



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



Menschen. Innovationen. Lösungen.



„Orchestrator“

IT-Paradigmenwechsel im Zeitalter des Cloud Computing

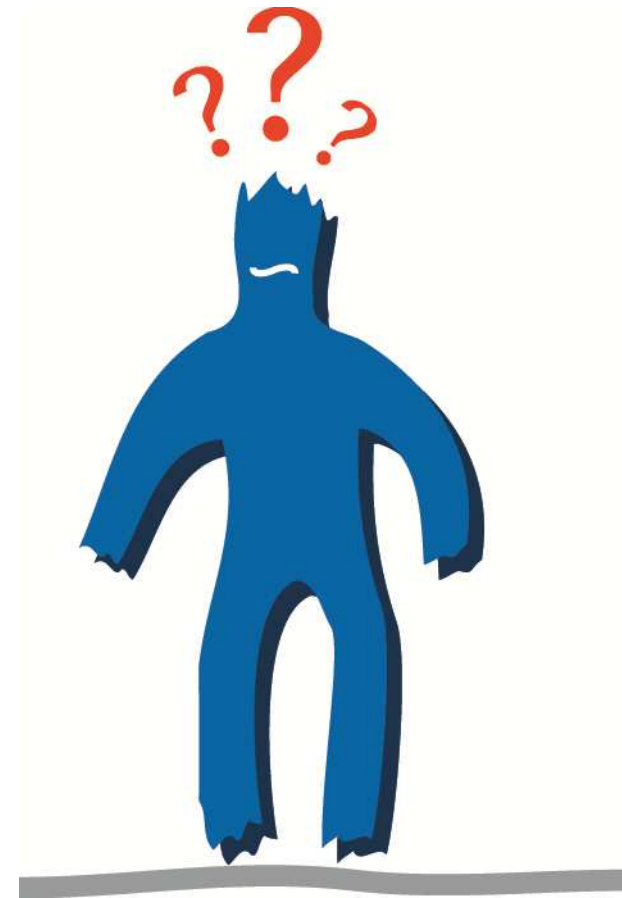
Mohammad Esad-Djou, Solution Architect
OPITZ CONSULTING Deutschland GmbH



Mainz, 06. Juni 2013, DOAG 2013 IM Community Summit

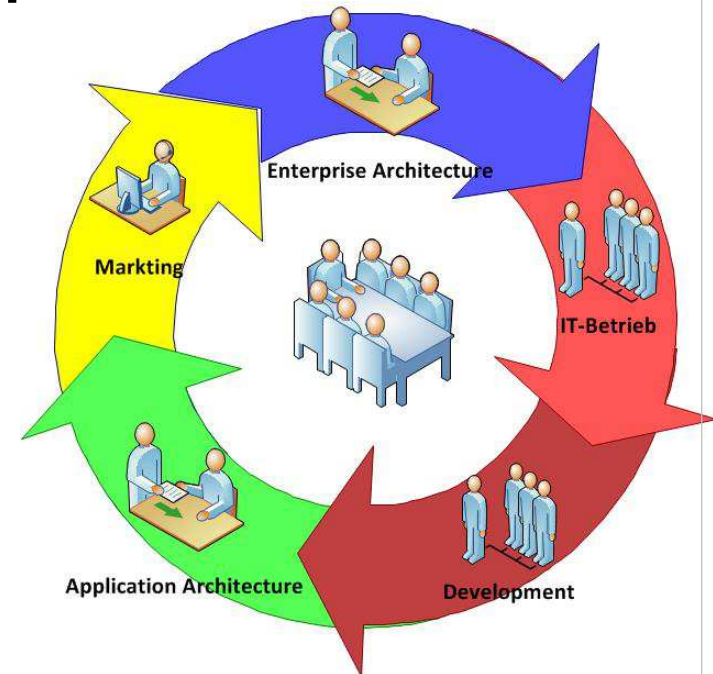
IT-Landschaft wird noch komplexer!

