heinlein akademie

Samba4 mit Debian-Wheezy als DC

Author:
Stefan Kania

Ort:
Berlin

October 21, 2013

Contents

1 Einleitung

Mit samba4 kommt eine völlig neu Möglichkeit auf Sie zu, Linux in eine Windows-Umgebung zu integrieren. Mit samba4 wir sich die Art der Administration für Sie sehr stark ändern. Wenn Sie bis jetzt sehr viel über der Kommandozeile administriert haben, müssen Sie sich bei der Administration eines samba4 in vielen Fällen davon verabschieden. Samba4 ist ein Abbild des *Microsoft Active Directory (AD)* und kann und sollte mit den selben Werkzeugen verwaltet werden wie ein nativer AD. Natürlich gibt es auch Kommandos mit denen Sie samba4 auch weiterhin über die Kommandozeile administrieren können. Aber die Möglichkeiten der Kommandos sind oft nicht so umfangreich wie die der grafischen Werkzeugen und in einigen Fällen sind auch nicht alle administrative Tätigkeiten mit den Kommandos möglich. Deshalb wird in diesem Kurs eine großer Teil der Administration über grafische Werkzeuge stattfinden. An einigen Stellen dieses Kurses werden Sie denken: "Bin ich in einem Windows-Kurs?" Da kann ich Sie beruhigen, "Sind Sie nicht!"
Hier in diesem Kurs soll es darum gehen, den samba4 in den verschiedenen Situationen zu administrieren. Nach der Installation geht es weiter mit der Konfiguration eines *Domain Controllers (DC)*. Hierbei wird die Installation eines DNS-Servers eine große Rolle spielen.
Der DNS-Server ist ein Hauptbestandteil des ADs. Es gibt verschiedene Möglichkeiten den DNS-Server in Ihrer samba4-Domäne einzurichten. Zum einen die Verwendung des *Bind9* als eigenständiger Dienst und zum anderen die Verwendet des von samba4 integrierten DNS-Servers. Hier im Kurs soll die Verwendung des integrierten DNS-Servers Verwendung finden. Im Anhang finden Sie zusätzliche Informationen, wie Sie *bind9* als DNS-Server einrichten können.

2 Vorbereitung

Als erste installieren Sie Debian in der Grundinstallation, ohne weitere Zusatzpaket. Nur den *ssh-Server* sollten Sie bei der Installation mit installieren um gegebenenfalls den Server über `ssh` erreichen zu können.
Nach der Installation sollten Sie darauf achten, dass bei allen Partitionen, die von samba4 verwendet werden, die Optionen `acl` und `user_xattr` aktiviert sind, so wie im folgenden Auszug aus der Datei /etc/fstab:

```
UUID=d65b8d78-f125-46b6-a78e-a3614d98e5ed /  ext3   \
    errors=remount-ro,user_xattr,acl 0  1
```

Hinweis !

Bei Debian-Wheezy ist die Unterstützung von ACLs und den erweiterten Attributen schon fest eingebunden, hier müssen Sie die Datei fstab nicht anpassen. Testen Sie einfach mit den Kommandos `setfacl` und `setfattr` ob Ihr Dateisystem ACLs und Atribute unterstützt. Wenn das der Fall ist, müssen Sie die Datei fstab nicht anpassen.

Für den samba4 wird, wie auch bei einem Windows-Domaincontroller, auf jeden Fall ein *Kerberos-Server* für die Authentifizierung der Benutzer benötigt, der auch von *samba4* bereitgestellt wird. Auf jeden Fall wird ein DNS-Server benötigt, der nicht nur zur Auflösung der Hostnamen dient, sondern auch zur Auflösung der benötigten Dienste in der Domäne. Der DNS-Server kann entweder vom *samba4* bereitgestellt werden, oder Sie können eine *Bind9*-Nameserver im Netz einsetzen. Hier in der Unterlage, soll bei der Installation der integrierten DNS-Server verwendet werden. Der integrierte DNS hat Vorteile, auf die später näher eingegangen wird.
Der DNS-Server ist für die Auflösung der benötigten `SRV`-Einträge verantwortlich. Alle Hosts in Ihrem Netzwerk sollten über DNS auflösbar sein. Wenn Sie bereits einen *Bind9*-Nameserver in Ihrem Netzwerk laufen haben und diesen auch für samba4 verwenden wollen, ist das auch möglich. Als erstes sollten Sie die Version Ihres Bind-Servers prüfen. Sie benötigen mindestens die Version 9.7.x besser wäre auf jeden Fall die Version 9.8.x, da samba4 auf einige Funktionen zurückgreift, die

nur die Version 9.8.x bietet. Wenn Sie die Version 9.7.x verwenden, gibt es einige Einschränkungen hinsichtlich des dynamischen Updates des DNS-Servers

3 Installation des samba4 mit den SerNet-Paketen

Einige Distributionen bringen bereits samba4-Pakete in ihren eigenen Repositories mit, aber diese Pakete sind meist sehr veraltet, deshalb macht es keinen Sinn, diese Pakete zu installieren. Bei den SerNet-Paketen sind Sie immer auf einem aktuellen Stand und die Updates kommen, dank einem eigenen Repository, automatisch.
Als erstes müssen Sie sich auf der Webseite der Firma SerNet ein Account einrichten, da Sie sonst nicht an die aktuellen Pakete kommen. Die Anmeldung dort ist kostenlos und die Pakete samt aller updates sind open-source. Sie müssen lediglich eine Mail-Adresse angeben. Für die Anmeldung gehen Sie auf die Webseite `https://portal.enterprisesamba.com/` nach der Anmeldung können Sie jetzt die Datei /etc/apt/sources.list wie im folgenden Listing anpassen:

```
deb https://user:id@download.sernet.de/packages/samba/4.0/debian wheezy main
deb-src https://user:id@download.sernet.de/packages/samba/4.0/debian wheezy main
```

Hinweis !

Um die Pakete aus https-Quellen installieren zu können, müssen Sie das PAket apt-transport-https auf Ihrem System installieren.

Anschließend sollten Sie sich noch den *public-key* der Firma SerNet installieren, um die Pakete auch bei der Installation auf Echtheit prüfen zu können. Gehen Sie dazu so vor, wie im folgenden Listing:

```
root@samba4-1:~# gpg --keyserver wwwkeys.pgp.net --recv-keys F4428B1A
gpg: Verzeichnis ‘/root/.gnupg’ erzeugt
gpg: Neue Konfigurationsdatei ‘/root/.gnupg/gpg.conf’ erstellt
gpg: WARNUNG: Optionen in ‘/root/.gnupg/gpg.conf’ sind während dieses Laufes noch\
              nicht wirksam
gpg: Schlüsselbund ‘/root/.gnupg/secring.gpg’ erstellt
gpg: Schlüsselbund ‘/root/.gnupg/pubring.gpg’ erstellt
gpg: fordere Schlüssel F4428B1A von hkp-Server wwwkeys.pgp.net an
gpg: /root/.gnupg/trustdb.gpg: trust-db erzeugt
gpg: Schlüssel F4428B1A: Öffentlicher Schlüssel "Samba Support <Samba@SerNet.DE>"\
             importiert
gpg: keine uneingeschränkt vertrauenswürdigen Schlüssel gefunden
gpg: Anzahl insgesamt bearbeiteter Schlüssel: 1
gpg:                                importiert: 1

root@samba4-1:~# gpg --export --armor F4428B1A | apt-key add -
OK

root@samba4-1:~# gpg --fingerprint F4428B1A
pub   1024D/F4428B1A 2008-03-11 [verfällt: 2014-02-15]
  Schl.-Fingerabdruck = 7975 0C31 87AF 92DD AC46  086F D992 1B1C F442 8B1A
uid                  Samba Support <Samba@SerNet.DE>
```

Hinweis !

Sollte der Key-Server nicht erreichbar sein, können Sie das Paket auch per `wget http://ftp.sernet.de/pub/sernet-samba-keyring_1.3_all.deb` herunterladen und installieren

Jetzt können Sie ein `apt-get update` durchführen und die Pakete mit dem Kommando `apt-get install sernet-samba-ad` installieren. Dabei werden alle Abhängigkeiten automatisch aufgelöst. Damit ist die Installation des des samba4-DC abgeschlossen. Alle Dateien und Verlinkungen wurden automatisch erstellt, so dass es im nächsten Schritt mit der Konfiguration des Domaincontrollers weitergehen kann.
Wenn Sie später den Kerberos-Server des samba4 mit den Kommandozeilentools testen möchten, müssen Sie jetzt noch das Paket *heimdal-clients* per `apt-get` installieren.

3.1 Aufgaben

- Melden Sie sich auf der Webseite von SerNet an um die Repositories einbinden zu können.
- Konfigurieren Sie die Datei /etc/apt/sources.list.
- Installieren die den PGP-Key der Firma SerNet.
- führen Sie ein Upgrade und update der Maschine durch.
- Installieren Sie das Paket sernet-samba-ad und dessen Abhängigkeiten.

4 Konfiguration von samba4 mit dem integrierten DNS-Server

Für die Konfiguration und die Administration eines samba4-Servers steht Ihnen ein neues Werkzeug zur Verfügung, das Kommando `samba-tool`. Mit diesem Kommando können Sie die Domäne einrichten und verwalten, aber auch später die Benutzer und Gruppen sowie die Gruppenrichtlinen und den DNS-Server verwalten.
Jetzt könne Sie die Konfiguration des Domaincontrollers mit dem Kommando `samba-tool domain provision` durchführen. Bei der Konfiguration des Domaincontrollers werden alle benötigten Informationen abgefragt. Die folgenden Informationen sollten Sie für die Konfiguration bereit halten:

- Den REALM
  Der REALM wird für den Kerberos-Server benötigt. Der REALM wird bei der Einrichtung des DNS-Servers auch als DNS-Domainname verwendet.
- Den NetBIOS-Domainname
  Der NetBIOS-Domainname ist die Adresse, über die der Server per NetBIOS-Protokoll erreichbar ist. Der NetBIOS-Name sollte immer der erste Teil des REALMs sein.
- Funktion des Servers
  Sie sollten wissen, welche Rolle der Server in der Domäne übernehmen soll. In diesem Fall die Rolle des Domaincontrollers.
- Welcher DNS-Server soll verwendet werden
  Sie müssen wissen, ob Sie den internen DNS-Server des samba4 verwenden wollen oder eine bereits bestehenden *bind9* nutzen wollen.
- Die IP-Adresse eines eventuell benötigten DNS-Forwarders: An diese IP-Adresse werden alle DNS-Anfragen weitergeleitet, die nicht zur eigenen Zone gehören. Ohne einen Forward ist die Namensauflösung im Internet nicht möglich.

Im folgenden Listing sehen Sie den Ablauf der Konfiguration:

```
root@samba4-1:~# samba-tool domain provision
Realm [EXAMPLE.NET]:
Domain [EXAMPLE]:
Server Role (dc, member, standalone) [dc]:
DNS backend (SAMBA_INTERNAL, BIND9_FLATFILE, BIND9_DLZ, NONE) [SAMBA_INTERNAL]:
DNS forwarder IP address (write 'none' to disable forwarding) [172.21.0.1]: none
Administrator password:
Retype password:
Looking up IPv4 addresses
More than one IPv4 address found. Using 192.168.56.100
Looking up IPv6 addresses
No IPv6 address will be assigned
Setting up share.ldb
Setting up secrets.ldb
Setting up the registry
Setting up the privileges database
Setting up idmap db
Setting up SAM db
Setting up sam.ldb partitions and settings
Setting up sam.ldb rootDSE
Pre-loading the Samba 4 and AD schema
Adding DomainDN: DC=example,DC=net
Adding configuration container
Setting up sam.ldb schema
Setting up sam.ldb configuration data
Setting up display specifiers
Modifying display specifiers
Adding users container
Modifying users container
Adding computers container
Modifying computers container
Setting up sam.ldb data
Setting up well known security principals
Setting up sam.ldb users and groups
Setting up self join
Adding DNS accounts
Creating CN=MicrosoftDNS,CN=System,DC=example,DC=net
Creating DomainDnsZones and ForestDnsZones partitions
Populating DomainDnsZones and ForestDnsZones partitions
Setting up sam.ldb rootDSE marking as synchronized
Fixing provision GUIDs
A Kerberos configuration suitable for Samba 4 has been generated at \
  /var/lib/samba/private/krb5.conf
Once the above files are installed, your Samba4 server will be ready to use
Server Role:           active directory domain controller
Hostname:              samba4-1
NetBIOS Domain:        EXAMPLE
DNS Domain:            example.net
DOMAIN SID:            S-1-5-21-162095240-4194617395-2338447390
```

Wie Sie in dem Listing sehen können, wird jetzt der interne DNS verwendet.
Da bei dieser Konfiguration der interne DNS des samba4-Servers verwendet wird, brauchen Sie hier keine Konfiguration des Nameservers vornehmen.

Achtung !

Stellen Sie sicher, dass jetzt in der Datei /etc/resolv.conf die IP-Adresse `nameserver 127.0.0.1` oder die IP des Servers selber eingetragen ist. Sonst wird nicht der eigene DNS für die Auflösung der Hostnamen und Dienste in der AD-Domäne verwendet.

Damit ist die Konfiguration des ersten Domaincontrollers in der Domäne abgeschlossen.

5 Erster Start des samba4-Servers

Da der samba4 verschieden Rollen in einem Netzwerk übernehmen kann, müssen auch verschieden Prozesse beim Start des Server gestartet werden. Um dem Init-Skript mitzuteilen welche Prozesse der samba4-Server starten soll, müssen Sie die Datei /etc/default/sernet-samba wie im folgenden Listing anpassen:

```
# SAMBA_START_MODE defines how Samba should be started. Valid options are one of
#   "none"    to not enable it at all,
#   "classic" to use the classic smbd/nmbd/winbind daemons
#   "ad"      to use the Active Directory server (which starts the smbd on its own)
# (Be aware that you also need to enable the services/init scripts that
# automatically start up the desired daemons.)

SAMBA_START_MODE="ad"
```

Durch setzen der Variable `SAMBA_START_MODE="ad"` sorgen Sie dafür, dass der samba4-Server in Zukunft immer als Domaincontroller startet. Anschließend können Sie den Domaincontroller wie folgt starten:

```
root@samba4-1:~# service sernet-samba-ad start
[ ok ing SAMBA AD services : .
```

Anschließend können Sie mit dem Kommando `netstat` prüfen, welche Ports alle vom Samba geöffnet wurden und ob auch die entsprechenden Dienste bereitgestellt werden. Im folgenden Listing sehen Sie den Test:

```
root@samba4-1:~# netstat -tlp | grep samba
tcp        0      0 *:domain                *:*                     LISTEN      3999/samba
tcp        0      0 *:kerberos              *:*                     LISTEN      3993/samba
tcp        0      0 *:ldaps                 *:*                     LISTEN      3991/samba
tcp        0      0 *:1024                  *:*                     LISTEN      3987/samba
tcp        0      0 *:3268                  *:*                     LISTEN      3991/samba
tcp        0      0 *:3269                  *:*                     LISTEN      3991/samba
tcp        0      0 *:ldap                  *:*                     LISTEN      3991/samba
tcp        0      0 *:loc-srv               *:*                     LISTEN      3987/samba
tcp        0      0 *:kpasswd               *:*                     LISTEN      3993/samba
tcp6       0      0 [::]:domain             [::]:*                  LISTEN      3999/samba
tcp6       0      0 [::]:kerberos           [::]:*                  LISTEN      3993/samba
tcp6       0      0 [::]:ldaps              [::]:*                  LISTEN      3991/samba
tcp6       0      0 [::]:1024               [::]:*                  LISTEN      3987/samba
tcp6       0      0 [::]:3268               [::]:*                  LISTEN      3991/samba
tcp6       0      0 [::]:3269               [::]:*                  LISTEN      3991/samba
tcp6       0      0 [::]:ldap               [::]:*                  LISTEN      3991/samba
tcp6       0      0 [::]:loc-srv            [::]:*                  LISTEN      3987/samba
tcp6       0      0 [::]:kpasswd            [::]:*                  LISTEN      3993/samba
```

Jetzt können Sie den Verbindungsaufbau zum samba4-Server testen. Erst wenn dieser Test erfolgreich war, sollten Sie mit der weiteren Konfiguration des Servers fortfahren. Im folgenden Listing sehen Sie den Test des Verbindungsaufbaus mit dem Kommando `smbclient`:

```
root@samba4-1:~# smbclient -L localhost -Uadministrator
Enter administrator's password:
Domain=[EXAMPLE] OS=[Unix] Server=[Samba 4.0.5-SerNet-Debian-1.wheezy]

        Sharename       Type      Comment
        ---------       ----      -------
        netlogon        Disk
        sysvol          Disk
        IPC$            IPC       IPC Service (Samba 4.0.5-SerNet-Debian-1.wheezy)
Domain=[EXAMPLE] OS=[Unix] Server=[Samba 4.0.5-SerNet-Debian-1.wheezy]

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
```

Im Listing sehen Sie, dass bereits zwei Freigaben auf dem Domaincontroller bereitgestellt werden. Die Freigaben sysvol und netlogon. Diese beiden Freigaben werden auf einen Domaincontroller immer benötigt und somit bei der Erstkonfiguration auch immer angelegt. Die Verwendung der beiden Freigaben wird im Verlauf des Kurses genau erklärt.
Weiter sehen Sie in dem Listing, dass keine NetBIOS-Informationen über Server und Workgroup angegeben werden. Das ist auch korrekt so, denn der Domaincontroller kann später in der Netzwerkumgebung der Clients nicht gesehen werden. Sie sollten auch auf dem Domaincontroller keine weiteren Freigaben einrichten, sondern alle Daten immer auf einem Fileserver speichern. Der Grund dafür ist das unterschiedliche ID-Mapping der UIDs und GIDs der Linux-Benutzer. Mehr dazu im Verlauf des Kurses.
Jetzt laufen alle Dienste und der der Server ist erreichbar.

6 Erste Tests des Kerberos-Dienst

Um den Kerberos-Server zu testen, können Sie sich, mit `kinit` ein Ticket für den *administrator* der Domäne vom *KDC* holen und anschließend mit `klist` testen. Wenn Sie die SerNet-Pakete installiert haben, müssen Sie erst das Paket `heimdal-clients` mit allen Abhängigkeiten installieren. Die Datei /etc/krb5.conf die für die Authentifizierung nötig ist, wird bei der Konfiguration des Domaincontrollers automatisch erzeugt. Listing sehen Sie jetzt das Ergebnis eines Kerberos-Tests:

```
root@samba4-1:~# kinit administrator@EXAMPLE.NET
Password for administrator@EXAMPLE.NET:
Warning: Your password will expire in 40 days on Mon Jun 10 16:03:41 2013
root@samba4-1:~# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: administrator@EXAMPLE.NET

Valid starting       Expires              Service principal
30.04.2013 16:42:01  01.05.2013 02:42:01  krbtgt/EXAMPLE.NET@EXAMPLE.NET
        renew until 01.05.2013 16:41:56
```

Das Passwort für den *administrator* haben Sie bei der Konfiguration des *DC* festgelegt. Damit ist die Installation und Grundkonfiguration des Samba4-Servers abgeschlossen.

6.1 Aufgaben

- Konfigurieren Sie Ihre Domäne mit dem Kommando `samba-tool domain provision`
- Legen Sie die Startart des samba4 auf die Funktion Domaincontroller fest
- Starten Sie den Domaincontroller und prüfen Sie die Ports mit `netstat`
- Testen Sie die Funktionalität des Kerberos-Servers indem Sie sich ein TGT für den Administrator holen
- Testen Sie den Zugriff auf den Samba-Server mit dem Kommando `smbclient`

7 Konfiguration des Zeitservers

Da sämtliche Zugriffe auf den Kerberos sehr zeitkritisch sind, sollte in Ihrem Netz auf jeden Fall ein Zeitserver laufen. Der Zeitserver wird über den Dienst *ntp* bereit gestellt. Achten Sie darauf, dass der *ntpd* mindestens die Version als 4.2.6 hat, da ältere Versionen keine Signierung erlauben. Die Signierung des Zeitservers wird aber vom AD benötigt. Ein Zeitserver ohne Signierung kann nicht mit dem AD zusammenarbeiten. Bei Debian-Wheezy ist bereits ein passende Version enthalten. Sie müssen diese nur mit `apt-get install ntp` installieren. Anschließend müssen Sie die Datei /etc/ntp.conf wie im folgenden Listing anpassen:

```
server 127.127.1.0
fudge  127.127.1.0 stratum 10
server 0.pool.ntp.org  iburst prefer
server 1.pool.ntp.org  iburst prefer
driftfile /var/lib/ntp/ntp.drift
logfile /var/log/ntp
ntpsigndsocket /var/libsamba/ntp_signd/
restrict default kod nomodify notrap nopeer mssntp
restrict 127.0.0.1
restrict 0.pool.ntp.org mask 255.255.255.255 nomodify notrap nopeer noquery
restrict 1.pool.ntp.org mask 255.255.255.255 nomodify notrap nopeer noquery
```

Vor dem Neustart des Zeitservers müssen Sie dem *ntpd* noch das Recht geben auf den signierten Socket vom samba4 zugreifen zu können. Dazu ändern Sie die besitzenden Gruppe am Verzeichnis /var/lib/samba/ntp_signd wie im folgenden Listing:

```
root@samba4-1:~# chgrp ntp /var/lib/samba/ntp_signd/
```

Die Gruppe muss nur die Rechte *r* und *x* besitzen. Nach erstellen der Konfiguration starten Sie den Zeitserver neu. Jetzt können alle Windows-Clients und alle Windows-Server in der Domäne den Zeitserver für die Zeitsynchronisation nutzen.

7.1 Aufgaben

- Installieren Sie den *ntp*
- Konfigurieren Sie den Zeitserver in der Datei /etc/ntp.conf und starten den Zeitserver neu

8 Benutzer- und Gruppenverwaltung

Ein positiver Punkt schon mal am Anfang: Im Gegensatz zu Samba3 müssen Sie bei samba4 kein Linux-Konto erstellen, bevor Sie ein Samba-Konto erstellen können. Hier zeigt sich dann ganz klar die Unterschiede in dem Konzept von Samba3 und samba4. Sie legen nur noch ein Samba-Konto an. Der samba4-Server sorgt später über das ID-Mapping dafür, dass auch Linux-Benutzer das System zur Authentifizierung nutzen können.
Nach der Installation und Konfiguration des Samba4-Servers haben Sie jetzt einen AD-Controller, jetzt müssen Sie die Benutzer und Gruppen auch so verwalten, dass sie AD-konform sind. Für die Benutzerverwaltung gibt es jetzt verschieden Wege:

- Mit dem samba4-Werkzeug `samba-tool`
  Mit dem `samba-tool` können Sie Benutzer und Gruppen über die Kommandozeile verwalten. Damit haben Sie dann auch die Möglichkeit mehrere Benutzer über Skripte zu erzeugen.
- Mit dem *swat2*
  Mit dem *swat2* können Sie Benutzer und Gruppen grafisch verwalten. Mit swat haben Sie ein Werkzeug, dass sehr gut mit der Benutzer- und Gruppenverwaltung von samba4 zurecht kommt. Da der *swat2* aber im Moment nicht weiterentwickelt wird, soll in diesem Seminar nicht näher darauf eingegangen werden. Im Anhang dieser Unterlage finden Sie die Installation und Konfiguration und die Verwaltung von Benutzern und Gruppen mittels des *swat2*.
- Mit dem *LDAP-Account-Manager(LAM)*
  Dank dem Einsatz von Roland Gruber gibt es jetzt ein Modul für den *LAM* mit dem Sie die Benutzer und Gruppen über das webbasierte Werkzeug verwalten können, obwohl bei samba4 kein *openLDAP* zum Einsatz kommt, sondern ein eigener LDAP-Server.
- Über eine Windows-Client mit den *Windows Remote Administration Tools(RSAT)*
  Für Windows7 können Sie die *Windows Remote Server Administration Tools* bei Microsoft herunterladen und dann von Windows aus die Verwaltung von Benutzern und Gruppen vornehmen. Voraussetzung ist mindestens eine Windows7 Professional.

Hier im Kurs sollen die Möglichkeiten erklärt werden, wie Sie Benutzer und Gruppen über die Kommandozeile, den LAM und die RSAT durchführen können.

8.1 Benutzer- und Gruppenverwaltung über die Kommandozeile

Im ersten Teil geht es um die Verwaltung der Benutzer und Gruppen über die Kommandozeile. Die gesamte Verwaltung der Benutzer und Gruppen geht hier über das Kommando `samba-tool`. Das *samba-tool* ist die Zusammenfassung der unter Samba3 bekannten *net*-Tools und ersetzt diese bei der Verwaltung von Gruppen und Benutzern vollständig.

8.1.1 Verwaltung von Gruppen

Mit dem Kommando `samba-tool group` verwalten Sie die Gruppen. Zu dem Kommando gibt es die verschieden Optionen für die Verwaltung:

- Auflisten der Gruppen mit `group list`
  Eine Übersicht über alle Gruppen im System erhalten Sie, wie im folgenden Listing zu sehen, mit `samba-tool group list`:

```
root@samba4-1:~# samba-tool group list
Allowed RODC Password Replication Group
Enterprise Read-Only Domain Controllers
Denied RODC Password Replication Group
Pre-Windows 2000 Compatible Access
Windows Authorization Access Group
Certificate Service DCOM Access
Network Configuration Operators
Terminal Server License Servers
Incoming Forest Trust Builders
Read-Only Domain Controllers
Group Policy Creator Owners
Performance Monitor Users
Cryptographic Operators
Distributed COM Users
Performance Log Users
Remote Desktop Users
Account Operators
Event Log Readers
RAS and IAS Servers
Backup Operators
Domain Controllers
Server Operators
Enterprise Admins
Print Operators
Administrators
Domain Computers
Cert Publishers
DnsUpdateProxy
Domain Admins
Domain Guests
Schema Admins
Domain Users
Replicator
IIS_IUSRS
DnsAdmins
Guests
Users
```

Hier sehen Sie eine Liste aller Gruppen, die nach der Installation des Systems vorhanden sind. Bei diesen Gruppen handelt es sich um Gruppen, die auch für die Verwaltung des ADs unter Windows benötigt werden. Löschen Sie keine der hier aufgelisteten Gruppen aus Ihrem System.

- Auflisten der Gruppenmitglieder einer Gruppe mit `group listmembers <group>`
  Wenn Sie wissen wollen, welche Benutzer Mitglied einer Gruppe sind, können Sie, wie im folgenden Listing zu sehen, dieses mit `group listmembers <group>` realisieren:

```
root@samba4-1:~# samba-tool group listmembers administrators
Administrator
Enterprise Admins
Domain Admins
```

Beim Auflisten der Gruppe `administrators` sehen Sie, dass die Gruppe `Domain Admins` Mitglied der Gruppe ist. Samba4 kann mit den verschachtelten Gruppen umgehen. Auch Sie können später bei der Administration Gruppen verschachteln. Im Gegensatz zu Samba3 müssen Sie bei samba4 die Möglichkeit der verschachtelten Gruppen nicht mehr in der Datei smb.conf aktivieren.

- Anlegen einer neuen Gruppe mit `group add <groupname>`
  Eine neu Gruppe können Sie mit dem Kommando `group add <groupname>` zu Ihrer Gruppenliste hinzufügen. Das folgenden Listing zeigt das Anlegen einer neuen Gruppe:

```
root@samba4-1:~# samba-tool group add datengruppe
Added group datengruppe
```

  Die gerade angelegte Gruppe ist eine reine Windows-Gruppe. Sie könne Die Gruppe mit dem Kommando `wbinfo -g` sehen, aber im Moment noch nicht mit `getent group`. Auch können Sie mit `chgrp <neu-Gruppe> <Eintrag>` keine Berechtigungen setzen.
  Für die Verwendung der Gruppe unter Linux müssen Sie das ID-Mapping aktivieren. Hier müssen Sie zwischen dem ID-Mapping auf einen Domaincontroller und dem ID-Mapping auf einem Fileserver oder einem Linux-Client unterscheiden. Auf dem Domaincontroller übernimmt samba4 selber das ID-Mapping und weißt den Windows-Benutzern und Gruppen eigene IDs zu. Auf einen Fileserver oder einem Linux-Client übernimmt diese Aufgabe der *winbind*. Mehr zu dieser Problematik erfahren Sie im verlauf des Kurses.
  Um die Gruppen und später auch die Benutzer im Linux-System sehen und nutzen zu können, muss die Datei /etc/nsswitch.conf wie im folgenden Listing angepasst werden:

```
passwd compat winbind
group compat winbind
```

  Nach der Anpassung der Datei /etc/nsswitch.conf können Sie jetzt mit dem Kommando `getent group` alle Gruppen sehen und auch Rechte an die Gruppen über die Kommandozeile vergeben.
  Hinweis !

In einer Umgebung mit mehreren Servern werden auf dem DC keine Daten gespeichert, somit müssen Sie die Einträge in die Datei nsswitch.conf hier nicht vornehmen

- Hinzufügen eines oder mehrerer Benutzer zu einer bestehenden Gruppe mit `group addmembers <groupname> <members>`
  Über `group addmembers <groupname> <members>` können Sie mehrere Benutzer gleichzeitig zu einer Gruppe hinzufügen. Das folgende Listing zeigt dieses Vorgehen:

```
root@samba4-1:~# samba-tool group addmembers datengruppe "Domain Users"
Added members to group datengruppe

root@samba4-1:~# samba-tool group listmembers datengruppe
Domain Users
```

  Da Sie Gruppen verschachteln können, können Sie auch eine oder mehrere der Standardgruppen zu Ihrer Gruppe hinzufügen, achten Sie darauf, dass einig der Gruppen ein Leerzeichen im Namen haben. Dann müssen Sie den Gruppennamen beim hinzufügen mit Hochkommata quotieren.
  Hinweis !

Sie können mit dem Kommando `group addmembers <groupname> <members>` keine lokalen Gruppen des System zu den AD-Gruppen hinzufügen.

- Entfernen von einem oder mehreren Benutzern aus einer Gruppe mit `group removemembers <groupname> <members>`
  Wenn Sie einen oder mehrere Benutzer aus eine Gruppe entfernen möchten, geht das mit dem Kommando `group removemembers <groupname> <members>`. Das folgenden Listing zeigt auch hierfür ein Beispiel:

```
root@samba4-1:~# samba-tool group removemembers datengruppe "Domain Users"
Removed members from group datengruppe
```

  Sie können hier auch mehrere Mitglieder, durch Leerzeichen getrennt, aus der Gruppe entfernen.

8.1.2 Aufgaben

- Erstellen Sie eine neu Gruppe mit dem Kommando `samba-tool`. Diese Gruppe später dazu verwendet werden um allen Benutzern Recht an einer Freigabe zu geben.
- Fügen Sie den Administrator zu Ihrer neuen Gruppe hinzu.
- Lassen Sie sich die Mitglieder anzeigen.
- Sorgen Sie dafür, dass Sie die Benutzer mit dem Kommando `getent passwd` angezeigt bekommen.
- Erstellen Sie ein Verzeichnis */alle* und weisen diese Verzeichnis der neuen Gruppe zu.

8.1.3 Verwaltung von Benutzern

Für die Verwaltung der Benutzer verwenden Sie das Kommando `samba-tool user`. Genau wie bei der Verwaltung der Gruppen gibt es auch hier wieder die verschieden Kommandos für die verschieden Aufgaben:

- Auflisten der Benutzer mit `user list`
  Alle Benutzer können Sie sich mit den Kommando `user list` anzeigen lassen. Das folgende Listing zeigt eine Liste alle Benutzer nach der Installation des Systems:

  ```
  root@samba4-1:~# samba-tool user list
  Administrator
  dns-samba4-1
  krbtgt
  Guest
  ```

  Wie schon zuvor bei den Gruppen, sehen Sie hier alle Benutzer die nach der Installation im System vorhanden sind. Auch hier gilt, löschen Sie keinen der Benutzer.

- Anlegen eine Benutzers mit `user create username <password>`
  Um einen neuen Benutzern über die Kommandozeile anzulegen, verwenden Sie das Kommando `samba-tool user create username <password>`. Achten Sie bei dem Passwort auf die Komplexitätsregel. Im folgenden Listing sehen Sie eine Beispiel mit einem Passwort, dass diesen Regeln nicht entspricht. Erst im zweiten Versuch wird der Benutzer angelegt.

  ```
  root@samba4-1:~# samba-tool user create Stefan geheim --given-name=Stefan \
  --surname=Kania
  samba-tool user create Stefan geheim --given-name=Stefan --surname=Kania
  ERROR(ldb): Failed to add user 'Stefan':  - 0000052D: Constraint violation - \
      check_password_restrictions: the password does not meet the complexity criteria!

  root@samba4-1:~# samba-tool user create Stefan geheim\!123 --given-name=Stefan \
  --surname=Kania
  User 'Stefan' created successfully

  root@samba4-1:~# samba-tool user list
  Administrator
  Stefan
  dns-samba4-1
  krbtgt
  Guest
  ```

Wie sie in dem Beispiel sehen, können Sie beim Anlegen des Benutzers gleich Parameter mit angeben. In den Beispiel ist es der Vor- und der Nachname. Alle Werte die im LDAP Verwendet werden, können hier mit übergeben werden. Da es sich dabei um eine größere Anzahl von Parametern handelt, kann an dieser Stelle nicht darauf eingegangen werden. Bei der Benutzerverwaltung mit grafischen Werkzeugen, werden Sie alle Parameter sehen und anpassen können.

Hinweis !

Das Home-Verzeichnis des Benutzers wird nicht mit angelegt, das müssen Sie selber auf dem entsprechenden Server anlegen und mit Rechten versehen.

