🌐 IT 네트워크 시스템 *IT Network Systems Administration* 🏵

Written by ***Donghyun Choi*** (**KGU**)

✨ - Worldskills Korea ▫ Assessment Task (IT Network Systems) - 💫 [*Written by NullBins*]

- By default, the commands are executed as a root user.

[*Project-1*] < *Linux Environments*>

1. 네트워크 구성 (Network Configuration)

- ✨ *서버 및 호스트 네트워크 IP 설정* 호스트네임 변경 및 IP 주소 지정.

< ***Configuration*** >

- [**DONG-R**]

```
ip link show            # 네트워크 이더넷 이름 확인 (ex. ens3X | ens32, ens33)
```

```
vim /etc/network/interfaces
```

```
auto ens32 ens33
iface ens32 inet static
  address 117.121.35.100/24
iface ens33 inet static
  address 192.168.1.254/24
  dns-nameservers 192.168.1.1
```

```
vim /etc/resolv.conf
```

```
nameserver 192.168.1.1
domain donghyun.net
search donghyun.net
```

```
vim /etc/hosts
```

```
  127.0.1.1   DONG-R.donghyun.net     DONG-R
```

```
hostnamectl set-hostname DONG-R
reboot
```

- [**DONG-SRV1**]

```
ip link show            # 네트워크 이더넷 이름 확인 (ex. ens3X | ens32)
```

```
vim /etc/network/interfaces
```

```
  auto ens32
  iface ens32 inet static
    address 192.168.1.1/24
    gateway 192.168.1.254
    dns-nameservers 192.168.1.1 192.168.1.2
```

```
vim /etc/resolv.conf
```

```
  nameserver 192.168.1.1
  nameserver 192.168.1.2
  domain donghyun.net
  search donghyun.net
```

```
vim /etc/hosts
```

```
  127.0.1.1   DONG-SRV1.donghyun.net     DONG-SRV1
```

```
hostnamectl set-hostname DONG-SRV1
reboot
```

- [**DONG-SRV2, DAE-R, DAE-SRV**] -> 과제지를 참고하여 위처럼 동일하게 설정.

---

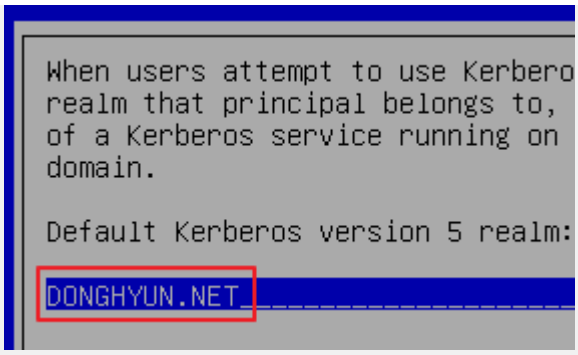
2. SAMBA AD 서비스 구성 (Samba Active Directory Service Configuration)

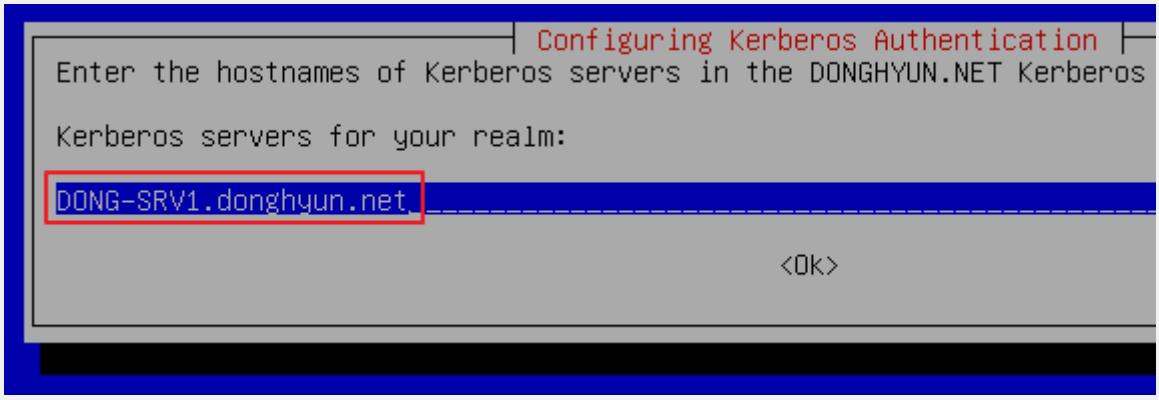
- ✨ *DONG-SRV1 에서 Samba Active Directory Service 구성* 구성 시 패키지 도구는 BIND9 및 SAMBA-AD-DC를 사용함.