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

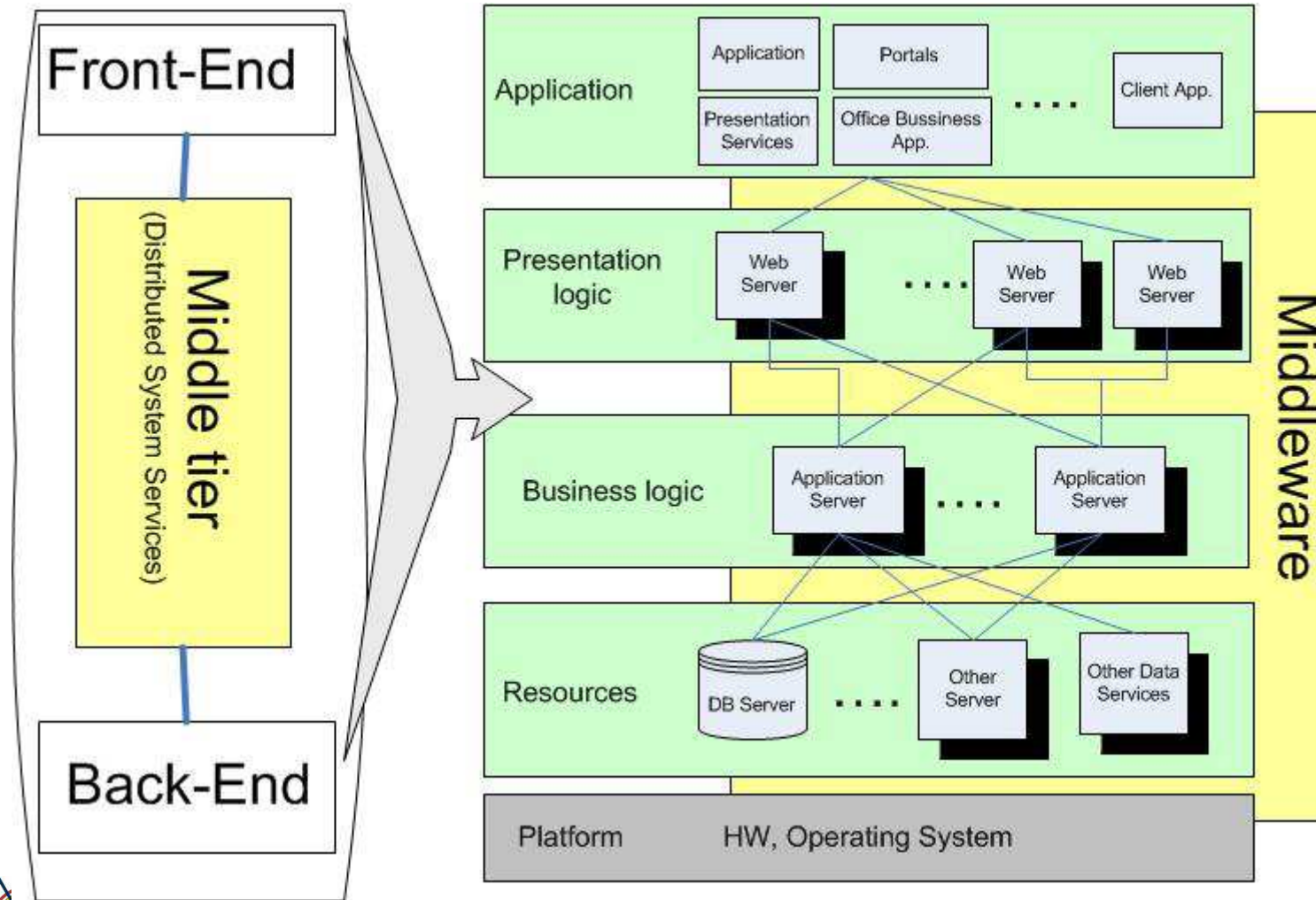


Erste Dimension: Horizontale Komplexität

- **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**

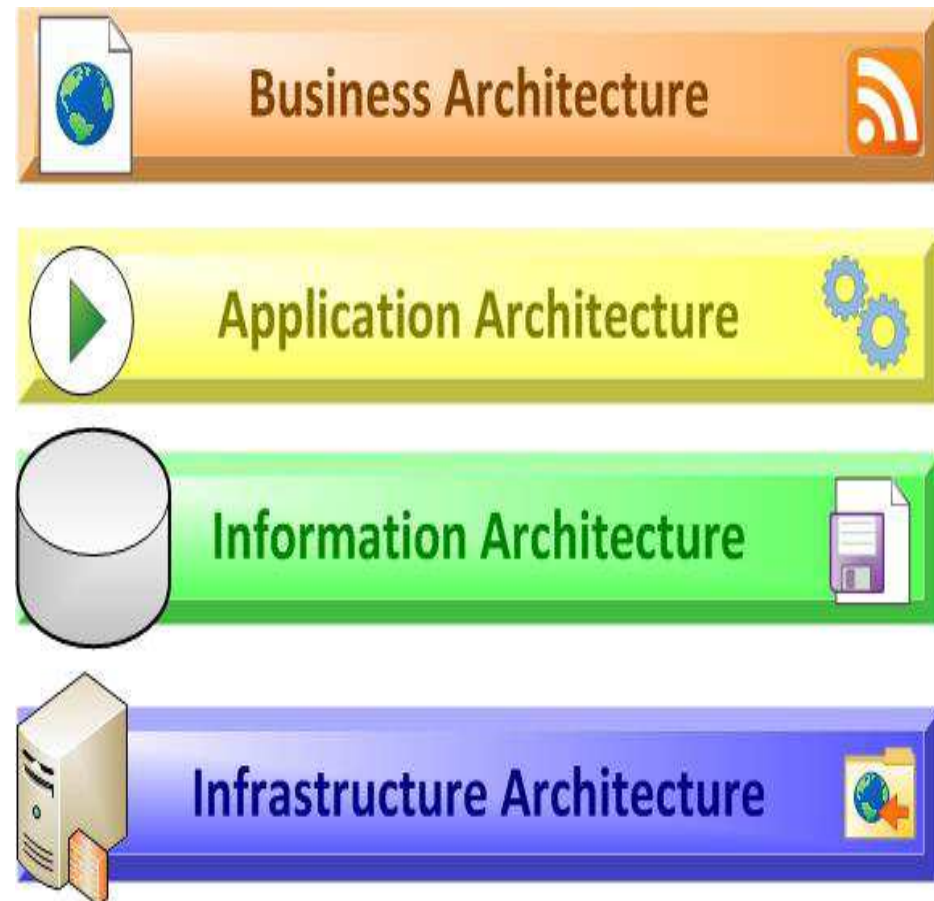


