

RUHR-UNIVERSITÄT BOCHUM

Zentrale Authentifizierungsdienste an der RUB

Herbsttreffen zki AK Verzeichnisdienste 09.10.2012

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

Agenda

- Identity-Management-System RUBiKS
- Active Directory
- LDAP
- Fragen

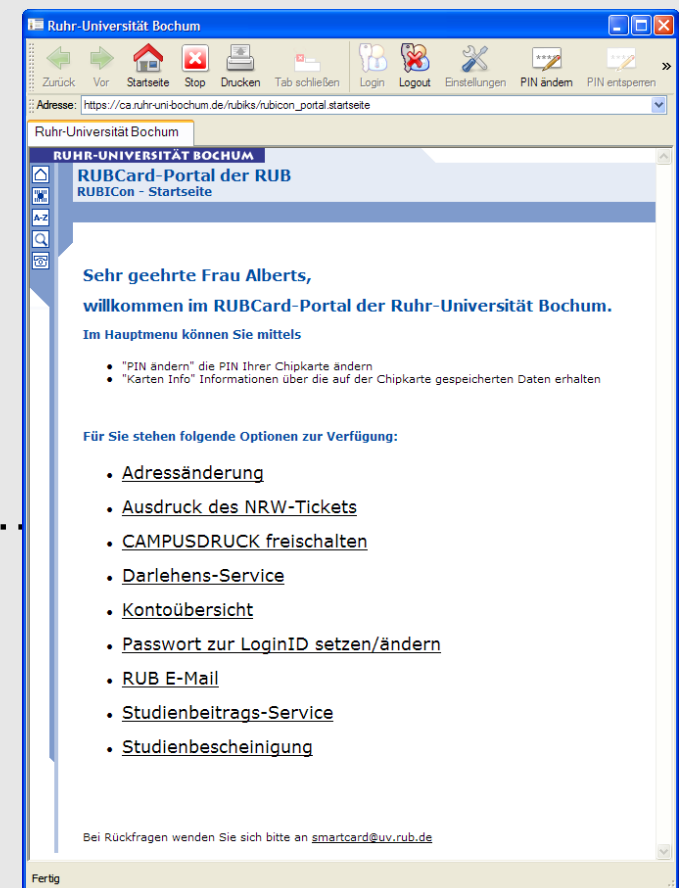
Ruhr-Universität Bochum

- 37.000 Studierende in
 - 150 Studiengängen
- 5.200 Beschäftigte in
 - 20 Fakultäten
 - 10 zentralen wiss. Einrichtungen
 - 7 An-Instituten



RUBiKS (RUB integrierter KundenService)

- Verwaltung von 70.000 Identitäten
 - Studierende, Beschäftigte, Ehemalige
 - Veranstaltungs- / temporäre Accounts
- 150 Online-Dienstleistungen
 - Single Sign On
 - Email, Internet-Zugang, Prüfungsverwaltung, ...
 - RUBCard (Studierende, Bedienstete, Gäste)



RUBiKS - Geburtstag (2008)



RUBiKS - Rollen

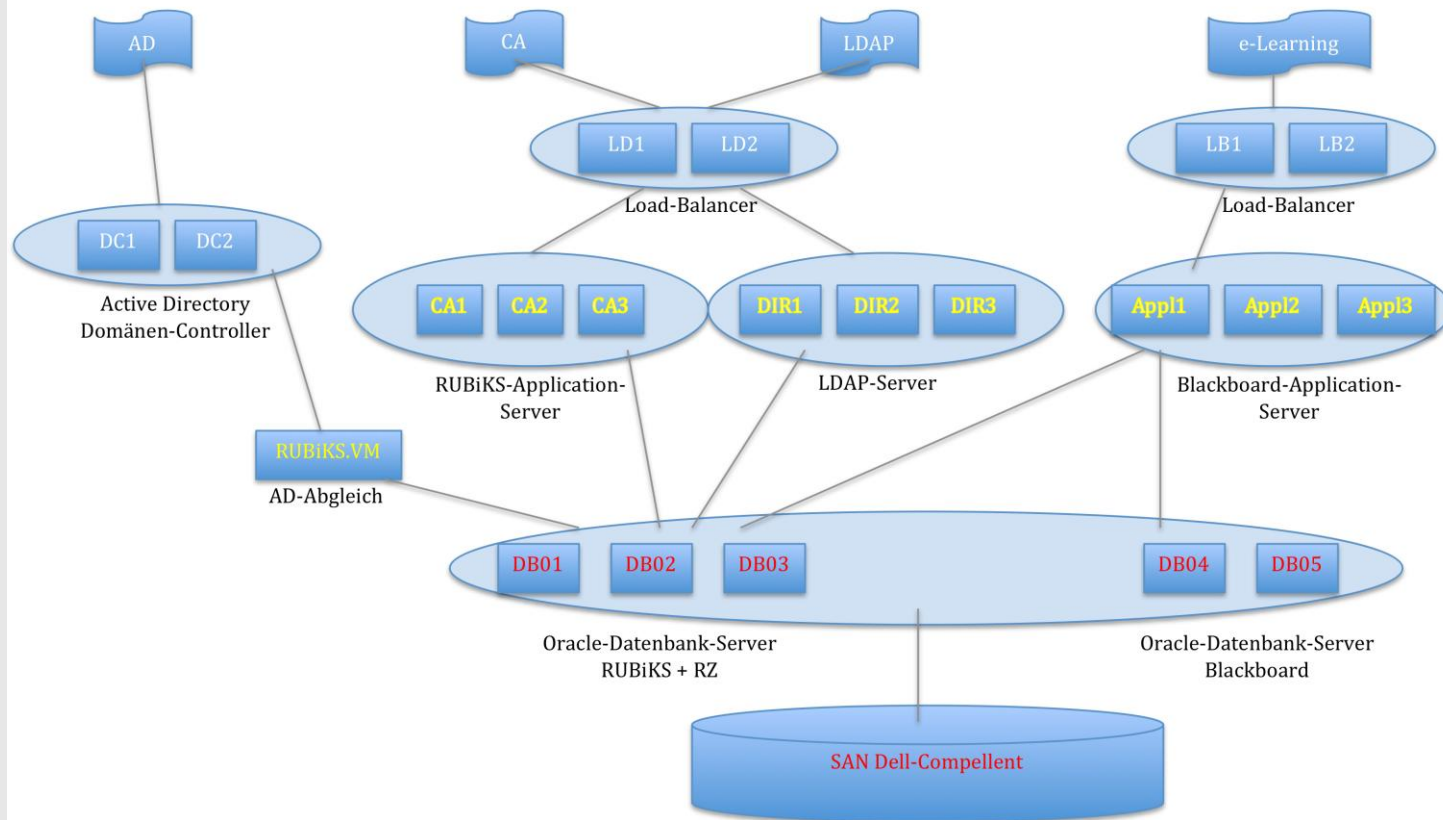
staff	Mitarbeiter
student	Studierende
student guest	Gaststudenten
auditor	Zweithörer
affiliate	Beschäftigter ohne Festvertrag
alum	Ehemalige
retired	Pensionäre
Sprachschueler	Sprachschüler
externe	Externe
library-walk-in	externe Bibliotheksnutzer
kombi	Kombidienste
Nrwwissweb	Wissenschaftsnetz NRW
Tmpaccount	temporäre Accounts
Veranstaccount	Veranstaltungsaccounts
Fileshare	Nutzer von Fileshare

