1. #사용자 계정 설정

   사용자 추가시 www 디렉토리 기본 제공 ➜ mkdir /etc/skel/www

   사용자 계정의 속성 설정을 위한 기본값 ➜ vi /etc/login.defs

   사용자 추가시 생성되는 홈 디렉토리를 /home2 하위로 영구변경 ➜ useradd -D -b /home

   사용자 추가시 기본 쉘을 /bin/zsh로 영구변경 ➜ useradd -D -s /bin/zsh

   사용자 설정 파일의 위치 ➜ /etc/default/useradd

   idh 사용자의 주 그룹이 kait, 추가로 admin 그룹 포함 ➜ usermod -G admin idh

   john 계정 잠금, 잠금해제일자 25/12/31, 3일 유예 ➜ usermod -L -e 2025-12-31 -f 3 john

   john 암호 만료일 26/06/30 ➜ chage -E 2026-06-30 john

   pub 사용자 생성시, 주그룹은 kait, 추가 그룹은 ihd로 지정 ➜ useradd -g kait -G ihd pub

   idh 사용자를 linux그룹에 추가한다 ➜ usermod -aG linux idh

   idh 사용자 정보 확인 ➜ passwd -S idh

   idh 로그인 일시 제한 ➜ passwd -l idh

   idh 로그인 제한 해제 ➜ passwd -u idh

2. #소유권 (chown, chgrp, chmod)

   kimpro 디렉토리의 그룹 소유권을 linuxmaster로 변경한다 ➜ chgrp linuxmaster kimpro

   kimpro 디렉토리에는 linuxmaster그룹만 접근할 수 있고, 생성시 자동으로 그룹 소유권이 linuxmaster로 지정되게 한다, 파일 삭제는 본인 소유인 경우만 가능하다 ➜ chmod 3770 kimpro

   leepro 디렉토리의 소유권을 ihduser, 그룹소유권을 linux로 변경 ➜ chown ihduser:linux leepro

3. #파일시스템 생성 및 정보확인

   /dev/sdb1 장치를 XFS로 생성 ➜ mkfs.xfs /dev/sdb1 (ext4, btrfs 모두 mkfs.format 형태)

   /dev/sdb1의 UUID 값 확인 명령 (종류 확인) ➜ blkid /dev/sdb1

   a.txt 파일 문자를 전부 소문자 변환 b.txt 백업 ➜ dd if=a.txt of=b.txt conv=lcase //대문자 ucase

   /dev/sdb1 내용 그대로 /dev/sdc1 백업(블록크기 1K) ➜ dd if=/dev/sdb1 of=/dev/sdc1 bs=1k

스왑파일 생성 형식	**dd if=[입력파일] of=[출력파일] [옵션]**
1G 스왑파일생성	dd if=/dev/zero of=/swapfile bs=1k count=1024000
스왑영역 설정	mkswap /swapfile
스왑파일 활성화	swapon /swapfile

4. 디스크 추가(/etc/fstab)

   Q) ext4 포맷 /dev/sdb1을 /home2로 자동 마운트 되도록 설정, Quota 설정

   ➜ vi /etc/fstab

   /dev/sdb1 /home2 ext4 defaults,usrquota,grpquota 0 0

5. #쿼터 설정(quota, edquota)

   쿼터 정보 확인 ➜ quota user1

   user1 쿼터 용량을 user2에 동일하게 부여 ➜ edquota -p user1 user2

   user1 쿼터 설정 ➜ edquota user1

   유예기간 설정 ➜ edquota -t

6. #파일시스템 점검

   XFS ➜ xfs_refair /dev/sdb1

   Btrfs ➜ btrfs check

   ext4, vafat, exfat ➜ fsck.format (fsck.ext4 /dev/sda1)

7. #crontab

   Q) ihd 사용자가 예약한 cron작업 파일을 삭제 ➜ rm /var/spool/cron/ihd

   Q) /etc/heartbeat.sh 명령을 매주 일요일 10분 주기 실행 (분/시/일/월/요일)➜ 0-59/10 * * * 0

   Q) ihd 사용자가 예약한 작업 시간 변경을 위해 해당 사용자의 cron을 불러온다

   ➜ crontab -e -u ihd

   Q) /home/ihd/work.sh 명령을 1월부터12월까지 2개월마다 1일 오전 오전 4시 10분에 실행

   ➜ 10 4 1 1-12/2 * /home/ihd/work.sh

8. #컴파일 C

   sum.c 를 컴파일하여 object 생성 ➜ gcc -c sum.c

   sum.o avg.o 2개의 object 이용하여 실행파일 생성 ➜ gcc -o sum.o avg.o

9. #압축 (tar, gz, bz2, xz)

