**LDAP 서버 & 클라이언트 & NFS 연동실습**

**LSC Systems**

**DT**

**이준호 사원**

* **초기값**

Openldap **Server** : 192.168.111.100 /etc/hosts : testldap.co.kr

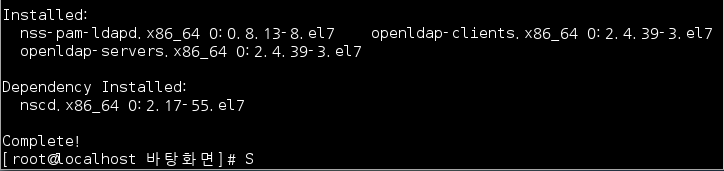
Openldap **Client** : 192.168.111.200 /etc/hosts : ldapclient.co.kr

NFS **Server** : 192.168.111.250 /etc/hosts : mountserver.co.kr

* OpenLdap Server 구축 ( 192.168.111.100 )

# **yum install -y openldap-servers openldap-clients nss-pam-ldapd**

// 기본 패키지 인스톨

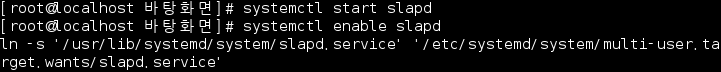


# **systemctl start slapd**

// 데몬시작 ( 389포트)

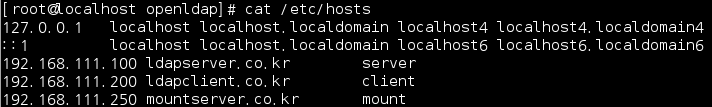
# **systemctl enable slpad**

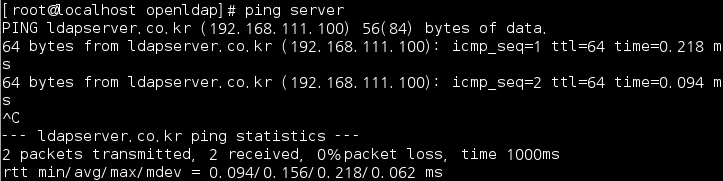
// 자동시작 등록

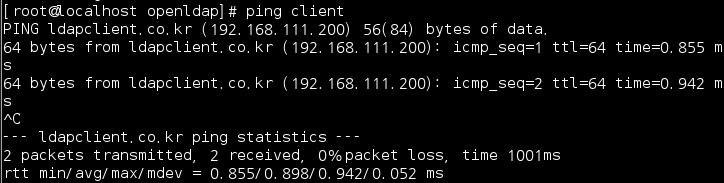


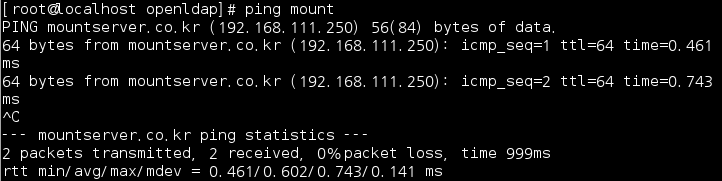
# /etc/hosts 에서 hosts 설정 ( Server & Client 양쪽 모두 설정 )

* 도메인 설정 및 핑 테스트









* openldap의 환경설정은 /etc/openldap/slapd.d/cn=config/olcDatabase=~.ldif를 읽어오는데, 해당 파일을 수동편집하는게 아니라 Config 양식을 생성 후, ldapmodify 명령어로 업데이트를 하는 방식이다.

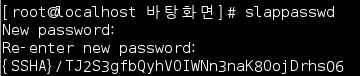
# **cp /usr/share/openldap-servers/slapd.ldif /etc/openldap/slapd.conf**

// 환경설정 템플릿을 복사



# **slapasswd**

// ldap 관리자 설정 {SSHA}/TJ2S3gfbQyhVOIWNn3naK8OojDrhs06 메모.



