D D S

Weitere Entwicklungen um LDAP

33. DFN Betriebstagung

Directory Forum

Berlin 10.10.2000

Peter Gietz

Peter.gietz@directory.dfn.de

D D S

Agenda

- IETF
  - LDAPext (LDAP Extensions)
  - LDAPbis (LDAP Revision)
  - LDUP (LDAP Duplication and Replication Protocols)
  - LCUP (LDAP Client Update Protocol)
- DIRECT (Directory Replication Coordination)
- TF LSD (Task Force LDAP Service Deployment)
- [LDAP und DEN (Directory Enabled Networks)]

D D S

IETF LDAPext, neue RFCs (1)

- **RFC 2820:** E. Stokes, D. Byrne, B. Blakley, P. Behera, Access Control Requirements for LDAP, May 2000 (wir berichteten)
  - Architektur Dokument steht kurz vor RFC Status

- **RFC 2829:** M. Wahl, H. Alvestrand, J. Hodges, R. Morgan, Authentication Methods for LDAP, May 2000 (wir wollten berichten)

D D S

IETF LDAPext, neue RFCs (2)

- **RFC 2830:**
  J. Hodges, R. Morgan, M. Wahl, Lightweight Directory Access Protocol (v3): Extension for Transport Layer Security, May 2000
  - **neue LDAP Operation: StartTLS request und response**
  - **öffnet einen geschützen TLS Kanal**
  - **kann auch zur Authentifizierung verwended werden**

D D S

IETF LDAPext, neue RFCs (3)

- **RFC 2891: T. Howes, M. Wahl, A. Anantha, LDAP Control Extension for Server Side Sorting of Search Results, August 2000**
  - **Erweiterung der search-Operation**
  - **ermöglicht Client sortierte Liste der Ergebnisse anzufordern**
  - **Client kann spezifizieren**
    - **nach welchem(n) Attribut(en) sortiert werden soll**
    - **nach welchen Sortierregeln (als matching rules zu definieren)**

D D S

LDAPbis

- LDAP (v3) Revision BoF bei der IETF 48 in Pitzburg
- Die LDAPv3 RFCs (RFC 2251-56) haben bisher noch keinen Draft Standard Status, weil damals bessere Authentifikationsmechanismen als ungeschütztes Passwort nicht zur Verfügung standen
- Mit RFC 2829 und RFC 2830 stehen solche Mechanismen jetzt zur Verfügung
- Auch an einigen anderen Stellen sind die LDAPv3 RFCs Revisionsbedürftig
- Es geht nur um die Core-Dokumente, LDAPExt bleibt unberührt.

D D S

IETF LDUP (1)

- LDAP Duplication/Replication/Update Protocols
- Zwei Replikationsmodelle:
  - Multi-Master Replikation
    - Einträge können auf jeder Kopie (Replikat) verändert werden
  - Master-Slave oder Single-Master Replikation
    - Nur eine Kopie darf verändert werden alle anderen sind Replikate
- Gemeinsame Replikationsarchitektur
- Kommt nur sehr mühsam voran
  - seit August 1998 tätig und noch kein RFC
  - selbst Requirements-Dokument noch umstritten
  - Problem: Multi-Master und gelöschte Einträge (tomb stones)

D D S

IETF LDUP (2)

- 6 Arbeitsbereiche:
  - LDAPv3 Replication Architectur
    - Replikations-Komponenten, ihre Funktion und Interaktion
  - LDAPv3 Replication Information Model
    - Schema und Semantik der benötigten Information
  - LDAPv3 Replication Information Transport Protocol
  - LDAPv3 Mandatory Replica Management
    - LDAPv3 Erweiterungen für Administration, Replika-Bereitstellung, Replikations-Vereinbarungen
  - LDAPv3 Update Reconciliation Procedures
    - Prozeduren für Konflikt-Entdeckung und -Auflösung
  - LDAPv3 Profiles
    - Teilmenge der anderen Bereiche für Multi-Master- und Single-Master-Replikation

D D S

IETF LDUP (3)

- **Neuer Draft:**
  Ellen Stokes, Roger Harrison, Gordon Good,
  Extended Operations for Framing LDAP Operations,
  <draft-ietf-ldup-framing-00.txt>, March 10, 2000
  - **Mechanismus um Anfang und Ende einer Gruppe von LDAP-Operationen spezifizieren zu können**
  - **Ähnelt einem Transaktions-Mechanismus**
  - **Wird bei Multi-Master-Replikation benötigt um sicherzustellen, das Replikation vollständig geschah**

D D S

LCUP

- O. Natkovich, M. Smith, M. Armijo, LDAP Client Update Protocol, <draft-natkovich-ldap-lcup-01.txt>, July 2000
  - Erlaubt Client lokal Daten zu speichern und diese mit einem Server zu synchronisieren
  - Keine Replikations-Vereinbarungen
  - Jede Aktion geht vom Client aus
  - Micro$oft ist kürzlich mit ins Boot gekommen
- LDUP WG überlegt sich dieses Thema aufzunehmen

D D S

DIRECT (1)

- DIrectory REplication CoordinaTion
- TERENA Projekt mit Mitwirkung von SURFnet
- DANTE integriert Ergebnisse in NameFLOW
- Final Report vom 23.8.2000
- Vgl. http://www.terena.nl/projects/direct/index.html

D D S

DIRECT (2)

- Für den Aufbau einer LDAP Server Infrastruktur
- Mit Referral-Mechanismus kann man auf andere Server verweisen
- Projekt sammelt eine Liste von Country-Level-LDAP-Server
- Wegen fehlenden Replikationsstandard wird diese Liste als LDIF-File erstellt und via HTTP bzw. FTP verteilt

D D S

DIRECT (3)

- Liste enthält neben Referrals auch zusätzliche Daten über den Länderknoten
- Proprietärer Mechanismus definiert:
  - Wenn baselevel oder onelevel search, werden die zusätzlichen Daten angezeigt
  - Wenn subtree search, wird der Referral zurückgegeben und Client auf den Server selbst verwiesen
  - Innosoft hat dieses Feature für DIRECT in Server eingebaut
  - Wird nach Aufkauf durch iPlanet (Netscape/SUN) dort weiter unterstützt
  - Es gibt Bemühungen, dieses Feature zu standardisieren

D D S

TF-LSD (1)

- TERENA Task Force “LDAP Service Deployment”
- Nach zwei LSD-Versuchen in der IETF nun ausserhalb
  - Erfolglose LSD WG (kein RFC)
  - Erfolgloser Versuch einer LSD2 BoF bei der IETF 45 in Oslo
- TF-LSD BoF am 12.5.2000 in Amsterdam
- Erste konstituierende Sitzung am 20.9.2000 in Utrecht
  - 18 Teilnehmer vorwiegend von europäischen Forschungsnetzten
- Vgl. http://www.terena.nl/task-forces/tf-lsd/

D D S

TF-LSD (2)

- **Ziele:**
  - **Forum für Erfahrungsaustausch**
  - **Untersuchung von LDAPv3 für Informationsdienste für die Forschungsgemeinschaft in Europa**
  - **Aufbau eines Index-basierten europäischen White Pages Dienst für LDAP Server**
  - **Aufbau einer LDAP basierten PKI (public Key Infrastructure) für die europäische Forschungsgemeinschaft**
  - **Definition weiterer LDAP basierten Dienste unter Berücksichtigung neuer Technologien (z.B. DSML, DEN)**
  - **Beteiligung an Standardisierungsprozessen (z.B. IETF, ITU, CEN)**