@CA.worldsign.org

apt-get install krb5-admin-server krb5-kdc

vim /etc/krb5.conf

```
1 [libdefaults]
2         _default_realm = WORLDSIGN.ORG
3
```

```
39 [realms]
40         WORLDSIGN.ORG = {
41                 kdc = ca.worldsign.org
42                 admin_server = ca.worldsign.org
43         }
```

```
127 [domain_realm]
128         .worldsign.org = WORLDSIGN.ORG
129         worldsign.org = WORLDSIGN.ORG
```

krb5_newrealm

Password 입력

Password 입력

vim /etc/krb5kdc/kadm5.acl   // root사용자에게 모든 권한 부여

```
  6 */root *
  7 root *
```

kadmin.local

```
root@ca:/openvpn# kadmin.local
Authenticating as principal root/admin@WORLDSIGN.ORG with password.
kadmin.local:  addprinc root
WARNING: no policy specified for root@WORLDSIGN.ORG; defaulting to no policy
Enter password for principal "root@WORLDSIGN.ORG":
Re-enter password for principal "root@WORLDSIGN.ORG":
```

kadmin -p root

```
root@ca:~# kadmin -p root
Authenticating as principal root with password.
Password for root@WORLDSIGN.ORG:
kadmin:  addprinc root/admin
WARNING: no policy specified for root/admin@WORLDSIGN.ORG; defaulting to no policy
Enter password for principal "root/admin@WORLDSIGN.ORG":
Re-enter password for principal "root/admin@WORLDSIGN.ORG":
add_principal: Operation requires ``add'' privilege while creating "root/admin@WORLDSIGN.ORG".
kadmin:
```

addprinc host/ca.worldsign.org

ktadd host/ca.worldsign.org

addprinc user01

addprinc user02

addprinc user03

addprinc user04

addprinc user05

addprinc sysop

kadin: list_principals

```
kadmin:   list_principals
K/M@WORLDSIGN.ORG
host/ca.worldsign.org@WORLDSIGN.ORG
kadmin/admin@WORLDSIGN.ORG
kadmin/ca.worldsign.org@WORLDSIGN.ORG
kadmin/changepw@WORLDSIGN.ORG
krbtgt/WORLDSIGN.ORG@WORLDSIGN.ORG
root/admin@WORLDSIGN.ORG
root@WORLDSIGN.ORG
sysop@WORLDSIGN.ORG
user01@WORLDSIGN.ORG
user02@WORLDSIGN.ORG
user03@WORLDSIGN.ORG
user04@WORLDSIGN.ORG
user05@WORLDSIGN.ORG
kadmin:  _
```

exit

root@ca:~# ktutil

```
ktutil:  rkt /etc/krb5.keytab
ktutil:  l
slot KVNO Principal
---- ---- ---------------------------------------------
   1    2       host/ca.worldsign.org@WORLDSIGN.ORG
   2    2       host/ca.worldsign.org@WORLDSIGN.ORG
   3    2       host/ca.worldsign.org@WORLDSIGN.ORG
   4    2       host/ca.worldsign.org@WORLDSIGN.ORG
ktutil:
```

root@ca:~# /etc/ssh/sshd_config

```
54 # Kerberos options
55 KerberosAuthentication yes
56 #KerberosGetAFSToken no
57 #KerberosOrLocalPasswd yes
58 KerberosTicketCleanup yes
59
60 # GSSAPI options
61 GSSAPIAuthentication yes
62 GSSAPICleanupCredentials yes
63
```

SSH데몬 재 시작

systemctl restart ssh

systemctl restart sshd

@ remote 설정

#apt-get install krb5-user 설치

vim /etc/krb5.conf

```
1 [libdefaults]
2         default_realm = WORLDSIGN.ORG
```

```
9 [realms]
0         WORLDSIGN.ORG = {
1                 kdc = ca.worldsign.org
2                 admin_server = ca.worldsign.org
3         }
```

```
[domain_realm]
        .worldsign.org = WORLDSIGN.ORG
        worldsign.org = WORLDSIGN.ORG
```

sysop@remote:~# kinit sysop

Password: *******

sysop@remote:~# klist

```
root@remote:~# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: sysop@WORLDSIGN.ORG

Valid starting       Expires               Service principal
03/26/2017 22:03:55  03/27/2017 08:03:55   krbtgt/WORLDSIGN.ORG@WORLDSIGN.ORG
        renew until 03/27/2017 22:03:51
root@remote:~# █
```

sysop@remote:~# ssh –k sysop@ca.worldsign.org -> 패스워드 입력 없이 접속 가능해야 함.

만약 위에 방식이 안 된다면 야매를 쓰자. 공개키 방식으로 SSH gogo

@@#@@ ca.worldsign.org

#vim /etc/ssh/sshd_config

커버로스 인증 관련 주석처리 후 아래 설정 주석 해제

```
33 AuthorizedKeysFile        %h/.ssh/authorized_keys
```

systemctl restart sshd

@@@ Remote

sysop사용자로 로그인 후, 키 생성

ssh-keygen -t rsa

공개키를 ca서버에 sysop사용자의 홈 폴더 아래 .ssh/authorized_keys로 옮김

scp /home/sysop/.ssh/id_rsa.pub root@95.201.100.1:/home/sysop/.ssh/authorized_keys

Remote에서 SSH접속 시, 패스워드를 물어보면 안됨

ssh -K sysop@ca.worldsign.org