# **vi /etc/openldap/domain.ldif**

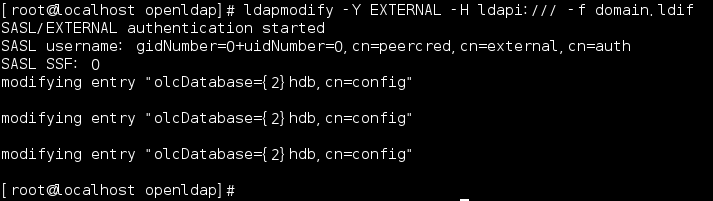


// dc 설정 ( ldaperver.co.kr )

// dc 설정 ( Manager 계정 = root )

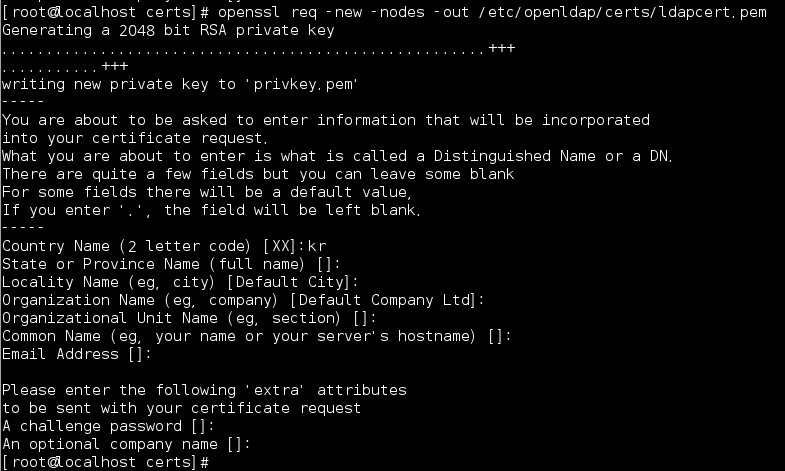
// 원본설정 수정선언, RootPW 설정선언, 패스워드 기입

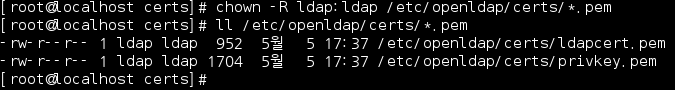
# ldapmodify -Y EXTERNAL -H ldapi:/// -f domain.ldif

// LDAP Server에 환경설정 업데이트.

* LDAP 인증서 만들기.

LDAP 서버에 대한 자체 서명 된 인증서를 작성하자. 아래 명령은 / etc / openldap / certs 디렉토리에 인증서와 개인 키를 모두 생성.



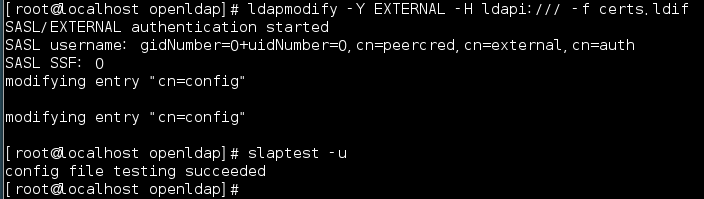
# /etc/openldap/certs/\*.pem 의 권한을 ldap으로 변경 후 확인.

# vi certs.ldif



# **ldapmodify -Y EXTERNAL -H ldapi:/// -f certs.ldif**

# slaptest -u 로 환경설정 적용확인.



* 유저 계정 관련 스키마 & 계정생성
* 유저 DB ( ldap 디렉터리 설정 및 Account 추가 ) 설정

# cp /usr/share/openldap-servers/DB\_CONFIG.example /var/lib/ldap/DB\_CONFIG

설정 템플릿 복사

# chown -R ldap:ldap /var/lib/ldap

// 해당 폴더 전체 ldap 소유로 변경.

