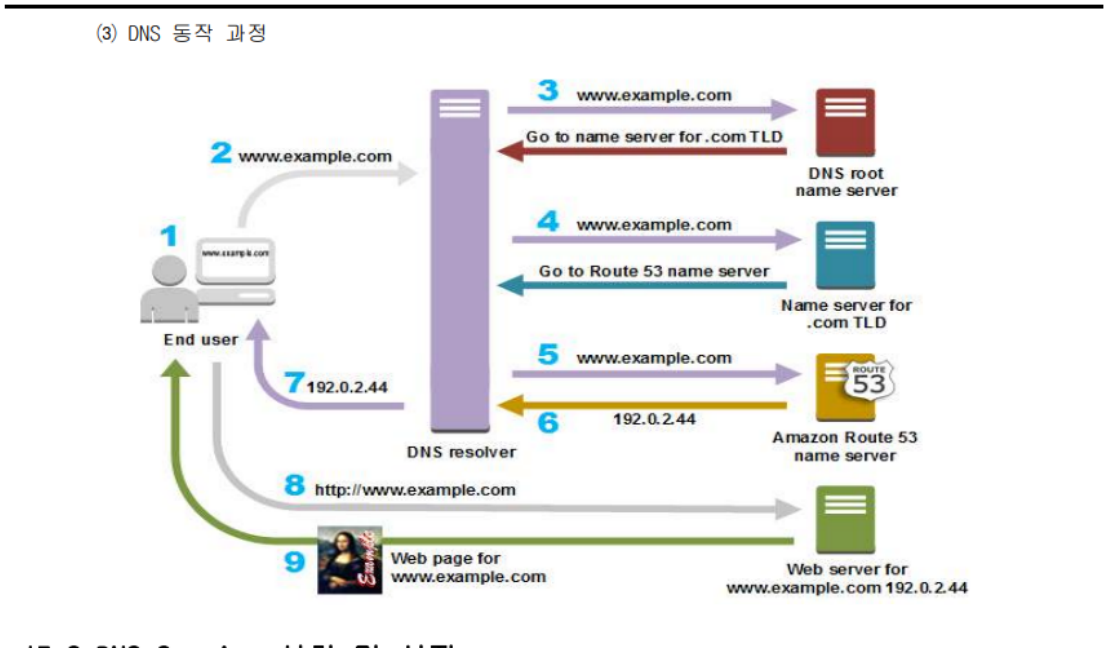
7/3

DNS Service

IP 주소를 이름 주소로 바꿔서 사용하기 편하게



중간에 PROXY 서버처럼 캐시가 하나 있다. 없으면 이 전체과정을 해야 한다.

이 서버의 이름을 캐싱 네임 서버라 한다. 구글의 8.8.8.8이 똑같은 역할이다.

캐싱 네임 서버: 자신이 관리하는 도메인은 없고, 클라이언트의 요청에 응답만 하는 name server

존 : 도메인을 가리키며 zone file에 도메인의 호스트 정보를 등록한다.

/etc/named.rfc1912.zones : 도메인을 등록하는 파일이고 도메인 등록 시 zone 파일의 위치를 지정함.

zone 파일이 저장되는 위치 : /var/named

Resource Record : NS(name server), A(IPv4주소), AAAA(IPv6주소), MX(메일서버), CNAME(canonical name), PTR(pointer)

1) bind 설치

dnf install bind-chroot

/var/named/chroot/var/named

패키지명은 bind 이지만 서비스명은 named이다.