Vertikale Komplexität: Schichtenarchitektur



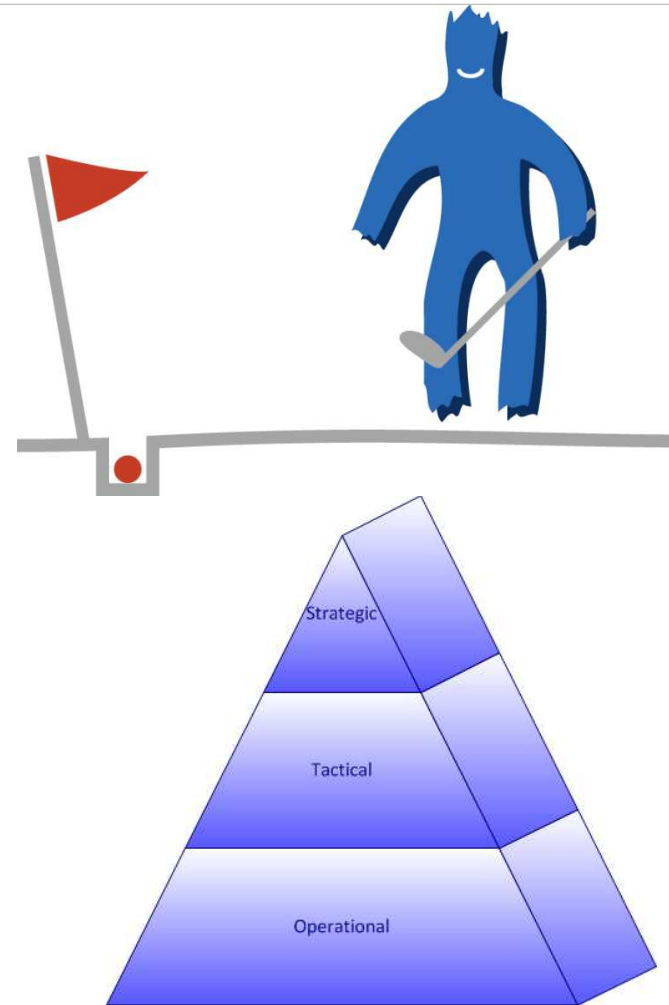
Vertikale Komplexität: Schichtenarchitektur

- **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?

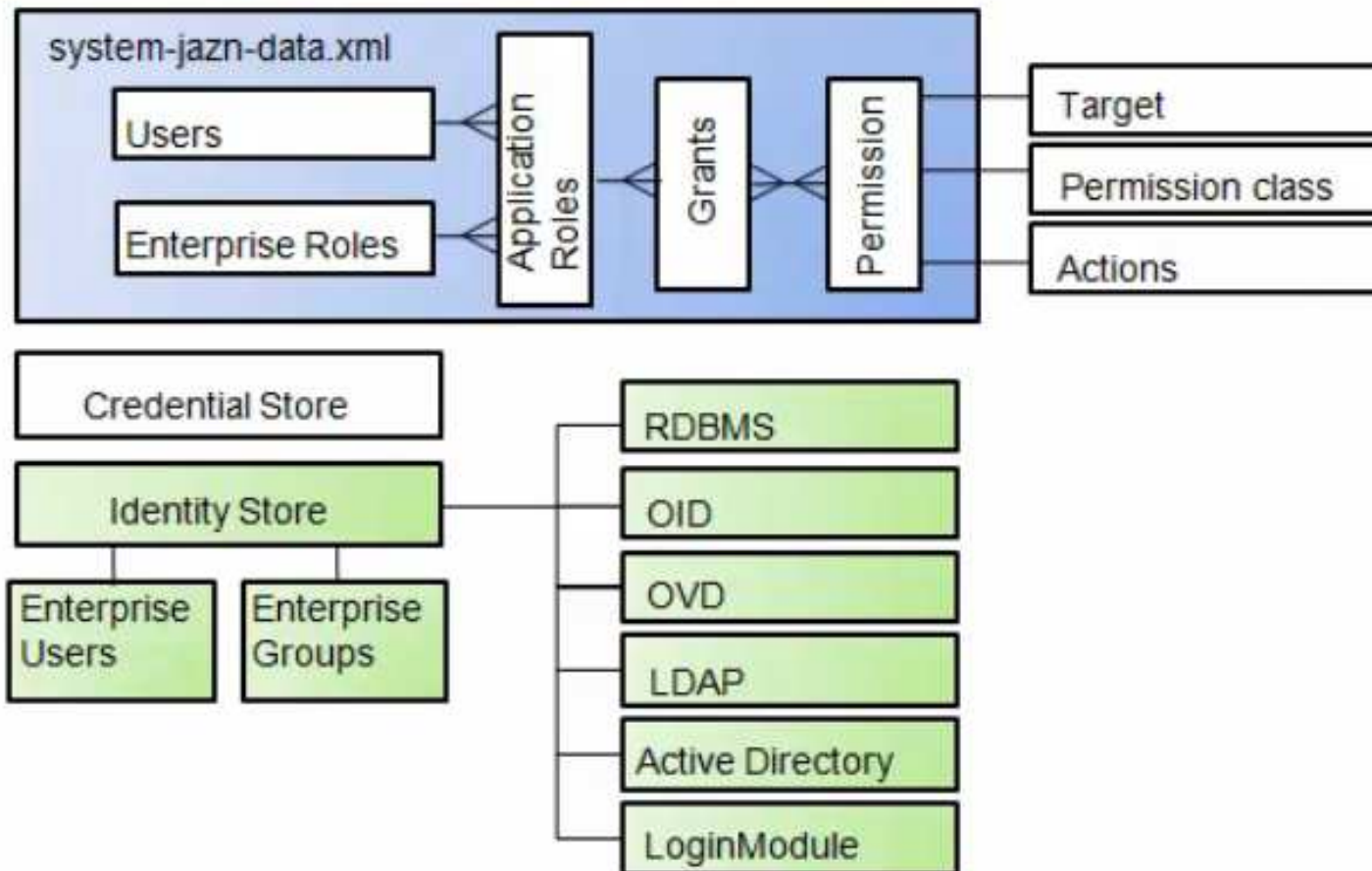
Rahmenarchitektur für eine Lösung (2)

