

# Von der Datenbank zum LDAP-Server schnell und einfach mit Oracle Virtual Directory

DOAG 2014 - Konferenz Nürnberg 18.-20.11.2014

**Hans-Ulrich Beres**  
Rechenzentrum der RUB  
Hans-Ulrich.Beres@rub.de

**Suvad Sahovic**  
Oracle Corporation  
Suvad.Sahovic@oracle.com

# Agenda

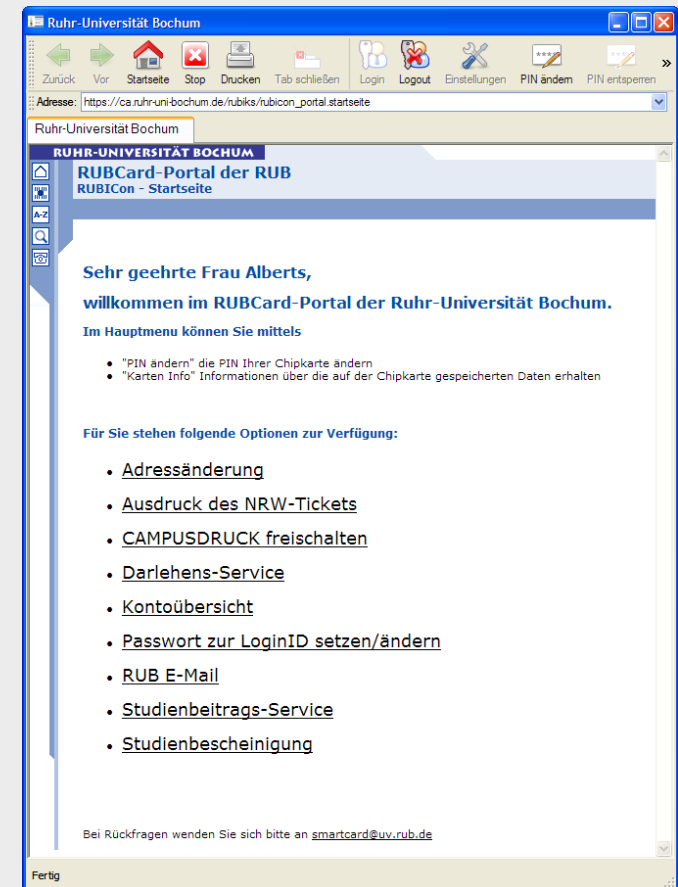
- Ausgangslage und Anforderungen
- Lösung und Optimierungen
- Fragen

# Ruhr-Universität Bochum

- 41.000 Studierende in
  - 150 Studiengängen
- 5.600 Beschäftigte in
  - 20 Fakultäten
  - 10 Zentralen  
wiss. Einrichtungen
  - 7 An-Instituten

# RUBiKS (RUB integrierter KundenService)

- Verwaltung von 90.000 Identitäten
  - Studierende, Bedienstete, Gäste, Ehemalige
  - Veranstaltungs-Accounts
  - Temporäre Accounts
- 150 Online-Dienstleistungen
  - Single Sign On
  - RUBCard (Studierende, Bedienstete, Gäste)



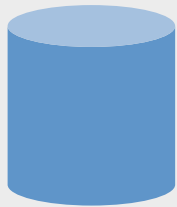
# RUBiKS Verzeichnisdienste

- Active Directory
  - ruhr-uni-bochum.de
  - wird stündlich mittels perl-script provisioniert
  - Passwortänderungen online
  
- LDAP
  - dc=ruhr-uni-bochum,dc=de
  - Oracle Virtual Directory
  
- Datenquelle ist immer RUBiKS
  - AD und LDAP nur lesend

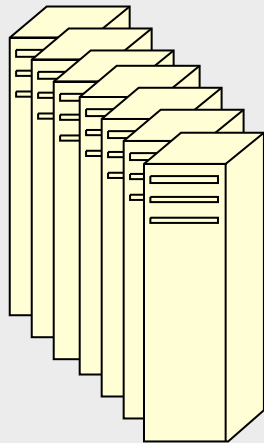
# RUBiKS Online-Dienstleistungen

- Mehrere Mailserver mit insgesamt 60.000 Mailboxen
- Radius-Server zur Verwaltung der Internetzugänge
  - aus den Studentenwohnheimen
  - von HIRN-Ports (hochschulinternes Rechnernetz)
  - über WLAN (eduroam)
  - über VPN
- Shibboleth-Server
- diverse Unix-Server mit speziellen Berechtigungen
  - eigene LDAP-Gruppen (Verwaltung über Web-Formular)

