

Openldap ??

- [LDAP\[1\] -1. \[1\]\[1\]\[1\]\[1\]](#)
- [LDAP\[1\] -2. \[1\]\[1\]\[1\] \[1\]\[1\]](#)
- [LDAP\[1\] -3. SAMBA\[1\]\[1\] \[1\]\[1\]](#)
- [LDAP\[1\] -4. rootdn\[1\]](#)

LDAP??-1. ???????

????

1. OS : Centos 6.5
2. LDAP 서버 IP : 192.168.10.10
3. LDAP 클라이언트 IP : 192.168.100.10
4. LDAP root dn(서버명 서버명) : Manager (cn=manager,dc=example,dc=com)

LDAP ?? ??

1. 서버 패키지 설치

```
$> yum install openldap-servers openldap-clients -y
```

2. 기본 설정 파일 복사

```
$> cp /usr/share/openldap-servers/slapd.conf.obsolete /etc/openldap/slapd.conf
```

3. 비밀번호 생성

```
$> slappasswd
$> New password:
$> Re-enter new password:
{SSHA}qZsVpahyjRbub0KXgtaNuLs11JGMud/G
* 비밀번호 16자 이하로 설정하십시오.
```

4. 기본 설정 파일 수정

```
$> vi /etc/openldap/slapd.conf
...
my-domain test.co.kr
...
rootpw #비밀번호 16자 이하로 설정하십시오
```

5. DB 파일 복사

```
$> cp /usr/share/openldap-servers/DB_CONFIG.example /var/lib/ldap/DB_CONFIG
```

6. 删除 slapd.d 目录

```
$> rm -rf /etc/openldap/slapd.d/*
```

7. 创建 slapd.d 目录

```
$> cat /root/root.ldif
dn: dc=my-domain,dc=com
dc: my-domain
objectClass: dcObject
objectClass: organizationalUnit
ou: my-domain.com

dn: ou=people,dc=my-domain,dc=com
ou: people
objectClass: organizationalUnit

dn: ou=groups,dc=my-domain,dc=com
ou: groups
objectClass: organizationalUnit
```

8. 添加 slapd.d 目录

```
$> slapadd -v -n 2 -l /root/root.ldif
```

9. 测试 slapd.d 目录

```
$> slaptest -f /etc/openldap/slapd.conf -F /etc/openldap/slapd.d
```

10. 设置 slapd.d 目录权限

```
$> chown -R ldap:ldap /var/lib/ldap
$> chown -R ldap: /etc/openldap/slapd.d/
```

11. 配置 LDAP 服务

```
$> echo "local4.* /var/log/slapd/slapd.log" >> /etc/rsyslog.conf
$> /etc/init.d/rsyslog restart
```

配置 slapd.d 目录，创建 slapd.d 目录，并设置权限

12. logrotate  (/etc/logrotate.d/syslog)

```

[ ] [ ] [ ] - /var/log/slapd/slapd.log

```

13. $\frac{100}{100} \div \frac{100}{100}$

```
$> /etc/init.d/slapd start
```

```
$> chkconfig slapd on
```

14.

```
$> netstat -antp | grep slap
```

```
tcp        0      0 0.0.0.0:389          0.0.0.0:*        LISTEN
1339/slapd
```

```
tcp        0      0 :::389                                :::*                                LISTEN
1339/slapd
```

SSL??? Idap ????

- (SSL [] ldap[] [] [] [] [] [] [] [] [] .) example.pem
key[] .

1.

--	--	--	--	--

```
$> openssl req -new -x509 -nodes -out /etc/pki/tls/certs/example.pem -keyout  
/etc/pki/tls/certs/examplekey.pem -days 365
```

2.

--	--	--

--	--	--

--	--

```
$> chown -R :ldap /etc/pki/tls/certs/example*
```

3. /etc/openldap/slapd.conf ☐ ☐ ☐

```
$> cat /etc/openldap.slapped.conf
TLSCertificateFile /etc/pki/tls/certs/example.pem
TLSCertificateKeyFile /etc/pki/tls/certs/examplekey.pem
TLSCACertificatePath /etc/pki/tls/certs
```

4. ☐ ☐ ☐ ☐ ☐ ☐ LDAPS ☐ ☐

```
$> vi /etc/sysconfig/ldap
...
SLAPD_LDAPS=yes
```

5. `ss` `ss` `tcp/636` `ss` `ss`

```
$> netstat -antp | grep slapd | grep :636
tcp        0      0 0.0.0.0:636          0.0.0.0:*          LISTEN
        1339/slapd
tcp        0      0 :::636              :::*                LISTEN
        1339/slapd
SSL:636 ss, ss 389ss ss.
```

Idap ??? ?????? ?????? ??????

