

LDAP på RUC

Finn Dorph-Petersen
&
Mads Freek Petersen

sslug 11. marts 2003

Program

- kort intro til LDAP
- LDAP og Linux på RUC
- LDAP og andre systemer på RUC

Kort intro til LDAP

- LDAP info struktur
- Søge sprog/filtre
- Udvekslingsformat
- Servere, værktøjer og biblioteker

• Letvægts telefonbogs tilgangs protokol

- A book containing an alphabetical or classified listing of names, addresses, and other data, such as telephone numbers, of specific persons, groups, or firms.

• Meget læsning - lidt skrivning

• Eneste standard on-the-wire db protokol incl. c-api, søgesprog, tekst db format

• "Binær" protokol - ikke som smtp et al.

• Erstatning for nis, netinfo ...

- Hierarkisk opbygget - à la dns - men kan have flere navnerum på hvert niveau
- "Stien" til en post kaldes "distinguished name"
DN
- Moderne navngivning - brug dns navnet - domain component dc fx:
dn: uid=freek,ou=users,dc=ruc,dc=dk

Poster med repeterende felter

```
dn: uid=freek,ou=users,dc=ruc,dc=dk
objectClass: rndentry
cn: Mads Freek Petersen
title:: SW5nZW5pw7hy
department: Datalogidrift
mail: freek@ruc.dk
forward: freek@imap.ruc.dk
group: BSCW-allow
group: DATCAL-allow
house: 42.1
labeledURI: http://akira.ruc.dk/~freek
office: 42.1.06
postalAddress: 42.1
rndid: 516
serialNumber: 4
telephoneNumber: 4674-3882
uid: freek
userPassword: {SSHA}fVRB6UcelrVducrhHahLcK2OpGrqEVTZ
x: Datalogidrift
x: Mads
x: Freek
x: Petersen
x: 3882
```

```
attributetype ( 1.3.6.1.4.1.9223.1.2.19
  NAME 'x'
  EQUALITY caseIgnoreMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{256} )
```

```
objectclass (1.3.6.1.4.1.9223.1.1.1 NAME 'rndentry' SUP top STRUCTURAL
  MUST (uid)
  MAY (rndid $ x $ cn $ gn $ sn $ mail $ forward $
    telephoneNumber $ fax $mobile $
    house $ office $ postalAddress $ homepage $
    title $ education $ function $ ou $ department $
    ppp $type $ comment $ userPassword $ invisible $ inactive $
    vacationMessage $vacationForward $ vacationInterval $
    labeledURI $ group $ serialNumber) )
```

456 apple.schema
23 autofs.schema
162 collective.schema
222 corba.schema
535 core.schema
2558 cosine.schema
142 inetorgperson.schema
388 java.schema
134 krb5-kdc.schema
5383 microsoft.ext.schema
4835 microsoft.schema
480 microsoft.std.schema
59 misc.schema
178 nadf.schema
183 netinfo.schema
209 nis.schema
40 openldap.schema
138 rnd.schema

Operationer

- Søge / Læse attributter
- Modificere/tilføje/fjerne attributter
- Tilføje/fjerne objekter
- Ændre navn dn
- Identificere - binde

Søgesprog / Filtre

- Lighed - (attr=værdi)
- Approx - (attr~værdi)
- Trunkering - (attr=*væ*rdi*)
- Større/mindre end - (attr>værdi)
(attr<værdi)
- Eksistens - (attr=*)

Kan Kombineres med boolske operatorer

- Og - (<filter1>(<filter2>)...)
- Eller - (|(<filter1>(<filter2>)...)
- Ikke - (!(<filter>))

Tekst rep. statistisk / ændringer

Ldap Data Interchange Format (LDIF)

Delete an existing entry

```
dn: cn=Robert Jensen, ou=Marketing, dc=airius, dc=com
changetype: delete
```

Modify an entry's relative distinguished name

```
dn: cn=Paul Jensen, ou=Product Development, dc=airius, dc=com
changetype: modrdn
newrdn: cn=Paula Jensen
deleteoldrdn: 1
```

Rename an entry and move all of its children to a new location in
the directory tree (only implemented by LDAPv3 servers).

```
dn: ou=PD Accountants, ou=Product Development, dc=airius, dc=com
changetype: modrdn
newrdn: ou=Product Development Accountants
deleteoldrdn: 0
newsuperior: ou=Accounting, dc=airius, dc=com
```

