ARS

Member of

TIMETOACT GROUP
SOFTWARE & CONSULTING

Java EE Security

Java EE Grundlagen

ARS

Inhalte dieses Kapitels

Maßnahmenbereiche

Arten der Zugriffskontrolle

Deklarative Zugriffskontrolle

Zusammenfassung

ARS

Maßnahmenbereiche [1|3]

Authentifizierung des Clients gegenüber dem Server

- Überprüfung der Identität des Benutzers
- JavaEE-Spezifikation fordert verschiedene Arten
  - HTTP Basic Authentifizierung (Default)
  - HTTP Digest Authentifizierung
  - Formular-basierte Authentifizierung
  - Authentifizierung über SSL (HTTPS)

Zugriffskontrolle auf Ressourcen (Webressourcen bzw. EJBs)

- Autorisierung der Benutzer für bestimmte Ressourcen
- Ist wesentlicher Bestandteil der JavaEE-Spezifikation
  - Servlet-Spezifikation und JSP-Spezifikation
  - EJB-Spezifikation

ARS

Maßnahmenbereiche [2|3]

Datenintegrität

- Ausgetauschte Daten dürfen nicht modifiziert werden
- Bestandteil der JavaEE-Spezifikation
- Application Server muss Mechanismen zur Sicherung der Datenintegrität bereitstellen

Vertraulichkeit der Daten

- Ausgetauschte Daten dürfen nicht eingesehen werden
- Bestandteil der JavaEE-Spezifikation
- Application Server muss Mechanismen zur Sicherung der Vertraulichkeit bereitstellen

ARS

Maßnahmenbereiche [3|3]

Verbindlichkeit bzw. Sicherung gegen Ableugnung

- Benutzer kann nicht ableugnen, dass bestimmte Aktionen ausgeführt wurden
- Ist ***kein*** expliziter Bestandteil der Java-EE-Spezifikation

Auditing

- Aufzeichnen von sicherheitsrelevanten Ereignissen
- Ist ***kein*** expliziter Bestandteil der Java-EE-Spezifikation

ARS

Arten der Zugriffskontrolle [1|3]

