Open Source Open Training

LDAP Basics

Andrew Findlay
Skills 1st Ltd

November 2015

Course Overview

- Directory service basics
- LDAP data model
- LDAP service model
- Authentication with LDAP

Open Source Open Training

1: Directories and LDAP

Directories everywhere

- You look things up in them...
- The Phone Book (White Pages)
- Yellow Pages
- Business Directories
- DNS
- Google? No: unstructured data

Directory services need

- Standard network protocol
- Highly structured data
- Very fast search and read
- Ability to distribute data
- Ability to cache data
- Ability to replicate data

Directory service standards

- ECMA TR32 (1985)
- X.500: ISO/CCITT standard 1988/1993...
  - Data model
  - Directory Access Protocol
  - Directory System Protocol
  - X.509 Certificates for strong authentication
- LDAP: Internet RFCs 1993 onwards
  - RFC4510 (2006) is current master doc
  - 60+ relevant RFCs

LDAP Overview

- Lightweight Directory Access Protocol
- Based on X.500 / ISO9594
- Read-mostly datastore
- Replication, distributed data
- Standard *protocol* rather than *API*
- Tree of data - the *DIT*
- Attribute-value in nodes

Data model 1: entries

- An entry represents a person, organisation, room, printer...
- Attribute-value data:

  commonName: Dr A J Findlay

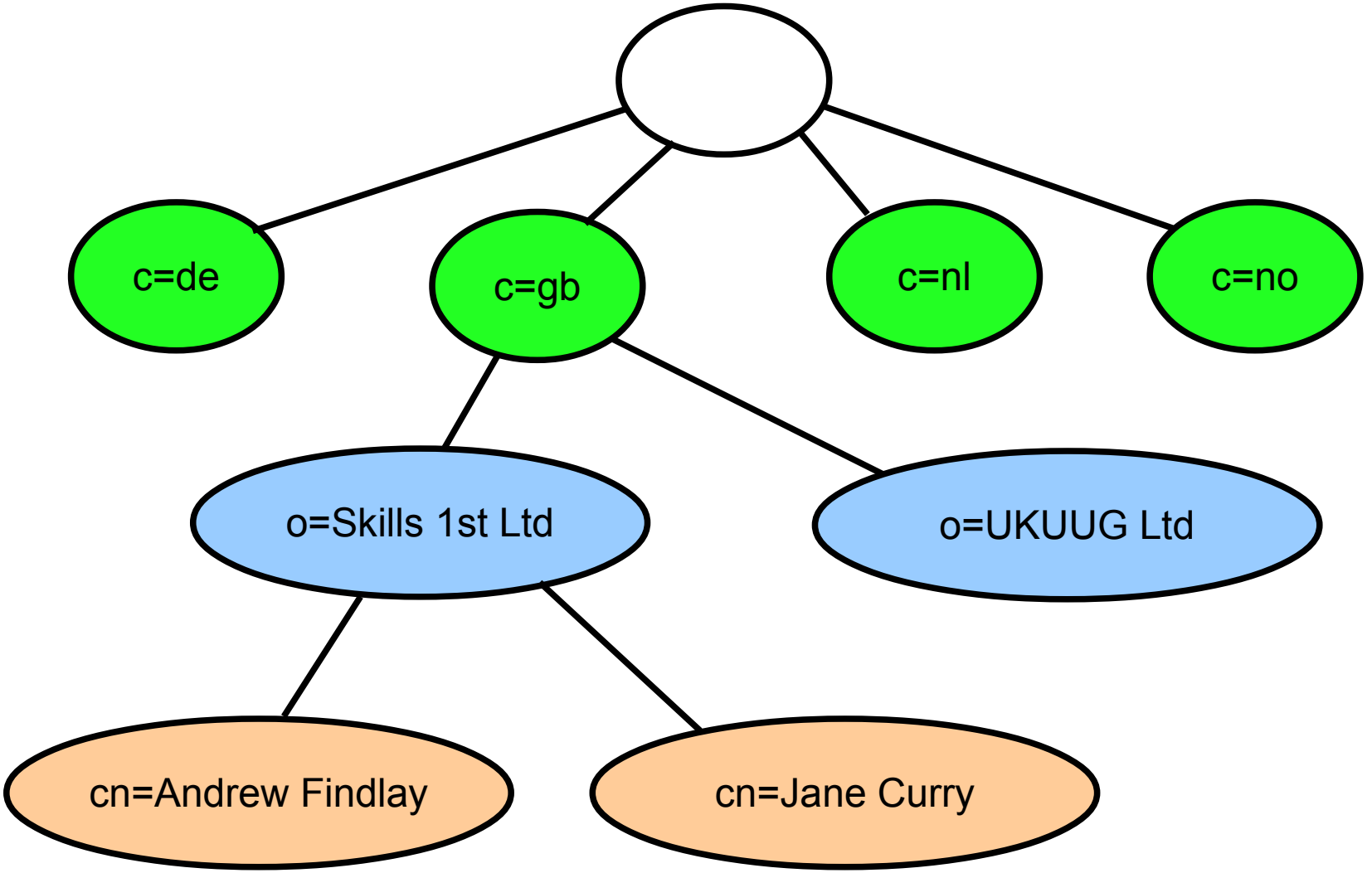
  commonName: Andrew Findlay

  surname: Findlay

  mail: andrew.findlay@skills-1st.co.uk

  telephoneNumber: +44 1628 782565

Data model 2: the DIT



Entry names

- Select one attribute-value pair
  - This becomes the RDN
- The full DN is the catenation of all entry names on the path up to the root
  - cn=J Smith,o=Big PLC,c=GB
- Potential for clashes
- Multi-valued RDNs are permitted
  - cn=J Smith+uid=js763,o=Big PLC,c=GB

Simple Search

- Specify:
  - A subtree to be searched
    `o=Skills 1st,c=gb`
  - A filter to match entries of interest
    `sn=Findlay`
    `cn=Andrew*`
- Get back:
  - Zero or more entries
  - Status

Exercise 1

- Login and explore
- Create LDAP Server
- Simple searches

Open Source Open Training

2: LDAP Data Definitions

Acronyms

- DSA – Directory System Agent
  - LDAP Server
- DUA – Directory User Agent
  - LDAP client library
- DIT – Directory Information Tree
- DN – Distinguished Name

