



Priprema za laboratorijsku vježbu iz imeničkih servisa

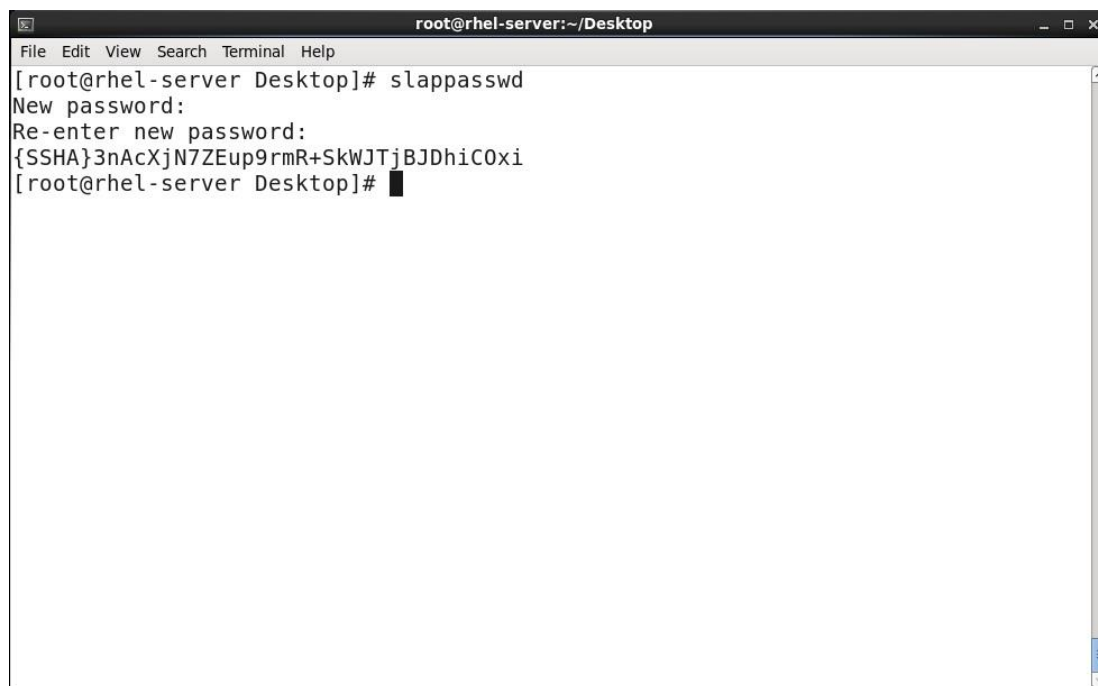
Konfiguracija openLDAP servera i klijenta

1. Konfiguracija openLDAP servera

Prije svega, otrebno je napraviti instalaciju paketa, što ćemo napraviti koristeći komandu:

```
yum install -y openldap-servers openldap-clients nss-pam-ldapd mlocate rsync vim sudo perl-  
LDAP migrationtools pam_ldap
```

Nakon toga, potrebno je napraviti lozinku koji ćemo koristiti za administraciju openLDAP servera. To ćemo napraviti sa komandom `slappasswd`, upisujući dva puta lozinku. U primjeru na slici za lozinku je korištena riječ "centos123":



Slika 1. Kreiranje lozinke za administraciju openLDAP servera

U slijedećem koraku potrebno je podesiti konfiguracijske datoteke od openLDAP server. Prvi korak je popravljjanje datoteke `/etc/openldap/slapd.d/cn=config/olcDatabase={2}bdb.ldif`, gdje ćemo na mjesto `dc=my-domain,dc=com` postaviti `dc=example,dc=com` pošto je `example.com` openLDAP domena sa kojom ćemo raditi. Dakle, u dvije konfiguracijske linije potrebno je samo `dc=my-domain,dc=com` promijeniti u `dc=example,dc=com` (konfiguracijska linija `olcSuffix: dc=my-domain,dc=com` i `olcRootDN: cn=Manager,dc=my-domain,dc=com`). Također, na kraj konfiguracijske datoteke potrebno je dodati:

```
olcRootPW:{SSHA}3nAcXjN7ZEup9rmR+SkWJTjBJDhiCOxi  
olcTLSCertificateFile: /etc/pki/tls/certs/certifikat.pem  
olcTLSCertificateKeyFile: /etc/pki/tls/certs/kljuc.pem
```

U prvoj konfiguracijskoj liniji (`olcRootPW`) potrebno je nakon `{SSHA}` copy-pasteati lozinku koju smo dobili korištenjem komande `slappasswd`. Druge dvije se odnose na certifikate koji su nam potrebni za sigurnost korištenja openLDAP-a kao autentifikacijskog sustava.