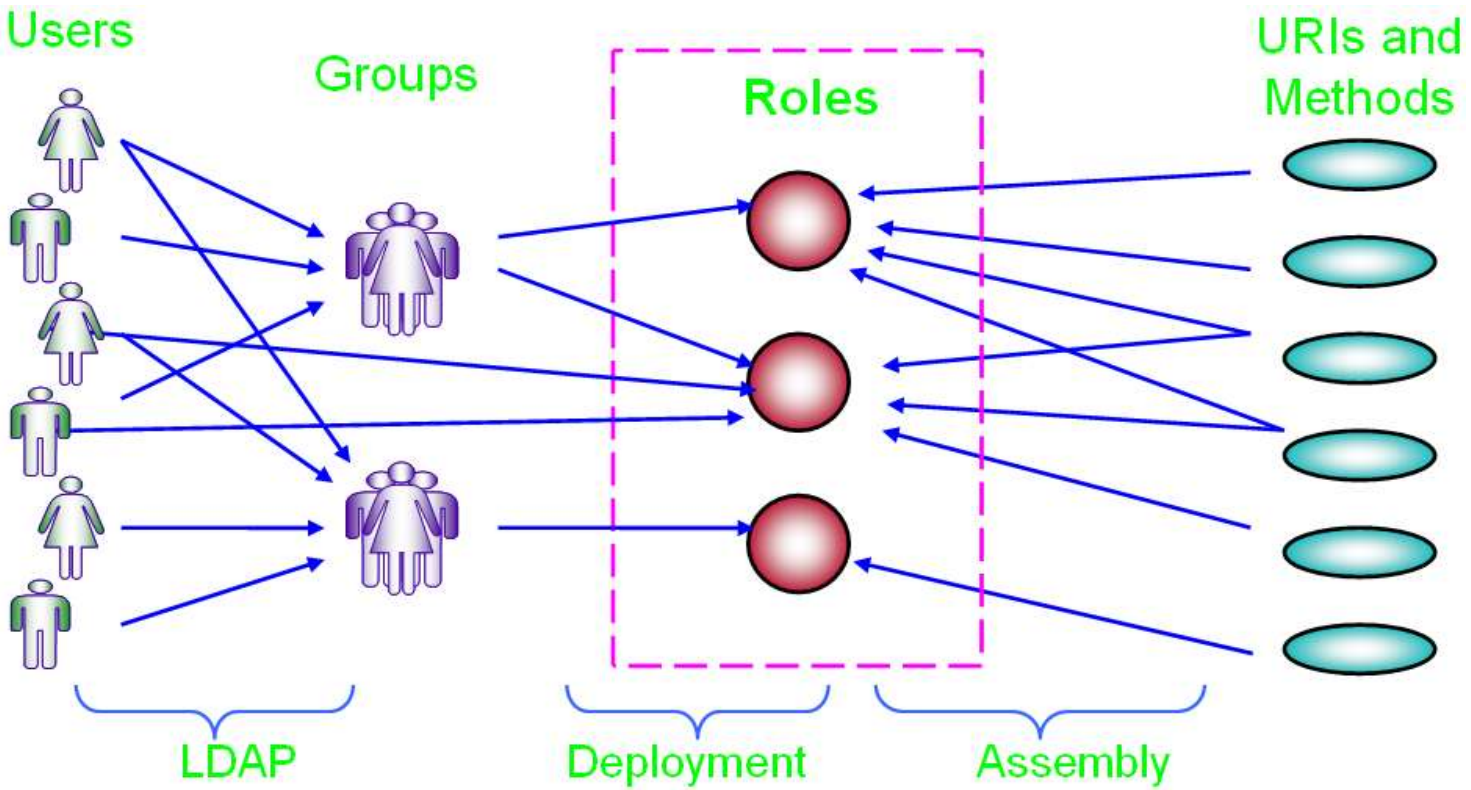
Deklarativ

- Bevorzugte Variante
- Wird per Annotation oder im Deployment Descriptor festgelegt
- Flexibel
  - In der Applikation werden logische Rollen und deren Zuordnung auf Ressourcen festgelegt
  - Logische Rollen entsprechen nicht direkt Benutzer oder Gruppen der Laufzeitumgebung
  - Logische Rollen werden erst bei Inbetriebnahme der Anwendung auf reale Benutzer oder Gruppen abgebildet
  - Änderungen in den Sicherheitsberechtigungen erfordern in der Regel keine Anpassung im Quelltext

ARS

Arten der Zugriffskontrolle [2|3]

Logische Rollen



ARS

Arten der Zugriffskontrolle [3|3]

Programmatisch

- Implementierung explizit im Quellcode
- Bestimmte Methoden in der Servlet- bzw. EJB-API
  - Methoden der Klasse `HttpServletRequest`
    - `isUserInRole()`
    - `getUserPrincipal()`
  - Methoden der Klasse EJBContext
    - `isCallerInRole()`
    - `getCallerPrincipal()`
- Verwendung als Ausnahme
  - Tageszeitabhängige Rechtevergabe
  - Zugriff abhängig vom Zustand der Anwendung
  - Zugriff abhängig von Methodenparametern

ARS

Deklarative Zugriffskontrolle [1|3]

Festlegung der Zugriffskontrolle im Deployment Deskriptor

- Webkomponenten: Datei `web.xml`
  - Sicherheitsrollen (*Security Roles*)
  - Sicherheitsvorgaben (*Security Constraints*)
    - Webressourcensammlung
    - Zugriffsbeschränkung
    - Transportgarantie
  - Art der Authentifizierung
- EJBs: Datei `ejb-jar.xml`
  - Sicherheitsrollen (*Security Roles*)
  - Zugriffsschutz für EJB-Methoden (*Method Permissions*)
  - Aufrufidentität (*Security Identity*)
- Java-EE-Applikation: Datei `application.xml`
  - Sicherheitsrollen zum Mapping am Zielserver

ARS

Deklarative Zugriffskontrolle [2|3]

