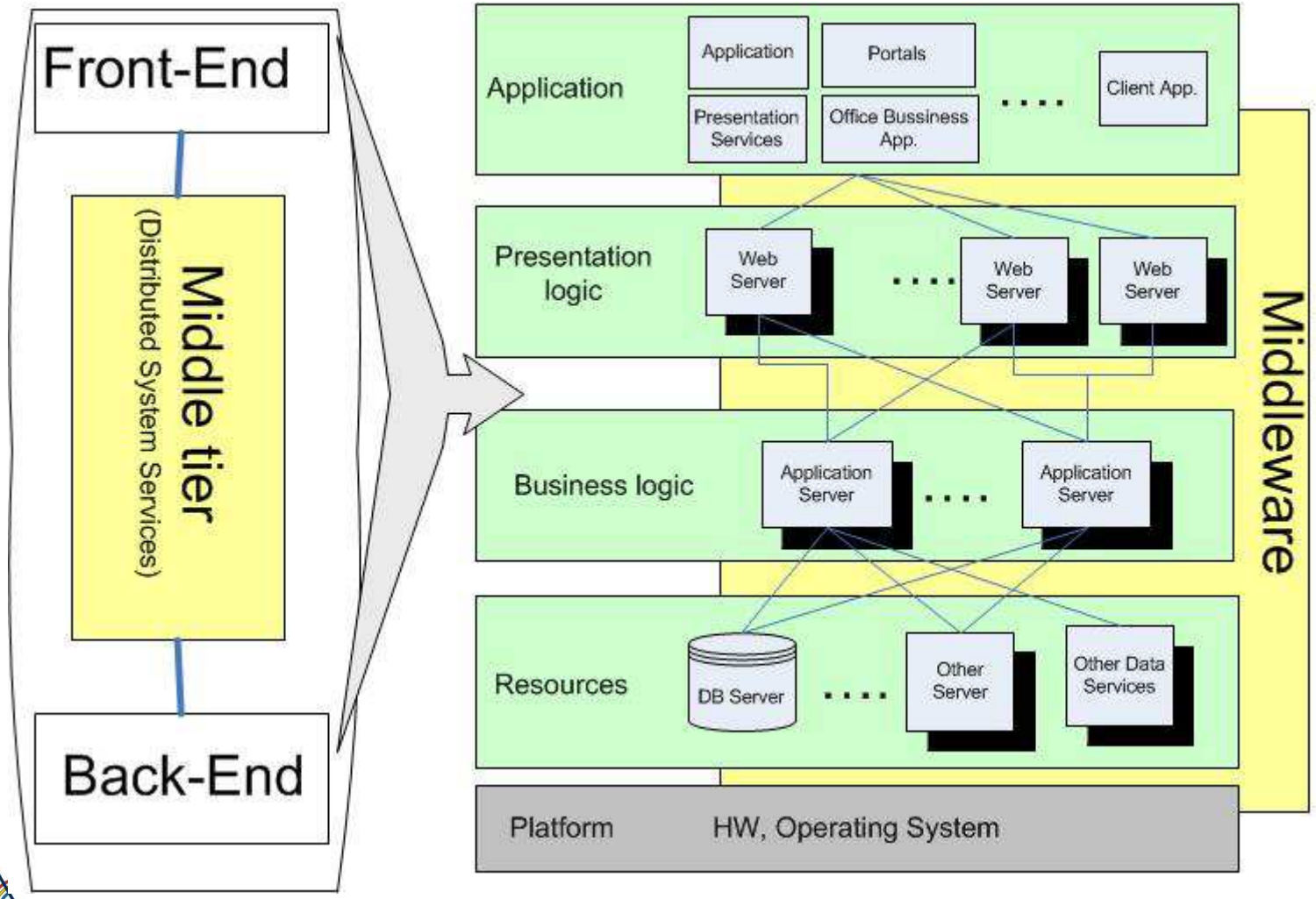


Erste Dimension: Horizontale Komplexität

- **Wie funktionieren die Beziehungen zwischen den Abteilungen in Großunternehmen?**
  - **EA- und App.-Architektur-Abteilungen**
  - **Development**
  - **IT-Betrieb**
  - **Marketing**
- **(+) Entdeckung einer Lücke: interdisziplinäre IT-Experten**
- **(-) Es liegt kein klares Gesamtkonzept vor**

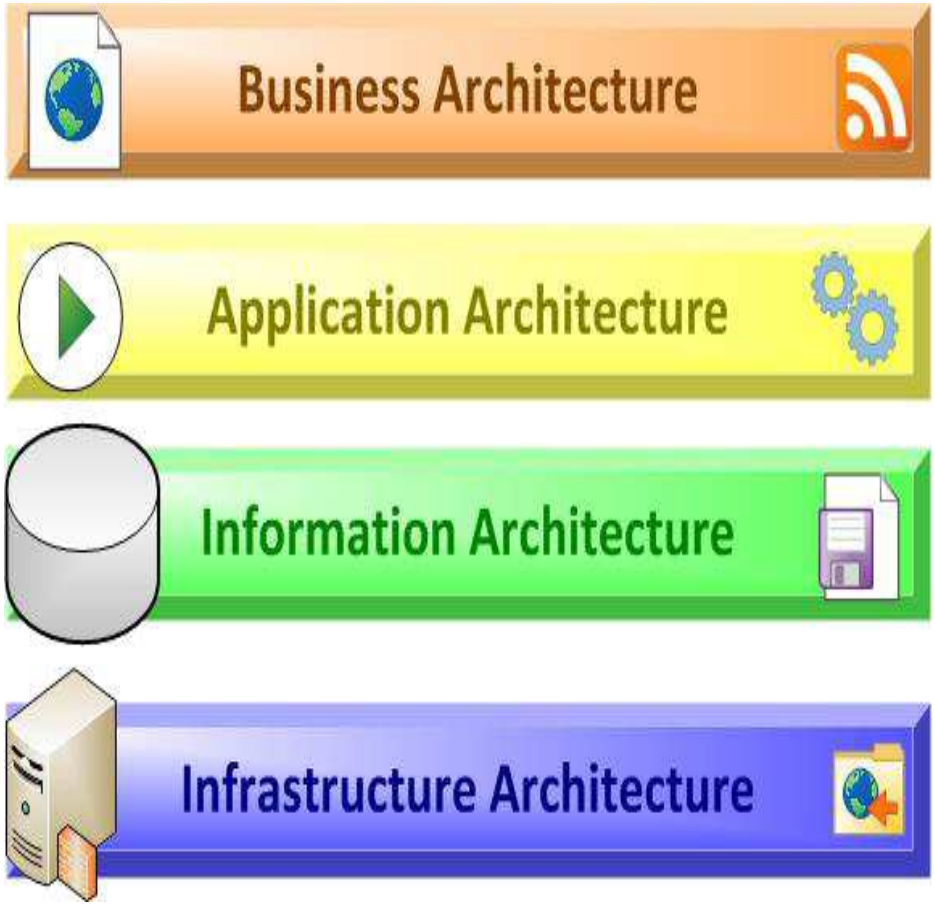


Vertikale Komplexität: Schichtenarchitektur



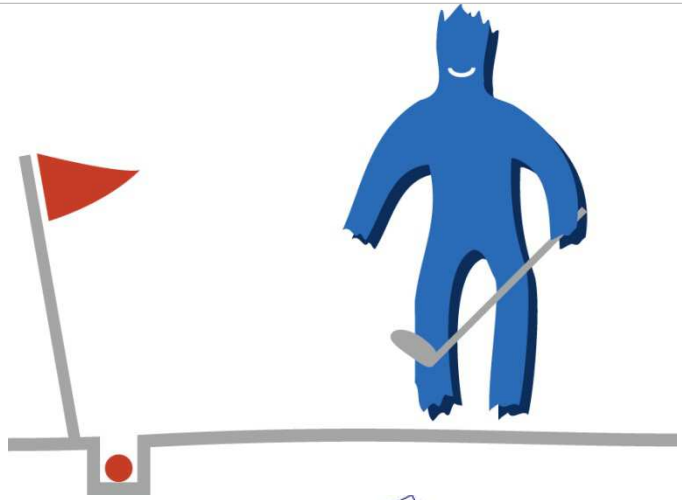
Vertikale Komplexität: Schichtenarchitektur

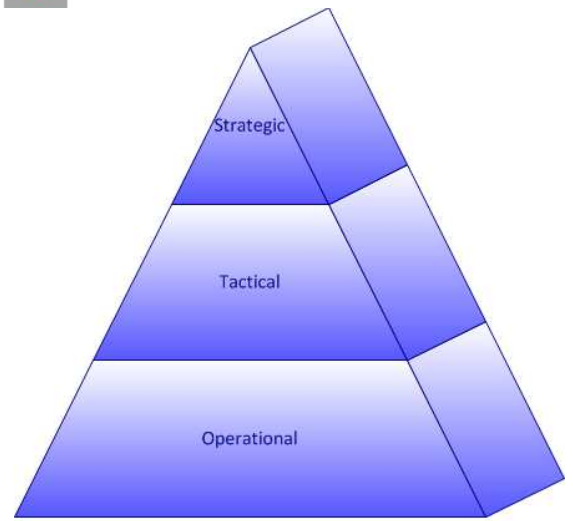
- Wartbarkeit
- Sicherheit
- Schwachstellen
- Automatisierte bzw. semi-automatisierte Upgrades, Deployment
- Schichtenübergreifende Probleme