1. nfs`ss` `ss` `ss` `ss` `ss`

```
$> yum install nfs-utils* -y
```

2. NFS `ss`

```
$> cat /etc/exports
/home 192.168.100.10(rw,no_root_squash)
```

3. NFS`ss` `ss` & `ss`

```
$> /etc/init.d/rpcbind start
$> /etc/init.d/rpcidmapd start
$> /etc/init.d/nfs start
$> chkconfig rpcbind on
$> chkconfig rpcidmapd on
$> chkconfig nfs on
```

4. nfs`ss` `ss`

```
$> showmount -e localhost
Export list for localhost:
/home 192.168.10.10
```

LDAP??-2. ?????? ?????

LDAP ?????? ??

1. `yum` `install`

```
$> yum install openldap-clients nss-pam-ldapd \
pam_ldap autofs nfs-utils -y
```

2. `ldap` `LDAP` `??`

1. `setup` `??` -> Authentication configuration -> Use LDAP, Use LDAP Authentication

`??` `??` `NEXT`

2. Server: [ldap://](#)`??`

3. Base DN: `dc=my-domain,dc=com`

4. `??` `OK` `??` `??`, `SSL` `??` `??` `Use TLS` `??` `??` `??`.

3. `??` `??`

```
$> cat /etc/pam.d/system-auth | grep ldap
session      optional      pam_ldap.so
```

4. `ldap` `??` `??` `??` `??` `??`

```
$> cat /etc/auto.master
/home /etc/auto.home

$> cat /etc/auto.home
* -rw,soft,intr,rsiz=8192,wsiz=8192 192.168.10.10:/home/&
```

5. `ldap` Client `??` `??` & `??`

```
$> /etc/init.d/nslcd start
$> chkconfig nslcd on
```

6. `autofs` `??` `??` & `??`

```
$> /etc/init.d/autofs start
$> chkconfig autofs on
```

LDAP??-3. SAMBA???? ???? ?

Samba??? LDAP???? – LDAP???? ??

1. ??? ?

```
$> yum install -y samba samba-devel
```

2. samba?? ?

```
$> vi /etc/samba/smb.conf ?? ?
...
security = user
ldap admin dn = cn=Manager,dc=my-domain,dc=com
ldap suffix = dc=my-domain,dc=com
ldap group suffix = ou=groups
ldap user suffix = ou=people
ldap passwd sync = yes
ldap delete dn = Yes
domain logons = yes
```

3. LDAP? samba??

```
$> vi /etc/openldap/slapd.conf
...
include /etc/openldap/schema/samba.schema
access to attrs=userPassword,sambaLMPassword,smabaNTPassword,shadowLastChange
by dn.children="ou=Manager,dc=my-domain,dc=com" write
by self write
by anonymous auth
by * none
access to *
by dn.children="ou=Manager,dc=my-domain,dc=com" write
by * read
```

4. ldap admin ???? ?

```
$> smbpasswd -w
```

5. LDAP[] samba [] []

```
$> smbpasswd -a test
$> New SMB password:
$> Retype new SMB password:
```

6. [] [] [] []

```
$> /etc/init.d/smb start
$> chkconfig smb on
```

7. samba [] [] []

```
$> smbclient -U test //192.168.10.10/home
```

- [] [] [] [] [] [] [] []

LDAP??-4. rootdn??

LDAP root dn ????? ??

1. `slappasswd` `openssl` `openssl`

```
$> slappasswd
$> New password:
$> Re-enter new password:
{SSHA}qZsVpahyjX0F1fkdlXgtLsfAr11JGMfj.h
```

2. LDIF`ldif` `password.ldif` `olcRootPW` `olcRootPW`

```
$> cat password.ldif
dn: 0lcDatabase={2}bdb,cn=config
replace: olcRootPW
olcRootPW: {SSHA}qZsVpahyjX0F1fkdlXgtLsfAr11JGMfj.h
```

3. `ldapmodify` `-Y EXTERNAL` `-H ldapi:///` `-f password.ldif`

```
$> ldapmodify -Y EXTERNAL -H ldapi:/// -f password.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
modifying entry "0lcDatabase={2}bdb,cn=config"
```