LDAP: Technologie, Anwendungen und Ausblicke

H. Pfeiffenberger
Alfred Wegener Institut
für Polar- und Meeresforschung
Bremerhaven,

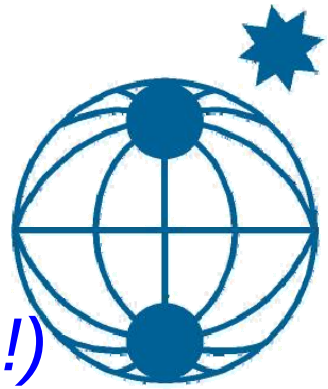
Einführung

- *Was ist LDAP*
- *(Wie unterscheidet es sich von SQL (RDBMS))*

- *Wozu kann man es gebrauchen*
- *Was verspricht man sich davon*
- *Was gibt es heute tatsächlich (am AWI, z.B.)*
- *Welche Entwicklungen / Produkte sind absehbar*

- *Warum soll sich ausgerechnet die Wissenschaft (Polar- und Meeresforschung !!!) damit beschäftigen ??*

Was ist LDAP ?



- *LDAP: Lightweight Directory Access Protocol*
- *Directory: Verzeichnisdienst (nicht nur Personen!)*
- *Lightweight: Im Gegensatz zu X.500 (DAP, 1988?)*
  (nicht standardisiert: Verzeichnis-Synchronisierung)
- *RFCs 1777-79,-81, 1823, 2251-56 u.a. definieren LDAP*
  - **Protokoll (ASN.1, siehe X.500) und (!!)**
  - **API: ldap_open, _close, _search, _modify, _delete**
  - **Exportformat LDIF (Text, Base64), s. Bsp. 1-4**
  - **einige Objektklassen mit Attributnamen und -semantik**
  - **ACLs auf Attributebene !!**
  - **implizite Zuhilfenahme des DNS (dc, s.u.) : dadurch im Unterschied zu X.500 kein Root-Verzeichnis notwendig!!**

Unterschiede zu SQL-RDBMS

- *Abfrage-Protokoll und API standardisiert, (SQL: nur Abfrage-Sprache) daher: ziemlich herstellerunabhängige Client / Server - Interoperabilität*
- *Erkennbare Spezialisierung auf Verzeichnisse*
- *RDB: Menge von Tabellen <=> Hierarchie von Objekten*
- *Multivalued-ness (Bsp.: cn)*
- *Objekte müssen (und werden i.A.) nicht der 3. Normalform entsprechen (Bsp.: cn <=> displayname)*
- *Server wesentlich stärker optimiert auf Abfrage (z.B. für Verzeichnisse mit 20-50 Mio Einträge)*

Beispieleintrag (Teil 1)

- **dn: uid=hpfeiffenberger,ou=People, dc=awi-bremerhaven, dc=de, o=awi**
- **objectclass: top**
- **objectclass: person**
- **objectclass: organizationalPerson**
- **objectclass: inetOrgPerson**
- **objectclass: AWIPerson**
- **givenname: Hans**
- **sn: Pfeiffenberger**
- **cn: Hans Pfeiffenberger**
- **sn;alternate: Pfeiffenberger**
- **cn;alternate: Hans Pfeiffenberger**
- **displayname: Hans Pfeiffenberger**

X.500: DN: CN=Hans Pfeiffenberger, OU=IT,O=Alfred Wegener Institut,C=DE

Klassen definieren required, allowed Attribute, eigene Erweiterungen (mit Vererbung) möglich

";alternate" hier für Umlaute auch ";lang=de" möglich

Beispiel (Teil 2)

- **uid: hpfeiffenberger** *(hier) SHA, nicht crypt*
- **userpassword: {SHA}uKm3kewpHcJrrlNnC7pPbidwAyo=**
- **ou: People** *(bloss) keine “echte” ou !!*
- **mail: hpfeiffenberger@AWI-Bremerhaven.DE**
- **telephonenumber: +49(471)4831-1305**
- **mobile: none**
- **facsimiletelephonenumber: +49(471)4831-1590**
- **l: Bremerhaven, buildingname: CC, roomnumber: 508**
- **postaladdress::** *Umlaut => Base64: “Bürgermeister Smidt Str.”*
  QsO8cmdlcm1laXN0ZXItU21pZHQtU3RyYcOfZSAyMCwgR C0yNzU2OCBCcmVtZXJoYXZlbg==
- **postofficebox: Postfach 120161, D-27515 Bremerhaven**

de: PO-Box => anderer ZIP Code

Beispiel (Teil 3)

- **title: Dr.** *personaltitle vs. (job-)title*
- **job: Physicist**
- **eduPersonOrgDN: cn=awi-2000-07, ou=Groups, dc=awi-bremerhaven,dc=de,o=awi** *“Nummer” statt Name!*
- **eduPersonOrgDN: cn= awi-2000-0701, ou=Groups, dc=awi-bremerhaven,dc=de,o=awi** *wg. Namensänderung*
- **personalhomepage: http://www.awi-bremerhaven.de/InfoCenter/IT/WorkingGroups/LDAP/**
- **duties: General user support; Infrastructure Distributed Systems**
- **researchinterest: Distributed Systems; High speed networks - ATM, IP, satellite; Integration of data and publication; Digital Library; Member of LDAP Group**