Dritte Dimension: IT-Strategie

- **Diskrepanz zwischen strategischer-, taktischer- und operativer Sicht**
- **Enterprise Architecture (EA)**
- **IT-Architektur**
- **IT-Projekte**
- **IT-Governance**
- **IT-Prozesse und Personal**





Vierte Dimension: Plattformübergreifende Probleme

- **Heterogene Umgebungen: IBM, Oracle, Microsoft, SAP…**

Was nun?
Rahmenarchitektur für eine Lösung (1)

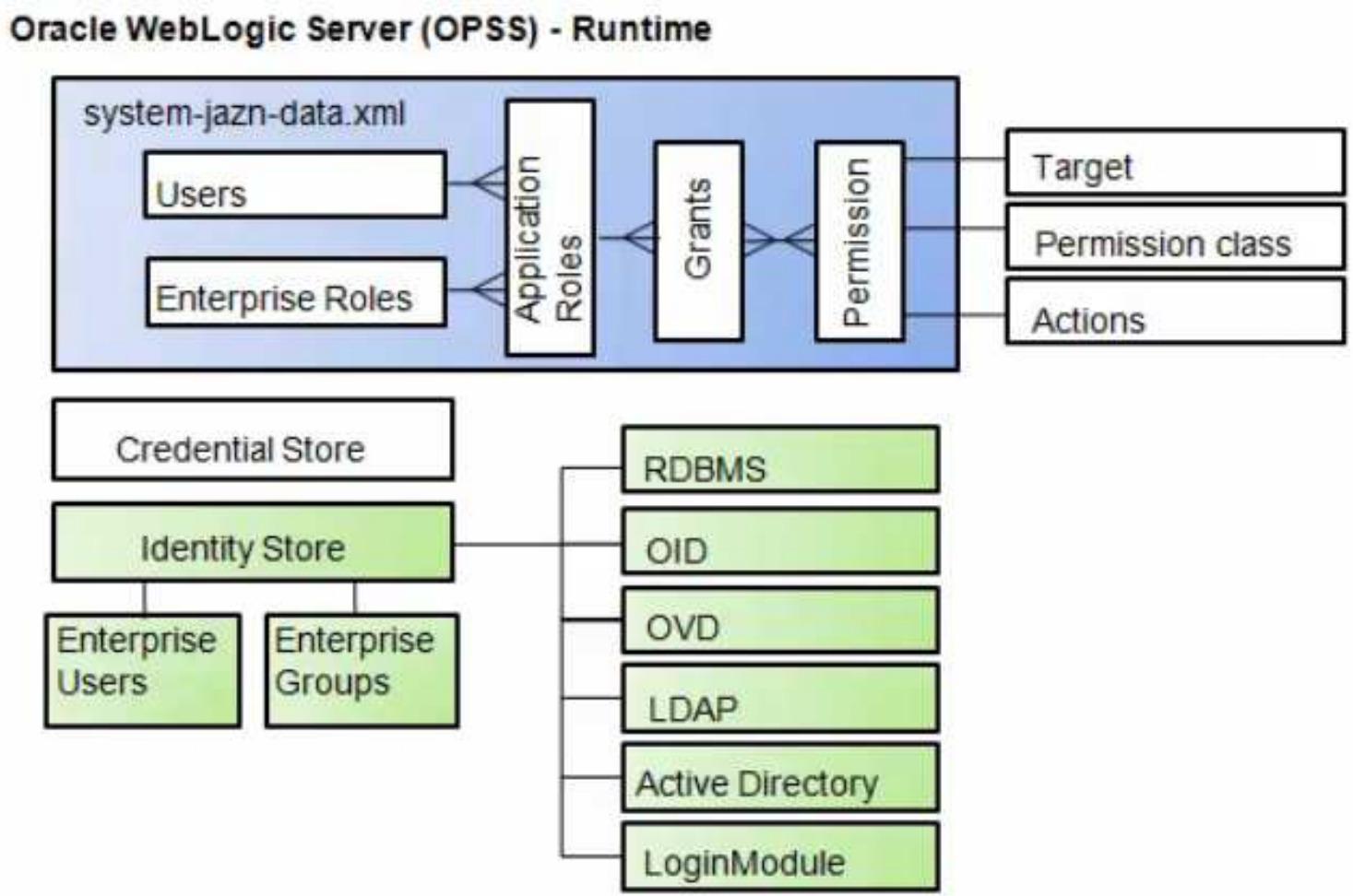
- **Orchestrierung: Definition**
- **Orchestrator vs. DevOps**
- **IT-Experten als „Orchestrators“**
- **Welche Voraussetzungen sind nötig?**

  Auf der untersten Ebene der Orchestrierung steht ein Mensch: ein IT-Experte

Was nun?
Rahmenarchitektur für eine Lösung (2)

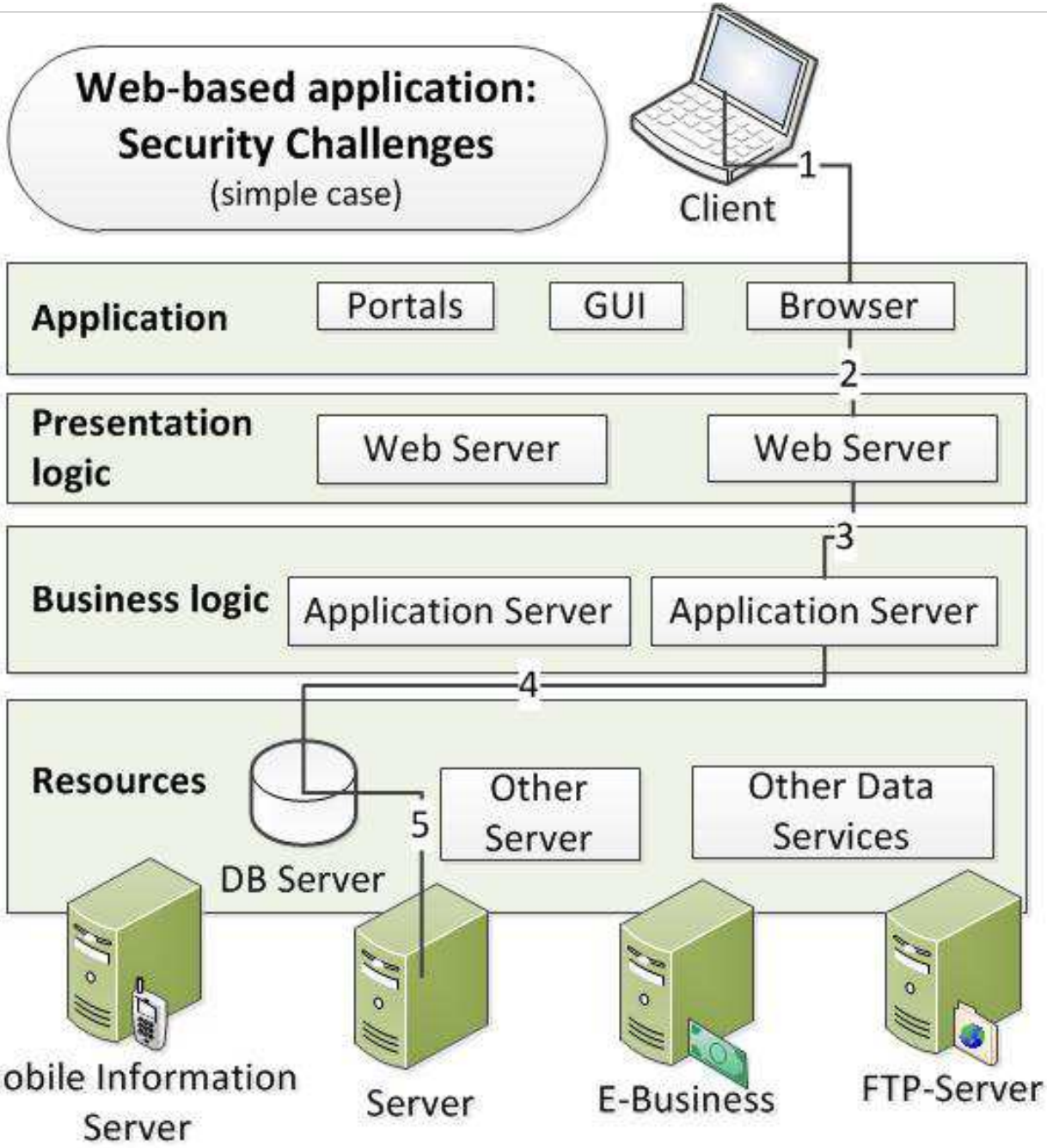
- **Interdisziplinäre IT-Experten auf strategischen, taktischen und operativen Ebenen**
- **Generalisten vs. klassische Spezialisten?**

Oracle Platform Security Services



Security: Einführung

- **Was ist Sicherheit?**
  - **Verfahren zur Gewährleistung, dass die Daten nicht manipuliert wurden**
- **Sicherheitsmaßnahmen**
  - **Proof Material: Gibt einem Benutzer Zugriff auf eine bestimmte Anwendung oder ein System**
  - **Datenverschlüsselung: Übersetzung von Daten in einer Form, die nicht ohne den Besitz oder den Erhalt der geheimen Schlüssel interpretiert werden kann**
- **Authentication, Authorization und Verschlüsselung**


