

Have you already been LDAPed?

Lightweight Directory Access Protocol



What it is, Why you want it, How to install it

Robert Sprockeels



OTA Linux SIG workshop 12/06/1999
5th Linux SIG anniversary

1



What it is...

- Centralized database to store information
 - Generally directories
 - But can store *any* information
 - No central authority
- Responds to queries over TCP/IP
- Can access X.500 directories
- Is mostly used stand-alone



Why you want it...

- Distributes information to client machines
 - To build a local or public directory service
 - Will replace existing Linux NIS services
- Has support for Access Control Lists (ACLs)
- Supports (will support 😊) SSL encryption
- Has hooks to code your own applications
 - C, Perl, PHP, Java...



OTA Linux SIG workshop 12/06/1999
5th Linux SIG anniversary

3



Object–related data structure...

- Hierarchical, built on a data schema
 - Based on a DIT (Directory Information Tree)
 - Standard schema is delivered
 - You can build your own
 - Entries have names (attributes)
 - Attribute is a data type with associated value
- One master server, multiple slave servers



Data hierarchy...

- Root of DIT is a "Base DN"
 - DN = Distinguished Name
 - One or more attributes form the RDN (Relative Distinguished Name) which MUST be unique
 - Top of your hierarchy (like SOA in DNS)
 - In general: o=Organization, c=Country
 - Not part of the naming context



The data...

- Set of attributes
 - Attribute = a data type with one or more associated values
 - Type:
 - number of values, syntax, matching on values, ...
 - Ex.: data type 'mail': one or more values, of type IA5 (ASCII), case insensitive
- Schema = collection of attribute definitions
- Each entry must have an objectClass



ObjectClass...

- Specifies the object class(es) of an entry
- Will determine the permitted attributes using the system and the user schema
- Values can be modified/removed, not the class
- Some are used by the server(s) for administering the directory system



Tools...

- A number of conversion programs
- A number of basic tools
 - ud - an interactive tool
 - ldapadd / ldapdelete / ldapmodify
ldapmodrdn / ldappasswd / ldapsearch
 - ldbmcat / ldbmtest / ldbminindex
- A number of servers
- A number of sample clients (contrib)



Where to get it...

- Commercial
 - Netscape's directory server
 - Siemens' DIR.X
 - ...
- Open source:
 - University of Michigan (now defunct)
 - OpenLDAP (<http://www.openldap.org>)



OTA Linux SIG workshop 12/06/1999
5th Linux SIG anniversary

9



Where to get information...

- RFC2251 through RFC2256 (in doc/rfc)
- LDAP FAQ
<http://www3.innosoft.com/ldapworld/ldapfaq.html>
- OpenLDAP Software FAQ
<http://www.openldap.org/faq/>
- Netscape Directory SDK
<http://www.mozilla.org/directory/>
- Linux Directory Services
<http://www.rage.net/ldap/>



OTA Linux SIG workshop 12/06/1999
5th Linux SIG anniversary

10



Installing the stuff...

- Get the software from <http://www.openldap.org/software/download>
- Extract, configure and build the software

```
tar xvzf openldap-release.tgz
cd ldap
./configure [--prefix=/opt/ldap --without-threads]
make depend; make
su
make install
```



An application example...

- An LDAP directory from your /etc/passwd
 - Write a shellscript, Perl script,... to extract data
 - Create an LDIF file with it, adding on top your Base DN
 - Must follow a specific structure
 - Use ldif2ldb to convert it
 - Create a slapd.conf file with your Base DN
 - Start slapd

