Directory Services mit LDAP

Dipl.-Chem. Rainer Orth
Technische Fakultät
Universität Bielefeld
ro@TechFak.Uni-Bielefeld.DE

Übersicht

- Directory Services
- Von X.500 zu LDAP
- LDAP-Modelle
- Implementierungen
- Anwendungen
- Probleme
- Zusammenfassung

Directory Services

- Hierarchisches Online-Informationssystem
- spezialisierte Datenbank, optimiert für Lesezugriffe
- dynamische Updates
- flexible Datentypen, -organisation
  - Text, URLs
  - Zertifikate
  - Fotos
- Netzwerk-Zugang über dediziertes Protokoll
- u.U. verteilt, repliziert
- Beispiele: DNS, NIS, X.500, LDAP, ...

X.500: Die Mutter von LDAP

- X.500: OSI-Protokoll für weltweites verteiltes Directory
- erster Standard 1988, Weiterentwicklung bis heute (v4: 2001)
- Anwendungen: White Pages, Mail-Routing für X.400
- Client-Server-Modell: DUA (Directory User Agent), DSA (Directory System Agent)
- mehrere Protokolle: DAP, DSP, DOP, DISP

X.500: Vor- und Nachteile

- Vorteile:
  - ausgefeilter, mächtiger Standard für verteiltes, repliziertes Directory mit starker Authentisierung
- Nachteile:
  - komplexer OSI-Stack als Transport
  - ASN.1-Spezikation des Protokolls mit aufwendiger Kodierung
  - nur eine freie Implementierung (QUIPU)
  - anfangs Interoperabilitätsprobleme

LDAP: Lightweight Directory Access Protocol

- vereinfachte Version nur von X.500 DAP
- arbeitet über TCP/IP statt OSI-Stack
- String-Kodierung vieler Daten/Protokoll-Elemente
- einfacher zu implementieren, performanter als X.500
- erste Implementierung: LDAPv1/DIXIE (RFC 1249), University of Michigan, 1991
- aber: abhängig von der QUIPU-Implementierung

LDAP: Weitere Entwicklung

- LDAPv2: 1993, 1995: RFC 1777, 1778, Draft Standard
  - Server unabhängig von X.500
- LDAPv3: 1997, 2000: RFC 2251–2256, 2829, 2830, 3377, Proposed Standard
- Neu in LDAPv3:
  - Internationalisierung (UTF-8)
  - Referrals: Referenzen auf andere LDAP-Server
  - Security: SASL, StartTLS
  - Erweiterbarkeit: Controls und Extented Operations
  - Informationen über Features und Schemata
- Jetzt: ldapbis-WG: Überarbeitung von LDAPv3 für Draft-Status

LDAP-Modelle

- Informations-Modell: wie sehen Einträge aus?
- Naming-Modell: wie werden sie benannt?
- Funktions-Modell: LDAP-Operationen
- Security-Modell: Authentisierung

Das LDAP-Informationsmodell

- benannte Einträge:
  - getypte Attribute (manche zwingend, andere optional), festgelegt durch Objektklassen/Schema
  - einer oder mehrere Werte
  - Attribut-Syntax legt mögliche Werte fest
  - *matching rules* bestimmen, wie Vergleiche arbeiten

Objektklassen, Attribute und Schemata

- jeder Eintrag hat Objektklassen (structural, auxiliary)
- legen mögliche Attribute (zwingend, optional) fest
- bilden Hierarchie mit Vererbung von Attributen
- Satz von Objektklassen, Attributen, Syntaxen für einen bestimmten Zweck bilden ein Schema
- zahlreiche Schemata bereits in LDAPv3-Spezifikation (z.T. aus X.500 und Piloten)
- erweiterbar: Anwender kann neue Objektklassen und Attribute definieren, Syntaxen und *matching rules* nur mit Erweiterung der Server-Implementierung, Registry bei
  `http://www.schemareg.org/`

Ein Beispieleintrag

```
dn: cn=Rainer Orth,ou=Technische Fakultaet,o=Universitaet Bielefeld,c=DE
objectClass: top
objectClass: person
objectClass: pilotObject
cn: Rainer Orth
sn: Orth
telephoneNumber: +49 521 106 2901
userPassword: {CRYPT}XXXXXXX
uid: ro
mail: ro@TechFak.Uni-Bielefeld.DE
drink: {T.61}Milk \24 Tea
roomNumber: M3-106
lastModifiedTime: 940705170900Z
lastModifiedBy: cn=Rainer Orth,ou=Technische Fakultaet,o=Universitaet Bielefeld,c=DE
personalTitle: Mr
```

