Linux

※ CentOS7
1. 가상머신 이름 : mail-naver
2. CPU 1개, RAM 2G, HDD 40G, 네트워크 어댑터 NAT
3. 계정생성
계정이름 : kim 그룹이름 : myoffice 디렉토리 : /myoffice/kim
groupadd myoffice
useradd –g myoffice –d /myoffice/kim kim
4. IP는 각 대역의 20으로 설정
5. vim 설치 및 selinux diasbled 설정하기

■ 인터넷 시간과 동기화
rpm –qa | grep rdate
yum install –y rdate : rdate 인터넷 시간과 동기화 패키지 설치
rdate -s time.bora.net

■ 파일의 압축과 묶기
cp /boot/vmlinuz-3.10.0-1160.el7.x86_64 test

lib : 소스코드를 의미, lib만 있는 경우 프로그램이 설치가 되어있지 않음을 의미
yum install –y bzip2
yum install -y zip unzip

▷ 압축
Linux : xz, bzip2, gzip
<압축>
xz [파일] → 파일.xz
bzip2 [파일] → 파일.bz2
gzip [파일] → 파일.gz

<압축 풀기 : -d 옵션을 사용>
xz –d [파일].xz
bzip2 –d [파일].bz2 = bunzip2 [파일].bz2
gzip2 –d [파일].gz = gunzip [파일].gz

Window 호환용 : zip(압축), unzip(압축풀기)
압축
zip [파일].zip [대상]
압축 풀기

unzip [대상].zip
mkdir t
unzip –d t tt.zip => 디렉토리를 지정하여 압축 풀기

▷묶기 (tar)
묶어서 하나의 파일을 만드는 것은 압축과 똑같음 압축과 차이점은 용량은 그대로임
여러파일 혹은 디렉토리를 묶어서 하나의 파일로 만드는 것
tar [옵션] [파일].tar [대상]
※ [옵션] : 동작옵션과 기타옵션으로 나뉜다.
동작 : c(묶기), x(풀기), r(파일 추가), t(경로확인)
기타 : f(파일 : 필수 옵션), v(과정보이기)
묶기하면서 압축하는 옵션 : J(+xz), j(+bzip2), z(+gzip)

추가 옵션 : P : 묶을 디렉토리가 절대 경로로 설정되어 있을 때
–C[경로] : 풀고 싶은 경로를 지정

■ 네트워크 관련 필수 개념

◆ TCP/IP (TransmissionControlProtocol/InternetProtocol)
- 컴퓨터끼리 네트워크 상으로 의사소통을 하는 " 프로토콜 " 중 인터넷 표준 프로토콜
- TCP프로토콜 : 전송 데이터를 일정 단위(패킷)로 나누고 포장하는 것에 관한 규약
- IP 프로토콜 : 직접 데이터를 주고 받는 것에 관한 규약

◆ 호스트 이름(Hostname)과 도메인 이름(Domain name)
- 호스트 이름은 각각의 컴퓨터에 지정된 이름
- 도메인 이름(또는 도메인 주소)는 naver.com과 같은 형식

◆ IP 주소
- 각 컴퓨터의 랜카드에 부여되는 중복되지 않는 유일한 주소

◆ 네트워크 주소
- 같은 네트워크에 속해있는 공통된 주소 (네트워크를 대표함 ex) 192.168.111.0)

◆ 브로드캐스트 (Broadcast)주소
- 내부 네트워크의 모든 컴퓨터가 듣게 되는 주소
- 네트워크의 가장 마지막 IP

◆ 게이트웨이(Gateway), 라우터 (Router)
- 다른 네트워크와 연결해주는 역할을 하는 장비

◆ 넷마스크(Netmask), 클래스(Class)

- 넷마스크 = 서브넷마스크 : 네트워크의 규모를 결정
Classful, Classless

◆ DNS (Domain Name System) 서버 (= 네임서버)
- URL을 해당 컴퓨터(서버)의 IP주소로 변환해주는 서버
- CentOS7의 경우 설정 파일은 /etc/reslov.conf
※ Cache DNS, Master DNS Server가 있다.

◆ nmtui
- Network Manager Text User Interface : 네트워크와 관련된 작업
• DHCP 또는 고정 IP 주소 사용 결정
• IP주소, 서브넷, 게이트웨이 등 정보 입력
• DNS 정보 입력
• 네트워크 카드 드라이버 설정
• 네트워크 장치 (eth) 설정

◆ 네트워크 재시작 명령어
- systemctl restart NetworkManager (CentOS8)
- **systemctl restart network**
- service network restart
- /etc/init.d/network restart

CentOS 8은 ifdown ifup 인터페이스 켜고 꺼서 사용함.

