Verzeichnisdienste am Beispiel LDAP

Peter Schmid

Hochschule für Technik Zürich
Studiengang Informatik

29.10.2008

Outline

HOCHSCHULE FÜR TECHNIK ZÜRICH

Was ist ein Verzeichnisdienst (Directory Service)?

- Telefonbuch/Telefonverzeichnis/Phone Directory
- Bekanntester Verzeichnisdienst ist DNS. Umwandlung von Hostnames in IP-Adressen und umgekehrt. Verteiltes System.
- LDAP ist lediglich das Protokoll zur Kommunikation

HOCHSCHULE FÜR TECHNIK ZÜRICH

Geschichtlicher Rückblick

- Verzeichnisse lokal, z.B. `/etc/passwd`, werden von Hand verteilt und synchronisiert.
- Zusammen mit NFS wird NIS 1986 eingeführt (beruht auf RPCs, Client-Server Protokoll).
  - **N**etwork **I**nformation **S**ervice, auch bekannt unter Yello Pages (YP)
  - NIS ist flach organisiert, keine Replikation, unsicheres Protokoll, keine Zugriffsberechtigungen
- NIS+
  - Sun Microsystems 1993
  - Hierarchisch, sicher (Secure RPC), Zugriffsberechtigungen, replizierbar.
  - Kompliziert, blieb v.a. auf SUN beschränkt

Geschichtlicher Rückblick, cont.

- X.500
  - 1990, ITU-T (vormals CCITT)
  - Sehr umfangreicher Standard
  - Wurde nie komplett implementiert.
- LDAP Lightweight Directory Access Protocol
  - 1993, Universität von Michigan
  - Basiert auf X.500
  - Stark vereinfacht, darum *Lightweight*
- Active Directory Service, AD aka ADS
  - 2000, Microsoft, zusammen mit Windows 2000 Server eingeführt
  - Integriert Verzeichnisdienst (ähnlich LDAP), Authentifizierung (Kerberos) und DNS.

Wieso LDAP?

- Schneller Lesezugriff: Durch seine nichtnormalisierte Datenspeicherung mit einem Lesezugriff auf ein ganzes Objekt.
- Verteilte Datenhaltung, Teile des DITs können auf verschiedenen Servern sein. Proxy möglich.
- Flexibles, voll objektorientiertes Datenmodell. Aenderungen möglich ohne bereits implementierte Funktionalität zu beeinflussen.
- Breite Anwendungsunterstützung, Industrie-de-facto-Standard für Authentifizierung, Autorisierung und Benutzer- und Adressverzeichnisse.

HOCHSCHULE FÜR TECHNIK ZÜRICH

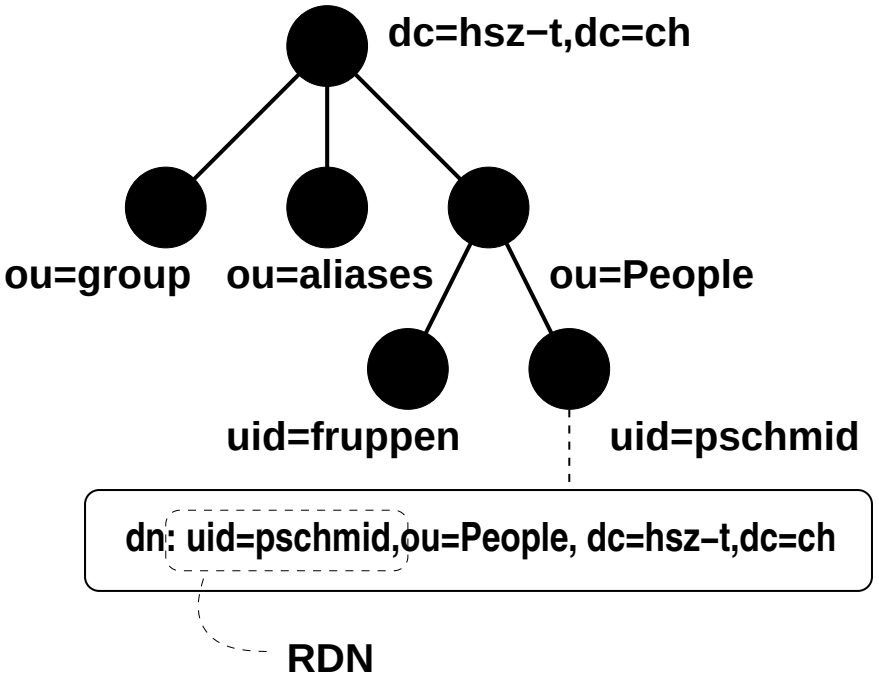
Information Model

- Directory Information Tree (DIT)
- Hierarchischer Baum mit Wurzeln, Zweigen und Blättern.
- Die Wurzel (root, suffix) ist das oberste Datenobjekt, kann mehrere Wurzeln haben.
- Verzeichniseinträge (entries) heissen LDAP-Objekte.
- Jedes Objekt gehört zu mindestens einer, in der Regel aber zu mehreren Klassen (Object Classes).
- Objekt-Klassen werden durch ihre Attribute bestimmt.