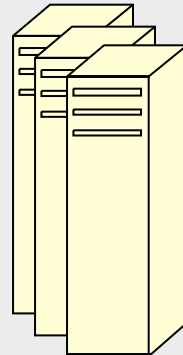
# Systemlandschaft



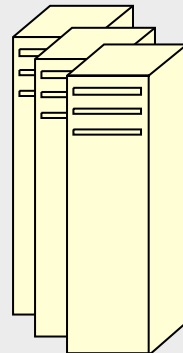
Dell  
Compellent  
SSD, 15k,  
7.2k



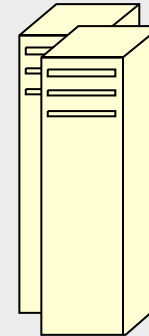
7-Knoten  
RAC  
11gR2



3 Application-  
Server



3 LDAP-  
Server



2 Load-Balancer für  
Application-  
und LDAP-Server



# Ausgangslage

- LDAP-Server mit Oracle Internet Directory (OID)
- Daten in lokaler Datenbank
- Pflege mit DBMS\_LDAP-Paket
- Nachteil:
  - DBMS\_LDAP ist langsam
  - hoher Pflegeaufwand
  - Inkonsistenzen zwischen RUBiKS und LDAP



# Anforderungen

- geringer Pflegeaufwand
- performant / skalierbar
- Vermeidung von Inkonsistenzen

# Lösung

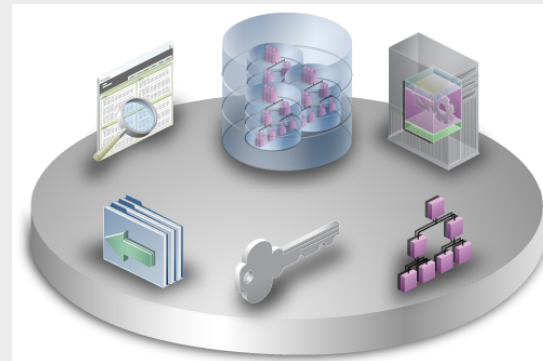
- geringer Pflegeaufwand
- performant / skalierbar
- Vermeidung von Inkonsistenzen