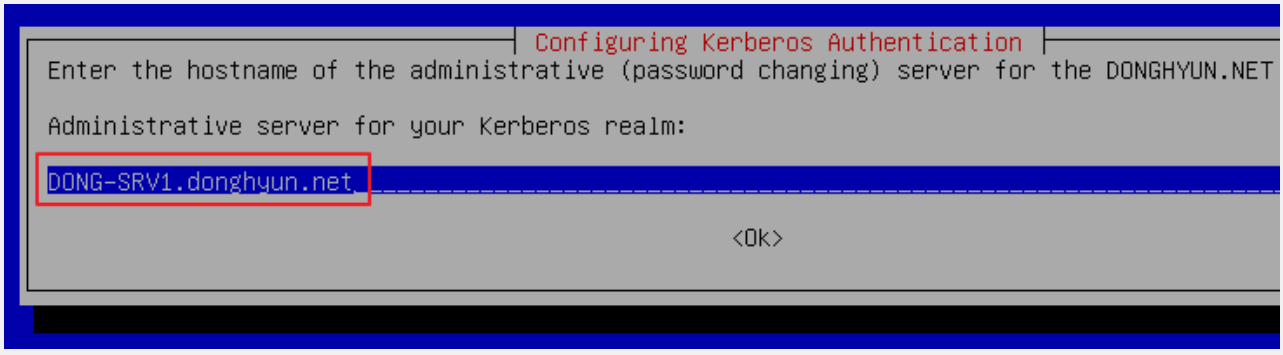
< *Configuration* >

- [**DONG-SRV1**]

```
apt install bind9 krb5-user krb5-config winbind samba smbclient migrationtools
ldb-tools -y
```







```
mv /etc/samba/smb.conf /etc/samba/smb.conf.bak
samba-tool domain provision --use-rfc2307 --interactive
```

```
root@DONG-SRV1:~# samba-tool domain provision --use-rfc2307 --interactive
Realm [DONGHYUN.NET]:
Domain [DONGHYUN]:
Server Role (dc, member, standalone) [dc]:
DNS backend (SAMBA_INTERNAL, BIND9_FLATFILE, BIND9_DLZ, NONE) [SAMBA_INTERNAL]: BIND9_DLZ
Administrator password:
Retype password:
```

```
cp /var/lib/samba/private/krb5.conf /etc/
```

```
vim /var/lib/samba/bind-dns/named.conf
```

```
dlz "donghyun.net" {
   database "dlopen /usr/lib/x86_64-linux-gnu/samba/bind9/dlz_bind9_16.so";
};
```

```
cat /var/lib/samba/bind-dns/named.txt | grep tkey >> /etc/bind/named.conf
```

```
vim /etc/bind/named.conf
```

```
// include "/etc/bind/named.conf.options";
// include "/etc/bind/named.conf.local";
include "/etc/bind/named.conf.default-zones";
include "/var/lib/samba/bind-dns/named.conf";

options {
   directory "/var/cache/bind";
   listen-on { any; };
   allow-query { any; };
   allow-update { any; };
   dnssec-validation no;
   tkey-gssapi-keytab "/var/lib/samba/bind-dns/dns.keytab";
};

zone "1.168.192.in-addr.arpa" {
   type master;
   file "192.rev";
};
```

```
zone "daeseong.net" {
   type forward;
   forwarders { 172.16.1.1; };
};
```

```
systemctl restart bind9
systemctl stop smbd nmbd winbind
systemctl disable smbd nmbd winbind
systemctl unmask samba-ad-dc
systemctl enable samba-ad-dc
systemctl restart samba-ad-dc
kinit Administrator
cd /usr/share/migrationtools/
```

```
vim migrate_common.ph
```

```
$NAMINGCONTEXT{'passwd'}    = "ou=DONG";
$DEFAULT_MAIL_DOMAIN = "donghyun.net";
$DEFAULT_BASE = "dc=donghyun,dc=net";
```

```
cp migrate_common.ph /usr/share/perl5/
./migrate_base.pl > ou.ldif
```

```
vim ou.ldif
```

```
1 dn: ou=DONG,dc=donghyun,dc=net
2 ou: DONG
3 objectClass: top
4 objectClass: organizationalUnit
```

```
ldbadd -H /var/lib/samba/private/sam.ldb ou.ldif
```

```
vim /root/users.sh
```

```

```

```
#!/bin/bash
for i in {01..05}
do
   samba-tool user create user1$i Skill39 --userou=ou=DONG --uid-number=10$i
--gid-number=1000 --script-path=/bin/bash --home-directory=/home/user1$i
   samba-tool user create visitor1$i Skill39 --userou=ou=DONG --uid-
number=20$i --gid-number=2000 --script-path=/bin/bash --home-
directory=/home/visitor1$i
done
```

```
chmod +x /root/users.sh
bash /root/users.sh
```

```
kinit Administrator
klist
wbinfo -u
```

- [**DONG-SRV2**]

```
apt install krb5-user krb5-config winbind samba smbclient -y
mv /etc/samba/smb.conf /etc/samba/smb.conf.bak
scp DONG-SRV1:/etc/krb5.conf /etc/
kinit Administrator
samba-tool domain join donghyun.net DC -UAdministrator
systemctl stop smbd nmbd winbind
systemctl disable smbd nmbd winbind
systemctl unmask samba-ad-dc
systemctl enable samba-ad-dc
systemctl restart samba-ad-dc
```

---

3. DNS 서비스 구성 (DNS Service Configuration)

- ✨ *DONG-SRV 및 DAE-SRV, DNS 도메인 네임서버 구성* 구성 시 패키지 도구는 BIND9을 사용함.

< ***Configuration*** >

- [**DONG-SRV1**]

```
kinit Administrator
```

```
samba-tool dns add 192.168.1.1 donghyun.net www.donghyun.net CNAME DONG-
SRV1.donghyun.net
samba-tool dns add 192.168.1.1 donghyun.net mail.donghyun.net CNAME DONG-
SRV2.donghyun.net
samba-tool dns add 192.168.1.1 donghyun.net @ MX "mail.donghyun.net 10"
samba-tool dns query 192.168.1.1 donghyun.net @ ALL -U Administrator
```

```
cp /etc/bind/db.127 /var/cache/bind/192.rev
chown bind:bind -R /var/cache/bind/
sed -i "s/localhost/DONG-SRV1.donghyun.net/g" /var/cache/bind/192.rev
```

```
vim /var/cache/bind/192.rev
```

```
1       IN      PTR     DONG-SRV1.donghyun.net
2       IN      PTR     DONG-SRV2.donghyun.net
```

```
systemctl restart bind9
```

- [**DAE-SRV**]

```
apt install bind9 -y
```

```
vim /etc/bind/named.conf
```

```
// include "/etc/bind/named.conf.options";
// include "/etc/bind/named.conf.local";
// include "/etc/bind/named.conf.default-zones";

options {
   directory "/var/cache/bind";
   listen-on { any; };
   allow-query { any; };
   dnssec-validation no;
};

view int {
   match-clients { 192.168.1.0/24; 172.16.1.0/24; localhost; };
```

```
    include "/etc/bind/named.conf.default-zones";
    zone "daeseong.net" {
        type master;
        file "int-daeseong.zone";
        allow-update { 172.16.1.254; };
    };
    zone "donghyun.net" {
        type forward;
        forwarders { 192.168.1.1; };
    };
};

view ext {
    match-clients { 117.121.35.0/24; };
    include "/etc/bind/named.conf.default-zones";
    zone "daeseong.net" {
        type master;
        file "ext-daeseong.zone";
    };
};
```

```
cp /etc/bind/db.0 /var/cache/bind/int-daeseong.zone
cp /etc/bind/db.0 /var/cache/bind/ext-daeseong.zone
chown bind:bind -R /var/cache/bind/
sed -i "s/localhost/DAE-SRV.daeseong.net/g" /var/cache/bind/int-daeseong.zone
sed -i "s/localhost/DAE-SRV.daeseong.net/g" /var/cache/bind/ext-daeseong.zone
```

```
vim /var/cache/bind/int-daeseong.zone
```

```
DAE-SRV     IN  A   172.16.1.1
www         IN  CNAME   DAE-SRV
```

```
vim /var/cache/bind/ext-daeseong.zone
```

```
DAE-SRV     IN  A   117.121.35.150
www         IN  CNAME   DAE-SRV
```

```
systemctl restart bind9
```

4. DHCP 서버 구성 (DHCP Service Configuration)

- ✨ *DONG-R 및 DAE-R, DHCP 서버 구성* 구성 시 패키지 도구는 ISC-DHCP-SERVER를 사용함.