Nach dem Anlegen des Benutzers können Sie sich den Benutzer wieder mit `samba-tool user list` auflisten lassen. Auch die Benutzer sehen Sie wieder mit `wbinfo -u`. Wie schon bei den Gruppen, werden die neuen Benutzer mit `getent passwd` nur angezeigt, wenn Sie die Datei /etc/nsswitch.conf angepasst haben.

Wichtig !

In manchen Anleitungen finden Sie noch das Kommando `samba-tool user add <username> <password>`. Diese Kommando ist nur aus Kompatibilitätsgründen noch vorhanden und sollte nicht verwendet werden.

- Deaktivieren eine Benutzers mit `samba-tool user disable <username>`
  Wenn Sie einen bestehenden Benutzer nur deaktivieren wollen, weil der Benutzer sich zur Zeit nicht anmelden darf oder soll, können Sie den Benutzer einfach deaktivieren und müssen den Benutzer nicht gleich löschen. Im folgenden Listing sehen Sie ein Beispiel für das Deaktivieren eines Benutzers:

  ```
  root@samba4-1:~# samba-tool user disable Stefan
  ```

  Leider erhalten Sie beim `disable` keine Meldung. Ob das so gewollt ist oder im Moment noch ein Bug ist, wird sich bei den nächsten Samba4 Versionen herausstellen.

- Aktiveren eines deaktivierten Benutzers mit `samba-tool user enable <username>`
  Um einen zuvor deaktivierten Benutzer wieder zu aktivieren, verwenden Sie das Kommando `samba-tool user enable <username>` wie Sie im folgenden Listing sehen können:

  ```
  root@samba4-1:~# samba-tool user enable Stefan
  Enabled user 'Stefan'
  ```

  Hier bekommen Sie eine Meldung, dass der Benutzer wieder `enabled` ist.

- Ändern des Passworts eines Benutzers mit `user setpassword <username>`
  Für den Fall, dass ein Benutzer sein Passwort vergessen hat oder Sie einem Benutzer aus einem anderen Grund ein neues Passwort zuweisen wollen, verwenden Sie das Kommando `samba-tool user setpassword <username>`. Im folgenden Listing sehen Sie ein Beispiel dafür:

  ```
  root@samba4-1:~# samba-tool user setpassword Stefan
  New Password:
  Changed password OK
  ```

  Beim setzen eines neuen Passworts achten Sie wieder auf die Komplexitätsregeln. Das neue Passwort wird nur einmal eingegeben, achten Sie also darauf, was Sie eingeben. Sonst müssen Sie den Vorgang wiederholen.

- Löschen eines Benutzers mit `samba-tool user delete <username>`
  Wenn Sie einen Benutzer aus dem System entfernen wollen, nutzen Sie dafür das Kommando `user delete <username>`, wie im folgenden Listing:

  ```
  root@samba4-1:~# samba-tool user delete Stefan
  Deleted user Stefan
  ```

Denken Sie daran, dass ein eventuelles Home-Verzeichnis des Benutzers nicht automatisch gelöscht wir.

8.1.4 Aufgaben

- Erstellen Sie einen neuen Benutzer mit dem Kommando `samba-tool`.
- Ändern Sie das Passwort für den neuen Benutzer.
- Fügen Sie den neuen Benutzer der vorher erstellten Gruppe als Mitglied zu.

8.1.5 Ändern und suchen von Benutzern mit den ldb-tools

Natürlich können Sie auch über die Kommandozeile nach Benutzern und Gruppen suchen und diese mittels Skripten verändern. Dazu gibt es verschieden Kommandos. Wenn Sie bis jetzt vielleicht schon mit *openLDAP* gearbeitet haben, wird Ihnen die Syntax bekannt vorkommen.

- Auflisten von Benutzern mittels `ldbsearch`
  Mit dem Kommando `ldbsearch` können Sie nach Objekten suchen, natürlich können Sie auch hier wieder Filter verwenden um die Ergebnisse einzugrenzen. Im folgenden sehen Sie ein paar Beispiele für die Suche mit `ldbsearch`:

```
root@samba4-1:~# ldbsearch -H ldaps://localhost "cn=stefan"
search error - LDAP error 1 LDAP_OPERATIONS_ERROR -  <00002020:\
    Operation unavailable without authentication> <>

root@samba4-1:~# ldbsearch -H ldaps://localhost "cn=stefan" -Uadministrator
Password for [EXAMPLE\administrator]:
# record 1
dn: CN=Stefan,CN=Users,DC=example,DC=net
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: Stefan
instanceType: 4
whenCreated: 20130506092056.0Z
uSNCreated: 3667
name: Stefan
objectGUID: 4856ec22-822e-465f-89ff-69144dcdf600
badPwdCount: 0
codePage: 0
countryCode: 0
badPasswordTime: 0
lastLogoff: 0
lastLogon: 0
pwdLastSet: 0
primaryGroupID: 513
objectSid: S-1-5-21-2424060308-3148540958-3219910488-1108
accountExpires: 9223372036854775807
logonCount: 0
sAMAccountName: Stefan
sAMAccountType: 805306368
objectCategory: CN=Person,CN=Schema,CN=Configuration,DC=example,DC=net
displayName: Stefan Kania
```

```
memberOf: CN=datengruppe,CN=Users,DC=example,DC=net
homeDrive: B:
userAccountControl: 544
givenName: Stefan
sn: Kania
whenChanged: 20130508085027.0Z
uSNChanged: 3691
distinguishedName: CN=Stefan,CN=Users,DC=example,DC=net

# Referral
ref: ldap://example.net/CN=Configuration,DC=example,DC=net

# returned 2 records
# 1 entries
# 1 referrals
```

Im ersten Teil dieses Beispiels sehen Sie, was passiert, wenn Sie ohne eine Authentifizierung versuchen auf den LDAP zuzugreifen. Denke Sie daran, wenn Sie über das Netz auf den LDAP zugreifen müssen Sie sich immer authentifizieren, so wie Sie es im zweiten Versuch sehen.
Im nächsten Beispiel wird nicht über das Netz auf die Benutzerdatenbank zugegriffen, sondern direkt auf dem Domaincontroller auf die Benutzerdatenbank.

```
root@samba4-1:~# ldbsearch  --url=/var/lib/samba/private/sam.ldb \
    "cn=stefan"
# record 1
dn: CN=Stefan,CN=Users,DC=example,DC=net
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: Stefan
instanceType: 4
whenCreated: 20130506092056.0Z
uSNCreated: 3667
name: Stefan
objectGUID: 4856ec22-822e-465f-89ff-69144dcdf600
badPwdCount: 0
codePage: 0
countryCode: 0
badPasswordTime: 0
lastLogoff: 0
lastLogon: 0
pwdLastSet: 0
primaryGroupID: 513
objectSid: S-1-5-21-2424060308-3148540958-3219910488-1108
accountExpires: 9223372036854775807
logonCount: 0
sAMAccountName: Stefan
sAMAccountType: 805306368
objectCategory: CN=Person,CN=Schema,CN=Configuration,DC=example,DC=net
displayName: Stefan Kania
memberOf: CN=datengruppe,CN=Users,DC=example,DC=net
homeDrive: B:
userAccountControl: 544
givenName: Stefan
sn: Kania
whenChanged: 20130508085027.0Z
```

```
uSNChanged: 3691
distinguishedName: CN=Stefan,CN=Users,DC=example,DC=net

# Referral
ref: ldap://example.net/CN=Configuration,DC=example,DC=net

# returned 2 records
# 1 entries
# 1 referrals
```

Wie Sie hier sehen, können Sie direkt auf dem Server auf die Datenbankdatei zugreifen. Bei diesem Zugriff wird keine Authentifizierung benötigt. Der Zugriff wird hier über die Dateisystemrechte gesteuert. Zugriff auf die Datei hat aber nur der *root*, so dass ein normaler Benutzer diese Möglichkeit nicht nutzen kann.
Auch ein Zugriff über den lokalen LDAP-Socket ist möglich. Auch hier kann dieser Zugriff nur vom Benutzer *root* durchgeführt werden. Da nur der Benutzer rechte am Socket hat.

```
root@samba4-1:~# ldbsearch -H ldapi:///var/lib/samba/private/ldap_priv/ldapi \
  "cn=stefan"
# record 1
dn: CN=Stefan,CN=Users,DC=example,DC=net
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: Stefan
instanceType: 4
whenCreated: 20130506092056.0Z
uSNCreated: 3667
name: Stefan
objectGUID: 4856ec22-822e-465f-89ff-69144dcdf600
badPwdCount: 0
codePage: 0
countryCode: 0
badPasswordTime: 0
lastLogoff: 0
lastLogon: 0
pwdLastSet: 0
primaryGroupID: 513
objectSid: S-1-5-21-2424060308-3148540958-3219910488-1108
accountExpires: 9223372036854775807
logonCount: 0
sAMAccountName: Stefan
sAMAccountType: 805306368
objectCategory: CN=Person,CN=Schema,CN=Configuration,DC=example,DC=net
displayName: Stefan Kania
memberOf: CN=datengruppe,CN=Users,DC=example,DC=net
homeDrive: B:
userAccountControl: 544
givenName: Stefan
sn: Kania
whenChanged: 20130508085027.0Z
uSNChanged: 3691
distinguishedName: CN=Stefan,CN=Users,DC=example,DC=net

# Referral
ref: ldap://example.net/CN=Configuration,DC=example,DC=net

#root@samba4-1:~# ldbsearch -H ldapi:///var/lib/samba/private/ldap_priv/ldapi\
```

```
  "cn=stefan"
# record 1
dn: CN=Stefan,CN=Users,DC=example,DC=net
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: Stefan
instanceType: 4
whenCreated: 20130506092056.0Z
uSNCreated: 3667
name: Stefan
objectGUID: 4856ec22-822e-465f-89ff-69144dcdf600
badPwdCount: 0
codePage: 0
countryCode: 0
badPasswordTime: 0
lastLogoff: 0
lastLogon: 0
pwdLastSet: 0
primaryGroupID: 513
objectSid: S-1-5-21-2424060308-3148540958-3219910488-1108
accountExpires: 9223372036854775807
logonCount: 0
sAMAccountName: Stefan
sAMAccountType: 805306368
objectCategory: CN=Person,CN=Schema,CN=Configuration,DC=example,DC=net
displayName: Stefan Kania
memberOf: CN=datengruppe,CN=Users,DC=example,DC=net
homeDrive: B:
userAccountControl: 544
givenName: Stefan
sn: Kania
whenChanged: 20130508085027.0Z
uSNChanged: 3691
distinguishedName: CN=Stefan,CN=Users,DC=example,DC=net

# Referral
ref: ldap://example.net/CN=Configuration,DC=example,DC=net

# returned 2 records
# 1 entries
# 1 referrals
 returned 2 records
# 1 entries
# 1 referrals
```

Auch eine eingeschränkte Suche auf bestimmte Attribute ist möglich, wie Sie es im folgenden Listing sehen können:

```
root@samba4-1:~# ldbsearch -H ldapi:///var/lib/samba/private/ldap_priv/ldapi\
    "cn=stefan" attr sn givenName
# record 1
dn: CN=Stefan,CN=Users,DC=example,DC=net
givenName: Stefan
sn: Kania

# Referral
ref: ldap://example.net/CN=Configuration,DC=example,DC=net
```

```
# returned 2 records
# 1 entries
# 1 referrals
```

- Ändern eines Objektes mit `ldbedit`
  Mit dem Kommando `ldbedit` können Sie einzelne Objekte ändern und die Änderung wieder im LDAP speichern. Für die Änderung wird der bei Ihnen im System eingestellte Standardeditor verwendet. Im nächsten Listing sehen Sie den Aufruf von `ldbedit`.

  ```
   root@samba4-1:~# ldbedit -H ldapi:///var/lib/samba/private/ldapi\
    -Uadministrator sAMAccountName=ktom
  Password for [EXAMPLE\administrator]:

  # 0 adds  1 modifies  0 deletes
  ```

  Wenn Sie beim Editieren einen Fehler machen, wird die Änderung nicht gespeichert und Sie bekommen eine Fehlermeldung wie im nächsten Listing zu sehen ist:

  ```
  root@samba4-1:~# ldbedit -H ldapi:///var/lib/samba/private/ldapi\
    -Uadministrator sAMAccountName=ktom
  Password for [EXAMPLE\administrator]:
  failed to modify CN=KTom,CN=Users,DC=example,DC=net - LDAP error 16\
        LDAP_NO_SUCH_ATTRIBUTE - <acl_modify: attribute 'ivenName' on\
        entry 'CN=KTom,CN=Users,DC=example,DC=net'\
        was not found in the schema!> <>
  ```

- Ändern eines Objektes mit `ldbmodify`
  Sie können einzelne Attribute eines oder mehrerer Objekte auch mithilfe des Kommandos `ldbmodify` und einer ldif-Datei ändern. Als erstes erstellen Sie eine ldif-Datei wie im folgenden Beispiel:

  ```
  dn: cn=ktom,cn=users,dc=example,dc=net
  changetype: modify
  replace: sn
  sn: Tom
  -
  add: description
  description: Ein Benutzer
  -
  delete: PostOfficeBox
  ```

  Anschließend spielen Sie die Änderung wie im folgenden Beispiel ein:

  ```
  root@samba4-1:~# ldbmodify -H ldapi:///var/lib/samba/private/ldapi\
    -Uadministrator ktom.ldif
  Password for [EXAMPLE\administrator]:
  Modified 1 records successfully
  ```

  Wollen Sie einen weiteres Objekt mit der selben ldif-Datei ändern, können Sie dieses einfach durch eine Leerzeile in die Datei eintragen. Die Syntax ist hier identisch mit der von `ldapmodify`.

8.1.6 Verwendung von `ldapsearch`

Sie können sich alle Objekte auch von einem beliebigen Linux-Client aus auflisten lassen. Dazu verwenden Sie das Kommando `ldapsearch` aus dem Paket *ldap-utils*. Nachdem Sie das Paket installiert haben, passen Sie die Datei /etc/ldap/ldap.conf so wie im folgenden Listing an:

```
BASE    dc=example,dc=net
URI     ldap://samba4-1.example.net
```

Anschließend können Sie mit `ldapsearch` den LDAP durchsuchen. Der Zugriff auf den LDAP geht nur über einen *strong-bind*, also dürfen Sie die Option `-x` auf keinen Fall setzen. Die Filter, die Sie von der Verwendung unter openLDAP kennen, funktionieren aber auch hier. Im folgenden Listing sehen Sie einen Zugriff mittels `ldapsearch` auf den LDAP:

```
root@lam:~# ldapsearch  -D "cn=administrator,cn=users,dc=example,dc=net" \
    "(cn=Stefan)" -W -LLL
Enter LDAP Password:
dn: CN=Stefan,CN=Users,DC=example,DC=net
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: Stefan
instanceType: 4
whenCreated: 20130506092056.0Z
uSNCreated: 3667
name: Stefan
objectGUID:: IuxWSC6CX0aJ/2kUTc32AA==
badPwdCount: 0
codePage: 0
countryCode: 0
badPasswordTime: 0
lastLogoff: 0
lastLogon: 0
pwdLastSet: 0
primaryGroupID: 513
objectSid:: AQUAAAAAAAUVAAAAlDl8kB7sqrtY7+u/VAQAAA==
accountExpires: 9223372036854775807
logonCount: 0
sAMAccountName: Stefan
sAMAccountType: 805306368
objectCategory: CN=Person,CN=Schema,CN=Configuration,DC=example,DC=net
displayName: Stefan Kania
memberOf: CN=datengruppe,CN=Users,DC=example,DC=net
homeDrive: B:
userAccountControl: 544
givenName: Stefan
sn: Kania
whenChanged: 20130508085027.0Z
uSNChanged: 3691
distinguishedName: CN=Stefan,CN=Users,DC=example,DC=net

# refldap://example.net/CN=Configuration,DC=example,DC=net
```

Hinweis !

Achten Sie darauf, dass der LDAP vom samba4 keinen *simple-bind* unterstützt und Sie deshalb die Option `-x` nicht verwenden dürfen.

Wie Sie sehen, lassen sich sehr viele Aufgaben über die Kommandozeile erledigen. Aber auf Grund der Komplexität der Konten sollten Sie besser eine der grafischen Möglichkeiten wählen, wenn es darum geht Benutzer im täglichen Geschäft zu verwalten. Um eine größere Anzahl an Gruppen und Benutzern zu verwalten, ist das Kommando `samba-tool` aber sehr gut geeignet.

8.2 Benutzer- und Gruppenverwaltung mit dem *LAM*

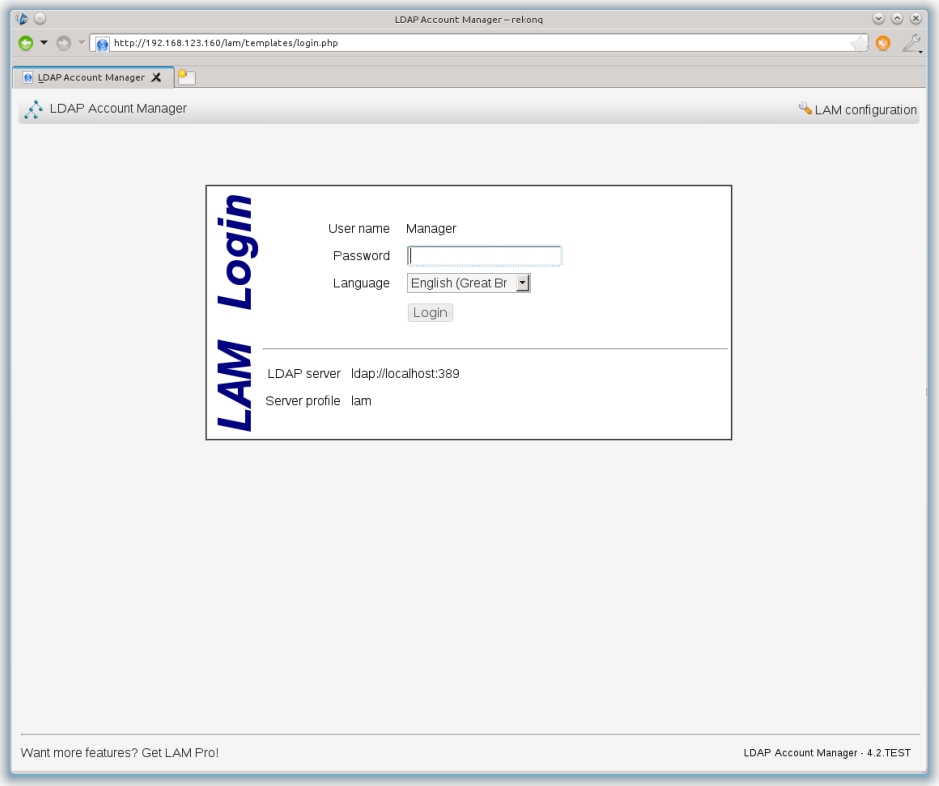
Der ein oder andere von Ihnen kennt den *LDAP-Account-Manager(LAM)* vielleicht schon als Werkzeug für den *openLDAP*. Seit der Version 4.2 ist der LAM auch in der Lage, *samba4* zu verwalten. Da mit dem LAM weitaus mehr Möglichkeiten bestehen den *samba4* zu verwalten als mit dem *swat2*, soll in diesem Abschnitt etwas genauer auf den LAM eingegangen werden.

8.2.1 Installation des LAM

Als erstes müssen Sie den LAM installieren. Dazu laden Sie sich die aktuelle Version des LAM von der Webseite https://www.ldap-account-manager.org/static/tmp/ herunter. Installieren Sie das Paket mit dem Kommando `dpkg` Bei der Installation kommt es zu nicht aufgelösten Abhängigkeiten. Diese können Sie mit `apt-get -f install` auflösen. Im folgenden Listing sehen Sie die Installation:

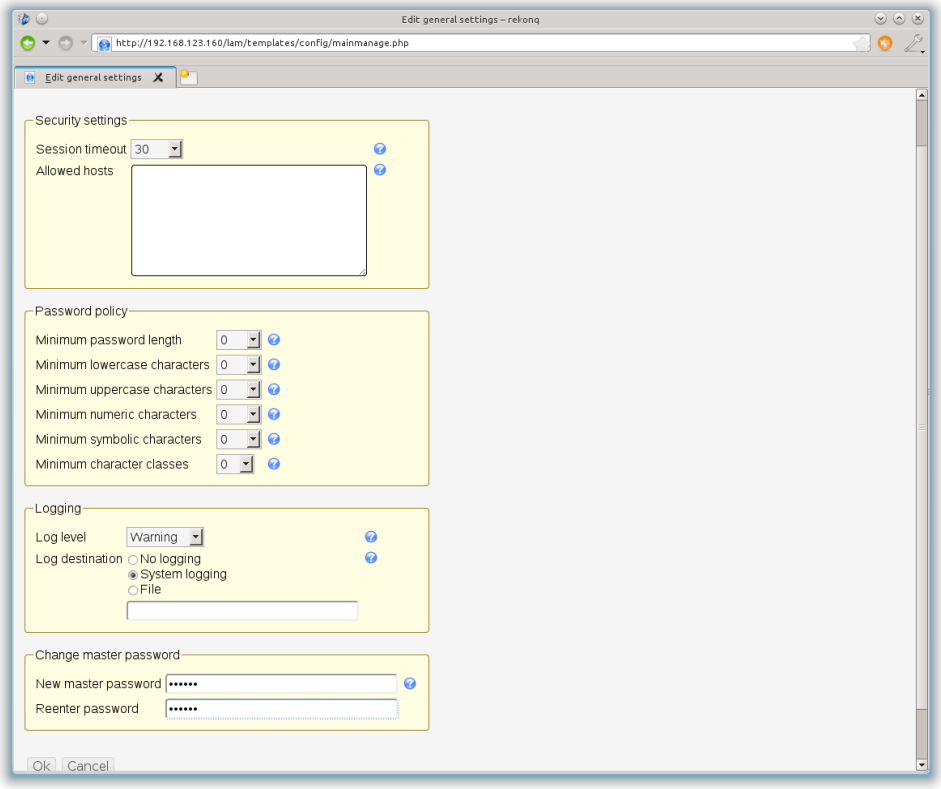
```
 root@lam:~# dpkg -i ldap-account-manager_4.2.TEST-1_all.deb
Vormals nicht ausgewähltes Paket ldap-account-manager wird gewählt.
(Lese Datenbank ... 23518 Dateien und Verzeichnisse sind derzeit installiert.)
Entpacken von ldap-account-manager (aus ldap-account-manager_4.2.TEST-1_all.deb) ...
dpkg: Abhängigkeitsprobleme verhindern Konfiguration von ldap-account-manager:
 ldap-account-manager hängt ab von php5 (>= 5.2.4); aber:
  Paket php5 ist nicht installiert.
 ldap-account-manager hängt ab von php5-ldap; aber:
  Paket php5-ldap ist nicht installiert.
 ldap-account-manager hängt ab von php5-gd; aber:
  Paket php5-gd ist nicht installiert.
 ldap-account-manager hängt ab von apache2 | httpd; aber:
  Paket apache2 ist nicht installiert.
  Paket httpd ist nicht installiert.
 ldap-account-manager hängt ab von php-fpdf (>= 1.7); aber:
  Paket php-fpdf ist nicht installiert.

dpkg: Fehler beim Bearbeiten von ldap-account-manager (--install):
 Abhängigkeitsprobleme - verbleibt unkonfiguriert
Fehler traten auf beim Bearbeiten von:
 ldap-account-manager

 root@lam:~# apt-get -f install
 .
 .
 .
 Trigger für libapache2-mod-php5 werden verarbeitet ...
[ ok ] Reloading web server config: apache2.
ldap-account-manager (4.2.TEST-1) wird eingerichtet ...
[ ok ] Reloading web server config: apache2.

root@lam:~# dpkg -l | grep ldap-account
ii  ldap-account-manager  4.2.TEST-1  all  webfrontend for managing accounts in an\
    LDAP director
```

Nach der Installation der Abhängigkeiten können Sie mit `dpkg -l | grep ldap-account` prüfen, ob der LAM vollständig installiert wurde. Nach der Installation können Sie den LAM jetzt über einen Browser erreichen. Geben Sie dafür in Ihrem Browser die URL:
`http://<ip-des-webservers/lam>` ein. Daraufhin erhalten Sie das folgende Fenster:



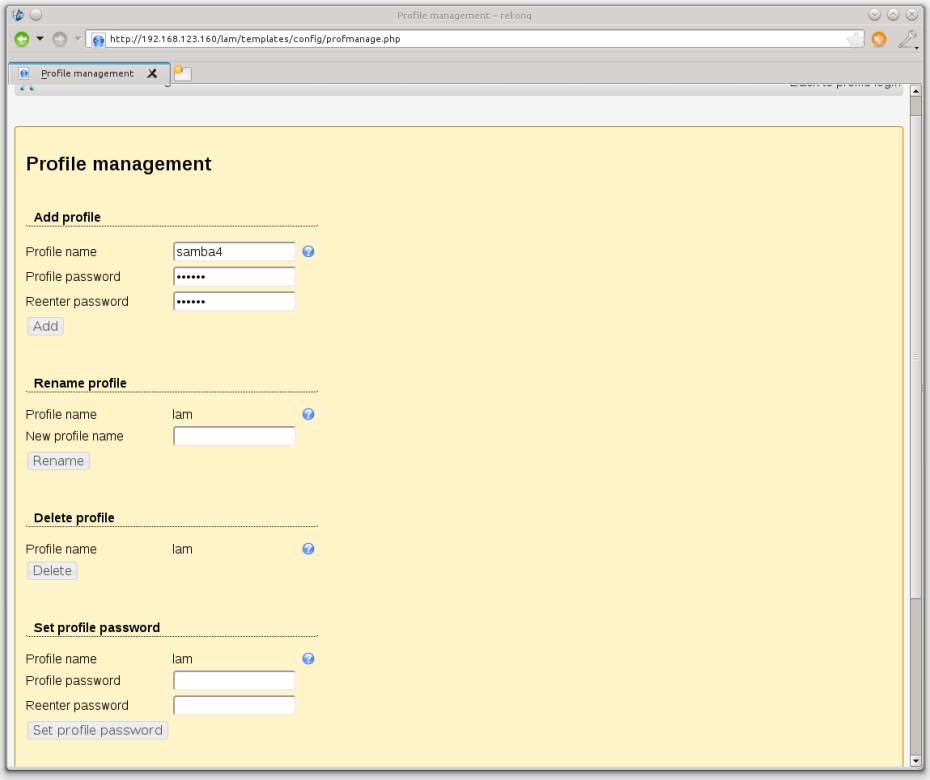
8.2.2 Konfiguration des LAM

Bevor Sie mit dem LAM Ihren Samba administrieren können, müssen Sie den LAM erst konfigurieren. Klicken Sie dazu auf *LAM configuration* in der oberen rechten Ecke des Startbildschirms. Sie erhalten daraufhin eine neue Ansicht. Dort wählen Sie den Punkt *Edit general settings*. Bei der Abfrage nach dem Passwort geben Sie das Standardpasswort `lam` ein und klicken sie auf *OK*.
Auf der folgenden Seite können Sie Einstellungen für den LAM vornehmen. Alle Einstellungen zu den Passwörtern betreffen nur die Anmeldung am LAM und haben nichts mit den Einstellungen der Benutzer zu tun. An dieser Stelle reicht es, wenn Sie erste einmal das Masterpasswort ändern und dann speichern, so wie es die folgende Abbildung zeigt:

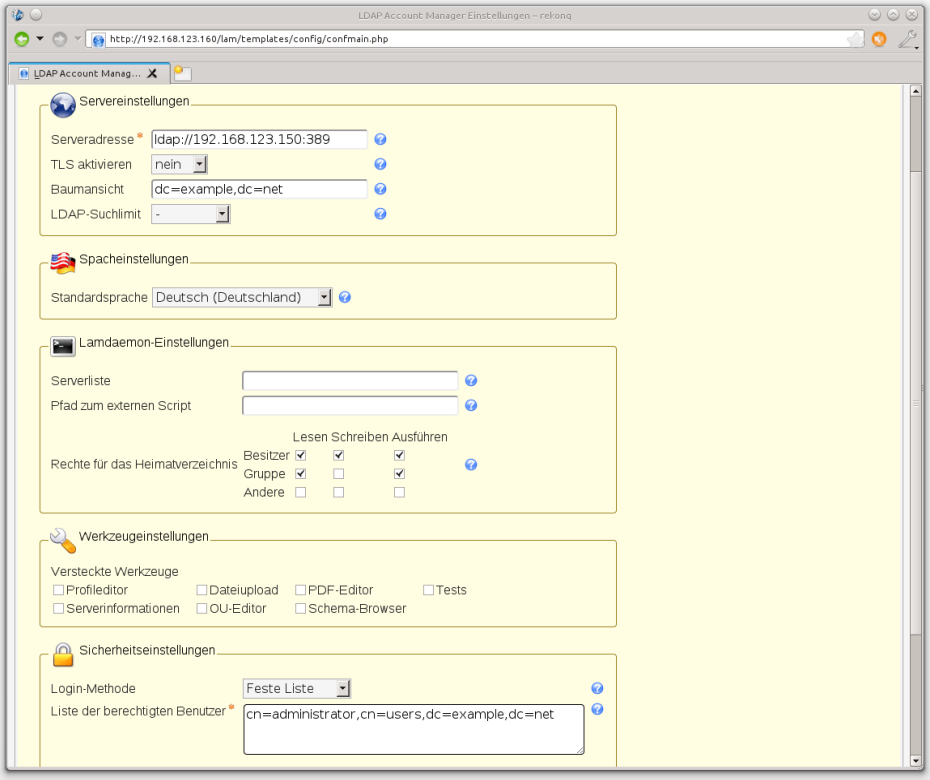


Anschließend landen Sie wieder auf der Anmeldeseite des LAM.

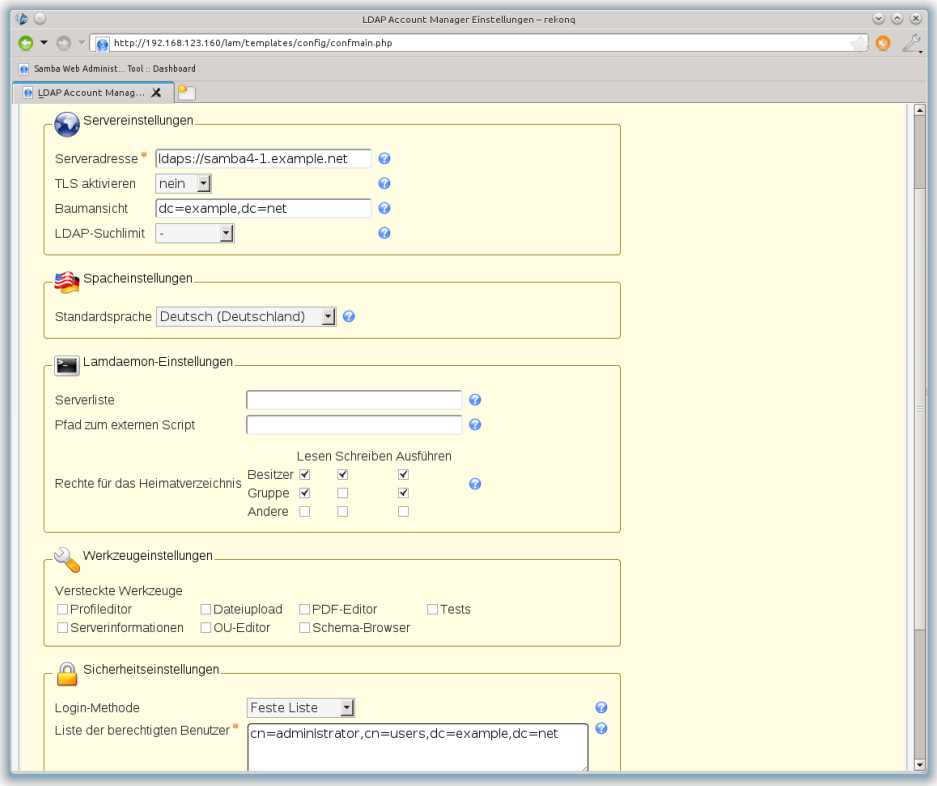
- Im nächsten Schritt müssen Sie ein Profil für Ihren Samba-Server erstellen, damit der LAM die Zugangsdaten für des Samba-Server verfügt. Dazu klicken Sie erneut auf ***LAM configuration*** und anschließend auf ***Edit server profiles***. Um ein neues Profil zu erstellen, klicken Sie hier auf ***Manage server profiles***. Hier legen Sie, so wie in der folgenden Abbildung zu sehen, ein neues Profil für Ihren samba4-Server an und vergeben ein Profilpasswort. Durch anklicken der Schaltfläche ***Add*** fügen Sie ein neues Profil zum LAM hinzu. Um das Profil auch anlegen zu können, werden Sie noch nach dem Masterpasswort gefragt. In der nachfolgenden Abbildung sehen Sie die Einstellungen für das Profil



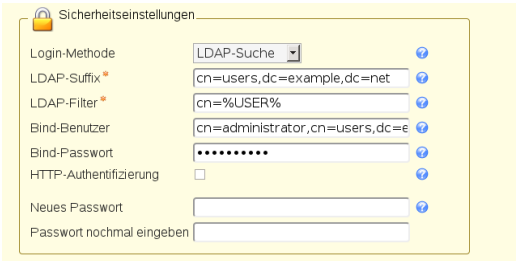
- Erst jetzt kommen Sie zu dem Punkt, an dem Sie Ihre Samba-Daten eingeben müssen. In dem Feld `Servereinstellungen` tragen Sie die Werte für Ihren Samba-Server ein hier in der Unterlage ist es `Serveradresse: ldap://192.168.123.150:389`, `TLS aktivieren = nein`, `Baumansicht = dc=example,dc=net`. Sie können unter der `Sprecheinstellung` noch die Sprache des LAM einstellen. Der Lamdaemon soll zu diesem Zeitpunkt nicht verwendet werden, Sie können diese Einstellung überspringen. Was Sie noch anpassen müssen, ist die `Sicherheitseinstellung` Hier gibt es zwei Möglichkeiten. Entweder Sie legen eine `Feste Liste` der Benutzer an, die sich am LAM anmelden dürfen, oder Sie verwenden die `LDAP-Suche`. In der folgenden Abbildung sehen Sie die Einstellung für die `Feste Liste`.