2) 설정파일 수정

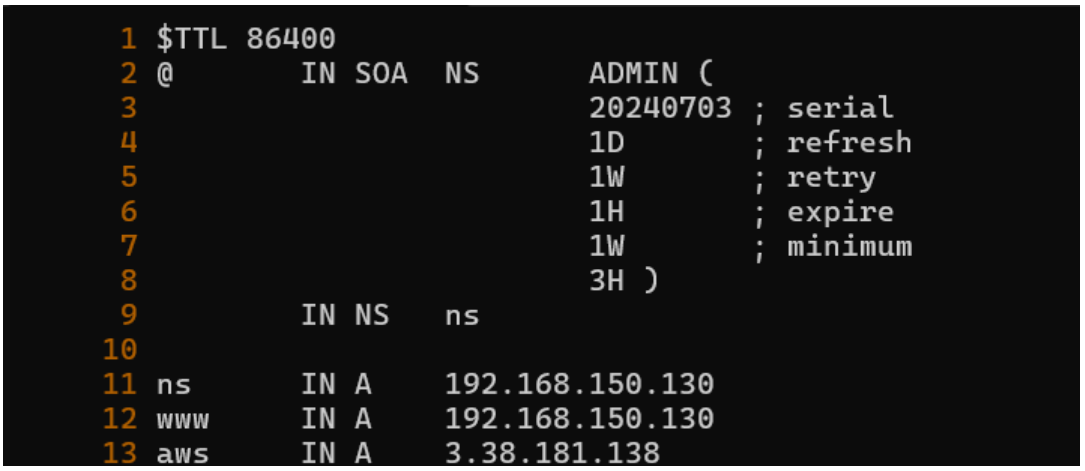
/etc/named.conf

```
//
// named.conf
//
// Provided by Red Hat bind package to configure the ISC BIND named(8) DNS
// server as a caching only nameserver (as a localhost DNS resolver only).
//
// See /usr/share/doc/bind*/sample/ for example named configuration files.
//

options {
        listen-on port 53 { 192.168.150.130; };
        listen-on-v6 port 53 { ::1; };
        directory       "/var/named";
        dump-file       "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        secroots-file   "/var/named/data/named.secroots";
        recursing-file  "/var/named/data/named.recursing";
        allow-query     { localhost; };

        /*
         - If you are building an AUTHORITATIVE DNS server, do NOT enable recursion.
         - If you are building a RECURSIVE (caching) DNS server, you need to enable
           recursion.
         - If your recursive DNS server has a public IP address, you MUST enable access
           control to limit queries to your legitimate users. Failing to do so will
           cause your server to become part of large scale DNS amplification
           attacks. Implementing BCP38 within your network would greatly
           reduce such attack surface
-- INSERT --
```

내 ip를 넣고 allow-query를 any로 한다. 범위를 전부로 한다.

```
leejeuk@DESKTOP-KM62UF8:/mnt/c/Users/kdt$ nslookup
> server 192.168.150.130
Default server: 192.168.150.130
Address: 192.168.150.130#53
> www.google.com
Server:         192.168.150.130
Address:        192.168.150.130#53

Non-authoritative answer:
Name:   www.google.com
Address: 172.217.31.4
Name:   www.google.com
Address: 2404:6800:4005:809::2004
>
```

wsl 환경에서 rocky에서 구축한 dns 서버를 이용하여 구글에 요청했을 때 잘 되는 모습을 확인 가능하다.



```
$TTL 86400
@       IN SOA  NS      ADMIN (
                        20240703 ; serial
                        1D       ; refresh
                        1W       ; retry
                        1H       ; expire
                        1W       ; minimum
                        3H )
        IN NS   ns

ns      IN A    192.168.150.130
www     IN A    192.168.150.130
aws     IN A    3.38.181.138
```

NS는 호스트 명이다.

ADMIN은 관리자 이메일 주소

SOA는 내가 이 목록들의 권한을 가진다.

높은 일련번호를 가지고 있으면 SLAVE 쪽으로 복사를 해준다

소문자 ns 뒤에는 ljw.com.이 생략돼있는 것

> 💡 도메인을 다 적을 때는 .을 붙여야 한다. 자동적으로 뒤에 ljw.com.이 붙게 된다.

파일 공유 서비스

FTP, Samba, NFS

FTP

FTP 서버에 파일을 저장하고 클라이언트에서 파일을 다운로드하거나 업로드하는 서비스

VSFTP 서버 프로그램을 사용하여 FTP서비스(TCP 21(세션), 데이터포트(20, 또는 임의의 포트)).

dnf install vsftpd

netstat -ntlp : n(numeric), t(tcp), l(listenling), p(pid)

설정파일 : /etc/vsftpd/vsftpd.conf /etc/vsftpd.conf(우분투)

local_enable = yes (서버 사용자로 로그인 가능)

anonymous = yes (익명 사용자로 로그인 가능 비밀번호 없음)

ftp 모드

active

클라이언트 세션 서버

임의의 포트 ————————————————> 21

클라이언트가 서버에게 접속할 데이터포트 알려줌

데이터

클라이언트가 알려준 포트 <———————— 20

클라이언트의 방화벽이 문제가 될 수 있다.

passive

클라이언트 세션 서버

임의의 포트 ————————————————> 21

서버가 클라이언트에게 접속할 데이터포트 알려줌

데이터

클라이언트가 알려준 포트 ————————————> 서버가 알려준 포트

일반적으로 방화벽 떄문에 수동형으로 많이 한다.