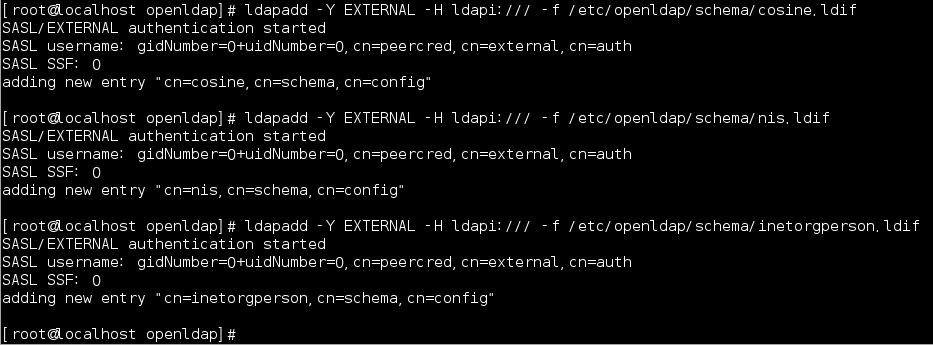


* 기본 디렉터리 DB 구조를 추가

ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/cosine.ldif

ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/nis.ldif

ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/inetorgperson.ldif



# 이제 각 부서(디렉터리)를 구분하는 스키마 업데이트

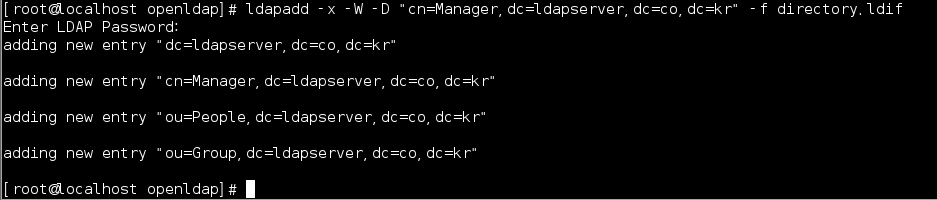


// ldaperver.co.kr 도메인의 LDAP Server Manager로 정의

// People & Group 구조 정의

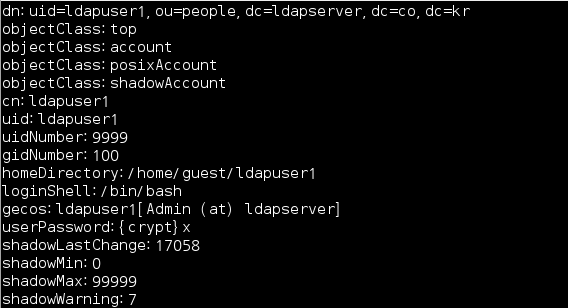
* 환경설정에 구조 추가하기 및 초기설정한 비밀번호 입력

# ldapadd -x -W -D “cn=Manager,dc=ldapserver,dc=co,dc=kr” -f directory.ldif



* ldapuser1 라는 계정을 만들어보기.

# vi ldapuser1.ldif



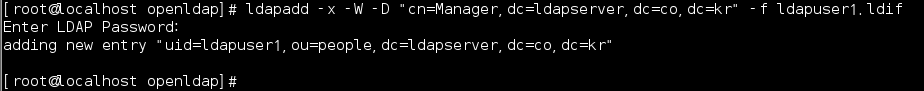
// ldapserver.co.kr 도메인의 People ou(그룹 조직)에

ldapuser1 이라는 dn(계정)을 선언.

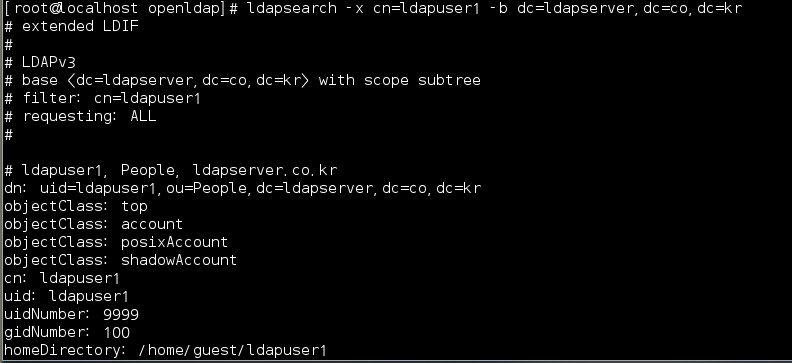
ㅣㅇ멩

ㄷㄹㄷ

# ldapadd -x -W -D “cn=Manager,dc=ldapserver,dc=co,dc=kr” -f ldapuser1.ldif 및 패스워드 입력



# ldapsearch -x cn=ldapuser1 -b dc=ldapserver,dc=co,dc=kr 로 ldapuser 계정 추가확인.



* Client 서버에서 LDAP 계정 로그인하기.

