Samba als Primary Domain Controller

25. Oktober 2004

Diese Kurzanleitung beschreibt die schrittweise Installation von Samba als Primary Domain Controller (PDC), dabei wurde die Samba Version 3.0.7 verwendet. Weiterhin werden Eckpunkte zur Migration von bestehenden Benutzern beschrieben.

Inhaltsverzeichnis

1 Kompilierung

Damit alle benötigten Funktionen in Samba zur Verfügung stehen und um Fehlerquellen zu minimieren ist es an zuraten Samba aus den Quellen zu erzeugen. Alle dafür nötigen Schritte werden in diesem Kapitel beschrieben. Die für Samba benötigten externen Bibliotheken müssen vor der Kompilierung in der Installationsumgebung installiert worden sein.

Das Samba Quellenpaket wird in ein beliebiges Verzeichnis heruntergeladen (bevorzugt wird das Verzeichnis `/usr/src/`) und entpackt. Nun muss das Quellenpaket an die Umgebung angepasst werden, dazu muss in das Verzeichnis `/usr/src/samba-3.0.7/source/` gewechselt werden. In diesem Verzeichnis wird in der Befehlszeile die folgende Befehlsabfolge eingegeben und ausgeführt:

```
% ./configure --with-ldap --with-ldapsam --enable-cups=no \
--prefix=/usr/local/samba
```

Nachdem das Quellpaket an die Umgebung vollständig und ohne Fehler angepasst wurde, kann nun der Kompilierungsvorgang gestartet werden. Dieser wird durch den Befehl

```
% make
```

gestartet. Ist der Kompilierungsvorgang erfolgreich abgeschlossen kann Samba installiert werden, dieses erfolgt über den Befehl

```
% make install
```

Nun ist Samba installiert und kann konfiguriert werden.

2 Konfiguration

Die Konfiguration von Samba setzt einen laufenden LDAP-Server voraus. Damit Domänen Benutzer und Workstations erstellt und modifiziert werden können muss der LDAP-Manager und das zugehörige Passwort vorliegen. Weiterhin muss der LDAP-Server das Samba Schema geladen haben. Dieses ist für die gängigen LDAP-Server im Verzeichnis

```
/usr/src/samba-3.0.7/examples/LDAP/
```

zu finden. Für den Sun Directory Server ist das Samba Schema unter der URL

```
http://ppbwiki.rz-berlin.mpg.de/uploads/Main.SambaPDC/ldap_schema.txt
```

verfügbar, das mitgelieferte Schema wies einige Fehler auf. Daher sollte das angegebenen Schema benutzt werden, da sort alle Fehler korrigiert wurden. Ist das Schema korrekt vom LDAP-Server geladen worden so kann mit der Konfiguration des Samba-Servers begonnen werden.

2.1 Domäne migrieren

Soll eine bereits bestehende Microsoft Windows Domäne migrieren, so wird der SID-Prefix der Domäne benötigt. Da dieser nicht öffentlich zugänglich ist kann dieser mit dem Tool "hivedumpërmittelt werden. Dazu wird jedoch die Datei NTUSER.DAT eines Domänen Benutzers benötigt. Ist diese Datei verfügbar so kann mit der folgenden Befehlszeile der SID-Prefix extrahiert werden:

```
% hivedump --findfirstsid NTUSER.DAT owner S-1-5-21-
```

Nach der Ausführung kommt eine Zeile die dem Muster der folgenden Zeile ähnelt, dabei ist der Platzhalter <RID> eine nicht Vorzeichen behaftet Zahl aus dem integer Zahlenraum.

```
S-1-5-21-1073446153-1192918827-1877560073-<RID>
```

Der SID-Prefix währe in diesem Falle:

```
S-1-5-21-1073446153-1192918827-1877560073
```

Dies sollte nicht nur bei einem Profile durchgeführt werden, da sich der SID-Prefix unter umständen unterscheiden kann. Sollte dies der Fall sein so muss mit der folgenden Befehlszeile der gemeinsame SID-Prefix ermittelt werden, dabei sollten mehr als zwei Profile untersucht werden.

```
% hivedump --getallsids NTUSER.DAT
```