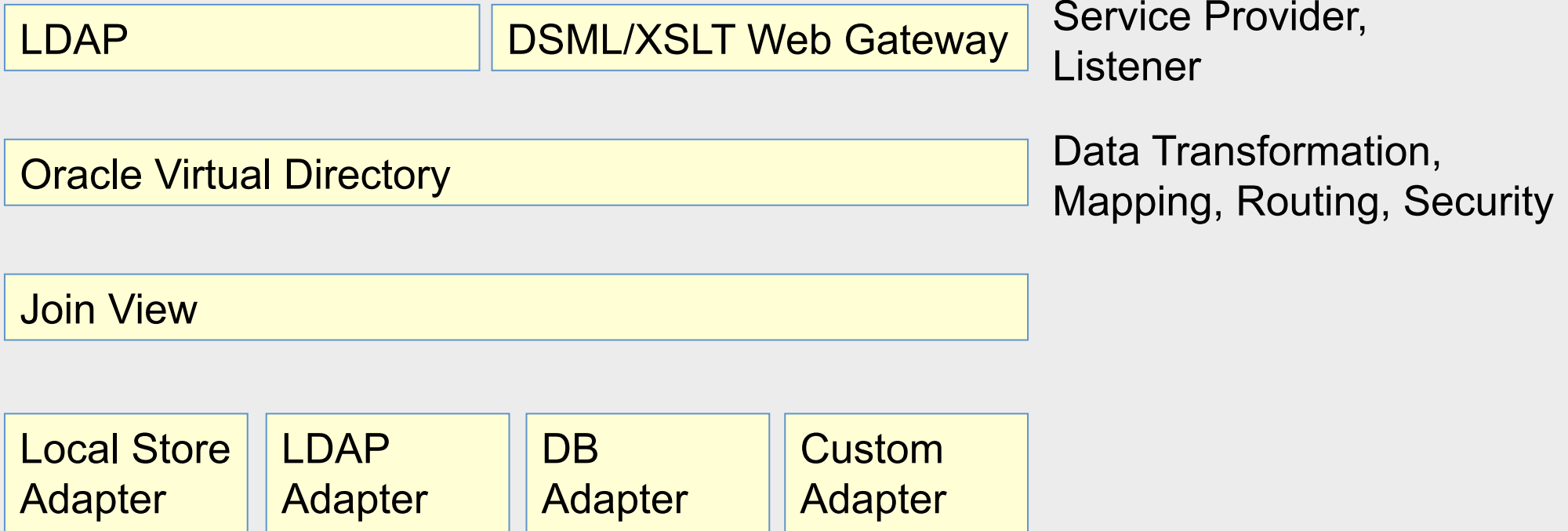
nur konfigurieren – sehr wenig Pflege

Parallelinstallation über Loadbalancer

Zugriff auf Originaldaten – keine Synchronisation



# Architektur von OVD

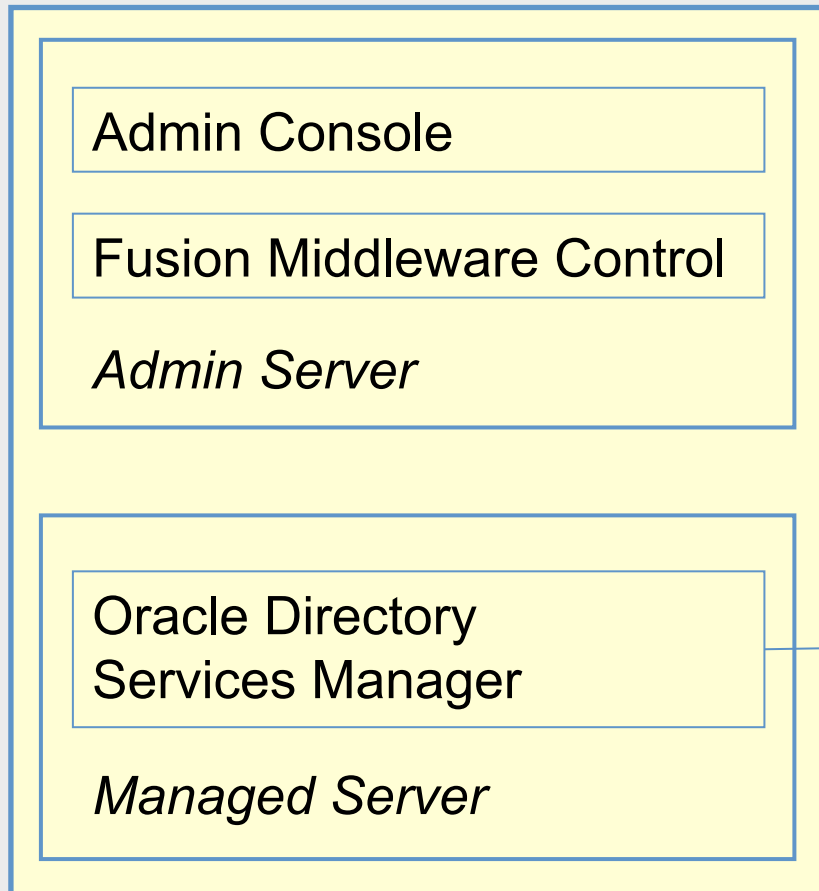


# Erweiterung von OVD

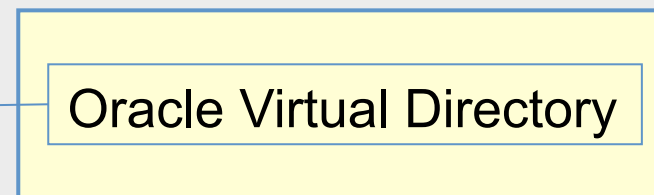
- Die Adapter lassen sich durch java-plugins erweitern, z.B.
  - für eine eigene Passwort-Verschlüsselung (bind)
  - zur Verwaltung von Passwortfehlern (bind)
    - globale Zählung, Account Lock/Unlock in RUBiKS-DB schreiben
  - für temporäre Accounts
    - Erstnutzung in RUBiKS-DB zurückschreiben
  - Manipulation von Search-Filtern (get)