# yum install -y openldap-clients nss-pam-ldapd

# authconfig –enableldap –enableldapauth –ldapserver=192.168.111.100 –ldapbasedn=”dc=ldapserver,dc=co,dc=kr” –enablemkhomedir –update

# systemctl restart nslcd

# getent passwd ldapuser1



# su - ldapuser1



// 로그인 성공

* 이제 NFS 서버에서 Mount 하기.

# yum install nfs-utils

# systemctl start nfs-server

# systemctl enable nfs-server

# mkdir /test

# vi /etc/exports



# exportfs -r

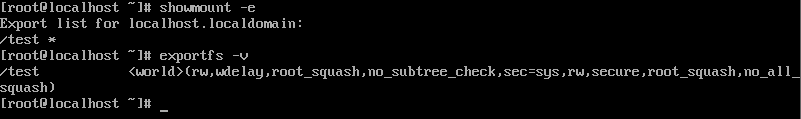
// 수정한 내용을 exportfs 명령으로 반환.

# firewall-cmd –permanent -add-service=nfs

# firewall-cmd --reload

# showmount -e

# exportfs -v

// NFS 설정 정상적인지 확인.

* 다시 클라이언트 서버로 돌아가 마운트 설정하기.

# autofs 작업

# yum install -y autofs

# systemctl start autofs

# systemctl enable autofs

# vi /etc/auto.master 에 아래문구 추가.

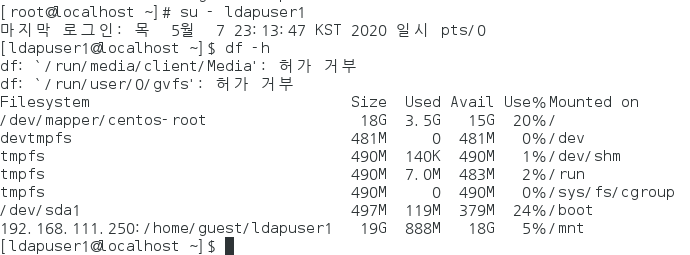


# vi /etc/auto.guest 파일 생성 후 문구추가.

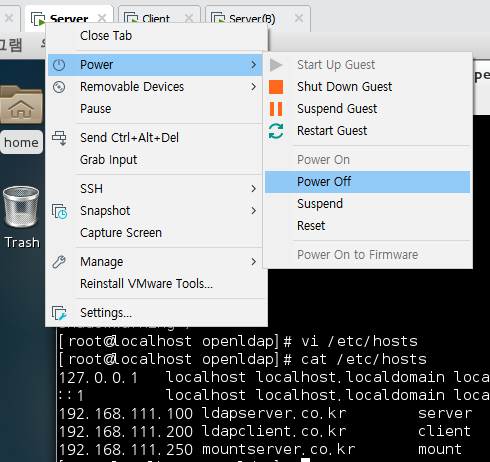
# systemctl restart autofs // 재시작

# su – ldapuser1

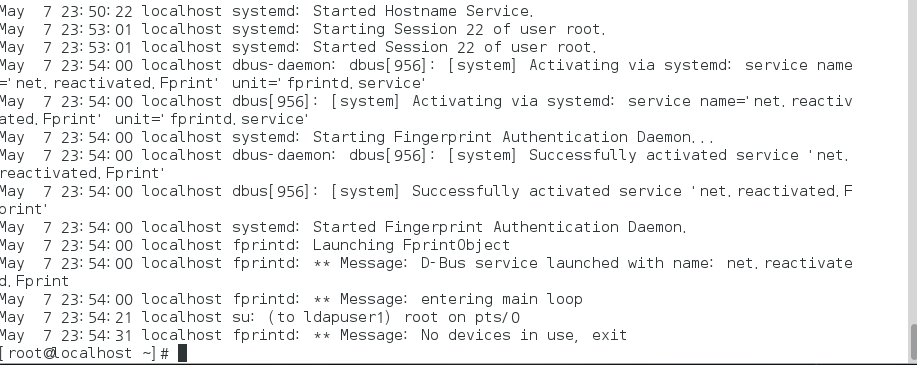
# df -h



* 엘답서버 강제 종료 후 클라이언트에서 로그관찰.



