LDAP Directory Servers: dc=hello,dc=world

Tony Cesaro

November 7, 2012

Topics

- **Overview**
  - What is an LDAP directory server?
  - Use Cases
  - History
- **Server Components**
  - Database
  - Schema
  - Directory Data
  - Directory Structures
  - LDAP Interface
- **Software**
- **Demo**
- **Future Topics**

What is an LDAP directory server?

- Protocol to query/update database (RFC 1777)
- Read-optimized database
- Platform independent data store
- Hierarchical data structures
- Extensible schema

Use Cases

- Organizational directory
- Centralized user authorization/authentication
- Group management
- Host naming services
- Autofs configuration
- NIS netgroups

History

- Roots in X.500 series - DAP (X.519)
- LDAP introduced as "Lightweight" DAP
- Initially the TCP/IP based alternative, X.500 bundled with OSI stack
- Less client side resource use
- Historical lineage of software

Database

- Typically a BDB backend
- Hierarchical structure, not relational (more OO)
- Attributes can be indexed
- Export/Import tools available - useful for backups

Schema

- Defines structure of objects/attributes
- Standards are usually default - RFC4519
- Can be extended for other object storage (e.g. RADIUS, NIS data)
- Defines optional, mandatory, single/multi-value attributes
- Example:

  ```
  attributetype ( 2.16.840.1.113730.3.1.4
  NAME 'employeeType'
  DESC 'RFC2798: type of employment for a person'
  EQUALITY caseIgnoreMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
  ```

Directory Data

- All entries identified by a Distinguished Name (DN)
- One or more ObjectClass values per entry
- Base DN defines the "root" of the directory
  - Usually defined similar to DNS zone: e.g. example.com = dc=example,dc=com
- Entries analogous to network/org objects with attributes
- Stores /etc/passwd,shadow,group,hosts and other data
- Also binary data such as pictures or audio

Directory Structures

- Thoughtful architecture important - define requirements first
  - Strive to store one entry per physical object, simplify
- Defines how objects are stored and accessed
- Can mimmick organizational structure
- Common branches:
  - ou=people
  - ou=groups
  - ou=hosts
  - ou=homedirs
  - ou=customers

LDAP Interface

- Network access for running queries and updating database
- LDIF is the standard ”interchange format”
- Filtering syntax available for complex queries
- Authorization in OS/applications through client side filters
- SSL/TLS encryption for transferring sensitive data

Software

- OpenLDAP
- pam_ldap
- nss_ldap
- 389 Server
- freeIPA
- ApacheDS
- OpenDS
- Samba

Demo

- Configure and start openldap (slapd)
- Import an LDIF file with sample data
- Run various queries against directory
- Update attributes of entries
- Export to LDIF, view

Future Topics

- Replication/Data Backup
- Heterogeneous Environments
- Advanced Search Filters
- Scripting LDAP calls