RUBiKS – Rollen und Dienste

Rolle	eMail	CIP	Homep.	VPN	HIRN	WLAN
staff	Ja	Ja	Ja	Ja	Ja	Ja
student	Ja	Ja	Ja	Ja	Ja	Ja
affiliate	Ja	Ja	Ja	Ja	Ja	Ja
alum	Ja	Nein	Nein	Nein	Ja	Ja
library-walk-in	Nein	Nein	Nein	Nein	Nein	Nein
kombi	Ja	Nein	Ja	Nein	Nein	Nein
auditor	Ja	Ja	Ja	Ja	Ja	Ja
student guest	Ja	Ja	Ja	Ja	Ja	Ja
nrwwissweb	Nein	Nein	Nein	Nein	Ja	Ja
tmpaccount	Nein	Nein	Nein	Nein	Ja	Ja
veranstaccount	Nein	Ja	Nein	Nein	Ja	Ja
sprachschueler	Ja	Ja	Nein	Nein	Nein	Nein
externe	Nein	Nein	Nein	Nein	Ja	Ja
fileshare	Nein	Nein	Nein	Ja	Ja	Ja
retired	Ja	Ja	Ja	Ja	Ja	Ja

RUBiKS - Technik

RUBiKS Upgrade 18.02.2012




Legende:
rote Beschriftung = Hardware + Software erneuert
gelbe Beschriftung = Software-Anpassungen

3 * 140 GB SSD
10 * 600 GB SAS (15.000 rpm)
6 * 2000 GB SAS (7.200 rpm)
= 18,4 TB (davon 9 TB für virtuelle Desktops)

Active Directory und LDAP-Server

- enthalten alle aktiven RUBiKS-Nutzer
- mit eventuellen Gruppenzugehörigkeiten (Administration über Web-Interface)
- nur lesender Zugriff
- gemeinsame Datenquelle ist RUBiKS-Datenbank

Active Directory und LDAP-Gruppen




RUHR-UNIVERSITÄT BOCHUM

RUBiKS

Identity Management

A-Z | ÜBERSICHT | SUCHE | KONTAKT



RUB » Das Rechenzentrum » RUBiKS

Administration der ldap/AD Gruppe: rz (Rechenzentrum)

☐ Nutzer hinzufügen

☐ Nutzer entfernen

☐ Vorhandene Nutzer anzeigen

☐ Administratoren anzeigen

☐ Administratoren hinzufügen

☐ Administratoren entfernen

Weiter

Reset

[Excel-Export](#)

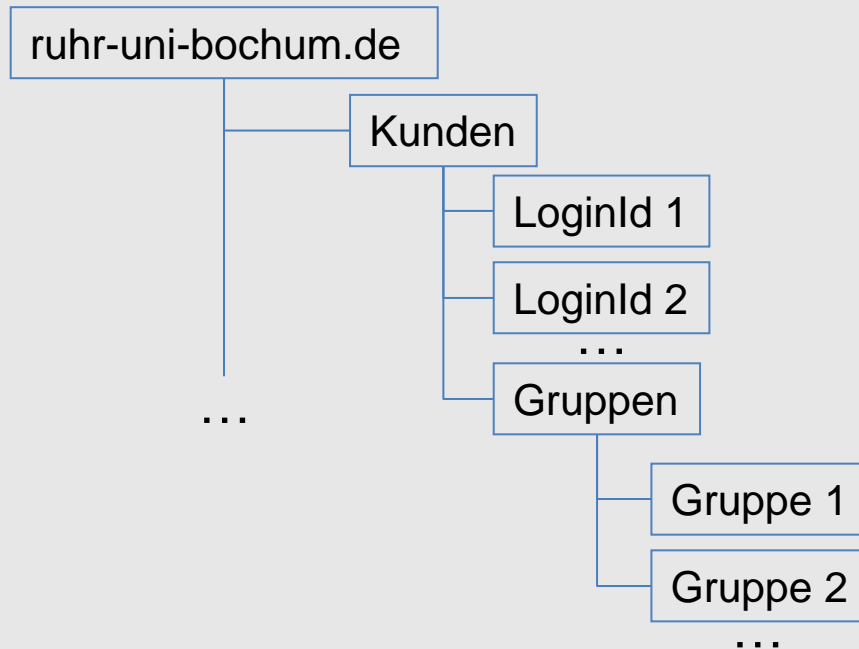
[zurück](#)