형식	확장자	압축	해제
tar	.tar	tar -cvf file.tar target	tar -xvf file.tar
gzip	.gz	gzip filename	gunzip filename
tar+gzip	.tar.gz	tar -zcvf file.tar.gz target	tar -zxvf file.tar.gz
tar+bzip2	.tar.bz2	tar -jcvf file.tar.bz2 target	tar -jxvf file.tar.bz2
tar+xz	.tar.xz	tar -Jcvf file.tar.xz target	tar -Jxvf file.tar.xz

tar를 이용하여 현재 디렉토리의 object를 묶어 obj.tar로 생성 ➜ tar -cf obj.tar *.o

linux.tar.xz 파일 압축 해제 ➜ tar -Jxvf linux.tar.xz

10. #모듈

리눅스 커널에 적재된 모든 정보 출력 ➜ lsmod

모듈의 alias, alias symbol, blacklist등 다양한 정보 출력 ➜ modprobe -c

iptable_filter 모듈 제거하면서 관련 모듈도 같이 제거 ➜ modprobe -r iptable_filter

vfat 모듈 정보 출력 ➜ modinfo vfat

모듈간 의존성 정보 갱신 ➜ depmod

모듈 의존성 정보 ➜ cat /lib/modules/*kernel version*/modules.dep

11. #볼륨

구분	스캔	생성	조회
물리 볼륨	pvscan	pvcreate	pvdisplay
모든 볼륨그룹	vgscan	vgcreate	vgdisplay
논리 볼륨	lvscan	lvcreate	lvdisplay

/dev/sdb1, /dev/sdc1 파티션을 물리적 볼륨으로 구성 ➜ pvcreate /dev/sdb1 dev/sdc1

물리적 볼륨을 lvm0이라는 볼륨 그룹으로 구성 ➜ vgcreate lvm0 /dev/sdb1 /dev/sdc1

lvm0에서 2G 논리적 볼륨 생성 이름 kdata1 ➜ lvcreate -L 2000M -n kdata1 lvm0

12. #시스템 로그설정 (/etc/rsyslog.conf)

facility	priority	action
auth(인증)	emerg (사용불가)	/path/*.log (지정로그에 메시지 기록)*
authpriv(보안,승인)	alert (즉시조치 필요)	*/dev/console (콘솔 메시지)*
cron(예약)	crit (심각)	*/dev/tty3 (특정터미널 메시지)*
daemon(ftps)	err (에러)	(로그인한 모든 사용자에 메시지)
mail	warning (경고)	root, admin (root, admin 터미널 메시지)
news	notice (안내)	@ip.or.domain(원격서버 udp514 전송)
syslog	info (정보)	@@ip.or.domain(원격서버 tcp 전송)
user, uucp local0~7	debug , none	

모든서비스에 최고수준의 위험 모든 사용자 터미널로 로그 전송➜ * .emerg *

ssh와 같은 인증 관련 로그는 /var/log/ssh.log에 기록 ➜ authpriv.* /var/log/ssh.log

메일시스템의 디버그 정보를 기록하기 위해 로그 레벨 설정➜ mail.debug

시스템 중요메시지만 기록하고 커널관련 로그 제외 ➜ *.=crit;kern.none

중요에러를 192.168.5.13으로 전송➜ *.crit @@192.168.5.13

모든서비스의 error 이상 메시지만 /var/log/critcal 파일에 기록하는데 커널 제외

➜ *.err;kern.none /var/log/critcal

모든서비스의 alert 수준 메시지만 로그인된 root 사용자의 터미널로 보내기➜ *.=alert root

메일시스템 모든 로그는 /maillog에 기록, debug 수준만 제외 ➜ mail. *;mail.!=debug /maillog

uucp, news발생 warning이상 로그는 /newslog에 기록 ➜ uucp,news.warn /newslog

모든서비스의 alert 수준 이상 메시지는 udp 192.10.10.10으로 전송➜ *.alert @192.10.10.10

13. #로그로테이트

(전체정책-/etc/logrotate.conf)

