Slaps

a Smalltalk LDAP server

by
Bruce Badger
OpenSkills
Intro

• Bruce Badger
  – A founder of OpenSkills
  – Smalltalk developer

• OpenSkills
  – It's a global association of individuals
  – Non profit corporation
  – Believe that open standards & FOSS help create an open market for skills.
  – www.openskills.org
Agenda

• What is LDAP
• Why use it
• The LDAP spec
• Examples
• Benefits
Housekeeping

- Mobile phones off, please.
- Questions welcome during the talk
  - But note ...
    - “Question” = Single sentence ending with “?”
    - Questions may be:
      - deferred
      - dodged
      - ignored
What is LDAP?

- Lightweight Directory Access Protocol
- "Lightweight" vs. X.400 DAP
- Wire protocol
- LDAP clients and Servers implement the protocol
What does an LDAP server do?

- Can be thought of as a DBMS that uses LDAP rather than SQL
- LDAP has equivalents of:
  - Data Definition Language (DDL)
  - Data Manipulation Language (DML)
- Data is held in a tree rather than tables
  - the Directory Information Tree (DIT)
Why use an LDAP server?

• Widely used for:
  – Authentication
  – Authorisation
  – Address Books

• e.g.
  – Email client address book
  – Login to a shell or connect to a database
  – Kerberos
  – ... and lots more
Why write an LDAP server?

- Fun (hahahahahaha)
- Seemed like a good idea at the time.
  - OpenSkills needed to handle authentication and authorisation for a Jabber server
- It looked like just another wire protocol like:
  - NMEA
  - PostgreSQL
  - HTTP
  - ...
No, really. Why?

- Directory information exchange for OpenSkills
  - Authentication- member login
  - Authorisation -e.g. may edit SkillsTree?
  - “address book” e.g. account status

- Using an external LDAP server is non-trivial:
  - Yet another schema
  - Yet another export format (LDIF)
  - Synchronisation
LDIF Example

• From Wikipedia:

```ldif
dn: CN=John Smith,OU=Legal,DC=example,DC=com
changetype: modify
replace: employeeID
employeeID: 1234
-
replace: employeeNumber
employeeNumber: 98722
-
replace: extensionAttribute6
extensionAttribute6: JSmith98
-

dn: CN=Jane Smith,OU=Accounting,DC=example,DC=com
changetype: modify
...
```
OK, so what's involved?
OK, so what's involved?

- ASN.1
- ASN.1
- ASN.1
- ASN.1
- ASN.1
- ASN.1
- ASN.1
- ASN.1
- ASN.1
- ... and LDAP semantics
LDAP – as seen from space

• LDAP server listens on a TCP/IP port
• Client connects and the conversation goes like:
  – > BindRequest (Hi! May I use your service?)
  – < BindResponse (Sure!)
  – > SearchRequest (Tell me about x please.)
  – < SearchResultEntry (Here is info about x.)
  – < SearchResultDone (... and that's all I have.)
  – > UnbindRequest (I'm done. Bye.)
• Simple enough, except for ...
ASN.1

- Abstract Syntax Notation 1
- Specification and implementation of wire protocols
- LDAP is completely specified in ASN.1
- Flexible and concise, but more horrible than you can possibly imagine
- Main specs for the bits Slaps uses:
  - ITU X.680 - the basics
  - ITU X.690 - encoding
ASN.1 an example

BindRequest ::= [APPLICATION 0] SEQUENCE {
   version INTEGER (1 .. 127),
   name LDAPDN,
   authentication AuthenticationChoice }

LDAPDN ::= LDAPString

LDAPString ::= OCTET STRING -- UTF-8 encoded

AuthenticationChoice ::= CHOICE {
   simple [0] OCTET STRING, -- 1 and 2 reserved
   sasl [3] SaslCredentials,
   ... }

ASN.1 Encoding

• Like Chinese in that:
  – One written form (i.e. ASN.1)
  – Many “spoken” forms
    • BER – Basic Encoding Rules
    • CER – Canonical Encoding Rules
    • DER – Distinguished Encoding Rules
    • ...

• LDAP uses BER
Parsing BER

• TLD
  – sometimes
  – no sure way to jump, so must parse
    • sequentially
    • completely

• Demo of a BindRequest being parsed
Why Bother – Part II

• Flexibility (really)
• A single object model can be viewed in many ways
• No duplication of data
LDAP Schemas

• A number of defined structures
  – posix account
  – address book
  – DNS configuration
  – SMTP server configuration
  – ... and lots of bespoke structures
Slap me

- Plan
  - What will query your LDAP server
- Configure
  - Set up the “views”
- Go
  - Start the server
Is it fast enough?

• Who knows?
  – Slaps is at the “make it work stage”
• Probably fine for most long-tail apps
• If not, use replication to a “real” LDAP server
Insane?

- The OpenSkills SkillsBase
  - Runs as a http/html service in GemStone
  - Led to the development of Sport
  - Built 2003, Presented @ StS 2004
- Using HTTP in GemStone is not viewed as insane today
- I think LDAP will be handy too
- ... and next?
  - Kerberos, perhaps (also an ASN.1 protocol)
Summary

• No need to understand ASN.1
• Everything in Smalltalk so:
  – Easy to configure
  – Easy (well, as easy as possible) to understand
• No maintaining duplicate data
  – One model
  – Many views
Questions?

• Complaints:
  – bbadger@openskills.org