Impressum | Bei Rückfragen wenden Sie sich bitte an dba@rub.de

Active Directory - Übersicht

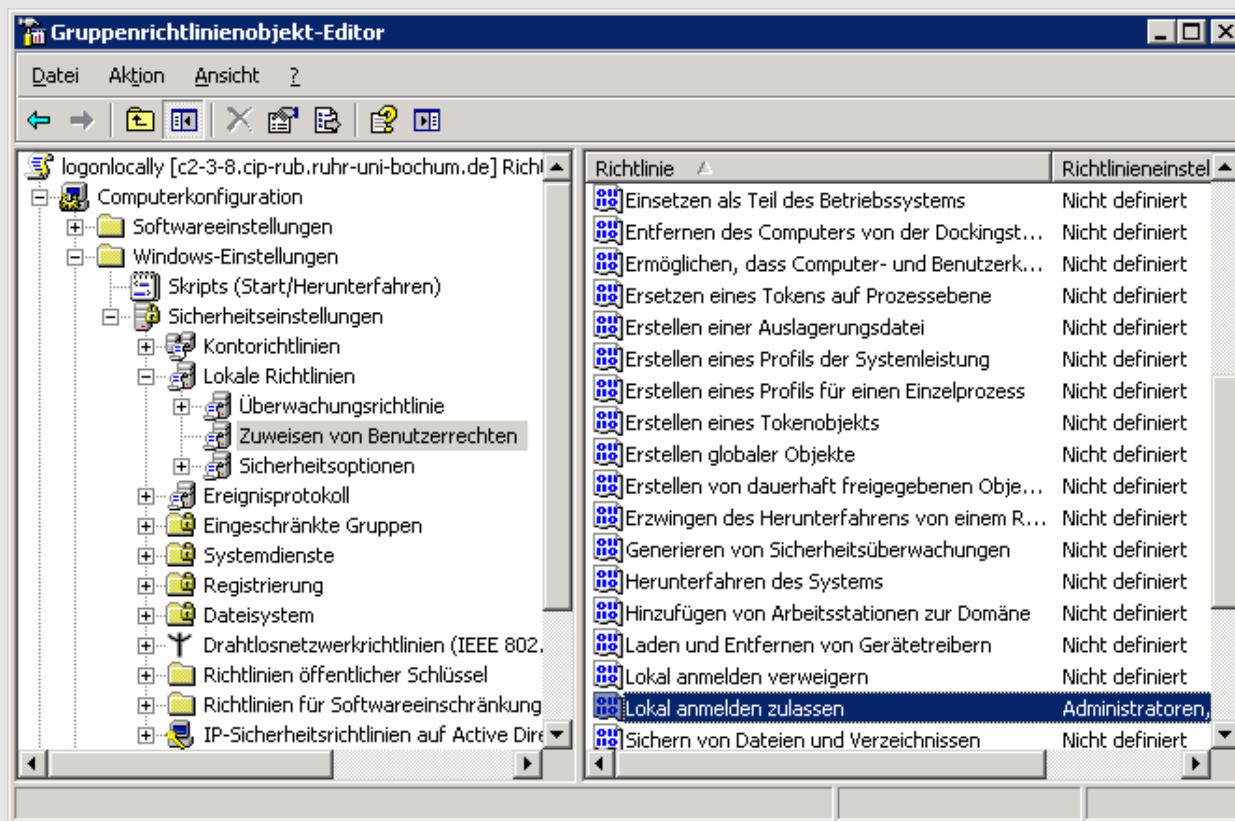
- Verzeichnisdienst von Microsoft Windows Server
- Aktualisierung jede Stunde
- Passwortänderungen sofort wirksam
- Auch bei RUBiKS-Ausfall verfügbar
- Hardware: 2 Domänencontroller

Active Directory - Struktur



Active Directory - Nutzung

■ Nutzung für Windows-Anmeldung



LDAP - 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

LDAP - Anforderungen

- geringer Pflegeaufwand
- performant / skalierbar
- Vermeidung von Inkonsistenzen

LDAP - Lösung

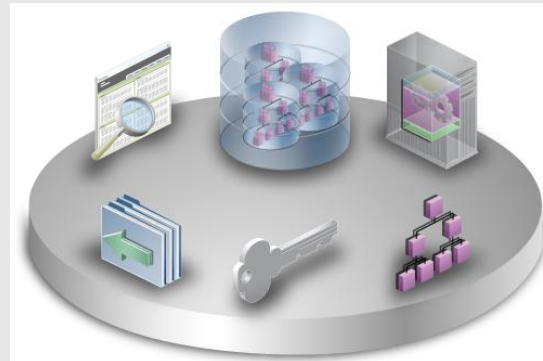


- geringer Pflegeaufwand
- performant / skalierbar
- Vermeidung von Inkonsistenzen