Web-based application:
Security Challenges
(simple case)
Client
1
Application
Portals
GUI
Browser
2
Presentation logic
Web Server
Web Server
3
Business logic
Application Server
Application Server
4
Resources
DB Server
5
Other Server
Other Data Services
Mobile Information Server
Server
E-Business
FTP-Server

WLS Sicherheit und Oracle Platform Security Services (OPSS)

- Sicherheitsherausforderungen in Multi-Tier- und verteilten Systemen
- Netzwerk-basierte Angriffe
- Anwendungssicherheit: Unterschiedlich bei jedem Tier
  - User Interface: Authentification
  - Application Server: Access Backend Database
- Herausforderungen der Anwendungsentwickler: Privacy, Identität Management, Compliance, Audit

WLS Security and Oracle Platform Security Services (OPSS)

- Ein Framework, das eine umfassende Reihe von Sicherheitsdienstleistungen bietet
- Java SE Fähigkeiten: Security APIs
  - Java Cryptography Archtecture (JCA)
  - Java Cryptography Extenstions (JCE)
  - Java Authentication and Autorization Services (JAAS)
  - Java Secure Socket Extensions (JSSE)
- Java EE bietet zusätzliche Sicherheitsfunktionen
  - Container-Managed Authentication
  - Coarse-grained Authorization

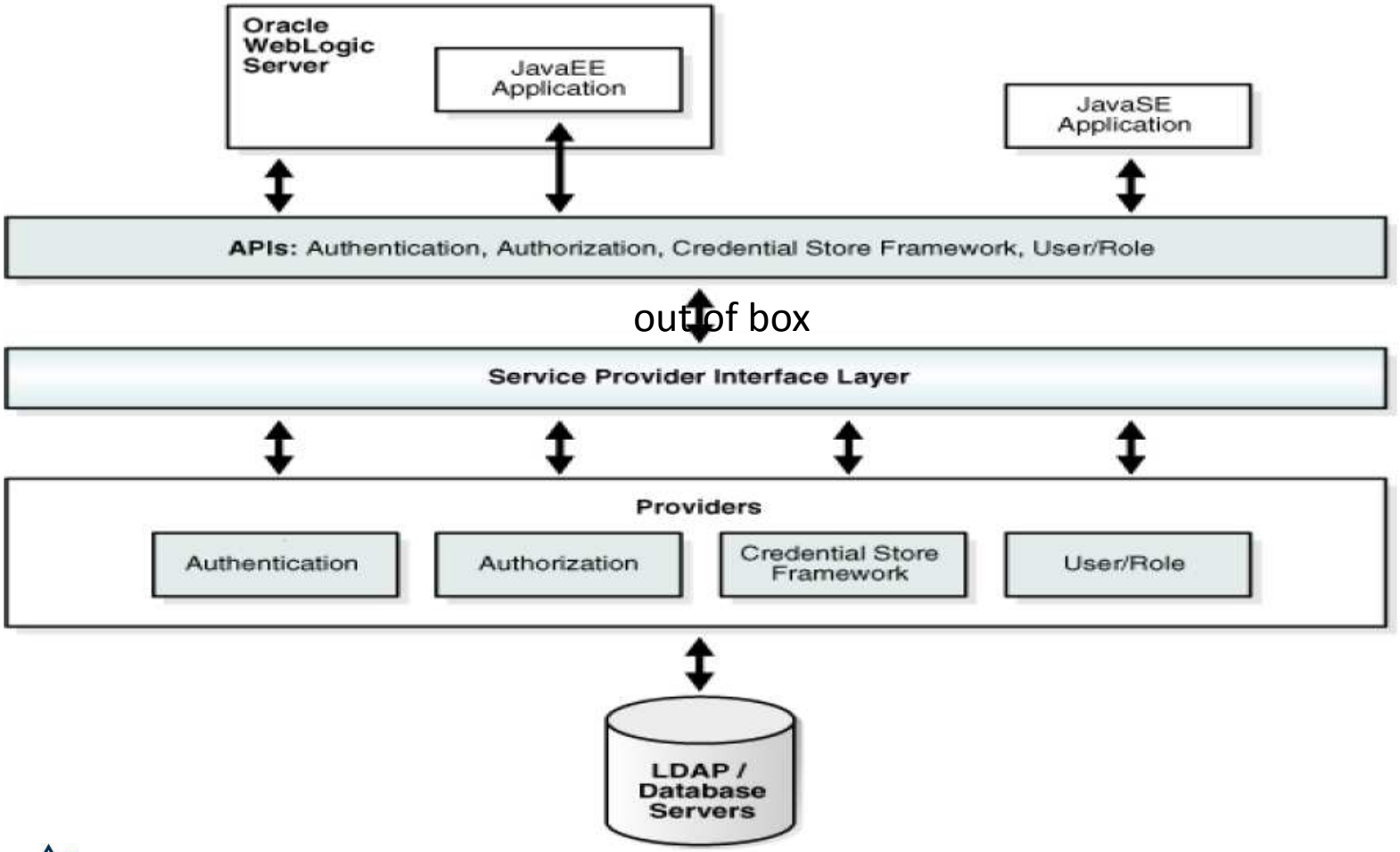
WLS Security and Oracle Platform Security Services (OPSS)

- **Java-Mangel**
  - **Audit**
  - **Single Sign-On (SSO)**
  - **Fine-grained Authorization**
  - **Management-Werkzeuge**

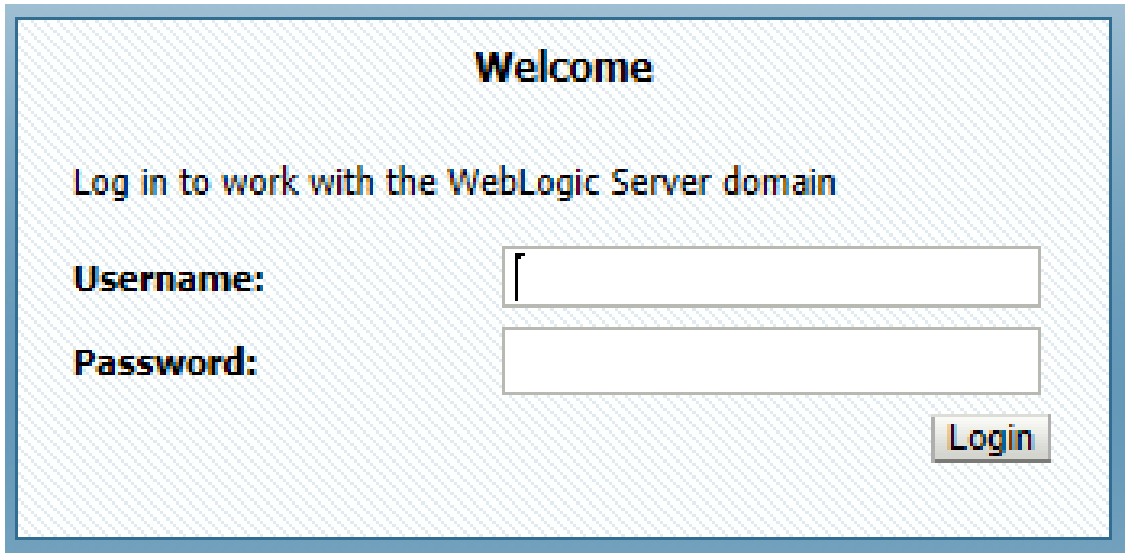
Oracle Platform Security Services

- **Enterprise Security Framework**
  - **ein in sich geschlossenes und unabhängiges Framework**
  - **einheitliche Sicherheitsmaßnahmen**
  - **Identität-Management**
  - **Audit-Dienste im gesamten Unternehmen**
- **Baut auf Java SE und Java EE**
- **Gemeinsame Sicherheitsplattform von OFM über WLS**
  - **Oracle SOA**
  - **Oracle WebCenter**
  - **Oracle Application Development Framework (ADF) und…**

OPSS: Architektur



WebLogic Server



WebLogic Server: Sicherheit

- **Eine sichere Grundlage für Anwendungen, die über das Web verfügbar sind**
- **Ein umfassendes und auf Standards basierendes Design**
- **End-to-End-Sicherheit für WebLogic Server-gehostete Anwendungen, vom Mainframe bis zum Web-Browser**

WebLogic Server: Sicherheit

- **Ein konsistentes Modell, um Sicherheitsrichtlinien auf Java EE und anwendungsdefinierte Ressourcen zu verwenden**
- **Eigenständig auf WebLogic Server-Anwendungen oder als Teil eines unternehmensweiten Sicherheitsmanagement-Systems zu nutzen**