weekly //주 1회

rotate 4 // 4주간 백업 보관

create //회전 후 새 로그파일 생성

dateext // 로그뒤에 날짜

include/logrotate.d //개별 설정 포함

(개별정책-/etc/logrotate.d/btmp)

```
/var/log/btmp {
missingok           # 로그파일이 없어도 에러없음
weekly              # 일주일 단위로 로테이션
size 1M             # 파일 크기가 1MB에 도달하면 즉시 로테이션
create 0600 root utmp   # 새 파일의 권한 및 소유자/그룹 지정
rotate 4            # 4개 백업 파일 보관
}
```

(개별정책-/etc/logrotate.d/app)

```
/var/log/myapp/*.log {
    daily       # 매일
    rotate 7    # 7개 보관
    compress    # 압축
    notifempty  # 비어 있으면 회전 안함
    create 640 root adm       # 새파일 권한 소유자/그룹
}
```

14. #로그명령

시스템로그에 메시지 기록 ➜ logger

시스템 일반적 로그파일 위치 ➜ /var/log/message

인증기반 접속 관련 로그 ➜ /var/log/secure

불법로그인 시도 확인 ➜ lastb [특정사용자 lastb id]

불법로그인 시도 로그 ➜ /var/log/btmp

최근 3일 로그인한 사용자 기록 출력 ➜ lastlog -t 3

kaituser 사용자의 마지막 로그인 정보 출력 ➜ lastlog -u kaituser

ihduser 사용자의 로그인 정보 출력 ➜ last ihduser

15. #SELinux 설정 (영구설정 /etc/selinux/config)

getenforce (상태 확인, Permissive, Enforcing)

setenforce 0 (Permisssive mode, 재부팅 전까지)

setenforce 1 (Enforcing mode, 재부팅 전까지)

16. #백업 (dump, restore, cpio)

/home 의 파일을 home.xdump 파일로 백업 ➜ dump -0f home.xdump /home

home.xdump 파일을 /home 디렉토리 복원 ➜ restore -rf home.xdump /home

/home 영역을 home.backup 파일로 백업하는데 진행되는 과정을 화면에 출력

➜ find /home | cpio -ocv > home.backup

백업내용 확인 ➜ cpio -tv < home.backup

home.backup를 이용하여 데이터 복원하는데 진행과정 화면에 출력

➜ cpio -icdv < home.backup

17. #원격백업 (rsync)

ip 192.168.100.10 의 /home 디렉토리를 로컬시스템으로 복사, root 권한접속하여 허가권,타임스탬프등 그대로 유지하며 진행상황표시, 전송시 압축 사용할 것

rsync -avz root@192.168.10.10:/home /mnt/backup/homeback

- `-a` : archive 모드. 권한, 소유자, 그룹, 타임스탬프, 심볼릭 링크 등 모두 보존.
- `-v` : verbose(진행상황 자세히 표시).
- `-z` : 전송 중 데이터 압축.
- `root@192.168.100.10:/home` : 원격지 소스 경로.
- `/로컬/저장/경로` : 복사할 로컬 경로로 변경.

18. #iptables NAT 설정

POSTROUTING 체인 SNAT(Source NAT) : 출발지 IP를 변경(내부->외부)

PREROUTING 체인 DNAT(Destination NAT) : 목적지 IP를 변경(외부->내부)

POSTROUTING 체인 규칙 확인 ➜ iptables -t nat -L POSTROUTING

PREROUTING 체인 규칙 확인 ➜ iptables -t nat -F PREROUTING

iptables -R (정책 수정) iptables -D (정책 제거) iptables -A (정책 추가)

Q) PREROUTING 체인에 규칙 추가 (80으로 오는 트래픽을 192.168.1.100 으로 전달)

A) iptables -A PREROUTING -p tcp —dport 80 -j DNAT —to-destination 192.168.1.100

Q) iptables 기반으로 1개의 공인 ip를 공유하여 다수 컴퓨터 사용환경 구축. 해당 시스템에는 이더넷카드 2개 중 1개에 공인IP(static)가 설정되어 있고, 해당 ip는 211.100.50.14이다.