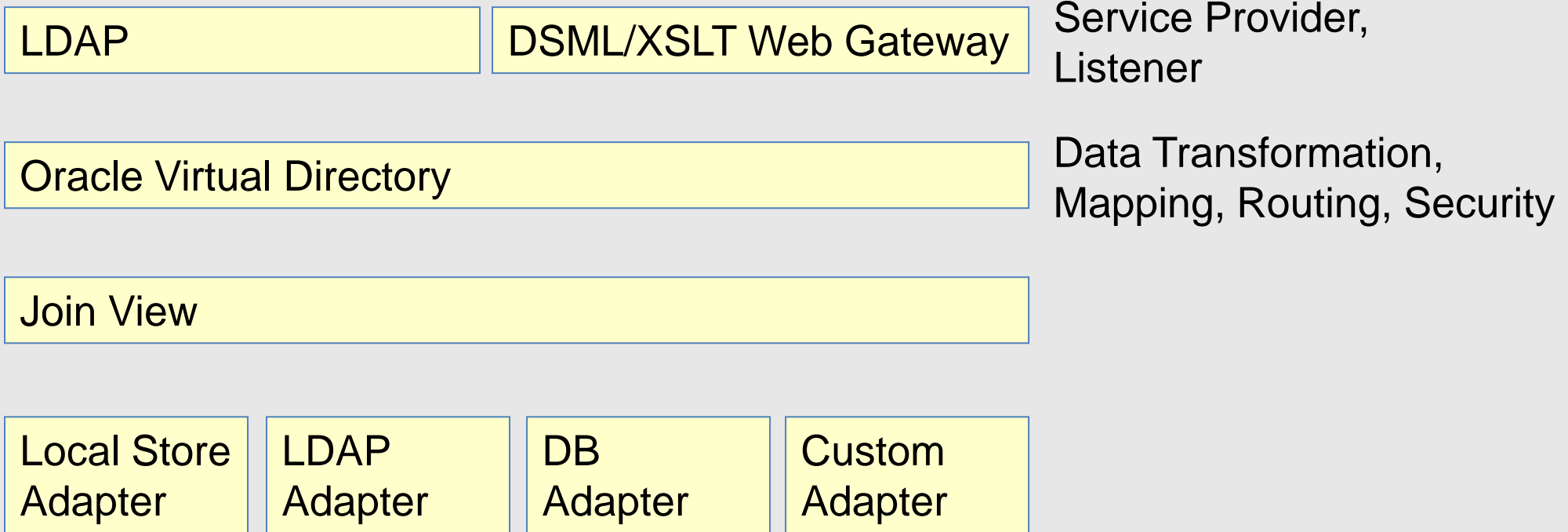
nur konfigurieren – sehr wenig Pflege

Parallelinstallation über Loadbalancer

Zugriff auf Originaldaten – keine Synchronisation



LDAP - Architektur von OVD

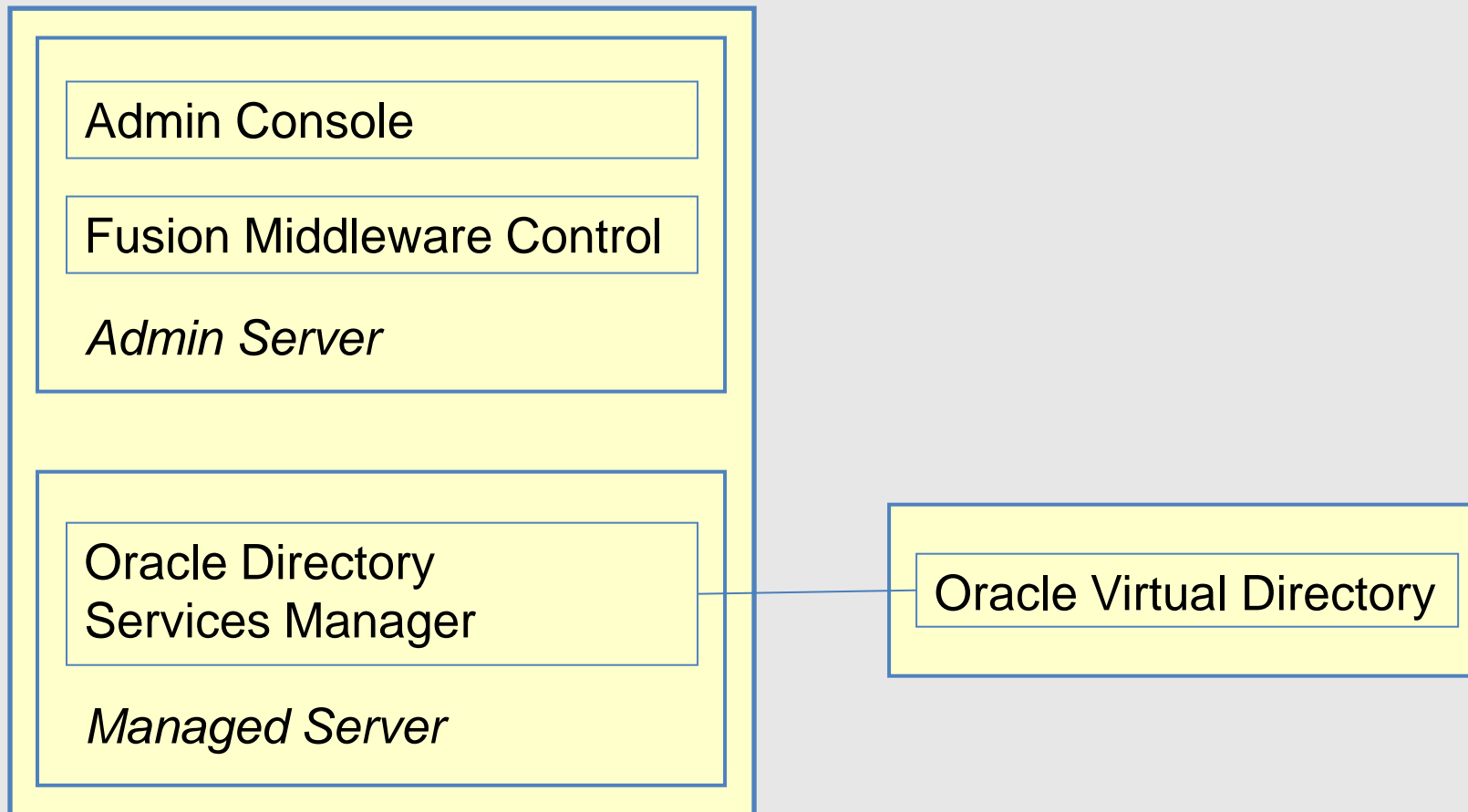


Die Adapter lassen sich durch java-plugins erweitern

LDAP - Installation von OVD

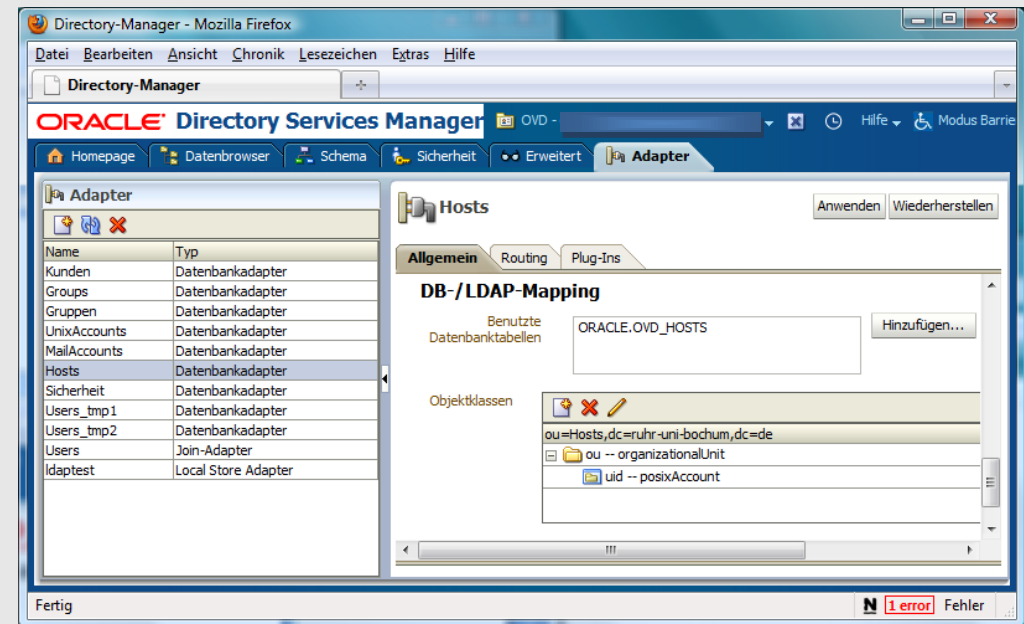
Oracle Weblogic Server Domain

Oracle Virtual Directory Instance



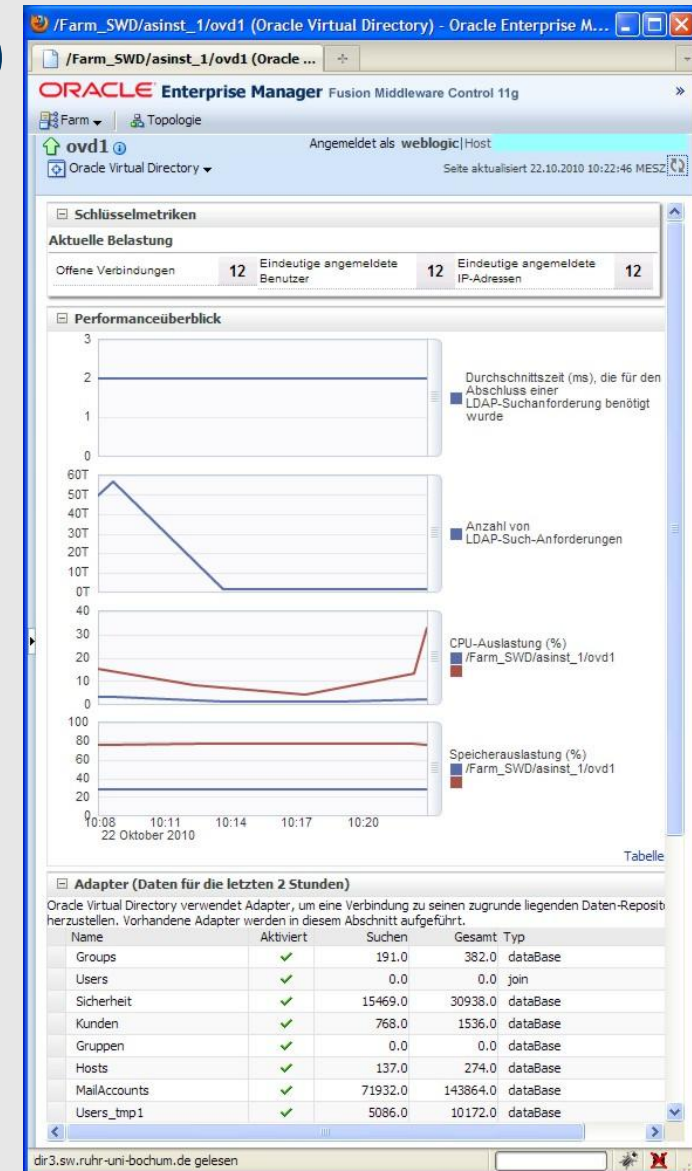
LDAP - Konfiguration von OVD

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



LDAP - Optimierungen von OVD

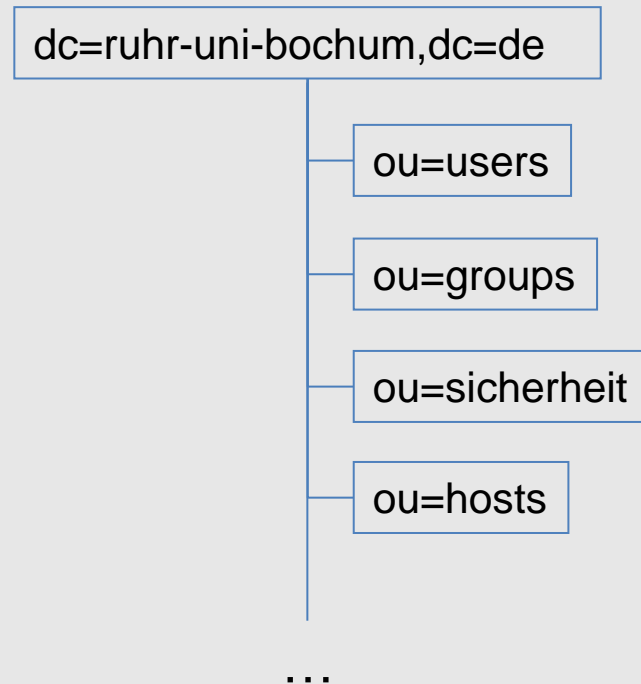