Wie Sie hier sehen, muss immer der komplette *distinguished Name* des Benutzers angegeben werden. Sie können an dieser Stelle auch mehrere Benutzer eintragen.
In dem folgenden Ausschnitt des Fensters sehen Sie die Einträge für die Einstellung `LDAP-Suche`.



Zu diesem Zeitpunkt müssen Sie als `Bind-Benutzer` auf jeden Fall den *administrator* Ihres System angeben, da sonst noch kein Benutzer vorhanden ist, der den Baum durchsuchen kann. Sie können später eine Benutzer anlegen, der die Rechte für da Durchsuchen hat aber keine administrativen Tätigkeiten durchführen kann. In der folgenden Abbildung sehen die entsprechenden Einstellungen für die `LDAP-Suche`.



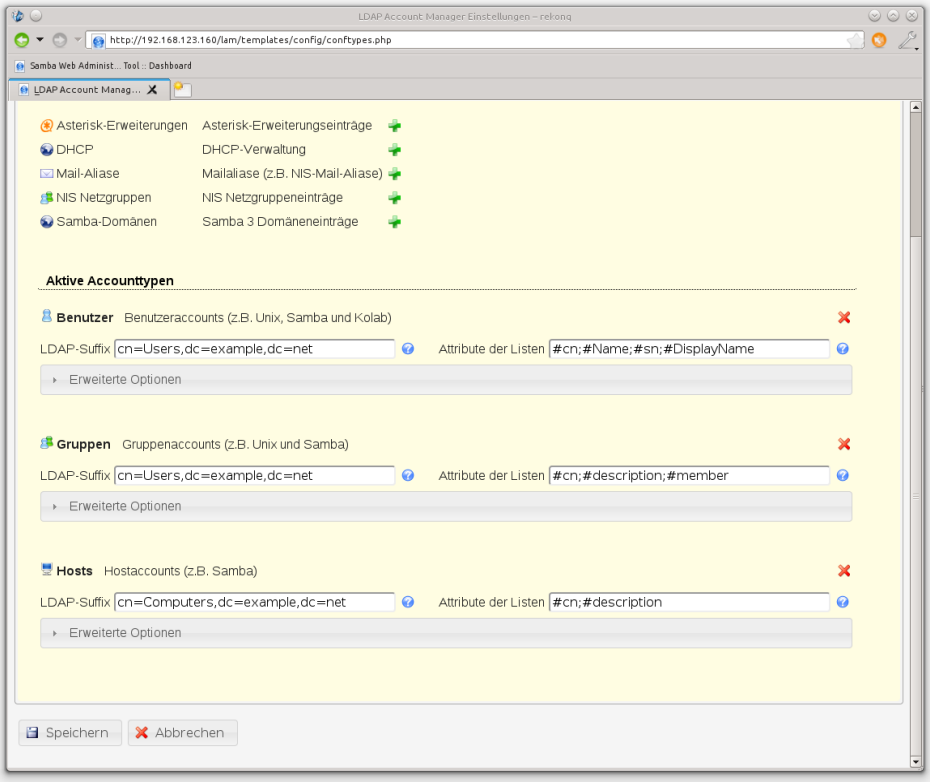
Damit ist der Teil der Konfiguration abgeschlossen.

- Jetzt geht es darum, dass der LAM die Benutzer, Gruppe und Hosts auch im System finden und anzeigen kann. Dazu klicken Sie auf den Karteireiter ***Accounttypen***. Hier müssen Sie jetzt die Werte für die Benutzer, Gruppen und Hosts wie folgt anpassen:

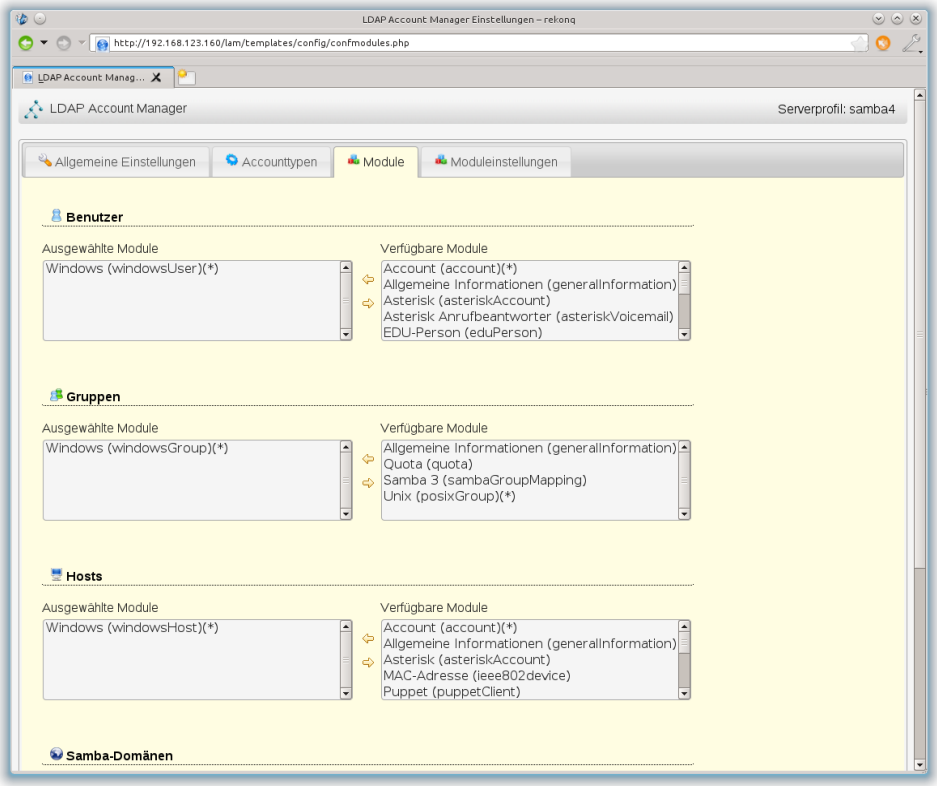
  – Benutzer
  Tragen Sie den LDAP-Suffix `cn=Users,dc=example,dc=net` ein und ersetzen Sie die Liste der Attribute durch die Werte `#cn;#Name;#sn;#DisplayName`

– Gruppen
  Auch hier tragen Sie den LDAP-Suffix `cn=Users,dc=example,dc=net` ein und ersetzen Sie die Liste der Attribute durch die Werte `#cn;#description;#member`
– Hosts
  Für die Hosts in Ihrer Domäne tragen die den LDAP-Suffix `cn=Computers,dc=example,dc=net` ein und ersetzen Sie die Liste der Attribute durch die Werte `#cn;#description`
– Samba-Domänen
  Dieser Accounttyp wird bei samba4 nicht mehr benötigt, Sie können diesen Typ entfernen.

Wenn Sie diese Einstellungen nicht korrekt durchführen, kann der LAM später Ihre Objekte nicht finden oder nicht richtig anzeigen. In der folgenden Abbildung sehen Sie eine Übersicht über die Einstellungen.

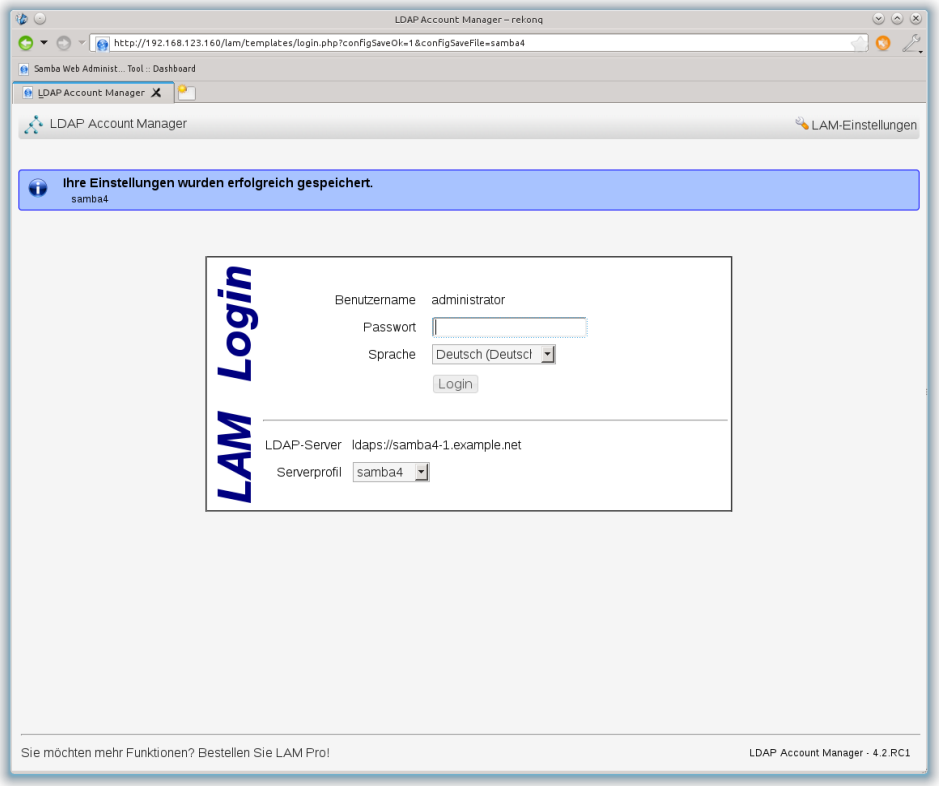


- Jetzt müssen Sie noch eine Anpassung der Module vornehmen, dazu klicken Sie auf den Karteireiter ***Module***. Auch hier finden Sie wieder die Unterteilung in Benutzer, Gruppen und Hosts.
  Da Samba4-Objektklassen jetzt vom Type *structural* sind, müssen Sie die derzeit eingetragen Objektklassen für alle drei Bereiche anpassen. Passen Sie Ihre Einstellung so an, wie Sie es in der folgenden Abbildung sehen.



Damit haben Sie jetzt die Konfiguration der Module abgeschlossen.

An dieser Stelle können Sie jetzt noch optional die Werte für einige Module anpassen. Das ist aber für die Funktion des LAM nicht zwingend erforderlich. Wenn Sie jetzt auf den Schaltfläche *Speichern* klicken, werden Ihre Einstellungen gespeichert und Sie gelangen zurück auf die Startseite des LAM. Achte Sie darauf, dass Sie die Meldung bekommen `Ihre Einstellung wurden erfolgreich gespeichert.` So wie Sie es in der folgenden Abbildung sehen.



Damit ist die Konfiguration des LAM abgeschlossen und Sie können sich am LAM mit dem *administrator* anmelden. Damit Sie vom LAM über `ldaps` auf den samba4-Server zugreifen können, müssen Sie die Datei /etc/ldap/ldap.conf noch anpassen. Der samba4 verwendet für `ldaps` self-signed-certificates, aus dem Grund kann die Echtheit des Zertifikates nicht geprüft werden. Wie Sie die Prüfung deaktivieren, sehen Sie im folgenden Listing:

```
BASE    dec=example,dc=net
URI     ldaps://samba4-1.example.net

TLS_REQCERT never
```

Diese Zeilen müssen Sie in die Datei /etc/ldap/ldap.conf eintragen, dann können Sie über `ldaps` auf den Server zugreifen.

8.2.3 Verwaltung von Gruppen mit dem LAM

Nach einem Klick auf den Karteireiter ***Gruppen*** gelangen Sie in die Gruppenübersicht. Hier sehen alle Gruppen, die Beschreibung und die Mitglied mit ihrem vollständigen *dn*. Um eine neue Gruppe anzulegen, klicken Sie auf ***Neue Gruppe***. In dem darauf folgenden Fenster können Sie die Einstellung der Gruppe vornehmen. Vergeben Sie als erstes einen Namen für die Gruppe, der Name der Gruppe ist das einzige Attribut, dass Sie zwingend angeben müssen. Weiter unten finden Sie dann noch die `Group scope`-Einstellung und `Gruppentyp`-Einstellung. Die drei Scopes und Typen, finden Sie auch in einem Microsoft-AD. Bei den Scopes haben Sie die Auswahl zwischen den folgenden drei Scopes:

- Domain local
  Eine Gruppe des Scope `Domain local` dient zur Vergabe von Rechten im Dateisystem. Hier sollten Sie keine Benutzer eintragen, sondern nur Gruppen der Art `Global`.
- Global
  Die Gruppen des Scopes `Global` diene zur Gruppierung von Benutzern. Diese Gruppen können Sie dann einer `Domain local`-Gruppe zuweisen. Dadurch erhalten alle Mitglieder der Gruppe die Rechte im Dateisystem.
- Universal
  Die Gruppen-Scopes `Universal` dient hauptsächlich für domänenübergreifende Zugriffe.

Hinweis !

Mehr zu den Gruppen-Scopes finden Sie unter der URL: `http://technet.microsoft.com/en-us/library/cc755692%28v=ws.10%29.aspx`

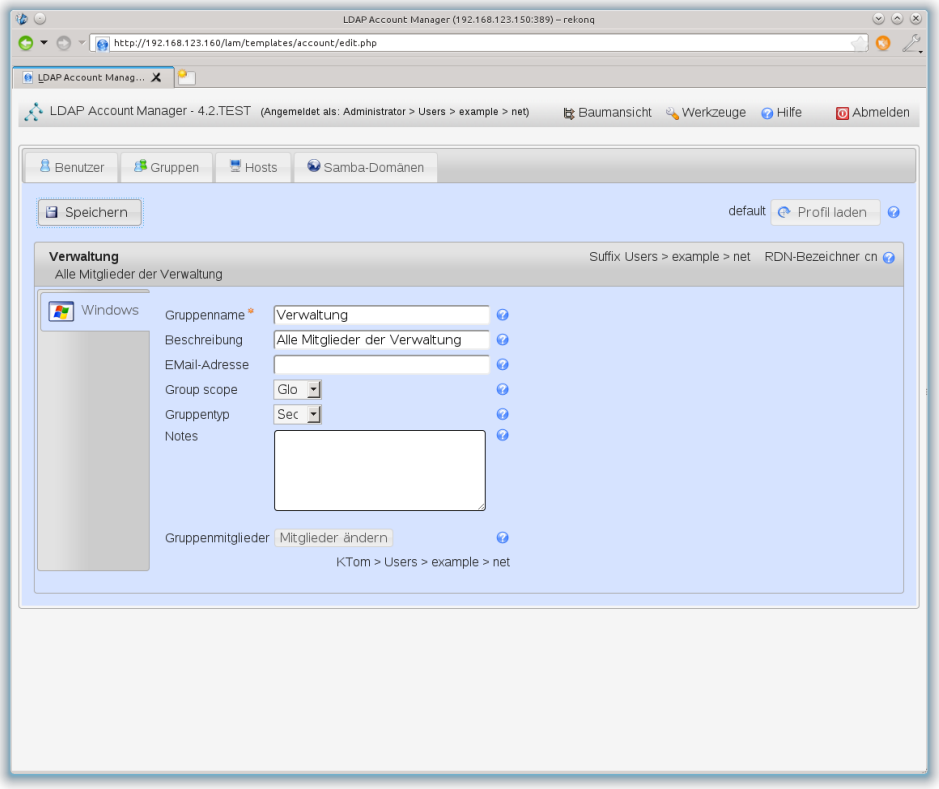
Bei den `Gruppentypen` haben Sie die Auswahl zwischen den folgenden beiden Typen:

- Security
  `Security`-Gruppen um den Zugriff auf Ressourcen, wie zum Beispiel im Dateisystem, zu gewähren.
- Distribution
  Die Gruppe vom Typ `Distribution` dient nur für E-Mailsystem wie *Exchange*.

Hinweis !

Mehr zu den Gruppentypen finden Sie unter der URL: `http://technet.microsoft.com/en-us/library/cc781446%28v=ws.10%29.aspx`

In der folgenden Abbildung sehen Sie ein Beispiel für eine Gruppe vom Scope `Global` und dem Typ `Security`:



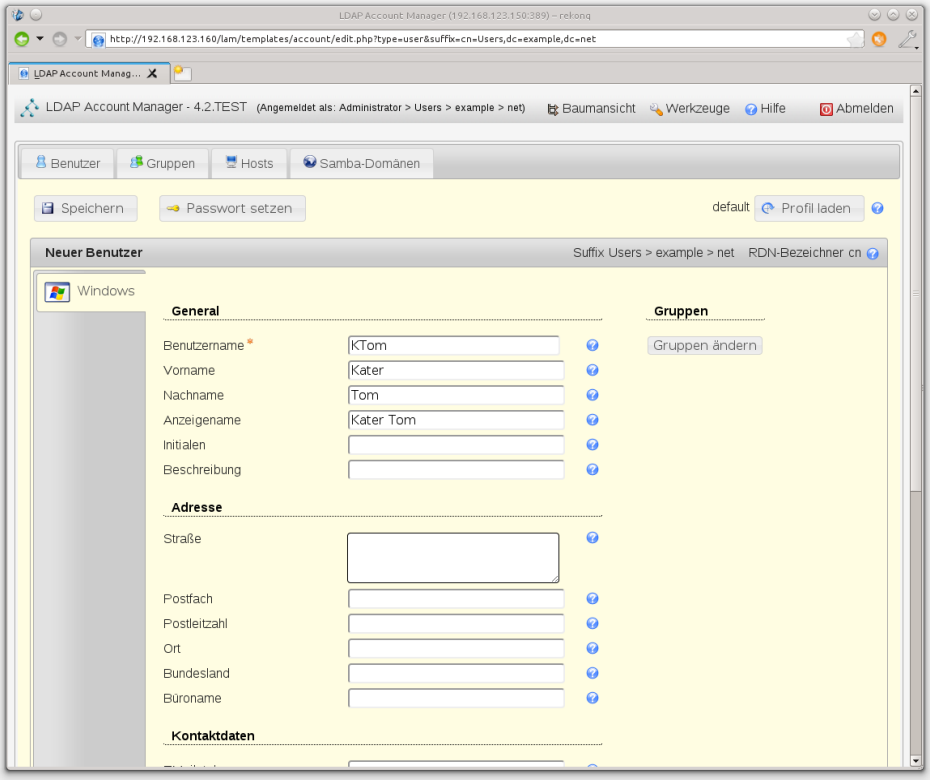
Hier sehen Sie auch, dass der neuen Gruppe gleich der zuvor erstellte Benutzer als Mitglied zugewiesen wurde. Nach dem Speicher und der Rückkehr auf die Übersichtsseite der Gruppen finden Sie dort Ihre neue Gruppe mit allen Informationen.
Wie schon zuvor bei den Benutzern können Sie über den LAM auch die bestehenden Gruppen editieren und löschen. Klicken Sie hierzu auf das entsprechende Symbol vor dem Gruppennamen.

Hinweis !

Im Moment lassen sich die Posixgruppen, wie Sie sie vielleicht vom openLDAP her kennen, noch nicht mit dem LAM verwalten, da die Objektklasse der *posixGroup* jetzt eine Auxiliary Objektklasse ist. Für etwaige Linux-Clients in Ihrem Netz gibt es aber später eine andere Lösung, damit sich die Benutzer auch am Linux-Client anmelden können. Im Abschnitt 16 wird auf diese Problematik näher eingegangen.

8.2.4 Verwaltung von Benutzern mit dem LAM

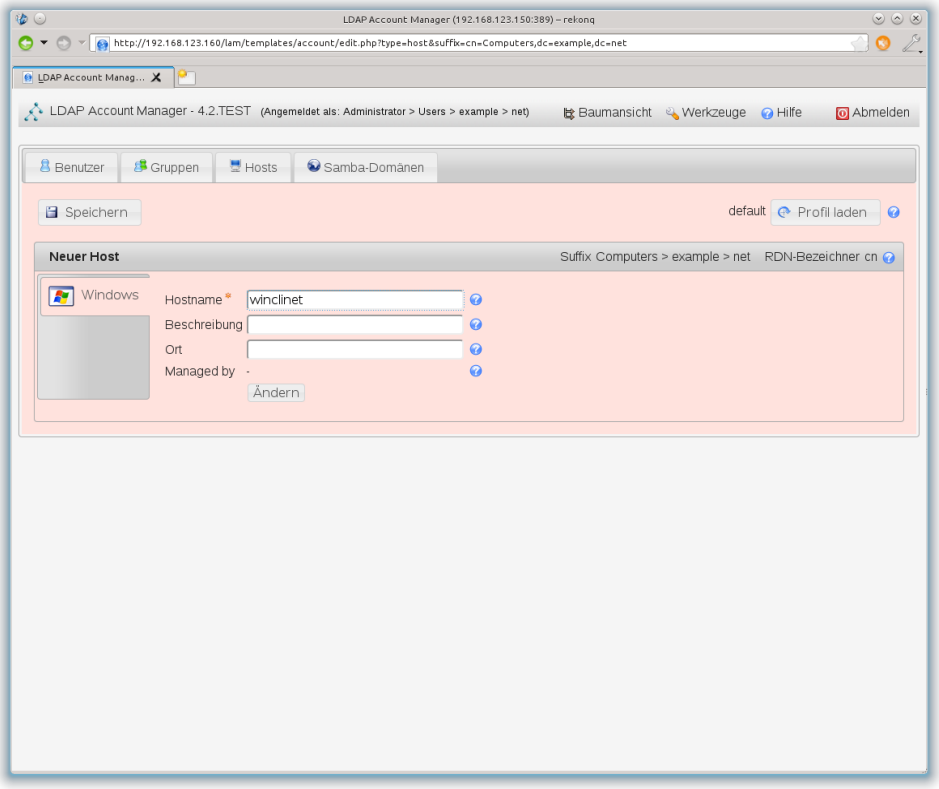
Nach der ersten Anmeldung sehen Sie ein Liste aller Benutzer im System, inklusive der Systembenutzer. Auch die Gruppen und Hosts können Sie sich hier anzeigen lassen.
Um jetzt einen Benutzer anzulegen, klicken Sie erst auf den Karteireiter ***Benutzer*** und dann auf die Schaltfläche ***Neuer Benutzer***. In der Maske die dann erscheint, müssen Sie mindestens einen Benutzername vergeben, alle anderen Attribute sind optional. Über die Schaltfläche ***Passwort setzen*** können Sie sofort das Passwort für den neuen Benutzer vergeben, denken Sie auch hier wieder an die Komplexitätsregel für Passwörter. In der folgenden Abbildung sehen Sie ein Beispiel für einen neuen Benutzer.



Wenn Sie alle Felder gefüllt haben, klicken Sie auf die Schaltfläche ***Speichern*** um den Benutzer anzulegen. Auf der Übersichtsseite der Benutzer sehen Sie jetzt Ihren neuen Benutzer. Einen bestehenden Benutzer können Sie über einen Klick auf das Symbol mit dem Bleistift editieren oder durch einen Klick auf das Symbol mit dem roten Kreuz löschen.

8.2.5 Verwaltung der Hosts mit dem LAM

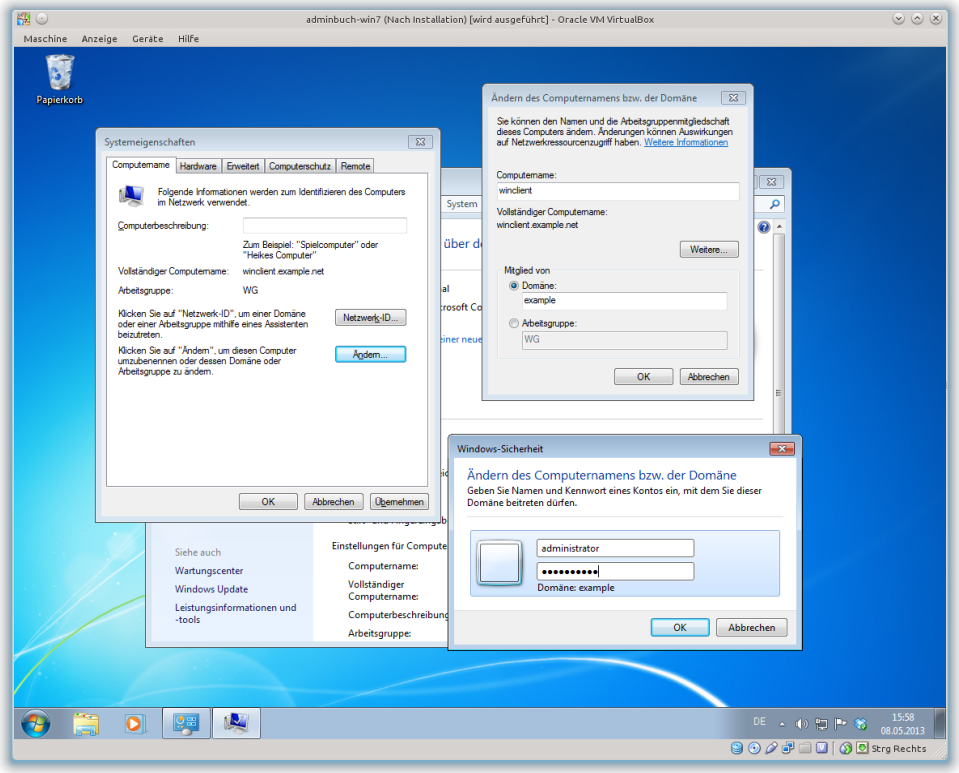
Wenn Sie Host-Konten vor dem Beitritt eines Clients zur Domäne erstellen wollen, geht das natürlich auch mit dem LAM. Klicken Sie hierfür einfach auf den Karteireiter ***Hosts***. Anschließend klicken Sie auf ***Neuer Host***. Hier müssen Sie nur den Namen für den Host angeben. Der Name muss hier dem *NetBIOS-Name* des Hosts entsprechen. Dann müssen Sie das nur noch auf ***Speichern*** klicken und der neu Host erscheint in der Übersicht der Hosts. In der folgenden Abbildung sehen Sie Das Fenster des LAM beim erstellen eines neuen Hosts.



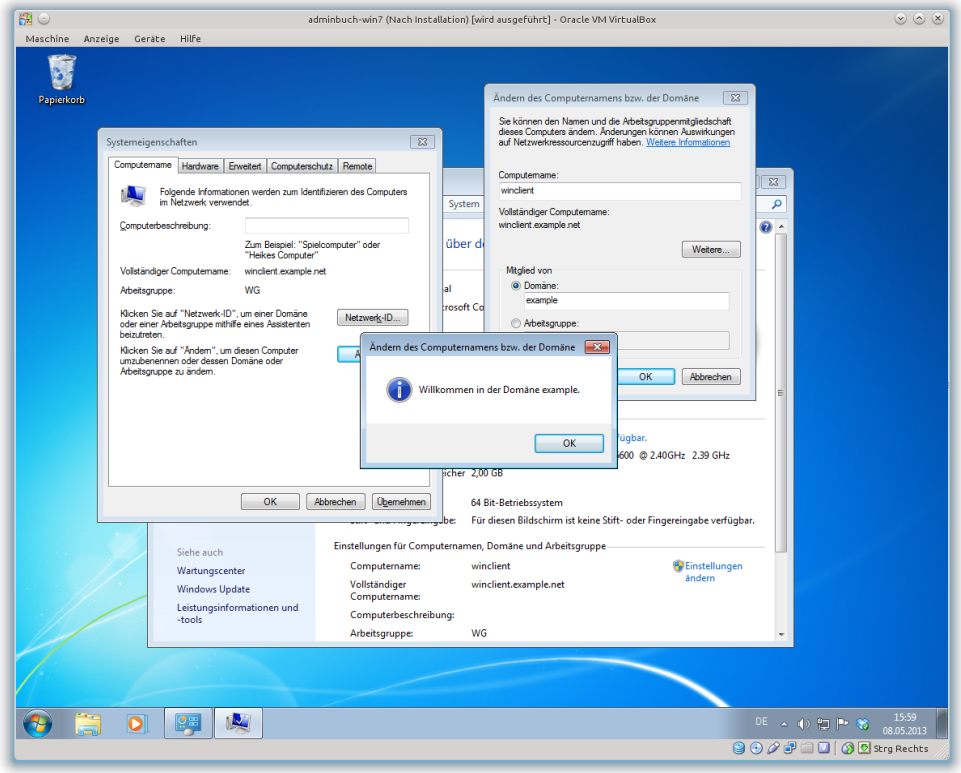
In Zukunft können Sie neue Hosts direkt im LAM anlegen.
Jetzt haben Sie mit dem LAM ein webbasiertes Werkzeug an der Hand, mit dem Sie auch mehr als nur die Grundeinstellung von Objekten vornehmen können.

8.3 Benutzer- und Gruppenverwaltung mit den *Windows Remote Server Administration Tools(RSAT)*

Um Benutzer und Gruppen über die *Windows Remote Server Administration Tools(RSAT)* verwalten zu können, müssen Sie mindestens einen Client mit Windows 7 Professionell in Ihrer Domäne haben. Aus diesem Grund nehmen Sie jetzt erst den zuvor erstellten Host in die Domäne auf. Melden Sie sich hierfür als lokaler Administrator an Ihrer Windows 7 Workstation klicken Sie anschließend auf *`Start`* und klicken dann mit der rechten Maustaste auf *`Computer -> Eigenschaften`*. Dort finden Sie die Schaltfläche *`Einstellungen Ändern`*. Durch einen Klick auf die Schaltfläche öffnet sich ein neues Fenster. In diesem Fenster können Sie jetzt den *NetBIOS-Name* und die Domänenzugehörigkeit ändern. Achten Sie darauf, dass bei `Vollständiger Computername:` der *fqdn* des Clients eingetragen ist. Zum Beitritt der Samba4-Domäne klicken Sie auf die Schaltfläche *`Ändern...`*. In dem neuen Fenster wählen Sie den Punkt *`Domäne:`* aus und geben den Domänennamen an. Hier wird der *NetBIOS-Name* der Domäne verlangt. In dieser Unterlage lautet der `example`. Klicken Sie anschließend auf die Schaltfläche *`OK`*. Es erscheint ein Fenster, in dem Sie den Benutzername, in diesem Fall `administrator`, und dessen Passwort eingeben müssen. In der folgenden Abbildung sehen Sie alle Fenster für den Vorgang:



Nach einem Klick auf die Schaltfläche *OK* dauert es eine Weile und Sie erhalten die Meldung `Willkommen in der Domäne example`, so wie Sie es in der folgenden Abbildung sehen:

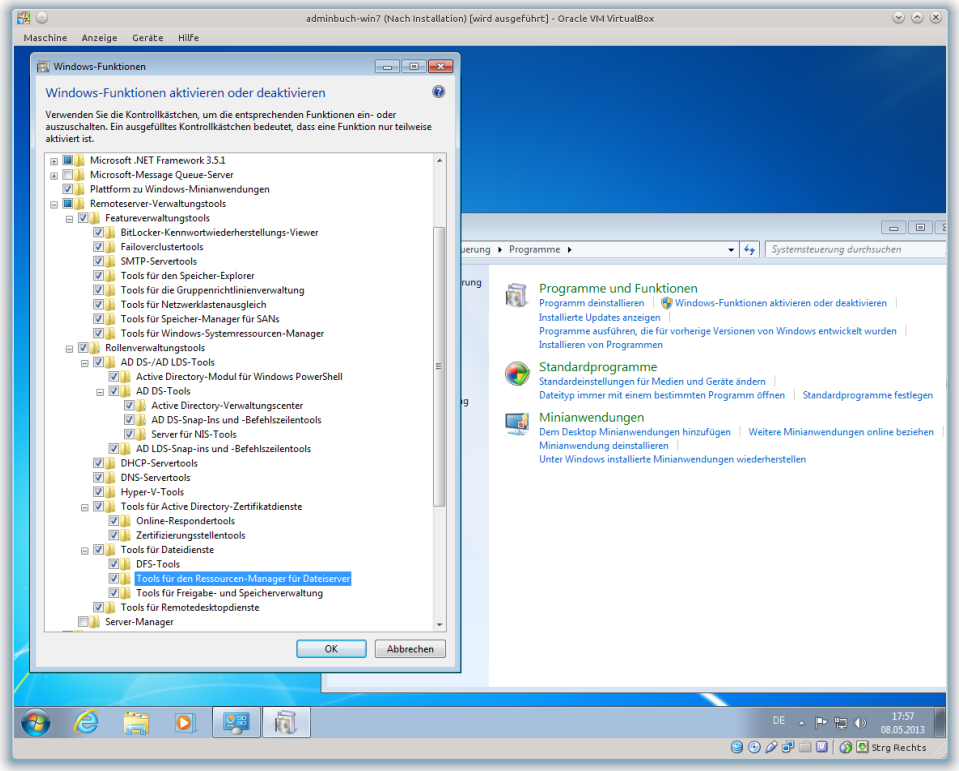


Um die Einstellung wirksam werden zu lassen, müssen Sie Windows Neustarten. Nach dem Neustart können Sie sich jetzt als *Domänenadministrator* anmelden, so wie in der folgenden Abbildung zu sehen:

Hinweis !

Im Abschnitt 16 wird auf die Verwaltung von Clients in der Domäne noch genauer eingegangen.