Beispiel (Teil 4)

- **top5publications: uid=Dod1997a,ou=Publications, dc=awi-bremerhaven,dc=de,o=awi**
- **top5publications: uid=Pfe1996a,ou=Publications, dc=awi-bremerhaven,dc=de,o=awi**
- **top5publications: uid=Dod1996a,ou=Publications, dc=awi-bremerhaven,dc=de,o=awi**
- **top5publications: uid=Dod1995a,ou=Publications, dc=awi-bremerhaven,dc=de,o=awi**

- **modifiersname: uid=hpfeiffenberger,ou=People, dc=awi-bremerhaven,dc=de,o=awi**
- **modifytimestamp: 20010924091125Z**

modify-ACL: self !!
s.a.: Datenschutz !!

LDAP(-URL) Filter Syntax

- *Bsp. Mailgruppe Klimasystem*
  ldap://e-net.awi-bremerhaven.de:389/o=awi?cn?sub?
  (&(objectclass=AWIPerson)
  (*eduPersonOrgDN* =*awi-2000-0101*))
- Alle Personen in Gebäude “D“ mit Vornamen „Dieter“
  (&(objectclass=AWIPerson)(buildingname=D)
  (givenname=Dieter))
- *Alle Personen mit Forschungsgebiet “Klima”*
  (&(objectclass=AWIPerson)(researchinterest=*climate*))

Wozu kann man LDAP gebrauchen

- *Wie X.500: Corporate Directory = Telefonbuch+*
  - **+ in dem Sinne: vordefiniert sind z.B. die Attribute manager (der Vorgesetzte der Person), roleOccupant**
  - **“RoleOccupant” gehört zur Klasse “OrganizationalRole” Die “Org.Role” ist ansonsten eine OrganizationalPerson, nicht z.B. (dynamisch) definiert durch LDAP-Filter**
- *LDAP als “Registry” für alle möglichen Anwendungen, z.B. (in chronologischer Reihenfolge am AWI:)*
  - **Netscape Mail-Server, -Client, Web-Server-Auth**
  - **SunRay (mit SmartCard-Einsatz)**
  - **Publikationsdatenbank**
  - **Windows2000, (Exchange2000)**
  - **=> für einen Zertfikatsdienst !!**

Was verspricht man sich von LDAP

- *Lokales Verbinden der Directories unterschiedlicher Systeme; Hoffungen :*
  - **nur noch ein Passwort (Nutzer, RZ)**
  - **Single Sign-On (Nutzer)**
  - **Nur eine Nutzerverwaltung (RZ, Nutzer)**
    - *schnelle Übersicht über Zugang zu Resourcen*
    - *schnelle (De-) Aktivierung von Accounts*
- *Aber: Nicht Ein(e) Directory(-Instanz) für alles !! (Ich jedenfalls glaube nicht daran) Statt dessen: Metadirectory*
- *Globales Verbinden der Directories: DoD(HE): DNS für Menschen (und Anderes)*

Reality Check #1a: Person

- *W2000 Directory*
  - dn: CN=pfeiff,OU=People, DC=dmawi,DC=de
  - memberOf: CN=Domain Users, CN=Users,DC=dmawi,DC=de
  - objectCategory: CN=Person,CN=Schema,CN=Configuration,DC=dmawi,DC=de
  - objectClass: user
  - cn: pfeiff
  - displayName: Hans Pfeiffenberger
  - objectSid:: AQUAAAAAAAUVA...
  - objectGUID:: tc+hKiMt+...
- *Netscape Directory*
  - dn: uid=hpfeiffenberger, ou=People, o=awi-bremerhaven.de
  - objectclass: top
  - objectclass: person
  - objectclass: organizationalPerson
  - objectclass: inetOrgPerson
  - objectclass: AWIPerson
  - cn: Hans Pfeiffenberger
  - uid: hpfeiffenberger

Reality Check #1b: Person

- *Win2000 Directory*
  - **userPrincipalName: pfeiff@awi-bremerhaven.de**
  - **pwdLastSet: 125376334350818125**
  - **primaryGroupID: 2266**
  - **name: pfeiff**
  - **sAMAccountName: pfeiff**
  - **sAMAccountType: 805306368**
  - **userAccountControl: 66048**
  - **uSNChanged: 632682**
  - **uSNCreated: 1544**
  - **whenChanged: 20010829112507.0Z**
  - **whenCreated: 20010103094658.0Z**
- *Netscape Directory*
  - **mail: hpfeiffenberger@AWI-Bremerhaven.DE**
  - **userpassword:{SHA}uKm3kew...**
  - **workingunit: StructOrgUnitID=awi-2000-07,ou=Units,o=...**
  - **workingunit: StructOrgUnitID=awi-2000-0701,ou=Units,o=...**
  - **modifiersname: uid=hpfeiffenberger,ou=People,o=...**
  - **modifytimestamp: 20010924091125Z**