# Installation von OVD

Oracle Weblogic Server Domain

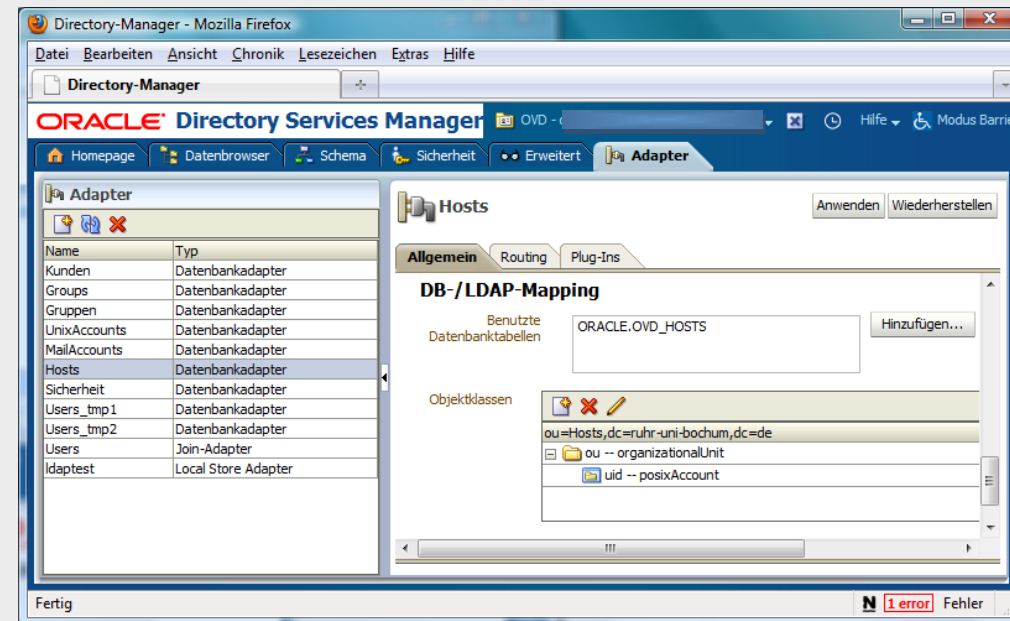


Oracle Virtual Directory Instance



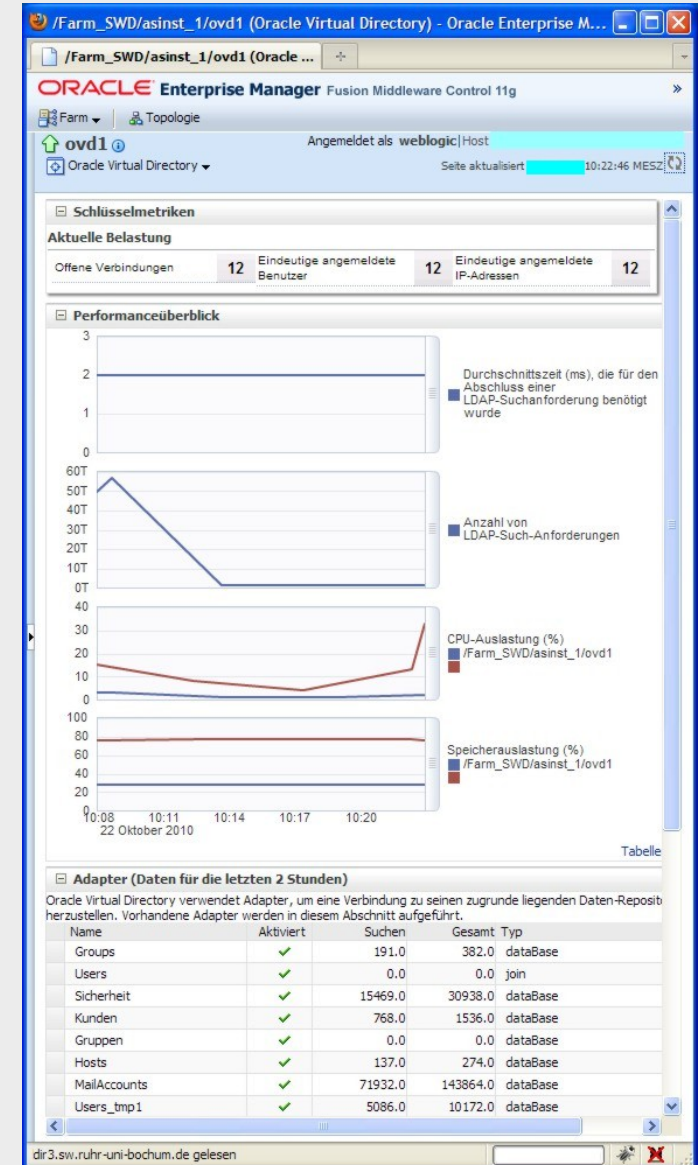
# Konfiguration von OVD

- eigene Objektklassen und Attribute
- Definition von Adaptern
- Attribut-Mapping
- dynamische Unterstrukturen
- Access-Control-Listen
- schreibender LDAP-Zugriff
- mehrstufiges Logging



# Optimierungen von OVD

- Listener mit **50** Threads (default 10)
- Materialized Views
- ... in lokaler Datenbank
- function-based Indizes: upper(<Spaltenname>)
- mehrere OVD-Server parallel



# Vielen Dank für Ihre Aufmerksamkeit



- Fragen
  
  
- Weitere Informationen:
  - email: [Hans-Ulrich.Beres@rub.de](mailto:Hans-Ulrich.Beres@rub.de)
  - email: [Suvad.Sahovic@oracle.com](mailto:Suvad.Sahovic@oracle.com)