

Werner-von-Siemens-Schule Hildesheim  
Fachpraxis Informationstechnik

**Projektarbeit**  
zum Thema

# Primary Domain Controller

Erstellt von Patrick Kreipe und Paul Szymanski

Hildesheim 3.Juni 2011

# Inhaltsverzeichnis

<b>1</b>	<b>Einleitung</b>	<b>3</b>
<b>2</b>	<b>Recherchen</b>	<b>4</b>
2.1	Begriffserklärung PDC . . . . .	4
2.2	Softwaretechnische Lösung . . . . .	4
<b>3</b>	<b>Ausführung</b>	<b>5</b>
3.1	Installation von Debian . . . . .	5
3.2	Installation von Samba . . . . .	5
3.3	Konfiguration von Samba . . . . .	5
3.4	Ordner anlegen . . . . .	8
3.5	Benutzer anlegen . . . . .	8
3.6	PC hinzufügen . . . . .	9
3.7	Windows-PC zur Domäne hinzufügen . . . . .	9
3.8	Einloggen auf einem Computer an einer Domäne . . . . .	9
<b>4</b>	<b>Probleme</b>	<b>10</b>
<b>A</b>	<b>Aufbau des Netzwerkes</b>	<b>11</b>

# 1. Einleitung

Unser Kursthema in Fachpraxis Informationstechnik ist die Projektarbeit im Bereich der Netzwerktechnik. Für die Erstellung der Facharbeit wurden uns verschiedene Geräte zur Verfügung gestellt. Zur Auswahl standen mehrere Fritzboxen der Firma AVM und mehrere Server. Wir entschieden uns für einen Server. Mit einem Server war die Vielfalt der Projektthemen umfangreicher.

Unsere Schule hat vor kurzem ein Primary Domain Controller (PDC) System für die Schüler eingeführt. Daher hatten wir die Idee einen solchen PDC zu erstellen.

## 2. Recherchen

Zunächst haben wir uns über PDCs informiert. Danach mussten wir noch herausfinden wie genau man einen PDC Softwaretechnisch umsetzt.

### 2.1. Begriffserklärung PDC

Mit Windows-NT oder neuer ist es möglich mehrerer Rechner eines Netzwerkes zusammen in eine Domäne einzubinden. Der Primary Domain Controller ist der zentrale Verwaltungscomputer dazu. Somit ist es möglich Daten von Nutzern eines Netzwerkes, zum Beispiel im Netzwerk einer Firma, Zentral auf einen Server – dem PDC – zu speichern. Dies ermöglicht das sich jeder Nutzer eines solchen Netzwerkes auf jedem Rechner innerhalb dieses Netzwerkes anmelden kann. Die Benutzer und die zugehörigen Passwörter werden auf dem PDC verwaltet. Außerdem können Gruppen erstellt werden, denen unterschiedliche Berechtigungen zugeordnet werden können. So kann zum Beispiel ein Gruppe „Buchhaltung“ erstellt werden, dessen Benutzer auf den Drucker im Buchhaltungsbüro und auf den Ordner „Rechnungen“ zugreifen können.

### 2.2. Softwaretechnische Lösung

Normalerweise kann ein PDC mit einem NT-Server aufgesetzt werden. Wir haben uns jedoch dazu entschieden, die Linux Distribution Debian auf unserem Server zu installieren, da sie kostenlos ist. Da dies jedoch nicht NT ist, mussten wir nun eine Software installieren, die eine NT-Domäne emuliert. Dies ist mit Samba möglich. In der Praxis wird dies häufig gemacht, da somit keine Lizenzkosten fällig werden.

## 3. Ausführung

### 3.1. Installation von Debian

Das unter der GPL-Lizenz veröffentlichte Betriebssystem Debian wurde von der Debian-Website<sup>1</sup> heruntergeladen und auf eine CD gebrannt. Da der Server kein CD-Laufwerk hatte, musste zunächst die Abdeckung abgenommen werden und ein CD-Laufwerk installiert werden.