- eth0: 외부망(공인 IP, 211.100.50.14)
- eth1: 내부망(사설 IP, 예: 192.168.0.1)

A) iptables -t nat -A POSTROUTING -o eth0 -j SNAT —to 211.100.50.14

Q) eth0 인터페이스로 나가는 모든 패킷의 출발지 IP를 203.0.113.10으로 변경

A) iptables -t nat -A POSTROUTING -o eth0 -j SNAT --to-source 203.0.113.10

Q) 203.0.113.10의 80번 포트로 들어오는 TCP 패킷을 내부 192.168.1.100:80으로 전달

A) iptables -t nat -A PREROUTING -d 203.0.113.10 -p tcp --dport 80 -j DNAT --to-destination 192.168.1.100:80

기본테이블 필터의 모든 사슬에 정책정보 출력 ➜ iptables -L

기본테이블 필터의 모든 사슬에 정책정보 숫자 값 출력 ➜ iptables -nL

기본테이블 필터의 모든 사슬에 정책정보 자세히 출력 ➜ iptables -vL

기본테이블 필터의 INPUT 사슬에 정책 정보 출력, 앞에 번호-> iptables -L INPUT —line-numbers

NAT 테이블의 모든 테이블에 정책 정보를 출력 ➜ iptables -t nat -L

19. #프로세스 우선순위(nice / renice)

구분	주요기능 및 차이(-20 ~ 19)
nice nice -n 숫자 프로세스명	새로운 프로세스 실행시 우선 순위 지정 nice -n 10 tar cf backup.tar /home
renice renice -n 숫자 -p PID	이미실행중인 프로세스 우선 순위 조정 renice -n 20 -p 1345623 1348234

bash 우선순위 -39 지정 ➜ nice -n 39 bash ## -20이 최대이므로 -20으로 설정 됨
1222 프로세스의 우선순위 -20 지정 ➜ renice -n -20 -p 1222
tomcat 그룹의 우선순위 -10 지정 ➜ renice -n -10 -g tomcat

20. 패키지관리자(dnf/yum/rpm)

구분	역할	사용법
dnf	yum 차세대 버전 centos/rhel 8, Fedora 22+ 기본	dnf install package
yum	rpm 기반 고수준 패키지 관리	yum install package
rpm	.rpm파일 설치/삭제/조회	rpm -ivh package.rpm

yum을 통한 vim 패키지 검색 ➜ yum search vim
yum 현재 활성화된 저장소 확인 ➜ yum repolist
yum powertools 저장소 활성화 ➜ yum —enablerepo=powertools
yum curl 패키지 설치 ➜ yum install curl
yum sendmail 문자열이 있는 패키지 검색 ➜ yum search sendmail
yum 작업이력 확인 ➜ yum history
yum 작업이력 초기화 ➜ yum new

rpm sendmail 패키지 변경 정보 확인위해 검증 실시 ➜ rpm -V sendmail
rpm nmap 패키지가 설치한 파일 목록 출력 ➜ rpm -ql telnet
rpm nmap 패키지명 확인 ➜ rpm -qf /usr/bin/nmap - 절대경로 $(which nmap)
rpm nmap 패키지 정보 확인 ➜ rpm -qi nmap
rpm nmap 패키지 제거 ➜ rpm -e telnet
rpm 패키지 설치여부 확인 ➜ rpm -qa | grep 패키지키워드 (rpm -q 패키지명)

21. #커널Kernel

구분	설명
make clean	산출물(환경설정 파일 유지)
make mrproper	산출물, 환경설정 파일 삭제
make distclean	산출물, 환경설정, 백업/패치등 모든 불필요 파일 삭제

리눅스 커널을 구성하기 위해 메뉴기반 설정 인터페이스 실행 - make menuconfig
커널이미지를 빌드 - make bzImage
커널버전 확인 - uname -r
시스템에 적용된 커널 매개변수와 값을 전부 출력 ➜ sysctl -a
ping에 응답하지 않도록 커널 매개변수 변경 ➜ sysctl -w net.ipv4.icmp_echo_ignore_all=1
위 작업이 재부팅 후에도 적용되도록 파일에 등록 ➜ vi /etc/sysctl.conf

22. #SSH (/etc/ssh/sshd_config)