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



Oracle Platform Security Services

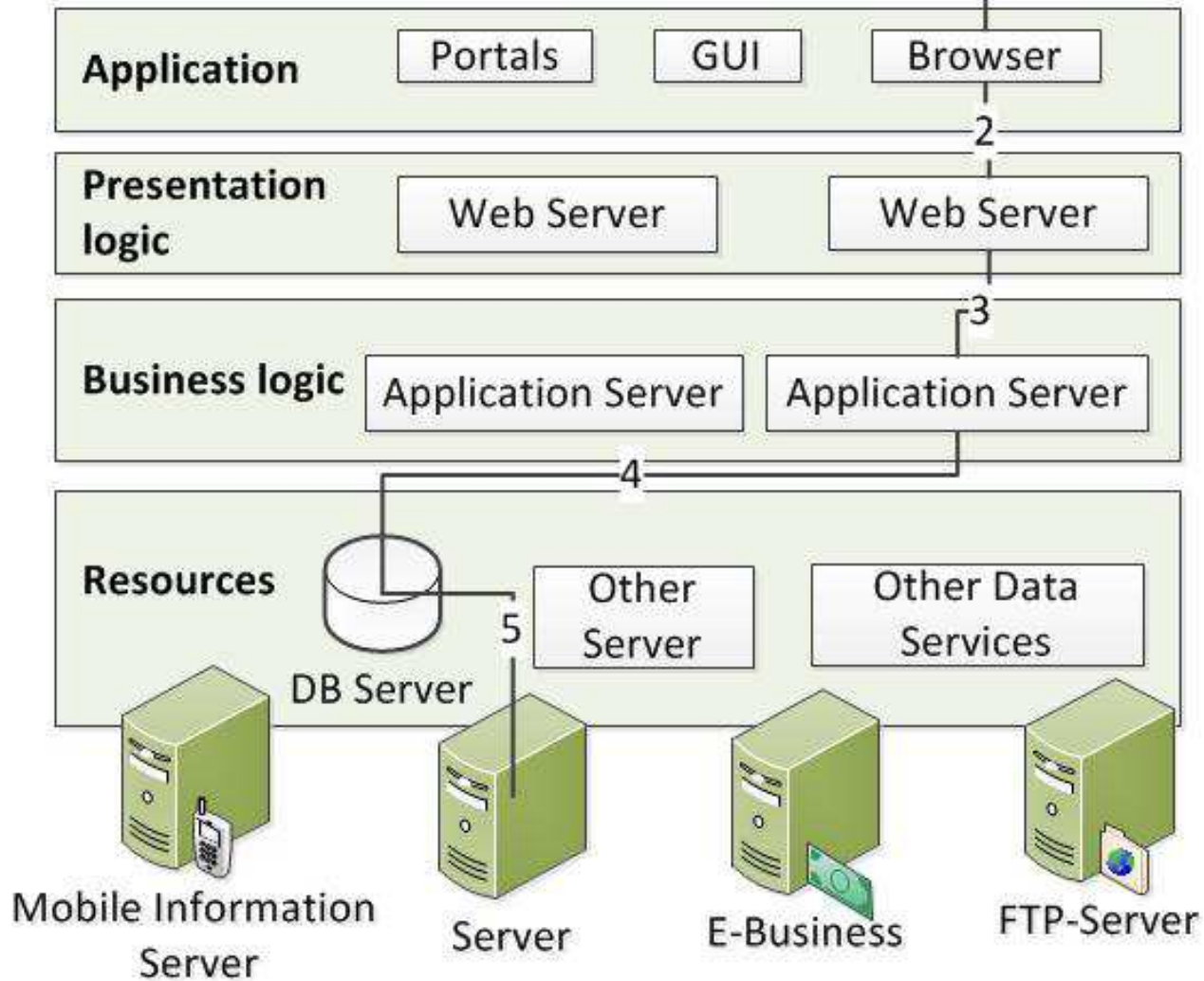
Oracle WebLogic Server (OPSS) - Runtime



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)



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: Authentication**
 - **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 Architecture (JCA)
 - Java Cryptography Extensions (JCE)
 - Java Authentication and Authorization Services (JAAS)
 - Java Secure Socket Extensions (JSSE)
- Java EE bietet zusätzliche Sicherheitsfunktionen
 - Container-Managed Authentication
 - Coarse-grained Authorization