Naming-Modell

- ein Attribut eines Eintrags ist ausgezeichnet:
- Relative Distinguished Named (RDN)
- Distinguished Name (DN) des Eintrags ergibt sich aus Verkettung des RDNs mit denen der Parents
- `cn=Rainer Orth,ou=Technische Fakultaet,o=Universitaet Bielefeld,c=DE`
- Namespaces
  - klassisch (X.500): länderbasiert
  - DNS-basiert: `dc=TechFak,dc=Uni-Bielefeld,dc=DE`
  - völlig frei: LDAP legt keine Namespace-Struktur fest
- Aliases: LDAP-Symlinks

Funktions-Modell

- LDAP-Operationen:
  - Abfrage: `search`, `compare`
  - Modifikation: `add`, `delete`, `modifydn`, `modify`
  - Authentisierung etc.: `bind`, `unbind`, `abandon`

LDAP-Suche

- viele Parameter, u.a.
  - Basis-Eintrag
  - Scope (base, subtree, onelevel)
  - Suchfilter (exakt, Substrings, *approximate match*, >=, <=, Attribut vorhanden, Kombinationen davon)
  - Attributliste

Beispiel: Suche im Uni-LDAP-Verzeichnis

```
$ ldapsearch -h ldap.uni-bielefeld.de. -b 'o=addrbook' \
  '(&(sn=Koch)(department~=biologie))' mail
version: 1
dn: uid=andreas.koch@uni-bielefeld.de,o=uni-bielefeld.de,o=addrbook
mail: andreas.koch@uni-bielefeld.de

dn: uid=linda.koch@uni-bielefeld.de,o=uni-bielefeld.de,o=addrbook
mail: linda.koch@uni-bielefeld.de

dn: uid=markus.koch@uni-bielefeld.de,o=uni-bielefeld.de,o=addrbook
mail: markus.koch@uni-bielefeld.de

dn: uid=stefanie.koch@uni-bielefeld.de,o=uni-bielefeld.de,o=addrbook
mail: stefanie.koch@uni-bielefeld.de

dn: uid=natalie.koch@uni-bielefeld.de,o=uni-bielefeld.de,o=addrbook
mail: natalie.koch@uni-bielefeld.de
```

Security-Modell

- Authentisierung: Bind mit DN und Credentials
- Möglichkeiten:
  - Anonymous Bind: keine Authentisierung
  - Simple Bind: Authentisierung mit Klartext-Passwort
  - SASL: DIGEST-MD5 zwingend, andere Verfahren möglich (z.B. GSSAPI mit Kerberos V5 oder EXTERNAL mit TLS-Client-Zertifikaten)
- Authentisierung und Verschlüsselung auch mit TLS
- Zugangskontrolle: nicht standardisiert, aber von den meisten Servern implementiert, teilweise nicht im Directory abgelegt, nicht interoperabel

Server-Implementierungen

- viele freie und kommerzielle basieren immer noch auf der LDAPv2-Referenzimplementierung von der U Michigan
- Open Source: OpenLDAP, `http://www.openldap.org/`, aktuell: 2.2.4
- kommerziell: Sun ONE Directory Server 5.2, Netscape Directory Server 6.2, aber auch Novell eDirectory (NDS), Microsoft Active Directory
- immer noch: Isode M-Vault R10.1, X.500- und LDAP-Server

LDAP als Nameservice

- Luke Howard, An Approach for Using LDAP as a Network Information Service, RFC 2307, 1998
- Schema für POSIX-Datenbanken: `passwd`, `group`, `services`, ...
- Alternative zu NIS, NIS+
- wird zunehmend von Betriebssytem-Herstellern integriert: `nss_ldap`, `pam_ldap` (PADL Software, `http://www.padl.com/`), ab Solaris 8, IRIX 6.5, Linux

Weitere Anwendungen

- Ablage von `sendmail`-Maps
- Authentisierung und Zugangskontrolle für Apache (`mod_auth_ldap`)
- Radius-Konfiguration
- Backend für DNS-Zonen

Probleme mit LDAP

- keine standardisierte Zugangskontrolle (bisher nur Requirements aus ldapext-WG)
- Replikation seit 1998 in Arbeit (ldup-WG)
- wirklich noch *lightweight*?
- Schema-Entwicklung unkoordiniert/inkonsistent

Zusammenfassung

- LDAP bietet allgemeines/erweiterbares Modell für Directory Service
- Möglichkeit der Konsolidierung zahlreicher Einzel-Directories etc.
- breite Unterstützung vieler Hersteller
- aber: bisher noch nicht vollständig spezifiziert