UNIVERSITÄT
DUISBURG
ESSEN

ZIM
Zentrum für Informations- und Mediendienste

Gruppenverwaltung mit “Grouper” an der Universität Duisburg - Essen

Burkhard.Wald@Uni-DuE.de

Februar 2010

Gruppen ...

- entstehen aus ...
  - Organisationsstruktur
  - Personenstatus
  - Arbeitskreise
  - Arbeitsaufträge
- sollen münden in ...
  - Berechtigungen
  - Berücksichtigungen

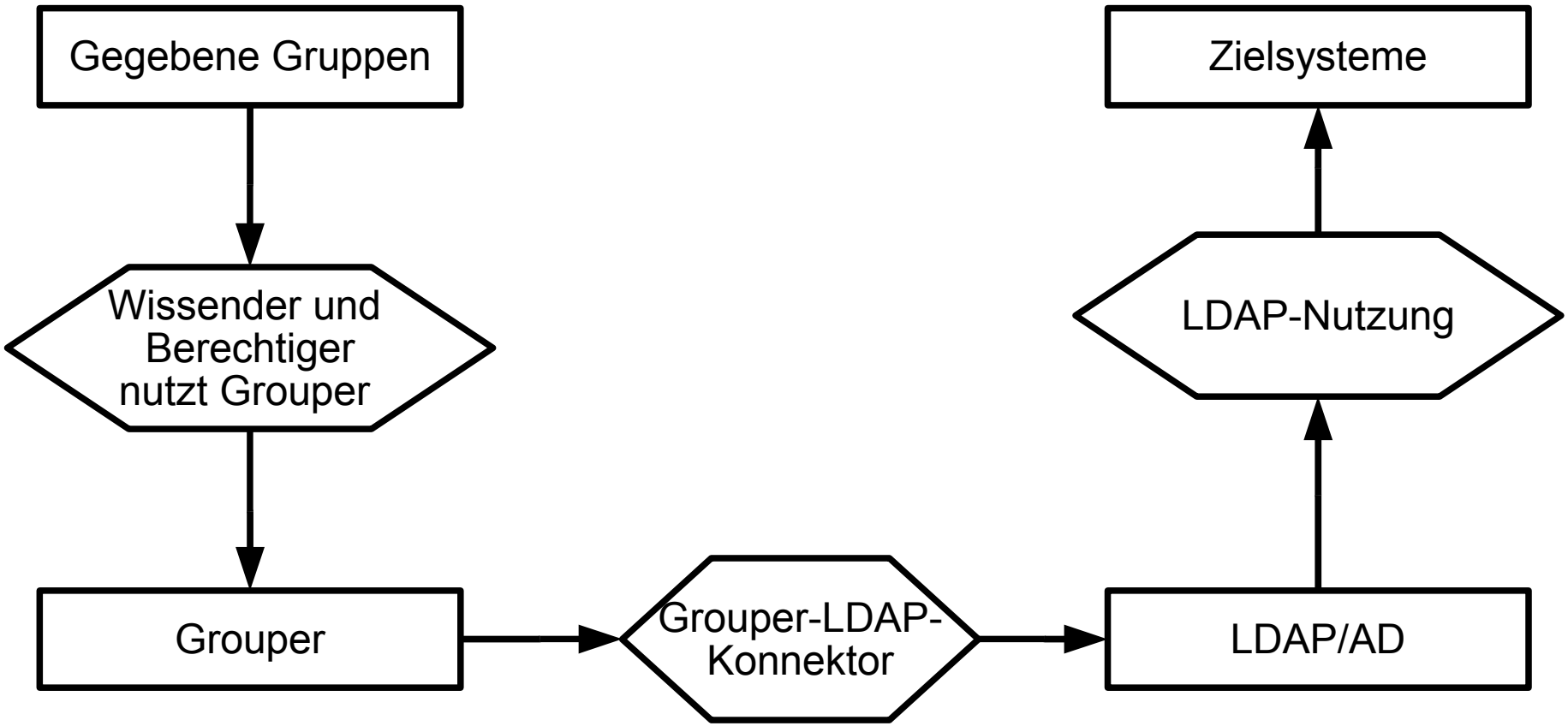
Gruppen verwalten

- Idealer Weise werden Gruppen in den Quellsystemen verwaltet
  - Das Identitätsmanagement die Information nur an die Zielsysteme weiter oder wertet Sie selbst aus.
- In der Realität entstehen relevante Gruppen aber vor Ort
- Gruppen müssen daher vor Ort verwaltet werden können.