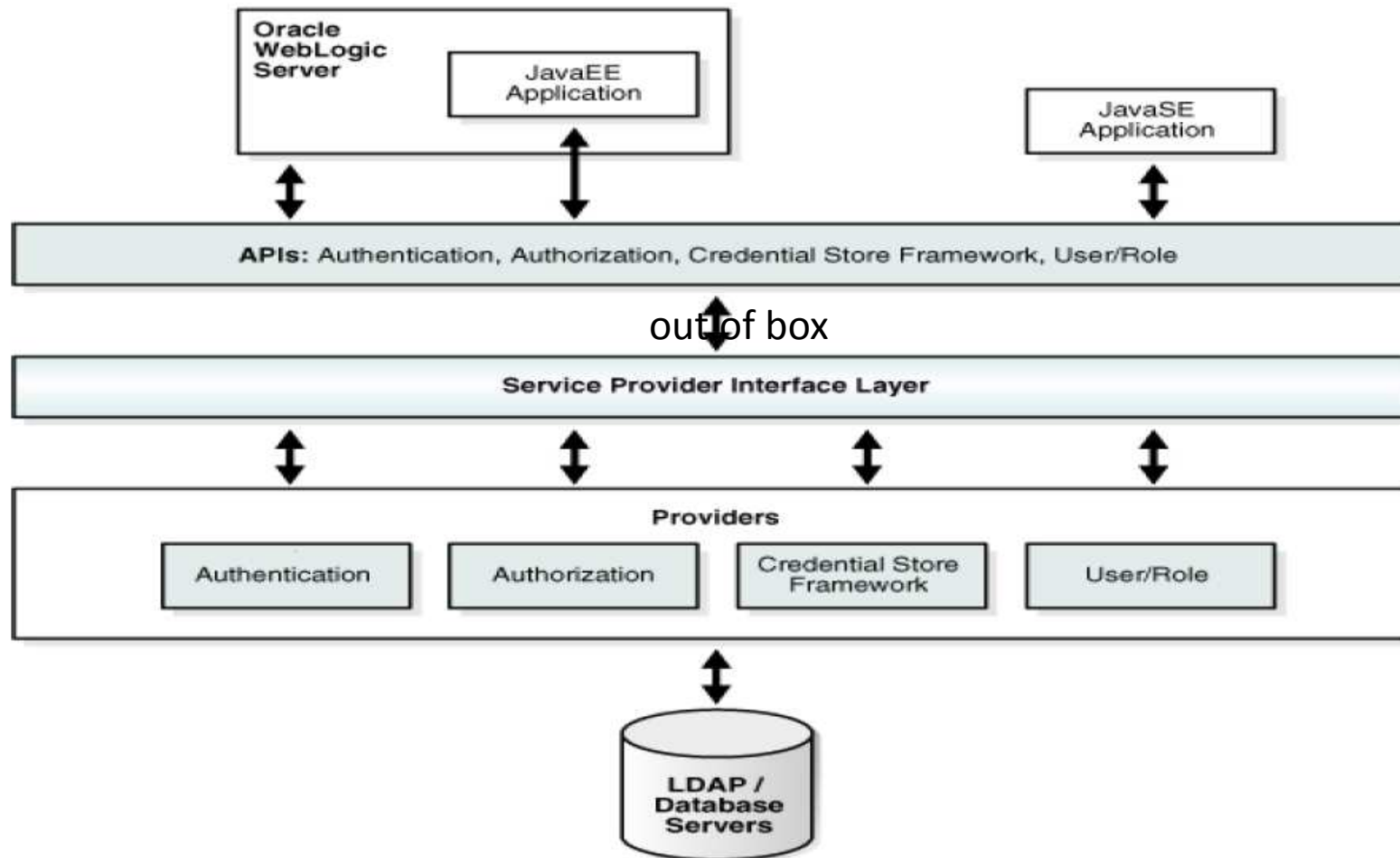
WLS Security and Oracle Platform Security Services (OPSS)

- **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

Welcome

Log in to work with the WebLogic Server domain

Username:

Password:

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

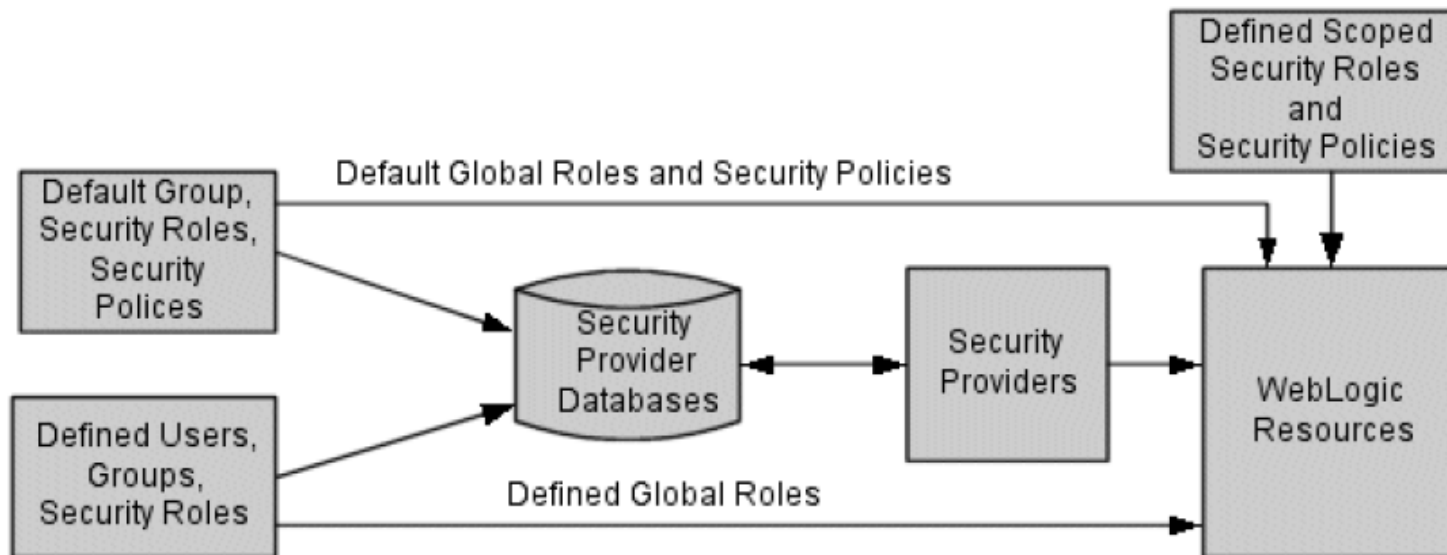
- **Ressourcen: eine Entität oder Aktion**
 - **Entität: z.B. Web Service, Server Instanz**
 - **Aktion: z.B. ein Verfahren im Web-Service, Abschaltung einer Serverinstanz**
- **Sicherheit: eine Herausforderung in Umgebungen mit unterschiedlichen Ressourcen**
- **Auditing: eine elektronische Spur von 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**