Nun wurde der Server gestartet und gleich darauf ins BIOS-Menü navigiert. Im BIOS-Menü wurde das erste Bootmedium auf das CD-Laufwerk umgestellt, anschließend wurde der Server neu gestartet und das Installationsprogramm von Debian erschien. Das Programm hat uns durch das Installationsverfahren geführt. Wie genau Debian installiert wurde, wird nicht weiter erläutert, da dieses nicht Thema der Facharbeit ist. Nach der Installation wurde das First-Boot-Device wieder auf die erste Festplatte umgestellt, das CD-Laufwerk ausgebaut und die Abdeckung vom Server wieder verschraubt.

### 3.2. Installation von Samba

Um den PDC zu realisieren musste Samba installiert werden. Dies geschieht mit den folgenden Befehlen:

```
apt-get update
apt-get upgrade
apt-get install samba
```

Dabei wird dem Paketmanagement-System APT<sup>2,3</sup> angewiesen die Paketliste zu aktualisieren, schon installierte – und veraltete – Pakete zu aktualisieren und dann Samba zu installieren.

### 3.3. Konfiguration von Samba

Nach der Installation von Samba wurde die Konfigurationsdatei angepasst. Sie ist zu finden unter `/etc/samba/smb.conf`. Die Bearbeitung wurde mit dem Programm Vim<sup>4</sup> getätigt.

---

<sup>1</sup>[www.debian.org](http://www.debian.org)

<sup>2</sup>Advanced Package Tool

<sup>3</sup>vgl. [/wiki.ubuntuusers.de/apt-get](http://wiki.ubuntuusers.de/apt-get)

<sup>4</sup>Vi Improved

```
cd /etc/samba
cp smb.conf smb.conf.original
vim smb.conf
```

In der ersten Zeile wurde in den Ordner /etc/samba gewechselt. Dann wurde eine Sicherheitskopie der Datei smb.conf erstellt. Mit vim wurde dann schließlich die Konfigurationsdatei im Editor Vim geöffnet. Die Konfigurationsdatei wurde wie folgt geändert:

```
[global]
# Domaenename und NetBIOS-Name:
workgroup = DOMAINCPAUL
netbios name = server4593

# Computername:
server string = Samba PDC von Patrick und Paul

# Hier werden die IPs angegeben, welche sich an der Domaene anmelden
duerfen. In diesem Fall werden alle IPs erlaubt, die mit 192.168 beginnen.
hosts allow = 192.168., 127.0.0.1/255.255.255.0

# Maximale Groesse der Log-Datei in kB.
max log size = 50

# Benutzer und Sicherheitseinstellungen:
# bei security = user werden bei der Benutzeranmeldung der Benutzername
und das Passwort uebermittelt und geprueft. Dies ist bei Windows-NT immer
noetig.
security = user

# Passwort Verschluesselung einschalten:
encrypt passwords = true
# Manche Betriebssysteme, z.B. Windows 95, unterstuetzen dies nicht.
Dann muss die Verschluesselung mit "false" abgeschaltet werden. Dies
stellt jedoch ein erhebliches Sicherheitsrisiko dar, da dann die Passwoerter
einfach ueber das Netzwerk mit Sniffing Programmen wie WireShark ausgelesen
werden koennen.

# Hier wird die Datei angegeben, in der die Benutzer und zugehoerigen
Passwoerter gespeichert sind. Bei jeder Anfrage einer Verbindung sieht
Samba in dieser Datei nach.
smb passwd file = /etc/samba/smbpasswd

# Die folgenden Zeilen werden benoetigt damit man in Windows das Passwort
eines Benutzers aendern kann.
```

```
unix password sync = yes
passwd program = /usr/bin/passwd %u
passwd chat = *Neues*Passwort* %n\n *Bitte*Passwort*Wiederholen* %n\n
*Passwort*erfolgreich*geaendert*

# Master-Browser 'Einstellungen':
# Mit dieser Angabe wird festgelegt, dass sich der Samba-Server als
Master-Browser fuer seine Domaene zur Verfuegung stellt.
local master = yes

preferred master = yes

#OS Chance des Samba-Servers Browser-Master zu werden
os level = 200

# Gast Account
guest account = nobody

# Samba zum WINS-Server machen:
wins support = yes
# Ende

# Samba zum Verwalter der Domaene machen:
domain master = yes

# Domaenen Logins aktivieren:
domain logons = yes

# Pfad in dem die Benutzerdateien gespeichert werden
# %L fuer diesen NetBIOS Namen, %U fuer den Benutzernamen
logon path = \\%L\Profiles\%U

# Heimatverzeichnis:
logon home = \\%L\Profiles\%U

# Laufwerk:
logon drive = H:

# Dieses Script wird ausgefuehrt, wenn Sich ein Benutzer an der Domaene
anmeldet:
logon script = netlogon.bat
```

```

#=== Freigaben ===
[homes]
comment = Heimatverzeichnis
browseable = no
read only = no
create mode = 0664
directory mode = 0775

# NT braucht den Ordner netlogon und profiles
[netlogon]
comment = Netzwerk Login Service
path = /home/samba/netlogon
writable = no

[Profiles]
path = /home/samba/profiles
browseable = yes
writeable = yes

