LDAP

Lightweight Directory Access Protocol

A directory storage

AKA a DB

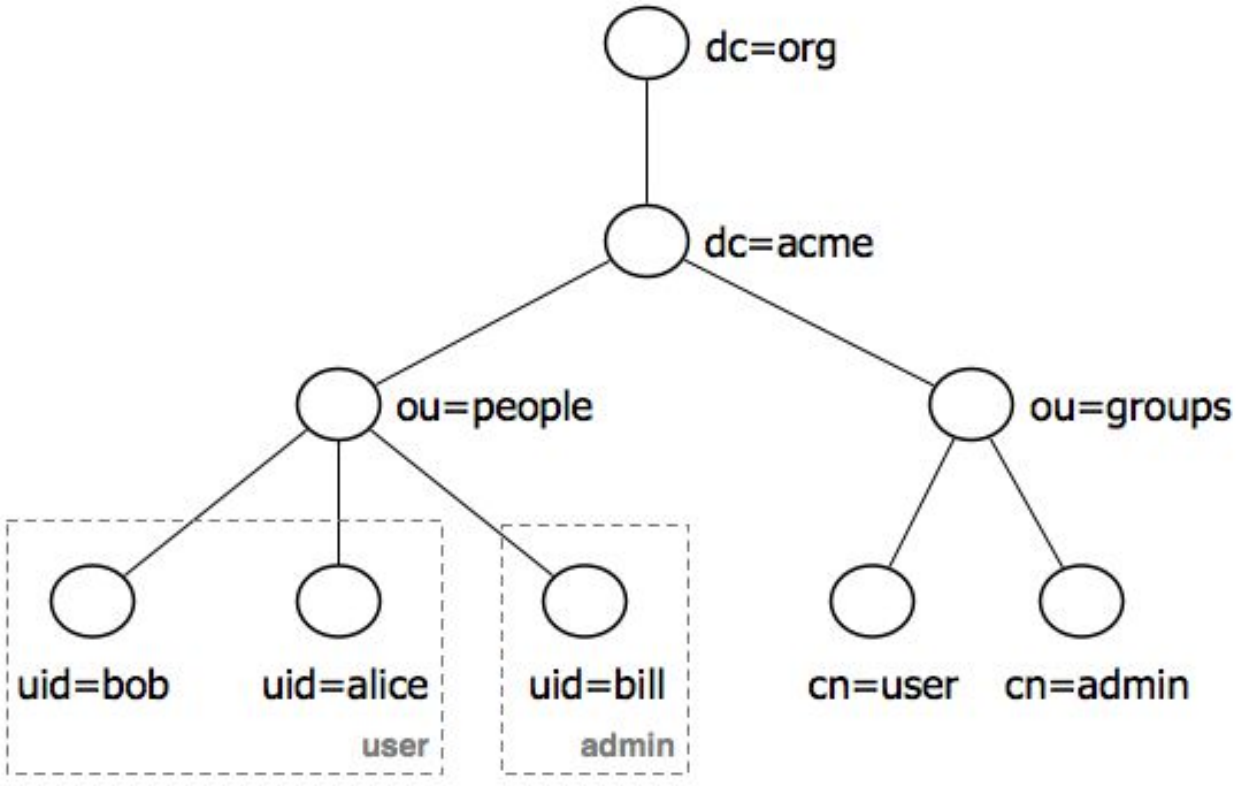
By Patrick Louis

In a few words

– – –

- Stores information in a central storage, accessible through standard protocol
- Based on the X.500 standard and RFC 2251
- Client/server model
- Hard terminology and abbreviations
- Usage
  - Identity management (AD: Active Directory)
  - DNS storage
  - Yellow page (phone number, addresses, departments)
  - Mail routing

What it looks like



Client/Server Model

– – –

- Client binds (authentication)
- The server restricts access to a specific part of the tree and attributes
- The client can query/search the server and do operations (CRUD)
- LDAP variations
  - Ldap (basic)
  - Ldaps (SSL/TLS)
  - Ldapi (local over IPC)