SSH 공개키 생성 ➜ ssh-keygen -t rsa
원격서버에 ssh 공개키 복사 ➜ ssh-copy-id id@domain.or.ip
Root 접근 차단 sshd_config ➜ PermitRootLogin no
다운로드 scp -P 2222 id@host:/remote/path/file.txt /local/path/
업로드 scp -P 2222 /local/path/file.txt id@host:/remote/path/

23. #방화벽 (firewall-cmd)

명령어	설명
firewall-cmd —permanent —add-port=80/tcp	80/tcp 영구허용
firewall-cmd —permanent —add-service=http	http 영구 허용
firewall-cmd —permanent —add-source=ip	특정 IP 영구 허용
firewall-cmd --reload	변경 적용
firewall-cmd —list-all	적용 확인

Q)웹서버를 public영역에 설정, 방화벽 정책 영구 적용되도록 설정하시오

➜ firewall-cmd —zone=public —permanent —add-service=http

24. #포트스캔 (nmap)

wellknown 포트 검색 - nmap -p0-1023 hostname or hostip

25. #RAID (mdadm)

RAID 장치인 /dev/md0에 대한 자세한 정보를 출력 ➜ mdadm -D /dev/md0

/dev/md0 장치를 비활성화 및 자원해제 ➜ mdadm -S /dev/md0

/dev/md1 구성에 사용된 /dev/sdb6 장치에 강제 오류 발생 ➜ mdadm /dev/md1 -f /dev

/dev/md1 구성에 사용된 /dev/sdb6 장치 제거 ➜ mdadm -r /dev/sdb6

2개의 HDD이용 스트라이핑 RAID 구성 명령

➜ *mdadm -C /dev/md0 -l 0 -n 2 /dev/sdb1 /dev/sdc2*

26. #프린터

linux.log 파일을 10장 출력하는 명령어, 2가지 방법으로 기재

lpr -# 10 linux.log

lp -n 10 linux.log

27. #프록시 (squid /etc/squid/squid.conf)

squid.conf 주요 설정	
# Squid가 수신할 포트 지정 (기본: 3128) http_port 3128 # 디스크 캐시 경로, 크기(MB), 1차/2차 디렉토리 수 cache_dir ufs /var/spool/squid 100 16 256 # 로그 파일 위치 cache_log /var/log/squid/cache.log access_log /var/log/squid/access.log # 캐시 서버의 관리자 이메일 cache_mgr admin@example.com # Squid 서버의 호스트 이름 visible_hostname proxy.example.com # 메모리 캐시 크기(MB) cache_mem 64 MB	# 캐시에 저장할 최대 객체 크기 (MB) maximum_object_size 4 MB # ACL(접근 제어 목록) 정의 acl localnet src 192.168.0.0/16 # 내부망 허용 acl all src 0.0.0.0/0.0.0.0 # 모든 IP # 접근 제어 규칙 http_access allow localnet # 내부망 허용 http_access deny all # 그 외 모두 차단 # 코어 덤프 디렉토리 coredump_dir /var/spool/squid # 캐시 갱신 패턴 (기본값) refresh_pattern . 0 20% 4320

Q) squid의 환경설정 파일에 접근제한 설정 과정이다. 192.168.1.0 네트워크 대역에 속한 호스트만 허가한다.
192.168.1.0 네트워크 대역은 'pass'라는 별칭으로 관리

A) acl pass src 192.168.1.0/24
http_access allow ihd
http_access deny all

28. #NFS (Network File System - /etc/exports)

Q) /ihd 디렉토리에 접근 가능한 호스트는 192.168.5.0, root 권한 읽기 쓰기 허용, /kait 디렉토리 접근 가능 호스트는 192.168.12.12만 가능, root포함 모든 사용자 권한 인정하지 않음(옵션 공백없이 작성,쉼표로구분)

A) vi /etc/exports
/ihd 192.168.5.0/24(rw,no_root_square)
/kait 192.168.12.12(rw,all_square)
exportfs -ra

29. #삼바samba (/etc/samba/smb.conf)