◆ ifup [device] 및 ifdown[device]
- 네트워크 장치를 On, Off

◆ ifconfig [device]
- 해당 장치의 IP주소 정보를 출력

◆ ping [IP주소] or[URL]
- 해당 컴퓨터가 네트워크 상에서 응답하는지 테스트 (연결이 되는지 테스트)

◆ netstat –nr : 라우팅 테이블 확인(netstat 관련은 뒤에 조금 더 자세히)

◆ route : 라우팅 테이블 확인 및 설정

◆ arp : arp 테이블 확인(arp -d : arpcache 삭제)

※ ifconfig와 ip addr show(ip a)의 차이점

```
[root@localhost ~]# ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.100.100  netmask 255.255.255.0  broadcast 192.168.100.255
        inet6 fe80::d089:76a5:6e39:6eff  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:78:7a:b2  txqueuelen 1000  (Ethernet)
        RX packets 837  bytes 384226 (375.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 555  bytes 99802 (97.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 68  bytes 5920 (5.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 68  bytes 5920 (5.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

```
[root@localhost ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP g
roup default qlen 1000
    link/ether 00:0c:29:78:7a:b2 brd ff:ff:ff:ff:ff:ff
    inet 192.168.100.100/24 brd 192.168.100.255 scope global noprefixroute ens33
       valid_lft forever preferred_lft forever
    inet6 fe80::d089:76a5:6e39:6eff/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
[root@localhost ~]#
```

ifconfig : 대표 IP만 보여줌

ip addr show : 네트워크에 설정되있는 IP 모두를 보여줌

nmtui : 그래픽같이 네트워크 환경설정 커맨드를 보여줌

nmcli : 커맨드 라인으로 네트워크 정보를 볼 수 있음

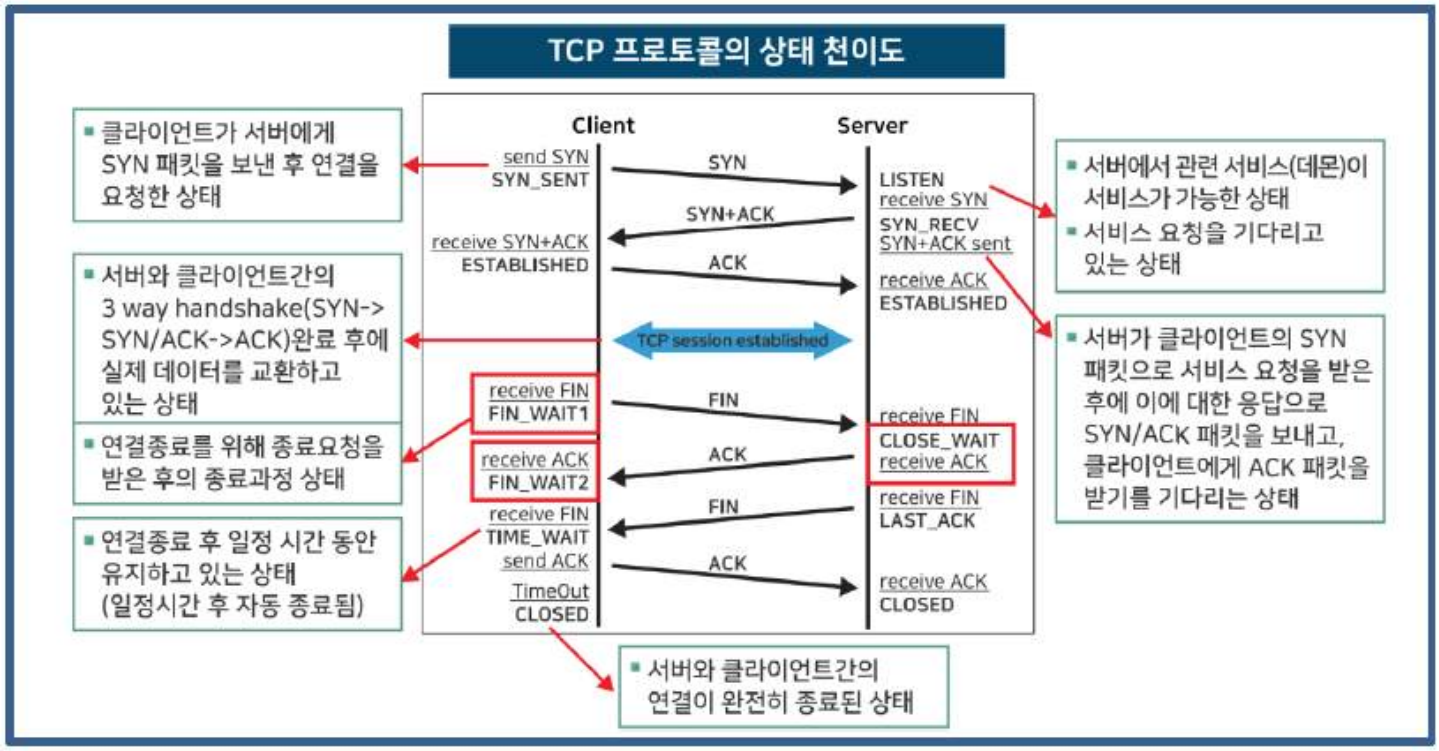
<nmcli 명령어 활용>

nmcli connection show ens33 = nmcli con show ens33

nmcli connection modify (+ or - : 추가 또는 제거 / +,- 없이 그냥 치면 해당 IP 주소로 변경)

ipv4.address x.x.x.x/24
여기서도 connection은 con으로 줄여서 사용가능
nmcli con show ens33 ipv4.gateway 192.168.100.2 → Gateway변경
nmcli con show ens33 ipv4.dns 162.128.63.1 → DNS 변경

TCP 통신



3 Handshake로 통신

<포트> - 암기할 필요 있음(자주 쓰는 것)
20,21(FTP) : 20(데이터 포트), 21(제어 포트)