WebLogic Server: Sicherheit

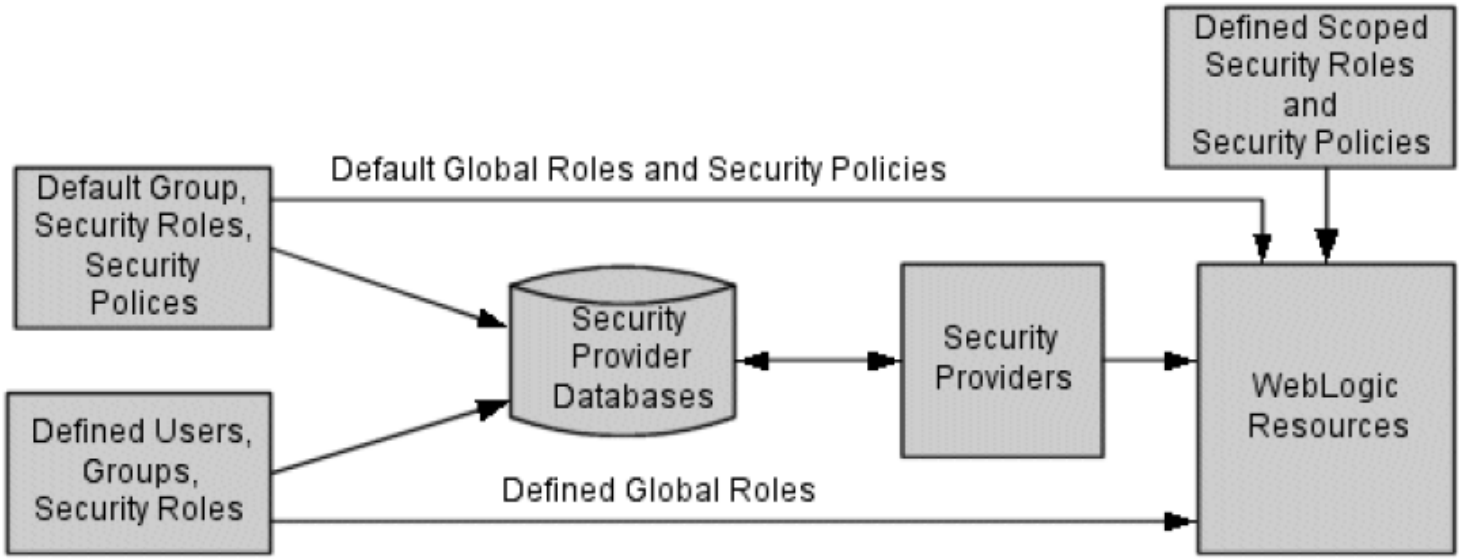
- **Ressourcen: eine Entität oder Aktion**
  - **Entität: z.B. Web Service, Server Instanz**
  - **Aktion: z.B. ein Verfahren im Web-Service, Abschaltung einer Serverinstanz**
- **Sicherheit: eine Herausforderung in Umgebungen mit unterschiedlichen Ressourcen**
- **Auditing: eine elektronische Spur von Computer-Aktivitäten**
- **Sicherheitsterminologie: Users, Groups, Roles, Role Mapping, Policy**

WLS Sicherheitskonzept

- **Authentication → Authorization → Role mapper → Access decision → Adjudication**
- **Authentication: Wer sind Sie?**
  - **Identität Information**
  - **Users, Groups, oder Roles**
- **Authorization: Worauf können Sie zugreifen?**
  - **Steuert die Interaktion zwischen Benutzer und Ressourcen**
- **Rolle Mapper: legt ein gültiges Token zu einem WLS-Benutzer fest**

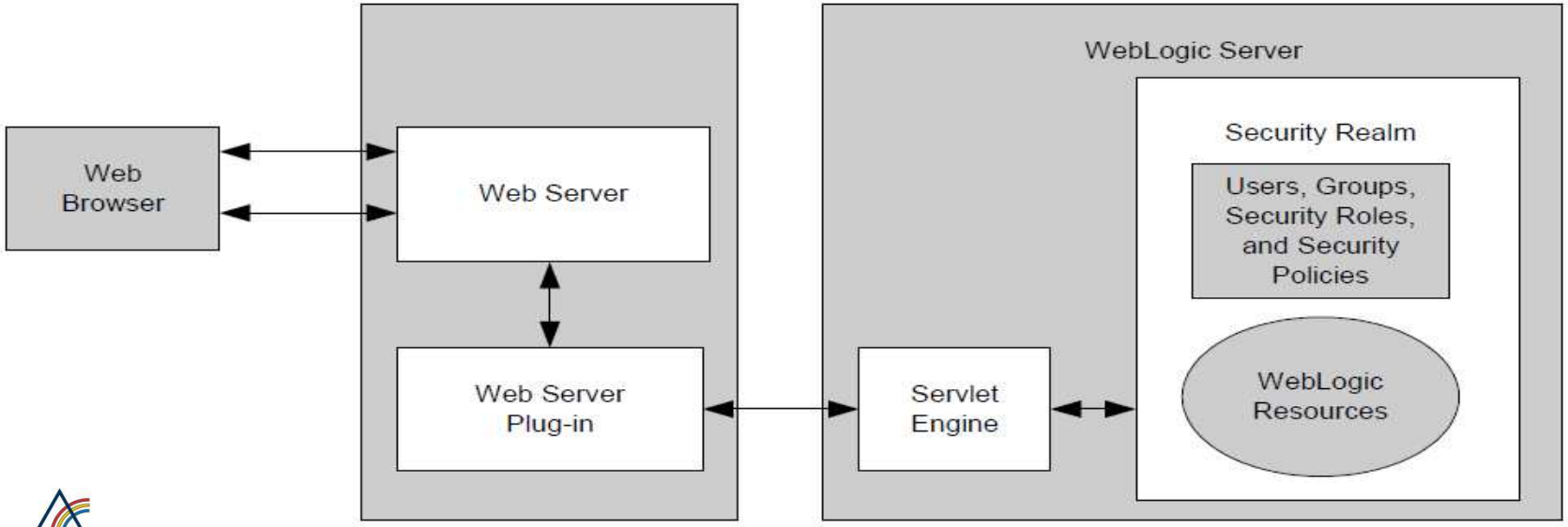
Security Realm

- **Mechanismen für den Schutz von WebLogic Ressourcen**
- **Eine Reihe von konfigurierten Security Providers, Users, Groups, Security Roles und Security Policies**

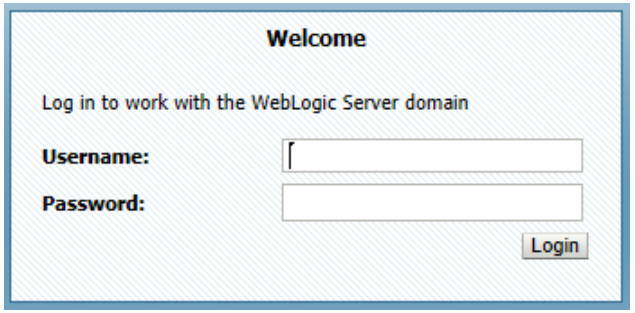


Benutzer

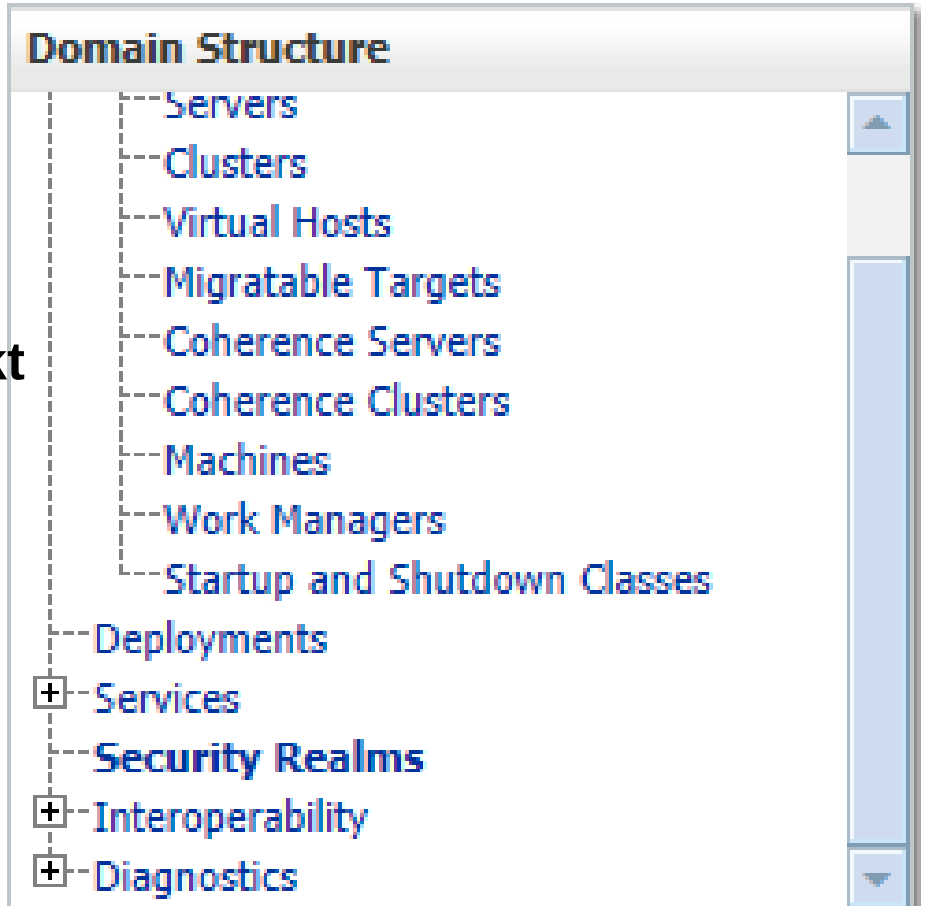
- **Benutzer: eine Entität, die in einem Sicherheitsbereich authentifiziert wird**
  - **Ein Mensch, wie Anwendungsendbenutzer**
  - **Eine Software-Einheit, wie eine Client-Anwendung**
  - **Andere Instanzen von WebLogic Server**