엘답Server 54분에 shutdown 후 엘답Client의 /var/log/messages



**DNS서버 구축**

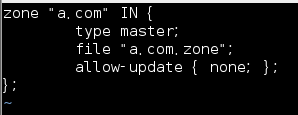
****

# yum -y install bind



# vi /etc/named.conf 수정

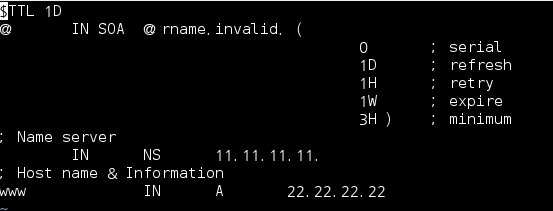
* named.conf 는 named 프로세스의 옵션 등을 설정하는 파일이다.
* listen-on port 53 { any; } : 서비스할 포트와 IP대역을 정의한다
* allow-quey { any; } : 질의를 허용할 IP대역을 정의한다.
* rexursion no : 상위 질의 허용여부를 설정하며, yes 사용시 보안상 취약 할 수 있다.



# vi /etc/named.rfc1912.conf 수정.

질의한 도메인의 DNS 정보를 가지고 파일을 zone 파일이라고 하며,

named.rfc1912.conf 파일에서 질의할 도메인 옵션 및 zone 파일의 경로를 설정한다.



# vi /var/named/a.com.zone 파일

* zone 파일은 기본적으로 /var/named 경로에 저장하도록 설정되어 있으며, 위에서 설정한 파일 이름과 동일하게 생성 해야함.
* < 레코드 설명 >

NS(Name Server) : zone을 풀이할 수 있는 DNS 서버의 목록을 가지고 있습니다.

A(Host) : 정규화된 도메인 이름/호스트명을 IPv4에 연결합니다.

CNAME(Canonical NAME) : 실제 호스트명과 연결되는 별칭을 정의합니다.

MX(Mail Exchange) : 메일서버에 도달할 수 있는 라우팅 정보를 제공합니다.

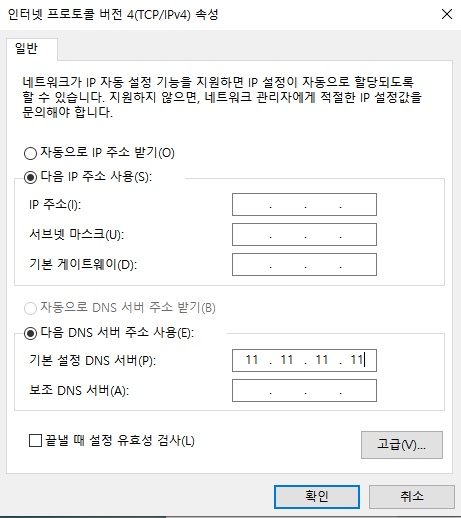
SOA(Start Of Authority) : DNS 영역의 주 DNS 서버 정의 및 refresh, retry 간격 등을 정의합니다.

PTR(PoinTeR) : 역방향 조회에서 A레코드를 가리킬 때 사용합니다.



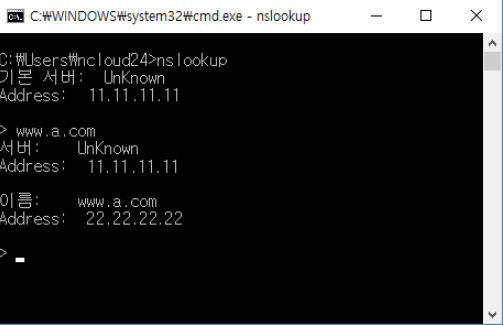
# systemctl start named

# netstat -nlpt 로 DNS 포트 LISTEN 확인.



# 이번엔 로컬컴퓨터의 네임서버를 수정

* 설정제어판 – 네트워크 연결 – 이더넷 – 인터넷 프로토콜버전 속성에서 기본 설정 DNS 서버 수정.



수정 후 명령 프롬포트에서 nslookup 실행하여 a.com의 질의결과를 확인 가능하다.