Example Implementations

– – –

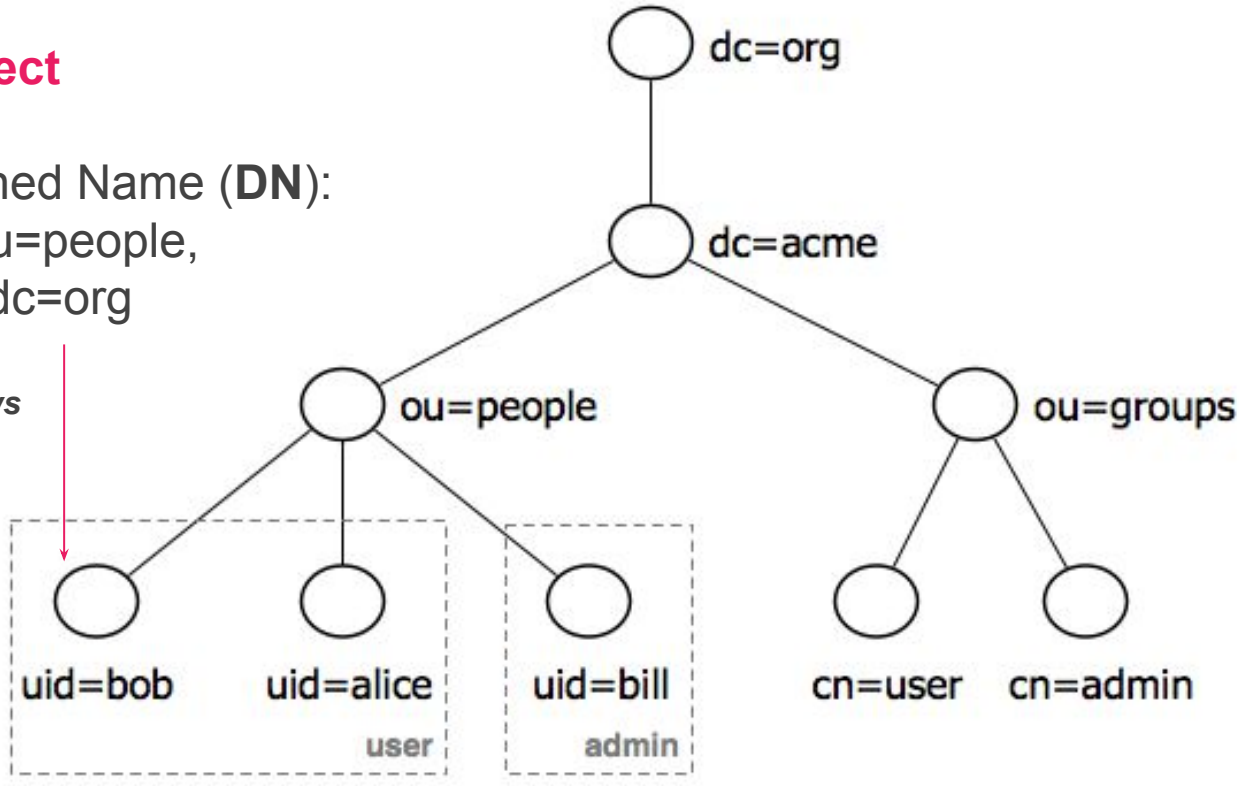
- OpenLDAP, an open source LDAP suite
- Samba
- Microsoft Active Directory
- 389 Directory Server
- IBM Security Directory Server
- NetIQ eDirectory

Terminology

Entry/Object

Distinguished Name (**DN**):
uid=bob,ou=people,
dc=acme,dc=org

RDB equiv: ***rows***



Terminology

– – –

Attribute

Within the Entry/Object

dn: uid=bob,ou=people, dc=acme,dc=org
objectClass: person # special meaning (specifies mandatory attributes in schema)
sn: Pat
cn: Patrick
email: patrick@example.com