< *Configuration* >

- [**DONG-R**]

```
apt install isc-dhcp-server -y
```

```
vim /etc/default/isc-dhcp-server
```

```
INTERFACESv4="ens33"    # 해당 인터페이스는 내부망 이더넷으로 지정해야 함.
```

```
vim /etc/dhcp/dhcpd.conf
```

```
subnet 192.168.1.0 netmask 255.255.255.0 {
   range 192.168.1.150 192.168.1.200;
   option routers 192.168.1.254;
   option domain-name "donghyun.net";
   option domain-name-servers 192.168.1.1;
   default-lease-time 600;
   max-lease-time 7200;
}

zone donghyun.net {
primary 192.168.1.1;
}

zone 1.168.192.in-addr.arpa {
primary 192.168.1.1;
}

ddns-update-style standard;
```

```
systemctl restart isc-dhcp-server
```

- [**DAE-R**]

```
apt install isc-dhcp-server -y
```

```
vim /etc/default/isc-dhcp-server
```

```
INTERFACESv4="ens33"    # 해당 인터페이스는 내부망 이더넷으로 지정해야 함.
```

```
vim /etc/dhcp/dhcpd.conf
```

```
subnet 172.16.1.0 netmask 255.255.255.0 {
   range 172.16.1.150 172.16.1.200;
   option routers 172.16.1.254;
   option domain-name "daeseong.net";
   option domain-name-servers 172.16.1.1;
   default-lease-time 600;
   max-lease-time 7200;
}

zone daeseong.net {
primary 172.16.1.1;
}

ddns-update-style standard;
```

```
systemctl restart isc-dhcp-server
```

---

5. [S2S] GRE-over-IPsec VPN 구성 (GRE-over-IPsec VPN Configuration)

- ✨ *DONG-R 및 DAE-R, VPN SITE 구성* 구성 시 패키지 도구는 STRONGSWAN을 사용함.

< ***Configuration*** >

- [**DONG-R**]

```
vim /etc/network/interfaces
```

```

```

```
auto tun0
iface tun0 inet tunnel
   address 10.0.0.1
   netmask 255.255.255.252
   dstaddr 10.0.0.2
   local 117.121.35.100
   endpoint 117.121.35.150
   mode gre
   ttl 255
   post-up ip route add 172.16.1.0/24 dev tun0
   pre-down ip route add 172.16.1.0/24 dev tun0
```

```
modprobe ip_gre
systemctl restart networking
```

```
apt install strongswan -y
```

```
vim /etc/ipsec.conf
```

```
conn GRE-IPSEC-VPN
   left=117.121.35.100
   leftprotoport=gre
   right=117.121.35.150
   rightprotoport=gre
   type=transport
   authby=secret
   keyexchange=ikev2
   auto=start
```

```
vim /etc/ipsec.secrets
```

```
117.121.35.150 117.121.35.100 : PSK "Skill39"
```

```
systemctl restart strongswan-starter
```

- [**DAE-R**]

```
vim /etc/network/interfaces
```

```
auto tun0
iface tun0 inet tunnel
   address 10.0.0.2
   netmask 255.255.255.252
   dstaddr 10.0.0.1
   local 117.121.35.150
   endpoint 117.121.35.100
   mode gre
   ttl 255
   post-up ip route add 192.168.1.0/24 dev tun0
   pre-down ip route add 192.168.1.0/24 dev tun0
```

```
modprobe ip_gre
systemctl restart networking
```

```
apt install strongswan -y
```

```
vim /etc/ipsec.conf
```

```
conn S2S-VPN
   left=117.121.35.100
   leftprotoport=gre
   right=117.121.35.150
   rightprotoport=gre
   type=transport
   authby=secret
   keyexchange=ikev2
   auto=start
```

```
vim /etc/ipsec.secrets
```

```
117.121.35.100 117.121.35.150 : PSK "Skill39"
```

```
systemctl restart strongswan-starter
```

---

6. Certificate Authority 구성 (Certificate Authority Configuration)

- ✨ *DONG-SRV1 에서 DONG-CA 인증기관 설립* 구성 시 패키지 도구는 OPENSSL를 사용함.

< *Configuration* >

- [**DONG-SRV1**]

```
apt install openssl -y
```

```
vim /etc/ssl/openssl.cnf
```

```
[ CA_default ]
dir             = /etc/ssl/DONG-CA
x509_extensions = v3_req
policy          = policy_anything

[ req_distinguished_name ]
countryName_default     = KR
#stateOrProvinceName_default       = Some-State
0.organizationName_default     = DONG
```

```
vim /usr/lib/ssl/misc/CA.pl
```

```
my $CADAYS = "-days 1825";      # 5년
my $CATOP = "/etc/ssl/DONG-CA";
```

```
/usr/lib/ssl/misc/CA.pl -newca        # CN=DONG-CA 설정
```

```
Common Name (e.g. server FQDN or YOUR name) []:DONG-CA
```

```
cp /etc/ssl/DONG-CA/cacert.pem /usr/local/share/ca-certificates/ca.crt
update-ca-certificates
```

7. LDAP 서버 구성 (LDAP Service Configuration)

- ✨ *DAE-SRV 에서 LDAP 서버 구성* 구성 시 패키지 도구는 SLAPD를 사용함.

< *Configuration* >

- [**DAE-SRV**]

```
apt install slapd migrationtools -y     # 설치시 비밀번호는 "Skill39"를 사용함.
```

```
vim /etc/ldap/ldap.conf
```

```
BASE    dc=daeseong,dc=net
URI     ldapi:///
```

```
systemctl restart slapd
ldapsearch -x       # dn: dc=daeseong,dc=net 확인
```

```
vim /root/users.sh
```

```
#!/bin/bash
for i in {01..05}
do
   echo -e "Skill39\nSkill39" | adduser --gecos "" --uid 20$i user2$i
done
```

```
chmod +x /root/users.sh
bash /root/users.sh
cd /usr/share/migrationtools/
```

```
vim migrate_common.ph
```

```

```

```
$NAMINGCONTEXT{'passwd'}     = "ou=users";
$DEFAULT_MAIL_DOMAIN = "daeseong.net";
$DEFAULT_BASE = "dc=daeseong,dc=net";
```

```
cp migrate_common.ph /usr/share/perl5/
./migrate_base.pl > ou.ldif
```

```
vim ou.ldif     # ou=users 제외하고 전부 삭제
```

```
1 dn: ou=users,dc=daeseong,dc=net
2 ou: users
3 objectClass: top
4 objectClass: organizationalUnit
```

```
./migrate_passwd.pl /etc/passwd > passwd.ldif
```

```
vim passwd.ldif     # user201 ~ user205 제외하고 전부 삭제
```

```
 1 dn: uid=user201,ou=users,dc=daeseong,dc=net
 2 uid: user201
 3 cn: user201
 4 objectClass: account
 5 objectClass: posixAccount
 6 objectClass: top
 7 objectClass: shadowAccount
 8 userPassword: {crypt}$y$j9T$.2502N.OZMPcxAADvGuVn1$5elBOApNLiC./uDguyRBN7cSDZCgsPnwTrCKtHWG094
 9 shadowLastChange: 20479
10 shadowMax: 99999
11 shadowWarning: 7
12 loginShell: /bin/bash
13 uidNumber: 2001
14 gidNumber: 65534
15 homeDirectory: /home/user201
16 gecos: ,,,
```