chroot

local_enable = YES 설정 시 사용자가 로그인 했을 경우 해당 사용자의 홈 디렉토리를

‘/’로 인식하도록 하는 설정

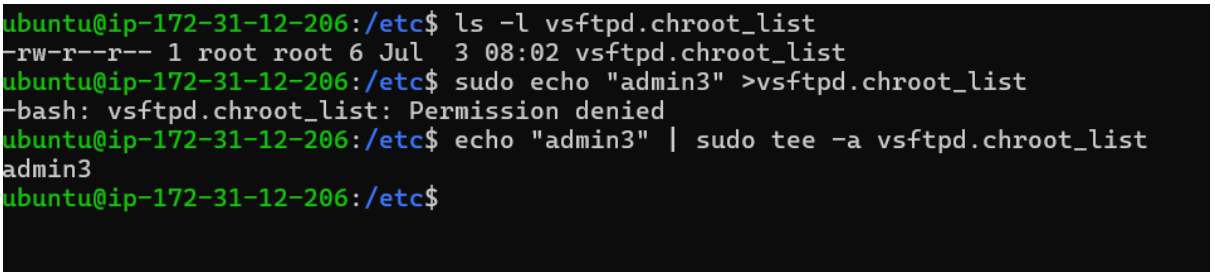
vi /etc/vsftpd/vsftpd.conf

chroot_local_user = YES

chroot_list_enable = YES

chroot_list_file = /etc/vsftpd.chroot_list ← 직접 만들어야

allow_writeable_chroot



echo 같은 경우 만들어 질 때 setuid가 안걸려 있기에 sudo가 안먹는다 파이프라인으로 빼서 tee를 이용

passive 모드 사용 시 포트 지정

vi /etc/vsftpd/vsftpd.conf

pasv_min_port=8001

pasv_max_port=8002

pasv_address = x. x. x. x

Samba

윈도우와 리눅스 간에 파일 및 장치 공유서비스

smb,cifs 프로토콜을 사용하여 공유 윈도우에서는 폴더 공유하면 리눅스에서 해당 폴더에 접근 가능

리눅스에서는 samba 패키지(서버) 설치, samba-client 패키지 설치

네트워크 드라이브로 연결해서 직접 연결된 드라이브처럼 사용 가능

TCP 137 , 139 , 445번 포트 사용

dnf install samba ⇒ samba 서버 패키지 설치

systemctl start smb

systemctl start nmb ⇒ ip 주소 대신 컴퓨터 이름으로 접근할 수 있는 서비스

/etc/samba/smb.conf ⇒ samba 설정 파일. 기본값은 로컬사용자의 홈디렉토리를 공유

samba 서비스를 사용하기 위해서는 samba 사용자로 등록해야함.

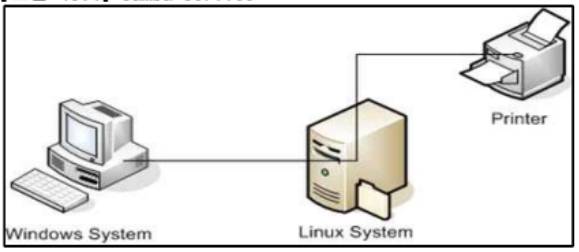
smbpasswd -a 사용자아이디 : smbpasswd -a admin

→ SMB 프로토콜과 달리 여러 유닉스 업체가 참여하여 결정된 표준이기 때문에 안정성 향상

⑵ Samba Service 특징

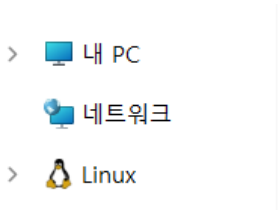
- Windows System과 Linux System간의 자원 공유
- 파일 공유뿐만 아니라 프린터 공유도 가능(Ex. Windows 사용자가 Linux 시스템에 연결된 프린터 사용 가능)
- SAMBA Service를 통한 NFS, FTP Service의 한계 극복 가능
  → NFS Service는 Linux와 Linux, Unix와 Unix 시스템 간에 파일 공유만 가능
  → FTP Service는 Windows와 Linux 시스템간의 파일 전송은 가능하지만 파일 전송 이외의 다른 서비스(Ex. Printer 공유)는 지원되지 않음. 또한 별도의 클라이언트 프로그램이 필요치 않음.