2.2 Konfigurationsdatei bearbeiten

Der erste Schritt ist die Bearbeitung der Konfigurationsdatei

```
% vi /usr/local/samba/lib/smb.conf
```

Sollte diese Datei bereits existieren ist anzuraten diese vollständig zu löschen. Die verwendete Konfiguration sollte die folgenden Einstellungen beinhalten:

```
[global]

workgroup                       = PDC
netbios name                    = PDC
server string                   = PP&B PDC

security                        = domain
encrypt passwords               = yes
obey pam restrictions           = no
time server                     = yes
passdb backend                  = ldapsam:ldap://belanna/
log level                       = 0
log file                        = /usr/local/samba/var/log.%m
socket options                  = SO_KEEPALIVE
load printers                   = No
lm announce                     = No
preferred master                = Yes
os level                        = 65
local master                    = Yes
domain master                   = Yes
domain logons                   = Yes
hosts allow                     = 141.14.

ldap admin dn                   = cn=Directory Manager
ldap suffix                     = dc=ppb,dc=rz-berlin,dc=mpg,dc=de
ldap group suffix               = ou=groups
ldap machine suffix             = ou=hosts
ldap user suffix                = ou=people
ldap port                       = 389
ldap delete dn                  = Yes
ldap passwd sync                = Yes
ldap ssl                        = no
```

2.3 LDAP Manager Passwort setzen

Damit Samba auf die Daten in LDAP vollständig zu greifen kann muss das LDAP Passwort gesetzt werden. Dies erfolgt mit Hilfe des Programms:

```
% /usr/local/samba/bin/smbpasswd -w <LDAP-PASSWORT>
```

Als Parameter muss das Passwort angegeben werden. Bei erfolgreicher Ausführung wird die folgende Statusmeldung ausgegeben:

```
% /usr/local/samba/bin/smbpasswd -w <LDAP-PASSWORT>
```

Standard-Ausgabe:

```
Setting stored password for "cn=Directory Manager" in secrets.tdb
```

Nun ist Samba vollständig konfiguriert nun müssen alle benötigten Elemente in LDAP erzeugt werden.

2.4 Standard Domänen Benutzer und Gruppen erstellen

Damit nun auch Workstations der Domäne beitreten können müssen zunächst der Benutzer "root" und die benötigten Gruppen angelegt werden. Dabei werden LDAP die Daten mit der folgenden Befehlszeile zugeführt:

```
% ldapadd -h belanna -D "cn=Directory Manager"
```