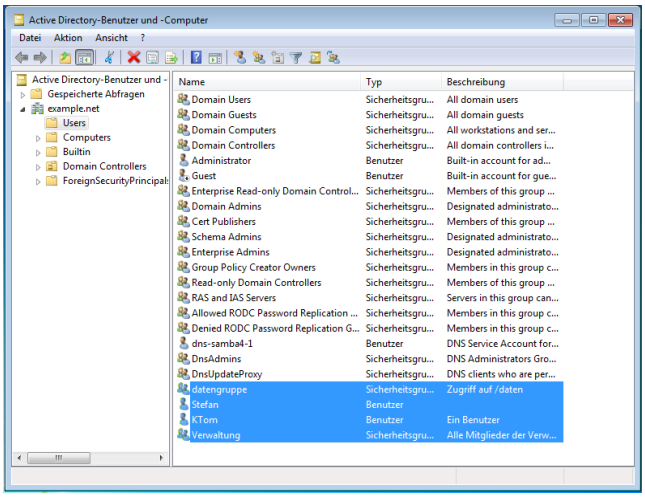
Nach der Anmeldung als Domänenadministrator laden Sie die RSAT von der URL: `http://www.microsoft.com/de-de/download/details.aspx?id=7887` herunter und installieren diese.
Nach der Installation können Sie die RSATs nicht sofort nutzen, Sie müssen diese erst aktivieren. Öffnen Sie hierfür die Systemsteuerung und klicken dann auf *Programme und Funktionen*, dort klicken Sie dann auf *Windows-Funktionen aktivieren oder deaktivieren* es öffnet sich ein neues Fenster in dem Sie jetzt die RSATs über den Unterpunkt *Remoteserver-Verwaltungstools* aktivieren. Sie müssen alle Unterpunkte öffnen und dann alle gewünschten Funktionen separat aktivieren. So wie Sie das in der folgenden Abbildung sehen:



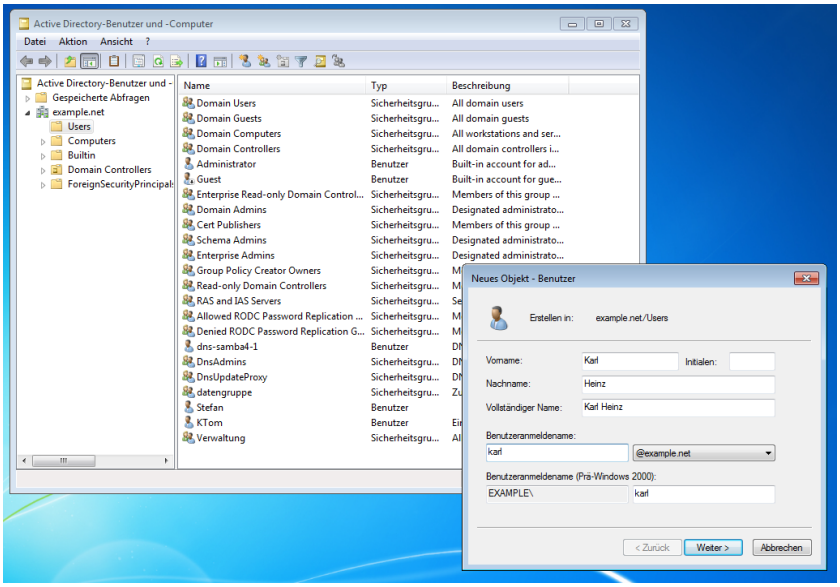
Anschließend klicken Sie auf *OK*. Jetzt werden Die RSAT im System aktiviert. Jetzt können Sie über *Start -> Alle Programme -> Verwaltung* auf die RSAT zugreifen.

8.3.1 Benutzer- und Gruppenverwaltung mit den RSAT

Wenn Sie jetzt das Tool *Active Directory-Benutzer und -Computer* starten, können Sie die von Ihnen erstellte Domäne sehen, und Benutzer und Gruppen verwalten. Eine Übersicht über alle Gruppen sehen Sie in der folgenden Abbildung:



Die vorher über die Kommandozeile und den LAM erzeugten Benutzer und Gruppen sehen Sie im unteren Teil der Abbildung markiert. Wenn Sie einen neuen Benutzer, eine neue Gruppe oder einen neuen Host anlegen wollen, führen Sie eine Rechtsklick auf die rechte Seite des Fensters aus. Dann öffnet sich ein Kontextmenü, dort klicken Sie auf `Neu`, es öffnet sich ein neues Menü in dem Sie dann das entsprechenden Objekt auswählen können. In der folgenden Abbildung sehen Sie als Beispiel das Anlegen eines neuen Benutzers:



8.3.2 Aufgaben

- Installieren Sie die *Remote Server Administration Tools* und aktivieren Sie alle Module.
- Legen Sie mindestens drei neue Gruppen an
- Legen Sie mindestens drei neue Benutzer an und weisen diese je einer Ihrer neuen Gruppen zu

9 Verwaltung von Freigaben

Nachdem Sie jetzt ein System haben, in dem Sie Benutzer, Gruppen und Hosts verwalten und in die Domäne aufnehmen können, soll es in diesem Abschnitt um die Verwaltung der Freigaben gehen. Die Funktion des Fileservers wurde weitestgehend aus dem Samba3 übernommen, somit können Sie alle Parameter die Sie vom Samba3 her kennen auch weiterhin in der Freigaben Ihres samba4-Servers verwenden.
Wenn Sie samba4 mit sehr vielen Clients in Ihrem Netzwerk einsetzen, sollten Sie die Freigaben nicht mehr in der Datei smb.conf verwalten, sondern in der *Registry* des samba4. Die Verwaltung der Freigaben in der Registry hat den Vorteil, dass nicht mehr jeder smbd-Prozess im System die Datei neu lesen muss, wenn Sie eine neue Freigabe erstellt haben. Denn bei jeder Änderung der smb.conf muss jeder smbd-Prozess die Datei neue lesen. Da für jeden angemeldeten Benutzer in der Domäne je ein smbd-Prozess gestartet wird, kann die Auslastung des Systems dann sehr hoch werden. Hier sollen beide Wege der Erstellung von Freigaben aufgezeigt werden.

9.1 Verwaltung von Freigaben in der Datei smb.conf

Als erstes sehen Sie hier Beispielen für Freigaben in der smb.conf:

```
[gemeinsam]
   comment = Daten der Verwaltung
   path = /daten/gemeinsam
   browsable = yes
   valid users = @alle
   admin users = @Abteilungsleiter
   read only = no
   force create mode = 0770
   force directory mode = 0770
   inherit permissions = yes
   inherit owner = yes
   hosts allow = 192.168.123.0/255.255.255.0
```

Im ersten Beispiel sehen Sie, wie Sie ein Verzeichnis freigeben können auf das die Mitglieder der Gruppe *alle* Zugriff haben sollen. Alle Mitglieder der Gruppe *Abteilungsleiter* sollen administrativen Zugriff auf die Freigabe erhalten.

```
[IT-Abteilung]
   comment = Verzeichnis für di IT-Abteilung
   path = /daten/it
   copy = gemeinsam
   force group = it
   hosts allow = 192.168.122.0/255.255.255.0
```

Bei dieser Freigabe werden die Informationen die nicht direkt in der Freigabe `IT-Abteilung` gesetzt werden aus der Freigabe `gemeinsam` kopiert.

```
[Abteilungen]
   comment = Abteilungsverzeichnisse
   path = /daten/abteilung
   browsable = yes
   hide unreadable = yes
   admin users = @abteilungsleiter
   read only = no
```

```
force create mode = 0770
force directory mode = 0770
inherit permissions = yes
inherit owner = yes
```

Hinweis !

Die beiden Parameter `security mask` und `directory security mask` werden bei samba4 nicht mehr unterstützt, da die Verwaltung der Berechtigungen jetzt im AD liegt

Um Freigabe zusammenfassen zu können, wird bei dieser Freigabe der Parameter `hide unreadable = yes` gesetzt. Wenn Sie dann die Rechte auf den untergeordneten Verzeichnissen für die entsprechenden Abteilungen richtig setzen, können die Mitarbeiter der einzelnen Abteilungen nur ihr eigenes Abteilungsverzeichnisse sehen. So können Sie mit einer Freigabe viele Verzeichnisse individuell bereitstellen. Im weiteren Verlauf der Unterlage wird dieser Vorgang noch genauer erklärt.

9.2 Verwaltung von Freigaben in der *Registry*

Wie schon in der Einleitung dieses Abschnittes beschrieben, haben Sie die Möglichkeit Freigaben über die Registry des samba4 einzurichten. Die Freigaben, die Sie über die Registry verwalten, werden in einer tdb-Datenbank abgelegt und verwaltet. Da ein Client beim Zugriff auf einen Server auch immer auf dessen Registry zugreifen, werden auch immer die Freigaben gelesen. Der Zugriff auf eine Datenbank ist schneller als auf die Datei smb.conf. Auch können sie so Freigaben über eine Netzwerkverbindung einrichten, ohne die Datei smb.conf zu editieren.
Für die Verwaltung der Freigaben in der *Registry* verwenden Sie das Kommando `samba-tool net <rpc> registry`. Ohne den Parameter `rpc` greifen Sie local auf die Registry zu. Mit dem Parameter `rpc` können Sie Freigaben über das Netzwerk verwalten. Dabei müssen Sie sich aber beim Server über den Parameter `-U administrator` authentifizieren.
Als erstes soll ein Blick auf die *Registry* geworfen werden. Dafür wird das Werkzeug `tdbtool` verwendet.

```
root@samba4-1:~# tdbtool  /var/lib/samba/registry.tdb keys
key 50 bytes: HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION
key 67 bytes: SAMBA_REGVAL\HKLM\SYSTEM\CURRENTCONTROLSET\SERVICES\REMOTEREGISTRY
key 76 bytes: SAMBA_REGVAL\HKLM\SYSTEM\CURRENTCONTROLSET\SERVICES\REMOTEREGISTRY\SECURITY
key 47 bytes: HKCU\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION
.
.
.
key 60 bytes: SAMBA_REGVAL\HKLM\SYSTEM\CURRENTCONTROLSET\SERVICES\SPOOLER
key 69 bytes: SAMBA_REGVAL\HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\PORTS
```

In dem Beispiel wurden über den Parameter `keys` alle Registryschlüssel der Datenbank angezeigt. Wenn Sie an der Stelle den Parameter `dump` verwenden, wird Ihnen auch der Inhalt der einzelnen Schlüssel angezeigt. Mit dem `tdbtool` können Sie die gesamte Registry auslesen, verwalten, prüfen und löschen. Weiter Informationen finden Sie in der Man-page zum Kommando `tdbtool`.
Für die Verwaltung der Freigaben ist aber nur ein ganz bestimmter Bereich der Registry wichtig. Im nachfolgenden Listing sehen Sie den Zugriff auf dem Bereich:

```
root@samba4-1:~# net registry enumerate HKLM\\software\\samba
Keyname   = smbconf
Modtime   = Do, 01 Jan 1970 01:00:00 CET

Keyname   = Group Policy
Modtime   = Do, 01 Jan 1970 01:00:00 CET
```

Hier wird der Bereich *HKEY_LOCAL_MACHINE (HKLM)* abgefragt, da sich dort die Freigaben befinden. Wie Sie sehen können, werden unter samba4 dort zwei Bereiche verwaltet. Zum einen alles was mit der Konfiguration des samba4 zu tun hat und zum anderen die Gruppenrichtlinien. Das Thema Gruppenrichtlinien finden Sie im Abschnitt 14.
Wollen Sie die selben Informationen über eine Netzwerkverbindung erhalten, müssen Sie, so wie im folgenden Listing, den Parameter `rpc` verwenden:

```
root@samba4-1:~# net rpc registry enumerate HKLM\\software\\samba -Uadministrator\
  -I 192.168.123.170
Enter administrator's password:
Keyname   = smbconf
Modtime   = Do, 01 Jan 1970 01:00:00 CET

Keyname   = Group Policy
Modtime   = Do, 01 Jan 1970 01:00:00 CET
```

Mit dem Parameter `-U` übergeben Sie einen Benutzername. Der Benutzer muss im AD bereits vorhanden sein. Über den Parameter `-I` geben Sie die IP-Adresse des Servers an, auf den Sie zugreifen wollen. Sie können anstelle von `-I 192.168.123.170` auch den Parameter `-S samba4-1.example.net` verwenden.
Eine weitere Möglichkeit die Informationen aus dem Bereich der Registry auszulesen, ist der Parameter `export`. Dieser Parameter kann auch später dazu verwendet werden den Teil der Registry in eine Datei zu sichern und mit dem Parameter `import` wieder zurück zu spielen. Im folgenden Listing sehen Sie auch hierfür ein Beispiel:

```
root@samba4-1:~# net registry export hklm\\software\\samba /dev/stdout
Windows Registry Editor Version 5.00

[hklm\software\samba]

[hklm\software\samba\smbconf]

[hklm\software\samba\Group Policy]
;Local Variables:
;coding: UTF-8
;End:
```

Wenn Sie an Stelle von `/dev/stdout` eine Datei angeben, werden die Daten in die Datei geschrieben und können später dann wieder importiert werden.

9.2.1 Erstellen einer Freigabe in der Registry

Jetzt soll die erste Freigabe erstellt werden. Wenn Sie eine Freigabe in der Registry erstellen, haben Sie erst einmal nur die Möglichkeit die Optionen `writable`, `guest_ok` und einen Kommentar zur Freigabe hinzuzufügen. Alle weiteren Parameter lassen sich erst nachträglich eintragen.

```
root@samba4-1:~# net conf addshare reg-freigabe /daten/reg-freigabe writeable=y \
  guest_ok=n "Eine Freigabe in der Registry"
```

Mit `net conf` verwalten Sie die Konfigurationseinträge der Registry, in diesem Fall soll zur Konfiguration eine Freigabe `addshare` hinzugefügt werden. Danach folgen, der Name der Freigabe, der Pfad zur Freigabe, ob auf die Freigabe geschrieben werden darf, ob ein Gastzugriff erlaubt ist und ein Kommentar.

Hinweis !

Wenn Sie einen Kommentar hinzufügen wollen, müssen Sie alle vorherigen Parameter auch setzen, auch wenn Sie zum Beispiel für `guest_ok` den Standardwert setzen wollen.

Anschließend können Sie sich die Freigabe, wie im folgenden Listing zu sehen, wieder anzeigen lassen:

```
root@samba4-1:~# net registry export hklm\\software\\samba /dev/stdout
Windows Registry Editor Version 5.00

[hklm\software\samba]

[hklm\software\samba\smbconf]

[hklm\software\samba\smbconf\reg-freigabe]
"path"="/daten/reg-freigabe"
"comment"="Eine Freigabe in der Registry"
"guest ok"="no"
"read only"="no"

[hklm\software\samba\Group Policy]
;Local Variables:
;coding: UTF-8
;End:
```

Selbstverständlich können Sie sich, wie auch unter Windows, die einzelnen Schlüssel und ihre Werte auflisten lassen. Im nächsten Listing sehen Sie auch hierfür ein Beispiel:

```
root@samba4-1:~# net rpc registry enumerate HKLM\\software\\samba\\smbconf\\reg-freigabe\
  -Uadministrator -S samba4-1.example.net
Enter administrator's password:
Valuename  = path
Type       = REG_SZ
Value      = "/daten/reg-freigabe"

Valuename  = comment
Type       = REG_SZ
Value      = "Eine Freigabe in der Registry"

Valuename  = guest ok
Type       = REG_SZ
Value      = "no"

Valuename  = read only
Type       = REG_SZ
Value      = "no"
```

9.2.2 Zugriff auf eine Freigabe aus der Registry

Wenn Sie sich jetzt mit `smbclient -L localhost -Uadministrator` die Freigaben auflisten lassen, werden Sie feststellen, dass die neue Freigabe noch nicht sichtbar ist. Um die Freigaben auch nutzen zu können, müssen Sie die Datei smb.conf in der `[global]`-Section um den Parameter `registry shares = yes` erweitern. Sie müssen den Samba-Dienst nach der Änderung der Datei smb.conf nicht neu starten. Wie Sie im folgenden Listing sehen, wird die neue Freigabe jetzt auch auch angezeigt:

```
root@samba4-1:~# smbclient -L localhost -Uadministrator
Enter administrator's password:
Domain=[EXAMPLE] OS=[Unix] Server=[Samba 4.0.5-SerNet-Debian-1.wheezy]

        Sharename       Type      Comment
        ---------       ----      -------
        gemeinsam       Disk      Daten der Verwaltung
        sysvol          Disk
        netlogon        Disk
        IT-Abteilung    Disk      Verzeichnis für di IT-Abteilung
        Abteilungen     Disk      Abteilungsverzeichnisse
        IPC$            IPC       IPC Service (Samba 4.0.5-SerNet-Debian-1.wheezy)
        reg-freigabe    Disk      Eine Freigabe in der Registry
Domain=[EXAMPLE] OS=[Unix] Server=[Samba 4.0.5-SerNet-Debian-1.wheezy]

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
```

9.2.3 Erweitern einer Freigabe in der Registry

Nach dem Sie eine Freigabe in der Registry erzeugt haben, soll es jetzt darum gehen, die Freigabe um weitere Parameter zu erweitern. Die zusätzlichen Parameter setzen Sie mit `net config setparm`. Im folgenden Listing soll die zuvor erstellte Freigabe um den Parameter `valid users = @domain user` und `hide unreadable = yes` ergänzt werden:

```
root@samba4-1:~# net conf setparm reg-freigabe "hide unreadable" "yes"
root@samba4-1:~# net conf setparm reg-freigabe "valid users" "@domain user"

root@samba4-1:~# net registry export hklm\\software\\samba /dev/stdout
Windows Registry Editor Version 5.00

[hklm\software\samba]

[hklm\software\samba\smbconf]

[hklm\software\samba\smbconf\reg-freigabe]
"path"="/daten/reg-freigabe"
"comment"="Eine Freigabe in der Registry"
"guest ok"="no"
"read only"="no"
"hide unreadable"="yes"

[hklm\software\samba\Group Policy]
;Local Variables:
;coding: UTF-8
;End:
```

Parameter aus der Registry-Freigabe können Sie, mit zum Beispiel, `net conf delparm reg-freigabe "valid users"` auch wieder löschen. Wollen Sie sich den gesetzten Wert eines Parameters einer in der Registry gespeicherten Freigabe auflisten lassen, geht das mit, zum Beispiel, `net conf getparm reg-freigabe "hide unreadable"`.

9.2.4 Sichern der Freigabeeinstellungen aus der Registry

Damit Sie für den Fall, dass der Server einmal ausfällt oder umgezogen werden muss, gerüstet sind, sollten Sie die Liste der Freigaben regelmäßig sichern. Nur dann können Sie später die Freigaben schnell wiederherstellen. Im folgenden Listing sehen Sie die Sicherung des Teils der Registry in der die Freigaben verwaltet werden:

```
root@samba4-1:~# net registry export hklm\\software\\samba freigaben.reg

root@samba4-1:~# cat freigaben.reg
Windows Registry Editor Version 5.00

[hklm\software\samba]

[hklm\software\samba\smbconf]

[hklm\software\samba\smbconf\reg-freigabe]
"path"="/daten/reg-freigabe"
"comment"="Eine Freigabe in der Registry"
"guest ok"="no"
"read only"="no"
"hide unreadable"="yes"

[hklm\software\samba\Group Policy]
;Local Variables:
;coding: UTF-8
;End:
```

Wie Sie sehen, werden alle Informationen aus der Registry als ASCII-Textdatei gespeichert.

9.2.5 Löschen einer Freigabe aus der Registry

Für den Fall, dass Sie mal eine Freigabe aus der Registry löschen wollen, können Sie dieses mit dem Kommando `net conf delshare reg-freigabe`. Es wird nicht nachgefragt ob Sie sicher sind, dass Sie die Freigabe löschen wollen, die Freigabe wird sofort aus der Registry entfernt.

9.2.6 Wiederherstellen von Freigaben in der Registry

Wenn Sie einmal aus versehen eine Freigabe gelöscht haben oder Sie die Freigaben auf einen anderen Server umziehen wollen, können Sie, sofern Sie ein export der Registry gemacht haben, die Freigaben einfach aus dem Export wieder einspielen. In den letzten beiden Abschnitten wurde zuerst die Freigabe exportiert und dann gelöscht. Dadurch lässt sich jetzt die Freigabe wieder aus der Sicherung mit dem Kommando `net registry import freigaben.reg` zurück sichern. Sie sollten immer ein aktuelles Backup der Registry bereithalten. Mehr zum Thema sichern der samba4-Datenbanken finden Sie im Abschnitt 20.

9.2.7 Aufgaben

- Erstellen Sie eine neue Freigabe für jede der Gruppen, die Sie bei der Benutzerverwaltung erstellt haben.
- Setzen Sie zusätzlich den Parameter `hide unreadable = yes` für alle Freigaben.

- Sichern Sie alle Freigaben in eine Datei.
- Löschen Sie alle Freigaben und spielen Sie anschließend die Sicherung wieder ein.

9.3 Verwaltung der Servergespeicherten Home-Directories

Hinweis !

Die Homedirectories der Benutzer werden in diesem Abschnitt auf den Domaincontroller angelegt. So lange Sie nur diesen einen samba4-Server in Ihren Netzwerk betreiben, ist dieses in Ordnung. Wenn Sie aber mehrere samba4-Server betreiben wollen, sollten Sie die Homedirectories auf jeden Fall auf einem Fileserver ablegen um das einheitliche ID-Mapping in der Domäne zu gewährleisten.

Wenn Sie später auch die Home-Directories beim anlegen der Benutzer auf dem entsprechenden Server durch die *RSAT* anlegen wollen, benötigen Sie dafür eine Freigabe.

Hinweis !

Hier darf nicht die Freigabe *[homes] von Samba3 verwendet werden, da diese über Macros angesprochen wird und sich in der Freigabe die Home-Directories nicht mit den RSAT anlegen lassen.*

Deshalb soll jetzt ein Freigabe `users` erzeugt werden, die anschließend für die Home-Directories der Benutzer verwendet wird. Im folgenden Listing sehen Sie, wie Sie das Verzeichnis anlegen und mit Rechten belegen und die Freigabe erzeugen:

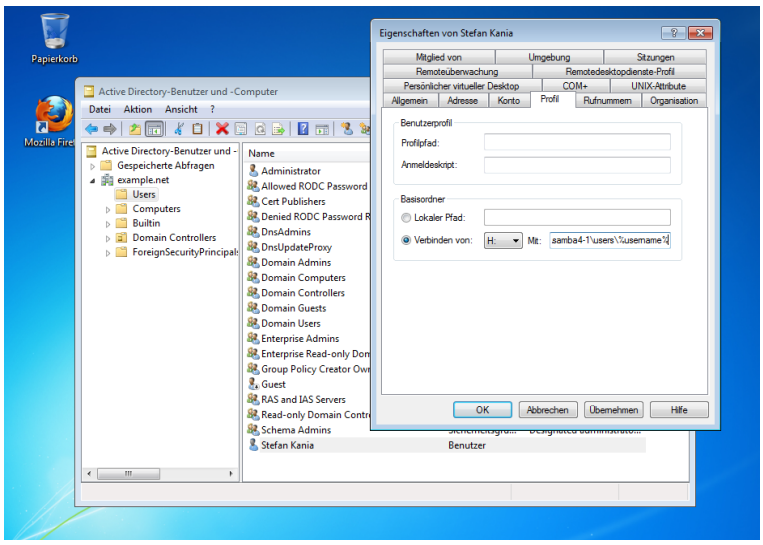
```
root@samba4-1:~# mkdir /home/EXAMPLE

root@samba4-1:~# chmod 775 /home/EXAMPLE/

root@samba4-1:~# net conf addshare users /home/EXAMPLE writeable=y guest_ok=n "Home-Dirs"

root@samba4-1:~# net conf setparm users "browsable" "no"

root@samba4-1:~# net conf setparm users "create mask" "700"

root@samba4-1:~# net conf setparm users "directory mask" "700"
```

Die Freigabe können Sie sich wieder, wie im folgenden Listing zu sehen, auflisten lassen:

```
root@samba4-1:~#  net rpc registry enumerate HKLM\\software\\samba\\smbconf\\users\
  -Uadministrator -S samba4-1.example.net
Enter administrator's password:
Valuename  = path
Type       = REG_SZ
Value      = "/home/EXAMPLE"

Valuename  = comment
Type       = REG_SZ
Value      = "Home-Dirs"

Valuename  = guest ok
Type       = REG_SZ
Value      = "no"

Valuename  = read only
Type       = REG_SZ
```

```
Value       = "no"

Valuename   = browseable
Type        = REG_SZ
Value       = "no"

Valuename   = create mask
Type        = REG_SZ
Value       = "700"

Valuename   = directory mask
Type        = REG_SZ
Value       = "700"
```

Jetzt können Sie mit den RSAT für einen bestehenden Benutzer ein Home-Directory, wie in der folgenden Abbildung zu sehen, anlegen:



Hinweis !

Die Freigabe muss den den Namen *users* haben. Mit anderen Namen funktioniert das Anlegen der Verzeichnisse nicht

Im folgenden Listing sehen Sie, wie die Rechte nach dem anlegen des Verzeichnisses aussehen und wie die Rechte geändert werden müssen.

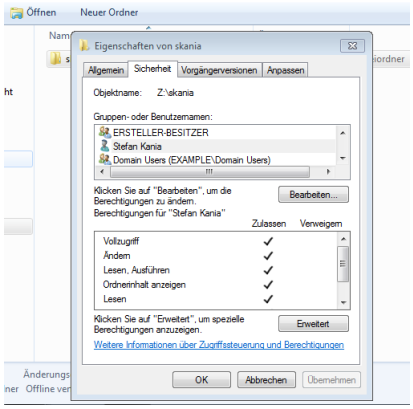
```
root@samba4-1:~# ls -l /home/EXAMPLE/
insgesamt 16
drwxrwx---+ 2 3000000 users 4096 Jun 10 11:58 skania
```

Mit dem Kommando `getfacl` können Sie sich die ACLs des Home-Directories anzeigen lassen. Im folgenden Listing sehen Sie, wie die Rechte gesetzt sind:

```
  root@samba4-1:/home/EXAMPLE# getfacl skania/
# file: skania/
# owner: 3000000
```

```
# group: users
user::rwx
group::---
group:users:---
group:3000000:rwx
group:3000020:rwx
mask::rwx
other::---
default:user::rwx
default:user:3000000:rwx
default:group::---
default:group:users:---
default:group:3000000:rwx
default:group:3000020:rwx
default:mask::rwx
default:other::---
```

Hier sehen Sie, dass als *owner* nur eine ID eingetragen ist. Die ID 3.000.000 ist dabei der Build-in Gruppe *Administrators* zugeordnet. Die ID 3.000.020 ist die ID des Benutzers *skania* die hier aber als Gruppe dargestellt wird. Das zeigt, dass die Zuordnung der IDs auf einem Domaincontroller eigene Regeln hat. Wenn Sie aber unter Windows die Eigenschaften des Ordners aufrufen sehen Sie unter dem Punkt *Sicherheit*, dass die Zuordnung unter Windows richtig ist. Sehen Sie dazu die folgenden Abbildung:



Wenn der Benutzer sich jetzt anmeldet, bekommt er automatisch ein Netzwerklaufwerk für sein Home-Directory eingebunden.

9.3.1 Aufgaben

- Erstellen Sie die Freigabe users und weisen Sie anschließend Ihren Benutzern ein Homedirectory zu.
- Melden Sie sich als Benutzer an und prüfen Sie, ob ein Netzwerklaufwerk für das Homedirectory vorhanden ist.

10 Server gespeicherte Profile

Hinweis !

Wie schon bei den Homedirectories ist es auch bei den Profilen besser, diese auf einem Fileserver abzulegen und nicht auf den Domaincontroller, auch wenn sie hier nicht auf die Probleme mit dem ID-Mapping stoßen können, da Linux-Benutzer die Profile nicht nutzen.

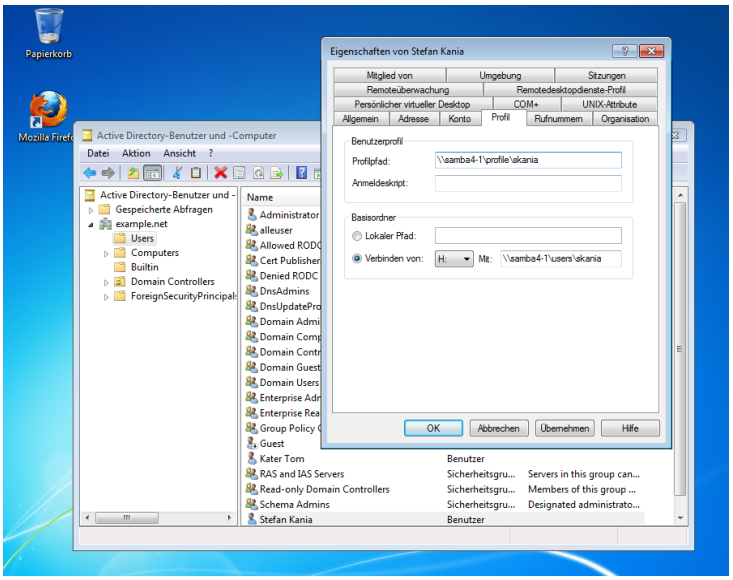
Natürlich können Sie auch die Profile der Benutzer auf dem Server speichern. In diesem Abschnitt geht es um die Verwaltung der servergespeicherten Profile. Für die Profile haben Sie zwei Möglichkeiten. Sie können die Profile im jeweiligen Home-Directory des Benutzers ablegen oder aber eine eigene Freigabe erstellen in der dann alle Profilverzeichnisse der Benutzer abgelegt werden. Der Vorteil des zweiten Weges ist der, dass Sie die Profile auch auf einem anderen Server ablegen können als die Home-Directories der Benutzer und das die Benutzer die Profile nicht direkt bearbeiten können. Hier soll nur die Lösung mit der eigenen Freigabe angesprochen werden.
Im ersten Schritt müssen Sie wieder eine Freigabe für die Profile erzeugen. Im folgenden Listing sehen Sie dafür auch wieder das Beispiel:

```
root@samba4-1:~# mkdir /profile

root@samba4-1:~# chmod 777 /profile/

root@samba4-1:~# net conf addshare profile /profile writeable=y guest_ok=n "User Profile"

root@samba4-1:~# net conf setparm profile "browsable" "no"

root@samba4-1:~# net conf setparm profile "profile acls" "yes"
```

Im folgenden Listing sehen Sie, wie die Freigabe in der Registry abgelegt wurde:

```
root@samba4-1:~# net rpc registry enumerate HKLM\\software\\samba\\smbconf\\profile\
  -Uadministrator -S samba4-1.example.net
Enter administrator's password:
Valuename  = path
Type       = REG_SZ
Value      = "/profile"

Valuename  = comment
Type       = REG_SZ
Value      = "User Profile"

Valuename  = guest ok
Type       = REG_SZ
Value      = "no"

Valuename  = read only
Type       = REG_SZ
Value      = "no"

Valuename  = browseable
Type       = REG_SZ
Value      = "no"

Valuename  = profile acls
Type       = REG_SZ
Value      = "yes"
```

Nachdem Sie die Freigabe erstellt haben, können Sie jetzt mit den RSAT unter Windows das Profil des Benutzers wie in der folgenden Abbildung anpassen:



Wenn der Benutzer sich das erste mal anmeldet, wird in der Freigabe ein Unterverzeichnis erzeugt. Wenn der Benutzer noch mit Windows XP arbeitet, heißt das Verzeichnis /profile/username. Bei Windows7 bekommt das Verzeichnis den Namen /profile/username.V2 so kann ein Benutzer an verschieden Systemen arbeiten und die Profile funktionieren immer und werden nicht gemischt. Erst wenn der Benutzer sich wieder abmeldet wird das Profil geschrieben und die Unterverzeichnisse im Profilverzeichnis werden erstellt.

10.1 Aufgaben

- Erstellen Sie die Freigaben für die servergespeicherten Profile und weisen anschließend den Benutzer ein servergespeichertes Profil über RSAT zu.
- Melden Sie sich als Benutzer an und prüfen Sie, ob das Profilverzeichnis in der Freigabe angelegt werden.
- Melden Sie sich wieder ab und prüfen Sie, ob das Profil geschrieben wird.

11 Die Freigabe *sysvol*

Der Freigabe *sysvol* hat in einem AD eine ganz besondere Bedeutung. Hier liegen die Gruppenrichtlinen und die Logonskripte der Benutzer. Die Freigabe muss auf jedem DC der Domäne verfügbar sein, da jeder der DCs die Anmeldung der Benutzer durchführen kann. Zur Zeit ist die Replikation auf andere DCs noch nicht so einfach durchführbar. Im Abschnitt17 wird eine Möglichkeit der Replikation beschrieben.

12 Logonskripte

Logonskripte können, wie auch bei Windows-DCs in der Freigaben NETLOGON erzeugt werden. Da die Freigabe NETLOGON auf allen DCs verfügbar sein muss, existiert diese Freigabe bereits und zeigt auf das Verzeichnis /var/lib/samba/sysvol/example.net/scripts. Wie Sie sehen, befindet sich das Verzeichnis innerhalb der Freigabe sysvol. Dadurch wird sichergestellt, dass bei mehreren DCs die Skripte auf allen DCs vorhanden sind, da ja jeder DC jede Benutzeranmeldung bearbeiten kann.

