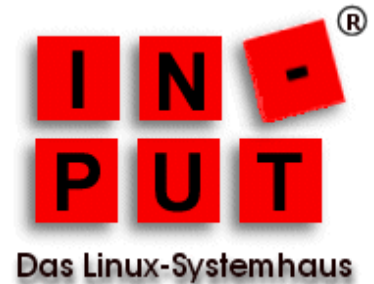


Inhaltsverzeichnis

SAMBA.....	3
Das SMB-Protokoll.....	4
Installation	5
Die smb.conf.....	9
Das Share [global].....	9
Das Share [netlogon].....	14
Das Share [homes].....	15
Das Share [printers].....	17
Weitere Shares.....	18
DOS/Windows-Datei-Attribute.....	20
Browsing.....	21
Paßwort-Synchronisation.....	21
Weitere Programme aus dem Samba 2.x -Paket	22
Die Befehl des Samba 3.0-Pakets.....	26
Samba als WINS-Server.....	47
Samba als PDC.....	49
Logon-Scripte und Profile.....	50
Samba als BDC.....	54
Samba und das MS Active Directory.....	55
Windows NT/2000/XP als Samba-Client.....	57
Samba als File-Server in einer Windows-Domäne.....	59
Benutzerverwaltung mit winbind.....	60
LDAP als Samba-Backend.....	63
SWAT (Samba Web Administration Tool).....	71
CUPS	72
Import und Export von Druckertreibern (Teil 1).....	90
Import und Export von Druckertreibern (Teil 2).....	119
Migration von Profile.....	128
Skripte.....	130
Links & Literatur.....	131

Samba und das MS Active Directory



Für die Anbindung an ein ADS muß der Samba-Server mit den Optionen `--with-ads` `--with-ldap` übersetzt worden sein. Unter SuSE bedingt dies, daß alle heimdal-Pakete (auch heimdal-devel) und openldap-Pakete (auch openldap-devel) installiert wurden. Wenn Sie wissen wollen, ob die vorliegenden Binaries mit den notwendigen Parametern übersetzt wurden, rufen Sie beiden folgenden Befehle auf:

```
ldd /usr/sbin/smbd
ldd /usr/sbin/nmbd
```

In den Ausgaben der beiden Befehle sollten die beiden folgenden Zeilen enthalten sein (die angezeigten Versionen können sich ggf. unterscheiden):

```
libldap-2.2.so.7 => /usr/lib/libldap-2.2.so.7 (0x40027000)
libkrb5.so.17 => /usr/lib/libkrb5.so.17 (0x4007a000)
```

Auf dem ADS muß zudem der DNS-Server aktiv sein. Die smb.conf sollte die folgenden Parameter enthalten:

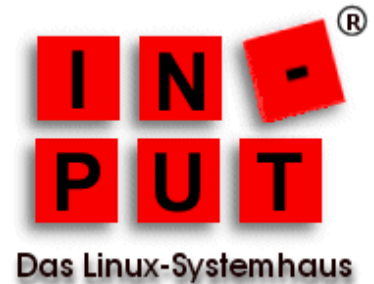
```
[global]
workgroup = INTERN
realm = INTERN.LOCAL
security = ADS
password server = *
idmap uid = 10000-20000
idmap gid = 10000-20000
winbind enum users = yes
winbind enum groups = yes
winbind enable local accounts = yes
winbind separator = +
template homedir = /home/%U
template shell = /bin/bash
```

Das Realm kann man unter Windows wie folgt ermitteln: ARBEITSPLATZ -> EIGENSCHAFTEN -> NETZWERKIDENTIFIKATION - Domäne.

In der `/etc/krb5.conf` sind die folgenden Eintragungen vorzunehmen:

```
[realms]
  INTERN.LOCAL = {
    kdc = name/ip des kerberos servers
  }
```

Samba und das MS Active Directory



```
[libdefaults]
    default_realm = INTERN.LOCAL
```

```
[domain_realm]
    .intern.local = INTERN.LOCAL
    intern.local = INTERN.LOCAL
```

In der `/etc/nsswitch.conf` sind die folgenden Änderungen vorzunehmen, damit für die Benutzeranmeldung auf den winbind und somit auf den Windows-Server zurückgegriffen werden kann:

```
vorher:
passwd:    files nis
group:     files nis
```

```
nachher:
passwd:    compat winbind
group:     compat winbind
shadow:    compat winbind
```

Zuätzlich ist darauf zu achten, daß der Name Service Cacheing Daemon (nscd) nicht läuft! Nun startet man den nmbd, den smbd und den winbind.

Unter SuSE sind in der Datei `/etc/security/pam_unix2.conf` die folgenden Änderungen vorzunehmen:

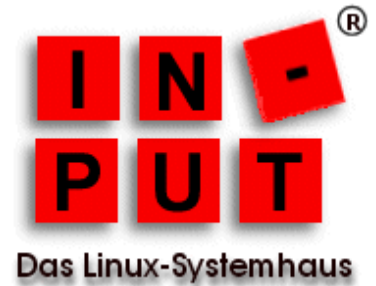
```
vorher:
auth:
account:
password:
```

```
nachher:
auth:         use_winbind
account:      use_winbind
password:     use_winbind
```

Starten Sie nun die Dienste nmbd, smbd und winbind. Mit Hilfe des Befehls `kinit Administrator` kann die Verbindung zum ADS getestet werden. Für eine erfolgreiche Verbindung kann es gegebenenfalls notwendig sein, den Namen und die IP des Kerberos-Servers in die `/etc/hosts` aufzunehmen, wenn Sie über keinen DNS verfügen.

Die Aufnahme in die Domain erfolgt dann mit dem Befehl:

Samba und das MS Active Directory



```
net ads join -UAdministrator%PASSWORT
```

Danach startet man die drei Dienste des Samba-Servers neu. Der Befehl `wbinfo -t` sollte nach einiger Zeit mit der Meldung „Checking the trust secret via RPC calls succeeded“ bestätigt werden.

Sollte stattdessen eine Fehlermeldung erscheinen, so löscht man mit `kdestroy` das erhaltene Kerberos-Ticket und wiederholt die Schritte, beginnend mit `kinit`, und überprüft die Konfiguration. Besonders ist darauf zu achten, daß das Realm stets in Großbuchstaben geschrieben wird.

Die Befehle `wbinfo -u`, `wbinfo -g`, `getent passwd` und `getent group` sollten dann die Liste der Benutzer und Gruppen des Linux-Systems und des Windows-Servers liefern.

Danach kann mit `smbclient` ein weiterer Test erfolgen, jedoch ist dabei der Parameter `-k` für die Kerberos-Authentifizierung anzugeben.

Es ist darauf zu achten, daß die Zeit auf dem Samba-Server und dem ADS identisch sind. Bei Abweichung ist es möglich, daß die Kerberos-Authentifizierung fehlschlägt.