- Listener mit **50** Threads (default 10)
- Materialized Views
- ... in lokaler Datenbank
- function-based Indizes: upper(<Spaltenname>)
- mehrere OVD-Server parallel



LDAP-Server - Übersicht

- LDAP-Server mit Oracle Virtual Directory (OVD)
- Aktualisierung alle 10 Minuten
- Daten in lokaler Datenbank
- auch bei RUBiKS-Ausfall verfügbar
- Hardware: 3 LDAP-Server hinter 2 Load-Balancern

LDAP-Server - Struktur



alle RUBiKS-Kunden

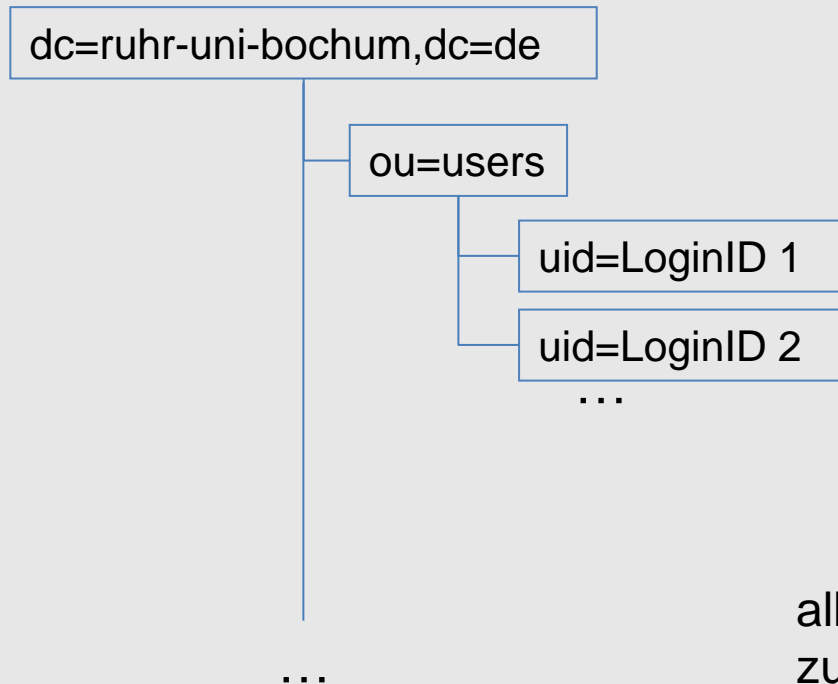
(mit APR1-MD5-Crypt-Passwort zur Authentifizierung durch ldap bind)

Gruppenmitgliedschaft für blogs, wikis, ...