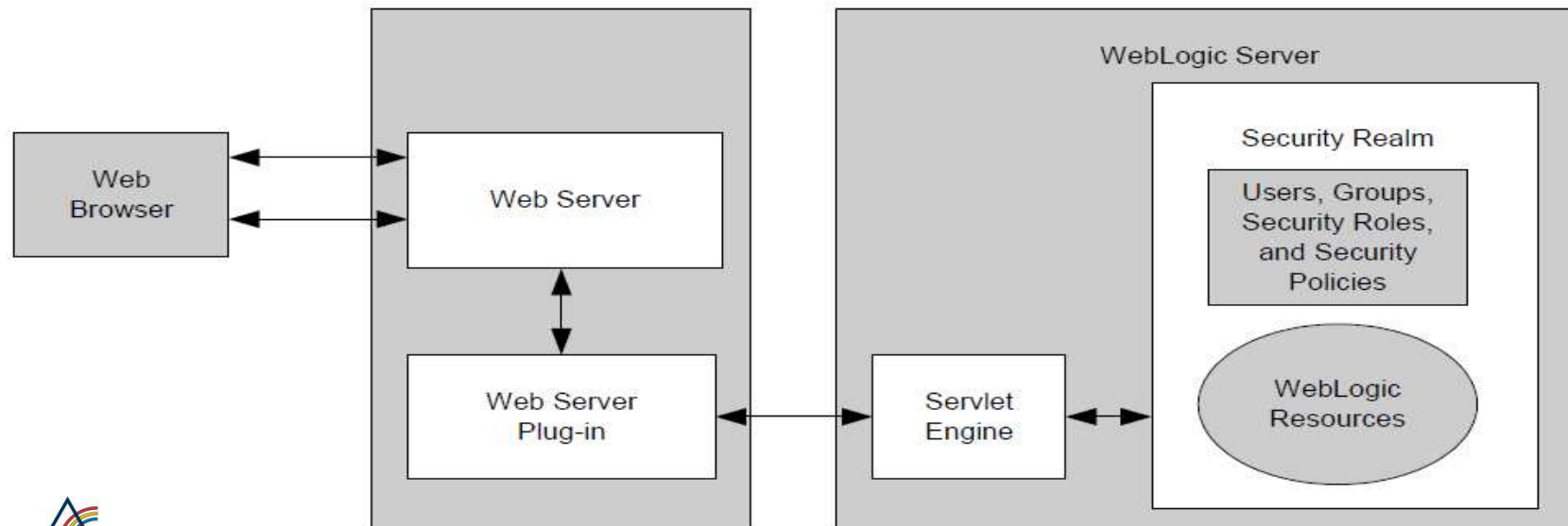
Security Realm

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

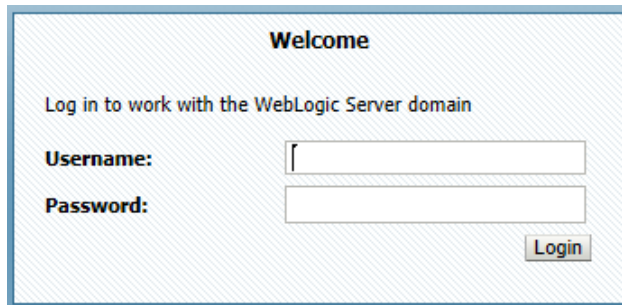


Benutzer

- **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



Welcome

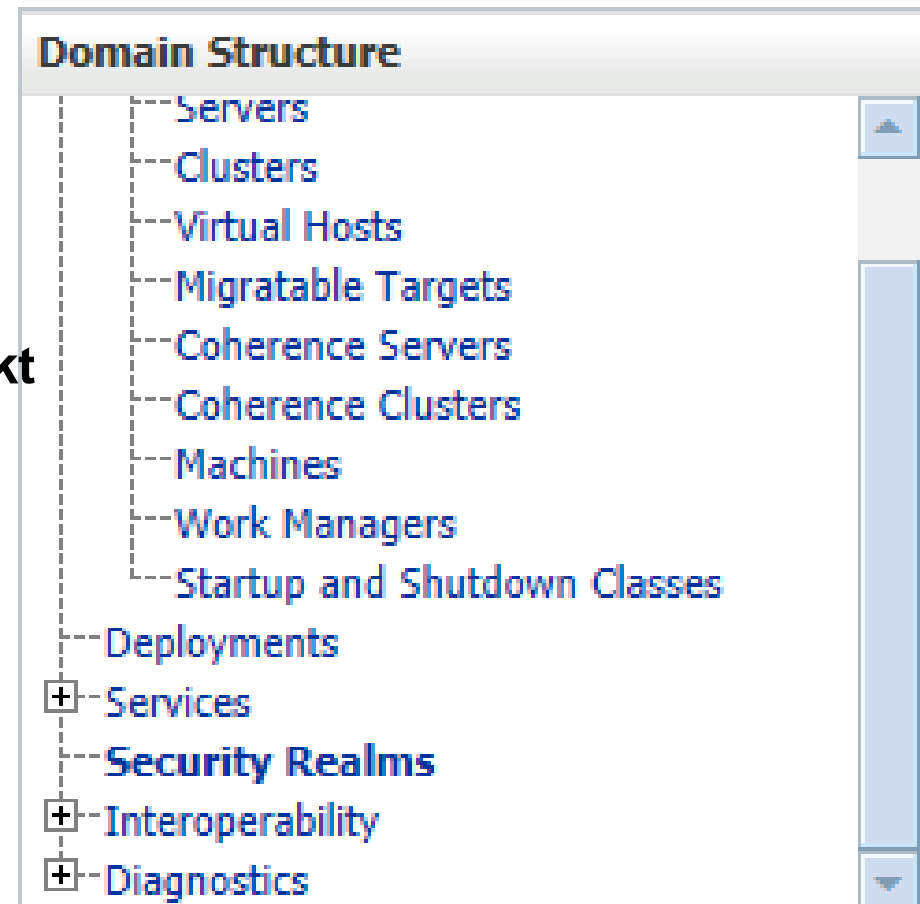
Log in to work with the WebLogic Server domain

Username:

Password:

Login

- 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

Realms (Filtered - More Columns Exist)

	Name
	myrealm

Domain Structure

- Servers
- Clusters
- Virtual Hosts
- Migratable Targets
- Coherence Servers
- Coherence Clusters
- Machines
- Work Managers
- Startup and Shutdown Classes
- Deployments
- + Services
- + Security Realms
- + Interoperability
- + Diagnostics