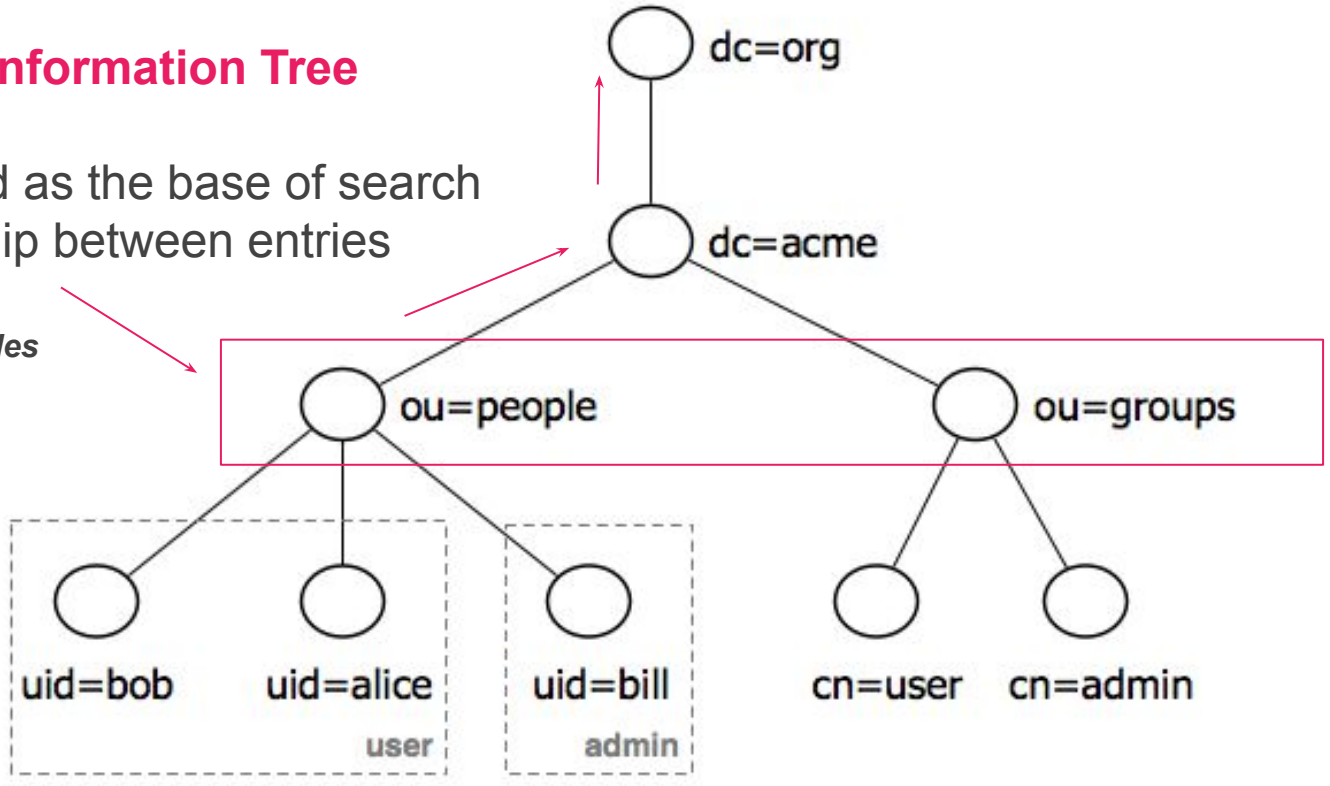
RDB equiv: ***columns***

Terminology

DIT/Data Information Tree

Often used as the base of search
Relationship between entries

RDB equiv: ***tables***



Terminology

– – –

Schema

The definition of the object classes, their inheritance, attribute types, rules for search (ex: case-sensitive or not), and the overall shape of the tree.