Aufgaben

- Gruppenzugehörigkeiten
  - erfassen
  - speichern
  - zur Verfügung stellen
  - konsumieren

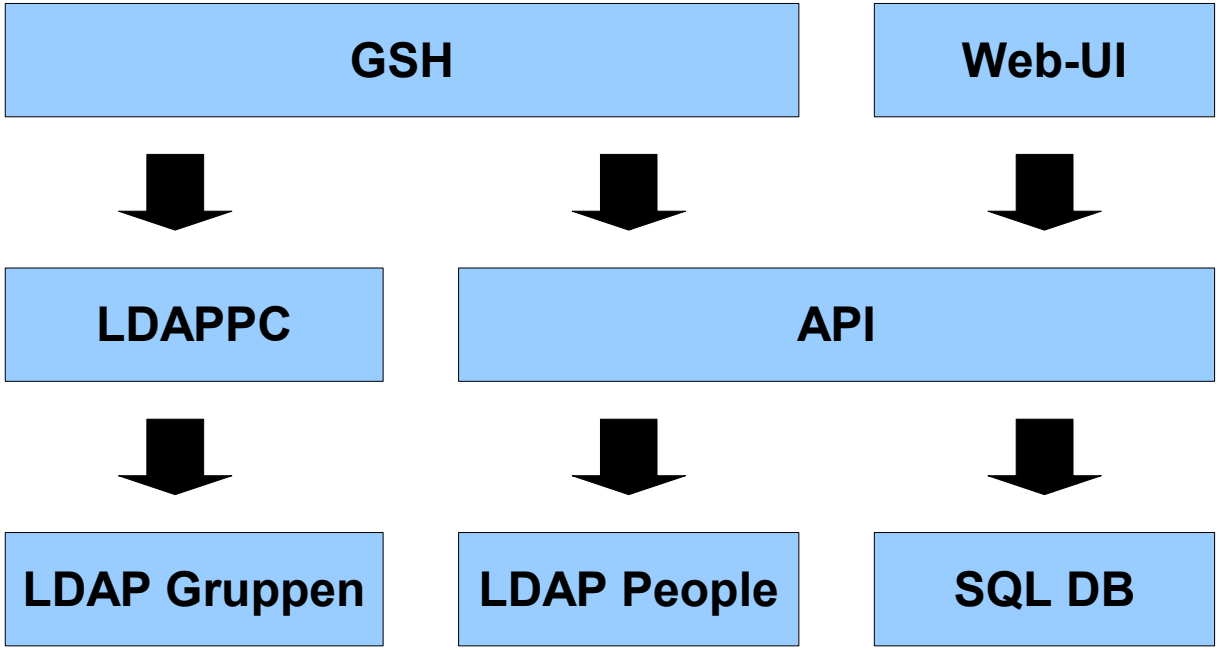
Informationsfluss



Grouper ist ...

- http://www.internet2.edu/grouper/
- Komponenten
  - Benutzt eine gegebene Quelle mit Personenobjekten (ldap oder jdbc)
  - SQL-Datenbank (Hibernate)
  - J2EE-UI (Tomcat-Anwendung)
  - Groupershell (gsh)
  - LDAP-Provisionierungskonnektor (ldappc)

Grouper Architektur



Grouper-Installation

- Build mit ant
- grouper.properties
- grouper.hibernate.properties
  - Zugang zur SQL-Datenbank
- sources.xml
  - Definition der Personenquelle (LDAP oder SQL)
  - Suchfilter oder SQL-Statements
  - Personenobjekt-ID
  - Display-Attribut für Personen (z.B. die Mailadresse)
- War-File in Tomcat deployen

LDAP-Provisioning-Connector (LDAPPC)

- ou für Grouper-Gruppen anlegen
- Objektklasse eduMember
- DNs der Mitglieder im Attribute member
- LDAP-Admin-Account für die Gruppen
- ldappc.xml
- bushy oder flat

