Zur Zukunft von Directories: X.500(93) und LDAP

Vortrag gehalten beim Directory-Betreiber-Treffen
„Zur Zukunft von Directories in Deutschland“
am 1. September 1999

Peter Gietz
DFN Directory Services,
Zentrum für Datenverarbeitung,
Universität Tübingen

Agenda

- Augenblickliche Situation
- LDAP
  - LDAP als zukünftige White Pages Infrastruktur
  - LDAP noch unvollständig
  - Plan eines LDAP DIT
  - Neue Anwendungen für LDAP
- Hybrides Directory
- Aufgaben in Deutschland

Augenblickliche Situation

- X.500(88) Infrastruktur obsolet
- Bisherige X.500(93) Tests unbefriedigend
- RFC 2120 zu Root Naming Context nicht implementiert
  - Es basiert auf Directory Operational Protocol (DOP)
  - DOP wird bisher von keinem Produkt unterstützt
- Interesse an LDAP (v3) steigt

Vorarbeiten in Deutschland

- Kein Rückwärtstrend im X.500 durch DFN-Engagement
- Teilweise schon X.500(93) (CDC, zunehmend Messaging Direct)
- DFN Projekt „Betrieb und Betreuung der deutschen Directoryinfrastruktur“
- DFN Projekt AMBIX, X.500 für alle mit LDAP-Integration
- DFN Projekt „Aufbau und Betrieb eines Directory-Kompetenzzentrums“
  - DFN Directory Services

LDAP als zukünftige White Pages Infrastruktur

- Viele Länder gehen zu reinen LDAP Lösungen über
  - Schweden: TISDAG (http://tisdag.sunet.se/)
  - Norwegen: Norwegian Directory of Directories (draft-hedberg-alvestrand-ndd-00.txt)
  - Holland: http://www.surfnet.nl/surfnet-zoektools/search.html
  - Griechenland: http://ds.grnet.gr/index_en.html

LDAP noch unvollständig

- Replikation (IETF WG ldup)
- Authentifizierung (IETF WG ldapext)
- Access control (IETF WG ldapext)

Plan eines LDAP DIT

- Neuer Referral-Mechanismus in LDAP v3
- draft-ietf-ldapext-knowledge-00.txt
  - Kein einheitlicher Namespace notwendig
  - Superior reference
  - Unnamed reference (entspricht nonspecific subordinate reference)
- Implementierung in Netscape Directory Server („smart referrals“)
- Replikation via LDIF möglich (Slurpd)

Neue Anwendungen für LDAP

- Betriebssystemintegration, z.B. als Network Information Service (NIS)
  - Linux (http://www.rage.net/ldap/)
  - SUN (Solaris 8)
  - Windows 2000 (Active Directory)
- Routing policy
  - IETF WG policy
  - Directory Enanbled Network (DEN)
- Keyserver für Public Key Infrastruktur

Hybrides Directory

- Umstieg auf X.500(93)
- Backbone von Firstlevel DSAs eines X.500(93) Produktes (Messaging Direct)
- Knowledge Information wird über einen Root DSA geshadowed
  - mittels DISP oder
  - mittels LDIF/FTP
- Konnektivität zu LDAP und anderen X.500 Servern (88 und 93)

Aufgaben in Deutschland

- Zwingender Umstieg auf X.500(93)
- LDAP Integration
- Integration in den europäischen Gesamt-Index, auf Basis der im EC-Projekt DESIRE II entwickelten Software
- Voranbringen von PGP
- Definition von Untergliederung und Sichtweisen für c=DE (geographisch, Schulen, KuMB, DFN, YP, WP ...)
- Richtlinien für die Güte eines Eintrags:
  - Minimal-Datensatz für O, OU und CN Einträge
  - Minimalanzahl von Einträgen unterhalb eines O-Eintrags
  - Qualität der Aktualisierungsmechanismen
  - Anforderung an die Erreichbarkeit von DSAs
- Namensrichtlinien
- Homogener Einsatz von Gateway-Software und deren Darstellungskonfigurationen
- Homogenere Access Controll