Samba 서버와 AD 연동 메뉴얼

Samba + AD연동하기

1. AD연동 조건

- AD구성이 되어 있고, 연동된 DNS구성이 되어 있어야 한다.

2. samba 설치

```
# yum -y install ntpdate samba4 samba4-client samba4-winbind krb5-workstation
policycoreutils-python samba4-winbind-clients
```

3. DNS 설정

/etc/resolv.conf 파일 수정

```
domain usoffcead.us.cdnetworks.kr //US AD서버를 지정 했습니다
nameserver 10.10.240.202 //AD서버가 DNS역할을 하고 있을 경우 지정
                         //AD서버를 인식하는 별도의 DNS을 운영 중이라면 지정 해도 됩니다. (단, 반드시
BIND 8.3 이상 버전 이어야하며, AD Query를 인식할 수 있도록 설정이 들어가 있어야 합니다.)
```

4. AD서버와 시간 동기화

```
#echo '0 */4 * * *  root /usr/sbin/ntpdate 10.10.240.202 or 10.10.240.201 >/dev/null
2>&1'>>/etc/crontab          //AD서버 IP 10.10.240.201 or 10.10.240.202
#service crond restart
```

5. 인증설정

/etc/nsswitch.conf 수정

```
passwd: files winbind //각 라인끝에 winbind를 추가해준다.
group: files winbind
```

/etc/krb5.conf 수정

```
[logging]
Default = FILE:/var/log/krb5libs.log
kdc = FILE:/var/log/krb5dc.log
```

```
admin_server = FILE:/var/log/kadmind.log


[libdefaults]
default_realm = usofficead.us.cdnetworks.kr    // AD Server Hostname (DNS naming)
dns_lookup_realm = true
  dns_lookup_kdc = true
ticket_lifetime = 24h
renew_lifetime = 7d
forwardable = true
```

6. Samba 설정

/etc/samba/smb.conf 파일 수정

6.1 global설정

```
[global]


        workgroup = TESTAD //작업그룹지정
        server string = Samba Server Version %v //서버 이름 지정
        security = ads //보안 정책을 AD로 지정
        realm = usofficead.us.cdnetworks.kr //AD서버 호스트명
        domain master = no
        local master = no
        preferred master = no

        idmap backend = hash
        idmap uid = 100000000-999999999
        idmap gid = 100000000-999999999
        idmap config usofficead.us.cdnetworks.kr : backend = hash
        idmap config usofficead.us.cdnetworks.kr : rang = 100000000-999999999

        inherit acls = Yes        //acl상속 지원
        inherit permissions = Yes //권한 상속
        map acl inherit = Yes //acl 맵핑


        winbind separator = . //도메인 분리문자
        winbind enum users = yes
        winbind enum groups = yes
        winbind use default domain = yes
        winbind nested groups = yes

        winbind refresh tickets = yes
        template homedir = /smb/%D/%U     //ad계정의 홈 폴
        template shell = /bin/bash
        restrict anonymous = 2            //익명 연결성 여부
                                          //0 사용자 및 그룹정보 반환
                                          //1 인증된 사용자만 사용자 및 그룹정보 반환
```

```
        winbind expand groups = 4
        vfs objects = acl_xattr
        ea support = yes

        log file = /var/log/samba/log.%m
        #log level = all:10
        max log size = 50

        store dos attributes = yes //dos 파일 시스템 속성 저장
```

6.2 사용자 home폴더 지정

```
[homes] //template homedir에 지정한 폴더를 공유
        comment = Home Direcotries
        valid users = %S
        read only = no
        browseable = no
```

6.3 그룹별 공유 지정

```
[Share_group1]
        comment = Test share
        path = /smb/G1
        read only = no
        valid users = @"TESTAD.G1" //도메인 그룹 지정
        force group = "Domain Users.G1" //도메인 그룹 지정
        directory mode = 0770
        force directory mode = 0770
        create mode = 0660
        force create mode = 0660
        access based share enum = yes
        hide unreadable = yes
        vfs objects = acl_xattr
        acl group control = yes
        write list = @"TESTAD.G1" //도메인 그룹 지정
```

6.4 도메인 사용자 전체 공유

```
[Share]
        comment = Test share
        path = /smb/share
        read only = no
        valid users = @"TESTAD.Domain Users"
```

```
        force group = "Domain Users" //도메인 그룹 지정
        directory mode = 0770
        force directory mode = 0770
        create mode = 0660
        force create mode = 0660
        access based share enum = yes
        hide unreadable = yes
        vfs objects = acl_xattr
        acl group control = yes
        write list = @"TESTAD.Domain Users" //도메인 설정
        browseable = yes
```

7. AD 서버 join 및 Daemon시작

join

```
#net ads join -U administrator //AD서버의 administrator암호 입력창이 나타난다.
                                        ( 이부분은 Nick.Huey에게 문의 해주세요. US AD 전용 관리자 계정이
있습니다)
```

Daemon 시작

```
#service winbind restart
#service nmb restart
#service smb restart
```

8. AD연결 확인

```
#wbinfo -u          //AD서버 유저 리스트 확인
#wbinfo -g         //AD서버 그룹 리스트 확인
#id ad_username          //AD서버에 등록된 사용자 확인
```