☑ 해당 사진처럼 user201 ~ user205 유저들만 남긴다.

```
ldapadd -cWD "cn=admin,dc=daeseong,dc=net" -f ou.ldif          # PW: Skill39
ldapadd -cWD "cn=admin,dc=daeseong,dc=net" -f passwd.ldif      # PW: Skill39
ldapsearch -x | grep dn
```

```
dn: dc=daeseong,dc=net
dn: ou=users,dc=daeseong,dc=net
dn: uid=user201,ou=users,dc=daeseong,dc=net
dn: uid=user202,ou=users,dc=daeseong,dc=net
dn: uid=user203,ou=users,dc=daeseong,dc=net
dn: uid=user204,ou=users,dc=daeseong,dc=net
dn: uid=user205,ou=users,dc=daeseong,dc=net
```

☑ 해당 사진처럼 출력되어야 한다.

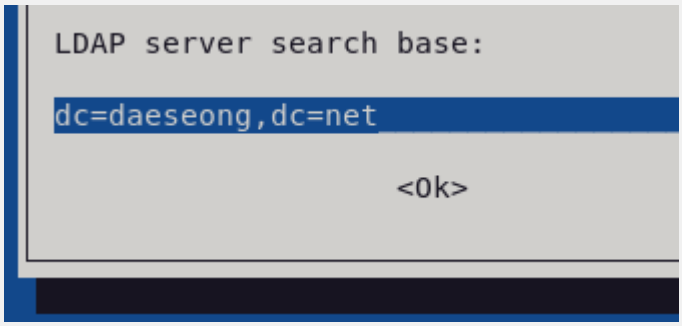
```
vim /root/users.sh
```

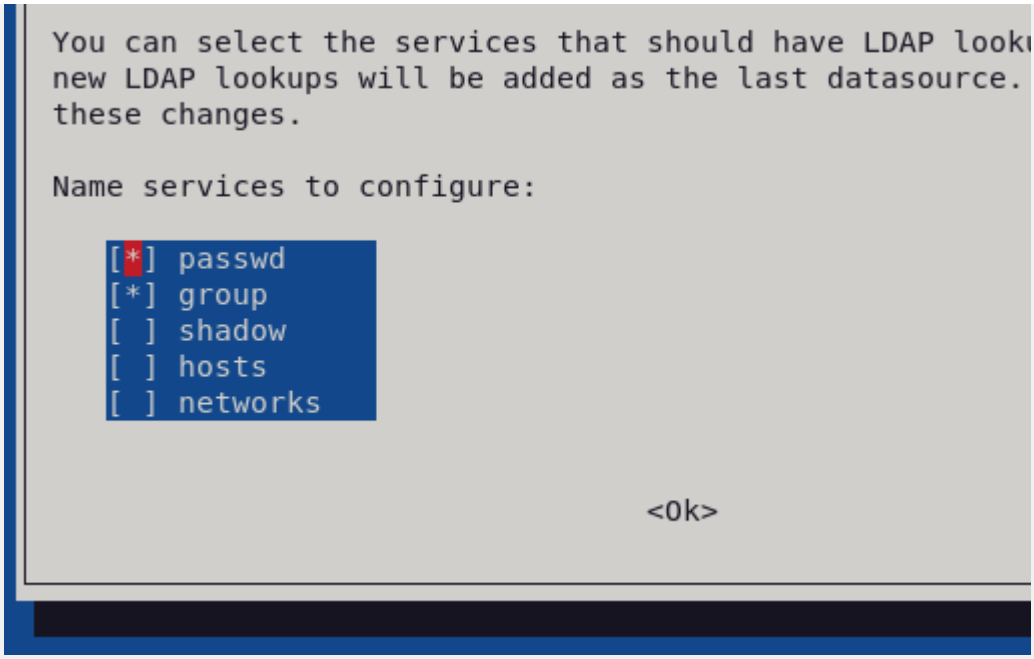
```
#!/bin/bash
for i in {01..05}
do
   # echo -e "Skill39\nSkill39" | adduser --gecos "" --uid 20$i user2$i
   userdel -r user2$i
done
```

```
bash /root/users.sh
```

- ✨ *DAE-CLI 에서 LDAP 서버 인증 설정* 구성 시 패키지 도구는 LIBNSS-LDAPD를 사용함.
- [**DONG-CLI**]

```
apt install libnss-ldapd -y
```



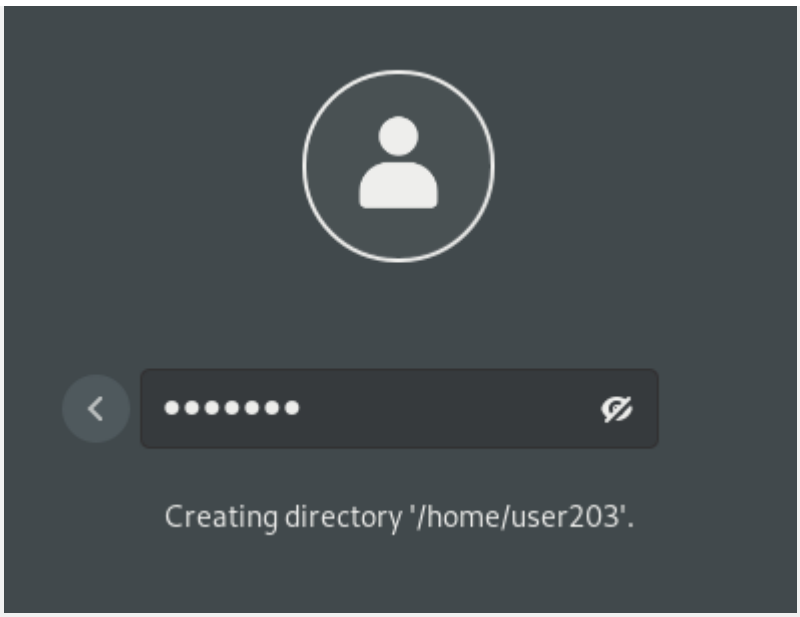


☑ 사진대로 설정

```
vim /etc/ldap/ldap.conf
```

```
BASE    dc=daeseong,dc=net
URI     ldap://DAE-SRV.daeseong.net/
```

```
echo "session optional pam_mkhomedir.so" >> /etc/pam.d/common-session
reboot
```



☑ 사진처럼 user201 ~ user205 유저로 로그인 되는지 확인

8. SSSD 구성 (Samba AD Client Joining)

- ✨ *DONG-CLI 에서 SSSD 구성*구성 시 패키지 도구는 SSSD를 사용함.