윈도우 호스트에서 접근시 보이는 컴퓨터명 SambaShare ➜ netbios name = SambaShare

윈도우 호스트에서 접근시 보이는 폴더명 web ➜ [web] //접근 방법 \\SambaShare\web

윈도우 운영체제 시스템과 공유 그룹명 ihd ➜ workgroup = ihd

삼바서버 설명 'ihd file server' ➜ server string = ihd file server

디렉토리 설명 'file shared dir' ➜ comment = file shared dir

디렉토리 경로 /usr/local/apache/html ➜ path = /usr/local/apache/html

접근 가능 사용자 ihduser, kaituser ➜ valid users = ihduser, kaituser

접근 가능 ip대역 192.168.1.0 ➜ hosts allow = 192.168.1. or 192.168.1.0/255.255.255.0

파일 생성 및 삭제 권한 사용자 설정 ➜ write list = ihduser

파일 생성 및 삭제 권한 설정 ➜ writable = yes or no

삼바 사용자 추가 ➜ smbpasswd -a username

30. #웹서버Apache (/usr/local/apache source 설치)

환경설정 파일 절대경로 오픈 ➜ vi /usr/local/apache/conf/httpd.conf

도메인명을 www.linux1st.kr로 지정하고 포트는 80 ➜ ServerName www.linux1st.kr:80

웹문서 경로 /usr/local/apache/html ➜ DocumentRoot "/usr/local/apache/html"

아파치 웹서버 데몬 실행 ➜ /usr/local/apache/bin/apachectl start

userdir_module 활성화 ➜ userdir_module modules/mod_userdir.so

사용자 디렉토리 설정파일 경로 ➜ conf/extra/httpd-userdir.conf

Apache에서 사용자 디렉토리 경로 지정 지시어 ➜ UserDir

추가 도메인 운영위해 설정시 관련 모듈과 환경설정 파일 활성화

➜ LoadModule vhost_alias_module modules/mod_vhost_alias.so

➜ Include conf/extra/httpd-vhosts.conf

관련 파일에서 추가 도메인 설정 진행

➜ vi /usr/local/apache/conf/extra/httpd-vhosts.conf

<VirtualHost 192.168.100.101:80>

31. #메일서버sendmail (/etc/mail/*)

파일명	용도	비고
sendmail.mc	sendmail.cf 생성용 m4 매크로 소스	
sendmail.cf	sendmail 설정파일(.mc에서 생성)	
access	릴레이 허용/차단 호스트 및 도메인	access.db(makemap 생성)
mailertable	도메인별 메일 전송경로 지정	mailertable.db
virtusertable	가상도메인별 사용자 메일 전달 지정	virtusertable.db
aliases	메일 별칭 지정	aliases.db

접근제어 목록 생성 : makemap hash /etc/mail/accdess < /etc/mail/access

가상사용자 목록 생성 : makemap hash /etc/mail/virtusertable < /etc/mail/virtusertable

별칭데이터 갱신 : newaliases

Sendmail 구성파일 생성 : sendmail.cf (m4 sendmail.mc > /etc/mail/sendmail.cf) sendmail restart

메일서버에 도메인 등록 : vi /etc/mail/local-host-names ➜ example.com

발신도메인 설정 : vi /etc/mail/sendmail.cf ➜ Djexample.com (권장하지 않음, mc파일로 생성)

Q)발신지 도메인의 spam.com에서 오는 메일 거부/별도 메시지 없음

A) vi /etc/mail/access

From:spam.com DISCARD (거부메시지 반환 REJECT)

Q)변경내용 갱신 명령 ➜ makemap hash /etc/mail/access < /etc/mail/access

Q)메일포워딩 admin계정 수신 메일 ihd와 kait에게 전달, help계정 수신메일 /etc/helpdesk 파일에 지정된 사용자에게 전달

A) vi /etc/aliases

admin: ihd, kait

help: :include:/etc/helpdesk

newaliases

32. #네임서버dns (/etc/named.conf)

