Die Bibliothek der
Helmut-Schmidt-Universität

HELMUT SCHMIDT
UNIVERSITÄT

Bibliothek der Helmut-Schmidt-Universität Hamburg
Ulrich Hahn

Virtual Directories

Attribute für das Identitymanagement?

10. Shibboleth Workshop des DFN
Hamburg, 7.4.2010

Ulrich.Hahn@hsu-bibliothek.de

Die Bibliothek der
Helmut-Schmidt-Universität

Helmut Schmidt Universität

- Virtual Directories vs. Metadirectories
- ein Beispiel: myvd LDAP Virtual Directory
- noch ein Beispiel: Penrose VD Server
- ein Vergleich

Metadirectories

- Aufbau eines eigenen Directories
- Konsolidierung in neuem Schema
- Synchronisierung Datenbestände, fortlaufend

Produkte von Novell, Microsoft, Hitachi, Oracle
Opensource: SUN, GANYMEDE2 von arlut.utexas.edu

Virtual Directories

keine Änderungen bestehender Strukturen "internal view"
hohe Flexibilität beim "external view"

- Schemaänderung sofort
- Datenänderungen sofort

Produkte, Opensource: myvd, Penrose,

HELMUT SCHMIDT UNIVERSITÄT

myvd: Inserts

modular durch Inserts, aka Plugins

- Insert Reference
  - Services and Access Management Inserts
  - Mapping Inserts
  - Joining Inserts
  - Directory Inserts
  - Database Inserts
  - Web Services Inserts
  - Active Director
- Creating Custom Inserts

mit Beispielen (Skeleton)

HELMUT SCHMIDT UNIVERSITÄT

myvd: Chains

Sequence of Inserts
Bearbeitungsreihenfolge konfigurierbar
Java: chain Object verzweigt nach Konfiguration

```
public void bind(BindInterceptorChain chain,
        DistinguishedName dn,
        Password pwd,
        LDAPConstraints constraints) throws LDAPException {

   //...

chain.nextBind(dn,pwd,constraints);
}
```

HELMUT SCHMIDT UNIVERSITÄT

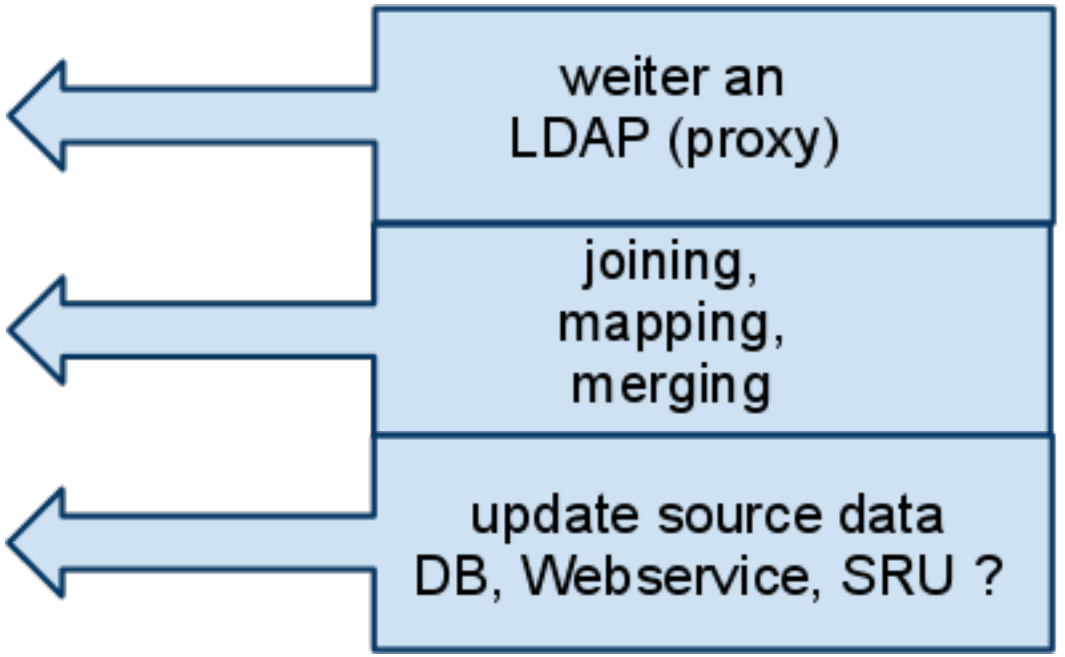
myvd: Routing

Differenzierung nach Anfragetyp: bind, read, update..