Nakon toga, potrebno je istu proceduru ponoviti i u datoteci `/etc/openldap/slapd.d/cn=config/olcDatabase={1}monitor.ldif` (zamijeniti `my-domain` sa `example`). Također, pošto i prva konfiguracijska datoteka spominje account koji se zove Manager (sa velikim slovom "M"), promijeniti ćemo i "manager" u "Manager" u istoj konfiguracijskoj liniji gdje smo promijenili i `my-domain` u `example`.



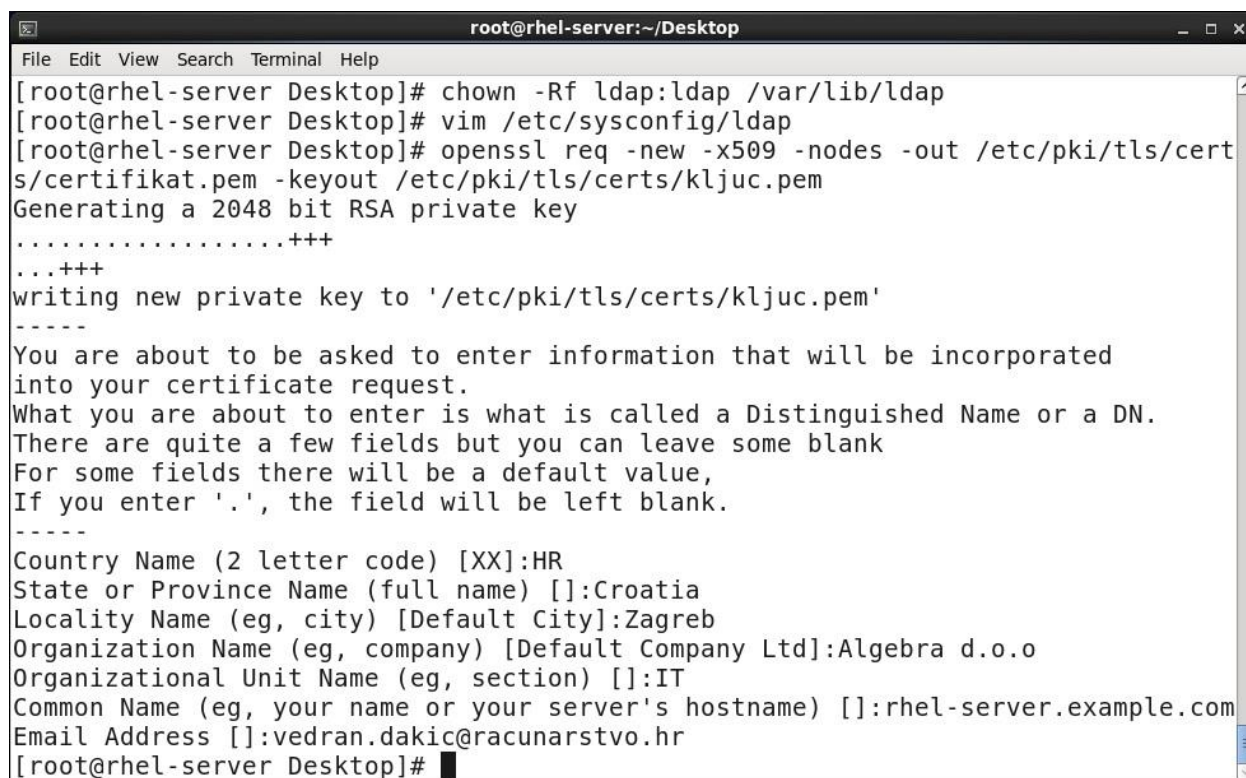
U sljedećem koraku, potrebno je napraviti inicijalnu konfiguraciju openLDAP servisa i autentifikacijskog sustava. To ćemo postići sljedećim komandama:

```
cp /usr/share/openldap-servers/DB_CONFIG.example /var/lib/ldap/DB_CONFIG
chown -Rf ldap:ldap /var/lib/ldap/
```