< *Configuration* >

- [**DONG-CLI**]

```
apt install krb5-user krb5-config samba sssd -y
```

```
scp DONG-SRV1:/etc/krb5.conf
```

```
vim /etc/samba/smb.conf
```

```
[global]
workgroup = DONGHYUN
realm = DONGHYUN.NET

client signing = yes
client use spnego = yes
kerberos method = secrets and keytab
security = ads
```

```
net ads join -UAdministrator
systemctl restart smbd nmbd
cp /usr/share/doc/sssd-common/examples/sssd-example.conf /etc/sssd/sssd.conf
```

```
vim /etc/sssd/sssd.conf
```

```
[sssd]
config_file_version = 2
services = nss, pam
domains = AD

[domain/AD]
id_provider = ad
auth_provider = ad

override_homedir = /home%u
```

```
default_shell = /bin/bash
ldap_id_mapping = false
enumerate = true

ad_hostname = DONG-CLI.donghyun.net
ad_server = DONG-SRV1.donghyun.net
ad_domain = donghyun.net
```

```
chown root:root /etc/sssd/sssd.conf
chmod 700 /etc/sssd/sssd.conf
echo -e "session optional pam_mkhomedir.so" >> /etc/pam.d/common-session
systemctl restart sssd
```

---

9. Docker 서버 구성 (Docker Service Configuration)

- ✨ *DONG-SRV2 에서 Docker 및 MySQL 서비스 구성* 구성 시 패키지 도구는 docker.io를 사용함.

< *Configuration* >

- [**DONG-SRV2**]

```
apt install docker* mariadb-client -y
docker load -i /mnt/mysql.tar
```

```
vim /etc/docker/daemon.json
```

```
{
   "insecure-registries":["192.168.1.2:5000"]
}
```

```
vim /etc/docker/registry/config.yaml
```

```
# auth:
#    htpasswd:
#        realm: basic-realm
#        path: /etc/docker/registry
```

```
systemctl restart docker
systemctl restart docker-registry
docker image tag mysql:latest 192.168.1.2:5000/mysql:latest
docker push 192.168.1.2:5000/mysql:latest
docker rmi 192.168.1.2:5000/mysql:latest
docker rmi mysql:latest
docker run -d --name MYSQL --hostname mysql --restart always -p 3306:3306 -e
MYSQL_ROOT_PASSWORD=Skill39 192.168.1.2:5000/mysql:latest
docker exec -it MYSQL mysql -u root -pSkill39
```

```
>create database WEB;
>create database MAIL;
>grant all privileges on *.* to 'root'@'%';
>flush privileges;
>exit
```

```
vim /root/web.sql
```

```
  create table web(
     username varchar(100) primary key not null,
     passwd varchar(100) not null
  )
```

```
vim /root/mail.sql
```

```
  create table mail(
     userid varchar(100) not null,
     uid int(100) primary key not null,
     gid int(100) not null default 65534,
     homedir varchar(100) not null default 'donghyun.net',
     password varchar(100) not null default 'Skill39'
  )
```

```
mysql -h 192.168.1.2 -u root -pSkill39 WEB < /root/web.sql
mysql -h 192.168.1.2 -u root -pSkill39 WEB < /root/mail.sql
```

```
docker cp MYSQL:/etc/my.cnf /root/
```

```
vim /root/my.cnf
```

```
[mysqld]
#secure-file-priv=/var/lib/mysql-files
general_log = 1
general_log_file = /var/log/mysql/mysql-container.log
```

```
docker cp /root/my.cnf MYSQL:/etc/
docker exec -it MYSQL bash
```

```
mkdir -p /var/log/mysql
touch /var/log/mysql/mysql-container.log
exit
```

```
docker restart MYSQL
docker exec -it MYSQL cat -n /var/log/mysql/mysql-container.log
```

---

10. Web 서버 구성 (Web Service Configuration)

- ✨ *DONG-SRV 및 DAE-SRV 에서 Web 서버 구성* 구성 시 패키지 도구는 APACHE2를 사용함.

< *Configuration* >

- [**DONG-SRV1**]

```
apt install apache2 libaprutil1-dbd-mysql maridb-client -y
```

```
cd /etc/ssl/DONG-CA/certs
openssl req -new -out dong-www.req -newkey rsa:2048 -keyout dong-www.key -nodes
# CN=www.donghyun.net
```

```
vim san
```

```
subjectAltName = DNS:www.donghyun.net
```

```
openssl ca -in dong-www.req -out dong-www.crt -extfile san        # PW: Skill39
```

```
vim /etc/apache2/sites-available/default-ssl.conf
```

```
<IfModule mod_ssl.c>
   <VirtualHost _default_:443>
       ServerName www.donghyun.net
       DocumentRoot /var/www/html
       DBDriver mysql
       DBDParams
"host=192.168.1.2,port=3306,dbname=WEB,user=root,pass=Skill39"

       <Directory /var/www/html>
           AuthType Basic
           AuthName "DB"
           AuthBasicProvider dbd
           AuthDBDUserPWQuery "SELECT passwd FROM web WHERE username = %s"
           Require valid-user
       </Directory>

       SSLCertificateFile      /etc/ssl/DONG-CA/certs/dong-www.crt
       SSLCertificateKeyFile   /etc/ssl/DONG-CA/certs/dong-www.key

       SSLCACertificatePath    /etc/ssl/DONG-CA/
       SSLCACertificateFile    /etc/ssl/DONG-CA/cacert.pem
   </VirtualHost>
</IfModule>
```

```
vim /var/www/html/index.html
```

```
<center><h2>Welcome to Donghyun Networks!</h2></center>
```

```
htpasswd -bns user01 Skill39 > /root/users.sql
```

```
vim /root/users.sql
```

```
INSERT INTO web (username, passwd) VALUES
('user01','{SHA}BerlDA2q7NChnl4D0Q1UuDmh0T8=');
INSERT INTO web (username, passwd) VALUES
('user02','{SHA}BerlDA2q7NChnl4D0Q1UuDmh0T8=');
INSERT INTO web (username, passwd) VALUES
('user03','{SHA}BerlDA2q7NChnl4D0Q1UuDmh0T8=');
INSERT INTO web (username, passwd) VALUES
('user04','{SHA}BerlDA2q7NChnl4D0Q1UuDmh0T8=');
INSERT INTO web (username, passwd) VALUES
('user05','{SHA}BerlDA2q7NChnl4D0Q1UuDmh0T8=');
INSERT INTO web (username, passwd) VALUES
('user06','{SHA}BerlDA2q7NChnl4D0Q1UuDmh0T8=');
INSERT INTO web (username, passwd) VALUES
('user07','{SHA}BerlDA2q7NChnl4D0Q1UuDmh0T8=');
INSERT INTO web (username, passwd) VALUES
('user08','{SHA}BerlDA2q7NChnl4D0Q1UuDmh0T8=');
INSERT INTO web (username, passwd) VALUES
('user09','{SHA}BerlDA2q7NChnl4D0Q1UuDmh0T8=');
INSERT INTO web (username, passwd) VALUES
('user10','{SHA}BerlDA2q7NChnl4D0Q1UuDmh0T8=');
```

```
mysql -h 192.168.1.2 -u root -pSkill39 WEB < /root/users.sql
```

```
a2enmod ssl dbd authn_dbd
a2ensite default-ssl.conf
systemctl restart apache2
```