22(SSH), 23(telnet), 25(SMTP), 53(DNS – 일반적으로 UDP이나 TCP에서도 사용), 80(http), 443(https)

◆ netstat
- 각 프로토콜별 활성화 된 서비스 및 서비스관련 프로세스 목록 확인
- netstat [옵션]
- tcp와 udp 각 프로토콜별로 활성화 된 서비스 및 관련 프로세스를 확인할 수 있는 도구
-l (listen) : 연결 가능한 상태
-n (number port) : 포트 넘버
-t (tcp) : tcp
-u (udp) : udp

netstat 사용 예
- netstat -anp : 연결을 기다리는 목록과 프로그램을 보여준다
- netstat -an | grep 포트번호 : 특정 포트가 사용 중에 있는지 확인
- netstat -antp | grep 상태값 : 특정 상태를 가진 tcp포트 등을 보여줌

- netstat -nlpt : TCP listening 상태의 포트와 프로그램을 보여준다
ex) netstat –an LISTEN | grep 22
netstat –antp | grep

■ 서비스와 소켓

◆ 서비스 (= 데몬 = 서버 프로세스)
- 백그라운드로 실행되는 프로세스로써 서비스 매니저 프로그램인 system 프로그램이 운영함
- 각각 독자적인 하나의 동작을 제공함
- 서비스 실행 스크립트 파일 : /usr/lib/systemd/system *.service
※ <foreground와 background>
foreground : 사용자와 상호작용을 통해서 돌아가는 프로그램(ex)문서작업(워드) 등)
background : 사용자와 상호작용 관계없이도 잘 동작하는 프로그램(ex)백신 실시간감시 등)

Socket은 서버 쪽으로 요청이 있을 경우에만 실행이 된다.
Service는 항상 백그라운드에서 실행이 됨

<소켓 동작 개요>

ntsysv : 그래픽처럼 생김(윈도우의 시작 프로그램 등록과 유사)
systemctl : service에 관련된 명령어
status : active 상태를 확인

■ 방화벽 관리

◆ 방화벽 관련 명령어
- 방화벽 실행/중지 :systemctl start/stop firewalld
- 방화벽 실행 여부 확인 : firewall-cmd --state
- 방화벽 재시작 : firewall-cmd --reload
: 포트/서비스 추가 및 제거 설정 후 적용할 때 사용
- 방화벽 상태 확인
firewall-cmd --list-all
- 서비스 추가/제거
firewall-cmd --permanent --zone=public --add-service=[service]
firewall-cmd --permanent --zone=public --remove-service=[service]
- 포트 추가/제거
firewall-cmd --permanent --zone=public --add-port=[number] firewall-cmd --permanent

--zone=public --remove-port=[number]
※ permanent옵션 : 시스템 재부팅 또는 방화벽 재시작 후에도 적용
서비스가 작동해야 할 것을 잘 알 때는 permanent 옵션을 사용함
test나 애매한 경우는 동작을 확인하고 사용함.
permanent 옵션 잘못하면 지우는데 고생함.

※ 공백후 시작 --, 단어와 단어를 이을때는 –로 표시

※ Whitelist vs Blacklist
화이트리스트 방식은 안전하다고 증명된 것만을 정책적으로 허용하고 나머지는 차단함으로써 내부 네트워크를 안전하게 유지시키는 방식이며, 블랙리스트 방식은 위협으로 인증된 것만을 관리자가 지정 및 차단하여 내부 네트워크를 안전하게 유지시키는 보안 방식입니다.
→ 화이트리스트가 보안적인 면에서 뛰어남

■ 방화벽 zone 설정
기본적으로 public이 설정되어 있음.

traceroute = 윈도의 cmd창에서 tracert 사용하는 것과 같음