Die folgende Auflistung muss dem LDAP-Server zugeführt werden.

```
1  dn: uid=root,ou=people,dc=ppb,dc=rz-berlin,dc=mpg,dc=de
2  cn:                     root
3  sn:                     root
4  objectClass:            inetOrgPerson
5  objectClass:            sambaSAMAccount
6  objectClass:            posixAccount
7  objectClass:            shadowAccount
8  gidNumber:              512
9  uid:                    root
10 uidNumber:              0
11 homeDirectory:          /dev/null
12 sambaPwdLastSet:        0
13 sambaLogonTime:         0
```

```
14 sambaLogoffTime:              2147483647
15 sambaKickoffTime:             2147483647
16 sambaPwdCanChange:            0
17 sambaPwdMustChange:           2147483647
18 sambaSID:                     S-1-5-21-1073446153-1192918827-1877560073-500
19 sambaPrimaryGroupSID:         S-1-5-21-1073446153-1192918827-1877560073-512
20 sambaAcctFlags:               [U]
21 sambaLMPassword:              XXX
22 sambaNTPassword:              XXX
23 loginShell:                   /bin/false
24 gecos:                        Domain Administrator
25
26 dn: sambaDomainName=PDC,dc=ppb,dc=rz-berlin,dc=mpg,dc=de
27 sambaSID:                     S-1-5-21-1073446153-1192918827-1877560073
28 sambaDomainName:              PDC
29 sambaAlgorithmicRidBase:      1000
30 objectClass:                  sambaDomain
31
32 dn: cn=Domain Admins,ou=groups,dc=ppb,dc=rz-berlin,dc=mpg,dc=de
33 objectClass:                  posixGroup
34 objectClass:                  sambaGroupMapping
35 gidNumber:                    512
36 cn:                           Domain Admins
37 memberUid:                    Administrator
38 description:                  Domain Administrators
39 sambaSID:                     S-1-5-21-1073446153-1192918827-1877560073-512
40 sambaGroupType:               2
41 displayName:                  Domain Admins
42
43 dn: cn=Domain Users,ou=groups,dc=ppb,dc=rz-berlin,dc=mpg,dc=de
44 objectClass:                  posixGroup
45 objectClass:                  sambaGroupMapping
46 gidNumber:                    513
47 cn:                           Domain Users
48 description:                  Domain Users
49 sambaSID:                     S-1-5-21-1073446153-1192918827-1877560073-513
50 sambaGroupType:               2
51 displayName:                  Domain Users
52
53 dn: cn=Domain Guests,ou=groups,dc=ppb,dc=rz-berlin,dc=mpg,dc=de
54 objectClass:                  posixGroup
55 objectClass:                  sambaGroupMapping
56 gidNumber:                    514
57 cn:                           Domain Guests
58 description:                  Domain Guests Users
59 sambaSID:                     S-1-5-21-1073446153-1192918827-1877560073-514
60 sambaGroupType:               2
61 displayName:                  Domain Guests
62
63 dn: cn=Print Operators,ou=groups,dc=ppb,dc=rz-berlin,dc=mpg,dc=de
64 objectClass:                  posixGroup
65 objectClass:                  sambaGroupMapping
66 gidNumber:                    550
67 cn:                           Print Operators
68 description:                  Domain Print Operators
69 sambaSID:                     S-1-5-21-1073446153-1192918827-1877560073-550
70 sambaGroupType:               2
71 displayName:                  Print Operators
72
73 dn: cn=Backup Operators,ou=groups,dc=ppb,dc=rz-berlin,dc=mpg,dc=de
74 objectClass:                  posixGroup
75 objectClass:                  sambaGroupMapping
76 gidNumber:                    551
77 cn:                           Backup Operators
78 description:                  Domain Backup Operators
79 sambaSID:                     S-1-5-21-1073446153-1192918827-1877560073-551
80 sambaGroupType:               2
81 displayName:                  Backup Operators
```

```
82
83 dn: cn=Replicator,ou=groups,dc=ppb,dc=rz-berlin,dc=mpg,dc=de
84 objectClass:                posixGroup
85 objectClass:                sambaGroupMapping
86 gidNumber:                  552
87 cn:                         Replicator
88 description:                Domain Replicator
89 sambaSID:                   S-1-5-21-1073446153-1192918827-1877560073-552
90 sambaGroupType:             2
91 displayName:                Replicator
92
93 dn: cn=Domain Computers,ou=groups,dc=ppb,dc=rz-berlin,dc=mpg,dc=de
94 objectClass:                posixGroup
95 objectClass:                sambaGroupMapping
96 gidNumber:                  553
97 cn:                         Domain Computers
98 description:                Domain Computers
99 sambaSID:                   S-1-5-21-1073446153-1192918827-1877560073-553
100 sambaGroupType:            2
101 displayName:               Domain Computers
```

Nun muss dem Domänen Benutzer "root" das Passwort gesetzt werden, damit eine Workstation dieser Domäne beitreten kann. Das Domänen Passwort und Unix-Passwort können unterschiedlich gewählt werden. Das setzen des Passwortes erfolgt mit der Befehlszeile:

```
% /usr/local/samba/bin/smbpasswd root
```

2.5 Samba starten

An dieser Stelle kann der Samba Server gestartet werden. Dies erfolgt über die beiden folgenden Befehlszeilen:

```
% /usr/local/samba/sbin/smbd
% /usr/local/samba/sbin/nmbd
```