- [**DAE-SRV**]

```
apt install apache2 php libapache2-mod-php -y
```

```
cd /etc/ssl/DONG-CA/certs
openssl req -new -out dae-www.req -newkey rsa:2048 -keyout dae-www.key -nodes
# CN=www.daeseong.net
```

```
vim san
```

```
subjectAltName = DNS:www.daeseong.net
```

```
openssl ca -in dae-www.req -out dae-www.crt -extfile san        # PW: Skill39
```

```
vim /etc/apache2/apache2.conf
```

```
<Directory /var/www/php>
   AuthType basic
   AuthName "ldap"
   AuthBasicProvider ldap
   AuthLDAPURL "ldap://DAE-SRV.daeseong.net/dc=daeseong,dc=net?uid"
   Require valid-user
</Directory>
```

```
vim /etc/apache2/sites-available/default-ssl.conf
```

```
<IfModule mod_ssl.c>
   <VirtualHost _default_:443>
       ServerName www.daeseong.net
       DocumentRoot /var/www/php

       SSLCertificateFile      /etc/ssl/DONG-CA/certs/dae-www.crt
       SSLCertificateKeyFile   /etc/ssl/DONG-CA/certs/dae-www.key

       SSLCACertificatePath    /etc/ssl/DONG-CA/
       SSLCACertificateFile    /etc/ssl/DONG-CA/cacert.pem
   </VirtualHost>
</IfModule>
```

```
mkdir -p /var/www/php
```

```
vim /var/www/php/index.php
```

```
<?php
   $username = $_SERVER['REMOTE_USER'];
```

```
    echo "<center><h2>Welcome to Daeseong Networks, $username</h2></center>";
?>
```

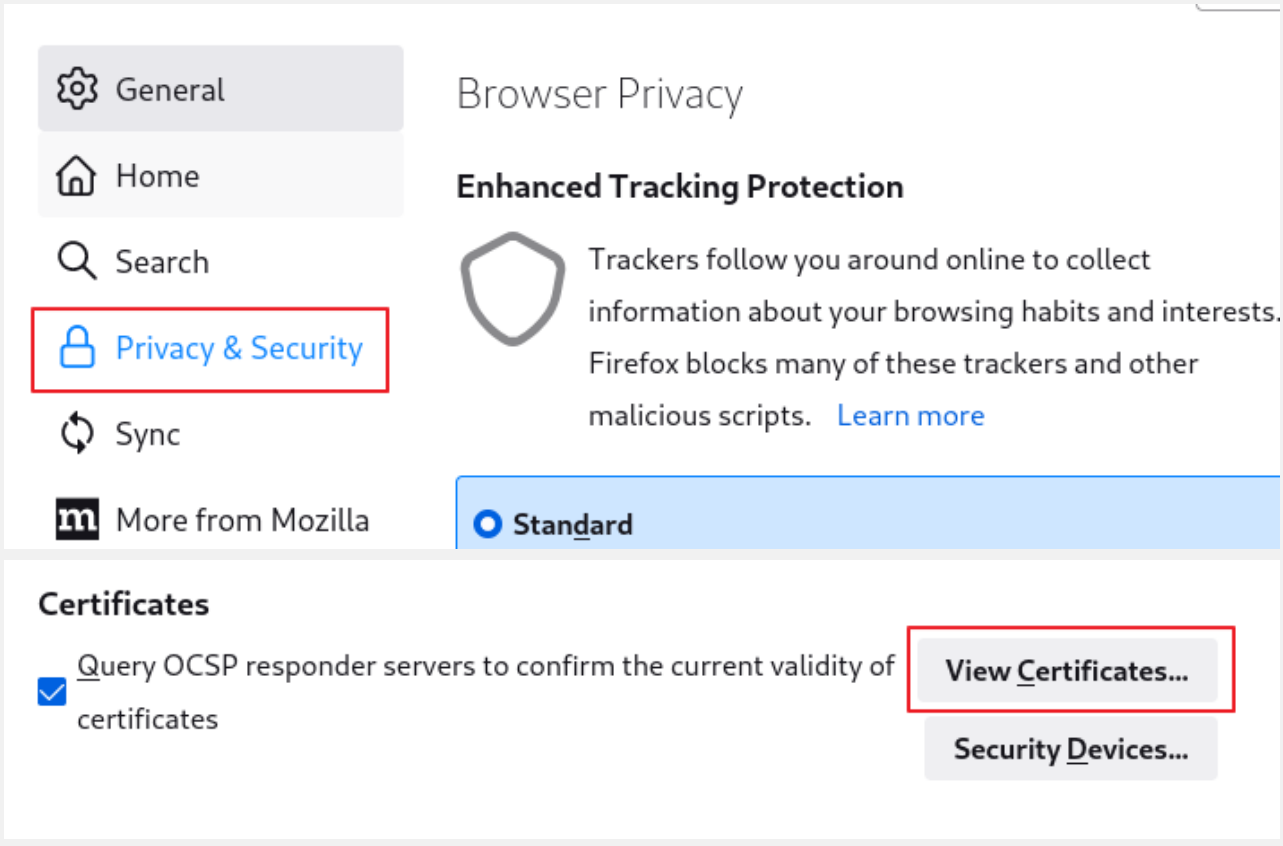
```php
<?php
        $username = $_SERVER['REMOTE_USER'];
        echo "<center><h2>Welcome to Daeseong Networks, $username</h2></center>";
?>
```

