

🌐 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 >

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

- 🔒 DONG-SRV1 // Samba Active Directory Service 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
```

When users attempt to use Kerberos realm that principal belongs to, of a Kerberos service running on domain.

Default Kerberos version 5 realm:

DONGHYUN.NET

Configuring Kerberos Authentication
Enter the hostnames of Kerberos servers in the DONGHYUN.NET Kerberos
Kerberos servers for your realm:

DONG-SRV1.donghyun.net

<OK>



```
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
```