Tekst rep. statistisk / ændringer

Ldap Data Interchange Format (LDIF)

```
# # Modify an entry: add an additional value to the postaladdress
# attribute, completely delete the description attribute, replace
# the telephonenumber attribute with two values, and delete a specific
# value from the facsimiletelephonenumber attribute
dn: cn=Paula Jensen, ou=Product Development, dc=airius, dc=com
changetype: modify
add: postaladdress
postaladdress: 123 Anystreet $ Sunnyvale, CA $ 94086
-
delete: description
-
replace: telephonenumber
telephonenumber: +1 408 555 1234
telephonenumber: +1 408 555 5678
-
delete: facsimiletelephonenumber
facsimiletelephonenumber: +1 408 555 9876
-
replace: postaladdress
-
```

Servere

OpenLDAP (open source)

iPlanet Directory Server

Novel Directory Services (eDirectory)

MS Active Directory

Oracle Internet Directory

IBM Directory Server

Innosoft IDDS

Critical Path Global Directory Server

Siemens DirX

OctetString Directory Server Express (java baseret)

Biblioteker og værktøjer

- C biblioteker med serverne
- Java
 - mozillas
 - novells (via openldap)
 - Sun (via JNDI)
- Perl
 - Net::LDAP "native perl"
 - + interface til c-bibs ...
- Ruby, Python, Tcl ???

Værktøjer

- Openldap cmdline:
 - ldapsearch, ldapmodify, ldapadd, slapdadd, slapppasswd, slapd, slurpd
- Diverse webbaserede: eL DAPo ...
- Grafiske java: seneca verisignlabs, LDAP browser/editor

For at kunne logge på en Linux klient er det nødvendigt med nogle oplysninger.

I vores tilfælde skal der bruges følgende:

- brugernavn
- kodeord
- uid
- gid
- grupper
- automountmap
- homeDirectory
- loginShell

Disse oplysninger hentes via ldap

Det er skal gøre på klient er meget simpelt.

Start altid med at kontroller at det er muligt at få ALLE de relevante oplysninger fra ldap. Først da er det tid til at lege med login opsætningen.

```
ldapsearch -x -b ou=users,ou=cs,ou=unix,dc=ruc,dc=dk  
-H ldap://smtp3.ruc.dk:3891 -ZZ '(uid=finnd)'
```

```
        dn: uid=finnd,ou=users,ou=cs,ou=unix,dc=ruc,dc=dk  
        uid: finnd  
        cn: finnd  
        objectClass: posixAccount  
        objectClass: top  
        objectClass: shadowAccount  
shadowLastChange: 11484  
        shadowMax: 99999  
shadowWarning: 7  
        userPassword: {SSHA}cKEULcmByIth5J7B0nsL05kwik2i235h  
                    (Denne bliver IKKE vist)  
        loginShell: /bin/bash  
        uidNumber: 1003013  
        gidNumber: 1003013  
homeDirectory: /home/remote/finnd
```

Gruppe information

```
dn: cn=finnd,ou=group,ou=cs,ou=unix,dc=ruc,dc=dk
objectClass: posixGroup
objectClass: top
        cn: finnd
        gidNumber: 1003013
        memberUid: finnd
```

Automount information

```
dn: ou=auto.master,ou=cs,ou=unix,dc=ruc,dc=dk
objectClass: top
objectClass: automountMap
ou: auto.master
```

```
dn: ou=auto.home,ou=cs,ou=unix,dc=ruc,dc=dk
objectClass: top
objectClass: automountMap
ou: auto.home
```

Automount information (Forsat)

```
ldapsearch -x -b ou=users,ou=cs,ou=unix,dc=ruc,dc=dk  
-H ldap://smtp3.ruc.dk:3891 -ZZ '(uid=finnd)'
```

```
dn: cn=finnd,ou=auto.home,ou=cs,ou=unix,dc=ruc,dc=dk  
objectClass: automount  
cn: finnd  
automountInformation: hibbert.ruc.dk:/home/remote/finnd
```

Nu har vi set at alle de nødvendige oplysninger er tilgængelige.

Så er det tid til at lege med config filer.

Godt råd:

Husk altid at have mindst en reserve root shell. Der kan let blive brug for den.

Der skal kun rettes i 4 filer.

/etc/exports (ufarlige)

/etc/ldap.conf (ufarlige)

/etc/pam.d/system-auth (farlige)

/etc/nsswitch.conf (farlige)

Export hjemme kataloger fra fil serveren

```
/etc/exports
```

```
/home/remote *.ruc.dk(rw,insecure)
```

De 3 sidste config filer er alle på klienten.