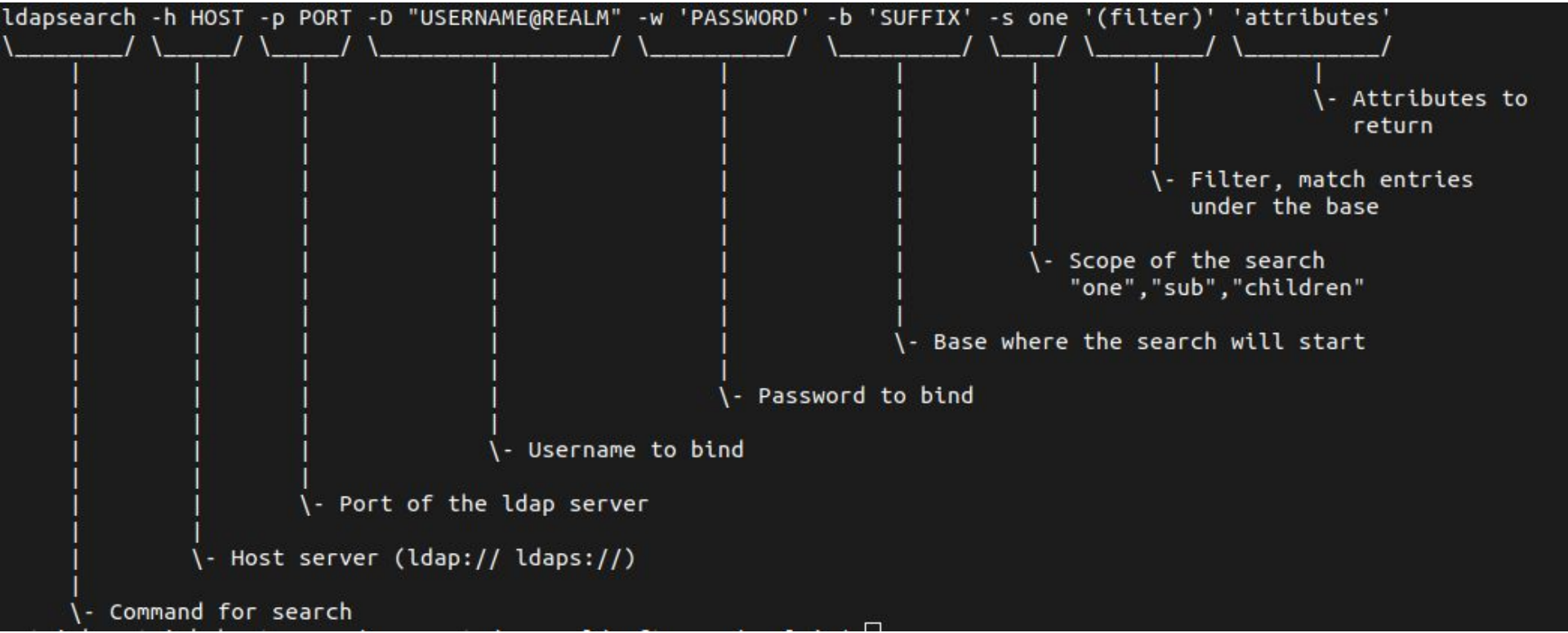
RDB equiv: ***schema***

Terminology

– – –

- DN = Distinguished Name
- CN = Common Name
- OU = Organizational Unit
- DC = Domain Component (domain name)
- SN = Surname

Anatomy of a search



Search criteria/Filter (RPN)