Festlegung der Zugriffskontrolle per Annotation

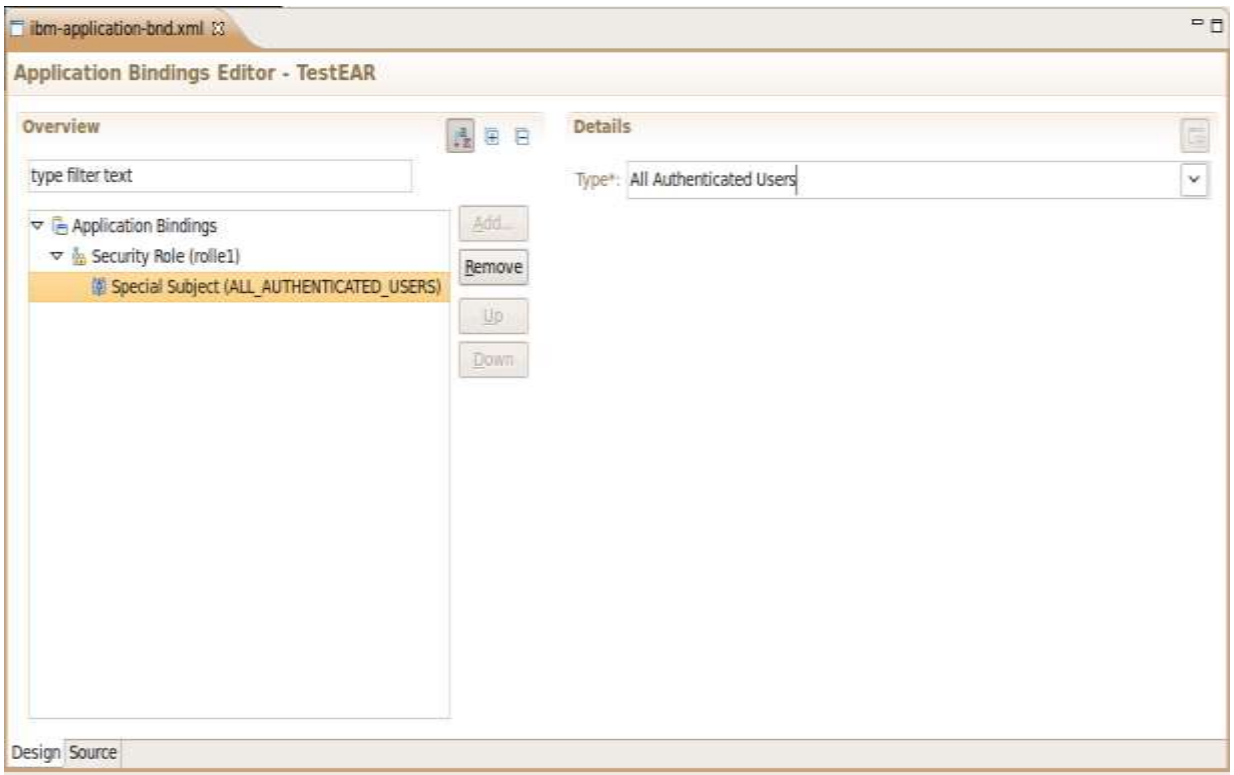
- **`@RolesAllowed`**
  - Kann auf Klassen- oder Methoden-Ebene angewendet werden
  - Durch Angabe eines String-Arrays werden die zugriffsberechtigten Rollen aufgeführt
- **`@PermitAll`**
  - Ist der Standardwert, d.h. grundsätzlich erfolgt keine Berechtigungsprüfung
  - Kann auf Klassen- oder Methoden-Ebene angewendet werden
- **`@RunAs`**
  - Gibt eine Rolle an, mit der diese Methode oder EJB ausgeführt wird
- **`@DeclareRoles`**
  - String-Array zur Definition von Rollen-Referenzen
  - Wird verwendet bei programmatischer Sicherheit (`SessionContext.isCallerInRole()`)

ARS

Deklarative Zugriffskontrolle [3|3]

Maaping am Beispiel Websphere Application Server

- Bei Installation des EARs am Server
- Während Entwicklung über Pre-Deployment Descriptor
  - Zuordnung der Benutzer und Benutzergruppen
  - Spezielle WAS-Benutzergruppen
    - Alle Benutzer des Systems (`Everyone`)
    - Alle erfolgreich authentifizierten Benutzer (`All authenticated users`)
  - Abbildung der Sicherheits-rollen wird in der Datei `ibm-application-bnd.xml` abgelegt



ARS

Kontrollfragen

- Was ist der Unterschied für Datenvertraulichkeit und –integrität?
- Für welche Beispiele aus dem praktischen Leben sind diese Anforderungen besonders wichtig?
- Warum werden Benutzer und Benutzergruppen nicht direkt auf Ressourcen der Applikation gemappt, sondern Rollen verwendet?
- Wo und in welcher Form können Sicherheitseinstellungen in Web-/EJB-Modulen vorgenommen werden?