[그림 15.1] Samba Service



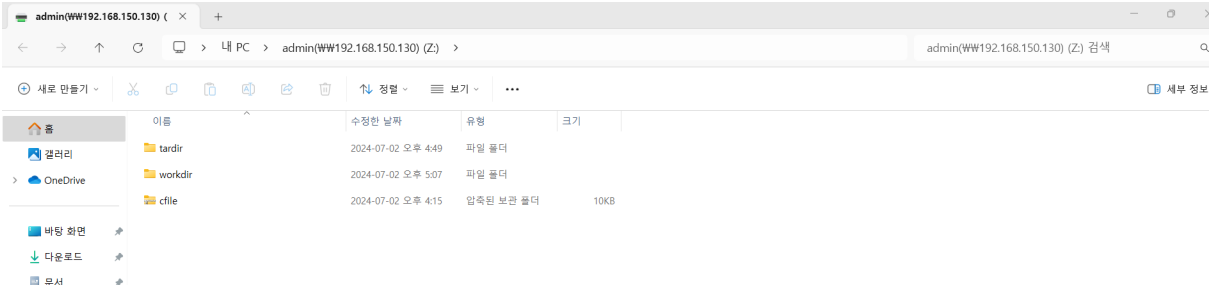
장치도 공유가 가능하다

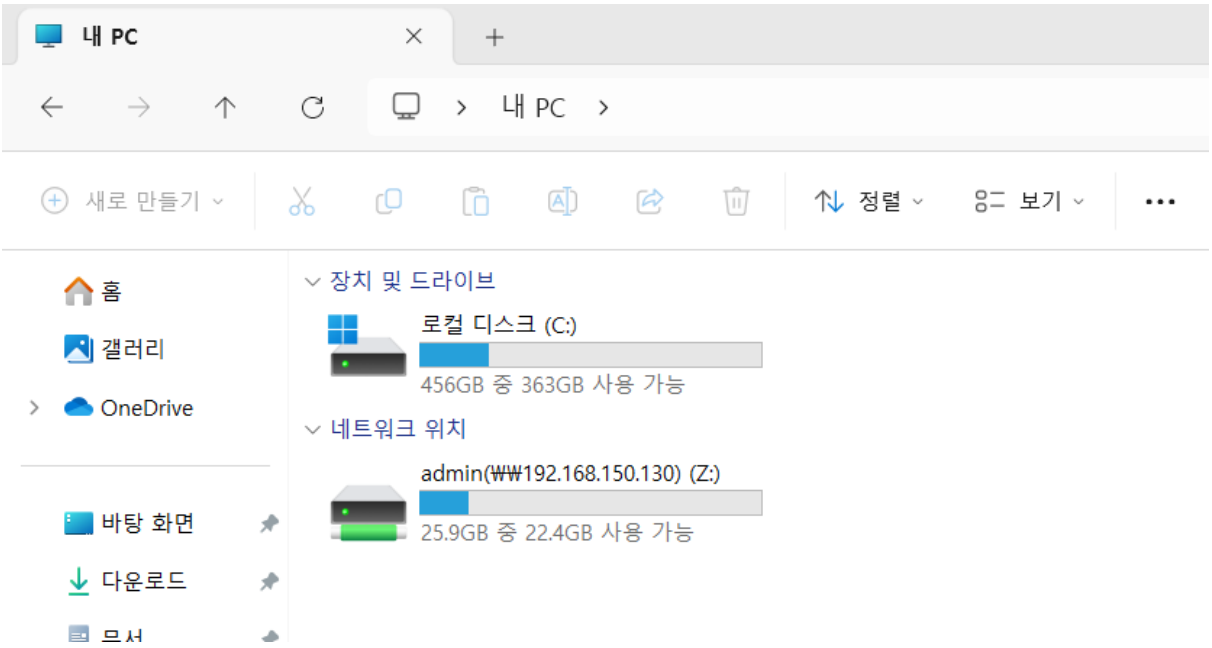
윈도우에서 연결



네트워크 우클릭 네트워크 드라이버 연결

\\192.168.150.130\admin으로 samba 연결





반대도 가능하다. 리눅스에서 윈도우의 드라이브를 사용이 가능

리눅스 우분투에서 연결

```
sudo -i
apt install samba-client cifs-utils

mkdir /mnt/admin
mount -t cifs //서버IP/admin /mnt/admin -o username=admin,password = 1234

df -Th

cd /mnt/admin
touch a b c d

Rocky에서 파일 확인
ls /home/admin
```

연결해제

할때는 해당 디렉토리에 있으면 안된다. 밖으로 나와야..

```
umount /mnt/admin
```

홈 디렉토리가 아닌 별도의 디렉토리를 공유하는 경우

```
Rocky 에서 진행
#vi /etc/samba/smb.conf
[share]
            path = /var/samba
            public = yes
            force_user = share
            force_group = share
            writable = yes

# systemctl restart smb
# useradd -s /bin/nologin share
# smbpasswd -a share
# mkdir /var/samba


우분투에서 연결
mkdir /mnt/share-dir
mount -t cifs //192.168.150.130/share /mnt/share-dir -o username=share,password=ys
```