U datoteci /etc/sysconfig/ldap, potrebno je opciju SLAPD_LDAPS=no promijeniti u. SLAPD_LDAPS=yes. Nakon toga, potrebno je generirati certifikate i napraviti potrebnu konfiguraciju da bi openLDAP server mogao pročitati sve potrebne datoteke:

```
openssl req -new -x509 -nodes -out /etc/pki/tls/certs/certifikat.pem -keyout
/etc/pki/tls/certs/kljuc.pem -days 3650
```

Proces izrade certifikata izgleda ovako:



```
root@rhel-server:~/Desktop
File Edit View Search Terminal Help
[root@rhel-server Desktop]# chown -Rf ldap:ldap /var/lib/ldap
[root@rhel-server Desktop]# vim /etc/sysconfig/ldap
[root@rhel-server Desktop]# openssl req -new -x509 -nodes -out /etc/pki/tls/cert
s/certifikat.pem -keyout /etc/pki/tls/certs/kljuc.pem
Generating a 2048 bit RSA private key
.....+++
...+++
writing new private key to '/etc/pki/tls/certs/kljuc.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:HR
State or Province Name (full name) []:Croatia
Locality Name (eg, city) [Default City]:Zagreb
Organization Name (eg, company) [Default Company Ltd]:Algebra d.o.o
Organizational Unit Name (eg, section) []:IT
Common Name (eg, your name or your server's hostname) []:rhel-server.example.com
Email Address []:vedran.dakic@racunarstvo.hr
[root@rhel-server Desktop]#
```

Slika 2. Izrada certifikata za openLDAP server

Pripazite da za common name **obavezno** iskoristite ime server na kojem trenutno radite, a to je rhel-server.example.com.

Nakon generacije certifikata, potrebno je napraviti završni dio konfiguracije openLDAP server, podesiti dozvole, testirati konfiguracijske datoteke i startati servis, što ćemo obaviti sljedećim komandama:

```
chown -Rf root:ldap /etc/pki/tls/certs/certifikat.pem
chmod -Rf 750 /etc/pki/tls/certs/kljuc.pem
slaptest -u
chkconfig slapd on
service slapd start
```

Završnu konfiguraciju potrebno je obaviti u datoteci /etc/openldap/ldap.conf, gdje ćemo dodati sljedeće opcije komentirajući sve druge:

```
TLS_CACERTDIR /etc/pki/tls/certs
TLS_CACERT /etc/pki/tls/certs/slapd_cert.pem
URI ldap://127.0.0.1
BASE dc=example,dc=com
```

Time smo završili konfiguraciju openLDAP servera. Sada je još potrebno u openLDAP server dodati korisnike, grupe i slične podatke, kao što bismo to napravili i u Active Directoryu. To možemo napraviti komandama ili učitavanjem unaprijed pripremljenih datoteka. Zbog jednostavnosti, koristiti ćemo unaprijed napravljene datoteke.

Prvo ćemo napraviti datoteku /etc/openldap/schema/base.ldif, slijedećeg sadržaja:

```
dn: dc=example,dc=com
dc: example
objectClass: top
objectClass: domain
```

-

```
dn: ou=Users,dc=example,dc=com
ou: Users
objectClass: top
objectClass: organizationalUnit
```

Time ćemo napraviti domenu example.com sa pripadajućim OU-om imena Users.

Nakon toga, napraviti ćemo datoteku /etc/openldap/schema/base2.ldif, slijedećeg sadržaja:

```
dn: ou=Groups,dc=example,dc=com
ou: Groups
objectClass: top
objectClass: organizationalUnit
```

Time smo napravili OU imena Groups.

