LDAP Overview

Kevin Moseley
Server Team Manager
Walgreen Co.

What is LDAP?

- LDAP (Lightweight Directory Access Protocol) is just that; a protocol.

- There are many implementations of LDAP including Sun iPlanet, RedHat Directory Server, and of course OpenLdap.

LDAP Overview

- Based on x.500 directory but has removed some of the more obscure features.

- Allows for full distinguished names. Allows for users to have same username since they are differentiated by context.

- Creates a central repository for user credentials and information.

- LDAP is optimized for reads.

LDAP Tree Example

LDAP Implementation

- Hardware requirements
  - Depends on number of users.
  - Fault tolerance requirements.
- Software requirements
  - This presentation is based on OpenLdap.
  - Any un*x based OS should be able to run OpenLdap.
  - Most likely you will get a precompiled binary from your distribution vendor.

LDAP Terminology

- Schema: Is what defines the characteristics of an object. (i.e. A user schema is name, password, email)

- Some options are required where others are optional.

- Relative distinguished name: dn:cn=Joe user

- Fully distinguished name: dn:cn=Joe user,ou=users,dc=company,dc=com.

LDAP Utilities

- Ldapsearch: Used to query the LDAP database.

- Ldapadd: Used to add entries to the LDAP database. Linked to ldapmodify.

- Ldapmodify: Used to modify existing entries in an LDAP database.

- Ldapdelete: Used to remove entries from a ldap database.

- Ldapmodrdn: Used to modify the RDN of an object.

LDAP Utilities cont.

- Slapcat: used to concatenate an ldap database into a LDIF file. Useful in creating slave LDAP servers and backup.

- NSSswitch used to allow a machine query an ldap server for credentials.

- pam_ldap allows for pam authentication against an ldap server.

Configuring LDAP

- Most configuration will be made to the slapd.conf file. This is the configuration file for the slapd daemon.

- Also configuration for the replication daemon is performed here. The replication daemon is called slurpd.

- Things you want to configure are context, replica-tion partners, database options.

Configuring LDAP cont.

- Slapd.conf is where you configure acl's for permissions on the directory.

- Also you configure the indexes for the database backend.

- Configure the number of cached objects in memory.

Example of slapd.conf

Adding users and objects

- Most additions can be made via a LDIF file. This file will allow for multiple additions to be made at one time.

- Nice because you can then script the addition of users or objects.

Replication overview

Verify LDAP is working

- Query the ldap server to verify it is responding to queries.

- Use ldapsearch -x -b "dc=company,dc=com" "(ob-jectclass=*)"

Possible uses of LDAP

- Samba authentication.

- Machine authentication.

- VPN and Radius authentication.

- Phone and email directory.

- Store sendmail configuration.

- Automount config.

- Store BIND zone files (with a patch)

- Interoperate with Active Directory.

More information....

- LDAP System Administration by O'Reilly
- OpenLdap website: www.openldap.org
- www.google.com
- www.padl.com

Questions and answers