Information Model, cont.

- Die Definitionen von Objekt-Klassen und Attributen werden zu Schemas zusammengefasst.
- Attribute können obligatorisch (mandatory) oder optional sein.
- Objekte, die selbst Objekte enthalten, werden als *Containerobjekte* bezeichnet.
- Die Enden des Baumes heissen *Blattobjekte*.
- Jedes Objekt ist eigenständig und aus Attributen zusammengesetzt.
- Jedes Attribut eines Objekts hat einen bestimmten Typ und einen oder mehrere Werte.

Directory Information Tree (DIT)



cn:	Peter Schmid
gidNumber:	1445
givenName:	Peter
homeDirectory:	/afs/hsz−t.ch/usr/pschmid
objectClass:	top person posixAccount sambaSamAccount
ou:	Informazikdienste aFuE
sambaHomePath:	\\jay\pschmid
uid:	pschmid

Attribut Types	Values

Naming Model

- Jeder Eintrag hat ein unique Attribut, dieses Attribut nennt man Relative Distinguished Names (**RDN**).
  - Vergleichbar mit Filename.
  - Kann aus mehreren Attributen bestehen.
  - Beispiel: `cn=pschmid`
- Den ganzen Pfad zum Eintrag nennt man Distinguished Name (**DN**).
  - Entspricht dem Pfad und Filenamen im Filesystem.
  - Reihenfolge ist aber umgekehrt (wie bei DNS, FQDN)
  - Beispiel: `cn=pschmid,ou=group,dc=hsz-t,dc=ch`
- Canonical Name, hat keine Attribut-Tags wie `ou`.
  - Umgekehrte Reihenfolge, Abtrennung durch Slashes.
  - Beispiel: `hsz-t.ch/group/pschmid`

HOCHSCHULE FÜR TECHNIK ZÜRICH

LDIF

- Für den Datenaustausch wird LDIF (LDAP Interchange Format) verwendet, RFC 2849.
- Es sind Plain-Text ASCII Files (7bit), für andere Zeichen wird UTF-8 base-64 kodiert.

```
dn: uid=pschmid,ou=People, dc=hsz-t,dc=ch
loginShell: /bin/bash
givenName: Peter
sn: Schmid
cn: Peter Schmid
o:: SG9jaHNjaHVsZSBmw7xyIFRlY2huaWsgWsO8cmljaA==
ou: Informatikdienste
ou: aFuE
l:: WsO8cmljaA==
```

HOCHSCHULE FÜR TECHNIK ZÜRICH

Objektklasse

- Beispiel Definition der Objektklasse `swissEduPerson` der SwitchAAI.
- Bei diesem Beispiel gibt es keine Muss-Attribute (nur `MAY` kein `MUST`).

```
objectClass ( SwissEduObjectClass:1
    NAME 'swissEduPerson'
    DESC 'Swiss eduPerson Object for use in e-Academia'
    SUP inetOrgPerson
        STRUCTURAL
    MAY ( swissEduPersonUniqueID $ swissEduPersonDateOfBirth $
          swissEduPersonGender $ swissEduPersonHomeOrganization $
          swissEduPersonHomeOrganizationType $ swissEduPersonStudyBran
          swissEduPersonStudyBranch2 $ swissEduPersonStudyBranch3 $
          swissEduPersonStudyLevel $ swissEduPersonStaffCategory $
          swissEduPersonMatriculationNumber $ eduPersonAffiliation $
          eduPersonOrgDN $ eduPersonOrgUnitDN $
          eduPersonEntitlement ) )
```

HOCHSCHULE FÜR TECHNIK ZÜRICH

Attribut

- Beispiel Definition des Attributs `swissEduPersonHomeOrganizationType`.
- Darf nur ein Wert enthalten `SINGLE-VALUE`.
- Beim Suchen wird Gross- und Kleinschreibung nicht unterschieden `EQUALITY caseIgnoreMatch`.
- Syntax wird über Object Identifiers (OIDs) bestimmt. IANA vergibt diese Nummern.

```
attributetype ( SwissEduAttributeType:5
        NAME 'swissEduPersonHomeOrganizationType'
        DESC 'Type of the home organization'
        EQUALITY caseIgnoreMatch
        SINGLE-VALUE
        SYNTAX '1.3.6.1.4.1.1466.115.121.1.15' )
```