Slijedeća datoteka koju ćemo napraviti je /etc/openldap/schema/group.ldif, u kojoj ćemo definirati Manager grupu:

```
dn: cn=Manager,ou=Groups,dc=example,dc=com
objectClass: posixGroup
objectClass: top
cn: admin
gidNumber: 999
```

I za kraj, dodati ćemo admin korisnika kreirajući datoteku /etc/openldap/schema/users.ldif, sadržaja:

```
dn: uid=admin,ou=Users,dc=example,dc=com
uid: admin
cn: admin
objectClass: account
objectClass: posixAccount
objectClass: top
objectClass: shadowAccount
userPassword: password
shadowLastChange: 15140
shadowMin: 0
shadowMax: 99999
shadowWarning: 7
loginShell: /bin/bash
uidNumber: 999
gidNumber: 999
homeDirectory: /home/ldap
```

Završili smo kreiranje ldif datoteka iz kojih ćemo importirati sve potrebne podatke za početak rada. To ćemo ostvariti korištenjem komandi:

```
ldapadd -x -W -D "cn=Manager,dc=example,dc=com" -f /etc/openldap/schema/base.ldif
ldapadd -x -W -D "cn=Manager,dc=example,dc=com" -f /etc/openldap/schema/base2.ldif
ldapadd -x -W -D "cn=Manager,dc=example,dc=com" -f /etc/openldap/schema/group.ldif
ldapadd -x -W -D "cn=Manager,dc=example,dc=com" -f /etc/openldap/schema/users.ldif
```

Korištenjem ovih komandi, importirali smo podatke u openLDAP server, kao što bismo pod Windowsima to napravili korištenjem komande Idifde.

2. Konfiguracija openLDAP klijenta

Za klijentsku konfiguraciju, već smo instalirali sve potrebne pakete u prvoj vježbi, pa nam ostaje samo klijentska konfiguracija. Na vašoj NAOOS1 virtualnoj mašini potrebno je u komandnoj liniji upisati (jedna komanda):

```
authconfig --enableldap --ldapserver="ldap://127.0.0.1" --ldapbasedn="dc=example,dc=com"
--updateall
```

Slijedeća komanda trajno pali nsld servis (lokalni LDAP name service):

```
chkconfig nsd on
```

Također, potrebno je napraviti i određenu konfiguraciju autentifikacijskog sustava na Linux virtualnom server. Konkretno, potrebno je napraviti slijedeće korake:

1. Konfigurirati datoteku /etc/pam_ldap.conf
2. Konfigurirati datoteku /etc/openldap/ldap.conf
3. Konfigurirati datoteku /etc/sysconfig/authconfig
4. Konfigurirati datoteku /etc/nsswitch.conf
5. Konfigurirati datoteke /etc/pam.d/system-auth, /etc/pam.d/password-auth datoteku

Zbog jednostavnosti, datoteke bi trebale izgledati ovako:

[illegible]

Slika 3. Konfiguracijska datoteka /etc/pam_ldap.conf. Postojeću konfiguracijsku datoteku potrebno je obrisati.



```
root@rhel-server:~/Desktop
File Edit View Search Terminal Help
#
# LDAP Defaults
#
# See ldap.conf(5) for details
# This file should be world readable but not world writable.
#BASE    dc=example,dc=com
#URI      ldap://ldap.example.com ldap://ldap-master.example.com:666
#
#SIZELIMIT    12
#TIMELIMIT    15
#DEREF        never
#
#TLS_CACERTDIR    /etc/pki/tls/certs
#TLS_CACERT /etc/pki/tls/certs/certifikat.pem
#URI ldap://127.0.0.1
#BASE dc=example,dc=com
#
~
~
~
~
"/etc/openldap/ldap.conf" 19L, 371C 16,1 All
```

Slika 4. Konfiguracijska datoteka /etc/openldap/ldap.conf

```
root@rhel-server:~
File Edit View Search Terminal Help
IPADOMAINJOINED=no
USEMKHOMEDIR=no
USEPAMACCESS=no
CACHECREDENTIALS=yes
USESSSDAUTH=no
USESHADOW=yes
USEWINBIND=no
USEDDB=no
FORCELEGACY=no
USEFPRINTD=yes
FORCESMARTCARD=no
PASSWDALGORITHM=sha512
# potrebno je postaviti ove dvije opcije u yes
USELDAPAUTH=yes
USELDAP=yes
# sve ostalo je potrebno ostaviti na default vrijednostima
USEPASSWDQC=no
IPAV2NONTP=no
USELOCALAUTHORIZE=yes
USECRACKLIB=yes
USEIPAV2=no
USEWINBINDAUTH=no
USESMARTCARD=no
-- INSERT --
```