Klienten bruger automount via ldap til automatisk munte brugernes hjemmekataloger.

```
/etc/ldap.conf
```

Små forskelle imellem distributionerne.

```
/etc/pam_ldap.conf (Debian)
```

```
/etc/ldap.conf (Redhat)
```

```
ldap.conf / pam_ldap.conf
```

```
ssl start_tls
```

```
HOST smtp3.ruc.dk:3891 g4-freek.ruc.dk:3891
```

```
smtp3.ruc.dk:3892
```

```
BASE ou=cs,ou=unix,dc=ruc,dc=dk
```

Der er normalt rigtigt meget ballade med at få SSL til at fungere.

```
/etc/pam.d/system-auth
```

PAM (Pluggable Authentication Modules) er ansvarlige for kontrolere at det er en lovlige bruger med et lovligt kodeord plus et par andre små ting.

Det kan anbefales at finde en services som f.eks. ftp og så starte med at få det til at fungere med dennes pam fil.

F.eks. /etc/pam.d/ftpd

/etc/pam.d/system-auth

##PAM-1.0

This file is auto-generated.

User changes will be destroyed the next time authconfig is run.

auth required /lib/security/pam_env.so

auth sufficient /lib/security/pam_unix.so likeauth

nullok

auth sufficient /lib/security/pam_ldap.so

use_first_pass

auth required /lib/security/pam_deny.so

account required /lib/security/pam_unix.so

account [default=ok user_unknown=ignore service_err=ignore system_err=ignore] /lib/security/pam_ldap.so

password required /lib/security/pam_cracklib.so retry=3

password sufficient /lib/security/pam_unix.so nullok

use_authtok

md5 shadow

password sufficient /lib/security/pam_ldap.so use_authtok

password required /lib/security/pam_deny.so

session required /lib/security/pam_limits.so

session required /lib/security/pam_unix.so

session optional /lib/security/pam_ldap.so

```
/etc/nsswitch.conf
```

nsswitch.conf (System Databases and Name Service Switch configuration file)

Er ansvarlige for at oversætte fra tal til navne.

Hvis man laver rod her så kan det give problemer med at logge ind.

/etc/nsswitch.conf

```
passwd:      files nisplus ldap
shadow:     files nisplus ldap
group:      files nisplus ldap

hosts:      files nisplus dns

bootparams: nisplus [NOTFOUND=return] files

ethers:     files
netmasks:  files
networks:   files
protocols:  files nisplus ldap
rpc:       files
services:   files nisplus ldap

netgroup:   files nisplus ldap

publickey:  nisplus

automount:  files nisplus ldap
```

slapd.conf

```
include          schema/core.schema.default
include          schema/rnd.schema (normalt vil dette være core.schema)
include          schema/nis.schema
include          schema/autofs.schema

TLSCipherSuite  HIGH:MEDIUM:+SSLv2
TLSCertificateKeyFile  certs/smtp3.ruc.dk.key.pem
TLSCertificateFile    certs/smtp3.ruc.dk.cert.pem
TLSVerifyClient  never

access to attrs=userPassword
                by ssf=112 auth
                by * none

access to dn=".*,ou=cs,ou=unix,dc=ruc,dc=dk"
                by peername="IP=a.b.c.d" read
                by * none

# read by clients on dat net + signon.ruc.dk + g4-freek.ruc.dk,
# buzz.ruc.dk and kimms g4
# and hibberts giganet interface
pidfile         ldap-unix/slapd.pid
argsfile        ldap-unix/slapd.args
```

slapd.conf fortsat ...

```
#####  
# ldbm database definitions  
#####  
database            ldbm  
suffix              "ou=unix,dc=ruc,dc=dk"  
cachesize           1000  
dbcachesize         10000  
rootdn              "cn=root,ou=unix,dc=ruc,dc=dk"  
sizelimit           25  
rootpw              {SSHA}secret  
directory           ldap-unix/slapd.db  
index default eq,sub  
index cn,uid  
index memberUid,uidNumber,gidNumber eq  
index objectClass eq,pres
```

```
perl user2ldif.pl  
| cat newldapdb2.pl -  
| ssh ldap@smtp3.ruc.dk perl - --scheme=ldap-unix  
  --job=newdb --host=smtp3.ruc.dk
```