Administration Console: Benutzer

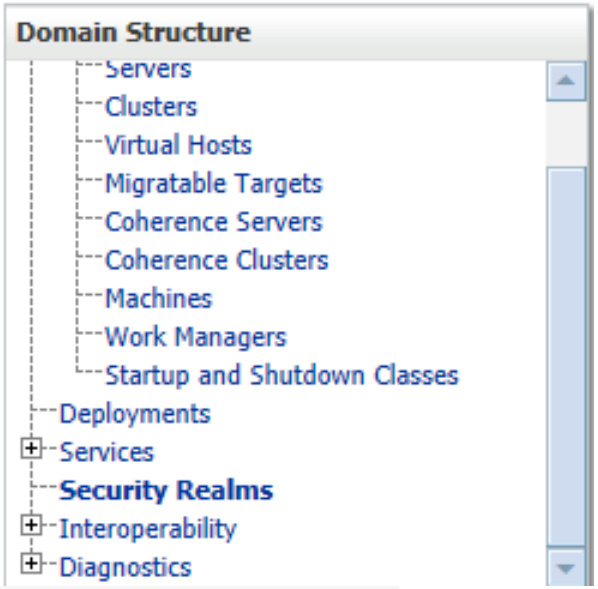


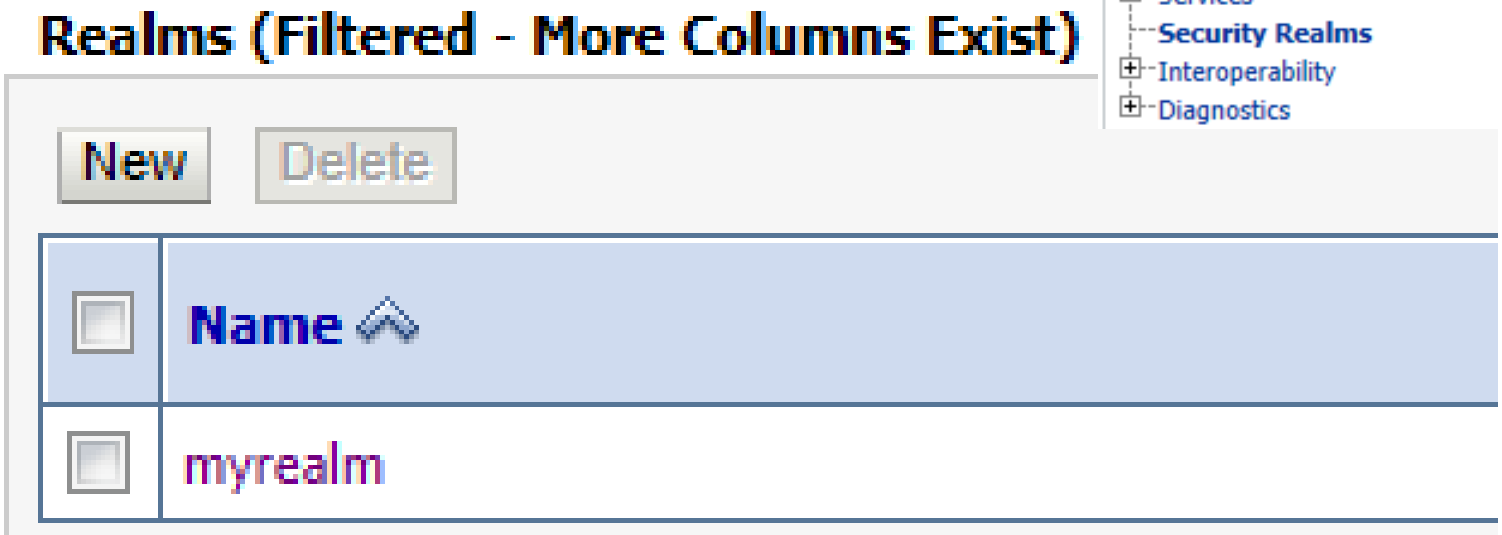
- **Benutzer können in Gruppen angeordnet werden oder direkt mit Sicherheitsrollen zugeordnet werden**
- **Zugriff WebLogic Server**
  - **Proof-Material in der Regel über ein JAAS LoginModule**



Administration Console: Benutzer

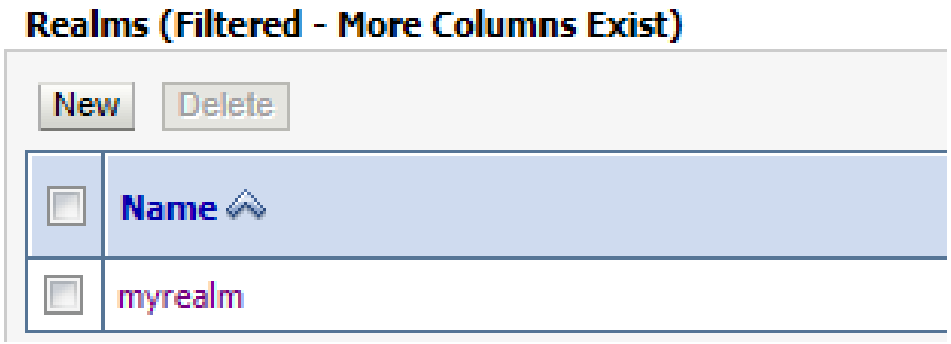
- **WLS verschlüsselt alle Passwörter**
- **Alle Benutzernamen und Gruppen müssen in einem Sicherheitsbereich eindeutig sein**

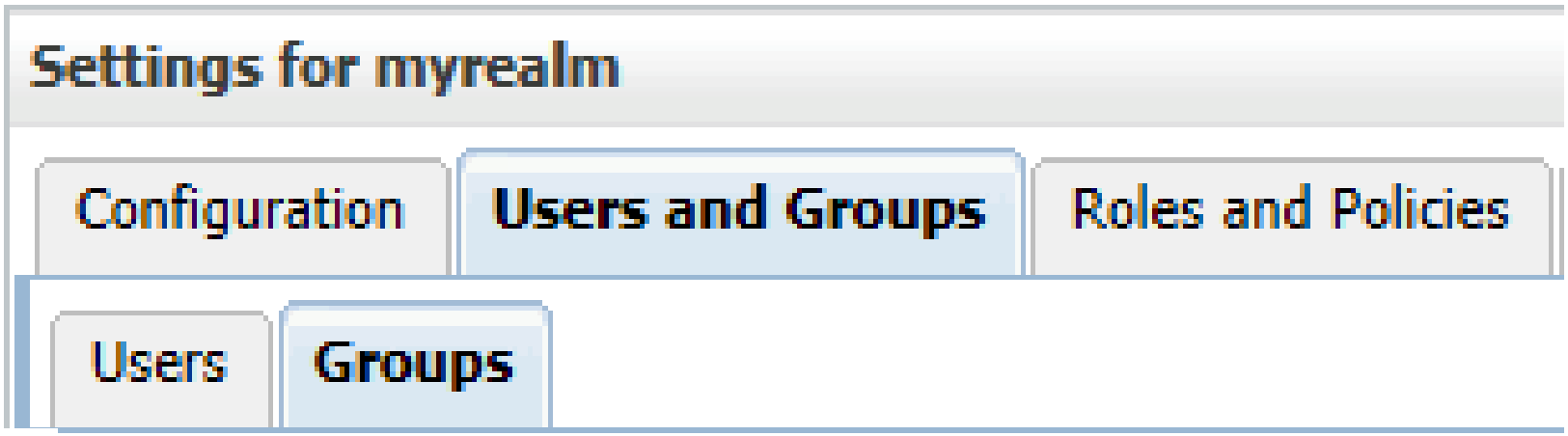




Administration Console: Gruppen

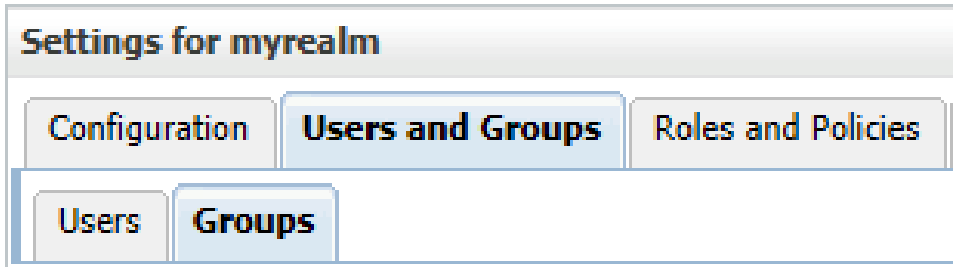
- **Gruppen sind logisch geordneten Mengen von Benutzern**
- **Mitglieder der Gruppe: "etwas gemeinsam"**