2.6 Domänen Benutzer erstellen

Für die Erstellung normaler Domänen Benutzer dient die folgende Vorlage, in der lediglich alle Platzhalter durch die entsprechenden Werte ersetzt werden müssen. Für das übertragen an LDAP siehe Kapitel 2.4.

```
1 dn: uid=<DOMAIN-USER>,ou=people,dc=ppb,dc=rz-berlin,dc=mpg,dc=de
2 objectClass:                top
3 objectClass:                account
```

```
4  objectClass:              sambaSamAccount
5  uid:                      <DOMAIN-USER>
6  sambaSID:                 S-1-5-21-1073446153-1192918827-1877560073-<RID>
7  sambaPrimaryGroupSID:     S-1-5-21-1073446153-1192918827-1877560073-513
8  sambaProfilePath:         <PATH-PROFILE>
9  sambaHomePath:            <PATH-HOME>
10 sambaHomeDrive:           <DRIVE-HOME>
11 sambaAcctFlags:           [U]
12 sambaPwdMustChange:       2147483647
13 sambaPwdLastSet:          1
14 sambaLMPassword:          <PASSWORT-LM>
15 sambaNTPassword:          <PASSWORT-NT>
```

Bei der Wahl der SID muss darauf geachtet werden das diese nicht bereits vergeben worden ist (jede SID muss Einzigartig sein). Mit der folgenden Befehlszeile lässt sich prüfen ob die eine SID bereits vergeben worden ist.

```
% ldapsearch -h belanna -b dc=ppb,dc=rz-berlin,dc=mpg,dc=de \
sambaSID=S-1-5-21-1073446153-1192918827-1877560073-<RID>
```

Für die Erstellung der beiden Passwörter (NT und LM) wird das Tool "mkntpwd" benötigt. Diese gibt die beiden Passwörter auf der Standardausgabe aus. Die Parametrierung des Tools sieht wie folgt aus:

```
% mkntpwd <PASSWORT>
```

Die Ausgabe des Tools sieht wie folgt aus:

```
<PASSWORT-LM>:<PASSWORT-NT>
```

Dieses Tool ist in den Samba Quellen enthalten und ist unter

```
% /usr/src/samba-3.0.7/examples/LDAP/smbldap-tools/mkntpwd/
```

zu finden.

2.6.1 Bestehendes Domänen Benutzer migrieren

Ersetzt der Samba PDC eine Microsoft Windows PDC so können die Microsoft Windows NT-Profile ohne Einschränkungen übernommen werden, dabei hilft das Tool "hivedump". Dieses Tool kann aus der NTUSER.DAT die bestehende SID des Domänen Benutzers auslesen, diese wird dann als SID des neuen Domänen Benutzers eingetragen. Dabei ist wichtig das der SID-Prefix der beiden Domänen übereinstimmt. Die Parametrisierung und Ausgabe des Tools sieht wie folgt aus:

```
% hivedump --findfirstsid /home/frosch/profile/ntuser.dat \
owner S-1-5-21-1073446153-1192918827-1877560073
```

Standard-Ausgabe:

```
S-1-5-21-1073446153-1192918827-1877560073-1000
```

Die so erhaltende SID kann als SID des neuen Domänen Benutzers eingetragen werden, somit ist Windows 2000, XP in der Lage das NT-Profile korrekt zu öffnen.

Sollten die beiden Passwörter (LM und NT) des bisherigen Domänen Benutzers zur Verfügung stehen so können diese ohne Einschränkungen übernommen werden.