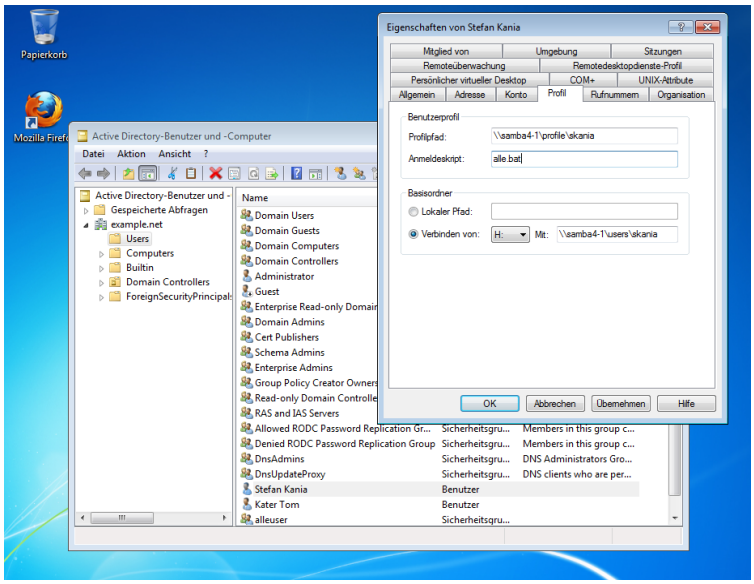
Hinweis !

Die Skripte sollten Sie unter Windows erstellen, oder mit einem Editor, der die Windows-Zeilenumbrüche kann. Da sonst die Skripte nicht ausgeführt werden.

Eine Beispiel für ein Skript sehen Sie im folgenden Listing:

```
net use i: \\samba4-1\abteilungen /persistent:no
net use j: \\samba4-1\gemeinsam /persistent:no
```

Durch den Schalter `/persistent` sind die Laufwerkszuordnungen nicht permanent und werden nicht in Registry des Benutzers als feste Laufwerkszuordnungen eingetragen. Das sollten Sie auf jeden Fall genau so machen, denn die Laufwerkszuordnungen aus der Registry des Benutzers werden nach dem Logonskript eingebunden. Wenn Sie die Verbindungen also persistent machen, würde eine Änderung am Logonskript immer durch den Eintrag in der Registry überschrieben.
Jetzt können Sie, mit den RSAT jedem Benutzer ein eigenes Skript zuweisen.
Alle Skripte legen Sie in der Freigabe NETLOGON ab. Die Dateiendung muss entweder .bat oder .cmd sein und die Datei muss von allen Benutzern gelesen und ausgeführt werden können. In der folgenden Abbildung sehen Sie wie das Logonskript in das Profil des Benutzers eingeben wird.



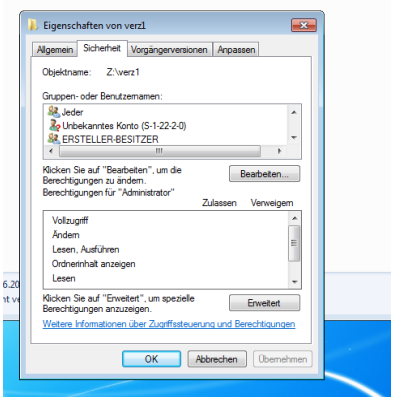
Hier wird nur der Name des Skripts eingetragen, da alles Logonskripte immer relativ zur Freigabe NETLOGON gesucht werden. Wenn sich der Benutzer jetzt anmeldet, werden die entsprechenden Laufwerkszuordnungen gleich erstellt.

12.1 Aufgaben

- Erstellen Sie für Ihre Benutzer je ein Logonskript, das die eigene Freigabe bei jeder Anmeldung einbindet.
- Weisen Sie die Logonskripte den Benutzern über die RSAT zu.
- Testen Sie, ob die Laufwerke bei der Anmeldung der Benutzer eingebunden werden.

13 Dateisystemberechtigungen

Damit die Benutzer auch mit den passenden Rechten auf die Freigaben zugreifen können, müssen Sie jetzt noch die Berechtigungen im Dateisystem vergeben können. Bei samba4 können Sie alle Rechte direkt über den Windows-Explorer vergeben. Damit das möglich ist, müssen Sie für alle Dateisystem die Sie unter Windows nutzen wollen, die mount-Optionen `acl` und `user_xattr` verwenden. In der folgenden Abbildung sehen Sie ein Verzeichnis, das als Administrator erzeugt wurde. Wenn Sie sich an der Stelle unter Windows die Rechte anschauen werden Sie feststellen, dass ein unbekanntes Konto mit der SID `S-1-22-2-0` eingetragen wurde. Sehen Sie dazu die folgenden Abbildung:



Dabei handelt es sich um die Linux-Gruppe `root`, da diese Gruppe und der Benutzer root mit SID `S-1-22-1-0` nicht mittels idmapping umgesetzt werden, werden Sie an der Stelle immer nur die SID sehen. Die Rechte und die gesetzten ACLs sehen Sie im folgende Listing:

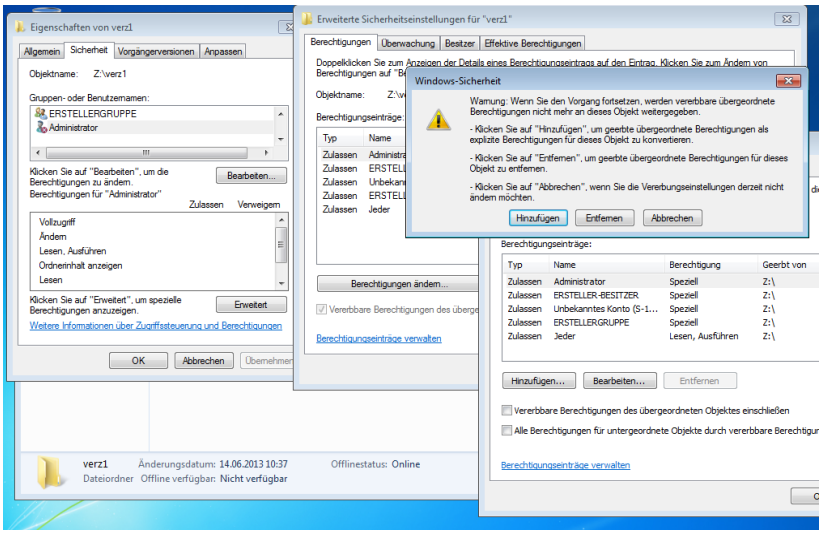
```
root@samba4-1:/daten/abteilung# ls -l
insgesamt 8
drwxrwxr-x+ 2 root root 4096 Jun 14 10:37 verz1

root@samba4-1:/daten/abteilung# getfacl verz1/
# file: verz1/
# owner: root
# group: root
user::rwx
user:root:rwx
group::rwx
group:root:rwx
mask::rwx
```

```
other::r-x
default:user::rwx
default:user:root:rwx
default:group::rwx
default:group:root:rwx
default:mask::rwx
default:other::r-x
```

Wie sie hier sehen, gehört das Verzeichnis dem user `root` und der Gruppe `root`. Wenn Sie sich den *administrator* einmal mit dem Kommando `id` anschauen, werden Sie den Grund für die Zuordnung sehen. Im folgenden Listing sehen Sie diese Informationen:

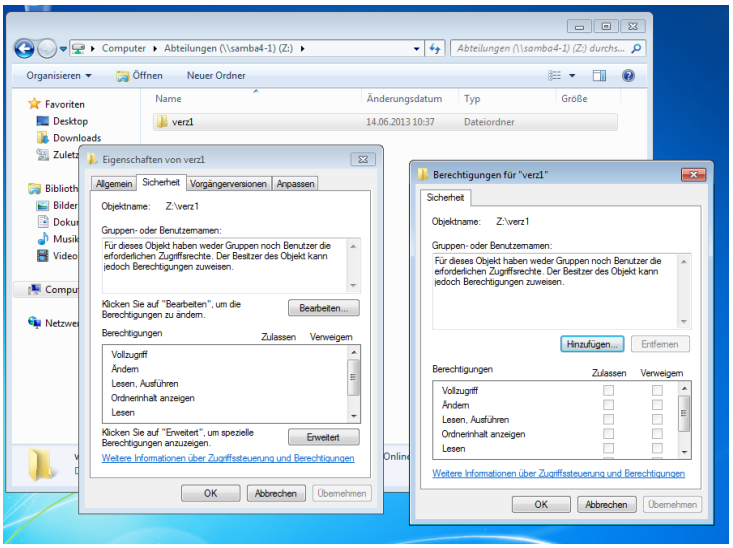
```
root@samba4-1:/daten/abteilung# id administrator
uid=0(root) gid=100(users) Gruppen=0(root),100(users),\
3000004(EXAMPLE\Group Policy Creator Owners),\
3000006(EXAMPLE\Enterprise Admins),3000008(EXAMPLE\Domain Admins),\
3000007(EXAMPLE\Schema Admins)
```

Wie Sie sehen, hat der *administrator* die UID 0 und auch die GID 0.
Wenn Sie unter Windows ein Verzeichnis anlegen, erbt das neue Verzeichnis immer die Rechte der darüber liegenden Verzeichnis. Ohne die Aufhebung der Vererbung können Sie keine bestehenden Berechtigungen ändern oder entfernen. Um die Vererbung zu beenden, klicken Sie, nach dem Sie die Eigenschaften des Verzeichnis geöffnet haben, auf ***Erweitert***, anschließend klicken Sie auf ***Berechtigungen ändern...*** und entfernen dann den Haken bei ***Vererbbare Berechtigungen des übergeordneten Objekts einschließen***. Daraufhin erscheint eine Meldung und Sie können entscheiden, ob Sie die bestehenden Rechte übernehmen wollen und eine neu Vererbung starten wollen, oder ob sie mit einer leeren Berechtigungsliste starten wollen. Hier soll jetzt eine neue Liste begonnen werden. Dazu wird auf die Schalter ***Entfernen*** geklickt. Es kommt noch eine Sicherheitsabfrage, ob Sie wirklich alles löschen wollen, wenn Sie das bestätigen, haben Sie anschließend eine leere Berechtigungsliste. In der folgenden Abbildung sehen Sie alle Fenster für den gesamten Vorgang:

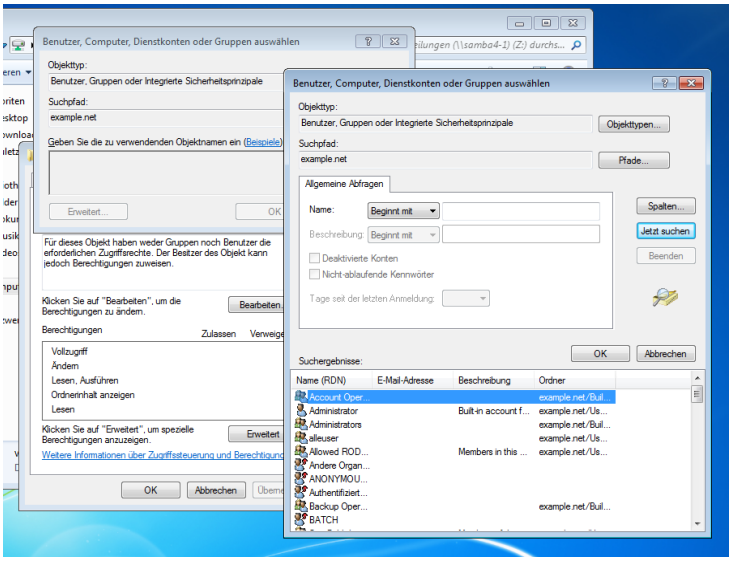


Sie können jetzt das Verzeichnis komplett neu mit Rechten belegen. Dafür klicken Sie, in den Eigenschaften des Verzeichnisses und dort auf den Karteireiter ***Sicherheit***, auf die Schaltfläche

Bearbeiten... Es öffnet sich ein neues Fenster, in dem Sie jetzt Einträge hinzufügen können. Dazu sehen Sie die folgende Abbildung:

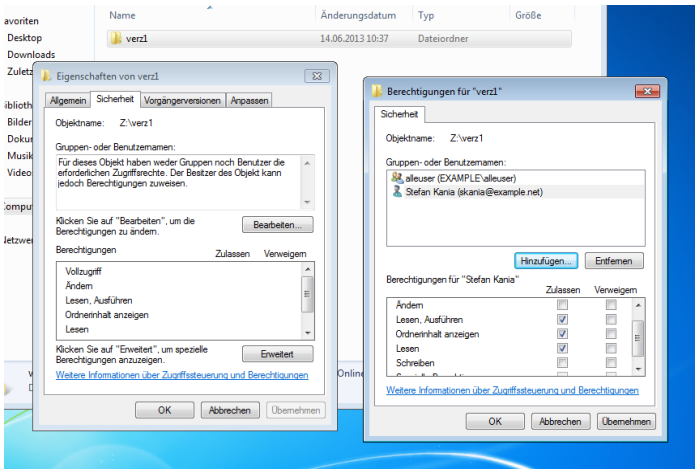


An der Stelle klicken Sie jetzt auf *Hinzufügen...* Es öffnet sich ein Fenster in dem Sie Benutzer und Gruppen eintragen können die Berechtigungen am neuen Verzeichnis erhalten sollen. Wenn Sie aus allen Benutzern und Gruppen der Domäne auswählen wollen, klicken Sie auf *Erweitert...*, es öffnet sich ein neues Fenster. Klicken Sie hier auf *Jetzt suchen* und es erscheint eine Liste mit allen Benutzern und Gruppen der Domäne. In der folgenden Abbildung sehen Sie die Liste:

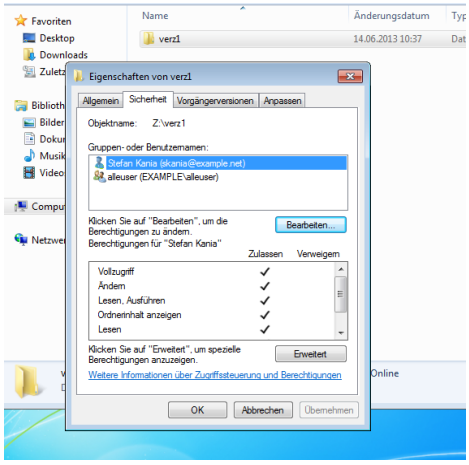


Wählen Sie hier, Schritt für Schritt, alle Benutzer und Gruppen aus, die Rechte an dem Verzeichnis erhalten sollen und bestätigen Sie Ihre Auswahl mit *OK*.
Jetzt sehen Sie Ihre Auswahl in der Liste und können die Rechte anpassen. Erst wenn Sie die

Rechte angepasst haben, werden die Objekte in die eigentlich Liste der Berechtigten übernommen. In der folgenden Abbildung sehen Sie die Änderung der Rechte, vor dem Abspeichern:



Anschließend erscheint im Eigenschaftenfenster des Verzeichnisses die Liste der Berechtigten, so wie Sie das in der folgenden Abbildung sehen können:



Jetzt ist es noch interessant, wie die Berechtigungen unter Linux direkt im Dateisystem aussehen. Im folgenden Listing sehen Sie die Rechte im Dateisystem:

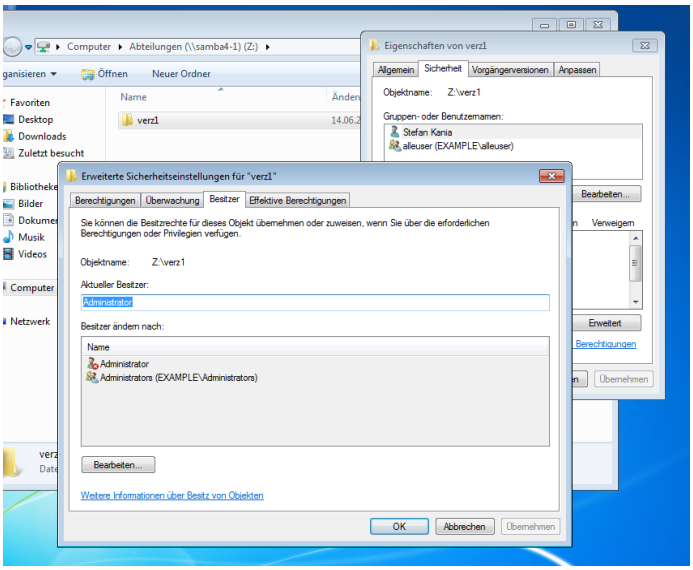
```
root@samba4-1:/daten/abteilung# getfacl verz1/
# file: verz1/
# owner: root
# group: root
user::rwx
user:root:rwx
group::---
group:root:---
group:3000020:rwx
```

```
group:EXAMPLE\134alleuser:r-x
mask::rwx
other::---
default:user::rwx
default:user:root:rwx
default:group::---
default:group:root:---
default:group:3000020:rwx
default:group:EXAMPLE\134alleuser:r-x
default:mask::rwx
default:other::---
```

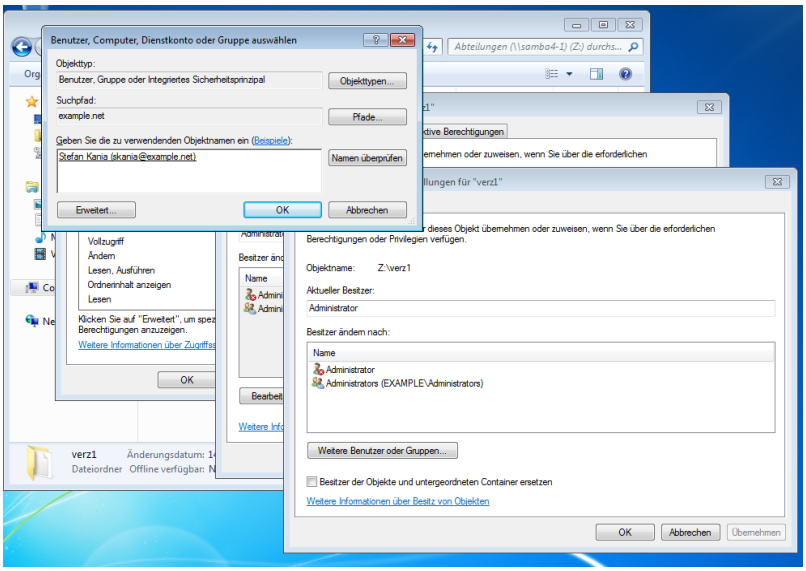
Sie sehen hier, dass die Gruppe `alleuser` in den ACLs eingetragen ist und eine Gruppe mit der GID 3.000.020 dabei handelt es sich nicht um deine Gruppe sondern um den Benutzer `skania`. Windows verwaltet an dieser Stelle Benutzer wie Gruppen.

13.1 Ändern des Besitzers

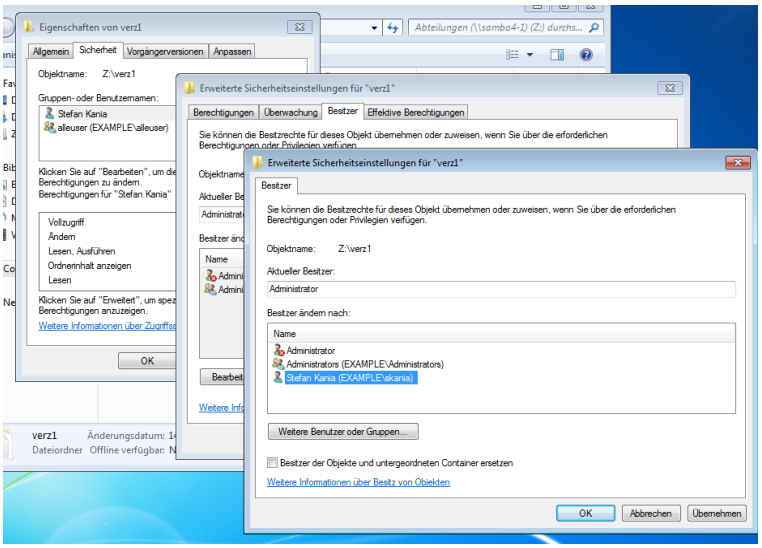
Bis jetzt wurden immer nur die Rechte an Verzeichnissen und Dateien angesprochen. Aber jeder Eintrag im Dateisystem hat auch immer einen Besitzer, unter Linux zusätzlich auch noch eine besitzenden Gruppe. Auch diese Einstellungen können Sie über Windows in der Sicherheit des Dateisystemeintrags anpassen. Öffnen Sie hierfür die Eingenschaften des Eintrags und klicken auf den Karteireiter *Sicherheit*. In dem Fenster klicken Sie dann auf *Erweitert*. Dort finden Sie verschiedene Karteireiter, unter anderem den Reiter *Besitzer*. Klicken Sie auf dem Karteireiter *Besitzer*. Sie sehen dann, so wie in der folgenden Abbildung, den derzeitigen Besitzer des Eintrags:



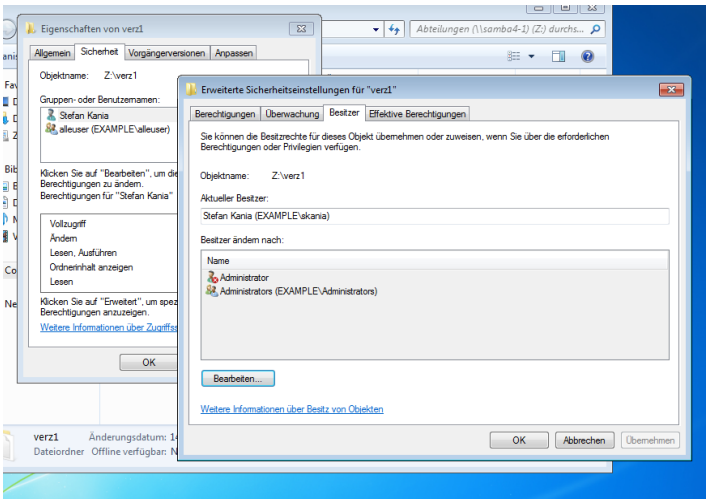
Sie können an dieser Stelle nur den Besitzer ändern, wenn Sie auf *Bearbeiten* klicken, öffnet sich ein neues Fenster in dem Sie dann über die Schaltfläche *Weitere Benutzer oder Gruppen...* in ein neues Fenster kommen, in dem Sie den gewünschten Benutzer direkt eingeben können, oder über die Schaltfläche *Erweitert...* aus der Liste alle Benutzer auswählen können. In der folgenden Abbildung sehen Sie die Zuweisung eines neuen Benutzers:



Nach einem Klick auf *OK* erscheint der Benutzer in der Auswahlliste. Wie die Liste jetzt aussieht, sehen Sie in der folgenden Abbildung:



Markieren Sie den gewünschten Benutzen mit einem Klick auf das Objekt und klicken dann auf die Schaltfläche *OK*. Es folgt eine Meldung die Sie darauf hinweist, dass Sie die Eigenschaften erneut aufrufen müssen, bevor die Änderung angezeigt wird. Bestätigen Sie die Meldung durch einen Klick auf *OK*. Anschließend sehen Sie, so wie in der nachfolgenden Abbildung, den neuen Besitzer des Eintrags.



Bestätigen Sie die Änderung mit einem Klick auf *Ok*. Wenn Sie das Eigenschaftenfenster jetzt mit einem Klick auf *OK* schließen und anschließend sofort wieder öffnen können Sie sich in der erweiterten Sicherheit den Besitzer anzeigen lassen. Dort wird jetzt der von Ihnen ausgewählte Benutzer stehen.
Unter Linux sehen die Rechte und die ACLs jetzt so aus wie im folgenden Listing:

```
root@samba4-1:/daten/abteilung# ls -ld verz1/
drwxrwx---+ 2 EXAMPLE\skania root 4096 Jun 14 11:54 verz1/

root@samba4-1:/daten/abteilung# getfacl verz1/
# file: verz1/
# owner: EXAMPLE\134skania
# group: root
user::rwx
user:root:rwx
group::---
group:root:---
group:3000020:rwx
group:EXAMPLE\134alleuser:r-x
mask::rwx
other::---
default:user::rwx
default:user:root:rwx
default:group::---
default:group:root:---
default:group:3000020:rwx
default:group:EXAMPLE\134alleuser:r-x
default:mask::rwx
default:other::---
```

Auch hier wurde jetzt der Besitzer geändert. Wollen Sie die besitzende Gruppe ändern, müssen Sie das über die Kommandozeile unter Linux durchführen. Jetzt können Sie die Rechte auf allen Dateien und Verzeichnissen von Windows aus verwalten.

13.2 Aufgaben

- Vergeben die Rechte für die Verzeichnisse auf die die Freigaben der Gruppen zeigen.

- Testen Sie mit den verschiedenen Benutzern die Zugriffe.

14 Gruppenrichtlinien

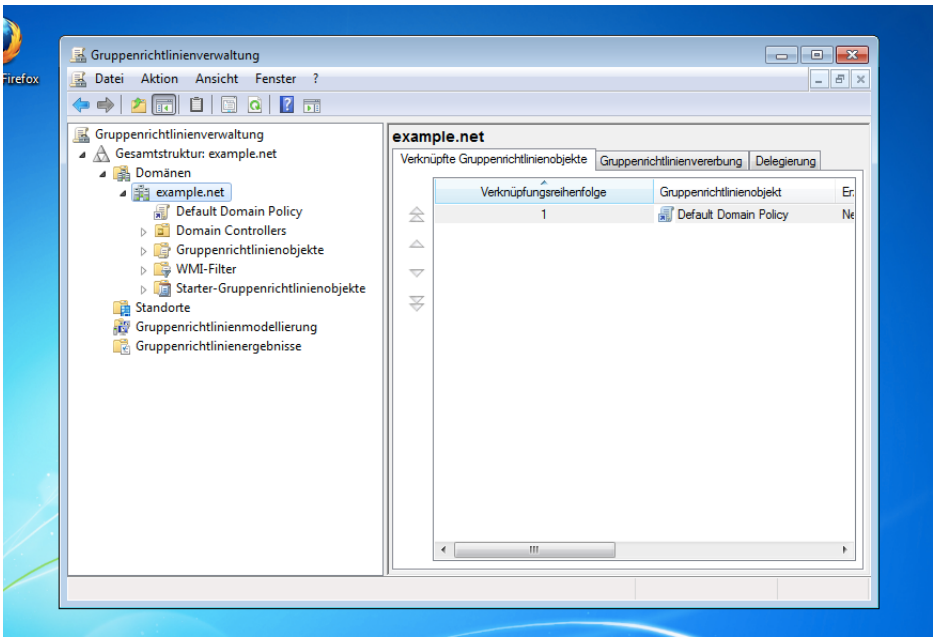
In einer Windowsdomäne können Sie über Gruppenrichtlinen (GPOs) Berechtigungen für Ressourcen vergeben oder Voreinstellungen für die Benutzer und Hosts vornehmen. Mit samba4 können Sie diese GPOs auch verwalten und erstellen. Mit dem Konsolenwerkzeug `samba-tool` sind Sie in der Lage, die Gruppenrichtlinen auch über die Kommandozeile zu verwalten. Im folgenden Listing sehen Sie, wie Sie sich die Standard-GPOs auflisten lassen können:

```
  root@samba4-1:~# samba-tool gpo listall -Uadministrator
Password for [EXAMPLE\administrator]:
GPO          : {31B2F340-016D-11D2-945F-00C04FB984F9}
display name : Default Domain Policy
path         : \\example.net\sysvol\example.net\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}
dn           : CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=example,DC=net
version      : 0
flags        : NONE

GPO          : {6AC1786C-016F-11D2-945F-00C04FB984F9}
display name : Default Domain Controllers Policy
path         : \\example.net\sysvol\example.net\Policies\{6AC1786C-016F-11D2-945F-00C04FB984F9}
dn           : CN={6AC1786C-016F-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=example,DC=net
version      : 0
flags        : NONE
```

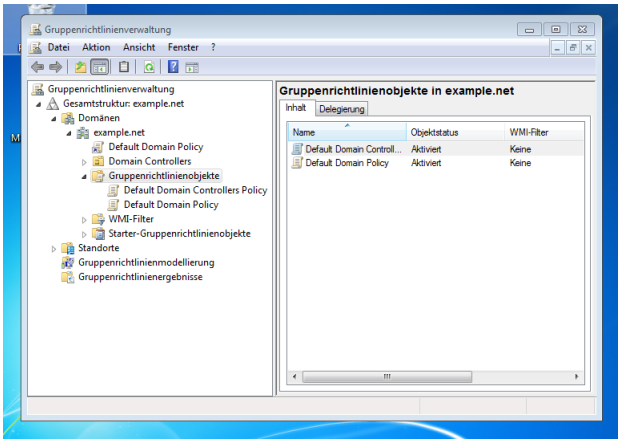
Natürlich haben Sie noch weitere Möglichkeiten, die GPOs über die Kommandozeile zu verwalten, aber besser ist es, die GPOs über die RSAT zu bearbeiten. Verwenden Sie für die Verwaltung der GPOs das Windows-Werkzeug `Gruppenrichtlinenverwaltung`.

14.1 Verwaltung der GPOs mit den RSAT

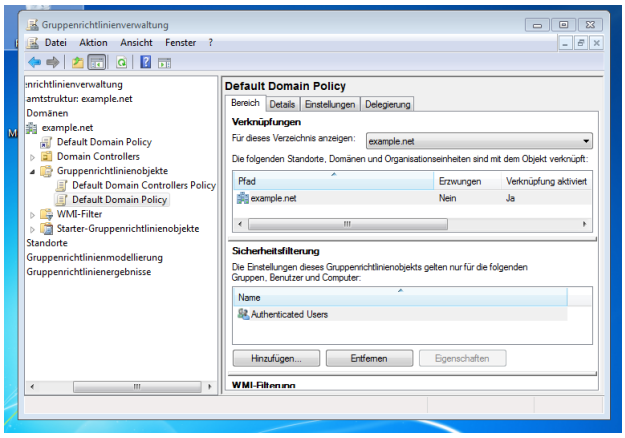
In der folgenden Abbildung sehen Sie das Werkzeug für die Verwaltung der Gruppenrichtlinen, ohne das Änderungen vorgenommen wurden.



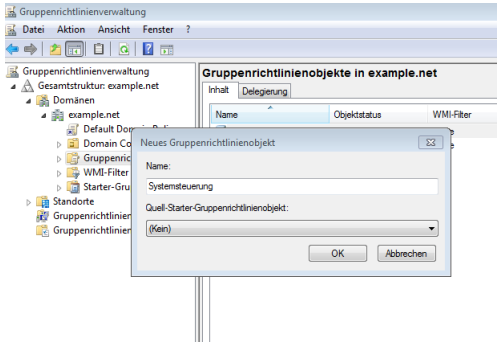
Wenn Sie hier den Unterpunkt *`Gruppenrichtlinienobjekte`* anklicken, sehen Sie alle bereits existierende Gruppenrichtlinen. In der folgenden Abbildung sehen Sie die beiden Standardgruppenrichtlinien.



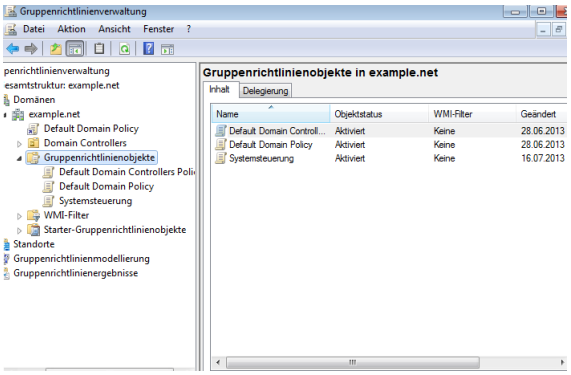
Klicken Sie jetzt auf eine der bestehenden Gruppenrichtlinen, so erhalten Sie eine Übersicht über die Pfade mit denen diese Gruppenrichtlinen verknüpft ist und für welche Objekte die Gruppenrichtline angewendet wird. In der folgenden Abbildung sehen Sie die Standardeinstellungen der *Default Domain Policy*



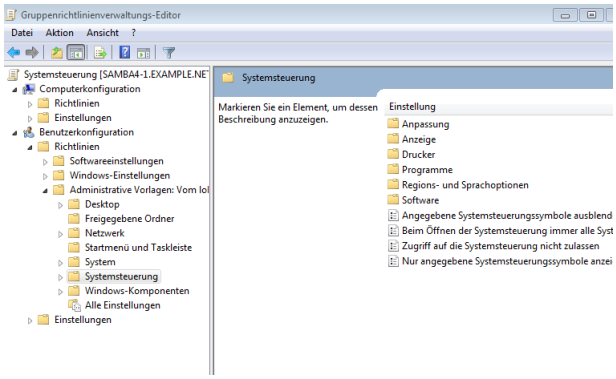
Wie Sie hier sehen, ist diese Gruppenrichtlinie für alle angemeldeten Benutzer der Domäne gültig und ist auch als `aktiv` markiert.
Wolle Sie jetzt eine neue Gruppenrichtline erstellen, können Sie diese direkt in dem Container Gruppenrichtlinienobjekte erstellen und später mit den gewünschten OUs verlinken.
Da GPOs nur auf der OU wirksam sind, mit der sie verknüpft sind, müssen Sie mindestens Eine OU anlegen, in die Sie anschließend alle Objekte verschieben, für die diese GPO wirksam sein soll. Gerade wenn Sie sehr viele Gruppenrichtlinen erstellen möchten, ist es aber sinnvoll, die Gruppenrichtlinen auch in Untercontainern abzulegen, da Sie nur dadurch unterschiedliche GPOs für verschiedene Benutzer und Gruppen vergeben können.
Wenn Sie jetzt eine neue GPO erstellen wollen, starten Sie als Domainadministrator in den RSAT die `Gruppenrichtlinenverwaltung`. Öffnen Sie die Ansicht auf der linken Seite, bis Sie Ihre Domäne und darunter den Ordner Gruppenrichtlinienobjekte sehen. Kicken Sie mit der rechten Maustaste auf *`Gruppenrichtlinienobjekte`* und anschließend auf *`Neu`* Es erscheint ein neues Fenster wie Sie es in der folgenden Abbildung sehen können. Vergeben Sie einen Namen für die neu GPO. In diesem Fall soll mit der GPO die Verwendung der Systemsteuerung unterbunden werden.