Reality Check #2: Replication

- *Replikation ist nicht standardisiert, aber nötig:*
  - **dn: DC=dmawi,DC=de**
  - **masteredBy: CN=NTDS Settings,CN=SYLTSRV1, CN=Servers,CN=Sylt,CN=Sites,CN=Configuration, DC=dmawi,DC=de**
  - **masteredBy: CN=NTDS Settings,CN=EDVP16, CN=Servers,CN=Bremerhaven,CN=Sites,CN=Configuration, DC=dmawi,DC=de**
  - **masteredBy: CN=NTDS Settings,CN=HELGSRV1, CN=Servers,CN=Helgoland,CN=Sites,CN=Configuration**
  - **,DC=dmawi,DC=de**
  - **masteredBy: CN=NTDS Settings,CN=POTSSRV1, CN=Servers,CN=Potsdam,CN=Sites,CN=Configuration,.....**

Anwendungen für den Nutzer

- *Nutzerverwaltung interessiert das RZ (und die Verwaltung)*
  - **Wer hat Zugang zu welchen Ressourcen (bis wann?)**
  - **Wie hoch ist der Aufwand, das zu pflegen?**
- *SAP / e-Procurement einmal aussen vorgelassen:*
- *Den Anwender interessiert z.B.:*
  - **“wer gehört zur Arbeitsgruppe XY?”**
  - **“Filtere das Informationsangebot durch Interessenprofil”**
  - **....**
  - **Die aktuelle (!) Publikationsliste der Arbeitsgruppe, der Sektion, des Fachbereichs, des Instituts**

Problem: Informationspflege

- *Die vielfältigen Informationen können nicht zentral gepflegt werden => Delegation*
  - **Vorzugsweise durch den einzelnen selbst (ab dem ersten Arbeitstag - ca. 1/4 bis 1/5 Fluktuation)**
  - **Korrektur, Redaktion möglichst auf der nächst höheren Ebene (mit Vertretungsregeln- Expeditionstätigkeit!!)**
- *=> Rechte erteilen - Abläufe gestalten*
  - **Rollenbasierte Authorisierung**
  - **Bsp. Docmaster (u.a. secretary), Daten-Kurator**
  - **Rolle als Attribut der Person, der Gruppe**
- *Authentisierung / Authorisierung => Identity / Policy*
- *“Business-Logic” => Workflow*

AWI-Anwendungen

- *Strukturierte Information*
  - **Formularbasierte Eingabe, kontrolliertes Vokabular**
  - **Dynamische Ausgabe**
  - **Bsp.: Persönliche Daten / Homepage**
  - **Bsp.: neue AWI-Publikation / Publikationslisten**
- *Unstrukturierte Information*
  - *Netscape Webserver Publish-Funktion*
  - *zukünftig Redaktionssystem ?*

- **Und jetzt live !! (hoffentlich)**

Ankündigungen und Visionen

- *Metadirectories: Microsoft und Iplanet haben M. angekündigt, um IDS und ADS zu synchronisieren. Implementierungen: unbekannt*
- *Internet2: Middleware ist eines von 4 Oberthemen (auf derselben Ebene wie Netze selbst*
  - **EduPerson (z.B. Ident. gegenüber e-Verlagen)**
  - **DoDHE = Directory of Directories of Higher Education**
  - **Videokonferenz-Geräte / Teilnehmer**
  - **GRID Authz**
  - **als Speicher für PKI Zertifikate**
- *AWI: Verbundene Verzeichnisse von Personen, Gruppen, Publikationen, Datensätzen, (Ereignissen?)*

Warum wir ?? (Wissenschaft)

- *Warum soll sich ausgerechnet die Wissenschaft (Polar- und Meeresforschung !) damit befassen ??*
  - **Hohe Fluktuation, nicht nur der Personen, sondern auch der Strukturen : Gruppen (Projekte) kommen und gehen - Alle wollen - als solche - gefunden werden und benötigen interne Kommunikation (angefangen beim Mail-Verteiler)**
  - **Beteiligung an DoD(HE): Entsprechende Argumente, aber auf globaler Ebene.**
  - **Insbesondere wichtig als Instrument zur Findung internationaler, multidisziplinärer Gruppen - also vor der Phase, in der es Veröffentlichungen gibt.**
    - So schön Polarstern als Treffpunkt auch ist ;-))
- *Wird uns der Datenschutz hindern oder helfen ??*

Zusammenfassung

- *LDAP ist ein hocheffizientes Werkzeug, um Verzeichnisse zu erzeugen und zu publizieren*
- *Eine “offene” LDAP-Implementierung (I-Planet, nicht Active Directory) bietet die Möglichkeit zur Erweiterung um wissenschafts-spezifische Klassen und Attribute*
- *These: Qualifizierte (globale) Verzeichnisse von Personen werden die wissenschaftliche Kommunikation verändern --- bis hin zum Paradigmenwechsel*
- *Die Wichtigkeit des Themas ist zumindest bei Internet2 erkannt*
-

Fragen ?