2.6.2 Beispiel

Anhand eines Beispieles für den Benutzer "frosch" soll die Vorgehensweise veranschaulicht werden.

```
% ldapsearch -h belanna -b dc=ppb,dc=rz-berlin,dc=mpg,dc=de \
sambaSID=S-1-5-21-1073446153-1192918827-1877560073-1000
```

Dabei dürfen keine Objekte gefunden werden. Sollte jedoch ein Objekt mit der gesuchten SID gefunden werden, muss eine andere SID gewählt werden. Wurde kein Objekt gefunden so können die beiden Passwörter (LM und NT) generiert werden, dazu wird das schon beschriebene Tool "mkntpwd" benutzt.

```
% mkntpwd testme
```

Standard-Ausgabe:

```
A5E9D1D6E318223AAAD3B435B51404EE:7BFCAB36832E298C37439259C80F6C08
```

Mit den so gewonnen Werten wird die Vorlage komplettiert.

```
dn: uid=frosch,ou=people,dc=ppb,dc=rz-berlin,dc=mpg,dc=de
objectClass:            top
objectClass:            account
objectClass:            sambaSamAccount
uid:                    frosch
sambaSID:               S-1-5-21-1073446153-1192918827-1877560073-1000
sambaPrimaryGroupSID:   S-1-5-21-1073446153-1192918827-1877560073-513
sambaProfilePath:       \\byers\homes\profile
sambaHomePath:          \\byers\homes
sambaHomeDrive:         R:
sambaAcctFlags:         [U]
sambaPwdMustChange:     2147483647
sambaPwdLastSet:        1
sambaLMPassword:        A5E9D1D6E318223AAAD3B435B51404EE
sambaNTPassword:        7BFCAB36832E298C37439259C80F6C08
```

Für die Datenübertragung an den LDAP-Server siehe Kapitel 2.4. Nun ist der Benutzer "frosch" eingerichtet und kann sich unter der Domäne einloggen.

2.7 Domänen Benutzer löschen

Um einen normalen Domänen Benutzer zu löschen, kann die folgende Befehlszeile genutzt werden. Die enthaltenden Platzhalter müssen durch die entsprechenden Werte ersetzt werden.

```
% ldapdelete -h belanna -D "cn=Directory Manager" \
uid=<DOMAIN-USER>,ou=people,dc=ppb,dc=rz-berlin,dc=mpg,dc=de
```

2.8 Domänen Benutzer de-/aktivieren

Um einen Domänen Benutzer de- bzw. aktivieren zu können, müssen die in den Vorlagen enthaltenden Platzhalter durch die entsprechenden Werte ersetzt werden. Danach werden die Daten mit dem Tool

```
% ldapmodify -h belanna -D "cn=Directory Manager"
```

an den LDAP Server übertragen. Dieses Tool erwartet nach dem starten die Daten über die Standardeingabe, somit kann mit "Copy&Paste" gearbeitet werden.

Die folgende Vorlage aktiviert einen Domänen Benutzer.

```
dn: uid=<DOMAIN-USER>,ou=people,dc=ppb,dc=rz-berlin,dc=mpg,dc=de
sambaAcctFlags:          [U]
```

Die folgende Vorlage deaktiviert einen Domänen Benutzer.

```
dn: uid=<DOMAIN-USER>,ou=people,dc=ppb,dc=rz-berlin,dc=mpg,dc=de
sambaAcctFlags:          [DU]
```

2.9 Domänen Administrator erstellen

Die Erstellung eines Domänen Administrator unterscheidet sich ausschließlich in einem Punkt zur Erstellung eines Domänen Benutzers (siehe Kapitel 2.6). Dieser Unterschied liegt in der `sambaPrimaryGroupSID`, diese hat beim Domänen Administratoren die RID 512. Daher wird ausschließlich eine abgewandelte Vorlage genutzt, die im folgenden dargestellt ist. Da die folgenden Schritte mit denen des Kapitels 2.6 übereinstimmen wird auf dieses Kapitel verwiesen, um die weiteren Schritte auszuführen.

```
dn: uid=<DOMAIN-ADMIN>,ou=people,dc=ppb,dc=rz-berlin,dc=mpg,dc=de
objectClass:             top
objectClass:             account
objectClass:             sambaSamAccount
uid:                     <DOMAIN-ADMIN>
sambaSID:                S-1-5-21-1073446153-1192918827-1877560073-<RID>
sambaPrimaryGroupSID:    S-1-5-21-1073446153-1192918827-1877560073-512
sambaProfilePath:        <PATH-PROFILE>
sambaHomePath:           <PATH-HOME>
sambaHomeDrive:          <DRIVE-HOME>
sambaAcctFlags:          [U]
sambaPwdMustChange:      2147483647
sambaPwdLastSet:         1
sambaLMPassword:         <PASSWORT-LM>
sambaNTPassword:         <PASSWORT-NT>
```