Slika 5. Konfiguracijska datoteka /etc/sysconfig/authconfig



```
root@rhel-server:~  
File Edit View Search Terminal Help  
#group: db files nisplus nis  
  
passwd: files ldap  
shadow: files ldap  
group: files ldap  
sudoers: files ldap  
  
#hosts: db files nisplus nis dns  
hosts: files dns  
  
# Example - obey only what nisplus tells us...  
#services: nisplus [NOTFOUND=return] files  
#networks: nisplus [NOTFOUND=return] files  
#protocols: nisplus [NOTFOUND=return] files  
#rpc: nisplus [NOTFOUND=return] files  
#ethers: nisplus [NOTFOUND=return] files  
#netmasks: nisplus [NOTFOUND=return] files  
  
bootparams: nisplus [NOTFOUND=return] files  
  
ethers: files  
netmasks: files  
networks: files  
protocols: files  
rpc: files  
services: files ldap  
  
netgroup: nisplus  
  
publickey: nisplus  
  
automount: files ldap  
aliases: files nisplus  
  
64,0-1 Bot
```

Slika 6. Konfiguracijska datoteka /etc/nsswitch.conf

```
root@rhel-server:~/Desktop  
File Edit View Search Terminal Help  
  
auth sufficient pam_unix.so nullok try_first_pass  
auth requisite pam_succeed_if.so uid >= 500 quiet  
auth required pam_deny.so  
  
account required pam_unix.so  
account sufficient pam_localuser.so  
account sufficient pam_succeed_if.so uid < 500 quiet  
account required pam_permit.so  
  
password requisite pam_cracklib.so try_first_pass retry=3 type=  
password sufficient pam_unix.so sha512 shadow nullok try_first_pass use_au  
thtok  
password required pam_deny.so  
  
session optional pam_keyinit.so revoke  
session required pam_limits.so  
session [success=1 default=ignore] pam_succeed_if.so service in crond quiet  
use_uid  
session required pam_unix.so  
# potrebno je na kraj dodati ove dvije opcije  
session optional pam_ldap.so  
session required pam_mkhomedir.so skel=/etc/skel umask=0077  
  
-- INSERT --  
26,1 Bot
```

Slika 7. Konfiguracijska datoteka /etc/pam.d/system-auth



```
root@rhel-server:~/Desktop
# User changes will be destroyed the next time authconfig is run.
auth      required      pam_env.so
auth      sufficient    pam_unix.so nullok try_first_pass
auth      requisite     pam_succeed_if.so uid >= 500 quiet
auth      required      pam_deny.so

account    required     pam_unix.so
account    sufficient    pam_localuser.so
account    sufficient    pam_succeed_if.so uid < 500 quiet
account    required     pam_permit.so

password   requisite     pam_cracklib.so try_first_pass retry=3 type=
password   sufficient    pam_unix.so sha512 shadow nullok try_first_pass use_au
thtok
password   required      pam_deny.so

session    optional     pam_keyinit.so revoke
session    required     pam_limits.so
session    [success=1 default=ignore] pam_succeed_if.so service in crond quiet
use_uid
session    required     pam_unix.so
# potrebno je dopisati opciju za korištenje pam_ldap modula
session    optional     pam_ldap.so
-- INSERT --
```

Slika 8. Konfiguracijska datoteka /etc/pam.d/password-auth

Nakon konfiguracije, potrebno je startati nsldc servis. Kao root korisnik u komandnoj ljsuci napišemo:

service nsldc start

Ako smo sve napravili kako treba, testiranje možemo provesti ovako:

```
admin@rhel-server:~
File Edit View Search Terminal Help
[root@rhel-server Desktop]# su - admin
[admin@rhel-server ~]$
```

Slika 9. Testiranje uspješne openLDAP konekcije

Korisnik "admin" ne postoji kao lokalni korisnik, već smo ga kreirali kao openLDAP korisnika. Ako komandu su možemo uspješno izvršiti i logirati se na korisnika "admin", vježba je uspješno završena.