Verwalter für obige Gruppen

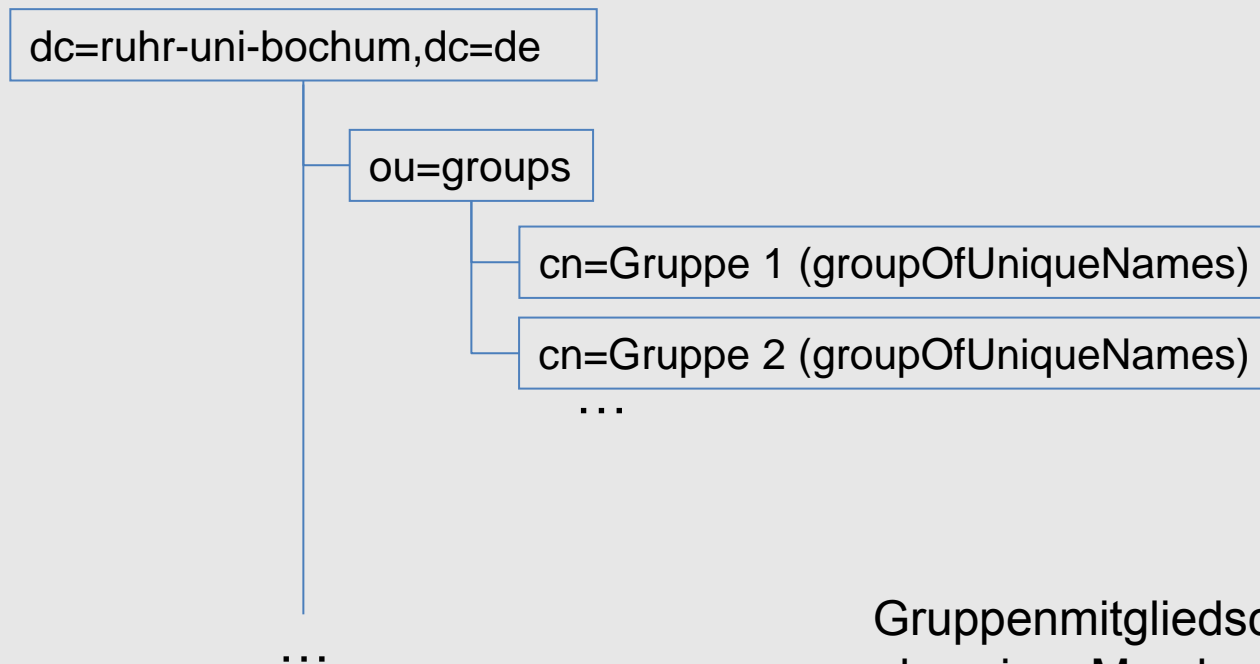
Gruppenmitglieder mit erweiterten Daten für linux-Server

LDAP-Server - Struktur: users



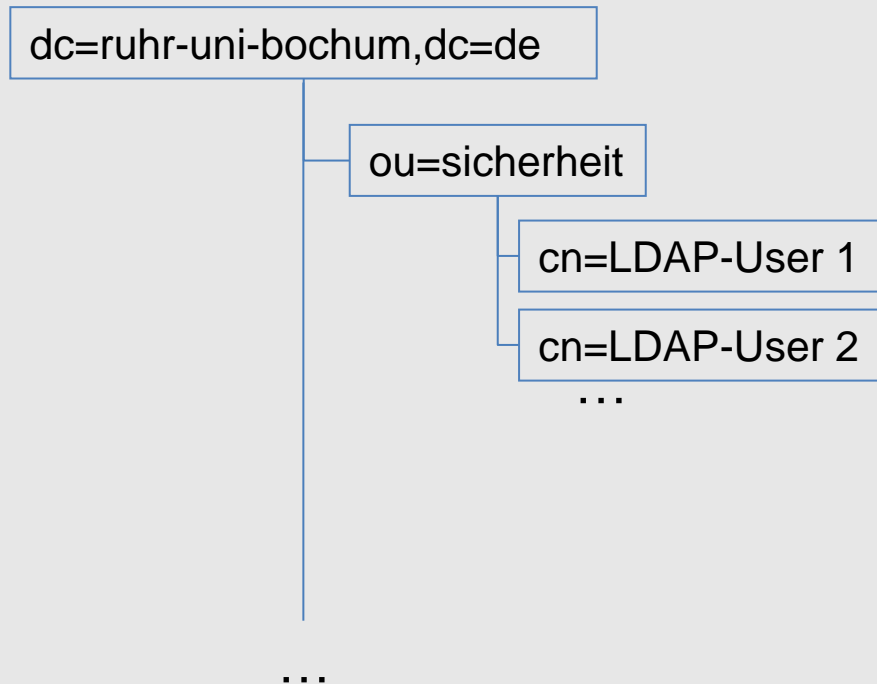
alle RUBiKS-Kunden inkl. APR1-MD5-Crypt-Passwort
zur Authentifizierung durch ldap bind