2.10 Workstation erstellen

Damit eine Workstation der Domäne hinzugefügt werden kann muss zunächst diese in LDAP eingetragen werden. Dies erfolgt über die folgende Vorlage, die enthaltenden Platzhalter müssen durch die entsprechenden Werte ersetzt werden. Für das übertragen an LDAP siehe Kapitel 2.4. Die SID muss, wie schon im Kapitel 2.6 beschrieben, auf ihre nicht Existenz kontrolliert werden.

```
dn: uid=<DOMAIN-HOST>$,ou=hosts,dc=ppb,dc=rz-berlin,dc=mpg,dc=de
objectClass:            top
objectClass:            account
objectClass:            sambaSamAccount
sambaPwdLastSet:        0
sambaPwdMustChange:     2147483647
sambaPwdCanChange:      0
sambaSID:               S-1-5-21-1073446153-1192918827-1877560073-<RID>
sambaPrimaryGroupSID:   S-1-5-21-1073446153-1192918827-1877560073-553
uid:                    <DOMAIN-HOST>$
sambaAcctFlags:         [W]
```

2.10.1 Beispiel

Anhand eines Beispieles für die Workstation "mpimage" soll die Vorgehensweise verschaulicht werden. Zunachst wird die nicht Existenz der gewählten SID kontrolliert, dieses erfolgt mit der folgenden Befehlszeile:

```
% ldapsearch -h belanna -b dc=ppb,dc=rz-berlin,dc=mpg,dc=de \
sambaSID=S-1-5-21-1073446153-1192918827-1877560073-1001
```

Dabei dürfen keine Objekte gefunden werden. Sollte jedoch ein Objekt mit der gesuchten SID gefunden werden, muss eine andere SID gewählt werden. Wurde kein Objekt gefunden so kann die Vorlage mit den so gewonnen Werten komplettiert werden.

```
dn: uid=mpimage$,ou=hosts,dc=ppb,dc=rz-berlin,dc=mpg,dc=de
objectClass:            top
objectClass:            account
objectClass:            sambaSamAccount
sambaPwdLastSet:        0
sambaPwdMustChange:     2147483647
sambaPwdCanChange:      0
sambaSID:               S-1-5-21-1073446153-1192918827-1877560073-1001
sambaPrimaryGroupSID:   S-1-5-21-1073446153-1192918827-1877560073-553
uid:                    mpimage$
sambaAcctFlags:         [W]
```

Für die Datenübertragung an den LDAP-Server siehe Kapitel 2.4.

2.11 Workstation löschen

Um eine Workstation aus der Domäne zu löschen, kann die folgende Befehlszeile genutzt werden. Die enthaltenden Platzhalter müssen durch die entsprechenden Werte ersetzt wer-

den.

```
% ldapdelete -h belanna -D "cn=Directory Manager" \
uid=<DOMAIN-HOST>,ou=hosts,dc=ppb,dc=rz-berlin,dc=mpg,dc=de
```

3 Workstation in die Domäne bringen

Ein wichtiger Unterschied für beim beitreten einer Workstation zur Domäne liegt beim verwendeten Benutzer. Dabei wird bei der Samba Domäne nicht mehr der Benutzer "Administrator", sondern der Benutzer "root" benutzt.

3.1 Registry Änderungen

Um mit Windows 2000 oder XP einer Samba Domäne beitreten zu können muss der Registry Schlüssel geändert werden:

```
1 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\netlogon\parameters
2 "RequireSignOrSeal"=dword:00000000
```