Schema and other difficult words

- Attribute Type
- Syntax
- Matching Rule
- Object Class
- Inheritance
- OID

Inheritance

- X.500 and LDAP are object-oriented
- Things defined as 'like this, but with these extras'
- Inheritance indicated in schema by 'SUP' (superior)

Attribute types

- Names used to describe a type of data
  - cn, sn, mail, telephoneNumber ...
- Attribute definition includes:
  - name
  - OID
  - syntax
  - permitted matching rules
  - single-value flag

Attribute definition

- Varies from one server to another

```
attributetype ( 0.9.2342.19200300.100.1.5
  NAME ( 'drink' 'favouriteDrink' )
  DESC 'RFC1274: favorite drink'
  EQUALITY caseIgnoreMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{256}
)
attributetype ( 2.5.4.3
  NAME ('cn' 'commonName')
  DESC 'RFC2256: name of the entity'
  SUP name
)
```

Syntaxes

- Data-types
  - directoryString
  - DN
  - generalizedTime
  - IA5String
  - telephoneNumber
  - postalAddress
- Always referred to by OID
- Text almost always UTF-8

Matching Rules

- Operations to be used in searches
  - caseExactMatch
  - caseIgnoreMatch
  - caseIgnoreSubstringsMatch
  - caseIgnoreOrderingMatch
  - telephoneNumberMatch
  - Many more...
- Beware! Not all implemented!

Object classes

- Define the *type* of the entry
- List permitted and required attributes
- Three types:
  - Structural
  - Auxiliary
  - Abstract
- Inheritance is supported

Objectclass definitions

```
objectclass ( 2.5.6.6
   NAME 'person'
   DESC 'RFC2256: a person'
   SUP top STRUCTURAL
   MUST ( sn $ cn )
   MAY ( userPassword $
         telephoneNumber $ seeAlso $
         description )
)
```

Objectclass rules

- STRUCTURAL class of entry cannot be changed after creation
- Entry cannot inherit from two *different* structural classes
  - *person, organizationalPerson, inetOrgPerson* is OK
  - *inetOrgPerson, pilotPerson* is not

OIDs

- Object Identifier – a unique “name”
- X.500 uses these in protocol
- LDAP *prefers* human-readable names
- 0.9.2342.19200300.100.1.5
- Infinitely extendable
- Various registries and allocation rules
  - 1.2.826.0.1.<UK company number>

Data model summary

- Tree of entries – the DIT
- Attribute-value data in entries
- Schema rules define what can/must be present