Grouper-Konzepte

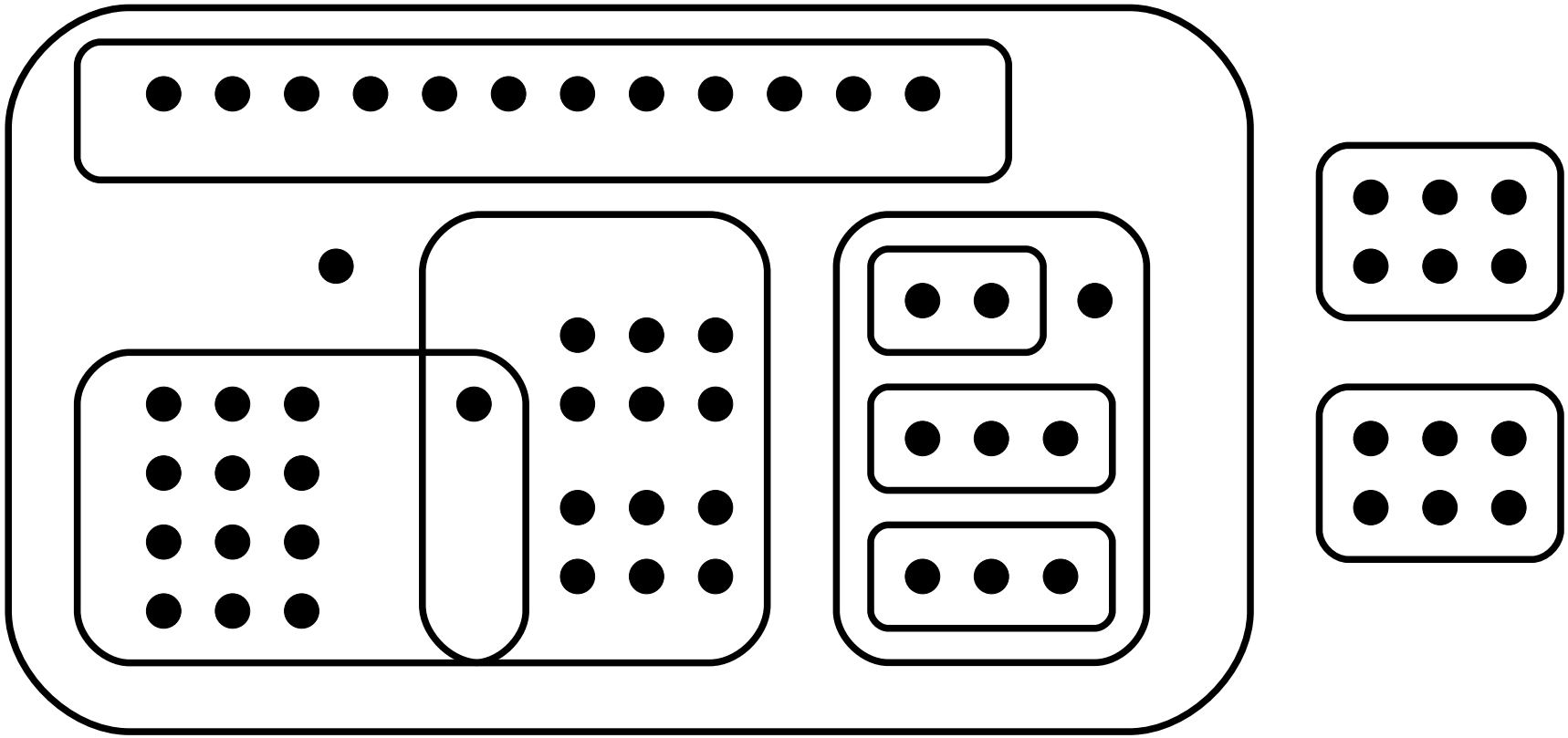
- Ordnerhierachie
- Gruppen
- Pfade (z.B. zim:systems:xymon)
- Displaynamen versus IDs
- Privilegien
  - Mitglied, Admin, Read, View, OptOn, OptOut
- Gruppenschachtelung (indirekte Mitgliedschaft)
- Alle Gruppen und Privilegien einer Person anzeigen

Konsumieren von Gruppen

- Zugriff auf einen Web-Bereich
- Zugriff auf eine Web-Anwendung
- Mitgliedschaft in einer AD-Gruppe
  - Zugriffsrechte im Filesystem
- Mailverteiler
  - Gruppenforward
  - Mailingliste

