PDC mit LDAP Backend

Vorraussetzung: slapd wie in samba-ldap beschrieben konfiguriert und nss-ldap konfiguriert.

Dieses Beispiel beschreibt eine minimale Konfiguration.

Samba

`/etc/samba/smb.conf`:

```
[global]
  workgroup = kurs
  interfaces = eth0

  #Samba als PDC:
  os level = 34
  domain logons = yes
  logon home =
  logon path =

  #LDAP Anbindung:
  passdb backend = ldapsam:ldap://ldap1.villa.local
  ldap suffix         = dc=villa,dc=local
  ldap admin dn       = "cn=admin,dc=villa,dc=local"
  ldap user suffix    = ou=people
  ldap group suffix   = ou=groups
  ldap machine suffix = ou=computers
  ldap idmap suffix   = ou=people
  ldap ssl = off

  obey pam restrictions = no
  #ldapsam:trusted = yes

[daten]
  path = /tmp
  writable = yes
```

Debian

```
/etc/init.d/samba restart
```

Das Passwort des in der `smb.conf` genannten LDAP Admin muß dem Samba Server im Klartext vorliegen:

```
smbpasswd -W
```

Testen

Ist der Samba-Server PDC?

```
nmblookup -m kurs#1b
```

Rechner der Domäne hinzufügen

Dazu gibt es 4 Möglichkeiten:

- von Hand
- mit den smbldap-tools
- `ldapsmb`
- und ab Samba 3.0.25 kann samba das mit den Parametern `ldapsam:trusted` und `ldapsam:editposix` selbst

von Hand

LDAP Verzeichnis anpassen

Im LDAP Verzeichnis müssen nun noch Einträge für

- den in der `smb.conf` im Parameter `ldap machine suffix` genannten Teilbaum,
- die Gruppe, der die Maschinenaccounts zugeordnet werden sollen
- 3 Gruppen mit den Namen „domadmin“, „domusers“, „domguests“ und der jeweils genannten sambaSID
- und einen Domänenadministrator

hinzugefügt werden.

```
DOMAIN="dc=villa,dc=local"
WORKGROUP=kurs
SID=`net getlocalsid $WORKGROUP | sed 's/.*:\ //'`
ldapadd -x -W <<LDIF
```

```
TODO muss neu erzerugt werden
```

Domänenadmin anpassen

```
smbpasswd -a smbadmin
```

Unter Windows hat der Domänenadmin immer die RID 500:

```
pdbedit -U $SID-500 -u smbadmin -r
```

Überprüfen:

```
pdbedit -L -v smbadmin
```

Und der soll das Recht haben, Rechner der Domäne hinzuzufügen:

```
net -U smbadmin rpc rights grant smbadmin SeMachineAccountPrivilege
```

Überprüfen:

```
net -U smbadmin rpc rights list smbadmin
```

Alternativ:

```
net sam rights grant ntadmin SeMachineAccountPrivilege SeAddUsersPrivilege
```

Rechner hinzufügen

Wie bei normalen Benutzern auch muß zu einem Samba-Maschinen-Account auch ein Unix/Linux Account existieren. Um einen Rechner mit dem Namen „vm2000“ der Domäne hinzuzufügen sind daher folgende Schritte notwendig:

posixAccount anlegen:

```
DOMAIN="dc=villa,dc=local"
MACHINE="appl2"
ldapadd -x -W <<LDIF
```

```
dn: cn=$MACHINE,ou=Computers,$DOMAIN
objectClass: top
objectClass: posixAccount
objectClass: account
cn: $MACHINE
uidNumber: 20000
gidNumber: 515
homeDirectory: /tmp
loginShell: /bin/false
uid: $MACHINE$

LDIF
```

Jetzt kann der Rechner unter Windows der Domaene hinzugefügt werden. [1)]

smbldap-tools

`/etc/samba/smb.conf` :

```
[global]
```

```
  ldap delete dn = Yes
  unix password sync = Yes
  passwd program = /usr/sbin/smbldap-passwd %u

  add user script = /usr/sbin/smbldap-useradd -m "%u"
  delete user script = /usr/sbin/smbldap-userdel "%u"
  add machine script = /usr/sbin/smbldap-useradd -t 2 -w "%u"
  add group script = /usr/sbin/smbldap-groupadd -a "%g"
  delete group script = /usr/sbin/smbldap-groupdel "%g"
  add user to group script = /usr/sbin/smbldap-groupmod -m "%u" "%g"
  delete user from group script = /usr/sbin/smbldap-groupmod -x "%u" "%g"
  set primary group script = /usr/sbin/smbldap-usermod -g "%g" "%u"
```

```
zcat /usr/share/doc/smbldap-tools/examples/smbldap.conf.gz > /etc/smbldap-
tools/smbldap.conf
cp /usr/share/doc/smbldap-tools/examples/smbldap_bind.conf /etc/smbldap-
tools/smbldap_bind.conf
```

/etc/smbldap-tools/smbldap_bind.conf :

```
slaveDN="cn=admin,dc=linuxhotel,dc=de"
slavePw="villa"
masterDN="cn=admin,dc=linuxhotel,dc=de"
masterPw="villa"
```

/etc/smbldap-tools/smbldap.conf :

```
#SID="S-1-5-21-2320849130-3131792283-2083377348"
```

```
sambaDomain="kurs"
```

```
slaveLDAP="localhost"
```

```
masterLDAP="localhost"
```

```
ldapTLS="0"
```

```
suffix="dc=linuxhotel,dc=de"
```

```
usersdn="ou=People,${suffix}"
```

```
idmapdn="ou=People,${suffix}"
```

```
userSmbHome=""
```

```
userProfile=""
```

```
userScript=""
```

```
chmod 0644 /etc/smbldap-tools/smbldap.conf
chmod 0600 /etc/smbldap-tools/smbldap_bind.conf
smbldap-populate -a smbadmin -e /tmp/samba.ldif
```

`/tmp/samba.ldif` prüfen [2)]

```
ldapadd -x -W -D cn=admin,dc=example,dc=com -f /tmp/samba.ldif -h
ldap1.example.com
```

[3)]

Doku

- `/usr/share/doc/smbldap-tools/README.Debian.gz`

ldapsmb

Alternativ gibt es bei SuSE das Paket `ldapsmb` als einfaches Beispiel für ein `add machine script`:

(noch nicht getestet)

ldapsam:editposix

siehe

```
man smb.conf
```

Ist beschrankt auf `objectclass=account`, kann aktuell noch nicht mit inetOrgPerson u.ä. umgehen.

Webmin - Modul LDAP Useradmin

SuSE:

```
http://www.webmin.com
```

Einstellungen `/etc/webmin/ldap-useradmin/config`: (SuSE)

```
samba_def=1
samba_class=sambaSamAccount
samba_gclass=sambaGroupMapping
samba_domain=S-1-5-21-2516115203-501549975-3175969160
```

Dokus & Links

- Howto für SuSE: http://en.opensuse.org/Howto_setup_SUSE_as_SAMBA_PDC_with_OpenLDAP%2C_DYNDNS_and_CLAM
- Alternatives LDAP Setup : http://wiki.samba.org/index.php/Ldapsam_Editposix

1)

samba-Maschinen-Account anlegen:

```
smbpasswd -a -m $MACHINE
```

2)

Todo: `smbadmin` checken: `uidNumber` und `gidNumber` auf einen anderen Wert als 0 ändern ...

3)

oder direkt

```
smbldap-populate -a smbadmin
```

eingeben und nachträglich `uidNumber` und `gidNumber` auf einen anderen Wert als 0 ändern