LDAP-Server - Struktur: groups



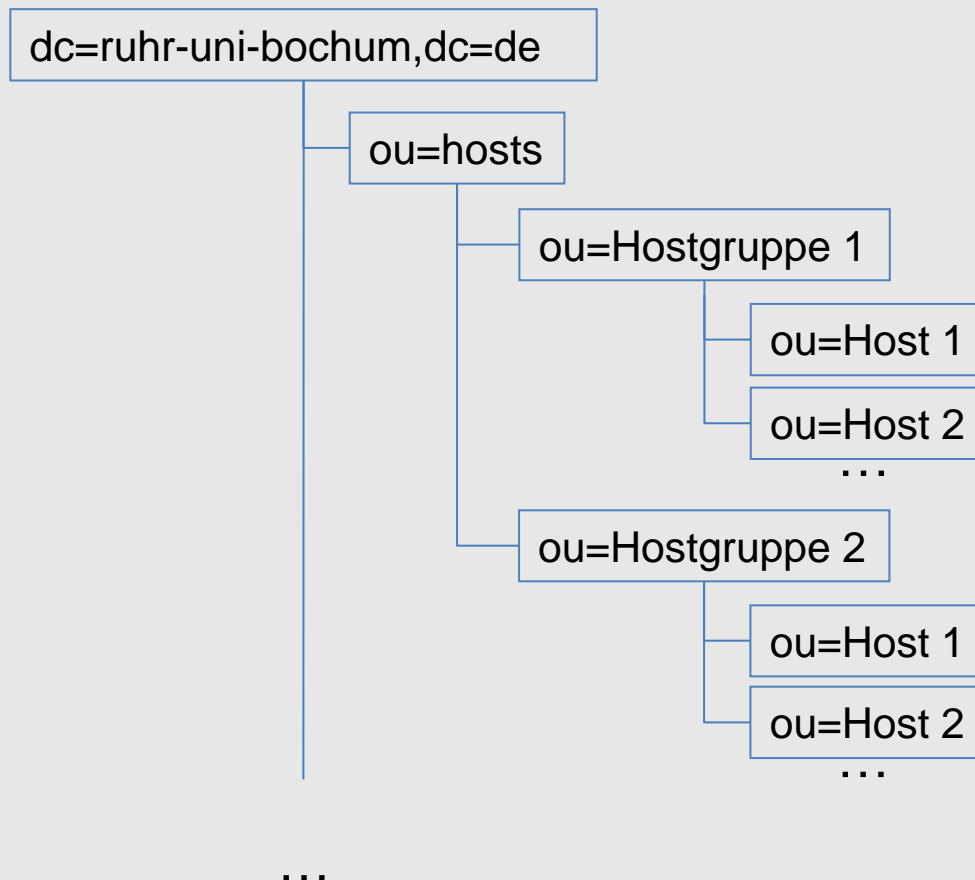
Gruppenmitgliedschaft für blogs, wikis, ...
als uniqueMember

LDAP-Server - Struktur: sicherheit



Verwalter für Idap-Gruppen

LDAP-Server - Struktur: hosts



erweiterte Daten für linux-Server
(posixAccount)

LDAP-Server - Nutzung: wiki

■ Wiki

```
vi /var/www/html/mediawiki/LocalSettings.php
```

```
require_once( 'LdapAuthentication.php' );  
$wgAuth = new LdapAuthenticationPlugin();  
$wgUseLDAP = true;  
  
$wgLDAPDomainNames = array("test-wiki");  
$wgLDAPServerNames = array("test-wiki" => "ldap.ruhr-uni-bochum.de");  
$wgLDAPBaseDNs = array("test-wiki" => "ou=Users,dc=ruhr-uni-bochum,dc=de");  
$wgLDAPSearchAttributes = array("test-wiki" => "(uid=USER-NAME)");  
$wgLDAPGroupFilters = array("test-wiki" => "(&(cn=<ldap-Gruppe>)(uniqueidentifier=USER-DN))");  
$wgLDAPGroupDNs = array("test-wiki" => "ou=Groups,dc=ruhr-uni-bochum,dc=de");  
  
$wgLDAPUseSSL = false; //Not Recommended!!  
$wgLDAPUseLocal = false; //Allow the use of the local database as well as the LDAP database  
  
//The following are for use in version 0.8+  
$wgLDAPAddLDAPUsers = false; //if true WikiDN and WikiPassword must be set  
$wgLDAPUpdateLDAP = false; //if true WikiDN and WikiPassword must be set  
$wgLDAPProxyAgent = "cn=<ldap-user>,ou=sicherheit,dc=ruhr-uni-bochum,dc=de";  
$wgLDAPProxyAgentPassword = "<ldap-user-password>";
```

LDAP-Server - Nutzung: debian-Server /1

■ debian

```
aptitude install libnss-ldap libpam-ldap nscd
```

Die darauffolgenden Fenster können weggedrückt werden,
da später direkt in den Konfigurationsdateien die Parameter eingestellt werden.

```
vi /etc/pam_ldap.conf
```

```
host ldap.ruhr-uni-bochum.de  
base ou=<Gruppe>,ou=hosts,dc=ruhr-uni-bochum,dc=de  
ldap_version 3  
binddn cn=<ldap-user>',ou=Sicherheit,dc=ruhr-uni-bochum,dc=de  
bindpw <ldap-user-passwort>  
pam_password crypt
```

```
vi /etc/libnss-ldap.conf
```

```
host ldap.ruhr-uni-bochum.de  
base ou=<Gruppe>,ou=hosts,dc=ruhr-uni-bochum,dc=de  
ldap_version 3  
binddn cn=<ldap-user>',ou=Sicherheit,dc=ruhr-uni-bochum,dc=de  
bindpw <ldap-user-passwort>
```

LDAP-Server - Nutzung: debian-Server /2

■ debian

```
vi /etc/nsswitch.conf
```

```
passwd: files ldap  
group: files ldap  
shadow: files ldap
```

```
vi /etc/pam.d/common-account
```

```
account sufficient pam_unix.so  
account sufficient pam_ldap.so  
account required pam_deny.so  
account required pam_unix.so
```

```
vi /etc/pam.d/common-auth
```

```
auth sufficient pam_ldap.so  
auth sufficient pam_unix.so use_first_pass  
auth required pam_deny.so  
auth required pam_unix.so nullok_secure
```

LDAP-Server - Nutzung: debian-Server /3

■ debian

```
vi /etc/pam.d/common-password
```

```
password sufficient pam_unix.so nullok obscure min=4 max=8 md5  
password sufficient pam_ldap.so  
password required pam_deny.so
```

```
vi /etc/pam.d/common-session
```

```
session required pam_unix.so  
session required pam_mkhomedir.so umask=0022
```

```
service nscd restart
```

LDAP-Server - Nutzung: RedHat 5-Server

■ RedHat 5

system-config-authentication starten

BaseDN: ou=<Gruppe>,ou=hosts,dc=ruhr-uni-bochum,dc=de
LDAP-Server: ldap://ldap.ruhr-uni-bochum.de

vi /etc/ldap.conf

```
base          ou=<Gruppe>,ou=hosts,dc=ruhr-uni-bochum,dc=de
binddn        cn=<ldap-user>,ou=sicherheit,dc=ruhr-uni-bochum,dc=de
bindpw        <ldap-user-password>
timelimit     120
bind_timelimit 120
idle_timelimit 3600
nss_initgroups_ignoreusers root,ldap,named,avahi,haldaemon,dbus,ravd,tomcat,radiusd,news,mailman,nsd,gdm
uri ldap://ldap.ruhr-uni-bochum.de/
pam_password  crypt
```