HOCHSCHULE FÜR TECHNIK ZÜRICH

Tools

- Standard Command Line Tools
  - ldapsearch
  - ldapmodify, ldapadd, ldapdelete
- Webbrowser wie Mozilla (nicht Firefox) oder den Internet-Explorer, die auch das LDAP Protokoll verstehen. Die URL sieht so aus:
  `ldap://<host>:<port>/<node>?<attributes>?<base|one|sub>?<filter>`
  Beispiel:
  `ldap://ldap.hsz-t.ch:389/ou=People,dc=hsz-t,dc=ch?givenname,sn?one?(uid=*schmid*)`
- GUIs: Sun Java System Server Console (Solaris), LDP (Windows)
- Webapplikationen wie z.B. phpLDAPadmin:
  `https://pubwww.hsz-t.ch/phpldapadmin/`
- Toolkits und APIs: PerLDAP, TCL Package LDAP, Java Naming and Directory Interface (JNDI) API

HOCHSCHULE FÜR TECHNIK ZÜRICH

Suchen

- Gross- und Kleinschreibung hat meistens keinen Einfluss (abhängig von den Attributen, Matching Rules).
- Wichtigste Optionen von `ldapsearch`:
  `-h ldaphost -b searchbase -s base|one|sub filter [attrs...]`

```
$ ldapsearch -h ldap.hsz-t.ch -b "dc=hsz-t,dc=ch" -s sub "uid=pschmid"
version: 1
dn: uid=pschmid,ou=People, dc=hsz-t,dc=ch
gecos: Peter Schmid
telephoneNumber: 043 268 2604
loginShell: /bin/bash
roomNumber: Zi117
...
```

HOCHSCHULE FÜR TECHNIK ZÜRICH

Suchfilter

- Syntax ist in RFC 2254 beschrieben.
- Syntax
  `<filter>=(<attribute><operator><value>)` oder
  `(<operator><filter1><filter2>)`

Logical operator	Description
=	Equal to
~=	Approximately equal to
<=	Lexic. less than or equal to
>=	Lexic. greater than or equal to
&	AND
|	OR
!	NOT

Suchmusterbeispiele

- Alle Objekte:

```
(objectClass=*)
```

- Alle Benutzer Objekte ausser Ruedi:

```
(&
(objectCategory=person)(objectClass=user)
(! cn=ruedi))
```

- Alle Objekte die mit dem Vornamen sm starten:

```
(sn=sm*)
```

- Alle Kontakte mit dem Nachnamne Schmid oder Keller:

```
(&
(objectCategory=person)(objectClass=contact)
(| (sn=Schmid)(sn=Keller)))
```

HOCHSCHULE FÜR TECHNIK ZÜRICH

Eingabe und Löschen von Daten

- Eingabe eines Objektes:

```
$ ldapadd -h ldap1.hsz-t.ch -D "cn=directory manager"
dn: cn=pschmid,ou=group,dc=hsz-t,dc=ch
memberUid: pschmid
gidNumber: 1445
objectClass: posixGroup
objectClass: top
cn: pschmid
```

- Löschen eines Objektes:

```
$ ldapdelete -h ldap1.hsz-t.ch -D "cn=directory manager" \
"cn=pschmid,ou=group,dc=hsz-t,dc=ch"
```

HOCHSCHULE FÜR TECHNIK ZÜRICH

Sicherheit und Zuverlässigkeit

- Bind, anonyme und Benutzer-Authentifizierung
- ACIs (Access Control Instructions)
- Replikation Multimaster
- Verschlüsselung über SSL

Wieso Sun Java System Directory Server?

- Multimaster Replikation über SSL (root-Zertifikat)
- Schema im DIT
- ACLs im DIT
- Nahtlose Integration in Solaris
- Hohe Sicherheit und Verfügbarkeit

Implementation

- Benutzerverwaltung POSIX für UNIX/Linux.
- Gruppenverwaltung POSIX.
- Mailaliase für MTA sendmail.
- Samba Benutzer, Gruppen und NT-Passwörter.
- Autorisierung in Webapplikationen wie EBS, Wikis usw.
- Autorisierung für SwitchAAI (Zugriff auf Ressourcen anderer Hochschulen).

HOCHSCHULE FÜR TECHNIK ZÜRICH