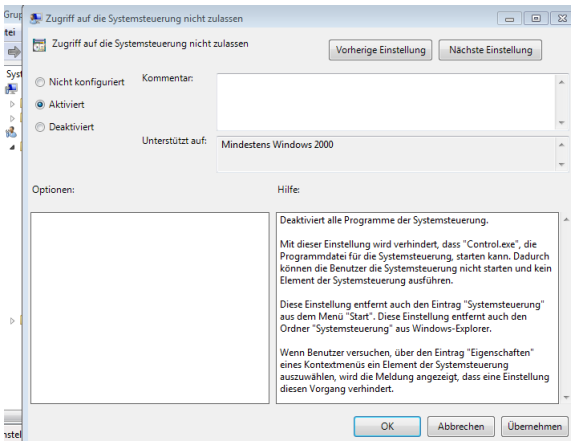
Bestätigen Sie die Eingabe mit einem Klick auf *`OK`*. Anschließend sehen Sie im Container Gruppenrichtlinienobjekte die neue GPO so wie in der folgenden Abbildung.



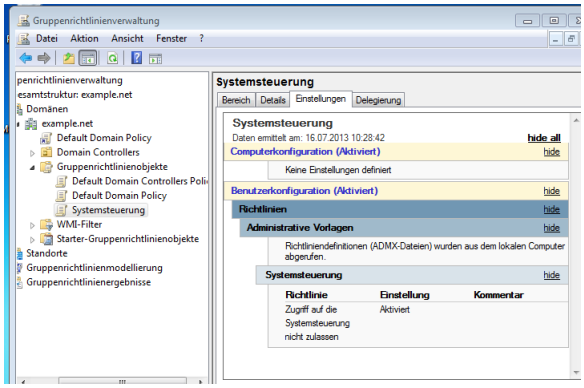
Jetzt haben Sie eine leere GPO erstellt in der Sie jetzt die entsprechenden Einstellungen vornehmen müssen. Dazu klicken Sie mit der rechten Maustaste auf die GPO und dann auf *Bearbeiten...* Daraufhin öffnet sich der `Gruppenrichtlinenverwaltungs-Editor`. Dort sehen Sie auf der linken Seite zwei Bereiche, einmal die `Computerkonfiguration` und die `Benutzerkonfiguration` Bei der Einschränkung die hier eingerichtet werden soll, handelt es sich um eine Benutzer-GPO, da die Systemsteuerung unabhängig von der Workstation sein soll an der sich ein Benutzer anmeldet. Öffnen Sie die Struktur unterhalb der `Benutzerkonfiguration` bis Sie den Ordner Systemsteuerung sehen. Klicken Sie dann auf der linken Seite auf *Systemsteuerung* Jetzt sehen Sie, wie in der nachfolgenden Abbildung, auf der Rechten Seite die Möglichkeiten die Sie hier haben um die GPO anzupassen.



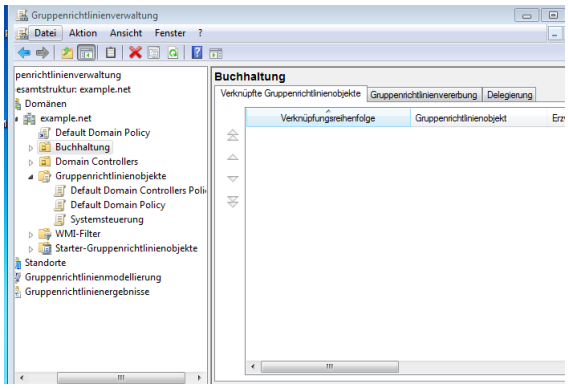
Die Richtlinie, die für die GPO benötigt wird heißt `Zugriff auf die Systemsteuerung nicht zulassen` eine Doppelklick auf die Einstellung öffnet ein neues Fenster. In diesem Fenster müssen Sie die Einschränkung jetzt aktivieren, so wie Sie das in der folgenden Abbildung sehen können.



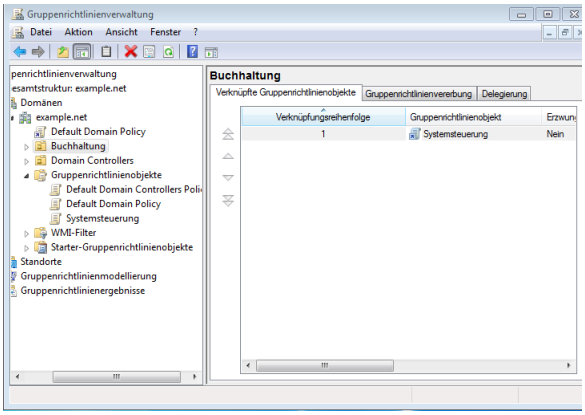
Bestätigen Sie die Einstellung mit einem Klick auf *OK*. Im Anschluss daran können Sie den *Gruppenrichtlinenverwaltungs-Editor* schließen. Sie gelangen dann wieder in die *Gruppenrichtlinienverwaltung* Führen Sie hier einen Doppelklick auf die neue GPO aus und klicken dann auf den Karteireiter *Einstellung* und dann auf *show all*. Jetzt sehen Sie, so wie in der folgenden Abbildung, alle Einstellungen der GPO.



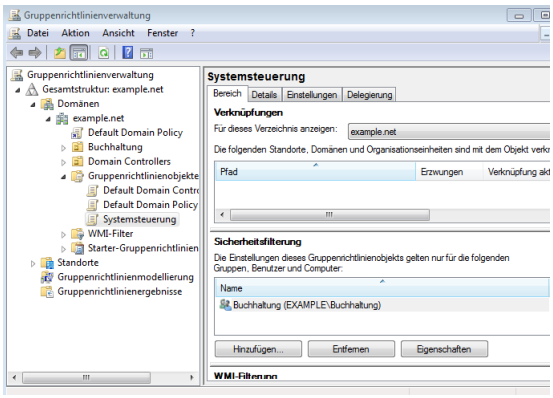
Bis zu diesem Zeitpunkt haben Sie zwar eine GPO angelegt, aber noch keinem Benutzer oder keiner Gruppe zugewiesen. Gruppenrichtlinen werden in bestimmten für diesen Zweck entworfenen OUs verwaltet und sind dann für Objekte in dieser OU gültig. Sie müssen also im nächsten Schritt eine Struktur für Ihre GPOs anlegen. Hier ist eine sehr gute Planung von Nöten. Je mehr GPOs Sie in Ihrem Netzwerk einsetzen wollen, um so genauer sollte Ihre Planung sein. Da sich Benutzerobjekte nur in einer OU befinden können. Hier soll jetzt eine kleine Struktur angelegt, werden um zu zeigen, wie die GPOs funktionieren. Klicken Sie hierfür mit der rechten Maustaste auf Ihr Domänenobjekt und wählen Sie den Punkt *Neue Organisationseinheit* aus. Es öffnet sich ein neues Fenster, in dem Sie nur den Namen für die neue OU angeben müssen. Vergeben Sie hier einen Namen und klicken Sie anschließend auf *OK*. Unterhalb Ihrer Domäne erscheint jetzt die neu OU mit dem Symbol der Gruppenrichtline im Ordner. In der folgenden Abbildung sehen Sie die Beispiel-OU `Buchhaltung`



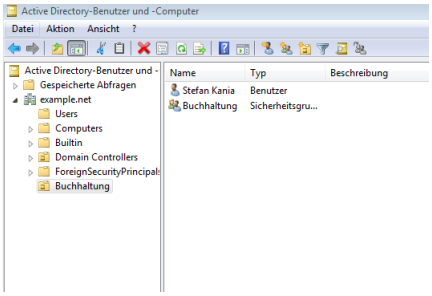
Wie Sie hier sehen, ist mit dieser OU noch keine GPO verknüpft worden. Im nächsten Schritt soll diese Verknüpfung erstellt werden. Klicken Sie hierfür mit der rechten Maustaste auf die gerade erstellte OU und anschließend auf *`Vorhandenes Gruppenrichtlinenobjekt verknüpfen...`*. Es erscheint eine Liste aller vorhanden GPOs. Doppelklicken Sie hier auf die von Ihnen erstellte GPO. Jetzt sehen Sie, so wie in der folgenden Abbildung, die Verknüpfung der GPO mit der OU.



Wechseln Sie jetzt auf den Karteireiter *`Bereich`*, im rechten unteren Teil sehen Sie den Punkt *Sicherheitsfilterung*. An dieser Stelle ist grundsätzlich immer erst der Eintrag `Authenticated Users` vorhanden, so dass diese GPO für alle Benutzer und Gruppen in der OU gültig ist. Hier müssen Sie jetzt die derzeitigen Einträge löschen und die Gruppe die die GPOs ziehen soll eintragen. Nach allen Anpassungen sollte Ihr Objekt So aussehen wie Sie es in der folgenden Abbildung sehen können:



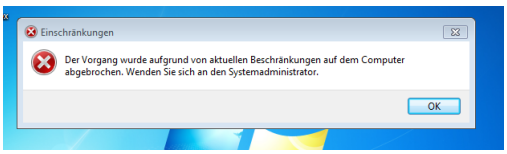
Jetzt müssen noch die Objekte für die die GPO wirksam sein soll, in die entsprechende OU verschoben werden. Dazu müssen Sie jetzt die Gruppe und alle Mitglieder der Gruppe in die OU verschieben. Nur so wird die GPO für alle Mitglieder der Gruppe wirksam. Die Gruppe und die Benutzer können Sie mit dem RSAT Active Directory-Benutzer und -Computer durchführen. Wenn Sie auf das entsprechende Objekt mit der rechten Maustaste klicken, sehen Sie einen Unterpunkt *Verschieben*. Durch einen Klick auf den Punkt können Sie das Objekt verschieben. Nachdem Sie alle Objekte verschoben haben, sieht der Inhalt der OU so aus, wie in der folgenden Abbildung:



Hinweis !

Die Möglichkeit, eine Gruppe an der Stelle einzutragen besteht erst seit Windows Server 2008. Samba4 unterstützt auch diese Möglichkeit

Wenn sich jetzt ein Benutzer aus der Gruppe an einem Client in der Domäne anmeldet, wird er im Startmenü die Systemsteuerung nicht mehr sehen. Ein Rechtsklick auf *Computer* zeigt nur noch das folgende Fester:



Natürlich ist das nur ein Einstieg in das Thema GPOs, aber die Vielzahl der Möglichkeiten würden den Rahmen dieser Unterlage sprengen.

14.2 GPOs über die Kommandozeile

Am Anfang des Abschnittes wurde schon erwähnt, dass Sie die GPOs auch über die Kommandozeile verwalten können. Hier soll jetzt noch einmal ein kurzer Blick auf die Möglichkeiten geworfen werden, die Sie auf der Kommandozeile haben.
Als erstes lassen Sie sich nochmal alle GPOs anzeigen. Im folgenden Listing sehen Sie die Übersicht über alle GPOs die momentan in der Domäne existieren:

```
 root@samba4-1:~# samba-tool gpo listall -Uadministrator
Password for [EXAMPLE\administrator]:
GPO          : {31B2F340-016D-11D2-945F-00C04FB984F9}
display name : Default Domain Policy
path         : \\example.net\sysvol\example.net\Policies\{31B2F340-016D-11D2-945F-\
  00C04FB984F9}
dn           : CN={31B2F340-016D-11D2-945F-00C04FB984F9},\
  CN=Policies,CN=System,DC=example,DC=net
version      : 0
flags        : NONE

GPO          : {6AC1786C-016F-11D2-945F-00C04FB984F9}
display name : Default Domain Controllers Policy
path         : \\example.net\sysvol\example.net\Policies\{6AC1786C-016F-11D2-945F-\
  00C04FB984F9}
dn           : CN={6AC1786C-016F-11D2-945F-00C04FB984F9},\
  CN=Policies,CN=System,DC=example,DC=net
version      : 0
flags        : NONE

GPO          : {3B02FC37-3901-4BCB-913B-6B9C620CA1E6}
display name : Systemsteuerung
path         : \\example.net\SysVol\example.net\Policies\{3B02FC37-3901-4BCB-913B-\
  6B9C620CA1E6}
dn           : CN={3B02FC37-3901-4BCB-913B-6B9C620CA1E6},\
  CN=Policies,CN=System,DC=example,DC=net
version      : 65536
flags        : NONE
```

Hier sehen Sie, dass jetzt neben den beiden Standard-GPOs auch noch die vorher angelegt GPO sichtbar ist. GPOs werden als Verzeichnisse im Dateisystem abgelegt. Die Verzeichnisse für die Gruppenrichtlinen finden Sie in dem Verzeichnis */var/lib/samba/sysvol/example.net/Policies*. Bei dem Verzeichnis *sysvol* handelt es sich um die gleichnamige Freigabe die später auf alle DC der Domäne repliziert werden muss.
Natürlich können Sie sich auch anzeigen lassen, welche Gruppenrichtlinen für einen bestimmten Benutzer wirksam sind. Das sehen Sie in dem folgenden Listing:

```
root@samba4-1:~# samba-tool gpo list skania -Uadministrator
Password for [EXAMPLE\administrator]:
GPOs for user skania
    Systemsteuerung {3B02FC37-3901-4BCB-913B-6B9C620CA1E6}
    Default Domain Policy {31B2F340-016D-11D2-945F-00C04FB984F9}
```

Die GPO `Systemsteuerung` wurde ja im letzten Abschnitt der Gruppe `Buchhaltung` zugewiesen. Der Benutzer `skania` ist Mitglied der Gruppe und somit ist die GPO für ihn auch relevant.
Alle OUs auf die diese GPO verlinkt wurde können Sie sich so wie im folgenden Listing auflisten lassen:

```
root@samba4-1:~# samba-tool gpo listcontainers {3B02FC37-3901-4BCB-913B-6B9C620CA1E6}\
  -Uadministrator
Password for [EXAMPLE\administrator]:
Container(s) using GPO {3B02FC37-3901-4BCB-913B-6B9C620CA1E6}
    DN: OU=Buchhaltung,DC=example,DC=net
```

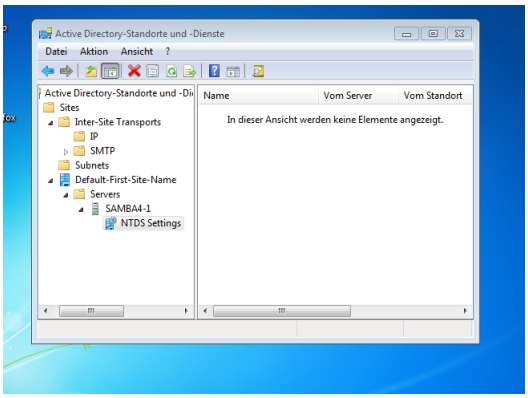
Leider können Sie an dieser Stelle nicht den Namen der GPO verwenden sondern müssen den eindeutigen Schlüssel verwenden. An dieser Stelle soll die Verwaltung der GPOs über die Kommandozeile nicht weiter ausgeführt werden. Sie haben aber auch die Möglichkeit GPOs zu erstellen und zu löschen und zu verändern, diese Aufgaben sind aber viel einfacher über die RSAT zu realisieren.

14.3 Aufgaben

- Erstellen Sie einen neuen Container für Ihre Gruppenrichtlinen und die zu verwaltenden Objekte.
- Erstellen Sie eine neue Gruppe für die Sie eine neue Gruppenrichtline erstellen wollen.
- Verschieben Sie zwei Benutzer in den neuen Container und fügen Sie diese zu Ihrer neuen Gruppe hinzu.
- Erstellen Sie eine neue benutzerbezogene Gruppenrichtlinie, in der es nicht mehr möglich ist, den Bildschirmhintergrund zu verändern.
- Weisen Sie der Gruppe dieser neuen Gruppenrichtline zu.
- Testen Sie, ob die Gruppenrichtlinie für die Mitglieder der Gruppe wirksam ist.

15 Sites

Wenn Ihr Unternehmen an verschiedenen Standorten Filialen hat, können Sie über die Verwaltung von *Sites* auch unter samba4 vornehmen. Dabei können Sie die verschiedenen Server Ihres Unternehmens auf die entsprechenden Standorte verteilen und die Replikation steuern. Die Verwaltung der Standorte führen Sie mit dem RSAT *Active Directory-Standorte und Dienste* durch. In der folgenden Abbildung sehen Sie die derzeitige Einstellung.



Wenn Sie weitere Server in Ihrem AD eingebunden haben, können Sie anschließend hier neue Standorte erstellen und die Server an diesen neuen Standort verschieben.

16 Clients in die Domäne aufnehmen

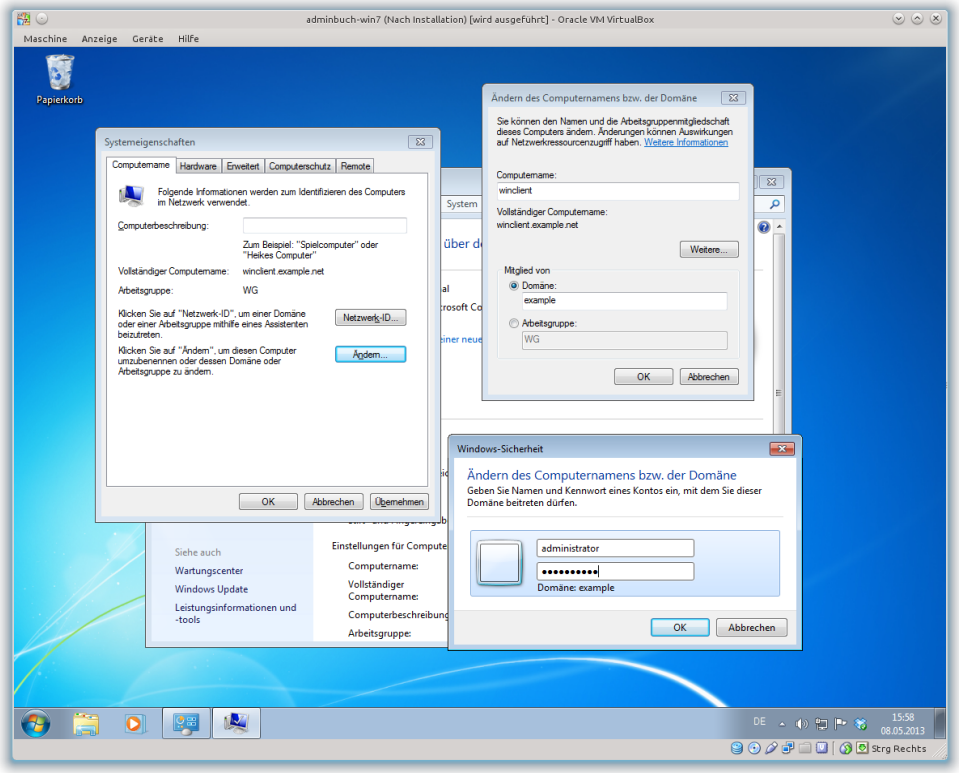
Jetzt geht es darum Windows- und Linux-Clients so in die Domäne aufzunehmen, dass sich Benutzer an beiden Systemen anmelden können und den Zugriff auf ihre Daten erhalten.

16.1 Windows7-Client in die Domäne aufnehmen

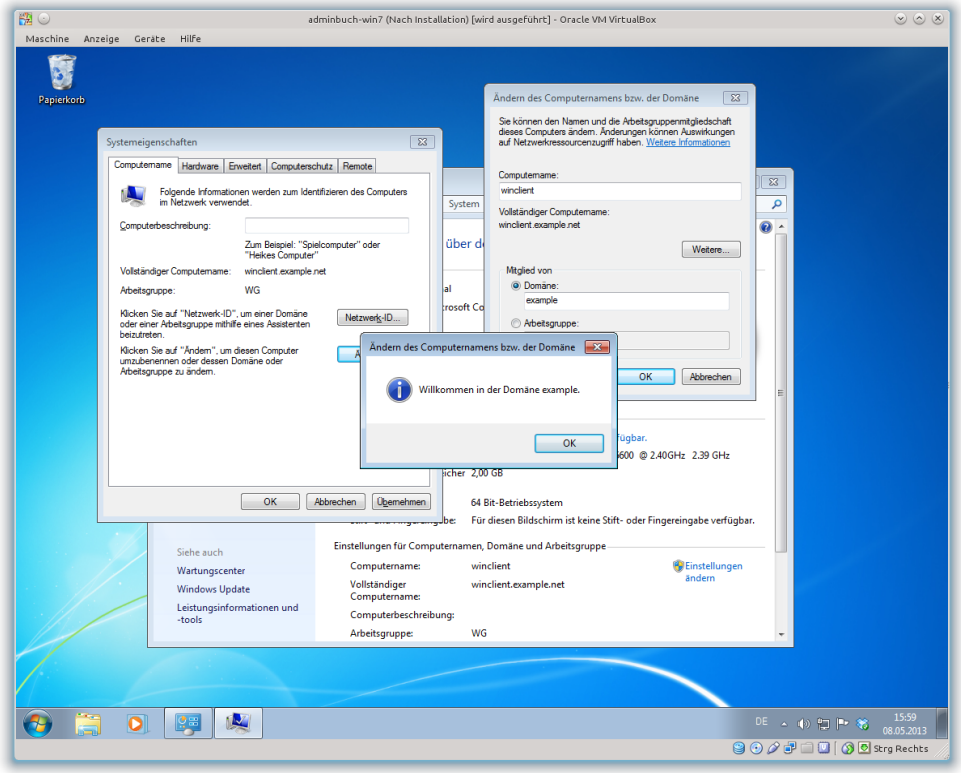
Da samba4 genau wie ein Windows-Server mit AD reagiert, ändert sich beim hinzufügen einer Workstation zur Domäne nichts im Vergleich zu einem Windows-Server.
Hinweis !

Bei der Verwendung von älteren samba4-Versionen als DC müssen Sie für Windows7 noch den Patch für die Registry einspielen. Gehen Sie dazu auf die URL `https://bugzilla.samba.org/attachment.cgi?id=4988&action=view` laden den Registrypatch herunter und installieren diesen auf dem Windows7-System

Melden Sie sich als lokaler Administrator an Ihrer Windows 7 Workstation klicken Sie anschließend auf *Start* und klicken dann mit der rechten Maustaste auf *Computer -> Eigenschaften*. Dort finden Sie die Schaltfläche *Einstellungen Ändern*. Durch einen Klick auf die Schaltfläche öffnet sich ein neues Fenster. In diesem Fenster können Sie den *NetBIOS-Name* und die Zugehörigkeit zur Domäne ändern. Achten Sie darauf, dass bei `Vollständiger Computername:` der *fqdn* des Clients eingetragen ist. Zum Beitritt der samba4-Domäne klicken Sie auf die Schaltfläche *Ändern...*. In dem neuen Fenster wählen Sie den Punkt *Domäne:* aus und geben den Domänennamen an. Hier wird der *NetBIOS-Name* der Domäne verlangt. In dieser Unterlage lautet der `example`. Klicken Sie anschließend auf die Schaltfläche *OK*. Es erscheint ein Fenster, in dem Sie den Benutzername, in diesem Fall `administrator`, und dessen Passwort eingeben müssen. In der folgenden Abbildung sehen Sie alle Fenster für den Vorgang:



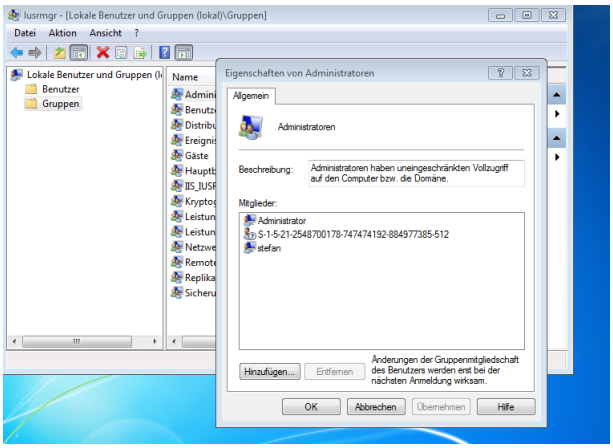
Nach einem Klick auf die Schaltfläche *OK* dauert es eine Weile und Sie erhalten die Meldung `Willkommen in der Domäne example`, so wie Sie es in der folgenden Abbildung sehen:



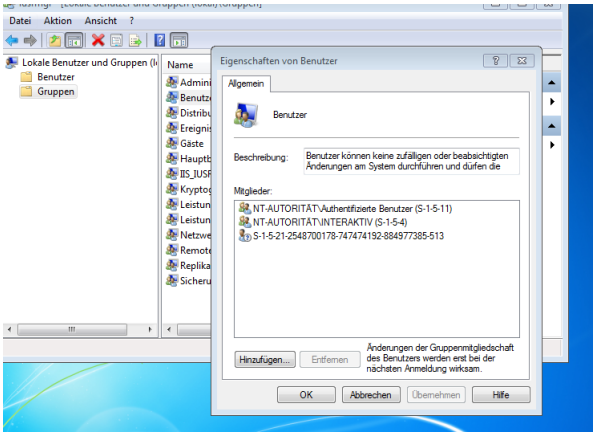
Hinweis !

Sollte das Hinzufügen zur Domäne nicht funktionieren, weil Windows den Domaincontroller nicht finden kann, prüfen Sie, ob der richtige DNS-Server in der Netzwerkkonfiguration des Clients eingestellt ist. Es muss hier ein DNS-Server der Domäne eingetragen sein.

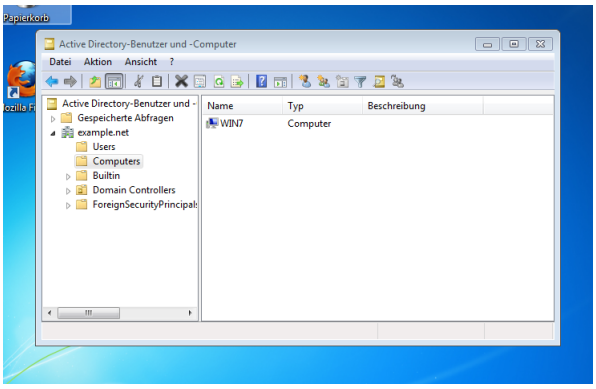
Um die Einstellung wirksam werden zu lassen, müssen Sie Windows neustarten. Nach dem Neustart haben Sie jetzt die Möglichkeit, sich in der Domäne anzumelden. Was passiert noch auf dem Client?
Beim hinzufügen eines Clients wird neben den Domäneninformationen noch an zwei lokalen Gruppen der Maschine Änderungen vorgenommen. Starten Sie den Manager für lokale Gruppen und Benutzer `lusrmgr` auf dem Windows-System klicken anschließend auf *Gruppen* und dann auf die Gruppe `Administratoren`, dort werden Sie, neben dem lokalen Administrator noch einen weiteren Eintrag sehen. Diese Eintrag wir eventuell nur mit dem SID angezeigt. An dem RID, mit dem Wert 512, am Ende des SID sehen Sie, dass es sich dabei um die Gruppe der `Domänenadmins` aus der AD-Domäne handelt. In der folgenden Abbildung sehen Sie ein Beispiel dazu:



die zweite Gruppe die verändert wird, ist die lokale Gruppe `Benutzer`. Hier wird die Gruppe der `Domänenbenutzer` beim Domänenbeitritt hinzu gefügt. Auch dort wird eventuell nur der SID angezeigt. In der folgenden Abbildung sehen Sie auch hierzu ein Beispiel:



Damit ist die Aufnahme einer Windows-Workstation zur Domäne abgeschlossen. Über diesen Weg können Sie jetzt alle Arbeitsstationen zur Domäne hinzufügen. Wenn Sie eine Workstation zur Domäne hinzugefügt haben, können Sie die Workstation hinterher auch im AD finden. Alle Ihre Workstations werden automatisch im AD angelegt. Wo Sie Ihre Workstations finden, sehen Sie in der folgenden Abbildung:



Über die Eigenschaften der Workstation können Sie diese jetzt auch an einen anderen Standort im AD verschieben, wenn Sie mit verschiedenen Standorten arbeiten.

16.2 Einen Linux-Client in den AD einbinden

Ein Linux-Client lässt sich nicht so in eine AD-Domäne einbinden wie ein Windows-Client, aber der Linux-Client kann die Authentifizierung auch über AD durchführen. Dazu müssen Sie lediglich PAM konfigurieren und den Kerberos-Client. In diesem Abschnitt geht es darum, die Authentifizierung des Linux-Clients zu konfigurieren. Damit der Linux-Client die Benutzer und Gruppen aus dem AD lesen und zur Authentifizierung nutzen kann, müssen Sie den Dienst *winbind* installieren und dafür sorgen, dass PAM die Authentifizierung über *winbind* durchführen kann. Dazu müssen Sie das entsprechende PAM-Modul installieren.
Im folgenden Listing sehen Sie, was passieren würde, wenn Sie die Installation der entsprechenden Pakete jetzt so durchführen würden:

```
 root@linux-client:~# apt-get install winbind libpam-winbind
Paketlisten werden gelesen... Fertig
Abhängigkeitsbaum wird aufgebaut.
Statusinformationen werden eingelesen.... Fertig
Die folgenden zusätzlichen Pakete werden installiert:
  libnss-winbind libtalloc2 libtdb1 libwbclient0 samba-common samba-common-bin
Die folgenden NEUEN Pakete werden installiert:
  libnss-winbind libpam-winbind libtalloc2 libtdb1 libwbclient0 samba-common\
samba-common-bin winbind
0 aktualisiert, 8 neu installiert, 0 zu entfernen und 0 nicht aktualisiert.
Es müssen 7.238 kB an Archiven heruntergeladen werden.
Nach dieser Operation werden 34,9 MB Plattenplatz zusätzlich benutzt.
```

Hier sehen Sie, dass die Paktet für den Samba3 installiert werden sollen.
Da alle System mit samba4 installiert werden sollen, dürfen Sie diese Pakete nicht installieren. Sondern müssen, so wie schon auf dem samba4-Server, das System für die Verwendung der SerNet-Pakte vorbereiten und diese installieren. Kopieren Sie hierfür die Zeilen für die SerNet-Pakete aus der Datei /etc/apt/sources.list vom samba4-Server in die Datei auf dem Client. Installieren Sie die entsprechenden public-keys zu den Paketlisten. Führen Sie dann das Kommando `apt-get update` aus. Anschießend können Sie das Paket sernet-samba-winbind und das Paket sernet-samba installieren Das Pakete sernet-samba benötigen Sie, da sich in dem Paket die benötigten Programme befinden um zum Beispiel der Domäne beitreten zu können. Im folgenden Listing sehen Sie die Installation der Pakete und deren Abhängigkeiten:

```
root@linux-client:~# apt-get install sernet-samba-winbind sernet-samba
Paketlisten werden gelesen... Fertig
Abhängigkeitsbaum wird aufgebaut.
Statusinformationen werden eingelesen.... Fertig
Die folgenden zusätzlichen Pakete werden installiert:
  dbus libavahi-client3 libavahi-common-data libavahi-common3 libcups2 libdbus-1-3\
  libdm0 libfam0 libreadline5 libsystemd-login0 sernet-samba-client\
  sernet-samba-common sernet-samba-libs\
  sernet-samba-libsmbclient0 sernet-samba-libwbclient0 xfsdump xfsprogs
Vorgeschlagene Pakete:
  dbus-x11 cups-common fam sernet-samba-ad acl attr quota
Die folgenden NEUEN Pakete werden installiert:
  dbus libavahi-client3 libavahi-common-data libavahi-common3 libcups2 libdbus-1-3\
  libdm0 libfam0 libreadline5 libsystemd-login0 sernet-samba sernet-samba-client\
  sernet-samba-common sernet-samba-libs\
  sernet-samba-libsmbclient0 sernet-samba-libwbclient0 sernet-samba-winbind\
  xfsdump xfsprogs
0 aktualisiert, 19 neu installiert, 0 zu entfernen und 49 nicht aktualisiert.
Es müssen 12,7 MB an Archiven heruntergeladen werden.
Nach dieser Operation werden 37,9 MB Plattenplatz zusätzlich benutzt.
Möchten Sie fortfahren [J/n]?
```

Im nächsten Schritt muss dann der *winbind* noch konfiguriert werden. Dazu müssen Sie die Datei /etc/samba/smb.conf erstellen und mit dem Inhalt aus dem folgenden Listing füllen:

```
[global]
      workgroup = example
      realm = EXAMPLE.NET
      security = ADS
      winbind separator = +
      winbind enum users = yes
      winbind enum groups = yes
      winbind use default domain = yes
      winbind refresh tickets = Yes
      template shell = /bin/bash
      idmap config * : range = 1000000 - 1999999
      idmap config EXAMPLE : backend = rid
      idmap config EXAMPLE : range =  1000000 - 1999999
```

Die Datei ist zu diesem Zeitpunkt nicht vorhanden, sie müssen die Datei neu anlegen. Die Parameter haben die folgenden Bedeutungen:

- `workgroup = example`

  Hier wird der NetBIOS-Name der Domäne angegeben. Auch als Mitglied im AD heißt der Parameter `workgroup`.

- `realm = EXAMPLE.NET`

  Bei dem `realm` handelt es sich um die Information für die Kerberos-Domäne. Für diesen realm wird sich der Samba-Server einen KDC suchen.

- `security = ADS`

  Damit legen Sie fest, dass Ihr Server ein Mitglied in einer AD-Domäne ist.

