

# Openldap 2.4

- LDAP 2.4 -1. 安装配置
- LDAP 2.4 -2. 用户管理
- LDAP 2.4 -3. SAMBA 集成
- LDAP 2.4 -4. rootdn 管理

# LDAP 서버 -1. 서버 구축

## 준비

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(관리자 계정) : Manager (cn=manager)

## LDAP 서버 구축

1. 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 확인 및 저장 완료
```

4. 기본 설정 파일 수정

```
$> vi /etc/openldap/slapd.conf
...
my-domain test.co.kr
...
rootpw # 비밀번호 관리자 계정
```

5. DB 초기화

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

6. `rm` `slapd.d`

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

7. `cat` `root.ldif`

```
$> 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. `DB` `slapadd`

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

9. `slaptest` `slapd.conf` `slapd.d`

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

10. `chown` `ldap`

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

11. `LDAP` `rsyslog`

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

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

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

logrotate - /var/log/slapd/slapd.log

13. 13. /

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

```
$> chkconfig slapd on
```

14. 14. 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 ldap

- (SSL ldap ) example.pem key .

1. 1. 1. 1.

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

```
/etc/pki/tls/certs/examplekey.pem -days 365
```

2. 2. 2. 2.

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

3. /etc/openldap/slapd.conf 3. 3. 3.

```
$> cat /etc/openldap.slapd.conf
```

```
TLSCertificateFile /etc/pki/tls/certs/example.pem
```

```
TLSCertificateKeyFile /etc/pki/tls/certs/examplekey.pem
```

```
TLSCACertificatePath /
```

4. 4. 4. 4. LDAPS 4.

```
$> vi /etc/sysconfig/ldap
```

```
...
```

```
SLAPD_LDAPS=yes
```

## 5. 检查端口是否监听tcp/636 是否

```
$> 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  636  0  ,  389  0  .
```

# ldap 检查 检查 检查 检查

## 1. nfs 检查 检查 检查 检查

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

## 2. NFS 检查

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

## 3. NFS 检查 检查 & 检查

```
$> /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 检查 检查

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

# LDAP -2.

## 

## LDAP

- 1.

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

2. 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 samba samba-devel

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

### 2. samba smb.conf

```
$> 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,sambaNTPassword,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 用户 权限

```
$> smbpasswd -w
```

#### 5. LDAP 用户 samba 用户 权限

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

#### 6. 用户 权限 用户 权限

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

#### 7. samba 用户 权限 用户 权限

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

- 用户 权限 用户 权限 用户 权限 用户 权限

# LDAP -4. rootdn

## LDAP root dn

1. 生成密码

```
$> slappasswd  
$> New password:  
$> Re-enter new password:  
{SSHA}qZsVpahyjXOF1fkdlXgtLsfAr11JGMfj.h
```

2. LDIF 文件

```
$> cat password.ldif  
dn: OlcDatabase={2}bdb,cn=config  
replace: olcRootPW  
olcRootPW: {SSHA}qZsVpahyjXOF1fkdlXgtLsfAr11JGMfj.h
```

3. 使用 ldapmodify 修改

```
$> 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 "OlcDatabase={2}bdb,cn=config"
```