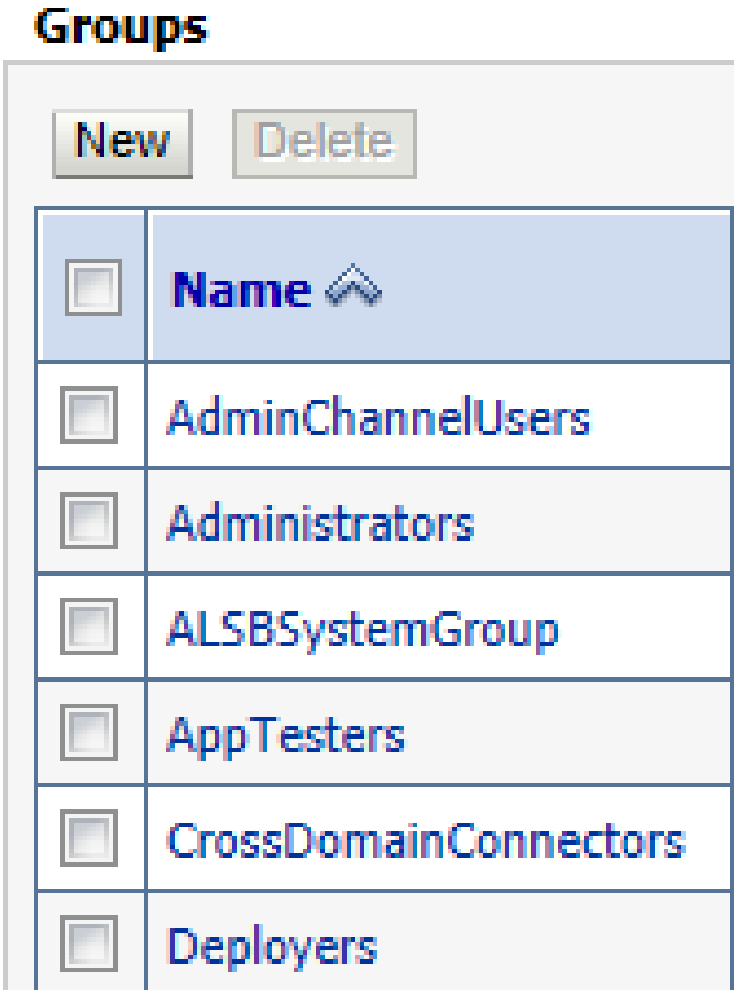




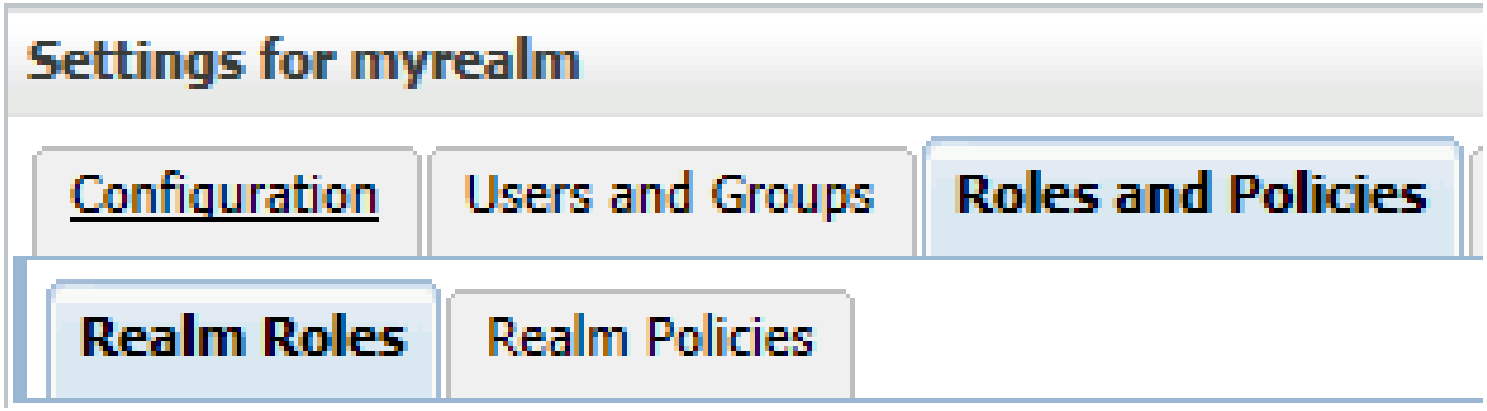
Administration Console: Gruppen

- **Verschiedene Ebenen der Zugang zu WLS-Ressourcen**
- **Vorteil: effizienter für die individuelle Verwaltung von Benutzern**





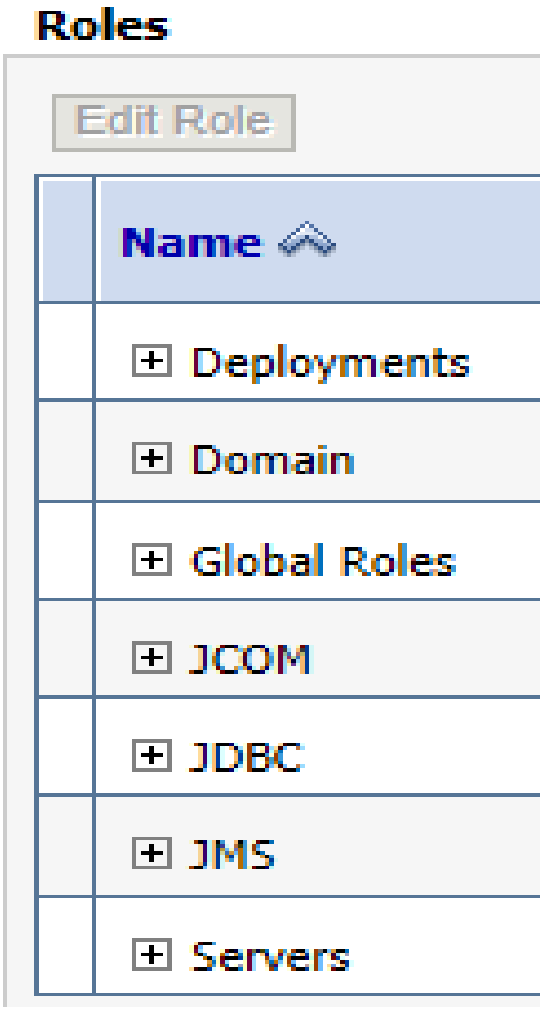
Administration Console: Sicherheitsrollen



- **Ein dynamisch berechnetes Privileg, das Benutzer oder Gruppen auf Basis von bestimmten Bedingungen teilt**
- **Mehrere Rollen können verwendet werden um Sicherheitsrichtlinien zu erstellen**

Administration Console: Sicherheitsrollen

- **Unterschied zwischen den Gruppen und Rollen**
  - **Gruppen: statische Identität und immer gültig auf die ganze WLS-Domäne**
  - **Rolle: dynamisch berechnet und kann innerhalb einer einzigen Anwendung in einer WLS-Domäne auf bestimmte Ressourcen eingeschränkt werden**



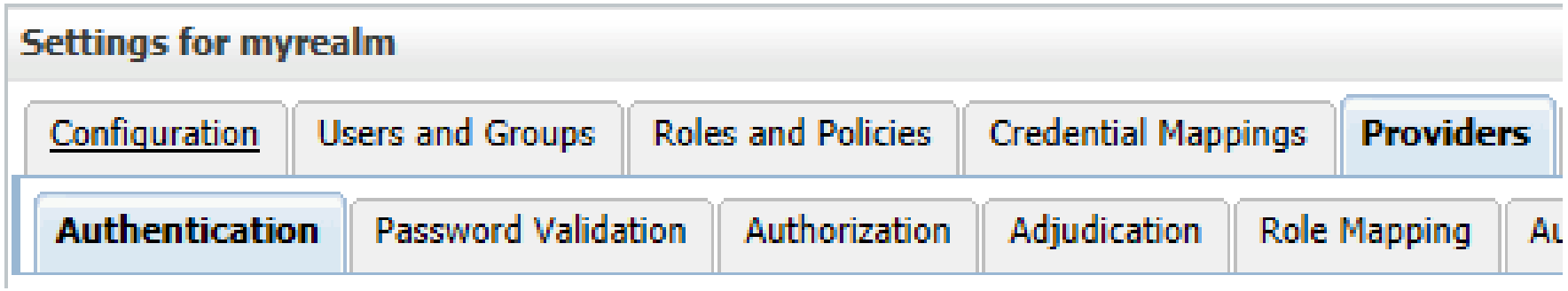
Standardgruppen und Rollen

- **Administrators**
- **Deployers**
- **Operators**
- **Monitors**
- **AppTesters**
- **CrossDomainConnectors**

Security Policy

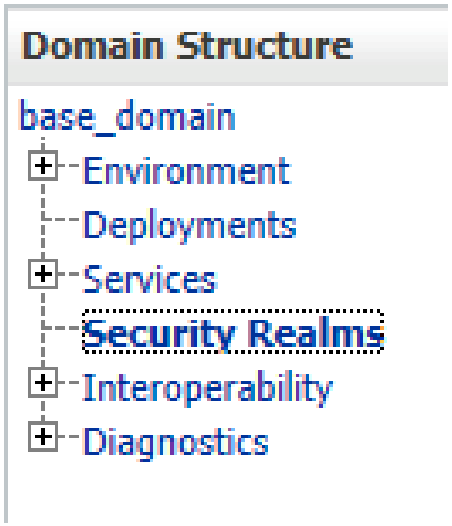
- **Policy: eine Assoziation zwischen einer WebLogic-Ressource und einem oder mehreren Benutzern, Gruppen oder Sicherheitsrollen**
- **Policy Bedingungen**
  - **EJB Method Parameter, HTTP Servlet Request und Session Attributes**
  - **Basic, Date und Time, Context Element**