- `winbind separator = +`

  Normalerweise werden die Benutzer vom *winbind* in der Form `DOMÄNE/Benutzer` dargestellt. Da der Schrägstrich aber im Dateisystem verwendet wird, ist es sinnvoll, das Zeichen durch ein anderes Zeichen, hier das plus, zu ersetzen.

- `winbind enum users = yes`

  Ohne diesen Parameter würden die Benutzer auf dem lokalen Linux-System nicht angezeigt und wären nicht nutzbar um Rechte im Dateisystem vergeben zu können.

- `winbind enum groups = yes`

  Auch hier sorgt der Parameter dafür, dass Ihre Gruppen im Linux-System sichtbar sind und für Berechtigungen verwendbar sind.

- `winbind use default domain = yes`

  Haben Sie nur eine Domäne, können Sie mit diesem Parameter dafür sorgen, dass nur die Benutzername von winbind übergeben werden, ohne die Domäne vor den Namen zu stellen. Wenn Sie diesen Parameter nutzem, können Sie den Parameter `winbind separator = +` aus der Konfigurationsdatei entfernen.

- `winbind refresh tickets = yes`

  Mit diesem Parameter werden Kerberos-Tickets automatisch erneuert wenn der Benutzer angemeldet ist und das Ticket abläuft.

- `template shell = /bin/bash`

  Diesen Parameter dürfen Sie auf gar keinen Fall vergessen. Ohne diesen Parameter kann sich ein Benutzer aus dem AD zwar anmelden, aber er wird sofort wieder abgemeldet, da der Benutzer im AD keine Shell zugewiesen bekommt, diese aber für eine erfolgreiche Anmeldung benötigt wird.

- `idmap config * : range = 1000000 - 1999999`

  Neben den Gruppen und Benutzern die Sie als Administrator anlegen, gibt es noch die *Build-in-Groups* diese Gruppen haben einen eigenen verkürzten SID. Für diese Gruppen müssen Sie auch das ID-Mapping konfigurieren. Die Konfiguration der *Build-in-Groups* wird über den Stern in `idmap config * : range = 1000000 - 1999999` Konfiguriert. Eigentlich müssten Sie auch noch den Parameter *idmap config * : backend = tdb* Konfigurieren, aber dieser Parameter wird vom samba4 automatisch gesetzt. Testen können Sie das mit dem Kommando `testparm`.

- `idmap config EXAMPLE : backend = rid`

  Die IDs der Benutzer müssen ja aus den SIDs der AD-Benutzer generiert werden. Dazu gibt es verschiedene Möglichkeiten. Die Standardeinstellungen für den Winbind ist die Verwendung von tdb-Dateien. Dabei werde zufällige ID generiert und den Benutzers zugewiesen und in der tdb-Datei gespeichert. Der Nachtteil dieses Verfahrens ist der, dass so jeder Benutzer auf jedem Linux-System eine andere ID bekommt. Durch den Wechsel auf das Backend `idmap_rid` wird immer der RID des Benutzers aus der AD-Domäne gewählt. Da dieser eindeutig ist, ist die ID der Benutzer und Gruppen auf dem Linux-System auch eindeutig. Der Benutzer hat dadurch auf allen Linux-System in der gesamten Domäne immer die selbe ID. Ein Problem bekommen Sie so aber nicht in den Griff, und zwar werden auf den DCs Ihrer Domäne die IDs immer im AD verwaltet und somit immer anders als auf den anderen Systemen in der Domäne. Die einfachste Möglichkeit dieses Problem zu umgehen ist die, die Domain-Controller nicht als File-Server zu verwenden und alle Dateien immer auf anderen Samba-Servern in der Domäne abzulegen.

- `idmap config EXAMPLE : = 1000000 - 1999999`

  Hier legen Sie den Bereich fest in dem sich die ID der Benutzer befinden sollen.

Jetzt können Sie mit dem Linux-Client der Domäne beitreten. Im folgenden Listing sehen Sie, wie Sie über die Kommandozeile den Linux-Client in die AD-Domäne bringen:

```
root@linux-client:~# net rpc join EXAMPLE -U administrator
Enter administrator's password:
Joined domain EXAMPLE.
```

Wenn Sie jetzt den *winbind* starten wollen, erhalten Sie den folgenden Hinweis:

```
root@linux-client:~# service sernet-samba-winbindd start
/etc/init.d/sernet-samba-winbindd wants to start but SAMBA_START_MODE is set to "none".
Disable /etc/init.d/sernet-samba-winbindd or set SAMBA_START_MODE in
/etc/default/sernet-samba to "classic".
[warn] Exiting gracefully now. ... (warning).
```

Sie müssen erst noch die Datei /etc/default/sernet-samba wie im folgenden Listing anpassen:

```
# SAMBA_START_MODE defines how Samba should be started. Valid options are one of
#   "none"    to not enable it at all,
#   "classic" to use the classic smbd/nmbd/winbind daemons
#   "ad"      to use the Active Directory server (which starts the smbd on its own)
# (Be aware that you also need to enable the services/init scripts that
# automatically start up the desired daemons.)
SAMBA_START_MODE="classic"
```

Da hier ja nur ein Client oder ein Fileserver konfiguriert werden soll, müssen Sie hier den Wert `classic` einsetzen. Jetzt können Sie den *winbind* starten und bekommen dann die Meldungen wie im folgenden Listing:

```
root@linux-client:~# service sernet-samba-winbindd start
[ ok ing SAMBA winbindd : .
```

Mit dem Kommando `wbinfo -u` sehen Sie jetzt alle Benutzer aus der AD-Domäne. Mit dem Kommando `wbinfo -g` sehen Sie alle Gruppen der AD-Domäne. Im folgenden Listing sehen Sie ein Beispiel dafür:

```
root@linux-client:~# wbinfo -u
ktom
administrator
skania
krbtgt
guest

root@linux-client:~# wbinfo -g
allowed rodc password replication group
enterprise read-only domain controllers
denied rodc password replication group
read-only domain controllers
group policy creator owners
ras and ias servers
domain controllers
buchhaltung
enterprise admins
domain computers
cert publishers
```

```
dnsupdateproxy
domain admins
domain guests
schema admins
domain users
dnsadmins
alleuser
```

Jetzt müssen Sie die Benutzer und Gruppen noch im Linux-System bekannt machen. Dazu muss die Datei /etc/nsswitch.conf wie im folgenden Listing angepasst werden:

```
  passwd compat winbind
  group  compat winbind
```

Wenn Sie jetzt das Kommando `getent passwd` und `getent group` verwenden, werden Ihnen die Benutzer und Gruppen aus der AD-Domäne als Linux-Benutzer angezeigt. Im folgenden Listing sehen Sie das Ergebnis des Kommandos `getent passwd`:

```
root@linux-client:~# getent passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
.
.
.
statd:x:102:65534::/var/lib/nfs:/bin/false
sshd:x:103:65534::/var/run/sshd:/usr/sbin/nologin
stka:x:1000:1000:stka,,,:/home/stka:/bin/bash
messagebus:x:104:107::/var/run/dbus:/bin/false
ktom:*:1001106:1000513:Kater Tom:/home/EXAMPLE/ktom:/bin/bash
administrator:*:1000500:1000513:Administrator:/home/EXAMPLE/administrator:/bin/bash
skania:*:1001105:1000513:Stefan Kania:/home/EXAMPLE/skania:/bin/bash
krbtgt:*:1000502:1000513:krbtgt:/home/EXAMPLE/krbtgt:/bin/bash
guest:*:1000501:1000514:Guest:/home/EXAMPLE/guest:/bin/bash
```

Wenn Sie die UIDs Benutzer jetzt mit dem RIDs der AD-Benutzer vergleichen, sehen Sie, dass beide identisch sind. Mit dem Kommando `tdbdump` können Sie sich das Mapping auch anzeigen lassen. Im folgenden Listing sehen Sie einen Ausschnitt aus dem Kommando:

```
root@samba4-1:~# tdbdump /var/lib/samba/winbindd.tdb
{
key(47) = "U/S-1-5-21-2272618568-2628634020-1511971479-501"
data(146) = "\00\00\00\00M\0F\00\00i\E0\F7Q\00\00\00\00\05Guest\05Guest\0B\
            /home/%D/%U\09/bin/bash\FF\FF\FF\FF-S-1-5-21-2272618568-2628634020\
            -1511971479-501-S-1-5-21-2272618568-2628634020-1511971479-514"
}
{
key(47) = "U/S-1-5-21-2272618568-2628634020-1511971479-502"
data(148) = "\00\00\00\00M\0F\00\00i\E0\F7Q\00\00\00\00\06krbtgt\06krbtgt\0B\
            /home/%D/%U\09/bin/bash\FF\FF\FF\FF-S-1-5-21-2272618568-2628634020\
            -1511971479-502-S-1-5-21-2272618568-2628634020-1511971479-513"
}
{
key(17) = "GL/BUILTIN/domain"
data(20) = "\00\00\00\00<\DF\F7Q\B6\E0\F7Q\00\00\00\00\00\00\00\00"
```

```
}
{
key(17) = "NS/EXAMPLE/SKANIA"
data(67) = "\00\00\00\00M\0F\00\00i\E0\F7Q\00\00\00\00\01\00\00\00.\
           S-1-5-21-2272618568-2628634020-1511971479-1105"
}
```

Hier sehen Sie, das der Benutzer `skania` den RID 1105 hat und als UID die 1001105. Der Wert setzt sich aus dem Eintrag in der Datei smb.conf `idmap config EXAMPLE : range = 1000000 - 1999999` und dem RID des Benutzers zusammen. **Hinweis !**

Sollten die UIDs jetzt nicht mit den RIDs der Benutzer übereinstimmen oder Sie an der Stelle der IDs bei `getent` den Wert 4294967295 sehen. Liegt es wahrscheinlich an der smb.conf. Überprüfen Sie die Parameter erneut. Da der *winbind* aber alle Informationen in einem Cache ablegt, müssen Sie diesen erst mit dem Kommando `net cache flush` löschen.

16.2.1 Konfiguration der Authentifizierung

Damit sich jetzt auch die Benutzer am System anmelden können, müssen Sie noch das PAM-System und der Kerberos-Client konfiguriert werden.
Installieren Sie als erstes das Paket heimdal-clients mit alle Abhängigkeiten. Für die Konfiguration des Kerberos-Clients können Sie sich die Datei krb5.conf einfach von einem anderen Client oder einem DC kopieren, da diese Datei immer identisch ist.
Hinweis !

Denke Sie daran, dass Sie für die Verwendung von Kerberos eine einheitliche Zeit benötigen und das die Namensauflösung mittels DNS funktionieren muss. Tragen Sie deshalb den neuen Client auf jeden Fall in den DNS ein.

Nach der Installation und der Konfiguration können Sie den Kerberos-Client testen, in dem Sie für einen Benutzer ein Ticket anfordern, so wie Sie es im folgenden Listing sehen können:

```
root@linux-client:/etc# kinit administrator
administrator@EXAMPLE.NET's Password:
root@linux-client:/etc# klist
Credentials cache: FILE:/tmp/krb5cc_0
        Principal: administrator@EXAMPLE.NET

  Issued                Expires               Principal
Jul 30 14:56:55 2013  Jul 31 00:56:55 2013  krbtgt/EXAMPLE.NET@EXAMPLE.NET
```

Damit ist die Konfiguration des Kerberos-Clients abgeschlossen und Sie können mit der PAM-Konfiguration fortfahren.
Zwar bringt das Winbind-Paket von SerNet das entsprechenden PAM-Modul mit, das Modul wird aber nicht sofort in die Konfigurationsdateien des PAM-Systems eingebunden. Dafür müssen Sie an dieser Stelle selber sorgen. Die Dateien die Sie anpassen müssen, finden Sie im Verzeichnis /etc/pam.d

- Die Datei common-auth

```
# for winbind start
auth sufficient pam_winbind.so
```

```
auth sufficient pam_unix.so nullok_secure use_first_pass
#auth   [success=1 default=ignore]      pam_unix.so nullok_secure
# for winbind end

# here's the fallback if no module succeeds
auth    requisite                       pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
auth    required                        pam_permit.so
```

- Die Datei common-account

```
# for winbind start
account sufficient pam_winbind.so
# for winbind end

account [success=1 new_authtok_reqd=done default=ignore]        pam_unix.so
# here's the fallback if no module succeeds
account requisite                       pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
account required                        pam_permit.so
```

Warnung !

Achten Sie beim Editieren der Dateien genau auf die Syntax. Wenn Sie in den Dateien einen Fehler haben, kann es passieren, dass Sie sich an dem System nicht mehr anmelden können. Deshalb sollten Sie immer eine *root-Konsole* geöffnet halte bis Sie alle Tests durchgeführt haben

Leider kommt jetzt noch ein Schritt den Sie unbedingt durchführen müssen. Die Authentifizierung der Benutzer über *winbind* und *Kerberos* funktioniert jetzt zwar, aber wenn Sie sich versuchen anzumelden, werden Sie direkt nach der Anmeldung sofort wieder abgemeldet. Das liegt daran, dass die Standardshell eines Linux-Benutzers `/bin/false` ist. Somit wird der Benutzer, bei einer Anmeldung über die Kommandozeile, direkt wieder abgemeldet. Darum müssen Sie den `[global]`-Bereich der smb.conf, auf allen DCs, um die folgende Zeile ergänzen:

```
template shell = /bin/bash
```

Jetzt ist der Linux-Client so konfiguriert, dass die Benutzer aus der AD-Domäne sich auch an den Linux-Clients anmelden können. Da die Freigaben noch nicht eingebunden sind, wird der Benutzer zu diesem Zeitpunkt noch ohne Heimatverzeichnisse angemeldet.

16.2.2 Aufgaben

- Installieren Sie einen neuen Linux-Client und binden diesen in die bestehende Domäne ein.
- Konfiguriere Sie den *winbind* so, dass das ID-Mapping über den *RID* der Benutzer und Gruppen durchgeführt wird.
- Konfigurieren Sie Kerberos und PAM so, dass die Benutzer aus dem AD sich an diesem Client auch anmelden können.

17 Zusätzliche Server in der Domäne

Natürlich können Sie weitere Server in die Domäne aufnehmen. In diesem Abschnitt soll es darum gehen, einen zweiten samba4-Server als DC in die Domäne einzubinden, einen dritten samba4-Server als Fileserver aufzunehmen und einen Windows-Server, sowohl als Fileserver als auch als DC, in die Domäne aufzunehmen.

17.1 Einrichten eines zusätzlichen Linux-Fileservers

Wie schon im Abschnitt 13 beschrieben kann es zu Problemen mit einheitlichen UIDs und GIDs kommen, wenn Sie Ihre Daten auf dem DC ablegen. Da auf dem DC ein eigenes ID-Mapping stattfindet. Um dieses Problem zu umgehen, macht es Sinn, alle Daten auf einem eigen Dateiserver abzulegen, inklusive der Heimatverzeichnisse der Benutzer und der Profilverzeichnisse der Benutzer. So haben Sie auch eine saubere Trennung der Benutzerverwaltung und Ihren Daten. Auch Microsoft empfiehlt DC und Dateiserver zu trennen. Durch diese Trennung haben Sie später keine Probleme mit einheitlichen UIDs und GIDs bei der Verwendung von Linux-Clients.
Damit Sie einen weiteren Server für die Daten der Benutzer in Ihre Domäne einbringen können, müssen Sie als erstes den Linux-Rechner wie im Abschnitt 16.2 als Domainmember installieren und konfigurieren. Dadurch bekommen Sie automatisch alle Benutzer und Gruppen der Domäne auf dem neuen Server angezeigt. Denken Sie auch an die Einstellungen in der Datei /etc/fstab um die ACL-Unterstützung für alle Dateisysteme einzutragen im folgenden Listing sehen Sie noch einmal diese Einstellungen:

```
UUID=140a4f78-5923-4962-88fd-1fc0c4dfa707 /  ext4 errors=remount-ro,user_xattr,acl 0  1
```

Hinweis !

Sollen sich Linux-Benutzer nicht direkt am Fileserver anmelden können, brauchen Sie den Kerberos-Client und PAM nicht konfigurieren.

Installieren Sie als erstes wieder die SerNet-Pakete sernet-samba-winbind und sernet-samba. Anschließend konfigurieren Sie den samba4 wie schon im Abschnitt 16.2 über die Datei smb.conf. Sorgen Sie dafür, dass der samba4 auch gestartet wird, in dem Sie die Datei /etc/default/sernet-samba anpassen und den samba4-Server im `classic`-Modus starten können. Starten Sie dann den *winbind* und treten der Domäne bei. Jetzt können Sie sich schon alle Benutzer der des ADs mit `wbinfo -u` anzeigen lassen. Damit Sie aber auch Rechte an die Benutzer im Dateisystem vergeben können, müssen Sie noch die Datei /etc/nsswitch.conf wie im folgenden Listing anpassen:

```
passwd:         compat winbind
group:          compat winbind
```

Anschließend können Sie sich mit `getent passwd` auch noch die gemappten Linux- Benutzer anzeigen lassen. Wenn Sie jetzt die UIDs der Benutzer auf dem Fileserver und denen auf dem Linux-Client vergleichen, werden Sie feststellen, dass die Benutzer auf beiden Systemen die selbe UID haben.

17.1.1 Umstellen der Heimatverzeichnisse

Nach dem jetzt sowohl die Samba- als auch die Linux-Benutzer auf dem Server bekannt sind, können Sie jetzt die Freigaben für die Heimatverzeichnisse erstellen. Jetzt ist es auch völlig gleich, ob sie für die Linux-System *cifs* oder *NFS* für die Heimatverzeichnisse verwenden. Als erstes wird nun wieder die Freigabe users erstellt, in der die Heimatverzeichnisse abgelegt werden sollen. Wie schon im Abschnitt 9.2 sollen die Freigaben auf dem neuen Fileserver in der Registry abgelegt werden. Dazu müssen Sie als erstes wieder die Datei smb.conf in der `[global]`-Section um die folgenden Zeile ergänzen:

```
registry shares = yes
```

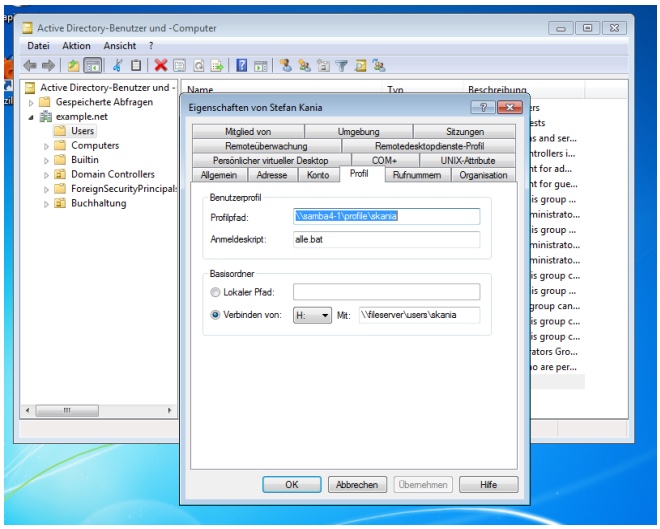
Da sonst keine Freigaben aus der Registry abgearbeitet werden. Legen Sie als nächstes das Verzeichnis /home/EXAMPLE/ an, da das die Freigabe für die Heimatverzeichnisse sein wird. Jetzt legen Sie, so wie im folgenden Listing, die Freigabe an:

```
root@fileserver:~# net conf addshare users /home/EXAMPLE writeable=y guest_ok=n "Home-Dirs"

root@fileserver:~# net conf setparm users "browsable" "no"

root@fileserver:~# net conf setparm users "create mask" "700"

root@fileserver:~# net conf setparm users "directory mask" "700"
```

Hinweis !

Achten Sie darauf, dass die Gruppe *domain admins* Schreibrecht an dem Verzeichnis /home/EXAMPLE hat. Sonst können die Heimatverzeichnisse der Benutzer nicht mit den RSAT angelegt werden.

Nach dem Sie jetzt die Freigabe eingerichtet haben, könne Sie jetzt aus den RSAT das Programm *Active Directory-Benutzer und -Computer* starten und den Benutzern ihr neues Heimatverzeichnisse auf dem neuen Fileserver zuweisen. In der folgenden Abbildung sehe Sie die Änderung:

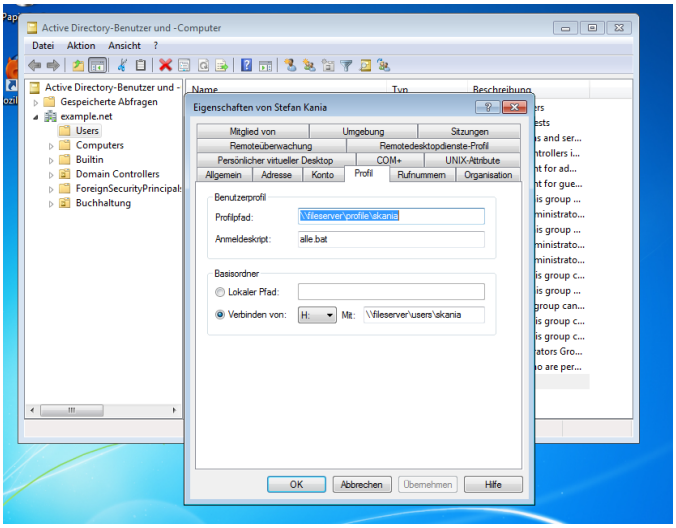


17.1.2 Umstellung der Profilverzeichnisse

Auch die Profile sollen vom DC auf den Fileserver umgezogen werden. Dazu erzeugen Sie wieder das Verzeichnis für die Profile und die Freigabe auf dem Fileserver wie im folgenden Listing:

```
root@fileserver:~# mkdir /profile

root@fileserver:~# chmod 777 /profile/

root@fileserver:~# net conf addshare profile /profile writeable=y guest_ok=n "User Profile"

root@fileserver:~# net conf setparm profile "browsable" "no"

root@fileserver:~# net conf setparm profile "profile acls" "yes"
```

Vergessen Sie hier auf gar keine Fall den Parameter `profile acls` zu setzen, da nur mit diesem Parameter die Freigabe für die Profile funktioniert. Nach dem Sie die Freigabe erzeugt haben, können Sie jetzt auch das Profilverzeichnis Ihrer Benutzer im RSAT *Active Directory-Benutzer und -Computer* wie in der folgenden Abbildung anpassen:



17.1.3 Weiter Freigaben

Selbstverständlich können Sie jetzt auch weitere Freigaben auf dem Server erstellen und über ein Logonskript den Benutzern zur Verfügung stellen. Auch hier ist es Sinnvoll, die Freigaben in der Registry einzutragen.
An einer kleinen Verzeichnisstruktur soll hier jetzt noch einmal auf die Vererbung der Rechte und die Besonderheit des Parameters `hide unreadable` eingegangen werden.
Als erstes legen Sie die Gruppen `buchhaltung`, `marketing` und `vertrieb` an, soweit diese in Ihrem System noch nicht vorhanden sind. Erstellen Sie anschließend die im folgenden Listing angezeigt Verzeichnisstruktur und vergeben die entsprechenden Rechte und weisen Sie den Verzeichnissen die entsprechenden Gruppen zu:

```
root@fileserver:~# tree -pg /daten/
/daten/
 [drwxrwxr-x domain admins]  abteilungen
     [drwxrwx--- buchhalt]  buchhaltung
     [drwxrwx--- marketin]  marketing
     [drwxrwx--- vertrieb]  vertrieb

4 directories, 0 files
```

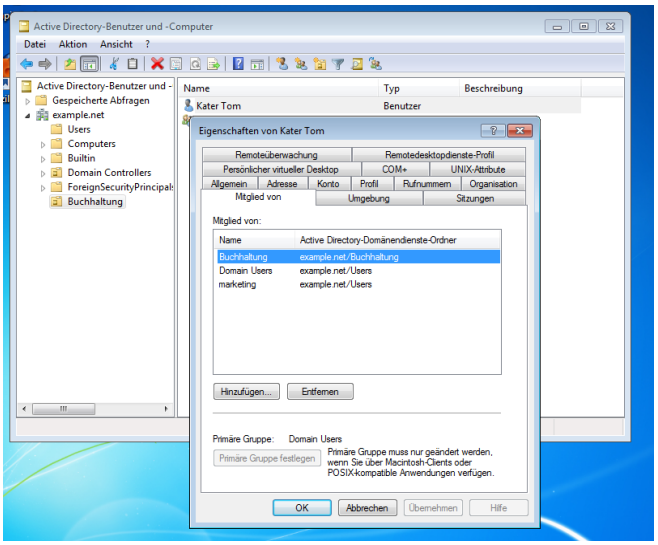
Im nächsten Schritt erstellen Sie die Freigabe so wie im folgenden Listing:

```
root@fileserver:~#  net conf addshare abteilungen /daten/abteilungen writeable=y\
                    guest_ok=n "Abteilungen"
root@fileserver:~# net conf setparm abteilungen "hide unreadable" "yes"
```

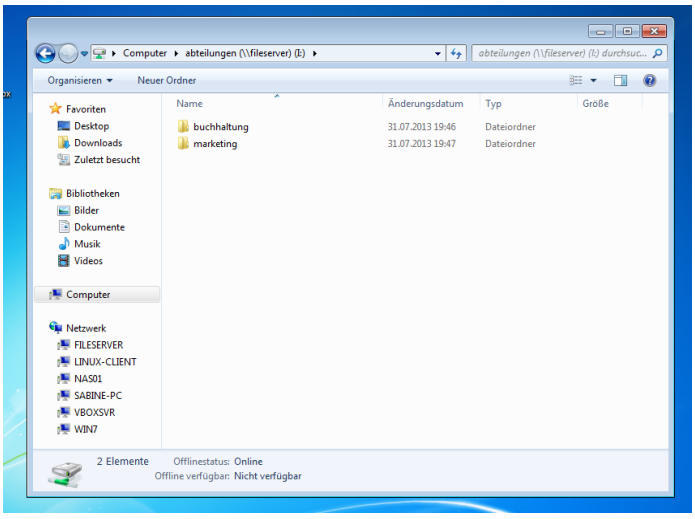
Erstellen Sie ein Logonskript mit der Zeile aus dem folgenden Listing:

```
net use i: \\fileserver\abteilungen /persistent:no
```

Weisen Sie allen Benutzern das Logonskript zu. In der folgenden Abbildung sehen Sie die Gruppenzugehörigkeit des Benutzers `Kater Tom`



Der Benutzer ist Mitglied der Gruppen `buchhaltung` und `marketing`, aber nicht der Gruppe `vertrieb`. Wenn Sie sich jetzt mit dem Benutzer anmelden und den Explorer öffnen, sehen Sie unter `Computer` ein Netzlaufwerk mit der Freigabe abteilungen sehen. Klicken Sie auf die Freigabe, sehen Sie dort nur die beiden Verzeichnisse buchhaltung und marketing, nicht aber das Verzeichnis vertrieb. In der folgenden Abbildung sehen Sie die Freigabe abteilungen beim Zugriff durch den Benutzer `Kater Tom`



17.1.4 Zugriff von Linux-Clients auf Samba-Freigaben

In einer heterogenen Client-Umgebung sollen auch die Linux-Clients die Freigaben des Samba-Servers nutzen können. Die Authentifizierung der Benutzer wird ja schon im Abschnitt 16.2 besprochen. Jetzt soll es darum gehen, dass auch die Freigaben genutzt werden können, so dass

die Benutzer auch unter Linux ihr Heimatverzeichnis und die Daten nutzen können.
Für die Datenfreigabe auf den Linux-Clients haben Sie jetzt zwei Möglichkeiten, Sie können *cifs* verwenden und damit smb-Protokoll des Samba-Servers oder aber zusätzlich einen *NFS-Server* einrichten. In diesem Seminar soll nur der Samba-Server für die Datenfreigabe genutzt werden.
Um *cifs* verwenden zu können, müssen Sie als erstes das Paket cifs-utils auf den Linux-Clients installieren, um überhaupt mit dem Kommando `mount` *cifs*-Freigaben mounten zu können. Bei der Verwendung von *cifs* wird beim Mounten des Dateisystems immer ein Benutzername und ein Passwort benötigt. Wenn immer nur eine Person einen Client nutzt, können Sie diese Information über eine Datei bei Systemstart übergeben. Das Problem ist dann nur, wenn der Benutzer sein Passwort ändert, muss die Datei auch geändert werden. Ein weiteres Problem tritt auf, wenn ein Benutzer die Freigabe mountet, sich abmeldet und sich dann ein anderer Benutzer anmeldet. Denn gemountete cifs-Freigaben gehören immer dem Benutzer, der sie gemountet hat. Aber *cifs* unterstützt auch die mount-Option `users`, mit der jeder Benutzer ein gemountetes Dateisystem dismounten kann, egal welcher Benutzer das Dateisystem vorher gemountet hat. Trotz aller dieser Nachteile hat *cifs* auch Vorteile gegenüber *NFS*. Die Datenübertragung findet verschlüsselt statt. *Cifs* ist stabiler und hat, ab der smb-Version 2.0 eine höhere Datendurchsatzrate. Die Einschränkungen zum Beispiel über den Parameter `hide unreadable = yes` sind auch für die Linux-Benutzer wirksam. Ein weiter Vorteil ist, Sie müssen nur einen Dienst für die Freigaben pflegen.
Zum Glück unterstützt cifs auch Kerberos für die Authentifizierung und mit samba4 wird auch die Kerberos-Authentifizierung angewendet. Dadurch können Sie das Problem mit der Anmeldung des Benutzers umgehen. Jeder Benutzer der sich am Linux-System anmeldet erhält automatisch ein *Ticket Granting Ticket (TGT)*, mit diesem *TGT* kann dann die Authentifizierung gegenüber dem Samba-Fileserver durchgeführt werden. Installieren Sie auf allen Linux-Clients das Paket libpam-heimdal. Änderungen an den PAM-Konfigurationsdateien müssen Sie nicht vornehmen wenn Sie bereits vorher die Authentifizierung über *winbind* eingerichtet haben und dafür die PAM-Konfigurationsdateien angepasst haben, werden Sie während der Installation des Paktes gefragt ob Sie die von Hand gemachten Änderungen rückgängig machen wollen. Sie sollten hier unbedingt die Änderungen rückgängig machen um Problemen mit dem PAM-System aus dem weg zu gehen.
Die Anmeldung wird auch mit den geänderten PAM-Einstellungen weithin funktionieren. Testen Sie anschließend die Anmeldung und prüfen Sie mit `klist`, ob der Benutzer auch sein *TGT* erhalten hat. Erst wenn das der Fall ist, sollten Sie weiter machen.
Damit Benutzer die Freigaben mounten können, müssen Sie bei dem Programm `/sbin/mount.cifs` das *SUID-Bit* mit `chmod u+s /sbin/mount.cifs` setzen, da sonst ein mounten der Dateisystem durch Benutzer nicht möglich ist.
Haben Sie die Voraussetzung bis zu diesem Punkt geschaffen, dann könne Sie jetzt das mounten testen. Im folgenden Listing sehen Sie verschieden Versuche Dateisystem zu mounten:

```
root@linux-client:~# mount -t cifs -o sec=krb5 //fileserver/abteilungen /abteilungen
mount error(126): Required key not available
Refer to the mount.cifs(8) manual page (e.g. man mount.cifs)

root@linux-client:~# su - skania

skania@linux-client:/$ klist
Credentials cache: FILE:/tmp/krb5cc_1001105
        Principal: skania@EXAMPLE.NET

  Issued                Expires               Principal
Aug  2 14:13:18 2013  Aug  3 00:12:29 2013  krbtgt/EXAMPLE.NET@EXAMPLE.NET

skania@linux-client:/$ mount -t cifs -o sec=krb5 //fileserver/abteilungen /abteilungen
mount: only root can do that
```

Was ist hier passiert? Im ersten Versuch, versucht der root das Dateisystem zu mounten, dieser Versuch scheitert daran, dass der root ein lokaler Benutzer ist und somit kein *TGT* besitzt. Dann

wird mit `su - skania` die Identität auf einen normalen Benutzer geändert und der selbe Befehl abgesetzt. Dieses mal scheitert der Mountversuch daran, dass nur der root mounten kann. Deshalb müssen Sie jetzt erst für normale Benutzer das Mounten ermöglichen. Dieses realisieren Sie, in dem sie den folgenden Eintrag in die Datei /etc/fstab erstellen:

```
//fileserver/abteilungen /abteilungen cifs users,sec=krb5 0 0
```

Durch die Option `users` ermöglichen Sie das Mounten dieses Dateisystems durch normale Benutzer. Weiterhin erlaubt die Option `users` gegenüber der Option `user`, dass jeder Benutzer jedes von einem anderen Benutzer gemountetes Dateisystem wieder dismounten kann. Jetzt kann der Benutzer das Dateisystem über den vereinfachten Mount-Befehl mounten, so wie Sie es im folgenden Listing sehen können:

```
skania@linux-client:/$ mount /abteilungen/
skania@linux-client:/$ mount
.
.
.
//fileserver/abteilungen on /abteilungen type cifs (rw,nosuid,nodev,relatime,sec=krb5,\
                        unc=\\fileserver\abteilungen,username=skania,\
                        uid=1001105,forceuid,gid=1000513,forcegid,addr=192.168.123.172,\
                        unix,posixpaths,serverino,acl,rsize=1048576,wsize=65536,actimeo=1)
```

Hier sehen Sie, das die Freigabe durch den Benutzer `skania` gemountet wurde. Alle Dateien und Verzeichnisse werden automatisch dem Benutzer zugewiesen. Aber die eigentliche Rechte bleiben erhalten, da diese auf dem Dateisystem des Servers verwaltet werden. Der Benutzer kann somit keine Dateien verändern an denn er keine Rechte hat. Auch bleiben die Einschränkungen der Freigabe erhalten. Bei der Einrichtung der Freigabe und der Berechtigten wurde ja in der Verzeichnis /abteilungen Unterverzeichnisse angelegt und bestimmten Gruppen zugeordnet. Der Benutzer `skania` ist nur Mitglied der Gruppe `vertrieb`. Deshalb wird der Benutzer auch in dem Verzeichnis /abteilungen nur das Unterverzeichnis vertrieb sehen, so wie im folgenden Listing:

```
skania@linux-client:/$ id
uid=1001105(skania) gid=1000513(domain users) Gruppen=1000513(domain users),\
                    1001111(vertrieb)

skania@linux-client:/$ ls -l /abteilungen/
insgesamt 0
drwxrwx--- 2 skania domain users 0 Aug  2 13:58 vertrieb
```

So können Sie jetzt alle Dateisystem eines Samba-Servers via *cifs* bereitstellen und mounten. Nur bleibt das Problem: Was passiert wenn der eine Benutzer sich abmeldet und sich ein andere Benutzer sich anmeldet? Im nachfolgenden Listing sehen Sie das Problem:

```
root@linux-client:~# su - ktom
-su: /home/EXAMPLE/ktom/.bash_profile: Keine Berechtigung

ktom@linux-client:~$ pwd
/home/EXAMPLE/ktom

ktom@linux-client:~$ ls -la
ls: lese Verzeichnis .: Keine Berechtigung
insgesamt 0

ktom@linux-client:~$ cd ..
```

```
ktom@linux-client:/home/EXAMPLE$ ls -la
insgesamt 4
drwxrwxr-x  5 skania domain users    0 Aug  1 11:17 .
drwxr-xr-x  4 root   root         4096 Aug  1 10:26 ..
drwxrwx---+ 4 skania domain users    0 Aug  1 11:14 ktom
drwxrwx---+ 2 skania domain users    0 Aug  1 11:20 ptau
drwxrwx---+ 2 skania domain users    0 Aug  1 14:23 skania
```

Der Benutzer `ktom` hat keine Rechte an seinem Verzeichnis, da das gemountete Dateisystem dem Benutzer `skania` gehört. Deshalb müssen Sie dafür sorgen, dass die Dateisystem beim abmelden der Benutzer dismountet und bei jeder Anmeldung neu gemountet werden.
Das Mounten der Dateisystem können Sie über die Datei /etc/profile realisieren, da diese bei jeder Anmeldung immer abgearbeitet wird. Das Dismounten der Dateisystem können sie über die Datei ~/.bash_logout regeln. Aber, wenn Sie das Heimatverzeichnis ebenfalls über *cifs* gemountet haben, ist das nicht möglich, da bei der Ausführung des Skripts der Benutzer noch angemeldet ist und das Dateisystem noch in Benutzung ist. Auch müssten Sie dann für jeden Benutzer eine Skript bereitstellen. Einfacher ist es, bei der Anmeldung bereits gemountete Dateisystem erst zu dismounten, was ja dank der Mount-Option `users`, möglich ist und dann die Dateisystem neu mounten. Ein sehr einfaches Beispiele dafür sehen Sie im folgenden Listing:

```
if [ "$USER" !=  "root" ]
then
        cd /
        umount /home/EXAMPLE 2>/dev/null
        umount /abteilungen 2>/dev/null
        sleep 1
        mount /home/EXAMPLE
        mount /abteilungen
        HOME=/home/EXAMPLE/$USER
        cd
fi
```

Hinweis !