bind

read

update



HELMUT SCHMIDT UNIVERSITÄT

Konfiguration der Inserts über Datei(en) mit Attributzuweisungen

- schnell unübersichtlich
- nicht unterstützt durch XML Tools

```
#Define RootDSE
server.Root.chain=RootDSE
server.Root.nameSpace=
server.Root.weight=0
server.Root.RootDSE.className=net.sourceforge.myvd.inserts.RootDSE
server.Root.RootDSE.config.namingContexts=o=db,o=ldap

server.DBEmployees.chain=DB
server.DBEmployees.nameSpace=o=db
server.DBEmployees.weight=0
server.DBEmployees.DB.className=net.sourceforge.myvd.inserts.jdbc.JdbcInsert
server.DBEmployees.DB.config.driver=com.mysql.jdbc.Driver
server.DBEmployees.DB.config.url=jdbc:mysql://127.0.0.1/myvdjoin
server.DBEmployees.DB.config.user=trenduser
server.DBEmployees.DB.config.password=secret
server.DBEmployees.DB.config.rdn=uid
server.DBEmployees.DB.config.mapping=uid=username,l=location,appAttrib1=appAttrib1,
appAttrib2=appAttrib2
server.DBEmployees.DB.config.objectClass=dbPerson
server.DBEmployees.DB.config.sql=SELECT username,location,appAttrib1,appAttrib2 FROM
userdata
server.DBEmployees.DB.config.useSimpleTrue
```

HELMUT SCHMIDT UNIVERSITÄT

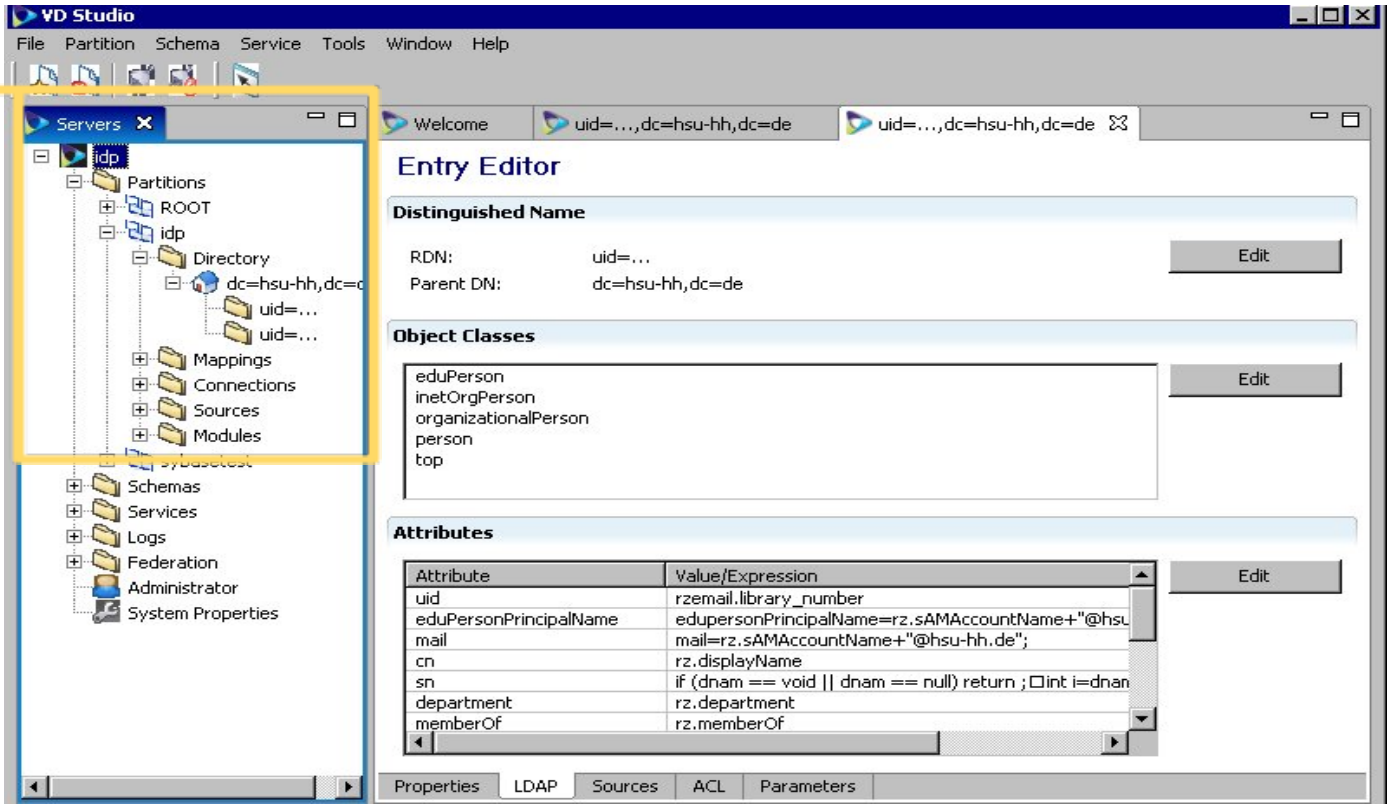
Penrose Virtual Directory

- Java RMX GUI: Penrose Studio
- Konfiguration in XML Dateien
- Standalone, als Tomcat Webapp oder embedded
- SUN, Apache, oder OpenLDAP als Server
- Schemata erweiterbar (Vorsicht: zweimal!)
- "Federation Server" synchronisiert NIS und LDAP (no DB Source)