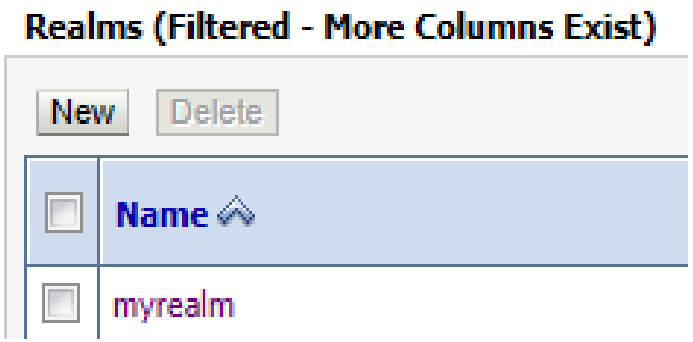
Security Provider

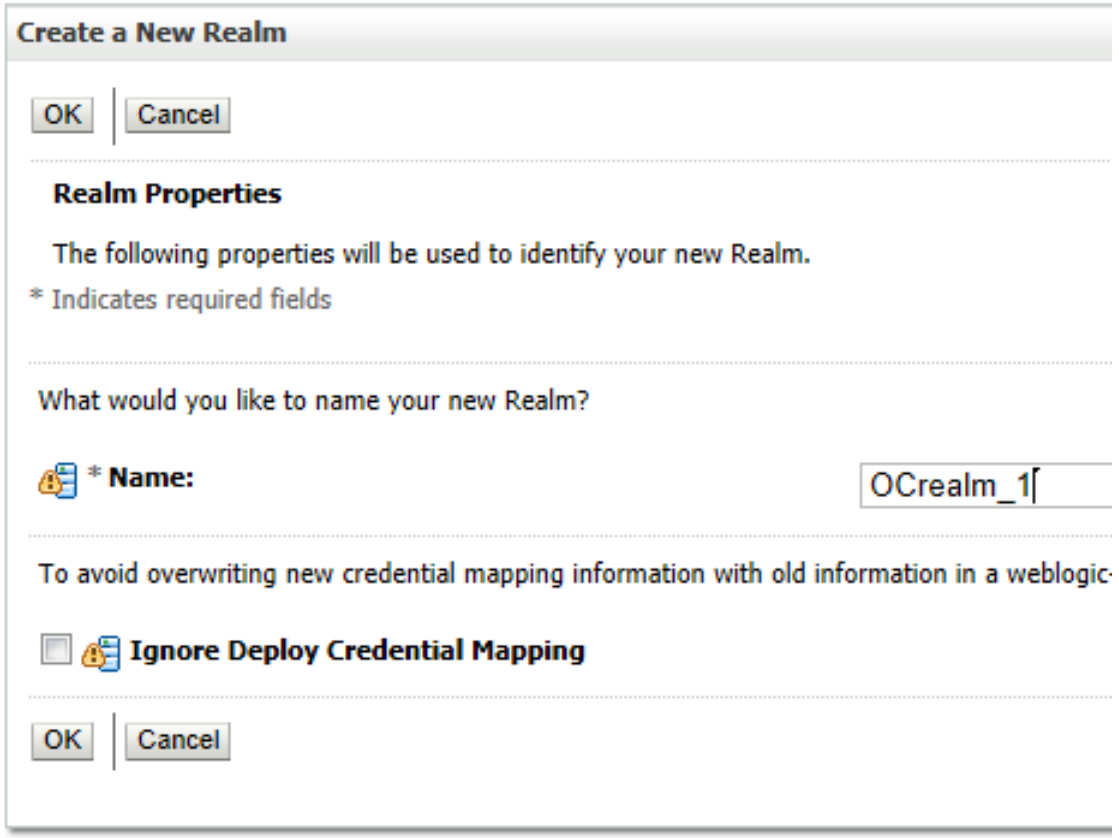


- **Module, die Sicherheitsdienste bereitstellen, um die Anwendungen auf WebLogic-Ressourcen zu schützen**
- **Security Providers**
  - **Ein Teil des WebLogic Server-Produkts**
  - **Benutzerdefinierte Security Provider von Dritt-Security-Anbieter**
  - **Eigenentwickelte benutzerdefinierte Security Provider**

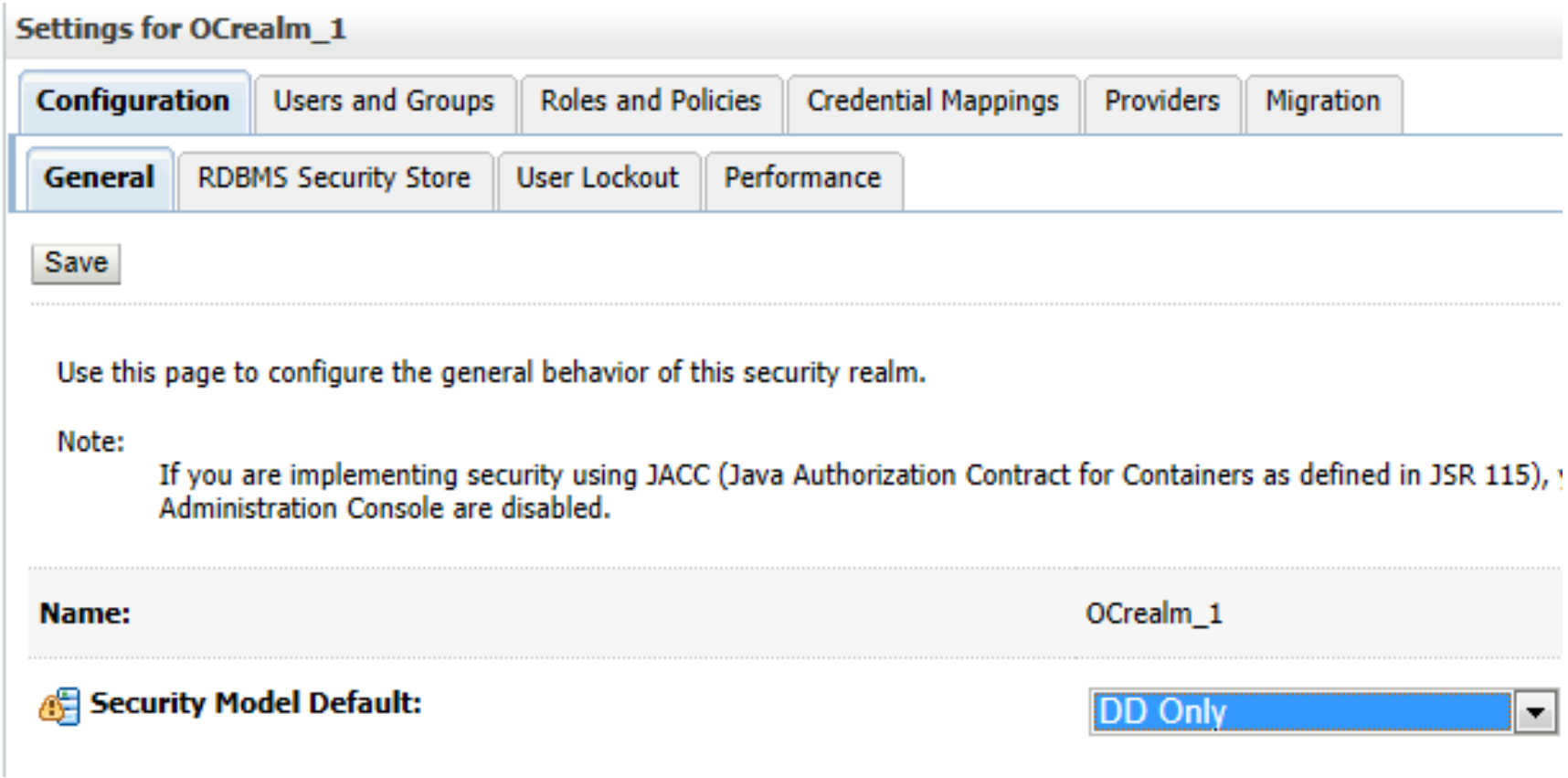
Admin Console: Erstellen eines neuen Realm