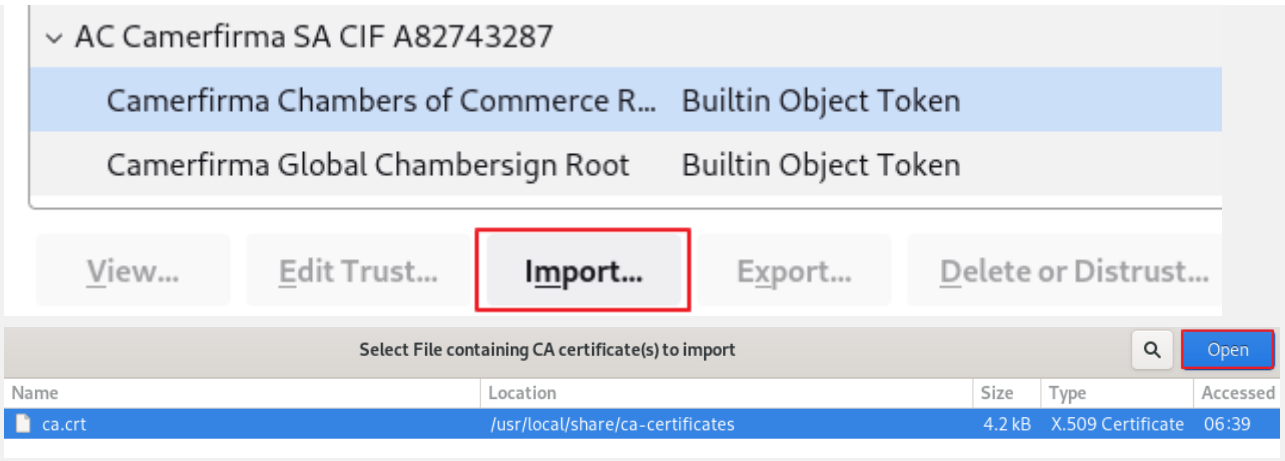
```
a2enmod ssl authnz_ldap
a2ensite default-ssl.conf
systemctl restart apache2
```

- ✨ *DONG-CLI 및 DAE-CLI 에서 Web 서버 인증 설정* DONG-CA에서 RootCA 인증서를 가져와 인증합니다.
- [**DONG-CLI**]

```
scp root@dong-srv.donghyun.net:/etc/ssl/DONG-CA/cacert.pem /usr/local/share/ca-certificates/ca.crt
update-ca-certificates
```

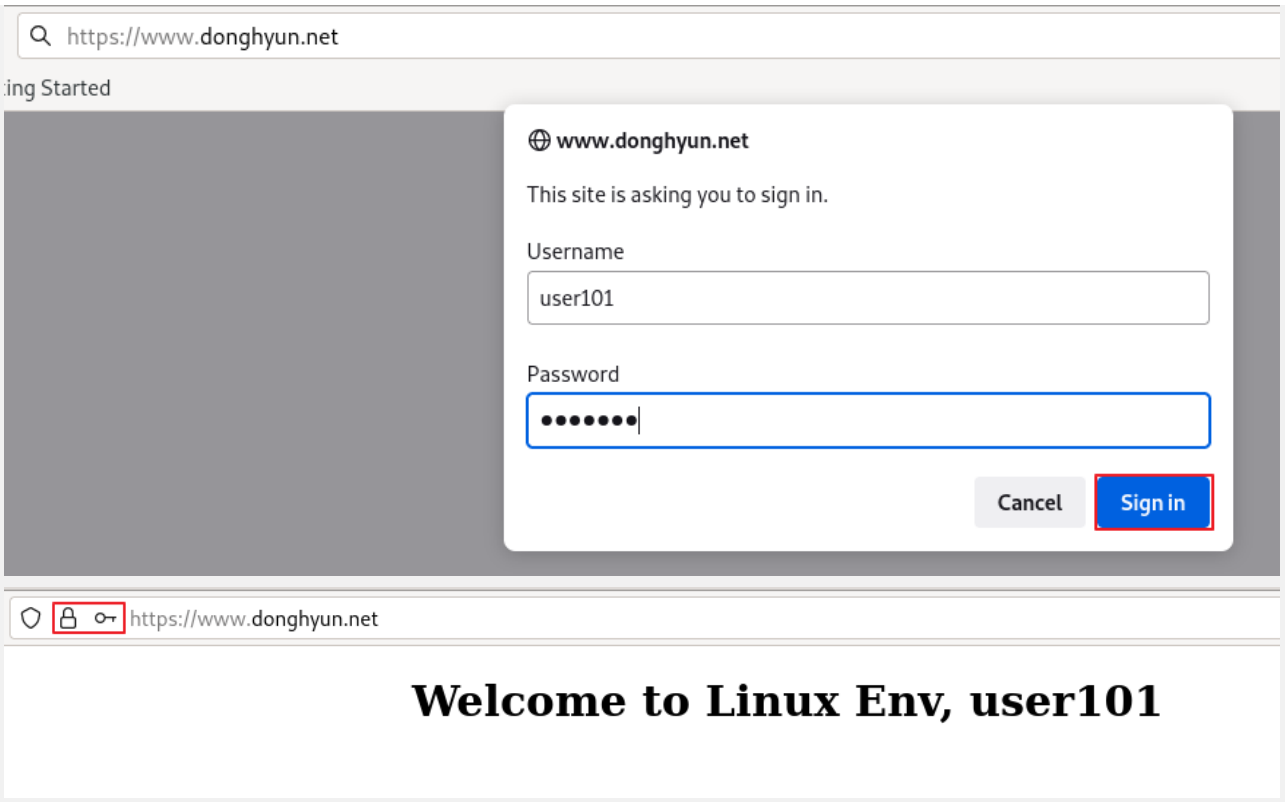
Open Firefox





☑ 위와 같이 설정합니다.

- ✨ *Web 서버 접속 테스트*



☑ 위와 같이 뜨면 성공입니다.

- [**DAE-SRV, DAE-CLI**] -> 과제지를 참고하여 위처럼 동일하게 Web Service 설정.

---

11. MAIL 서버 구성 (Mail Service Configuration)

- ✨ *DONG-SRV2 에서 Mail 서비스 구성* 구성 시 패키지 도구는 POSTFIX 및 DOVECOT을 사용함.