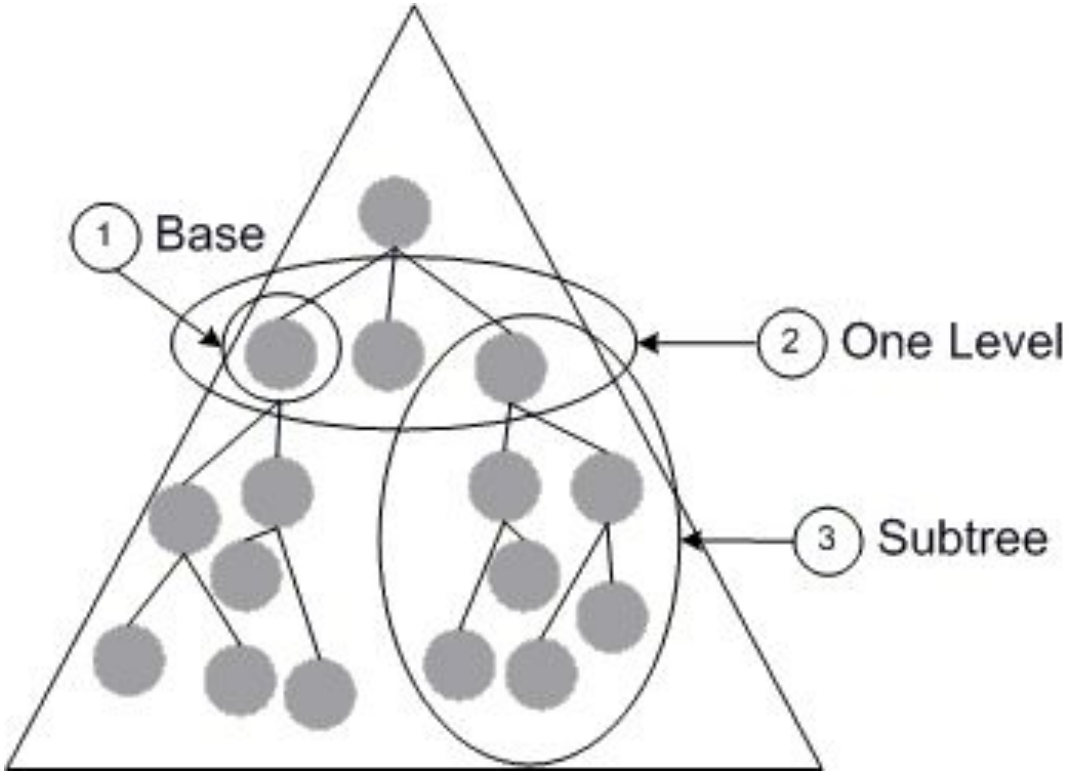
Operator	Meaning
&	AND, all conditions must be met
|	OR, any of the conditions must be met
!	NOT, the clause must evaluate to False

(objectClass=*)	All objects.
(&(objectCategory=person)(objectClass=user)(!(cn=andy)))	All user objects but "andy".
(sn=sm*)	All objects with a surname that starts with "sm".
(&(objectCategory=person)(objectClass=contact)(|(sn=Smith)(sn=Johnson)))	All contacts with a surname equal to "Smith" or "Johnson".

Search Scope

– – –

-s option in **ldapsearch**
Values:
{base|one|sub|children}
Default is sub



Common Search in AD

We bind with the user, this depends on implementation

`Search for objectClass=person` or `objectClass=user` entry containing that user's info under the base, they should have access to their own info

Possible filters:
`userPrincipalName=username@domain.principal` — the logon name for the user
`sAMAccountName=username` — a logon name that supports previous version of Windows

Get attribute memberOf either through just the list return or search for textual name of group through filter
`(&(objectClass=group)(cn=...))`

Local AD setup and demo

- Install samba winbind libpam-winbind libnss-winbind
- Disable everything samba and use samba-ad-dc only
- Edit `/etc/samba/smb.conf` to set `REALM` and disable strong auth
- Use `samba-tool` to create users and groups
- Then usual ldapsearch commands should work

```
ldapsearch -H 'ldap://127.0.0.1:389' -s one -D "testuser@PATRICKLOUIS.LAN" -w
'admin!!11'  -b 'CN=Users,DC=patricklouis,DC=lan' '(sAMAccountName=testuser)'
'objectClass' 'cn' 'name' '*'
```

Other info

- LDIF (LDAP Data Interchange Format)
- Object class definitions
- Openldap (slapd and slurpd)

```
dn: cn=Barbara Jensen,dc=example,dc=com
objectClass: person
cn: Barbara Jensen
cn: Babs Jensen
sn: Jensen
title: the world's most famous mythical manager
mail: bjensen@example.com
uid: bjensen

the command:

ldapadd -f /tmp/newentry
```

```
dn: cn=Modify Me,dc=example,dc=com
changetype: modify
replace: mail
mail: modme@example.com
-
add: title
title: Grand Poobah
-
add: jpegPhoto
jpegPhoto:< file:///tmp/modme.jpeg
-
delete: description
-

the command:

ldapmodify -f /tmp/entrymods
```

Thx

Questions?

By Patrick Louis