Administration Console: Gruppen

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

Realms (Filtered - More Columns Exist)

New

Delete



Name ↕



myrealm

Settings for myrealm

Configuration

Users and Groups

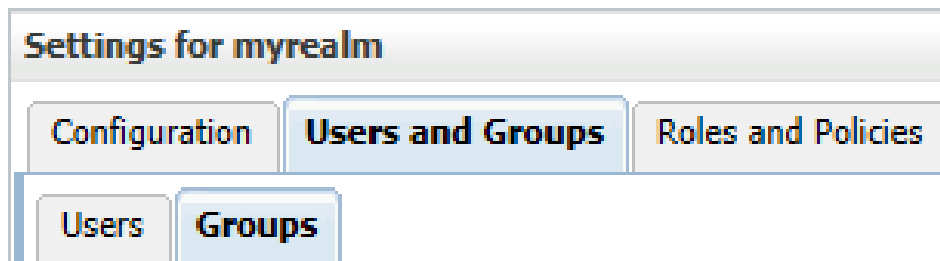
Roles and Policies

Users

Groups

Administration Console: Gruppen

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

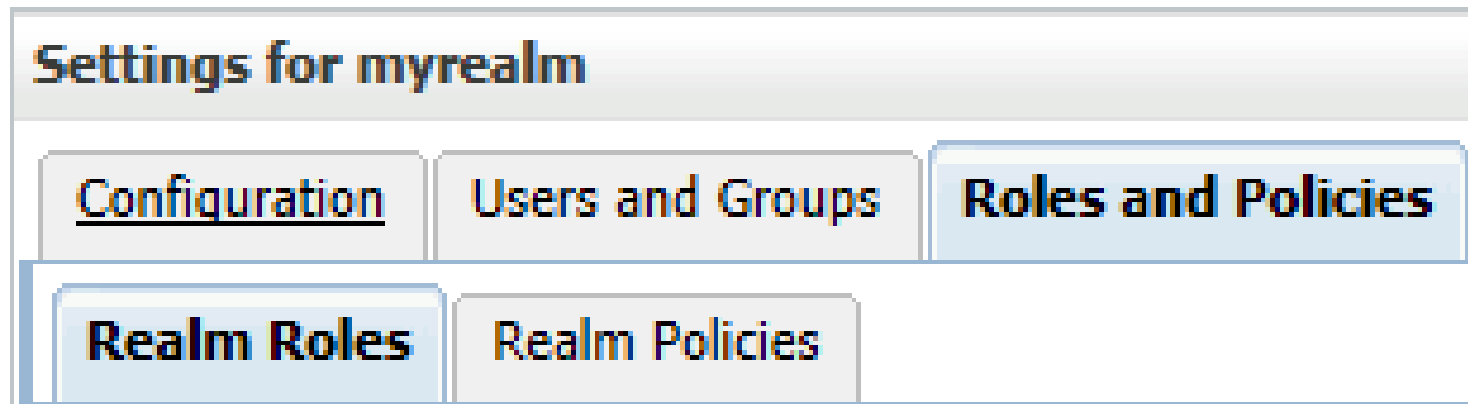


Groups

New Delete

<input type="checkbox"/>	Name
<input type="checkbox"/>	AdminChannelUsers
<input type="checkbox"/>	Administrators
<input type="checkbox"/>	ALSBSystemGroup
<input type="checkbox"/>	AppTesters
<input type="checkbox"/>	CrossDomainConnectors
<input type="checkbox"/>	Deployers