Weitere Informationen

- RZ-WIKI der RUB

<http://wiki.rz.rub.de>

- Oracle-Dokumentation (Understanding Oracle Virtual Directory)

http://docs.oracle.com/cd/E14571_01/oid.1111/e10046/und_ovd.htm

- Oracle Customer Snapshot

<http://www.oracle.com/us/corporate/customers/ruhr-identitymngt-ss-366803-de.pdf>

Oracle Customer Snapshot

Oracle Customer Snapshot



Ruhr-Universität Bochum
Bochum, Deutschland
www.ruhr-uni-bochum.de

Branche:
Forschung und Bildung

Mitarbeiter:
5.200

Oracle Produkte & Services:
Oracle Identity Management
Oracle Virtual Directory
Oracle Database, Enterprise Edition
Oracle Customer Support

Ruhr-Universität Bochum erzeugt einheitliche Sicht auf die Identitäten von mehr als 60.000 Usern

Die Ruhr-Universität Bochum (RUB) ist auf dem Weg, eine der führenden europäischen Hochschulen des 21. Jahrhunderts zu werden. Fast alle Studiengänge werden als Bachelor-Master-Programme angeboten, die ein forschendes Lernen ermöglichen. In den 20 Fakultäten des zentralen RUB-Campus studieren ca. 35.000 Studenten.

Herausforderungen

- Verwaltung der Identitäten von über 60.000 Studenten, Mitarbeitern und Gästen in 20 Fakultäten und 17 Instituten, die das zentrale Identity Management-System RUBiKS einsetzen
- Bereitstellung von mehr als 150 Services für die RUB-Community – z. B. Internet, Blackboard eLearning-System und OPAC-Bibliothekskatalog – auf der Basis von zugewiesenen Rollen
- Verwaltungskosten senken und Inkonsistenzen zwischen RUBiKS-Daten und LDAP-Daten (Lightweight Directory Access Protocol) beseitigen
- Compliance und Sicherheit erhöhen, indem Silolösungen im Bereich des Identity Managements abgebaut werden

Lösungen

- Mithilfe von Oracle Virtual Directory Darstellung einer virtuellen, einheitlichen Sicht auf die Identitäten und Aufbau einer einheitlichen Datenquelle für die Anwendungen der RUB, ohne die Daten in einen dedizierten Data Store zu konsolidieren
- Beseitigung der Zugriffsprobleme auf Identitätsdaten, dadurch Integration der vorhandenen Services und Anwendungen – z. B. des Internetzugriffs der Studenten – in das RUBiKS-System und beschleunigte Umsetzung neuer Anwendungen
- Ablösung eines älteren LDAP-Systems, um Inkonsistenzen bei der Datenbasis, Performance-Schwachstellen und redundante Identitätsdaten zu eliminieren
- Reduzierung der Anzahl der Identity Stores, indem auf Originaldaten statt auf synchronisierte Daten zugegriffen wird
- Zentrale Verwaltung der Konten und Rollen in einem Enterprise Directory in der Oracle Database Enterprise Edition: Reduzierung der Konten für individuelle Dienstleistungen und der benötigten Passwörter

“Mit Hilfe von Oracle Virtual Directory können wir auf einfache Weise und ohne weiteren Pflegeaufwand oder zusätzliche Kosten beliebige Daten unseres Identity-Management-Systems in Echtzeit für den LDAP-Zugriff zur Verfügung stellen. Wir verfügen jetzt über die komplette Sicht auf unsere 60.000 Studenten, Fakultäten und Gäste in einer einheitlichen Umgebung.” – Hans-Ulrich Beres, Projektmanager, Ruhr-Universität Bochum

Copyright © 2011, Oracle. All rights reserved.
Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

Veröffentlicht April 2011

ORACLE

Oracle Customer Snapshot



Ruhr-Universität Bochum
Bochum, Germany
www.ruhr-uni-bochum.de

Industry:
Education & Research

Employees:
5,200

Oracle Products & Services:
Oracle Identity Management
Oracle Virtual Directory
Oracle Database Enterprise Edition
Oracle Customer Support

Ruhr-Universität Bochum Creates a Unified View on More Than 60,000 Student and Employee Identities

Ruhr-Universität Bochum (RUB), one of the largest and leading research universities in Germany, competed for the title of Elite University in the Excellence Initiative by the German Government in 2007 and 2012. RUB's central campus has approximately 35,000 students enrolled in 20 university departments.

Challenges

- Optimize managing more than 60,000 student, employee, and guest identities in 20 university departments and 17 institutes using the central RUBiKS identity management system
- Offer more than 150 services—such as access to internet, blackboard eLearning system, and the library catalog. OPAC, to RUB's member community on the basis of role models
- Reduce administrative costs and avoid data inconsistencies between RUBiKS and lightweight directory access protocol (LDAP)
- Enhance compliance and security by eliminating identity silos

Solution

- Leveraged Oracle Virtual Directory for presenting a virtualized and unified view of RUB's identity data without needing to consolidate data into a single store, creating one source for RUB's applications
- Integrated existing services and applications—such as students' internet access—into RUBiKS and accelerated application deployment by resolving identity information access problems
- Removed an older LDAP system to eliminate data inconsistencies, performance bottlenecks, and redundant identity information
- Reduced the number of identity stores by accessing original data as opposed to synchronized data
- Centralized accounts and roles into an enterprise directory on Oracle Database Enterprise Edition to reduce the number of passwords that users must remember and eliminate the need to assign accounts to individual services
- Leveraged Oracle Customer Support to resolve problems immediately during implementation

“Oracle Virtual Directory enabled us to leverage real-time data from our identity management system and enabled simple LDAP access without adding any maintenance efforts or costs. We have now a full view of our 60,000 students as well as faculty and guests on one unified environment.” – Hans-Ulrich Beres, Project Manager, Ruhr-Universität Bochum

Copyright © 2011 Oracle. All rights reserved.
Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Published March 2011

ORACLE

Vielen Dank für Ihre Aufmerksamkeit

- Fragen



email: Hans-Ulrich.Beres@rub.de