

🌐 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-SRV**]

```
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
```

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

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

```
vim /etc/hosts
```

```
127.0.1.1 DONG-SRV.donghyun.net DONG-SRV
```

```
hostnamectl set-hostname DONG-SRV
reboot
```

- [DAE-R, DAE-SRV] -> 과제지를 참고하여 위치를 동일하게 설정.

2. DNS 서비스 구성 (DNS Service Configuration)

- ⚡ DONG-SRV 및 DAE-SRV, DNS 도메인 네임서버 구성구성 시 패키지 도구는 BIND9을 사용함.

< Configuration >

- [DONG-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; };
    allow-recursion { any; };
    recursion yes;
    dnssec-validation no;
};

zone "donghyun.net" {
    type master;
    file "donghyun.zone";
    allow-update { 192.168.1.254; };
};

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

```
cp /etc/bind/db.0 /var/cache/bind/donghyun.zone
chown bind:bind -R /var/cache/bind/
```

```
sed -i "s/localhost/DONG-SRV.donghyun.net/g" /var/cache/bind/donghyun.zone
```

```
vim /var/cache/bind/donghyun.zone
```

```
DONG-SRV      IN  A   192.168.1.1  
www           IN  CNAME  DONG-SRV
```

```
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; };  
    allow-recursion { any; };  
    recursion yes;  
    dnssec-validation no;  
};  
  
view int {  
    match-clients { 192.168.1.0/24; 172.16.1.0/24; localhost; };  
    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; };
    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
ftp	IN	CNAME	DAE-SRV

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

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

```
systemctl restart bind9
```

3. DHCP 서버 구성 (DHCP Service Configuration)

- ☞ DONG-R 및 DAE-R DHCP 서버 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;
}

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
```

4. Site-to-Site VPN 구성 (Site-to-Site VPN Configuration)

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

< Configuration >

- [DONG-R]

```
apt install strongswan -y
```

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

```
conn S2S-VPN
    left=117.121.35.100
    lefsubnet=192.168.1.0/24
    right=117.121.35.150
    rightsubnet=172.16.1.0/24
    type=tunnel
    authby=secret
    keyexchange=ikev2
    auto=start
```

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

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

- [DAE-R]

```
apt install strongswan -y
```

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

```
conn S2S-VPN
  left=117.121.35.150
  lefsubnet=172.16.1.0/24
  right=117.121.35.100
  rightsubnet=192.168.1.0/24
  type=tunnel
  authby=secret
  keyexchange=ikev2
  auto=start
```

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

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

4. Certificate Authority 구성 (Certificate Authority Configuration)

- ⚡ DONG-SRV 에서 DONG-CA 인증기관 설정 구성 시 패키지 도구는 OPENSSL를 사용함.

< Configuration >

- [DONG-SRV]

```
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
```

```
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
```

4. LDAP 서버 구성 (LDAP Service Configuration)

- ⚡ DONG-SRV 및 DAE-SRV에서 LDAP 서버 구성 시 패키지 도구는 SLAPD를 사용함.

< Configuration >

- [DONG-SRV]

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

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

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

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

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

```
#!/bin/bash
for i in {01..05}
do
    echo -e "Skill39\nSkill39" | adduser --gecos "" --uid 10$i user1$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 = "donghyun.net";
$DEFAULT_BASE = "dc=donghyun,dc=net";
```

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

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

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

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

```
vim passwd.ldif      # user101 ~ user105 제외하고 전부 삭제
```

```
1 dn: uid=user101,ou=users,dc=donghyun,dc=net
2 uid: user101
3 cn: user101
4 objectClass: account
5 objectClass: posixAccount
6 objectClass: top
7 objectClass: shadowAccount
8 userPassword: {crypt}$y$j9T$13EBg6Czv15FznpAKTN0m.$GRFYBzTUU2qK1h0jQzzEJ8CpL4uRaAmWAV3hmJIGtKC
9 shadowLastChange: 20469
10 shadowMax: 99999
11 shadowWarning: 7
12 loginShell: /bin/bash
13 uidNumber: 1001
14 gidNumber: 1001
15 homeDirectory: /home/user101
16 gecos: ,,,
```

해당 사진처럼 user101 ~ user105 유저들만 남긴다.

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

```
dn: dc=donghyun,dc=net
dn: ou=users,dc=donghyun,dc=net
dn: uid=user101,ou=users,dc=donghyun,dc=net
dn: uid=user102,ou=users,dc=donghyun,dc=net
dn: uid=user103,ou=users,dc=donghyun,dc=net
dn: uid=user104,ou=users,dc=donghyun,dc=net
dn: uid=user105,ou=users,dc=donghyun,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 10$i user1$i
    userdel -r user1$i
done
```

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

- ⚡ DONG-CLI 및 DAE-CLI에서 LDAP 서버 인증 설정 구성 시 패키지 도구는 LIBNSS-LDAPD를 사용 함.
- [DONG-CLI]

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

Multiple URIs can be separated by spaces.