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**

Roles

Edit Role

	Name 
	 Deployments
	 Domain
	 Global Roles
	 JCOM
	 JDBC
	 JMS
	 Servers

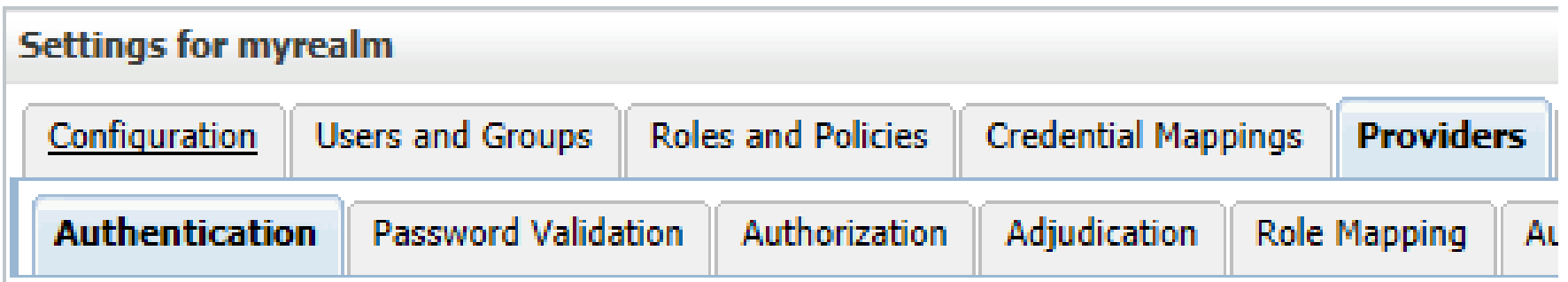
Standardgruppen und Rollen

- **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

Domain Structure

- base_domain
 - + Environment
 - Deployments
 - + Services
 - Security Realms**
 - + Interoperability
 - + Diagnostics

Realms (Filtered - More Columns Exist)

<input type="checkbox"/>	Name
<input type="checkbox"/>	myrealm

Create a New Realm

Realm Properties

The following properties will be used to identify your new Realm.

* Indicates required fields

What would you like to name your new Realm?

* **Name:**

To avoid overwriting new credential mapping information with old information in a weblogic

Ignore Deploy Credential Mapping

Admin Console: Erstellen eines neuen Realm

Settings for OCrealm_1

Configuration

Users and Groups

Roles and Policies

Credential Mappings

Providers

Migration

General

RDBMS Security Store

User Lockout

Performance

Save


Use this page to configure the general behavior of this security realm.

Note:

If you are implementing security using JACC (Java Authorization Contract for Containers as defined in JSR 115), Administration Console are disabled.

Name:

OCrealm_1

 **Security Model Default:**

DD Only

Admin Console: Erstellen neue Benutzer

Settings for myrealm

Configuration **Users and Groups**

Users Groups

	Name	Description
<input type="checkbox"/>	wlstdeployer	User for WLST programming

Settings for wlstdeployer

General Passwords Attributes Groups

Save

Use this page to change the description for the selected user.

Name: wlstdeployer

Description:

Save

Create a New User

OK Cancel

User Properties

The following properties will be used to identify your new User.

* Indicates required fields

What would you like to name your new User?

* **Name:**

How would you like to describe the new User?

Description:

Please choose a provider for the user.

Provider:

The password is associated with the login name for the new User.

* **Password:**

* **Confirm Password:**

OK Cancel

Admin Console: Erstellen neue Gruppe

Settings for myrealm

Configuration | **Users and Groups**

Users | **Groups**

Groups

New | Delete

<input type="checkbox"/>	Name ↕	Description
--------------------------	--------	-------------

Settings for OC_Training_1

General | **Membership**

Save

Use this page to add groups to other groups.

Parent Groups:

Available:

- ALSBSystemGroup
- AdminChannelUsers
- AppTesters
- CrossDomainConnectors
- Deployers
- IntegrationAdministrators

Chosen:

- Administrators

Create a New Group

OK | Cancel

Group Properties

The following properties will be used to identify your new Group.

* Indicates required fields

What would you like to name your new Group?

* **Name:**

How would you like to describe the new Group?

Description:

Please choose a provider for the group.

Provider:

OK | Cancel

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=f953c555a27bc2b6274cdf214ba3fd1](http://modj.org/index.php?id=3&tx_ttnews[tt_news]=7&cHash=f953c555a27bc2b6274cdf214ba3fd1)
- **Middleware: a short classification**
[http://modj.org/index.php?id=3&tx_ttnews\[tt_news\]=6&cHash=2405bf47d8fb5efe87e291deb6135b93](http://modj.org/index.php?id=3&tx_ttnews[tt_news]=6&cHash=2405bf47d8fb5efe87e291deb6135b93)
- **Orchestration (computing):**
[http://en.wikipedia.org/wiki/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?