```

Mit `/etc/init.d/samba restart` musste samba neu gestartet werden.

### 3.4. Ordner anlegen

Nun müssen die Ordner angelegt werden, welche in `/etc/samba/smb.conf` angegeben wurden. Das sind die Ordner `/home/samba/netlogon` und `/home/samba/profiles`.

```

mkdir /home/samba
mkdir /home/samba/netlogon
mkdir /home/samba/profiles

```

Anschließend müssen die Berechtigungen korrigiert werden:

```

chmod 777 /home/samba
chmod 755 /home/samba/netlogon
chmod 777 /home/samba/profiles

```

### 3.5. Benutzer anlegen

Danach wurden die Benutzer hinzugefügt. Dazu muss für jeden Benutzer ein Konto auf dem PDC angelegt werden.

```

adduser BENUTZERNAME

```

Dieser Benutzer muss nun noch samba bekannt gemacht werden:

```

smbpasswd -a BENUTZERNAME

```

Ausserdem benötigt jeder Benutzer ein eigenes Verzeichniss:

```
mkdir /home/samba/profiles/BENUTZERNAME
chmod 700 /home/samba/profile/BENUTZERNAME
chown BENUTZERNAME /home/samba/profile/BENUTZERNAME
```

### 3.6. PC hinzufügen

Damit sich ein Computer mit Windows an der Domäne anmelden kann, muss für den ihn auch noch ein Benutzer angelegt werden.

```
useradd -s /bin/false PC1$
smbpasswd -a -m PC1$
```

Hierbei ist darauf zu achten, dass 'PC1' mit dem NetBIOS Namen des Computers übereinstimmt. Den NetBIOS Namen findet man bei Windows unter **Systemeigenschaften** -> **Computername**.

### 3.7. Windows-PC zur Domäne hinzufügen

Die Konfiguration des PDCs' ist nun abgeschlossen und ein Windows-Computer kann zur Domäne hinzugefügt werden. Dies geschieht wie folgt:

1. „Systemsteuerung“ öffnen
2. „System“ öffnen
3. Den Reiter „Computername“ aktivieren
4. Auf „Ändern“ klicken
5. Den Punkt „Domäne“ auswählen und den Wert der Variable „workgroup“ der smb.conf eintragen. In unserem Fall ist das „DOMAINCPAUL“.
6. Nun erscheint ein Dialog in dem man den Adminnamen des PDC und das zugehörige Passwort eingibt. Also „root“ und das Kennwort.
7. Es erscheint eine Willkommensnachricht.

Die Einrichtung ist nun abgeschlossen.

### 3.8. Einloggen auf einem Computer an einer Domäne

Möchte nun ein Benutzer einer Domäne am Computer PC1 arbeiten, so gibt er seine Logindaten ein und wählt in dem Feld „Anmelden an:“ die Domäne aus. Nach dem Klick auf „Ok“ werden alle Benutzerdaten vom Server geladen sodass der Benutzer seine Dateien hat. Beim Abmelden werden die Daten wieder auf den Server geladen, sodass der Nutzer beim nächsten Login – auch an einem anderen Computer in der Domäne – wieder an seine Daten kommt.

## 4. Probleme

Es können sich nur Computer anmelden, die auf Windows-NT basieren. Ausserdem muss es sich immer um die Professional Edition von Windows handeln. Windows XP Home-Edition kann sich somit nicht an einer Domäne anmelden. Es gibt allerdings einen Trick um trotzdem an seine Dateien zu gelangen: Seinen Benutzerordner bindet man ganz einfach als Netzwerk-Laufwerk ein.

## A. Aufbau des Netzwerkes