/etc/named.conf	/var/named

// 네임서버 옵션 설정
options {
directory "/var/named"; // 존 파일이 위치한 디렉터리
forwarders { 8.8.8.8; 8.8.4.4; }; // 외부 DNS 포워더
allow-query { any; }; // 질의 허용 범위 (any: 모두 허용)
recursion yes; // 재귀 질의 허용
};
// 존(zone) 정의 - 정방향(Forward) 존
zone "example.com" IN {
type master;
file "example.com.zone"; // 존 데이터 파일
};
// 존(zone) 정의 - 역방향(Reverse) 존
zone "1.168.192.in-addr.arpa" IN {
type master;
file "192.168.1.rev"; // 역방향 존 파일
};
	$TTL 86400 ; 기본 TTL(초)
	@ IN SOA ns.ihd.com. mail.ihd.com. (
	2024050501 ; serial
	7200 ; refresh
	3600 ; retry
	1209600 ; expire
	86400) ; minimum
	; 네임서버 설정
	@ IN NS ns.ihd.com.
	@ IN NS mail.ihd.com.
	; 기타레코드 (www ip 192.168.5.13)
	www IN A 192.168.5.13
	; MX 레코드(메일서버가 mail.ihd.com.일 때)
	@ IN MX 10 mail.ihd.com.
	; 네임서버 및 메일서버의 A 레코드
	ns IN A 192.168.5.13
	mail IN A 192.168.5.14

Q)도메인 질의를 다른 dns 8.8.8.8로 넘기는데, 응답이 없을때도 처리하지 않는 설정

A) options {
forwarders { 8.8.8.8; };
forward only; //forward first; 응답 없을시 재귀적 수행
}

Q)zone 파일의 내용을 복사할 대상으로 192.168.5.0 네트워크대역의 호스트만 허가

A) allow-transfer { 192.168.5/24; };

Q) 네임서버 질의 가능호스트 192.168.12.0 네트워크대역, 192.168.3.13 만 가능

A) allow-query { 192.168.12/24; 192.168.3.13; };

Q) DNS ReverseZone 파일 설정(ip 10.0.0.10, domain ihd.or.kr, mail admin@ihd.or.kr, 네임서버 ns.ihd.or.kr 사용, 10.0.0.10 조회시 ihd.or.kr 나타나도록 설정

A) @ IN SOA ns.ihd.or.kr. admin@ihd.or.kr. (
- 중략 -
)
IN NS ns.ihd.or.kr. // ihd.or.kr의 권한있는 네임서버
10 IN PTR ihd.or.kr. //ip끝자리가 ihd.or.kr

Q) DNS Zone 파일 설정(ip 10.0.0.10, domain ihd.or.kr, mail admin@ihd.or.kr, ihd.or.kr 도메인으로 메일 받을 수 있도록 설정, www도메인 사용호스트 ip 111.20.20.10으로 설정

A) @ IN SOA ns.ihd.or.kr. admin.ihd.or.kr. (
- 중 략 -
)
IN NS ns.ihd.or.kr.
IN MX 10 ihd.or.kr.

ns IN A 10.0.0.10
www IN A 111.20.20.10

33. #FTP (/etc/vsftpd/vsftpd.conf)

VSFTP의 익명사용자 허용 ➜ anonymous_enable=YES
로컬 사용자의 chroot 환경 설정 ➜ chroot_local_user=YES
chroot 환경 쓰기권한 허용 ➜ allow_writeable_chroot=YES
VSFTP 접속차단 사용자 목록 파일 경로 ➜ /etc/vsftpd/ftpusers
특정사용자 접속을 허용위한 파일 경로 ➜ /etc/vsftpd/user_list

34. #DHCP 서버 (/etc/dhcp/dhcpd.conf)

/etc/dhcp/dhcpd.conf 주요 설정 항목	주요 구문

default-lease-time 600; # 기본 임대 시간(sec)
max-lease-time 7200; # 최대 임대 시간(sec)
 	
subnet 192.168.1.0 netmask 255.255.255.0 {
range 192.168.1.100 192.168.1.240; # 할당 IP 범위
option routers 192.168.1.1; # 게이트웨이
option domain-name-servers 8.8.8.8, 8.8.4.4; # DNS
option domain-name "example.com"; # 도메인
option broadcast-address 192.168.1.255; # 브로드캐스트
 	
host fantasia {
hardware ethernet 08:00:07:26:c0:a5;
fixed-address fantasia.example.com;
# 또는 fixed-address 192.168.1.200; 	
}
}
	기본라우터 설정
	option routers
	
	dns서버 IP
	option domain-name-servers
	
	도메인이름
	option domain-name
	
	브로드캐스트 주소
	option broadcast-adddress

Q) MAC주소가 08:00:07:26:c0:a5 인 경우에는 고정IP 192.168.1. 200 IP를 할당하고 호스트명은 ihd_com으로 관리한다.

A) host ihd_com {
hardware ethernet 08:00:07:26:c0:a5;
fixed-address 192.168.1.200;
}