LDAP

LDAP for Rocket Scientists

LDAP DIT - LDAP **D**irectory **I**nformation **T**ree

distinguished name

LDAP DNs and RDNs

- **DN** - distinguished name - full path of the object in the tree. Uniquely identifies an entry and describes its position. I.e *“uid=john.doe,ou=People,dc=example,dc=com”*
  - **DN**s are comprised of zero or more comma-separated components called **relative** distinguished names, or **RDN**s.
  - For example, the DN *“uid=john.doe,ou=People,dc=example,dc=com”* has four RDNs:
    - uid=john.doe
    - ou=People
    - dc=example
    - dc=com
  - DNs are case insensitive)
- **RDN** - is relative to its parent

Example DNs:

- *“uid=john.doe,ou=People,dc=example,dc=com”*
- *“cn=John Doe+telephoneNumber=+1 123-456-7890”* - to distinguish between more people named “John Doe”
- *””* - empty is also valid - NULL DN references special entry called **root DSE** (server data)
- *““dc=example,dc=com”*
- ~~*“dc=com”*~~ - the DN of top entry is a “naming context” or “suffix”

The same DN:

- *dc=example,dc=com*
- *dc=example, dc=com*
- *dc = example , dc = com*
- *DC=EXAMPLE,DC=COM*
- *0.9.2342.19200300.100.1.25=Example,0.9.2342.19200300.100.1.25=Com*

DN Components

- **dc** - domain component dc=company,dc=org (domain is **company.org**)
- **ou** - organization unit (ou=
- **cn** - common name (i.e. “John Smith”)
- **displayName** - one line summary (for people can be the same as **cn**)

objectClassess

Are predefined containers for **attributes**. For example OpenLDAP's “Generic: User Account” assigns **“inetOrgPerson”** class.

- inetOrgPerson
  - **cn**, **sn** - as required attributes
  - lots of optional attributes like: “photo”, “displayName”, “uid”, “postalCode”, “telephoneNumber”

common attributes

And container classes:

- cn,sn (inetOrgPerson)
- mail=rfc822Mailbox (inetOrgPerson)
- uid=userid (inetOrgPerson)
- userPassword (person, posixAccount, simpleSecurityObject)
  - hash: SSHA
- displayName (inetOrgPerson)

Structure design

- Unique name for each entry
  - **cn** collisions. Two people may have the same first and last name. Grouping under different parent is necessary (**ou**).
  - user can belong only to one **ou**.
- Stability of structure, but **people can change**:
  - names - Do not rename entries, use some unique id like serial number. I.e. *“uid=00003,ou=People, dc=example, dc=com”*.
  - position - departments - do not put users under specific departments (deep tree), better is to put it into one group and then use a attribute

to structurize and group users.

- security - separate some information by grouping it under another **ou**

http://www.ldapman.org/articles/tree_design.html

Example structure

- dc=company,dc=org
  - ou=people

        - uid=jdoe
            - cn=John Doe
            - cn=Johny
            - sn=Doe
            - mail=john.doe@company.org
            - mail=j.doe@company.org
        - uid=jblack
            - cn=Joe Black
            - sn=Black
            - ou=software
    - ou=software
    - ou=customers
        - cn=Google
        - cn=Wurth
    - ou=devices
    - ou=it
        - uid=nextcloudsystemuser,cn=nextcloudsystemuser,userPassword=…
        - root,www ,etc
    - ou=location
        - conference rooms location and phones, company address, etc