< *Configuration* >

- [**DONG-SRV1**]

```
openssl req -new -out mail.req -newkey rsa:2048 -keyout mail.key -nodes         #
CN=mail.donghyun.net
openssl ca -in mail.req -out mail.crt
```

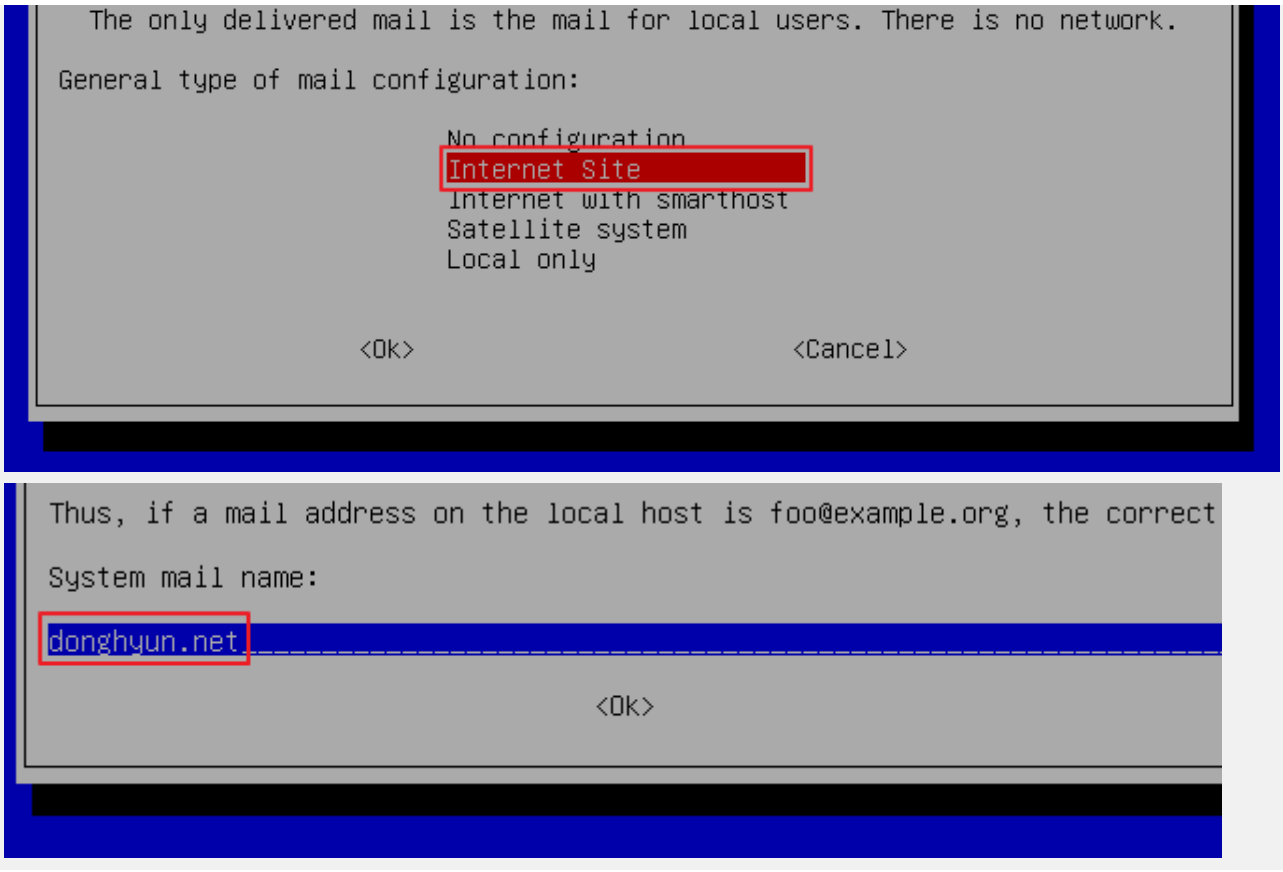
- [**DONG-SRV2**]

```
vim /root/mail-users.sql
```

```
INSERT INTO mail (userid, uid, homedir) VALUES
('user101','1001','/home/user101');
INSERT INTO mail (userid, uid, homedir) VALUES
('user201','2001','/home/user201');
```

```
mysql -h 192.168.1.2 -u root -pSkill39 MAIL < /root/mail-users.sql
scp DONG-SRV1:/etc/ssl/DONG-CA/certs/mail.* /etc/ssl/
```

```
apt install postfix dovecot-imapd dovecot-mysql dovecot-lmtpd -y
```



```
vim /etc/postfix/main.cf
```

```
# TLS parameters
smtpd_tls_cert_file=/etc/ssl/mail.crt
smtpd_tls_key_file=/etc/ssl/mail.key
smtpd_use_tls=yes

myhostname = mail.donghyun.net
mydestination = localhost
mynetworks = 0.0.0.0/0

virtual_mailbox_domains = donghyun.net
virtual_transport = lmtp:mail.donghyun.net
virtual_mailbox_maps = texthash:/etc/postfix/vmailbox
```

```
vim /etc/postfix/master.cf
```

```
smtps     inet  n       -       y       -       -       smtpd
   -o syslog_name=postfix/smtps
   -o smtpd_tls_wrappermode=yes
```

```
vim /etc/postfix/vmailbox
```

```
user101@donghyun.net user101@donghyun.net
user201@donghyun.net user201@donghyun.net
```

```
systemctl restart postfix
```

```
vim /etc/dovecot/conf.d/10-mail.conf
```

```
mail_location = maildir:/mail/%n/
```

```
vim /etc/dovecot/conf.d/10-ssl.conf
```

```
ssl = yes

ssl_cert = </etc/ssl/mail.crt
ssl_key = </etc/ssl/mail.key
```

```
vim /etc/dovecot/conf.d/10-master.conf
```

```
service lmtp {
   unix_listener lmtp {
   }
   inet_listener lmtp {
       address = 192.168.1.2
       port = 24
   }
}
```

```
vim /etc/dovecot/conf.d/10-auth.conf
```

```
disable_plaintext_auth = no

auth_username_format = %n

#!include auth-system.conf.ext
!include auth-sql.conf.ext
```

```
vim /etc/dovecot/dovecot-sql.conf.ext
```

```
driver = mysql

connect = host=192.168.1.2 port=3306 dbname=MAIL user=root password=Skill39

default_pass_scheme = PLAIN

password_query = \
   SELECT userid, domain, password \
```

```
    FROM mail WHERE userid = '%n' AND domain = 'donghyun.net'

user_query = \
    SELECT homedir, uid, gid \
    FROM mail WHERE userid = '%n' AND domain = 'donghyun.net'
```

```
mkdir -p /mail/user101
mkdir -p /mail/user201
chmod 777 -R /mail/
systemctl restart dovecot
```

---

12. Network 패킷 제어 (Network Packet Control)

- ✨ *DAE-R 및 DONG-R 에서 Destination NAT 및 Filtering 설정* 구성 시 패키지 도구는 IPTABLES를 사용함.

< *Configuration* >

- [**DAE-R**]

```
apt install iptables -y
```

```
vim /etc/network/interfaces
```

```
...

# 부가적으로 밑의 내용을 추가합니다.
up iptables -t nat -A PREROUTING -s 117.121.35.0/24 -d 117.121.35.150 -p tcp
--dport 443 -j DNAT --to 172.16.1.1
up iptables -t nat -A PREROUTING -s 117.121.35.0/24 -d 117.121.35.150 -p udp
--dport 53 -j DNAT --to 172.16.1.1
up iptables -t nat -A PREROUTING -s 117.121.35.0/24 -d 117.121.35.150 -p tcp
--dport 53 -j DNAT --to 172.16.1.1
```

```
reboot
```