HELMUT SCHMIDT UNIVERSITÄT

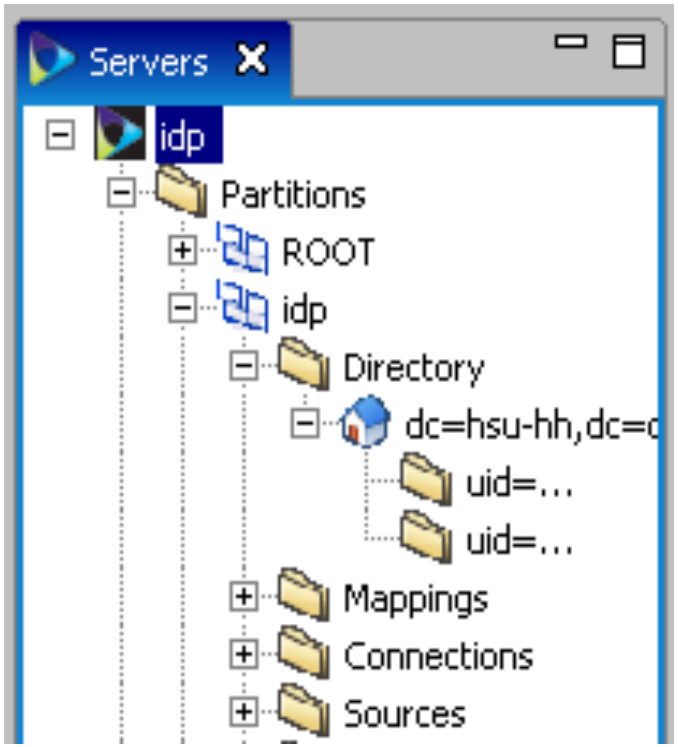
Penrose Virtual Directory

- Java RMX GUI: Penrose Studio



HELMUT SCHMIDT UNIVERSITÄT

Penrose Studio



HELMUT SCHMIDT UNIVERSITÄT

```
<source>
  <source-name>ads1</source-name>
  <field name="cn">
    <variable>uid</variable>
  </field>
</source>

<source>
  <source-name>borrower</source-name>
  <field name="borrower_bar">
    <variable>ads1.cn</variable>
  </field>
</source>
```

```
 <entry dn="uid=...,dc=hsu-hh,dc=de">
  <entry-class>org.safehaus.penrose.directory.DynamicEntry</entry-class>
  <oc>eduPerson</oc>
  <oc>inetOrgPerson</oc>
  <oc>organizationalPerson</oc>
  <oc>person</oc>
  <oc>top</oc>
  <at name="uid" rdn="true">
   <variable>rzemail.library_number</variable>
  </at>
  <at name="eduPersonPrincipalName">
   <expression>edupersonPrincipalName=rz.sAMAccountName+"@hsu-hh.de";</expression>
  </at>
  <at name="cn">
   <variable>rz.displayName</variable>
  </at>
```

HELMUT SCHMIDT UNIVERSITÄT

	Penrose VD 	myvd 
Entwicklung / Zukunft	nightly build vom 12/2009	jüngster Stand 2008 ?
GUI	Penrose Studio - Java RMX - Eclipse based	-
Quelltext?	OpenSource, Java,	OpenSource, Java, "Inserts" individuell
Features	Id Federation "Management" Directory Migration	Routing: bind,read,write,(update) Chains
Dokumentation	Tutorials, fertige Beispiele	Skeleton zur Erezugung eigener Inserts

HELMUT SCHMIDT UNIVERSITÄT

Vielen Dank!
Fragen?

Zum Weiterklicken:

Penrose Virtual Directory 	http://penrose.safehaus.org http://www.heise.de/kiosk/archiv/ix/2009/3/142 http://www.wiso-net.de/webcgi?START=A60&DOKV_DB=ZECO&DOKV_NO=PMGI2009021943&DOKV_HS=0&PP=1
MyVD LDAP Virtual Directory 	http://myvd.sourceforge.net/
Ganymede 2.0	http://tools.arlut.utexas.edu/gash2/ http://www.usenix.org/event/lisa98/full_papers/abbey/abbey.pdf
Dieser Vortrag	http://ub.hsu-hh.de/go/shib10