Exercise 2

- Install GUI browser
- Browse DIT
- Simple searches
- Browse schema

Open Source Open Training

3: LDAP Operations

LDAP operations

- Bind
- Search
- Add
- Delete
- Modify
- Compare
- Abandon
- Extended

Bind

- Authenticates to the server
- “Simple”: DN and password
- SASL
  - userID and credentials
    - Kerberos
    - DIGEST_MD5
  - external (e.g. client certificate)

Search

- Base – specifies starting point in DIT
- Scope – how far to look
  - base object, single level, subtree
- Filter – what to look for
- Attribute list – what to return
- Options – limits on size, time etc

Search filter examples

- (sn=Smith)
- (cn=Andrew*)
- (cn=and*w*fi*y)
- (objectClass=*)
- (&(objectclass=acct)(uid=zb42))
- (&(objectclass=person)(|(cn=*fred*)(sn=*fred*)(drink=*fred*)))

Search results

- Zero or more entry names
- Possibly some attributes for each entry
- Status code
  - Success
  - Various failures
  - Size limit exceeded
  - Admin limit exceeded
- Operational attributes can be requested

Modify

- Add/delete/change attribute-value pairs
- Accepts a list of changes
- The only atomic operation
- Modify/replace whole attributes or specified values
  - To specify values there must be a matching rule for the attribute

Add

- Add one directory entry
- Entry must conform to schema
- Parent entry must exist

  (unless adding a suffix entry)
- Bulk adds usually start from LDIF file

LDIF

- LDAP Data Interchange Format
- RFC2849
- Transfer complete entries / subtrees
- Specify attribute-level modifications
- Delete entries
- Portable format
  - backup
  - data transfer between DSAs

LDIF Example

```
dn: dc=people,dc=example,dc=org
objectclass: organizationalUnit
objectclass: dcObject
ou: People
dc: people

dn: uid=qr00042,dc=people,dc=example,dc=org
objectclass: inetOrgPerson
objectclass: person
cn: Fiona Pinnington
sn: Pinnington
uid: qr00042
mail: qr00042@example.org
telephoneNumber: +44 1234 567000
userPassword: secret
```

Command-line tools

- One tool for each LDAP operation:
  - ldapsearch
  - ldapadd
  - ldapmodify
  - ldapdelete
  - ldappasswd
- All can bind as specified ID

Command-line examples

```
ldapsearch -x -b dc=example,dc=org \
      sn=smith

ldapsearch -x \
  -D cn=root,dc=example,dc=org \
  -w secret \
  -b dc=example,dc=org \
  -s sub \
  '(&(sn=smith)(mail=*@example.org))'

ldapadd -x \
  -D cn=root,dc=example,dc=org \
  -y file-with-password \
  -f data.ldif
```

Exercise 3

- Load data from LDIF
- Modify data from GUI

Open Source Open Training

4: Authentication and Authorisation

Authentication using LDAP

- Normal process:
  - Bind anonymously or with fixed ID
  - Search for user entry (uid=username)
  - Bind as that entry with supplied password
- Alternative:
  - Bind directly using SASL

Authorisation using LDAP

- Authorisation normally expressed as group membership
- LDAP group is an entry
- Members represented by DN values of *member* attribute

```
dn: cn=Web Editors,ou=groups,dc=example,dc=org
objectclass: groupOfNames
cn: Web Editors
member: uid=qr0042,dc=people,dc=example,dc=org
member: uid=xa0003,dc=people,dc=example,dc=org
```

POSIX passwd data in LDAP

- RFC2307

```
ajf:x:1234:1234:Andrew Findlay:/home/ajf:/bin/bash
```

```
objectclass: inetOrgPerson
objectclass: posixAccount
cn: Andrew Findlay
sn: Findlay
uid: ajf
uidNumber: 1234
gidNumber: 1234
homeDirectory: /home/ajf
gecos: Andrew Findlay
userPassword: {SSHA}MCbiTYMHrt6GSReXxZ6dHzNviiUEE/xR
```

POSIX group data in LDAP

- RFC2307

```
objectClass: posixGroup
cn: dialout
gidNumber: 16
memberUid: ajf
memberUid: bjc
memberUid: mtr
```

Exercise 4

- Simple authentication
- Groups using DNs
- Using RFC2307
  - Passwd data
  - Groups using UIDs

More LDAP Topics

- TLS
- Replication
- Distributed DIT
- DIT Design
- Access Control
- Client-side programming

Open Source Open Training

LDAP Basics

Andrew Findlay
Skills 1st Ltd

November 2015

andrew.findlay@skills-1st.co.uk

Creative Commons