

Secure LDAP Access

Andrew Phillips
Hewlett-Packard Company
20 Perimeter Summit Blvd.
Atlanta, GA 30319
404.648.5159
404.648.1816
andy_phillips@hp.com

Agenda

- Architectural Overview – 5 min
- Queries & Example Data – 10 min
- Source Examples in:Perl,C – 20 min
- Update and References – 5 min
- Questions – 10 min

Introduction

- Technologies: Perl, C (or C++), LDAP, SSL, Digital Certificates
- Learn: LDAP Modules, SSL Libraries,
- Prerequisites: perl 5.6, ‘any’ C compiler, LDAP Server, network access, a digital certificate
- Ideally – should already have LDAP access, and be comfortable with C or Perl 5.6
- This is a “how to use some LDAP technologies” kind of presentation

History, Background, etc.

RFCs

IETF ldapext working group

-<http://tulip.india.hp.com/inetsvcs/ietf.html>

-uses X.500 data model, but SIMPLER (case insensitive)

- Implements a DIR -> fast, efficient READ access

- Servers can be ADMIN using LDAP (like SQL DBs)

Overview

- Need an LDAP Client for searching
- Anonymous bind
- Searching for an LDAP object
- Security using a DN w/ encryption



LDAP Information Model

ENTRY:

Name

Type

Value [value1,...]

ENTRY:

uid

String

ajp@atl.hp.com

DN = RDN + RDN + RDN

RDN= o=hp.com

RDN= ou=Employees

RDN= uid=ajp@atl.hp.com

RDN= sn=Phillips

LDAP programmatic Access

- Obtain the appropriate libraries, include files and/or modules
- Read the docs for the function calls & return values
- TEST with an anonymous bind
- Then LOOK SOMEBODY UP !

EXAMPLE in Perl (Net::LDAP)

- `use Net::LDAP;`
- `my $ldap = Net::LDAP->new ("ldap.hp.com");`
- `$rc = $ldap->bind(); # anonymous`
- `my $msg = $ldap->search(base => "o=hp.com",
filter => "(& (ou=Employees) (uid=ajp@atlhp.com))");`

limiting Results in a search

- **SET OTHER ATTRIBUTES**

- filter => "(&(hptelnetnumber=648-5159))"
- filter => "(&(sn=Phillips) (ou=Employees))"
- filter => "(|(sn=Phillips) (sn=Pennebaker))"
- filter => "(&(sn=Phillips) (!l=Atlanta))"
- sizelimit => 10,

EXAMPLE Data returned

- Cn ==> [Mike Phillips]
- Manager ==> [emailaddress=mike_porter@hp.com, ou=Employees, o=hp.com]
- O ==> [Hewlett-Packard Company]
- Uid ==> [mike_e_phillips@hp.com]
- c ==> [US]
- emailaddress ==> [mike_e_phillips@hp.com]
- employeetype ==> [Active - Regular]
- givenname ==> [Michael E]
- hptelnetnumber ==> [643-8707]
- l ==> [Bellevue]
- mail ==> [mike_e_phillips@hp.com]
- modifiersname ==> [cn=ldaped applications,ou=applications,o=hp.com]
- modifytimestamp ==> [20001125234140Z]
- o ==> [Hewlett-Packard Company]
- sn ==> [Phillips]
- telephonenumber ==> [+1 (425) 643-8707]

LDAP programmatic Access (secure version)

- Install Netscape SDK (4.1 as of this writing)
 - NT gives you dk41x32s.exe
 - UX gives you <name>.tar.gz
- Unpack, and explore

SSL EXAMPLE config in C

- `char[] appDN = "cn=MyApp, ou=Applications, o=hp.com" ;`
- `char[] appPW = "SECRET99" ;`
- `#define HOST "ldap.hp.com"`
- `#define PORT 389`
- `#define SECURE_PORT 636`
- `#define BASE "o=hp.com"`
- `#define CERT_PATH "./cert7.db";`

- `char * answer,user_filter_;`

Secure Access Process

- `Ldapssl_client_init(CERT_PATH, NULL) //certificate stuff`
- `ld = ldapssl_init(HOST, SECURE_PORT, 1)`
- `ldap_simple_bind_s(ld, APP_DN, APP_PW)`
- `ldap_search_s(ld, BASE, LDAP_SCOPE_SUBTREE,`
- `user_filter_ptr, NULL, 0, & result)`
- `ldap_get_dn(ld, result);`
- `entry = ldap_next_entry(ld, result);`
- `for (a = ldap_first_attribute (ld, result, & ber) ;`
- `a != NULL ;`
- `a = ldap_next_attribute (ld, result, ber)) {`
- `if ((vals = ldap_get_values(ld, result, a))`
- `LOOP THRU ALL ATTRS ,and display name & value !!!`

Source Listings

- Ldap6b.pl
- Ntauth.c
- Uxauth.c

Footnotes/URLs

- RFC 2251: <http://www.landfield.com/rfc/rfc2251.html>
- Lots more LDAP resources : <http://www.linc-dev.com/ldapres.html>
- MSDN : <http://msdn.microsoft.com/library/default.asp>
- Microsoft ADO/ADSI LDAP 'how-to'
: <http://support.microsoft.com/support/kb/articles/q187/5/29.asp>
- LDAP CORE SPECS : <http://www3.innosoft.com/ldapworld/v3core.html>
- Historical References : <http://www.umich.edu/~dirsvcs/ldap/>
- An LDAP Roadmap : <http://www.kingsmountain.com/ldapRoadmap.shtml>
- Good Intro from Stanford
: <http://www.stanford.edu/~hodges/talks/mactivity.ldap.97/index2.html>
- Developer.com Links : <http://developer.earthweb.com/dlink.index-jhtml.72.950.-.0.jhtml/pages/dir.ldap.html>
- Netscape SDK Download page (1place)
: <http://www.ipplanet.com/downloads/developer/>
- Tutorial for LDAP : <http://idm.internet.com/foundation/ldap.shtm>
- X.500 and LDAP Standards : <http://www.kuleuven.ac.be/ludit/ic/node59>

Summary

- LDAP data model
- Where to get LDAP modules/libraries
- Template source code on website
 - Modify for your local needs
 - Learn more using the URLs or Search
- Request feedback of training session