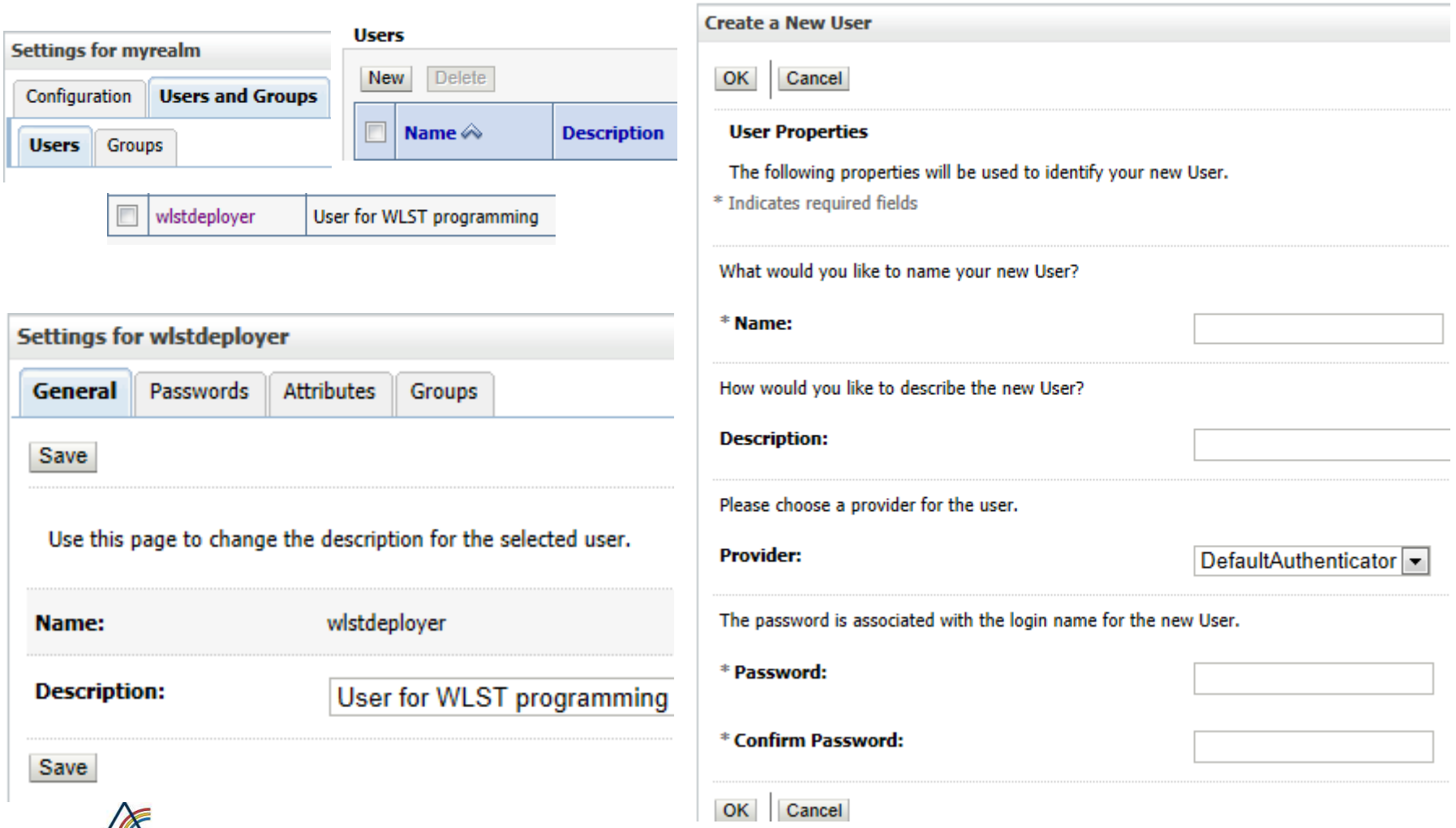




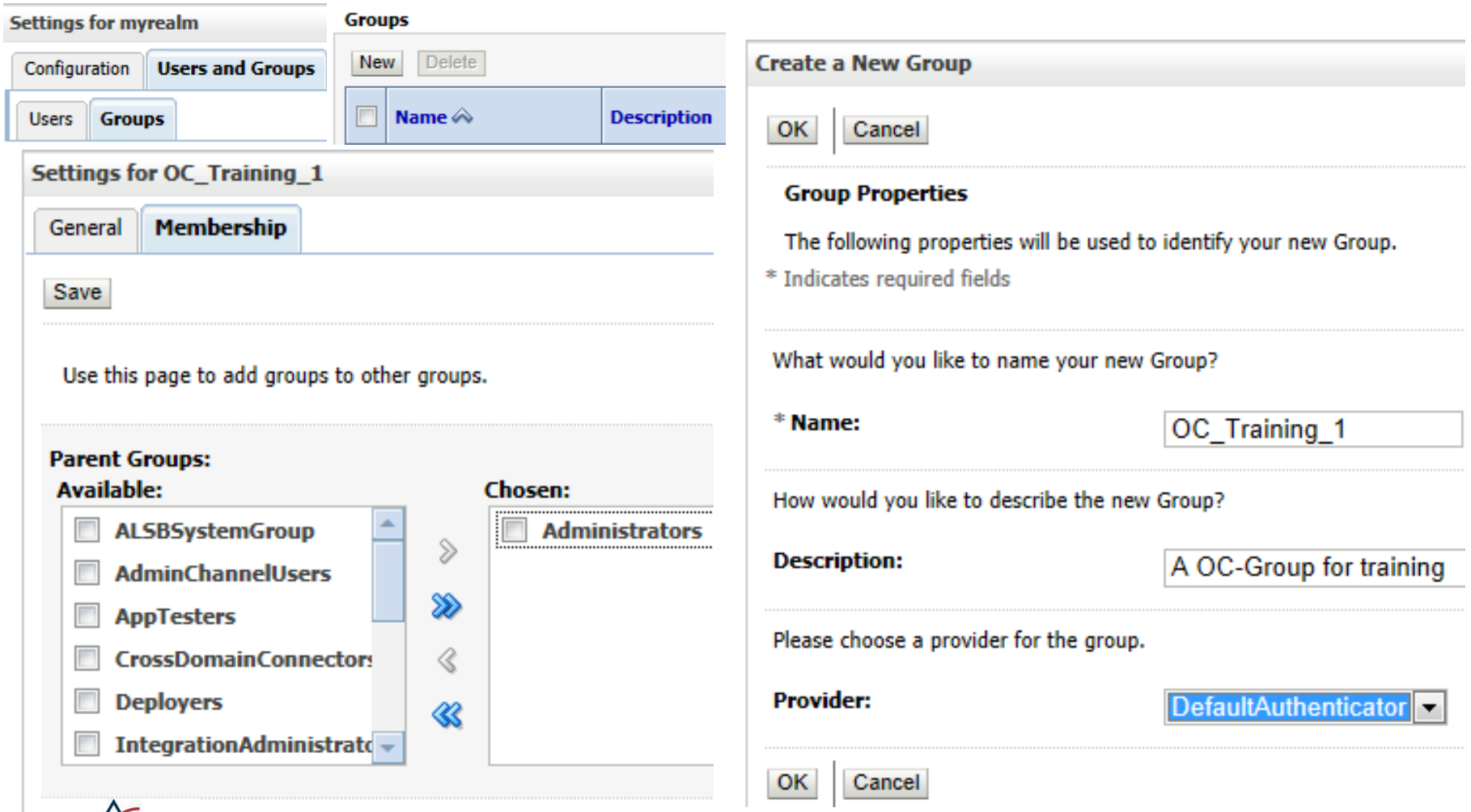
Admin Console: Erstellen eines neuen Realm



Admin Console: Erstellen neue Benutzer



Admin Console: Erstellen neue Groppe



Zusammenfassung

- IT-Landschaft wird noch komplexer!
- Mehrdimensionale Komplexität der IT-Landschaft: Mehrdimensionale Denkmuster
- Flexiblerer Umgang mit Problemen und Herausforderungen
- Neue Maßnahmen für Team- und Weiterbildung
- Oracle Platform Security Services (OPSS)
  - Architektur
  - Funktionalität
- WLS Sicherheit: Konzepte, Grundlagen, Resources, Auditing, Realms, Administration Console (User, Groups, Roles)

Quellenangaben

- IT-Paradigmenwechsel im Zeitalter des Cloud Computing: http://modj.org/fileadmin/user_upload/Mohammad_Esad-Djou_Orchestrator_V1.pdf
- Middleware and oracle fusion approach 11g: http://modj.org/home.html
- http://modj.org/index.php?id=3&tx_ttnews[tt_news]=7&cHash=f953c555a27bc2b6274cdfe214ba3fd1
- Middleware: a short classification http://modj.org/index.php?id=3&tx_ttnews[tt_news]=6&cHash=2405bf47d8fb5efe87e291deb6135b93
- Orchestration (computing): http://en.wikipedia.org/wiki/Orchestration_(computing)
- Oracle Fusion Middleware 11.1.1.5, Security Guides http://docs.oracle.com/cd/E21764_01/security.htm

Quellenangaben

- **Oracle® Fusion Middleware Understanding Security for Oracle WebLogic Server 11g Release 1 (10.3.5)**
  http://docs.oracle.com/cd/E21764_01/web.1111/e13710/toc.htm
- **Oracle® Fusion Middleware Securing Oracle WebLogic Server**
  http://docs.oracle.com/cd/E21764_01/web.1111/e13707/toc.htm
- **Oracle Platform Security Services 11gR1 (White Paper)**
  http://www.oracle.com/technetwork/middleware/id-mgmt/opss-tech-wp-131775.pdf

Danke
für Ihre Aufmerksamkeit!

Mohammad Esad-Djou, Solution Architect

OPITZ CONSULTING Deutschland GmbH
Mohammad.Esad-Djou@opitz-consulting.com
Fon +49 89 680098-1409
Mobil: +49 173 7279576

Fragen?