IETF work on LDAP

NameFLOW LDAP Pilot Meeting
29 May 1998, Novotel London, Heathrow

Karl-Peter Gietz, DANTE
Peter.Gietz@dante.org.uk
Working groups on LDAP

- IDS - Integrated Directory Services
- ASID - Access, Searching and Indexing of Directories
- LSD - LDAP Service Deployment
- LDAPEXT - LDAP Extension
- FIND - Common Index Protocol
- SCHEMA - Schema Registration
- SVRLOC - Service Location Protocol
- LDUP - (LDAP Duplication)
IDS - Integrated Directory Services

- White Pages Services (RFCs 2148, 2218)
  - X.500, SLAPD, Whois++, PH
- X.500 Root Naming Context (RFC 2120)
- DomainComponent in DN (RFC 2247, id ids-dirnaming-04)
- Network Services (RFC 2219)
- Internet Nomenclator (RFCs 2258, 2259)
ASID - Access, Searching and Indexing of Directories I: RFCs

- LDAP v2 (RFCs 1777-1779, 1959, 1960)
  - Protocol, attribute syntax, DN, URL, filters
- CLDAPv2 (RFC 1798)
- LDAP v3 (RFCs 2251-2255)
  - UTF-8/ISO 10646, referrals, SASL, extensions
  - no secure update!
- URI (RFC 2079)
- Schema definitions (RFCs 1804, 2247, 2256)
ASID II: Unfinished Work

- => LDAP Extensions WG
- Replication
  - LDAPv3 requirements (draft-weiser-replica-req-01) ==> LDUP
  - LDIF (draft-good-ldap-ldif-00)
  - Change logging (draft-good-ldap-changelog-00)
  - Multi master replication (id asid-ldap-mult-mast-rep-02)
- MIME Content Type (id asid-mime-direct-07)
  - Profile for vCard (id asid-mime-vcard-06)
  - Profile for LDAP schema ==> Schema WG
ASID III: What else?

- Caching (id asid-ldap-cache-01) outdated?
- Schema (draft-smith-ldap-inetorgperson-00)
- Whois++ (ids asid-whois-schema-03, asid-whois-url-02, asid-whoispp-02)
LSD - LDAP Service Deployment

- Schema
  - Minimum White Pages schema (id lsd-ldapv3-wp-00)
  - Guidelines (no id)
  - Inconsistencies and mappings (no id)

- Locating LDAP servers
  - (ids lsd-client-finding-00, lsd-server-finding-00)

- Naming and interconnectivity (id lsd-nandi-00)
- TISDAG reports (no id)
LDAP Extensions I: Security

- **Authentication**
  - Minimum subset of LDAPv3 authentication methods (id ldapext-authmeth-01):
    - anonymous authentication, SASL-CRAM-MD5, Start TLS with SASL EXTERNAL
    - TLS (id ldapext-ldapv3-tls-00)

- **Access control**
  - The model: ACLs (id ldapext-acl-model-00)
  - Requirements collection (id ldapext-acl-reqts-00)

- **Non-repudiation**
  - Signed LDAP-operations (draft-hassler-ldapv3-secparam-00)
  - Signed Directory Information (id ldapext-sigops-00)
LDAPEXT II: Where and what to search

- Knowledge reference
  - URI-Referral: attribute and objectclass (id ldapext-referral-00)
  - URL-Referral: LDAP control (draft-watts-orbell-ldapext-x500-referrals)
  - Server discovery: co-operation with == Svrloc-WG

- Search results
  - Server side sorting (id ldapext-sorting-00)
  - Simple paged results (id asid-ldapv3-simplepaged-02)
  - Persistent search (id ldapext-psearch-00)
  - Virtual list (id ldapext-ldapv3-vlv-01)
LDAP EXT III:
Application Program Interfaces

• LDAPv3 C API
  • C API definition (id ldapext-ldap-c-api-00)
    • includes LDAP extenden operations model
  • C API extensions
    • Extensions for persistent search (id ldapext-c-api-psearch-00)
    • Extensions for virtual lists (id ldapext-c-api-vlv-01)

• LDAPv3 Java API
  • Java API definition (id ldapext-ldap-java-api-01)
  • Extensions for server sorting, persistent search and virtual lists (draft-weltman-ldap-java-controls-01)
LDAPEXT IV: What else?

- Language tags (id ldapext-lang-00)
- Dynamic directories (id asid-ldapv3-dynamic-07)
- CLDAP v3 (no id)
- LDAP as Network Information Service (RFC 2307)
FIND Common Index Protocol

• The architecture (id find-cip-arch-01)
• MIME object definitions (id find-cip-mime-02)
• Transport protocol (id find-cip-trans-00)
• Tagged Index Object (id find-cip-tagged-06)

• When will CIP become RFCs?
SCHEMA - Schema Registration

- Centralized registration of MIME directory schemata
  - Definition of directory schema listing procedure (id schema-proc-list-01)
  - Requirements for a directory schema listing (id schema-rqmts-list-01)
  - MIME profile for meta data (id schema-mime-metadata-01)
  - MIME profiles for whois, whois++ and rwhois (ids schema-whois-00, schema-whoispp-00, schema-rwhois-00)
  - MIME profile for LDAP (id schema-ldap-00)
SVRLOC Service Location Protocol

- Definition of the SPL (RFC 2165)
  - Framework for the discovery and selection of network service
  - Dynamic configuration mechanism for applications in LANs
  - Not a global resolution system for the entire Internet
- Service discovery beyond SLP (id svrloc-discovery-06)
  - Aggregation of several concepts: SLP, “Sites” alias structure, DNS SRV records, “Well Known” alias, “service:” URLs
- Procedure of defining service types for the “service:” URLs (id svrloc-service-scheme-09)
- Definition of conversion LDAP schema <-> “service:” URLs (id svrloc-template-conversion)
LDUP - LDAP
Duplication/Replication/Update Protocol

- WG still in status nascendi
- Based on the work started in ASID
- BOF meeting was December 1997
- Mailinglist: subscribe to ietf-ldup-request@imc.org