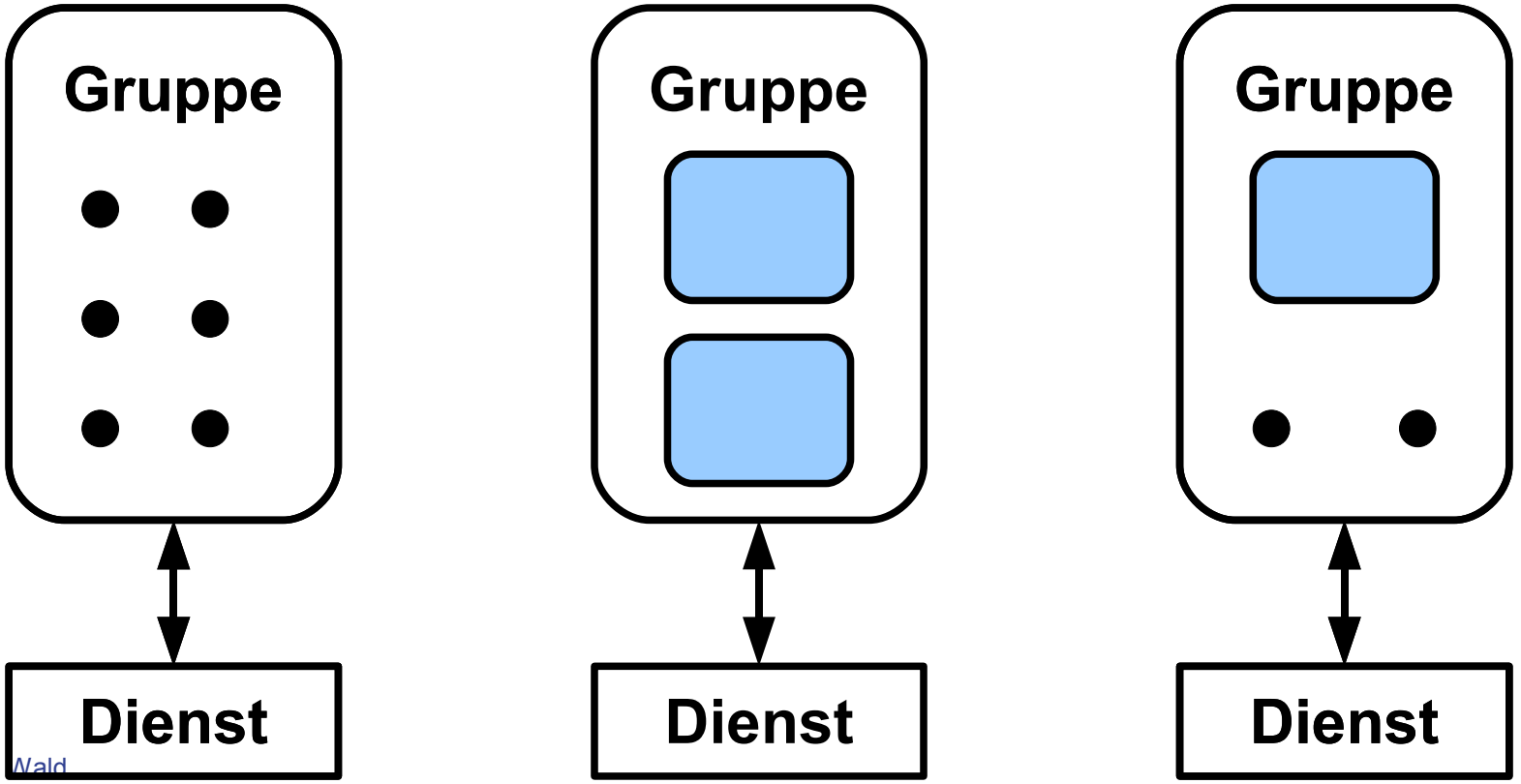
Organisationsstruktur einer Einrichtung als Gruppenstruktur

Alle Gruppen liegen flach in einem Ordner nebeneinander



Nutzungsbezogene Gruppen

Mitglieder sind Einzelpersonen oder Personalgruppen



Ordnerstruktur in Grouper

- 1. Ebene: Ein Ordner pro Einrichtung
- 2. Ebene: Administrationsstruktur innerhalb der Einrichtung
  - Ordner: Personal
    - Organisationsstruktur als Gruppen
    - Standortstruktur als Gruppen
  - Ordner: Zielsysteme
    - Allgemeine Zugänge und Verteiler
    - Adminzugänge und Verteiler
  - Ordner: Arbeitsgruppen

Zentrale Gruppen

- Allgemein
  - Gruppe W: Wheel-Group (Grouper-Konzept)
  - Gruppe G: Grouper-Zugang
  - Gruppe T: Zugang zu Tomcat-Manager
- Pro Einrichtung
  - Gruppe A: Administration (fast) aller Gruppen der Einr.
  - Gruppe L: Leserecht an allen Gruppen der Einr.
  - Gruppe Z: Grouper-Zugang aus der Einr.
  - „Z=L“ ?
  - (Neue Gruppen entsprechend einrichten)

Was wir nicht machen

- Jeder kann sich in Grouper einloggen
- OptIn/OptOut-Konzept nutzen
- Laden von Gruppen und Rollen aus anderen Quellen

Was wir uns vorgenommen haben

- Auditing mit neuer Version
- Shibboleth oder CAS-Authentisierung

Achtung

- Die Nutzung der durch Grouper verwalteten Gruppen spiegelt sich nicht wirklich in Grouper wieder.
  - Zusätzliche Dokumentation ist erforderlich
- Löschen von LDAP-Personen-Objekten führt in Grouper zu Fehler, wenn Sie noch zu Gruppen gehören.
  - LDAP-Löschvorgang muss mit Fehlermeldung abbrechen.

Einladung zum Nachmachen

- Strukturierungs- und Adminkonzept
- Konfigurationsdateien
- Eindeutschung
- Handout für Sekretariat
- Ein paar kleine Skripte