LDAP server URI:

```
ldap://DONG-SRV.donghyun.net/
```

<0k>

LDAP server search base:

```
dc=donghyun,dc=net
```

<0k>

Name services to configure:

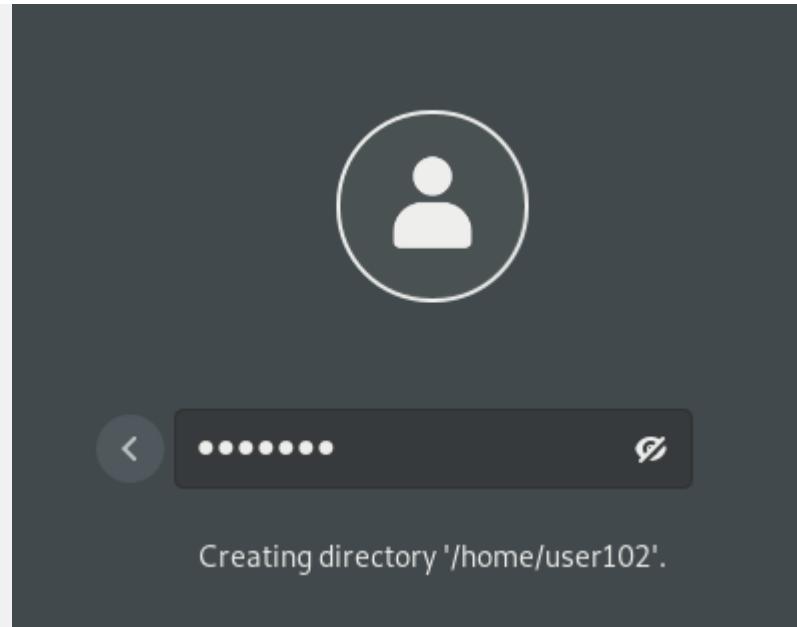
```
[*] passwd
[*] group
[ ] shadow
[ ] hosts
[ ] networks
[ ] ethers
[ ] protocols
[ ] services
[ ] rpc
[ ] netgroup
[ ] aliases
```

사진대로 설정

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

```
BASE      dc=donghyun,dc=net
URI       ldap://DONG-SRV.donghyun.net/
```

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



사진처럼 user101 ~ user105 유저로 로그인 되는지 확인

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

4. Web 서버 구성 (Web Service Configuration)

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

< Configuration >

- [DONG-SRV]

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

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

```
vim san
```

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

```
openssl ca -in www.req -out www.crt -extfile san      # PW: Skill139
```

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

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

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

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

        SSLCertificateFile      /etc/ssl/DONG-CA/certs/www.crt
        SSLCertificateKeyFile   /etc/ssl/DONG-CA/certs/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 Linux Env, $username</h2></center>";
>
```

```
1 <?php
2     $username = $_SERVER['REMOTE_USER'];
3     echo "<center><h2>Welcome to Linux Env, $username</h2></center>";
4 ?>
```

```
a2enmod ssl authnz_ldap
systemctl restart apache2
```

- ☞ DONG-CLI 및 DAE-CLI // 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

General

Home

Search

Privacy & Security

Sync

More from Mozilla

Browser Privacy

Enhanced Tracking Protection



Trackers follow you around online to collect information about your browsing habits and interests. Firefox blocks many of these trackers and other malicious scripts. [Learn more](#)

Standard

Certificates

Query OCSP responder servers to confirm the current validity of certificates

[View Certificates...](#)

[Security Devices...](#)

AC Camerfirma SA CIF A82743287

Camerfirma Chambers of Commerce R... Builtin Object Token

Camerfirma Global Chambersign Root Builtin Object Token

View... Edit Trust... **Import...** Export... Delete or Distrust...

Select File containing CA certificate(s) to import

Name	Location	Size	Type	Accessed
ca.crt	/usr/local/share/ca-certificates	4.2 kB	X.509 Certificate	06:39

위와 같이 설정합니다.

- ⚡ Web 서버 접속 테스트

https://www.donghyun.net

Starting

⊕ www.donghyun.net
This site is asking you to sign in.

Username
user101

Password

Cancel **Sign in**

https://www.donghyun.net

Welcome to Linux Env, user101

위와 같이 뜨면 성공입니다.

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

5. Network 패킷 제어 (Network Packet Control)

- ⚡ DAE-R 및 DONG-R에서 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
```

```
reboot
```

- [**DONG-R**]

```
apt install iptables -y
```

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

...

부가적으로 밑의 내용을 추가합니다.

```
up iptables -A FORWARD -s 172.16.1.0/24 -d 192.168.1.1 -p tcp --dport 443 -j  
DROP
```

```
reboot
```