Using LDAP & ICE to manage Novell eDirectory

Wylie Horn
OUCS
4 February 2005
Thanks

- Mike Weaver - Mindworks UK and Tenacious Integration Services (formerly University of Georgia)
- Luke Tracy - University of Michigan
- James Partridge (OUCS)
- Lyn Waddington (OUCS)
- Ian Atkin (OUCS)
Overview

• What is LDAP?
• LDAP fundamentals
• LDAP tools
• LDIF
• ICE
What is LDAP?

• Lightweight Directory Access Protocol
  • Based on Directory Access Protocol
  • Provides access to X.500 type directory trees (such as eDirectory)
  • No OSI stack, solely TCP (so light and fast)
• Developed at University of Michigan in the 1990’s
  • Now ratified by the Internet Engineering Task Force
LDAP fundamentals

- Names must be typeful, e.g. `cn=admin,o=oucs`
- Names must be distinguished
  - Fully distinguished. i.e., full containment to tree root
    - E.g. `cn=wylie,ou=staff,o=oucs`
    - Or relative `cn=wylie,ou=staff` in the context of the `o=oucs` base
More fundamentals

- Names are case insensitive
- Delimited with commas
- A fully distinguished name must be unique in the DIT
Novell’s LDAP

- Fully LDAP v3 compliant
- Based on Open standards
- Installed on NetWare by default
- Single NLM: NLDAP.nlm
LDAP tools

- Windows users
  - Command line tools available as part of the Novell LDAP SDK
  - Select “LDAP Classes for C - Netware and Windows”
  - Download all
  - Open clldap_all.exe at download location
LDAP Browsers & Tools

- Other useful LDAP tools on Novell Cool Solutions Site: [http://www.novell.com/coolsolutions/tools/](http://www.novell.com/coolsolutions/tools/)
Mac users

- Standard LDAP command line tools are incorporated into OSX: `ldapsearch`, `ldapmodify`, etc.

- Also see the Directory Service command line utility; for details type `man dscl` at an OSX terminal.
Linux users

• Download tools from http://www.openldap.org/software/download


• Unpack archive then use gcc to make the tools located in the /clients/tools directory
What can we do with the tools?

- Authenticate
- Query
  - Bind and unbind (anonymous or authenticated)
- Search
- Compare
What else can we do with the tools?

- Change Entries:
  - Modify
  - Add
  - Delete
  - ModDN
LDAP Data Interchange Format

- Begin with line: `version: 1`
- Comments are preceded by a `#`
- Records are delimited by empty lines
- All records must begin with: `<object’s DN>`:
- The dn must be fully distinguished
- Line breaks

---

```plaintext
version: 1
#
# Uploaded 01/08/2003 - Passed
# Verion: 1.0 01/08/2003 3:00 MST
#

dn: cn=schema
changetype: modify
add: objectclasses
objectclasses: ( 1.2.840.113556.1.3.23 NAME 'container' SUP top STRUCTURAL MUST ( cn )
X-NDS_CONTAINMENT ( 'country' 'organizationalUnit' 'locality' 'organization' 'domain' ) )

#
# User attributes 1.3.6.1.4.1.63.1000.1.1.1.1
#

dn: cn=schema
changetype: modify
add: attributeTypes
attributeTypes: ( 1.3.6.1.4.1.63.1000.1.1.1.6 NAME 'apple-user-homeurl' DESC 'home directory URL' EQUALITY caseExactIA5Match SUBSTR caseExactIA5SubstringsMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 SINGLE-VALUE )
```
LDIF

• Attributes are specified: `attribute_name: attribute_value`

• Lines may not exceed 76 characters in length (and must be folded if they are longer than 76 characters)

• Multi-valued attributes are listed as many times as needed to enumerate all values

• One attribute/value pair per line

• No blank lines are permitted in a record

• All lines must be fully left justified

• Non-ascii data must be base-64 encoded

• File:// urls may be used to reference binary content outside the LDIF file
Import Convert Export

• Novell’s Import Convert and Export tool
ICE command line demo

- Command line format is:
  - ice <general options>
  - -S <source handler> <source options>
  - -D <destination handler> <destination options>
C:\Novell\consoleone\1.2\bin>ice -S LDIF -f C:\ldifgen\michaelmas.1df -v -D LDAP -s dsdg1.oucs.ox.ac.uk -p 636 -d cn=wylie,o=oucs -w novell -v
ICE tips

- Schema mapping problems
- Change entry placement
- Add default attribute values for mandatory attributes
- Omit or Exclude Attributes (using the -o switch)
Speeding up LDIF Imports
(Source: “Using the Novell Import Convert Export Utility, Mclain, N and Harrison, R. Novell Appnotes 2000)

- Import to a server with a writeable replica
- Use LBURP (enabled by default in ICE)
- Configure database cache
- Use simple passwords
- Use indices appropriately
Potential problems

• SSL port 636
• Clear text port 389
• Forward references
• Search size and time limits
• Check syntax, try a limited sample first before running a large job
• Use the LDIF error file
References

- eDirectory developer documents
  - eDirectory Core Services
  - eDirectory Schema Reference
  - eDirectory Technical Overview
    - LDAP and NDS integration
    - Perl and LDAP
  - [http://ldap.perl.org](http://ldap.perl.org)
References

- This talk and links to various relevant articles and tids
  - http://users.ox.ac.uk/~wylie/talks/ldap