LDAP구성 -1. 서버구성하기

구성정보

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 정보) : Manager (기본설정값)

LDAP 서버 구성

1. 패키지 설치하기

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

2. 설정파일 복사

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

3. 관리자 패스워드 생성

```
$> slappasswd
$> New password:
$> Re-enter new password:
{SSHA}qZsVpahyjRbub0KXgtaNuLs11JGMud/G
```

* 생성된 패스워드 값은 일단 복사 .

4. 설정파일 내용변경

```
$> vi /etc/openldap/slapd.conf
...
my-domain test.co.kr
...
rootpw  #복사한 패스워드값 적용
```

5. DB 파일 복사

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

6. 기존내용 삭제

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

7. 기본 구성 세팅하기

```
$> 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. DB새로 생성

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

9. 설정파일 구문오류 확인하기

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

10. 소유권 변경

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

11. LDAP로그 분리

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

다른 방법이 있는걸로 알고 있는데 , 알게되면 다시 업데이트 할께요

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

    대상로그 - /var/log/slapd/slapd.log

13. 서비스 활성화 /시작

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

14. 포트 오픈상태 확인

```
$> 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
```

SSL기반의 ldap 사용하기

- (SSL 기반으로 ldap을 운영하려면 각 클라이언트에도 키파일을 가지고 있어야 함 .) examply.pem 파일이 key파일 .

1. 키파일생성

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

2. 키파일 소유권 변경

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

3. /etc/openldap/slapd.conf 파일 내용 수정

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

4. 설정파일에서 LDAPS 활성화

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

5. 서비스 재시작 후 tcp/636 오픈 확인

```
$> 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
```

SSL기반은 636번 포트 , 기본은 389번포트 사용함 .

ldap 사용자 로그인시 홈디렉토리 자동마운트

1. nfs서버 구성을 위한 패키지 설치

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

2. NFS 설정

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

3. NFS서비스 시작 & 활성화

```
$> /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. nfs활성화 확인

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

Revision #1
Created 7 June 2022 15:49:21 by artop0420
Updated 24 December 2023 02:30:52 by artop0420