Es gibt für *mount.cifs* die Option `multiuser`, damit wäre es theoretisch möglich den Benutzer je nach Anmeldung zu übergeben, dann müsste die Freigabe aber beim Systemstart vom *root* gemountet werden, der wiederum hat aber keinen Kerberos-key und kann sich für das Mounten nicht authentifizieren.

Diese if-Bedingung stellen Sie ans Ende der Datei /etc/profile. Für den Benutzer `root` wird der Teil des Skripts nicht ausgeführt, da der `root` kein *TGT* besitzt und somit ein mounten für ihn nicht möglich ist. Der Wechsel in die oberste Ebenen des Dateisystems muss aus dem Grund stattfinden, da bei einem gemounteten Dateisystem der Benutzer sofort in das Verzeichnis wechselt und somit ein dismount nicht möglich ist. Nach dem dismount kommt eine Pause von einer Sekunde, je nachdem wie schnell Ihr System ist, können Sie diese Pause auch weglassen. Anschließend werden alle Freigaben gemountet und die Variable `HOME` wird mit dem richtigen Wert belegt.
Jetzt werden alle Netzwerkdateisysteme ausschließlich über *cifs* gemountet und Sie benötigen kein NFS zusätzlich.

17.2 Einrichten eines zusätzlichen samba4 Domaincontrollers

Um die Anmeldung in Ihrem Netzwerk gegen Ausfälle zu sichern, sollten Sie immer mindestens zwei DCs in Ihrem Netzwerk haben. Auch wenn sich Ihre Domäne über mehrere Standorte verteilt, kann es Sinn machen, mehrere DCs im Einsatz zu haben. In diesem Abschnitt soll ein zusätzlicher

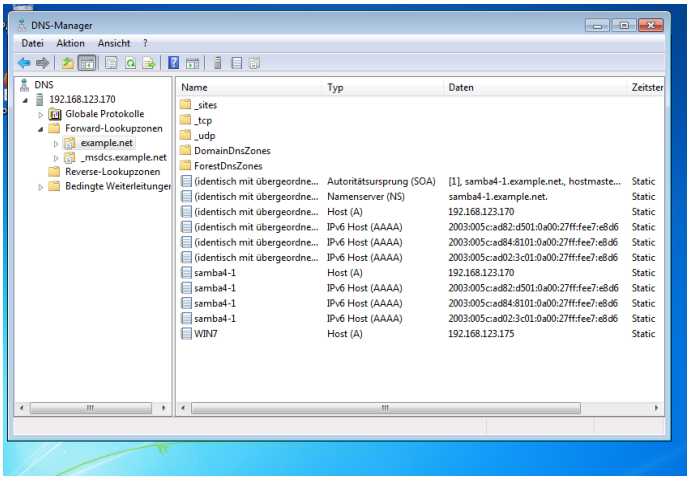
DC in die Domäne eingebunden werden. Ein Hauptaugenmerk wird dabei auf der Replikation der Freigabe sysvol liegen. Da in dieser Freigabe alle Informationen abgelegt sind, die auf allen DCs verfügbar sein müssen. Leider unterstützt samba4 noch keine Dateisystemreplikation, so dass diese Aufgabe mit einem externe Skript realisiert werden muss. Mehr dazu etwas später in diesem Abschnitt.

17.2.1 Installation des neuen DCs

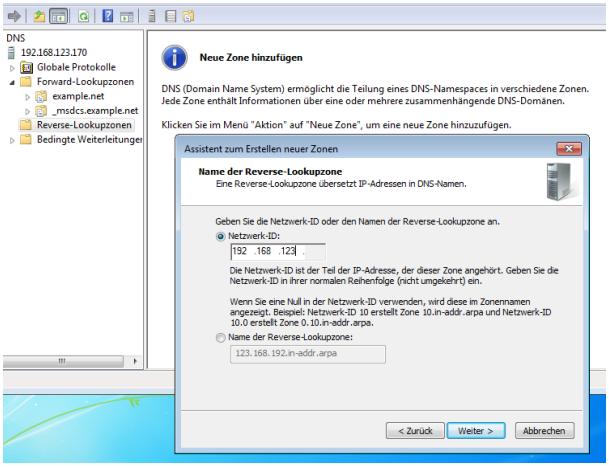
Als erstes installieren Sie ein Linux-System und binden das Repository der Firma SerNet ein und installieren dann wieder das Paket *sernet-samba-ad*.

17.2.2 Eintrag des neuen DC in den DNS

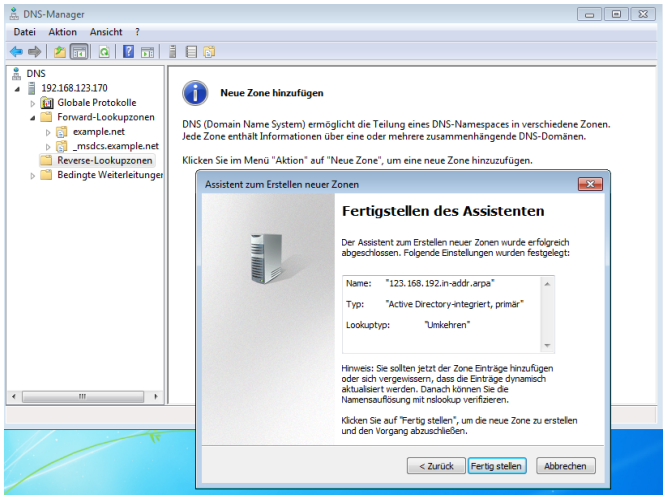
Damit die Kommunikation zwischen den DCs über die Namen möglich ist, sollten Sie an dieser Stelle erst den DNS um den neuen Server erweitern. Sollte bis zu diesem Zeitpunkt auch noch keine *reverse-Zone* in Ihrem DNS eingerichtet worden sein, können Sie diesen Schritt jetzt auch noch vornehmen. Dazu starten Sie, unter Windows, den *DNS-Manager*. Beim ersten Aufruf müssen Sie die IP-Adresse des Servers angeben, mit dem Sie sich verbinden wollen. Anschließend startet der DNS-Manager und Sie sehen Ihren Server. Ein Doppelklick auf den Server öffnet die untergeordnete Struktur. Dort sehen Sie die beiden Einträge `Forward-Lookupzone` und `Reverse-Lookupzone`. Wenn Sie beide Ordner öffnen, werden Sie sehen, dass bis zu diesem Zeitpunkt nur eine Forward-Zone verwaltet wird. Sehen Sie dazu die nächste Abbildung:



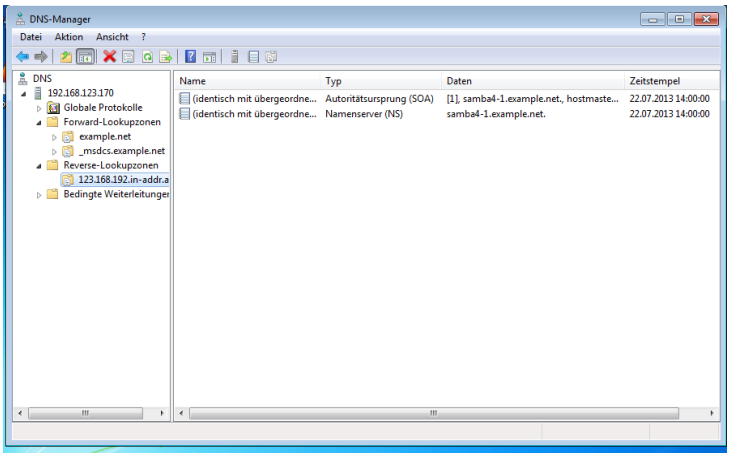
Mit einen Rechtsklick auf den Ordner `Reverse-Lookupzone` öffnet sich ein Kontextmenü, dort klicken Sie auf *`Neue Zone...`*. Dadurch starten Sie einen Assistenten für die Erstellung einer neuen Zone. Klicken Sie hier auf *`Weiter`*. Es öffnet sich ein neues Fenster, dort wählen Sie den Punkt `Primäre Zone` aus und klicken anschließend auf *`Weiter`*. Anschließend legen Sie fest, wie die Zonen repliziert werden sollen. Wählen Sie hier den Punkt `Auf alle DNS-Server, die auf Domänencontrollern dieser Domäne ausgeführt werden` aus und klicken anschließend auf *`Weiter`*. Im nächsten Fenster legen Sie fest, ob Sie eine IPv4 oder eine IPv6 Zone anlegen wollen. Wählen Sie die für Ihr Netz passende Auswahl und klicken Sie auf *`Weiter`*. Im nächsten Fenster geben Sie die Netzadresse Ihres Netzwerkes als `Netzwerk-ID` an. Daraus wird dann die neue Zone erstellt. In der folgenden Abbildung sehen Sie die entsprechenden Einstellungen:



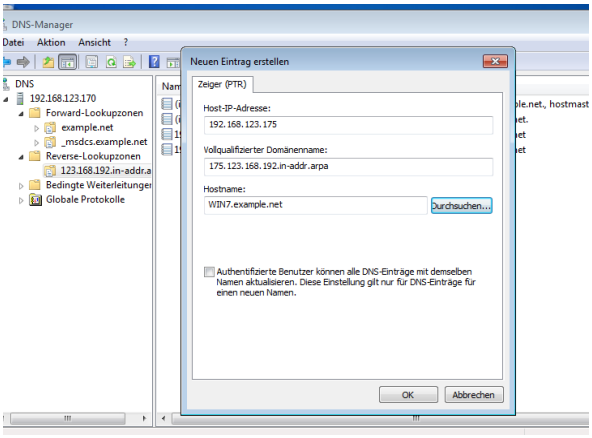
Klicken Sie anschließend auf ***Weiter***. Wählen Sie im nächsten Schritt den Punkt **Nur sichere dynamische Updates zulassen** aus und klicken Sie auf ***Weiter***. Im Anschluss bekommen Sie eine Zusammenfassung der neuen Zone angezeigt, so wie in der folgenden Abbildung:



Jetzt klicken Sie auf ***Fertig stellen*** und die Zone wird angelegt. Anschießend sehen Sie die neu Zone wie in der folgenden Abbildung:



Durch einen Rechtsklick in der Rechten Seite des *DNS-Managers* können Sie jetzt einen neuen *PTR-Record* für alle bestehenden Systeme erstellen. In der folgenden Abbildung sehen Sie ein Beispiel für einen neuen *PTR-Record*:



Erzeugen Sie jetzt in der Forward-Zone einen neuen Eintrag für den zweiten DC. Prüfen Sie anschließen ob der Name auch richtig aufgelöst wird. Am einfachsten geht das auf den ersten DC über die Kommandozeile mit dem Kommando `host`.
Sie können den Eintrag für den neuen DC im DNS auch über die Kommandozeile realisieren, wie Sie das machen können, sehen Sie im folgenden Listing:

```
root@samba4-1:~# samba-tool dns add 192.168.123.170 example.net samba4-2 A\
192.168.123.171 -Uadministrator
Password for [EXAMPLE\administrator]:
Record added successfully
```

Das Kommando müssen Sie auf dem ersten DC ausführen.

17.2.3 Konfiguration des DCs

Auch für den zweiten DC ist Kerberos für die Authentifizierung der Benutzer notwendig. Darum müssen Sie als erstes die Datei /etc/krb5.conf vom ersten DC auf den neuen DC kopieren. Den Inhalt der Datei /etc/krb5.conf muss wie im folgenden Listing aussehen:

```
[libdefaults]
 dns_lookup_realm = true
 dns_lookup_kdc = true
 default_realm = EXAMPLE.NET
```

Installieren, soweit noch nicht vorhanden, das Paket heimdal-clients auf dem neuen DC um die Kerberos-Authentifizierung testen zu können. Jetzt können Sie so wie Sie es im folgenden Listen sehen, die Kerberos-Authentifizierung testen:

```
root@samba4-2:/etc# kinit administrator
administrator@EXAMPLE.NET's Password:

root@samba4-2:/etc# klist
Credentials cache: FILE:/tmp/krb5cc_0
        Principal: administrator@EXAMPLE.NET

  Issued                Expires               Principal
Jul 22 14:45:41 2013  Jul 23 00:45:41 2013  krbtgt/EXAMPLE.NET@EXAMPLE.NET
```

Fahren Sie mit der Konfiguration des neuen DC erst fort, wenn die Authentifizierung funktioniert. Jetzt können Sie den neuen DC zur Domäne als DC hinzufügen. Dazu verwenden Sie wieder das Kommando `samba-tool` wie Sie im folgenden Listing sehen können:

```
root@samba4-2:/etc# samba-tool domain join example.net DC -Uadministrator \
--realm=example.net
Finding a writeable DC for domain 'example.net'
Found DC samba4-1.example.net
Password for [WORKGROUP\administrator]:
workgroup is EXAMPLE
realm is example.net
checking sAMAccountName
Adding CN=SAMBA4-2,OU=Domain Controllers,DC=example,DC=net
Adding CN=SAMBA4-2,CN=Servers,CN=Default-First-Site-Name,CN=Sites,\
CN=Configuration,DC=example,DC=net
Adding CN=NTDS Settings,CN=SAMBA4-2,CN=Servers,CN=Default-First-Site-Name,CN=Sites,\
CN=Configuration,DC=example,DC=net
Adding SPNs to CN=SAMBA4-2,OU=Domain Controllers,DC=example,DC=net
Setting account password for SAMBA4-2$
Enabling account
Calling bare provision
Provision OK for domain DN DC=example,DC=net
Starting replication
Schema-DN[CN=Schema,CN=Configuration,DC=example,DC=net] objects[402/1550]\
linked_values[0/0]
Schema-DN[CN=Schema,CN=Configuration,DC=example,DC=net] objects[804/1550]\
linked_values[0/0]
Schema-DN[CN=Schema,CN=Configuration,DC=example,DC=net] objects[1206/1550]\
linked_values[0/0]
Schema-DN[CN=Schema,CN=Configuration,DC=example,DC=net] objects[1550/1550]\
linked_values[0/0]
Analyze and apply schema objects
Partition[CN=Configuration,DC=example,DC=net] objects[402/1614] linked_values[0/0]
Partition[CN=Configuration,DC=example,DC=net] objects[804/1614] linked_values[0/0]
Partition[CN=Configuration,DC=example,DC=net] objects[1206/1614] linked_values[0/0]
Partition[CN=Configuration,DC=example,DC=net] objects[1608/1614] linked_values[0/0]
Partition[CN=Configuration,DC=example,DC=net] objects[1614/1614] linked_values[28/0]
Replicating critical objects from the base DN of the domain
```

```
Partition[DC=example,DC=net] objects[97/97] linked_values[23/0]
Partition[DC=example,DC=net] objects[312/215] linked_values[23/0]
Done with always replicated NC (base, config, schema)
Replicating DC=DomainDnsZones,DC=example,DC=net
Partition[DC=DomainDnsZones,DC=example,DC=net] objects[58/58] linked_values[0/0]
Replicating DC=ForestDnsZones,DC=example,DC=net
Partition[DC=ForestDnsZones,DC=example,DC=net] objects[18/18] linked_values[0/0]
Partition[DC=ForestDnsZones,DC=example,DC=net] objects[36/18] linked_values[0/0]
Committing SAM database
Sending DsReplicateUpdateRefs for all the replicated partitions
Setting isSynchronized and dsServiceName
Setting up secrets database
Joined domain EXAMPLE (SID S-1-5-21-2272618568-2628634020-1511971479) as a DC
```

Hier sehen Sie genau, was alles beim Eintritt in die Domäne passiert. In der letzten Zeile kommt die Meldung das der Rechner der Domäne beigetreten ist und zwar als neuer DC.
Jetzt müssen Sie noch dafür sorgen, dass der samba4-dc auch startet. Dafür editieren Sie die Datei /etc/default/sernet-samba wie im folgenden Listing:

```
# SAMBA_START_MODE defines how Samba should be started. Valid options are one of
#   "none"    to not enable it at all,
#   "classic" to use the classic smbd/nmbd/winbind daemons
#   "ad"      to use the Active Directory server (which starts the smbd on its own)
# (Be aware that you also need to enable the services/init scripts that
# automatically start up the desired daemons.)
SAMBA_START_MODE="ad"
```

Wenn Sie diesen Eintrag vergessen, lässt sich der samba4 nicht starten. Anschließend starten Sie den neuen DC mit dem Kommando `service sernet-samba-ad start`.

17.2.4 Testen des neuen DCs

Um die Funktion des neuen DCs zu testen fragen Sie als erstes die Domaininfos wie im folgenden Listing ab:

```
root@samba4-2:/etc# samba-tool domain info 192.168.123.171
Forest           : example.net
Domain           : example.net
Netbios domain   : EXAMPLE
DC name          : samba4-2.example.net
DC netbios name  : SAMBA4-2
Server site      : Default-First-Site-Name
Client site      : Default-First-Site-Name
```

Als IP-Adresse geben Sie hier die IP des neuen DCs an. Hier sehen Sie, dass der Rechner jetzt ein DC in der Domäne ist. Weiterhin ist es wichtig, zu prüfen, ob die Reverseauflösung des DNS-Namens funktioniert. Sehen Sie dazu das folgende Listing:

```
root@samba4-2:~# host -t A samba4-2.example.net.
samba4-2.example.net has address 192.168.123.171
```

Sollte hier nicht das richtige oder gar kein Ergebnis zurückkommen, prüfen Sie, ob der zweite DC einen Reverse-Record in der Zone hat. Wenn dieser fehlt, können Sie diesen entweder über das Windows-Tool zur Verwaltung des DNS hinzufügen, oder aber wie im folgenden Listing, über die die Kommandozeile:

```
root@samba4-2:~# samba-tool dns add 192.168.123.170 example.net samba4-2 A \
  192.168.123.171 -Uadministrator
Password for [EXAMPLE\administrator]:
Record added successfully
```

Im nächsten Schritt prüfen Sie, ob die *objectGUID* des neuen DCs auch auflösbar ist. Wie das geht, sehen Sie im folgenden Listing:

```
root@samba4-2:~# ldbsearch -H /var/lib/samba/private/sam.ldb '(invocationid=*)' \
  --cross-ncs objectguid
# record 1
dn: CN=NTDS Settings,CN=SAMBA4-2,CN=Servers,CN=Default-First-Site-Name,CN=Sites,\
CN=Configuration,DC=example,DC=net
objectGUID: 7d348e71-0d23-47f8-9694-15891fff5f56

# record 2
dn: CN=NTDS Settings,CN=SAMBA4-1,CN=Servers,CN=Default-First-Site-Name,CN=Sites,\
CN=Configuration,DC=example,DC=net
objectGUID: 9c9e9807-3442-4990-8b2f-eaf31d603641

# returned 2 records
# 2 entries
# 0 referrals
```

Hier sehen Sie die *objectGUID*s der beiden DCs Ihrer Domäne. Diese *objectGUID* benötigen Sie für den folgenden Test. Denn im nächsten Test prüfen Sie, ob die Funktion des DCs auch über den DNS erreichbar ist. im folgenden Listing sehen Sie, wie sie die Prüfung durchführen.

```
root@samba4-2:~# host -t CNAME 9c9e9807-3442-4990-8b2f-eaf31d603641._msdcs.example.net.
9c9e9807-3442-4990-8b2f-eaf31d603641._msdcs.example.net is an alias\
for samba4-1.example.net.

root@samba4-2:~# host -t CNAME 7d348e71-0d23-47f8-9694-15891fff5f56._msdcs.example.net.
7d348e71-0d23-47f8-9694-15891fff5f56._msdcs.example.net is an alias\
for samba4-2.example.net.
```

Sie sehen, beide DCs werden über den DNS aufgelöst und der Dienst steht somit allen Clients in der Domäne zur Verfügung. Sollte der Test fehlschlagen, können Sie diesen Eintrag auch nachträglich erstellen. Dazu verwenden Sie das Kommando

```
samba-tool dns add 192.168.123.170 _msdcs.example.net\
7d348e71-0d23-47f8-9694-15891fff5f56 CNAME samba4-2.example.net -Uadministrator
```

Als *objectGUID* verwenden Sie die ID des fehlenden DCs.
Bevor Sie jetzt die Replikation prüfen, führen Sie noch einen Konsistenztest durch. Dieser Test prüft, ob die Datenbanken der DCs konsistent sind. Die Befehle dazu sehen Sie im folgenden Listing:

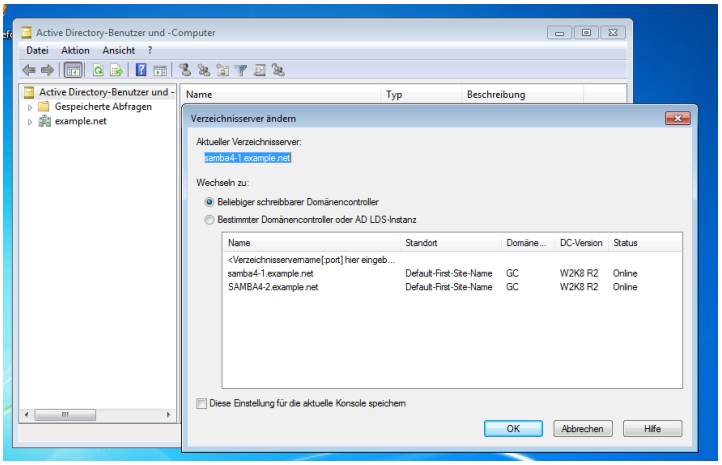
```
root@samba4-1:~# samba-tool drs kcc -Uadministrator samba4-2.example.net
Password for [EXAMPLE\administrator]:
Consistency check on samba4-2.example.net successful.

root@samba4-1:~# samba-tool drs kcc -Uadministrator samba4-1.example.net
Password for [EXAMPLE\administrator]:
Consistency check on samba4-1.example.net successful.
```

Beide DCs sind konsistent. Jetzt kommt der letzte Test, die Prüfung ob die Replikation der SAM-Datenbank funktioniert. Im folgenden Listing sehen Sie die Prüfung der Replikation:

```
root@samba4-1:~# samba-tool drs showrepl
Default-First-Site-Name\SAMBA4-1
DSA Options: 0x00000001
DSA object GUID: 9c9e9807-3442-4990-8b2f-eaf31d603641
DSA invocationId: e9f0d589-1f4f-4902-baf3-c0518d8f6426

==== INBOUND NEIGHBORS ====

DC=DomainDnsZones,DC=example,DC=net
        Default-First-Site-Name\SAMBA4-2 via RPC
                DSA object GUID: 7d348e71-0d23-47f8-9694-15891fff5f56
                Last attempt @ Mon Jul 22 15:42:29 2013 CEST was successful
                0 consecutive failure(s).
                Last success @ Mon Jul 22 15:42:29 2013 CEST

DC=ForestDnsZones,DC=example,DC=net
        Default-First-Site-Name\SAMBA4-2 via RPC
                DSA object GUID: 7d348e71-0d23-47f8-9694-15891fff5f56
                Last attempt @ Mon Jul 22 15:42:29 2013 CEST was successful
                0 consecutive failure(s).
                Last success @ Mon Jul 22 15:42:29 2013 CEST

DC=example,DC=net
        Default-First-Site-Name\SAMBA4-2 via RPC
                DSA object GUID: 7d348e71-0d23-47f8-9694-15891fff5f56
                Last attempt @ Mon Jul 22 15:42:29 2013 CEST was successful
                0 consecutive failure(s).
                Last success @ Mon Jul 22 15:42:29 2013 CEST

CN=Schema,CN=Configuration,DC=example,DC=net
        Default-First-Site-Name\SAMBA4-2 via RPC
                DSA object GUID: 7d348e71-0d23-47f8-9694-15891fff5f56
                Last attempt @ Mon Jul 22 15:42:30 2013 CEST was successful
                0 consecutive failure(s).
                Last success @ Mon Jul 22 15:42:30 2013 CEST

CN=Configuration,DC=example,DC=net
        Default-First-Site-Name\SAMBA4-2 via RPC
                DSA object GUID: 7d348e71-0d23-47f8-9694-15891fff5f56
                Last attempt @ Mon Jul 22 15:42:30 2013 CEST was successful
                0 consecutive failure(s).
                Last success @ Mon Jul 22 15:42:30 2013 CEST

==== OUTBOUND NEIGHBORS ====

DC=DomainDnsZones,DC=example,DC=net
        Default-First-Site-Name\SAMBA4-2 via RPC
                DSA object GUID: 7d348e71-0d23-47f8-9694-15891fff5f56
                Last attempt @ Mon Jul 22 15:44:07 2013 CEST was successful
                0 consecutive failure(s).
                Last success @ Mon Jul 22 15:44:07 2013 CEST

DC=ForestDnsZones,DC=example,DC=net
        Default-First-Site-Name\SAMBA4-2 via RPC
                DSA object GUID: 7d348e71-0d23-47f8-9694-15891fff5f56
```

```
                Last attempt @ Mon Jul 22 15:08:13 2013 CEST was successful
                0 consecutive failure(s).
                Last success @ Mon Jul 22 15:08:13 2013 CEST

DC=example,DC=net
        Default-First-Site-Name\SAMBA4-2 via RPC
                DSA object GUID: 7d348e71-0d23-47f8-9694-15891fff5f56
                Last attempt @ Mon Jul 22 15:08:14 2013 CEST was successful
                0 consecutive failure(s).
                Last success @ Mon Jul 22 15:08:14 2013 CEST

CN=Schema,CN=Configuration,DC=example,DC=net
        Default-First-Site-Name\SAMBA4-2 via RPC
                DSA object GUID: 7d348e71-0d23-47f8-9694-15891fff5f56
                Last attempt @ Mon Jul 22 15:08:14 2013 CEST was successful
                0 consecutive failure(s).
                Last success @ Mon Jul 22 15:08:14 2013 CEST

CN=Configuration,DC=example,DC=net
        Default-First-Site-Name\SAMBA4-2 via RPC
                DSA object GUID: 7d348e71-0d23-47f8-9694-15891fff5f56
                Last attempt @ Mon Jul 22 15:08:14 2013 CEST was successful
                0 consecutive failure(s).
                Last success @ Mon Jul 22 15:08:14 2013 CEST

==== KCC CONNECTION OBJECTS ====

Connection --
        Connection name: b5bdd36f-951c-4916-99f2-f0f331b5d03b
        Enabled        : TRUE
        Server DNS name : SAMBA4-2.example.net
        Server DN name  : CN=NTDS Settings,CN=SAMBA4-2,CN=Servers,\
        CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=example,DC=net
                TransportType: RPC
                options: 0x00000001
Warning: No NC replicated for Connection!
```

Auf beiden DCs sollte bei allen Tests ein `was successful` erscheinen. Sollte das nicht der Fall sein, prüfen Sie erneut, ob die Namensauflösung funktioniert und ob Sie eventuell eine IPv6 Adresse ansprechen die im DNS eingetragen ist, die der DC aber nicht mehr besitzt. Jetzt können Sie, am einfachsten über die RSAT eine Änderung an einem Objekt vornehmen und dann in dem RSAT auf den zweiten DC umschalten und prüfen, ob die Veränderung auch an dem zweiten DC angekommen ist. Führen Sie diesen Test an beiden DCs aus und testen Sie jeweils das Ergebnis. Auf dem anderen DC schalten Sie in den RSAT im *Active Directory-Benutzer und -Computer* um, in dem Sie mit der rechten Maustaste auf die oberste Ebenen klicken und dann den Punkt *Domänencontroller ändern...* anklicken. Es erscheint dann ein Fenster, so wie in der folgenden Abbildung, in dem Sie den jeweiligen DC auswählen können:



Damit ist die Konfiguration des zusätzlichen DCs für die Benutzerdatenbank abgeschlossen. Jetzt haben Sie zwei DCs und zwei DNS-Server in Ihrer Domäne. Denn der DNS-Server wird gleich mit repliziert. so können Sie jeder Zeit weitere DCs in Ihre Domäne einbinden. Nach dem Anlegen eines DCs können Sie diesen auch in einen anderen Standort verschieben.

17.2.5 Aufgaben

- Setzen Sie einen neuen samba4-Server auf und konfigurieren Sie diesen als Domaincontroller.
- Testen Sie die Replikation der Datenbank, in dem Sie auf jedem DC Objekte anlegen oder verändern.

17.2.6 Replikation der Freigabe sysvol

Bei mehreren DCs können sich ja alle Benutzer an jedem beliebigen DC anmelden. Damit dann auch die Logonskript und die Gruppenrichtlinen wirksam werden, müssen diese bei allen DCs in der Freigabe sysvol liegen. Da samba4 im Moment noch keine Dateisystemreplikation durchführen kann, müssen Sie einen anderen Weg finden um die Replikation durchführen zu können. Am einfachsten ist die Verwendung von `rsync`. In diesem Abschnitt sehe Sie, wie Sie die Replikation einrichten und prüfen.
Das Problem bei `rsync` ist, dass Sie nur in eine Richtung replizieren können. Würden Änderungen an beiden Seite vorgenommen, so würden Änderungen überschrieben. Daher müssen Sie die Replikation genau planen. Sie benötigen immer einen DC auf dem Sie die Änderungen durchführen und alle anderen DCs erhalten dann die Replikation. Wählen Sie den DC als Master auf dem die *fsmo PDC-Master* läuft. Bei der Verwaltung der Gruppenrichtlinen und der Logonskripte dürfen Sie Änderungen nur noch dort vornehmen. Den RSAT zur Verwaltung der Gruppenrichtlinen, können Sie den Server auf dem die Gruppenrichtlinen bearbeitet werden sollen aber voreinstellen. Dadurch erstellen und ändern Sie Gruppenrichtlinien automatisch auf dem richtigen Server. In den folgenden Schritten wird erst die Replikation eingerichtet und getestet und anschließend die RSAT eingestellt.

- Testen der fsmo-Rolle
  Im ersten Schritt müssen Sie den *PDC-Master* ermitteln, das können Sie am einfachsten über die Kommandozeile bei einem der DCs ermitteln. Im folgenden Listing sehen Sie die Vorgehensweise:

```
root@samba4-2:~# samba-tool fsmo show
InfrastructureMasterRole owner: CN=NTDS Settings,CN=SAMBA4-1,CN=Servers,\
   CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=example,DC=net
RidAllocationMasterRole owner: CN=NTDS Settings,CN=SAMBA4-1,CN=Servers,\
   CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=example,DC=net
PdcEmulationMasterRole owner: CN=NTDS Settings,CN=SAMBA4-1,CN=Servers,\
   CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=example,DC=net
DomainNamingMasterRole owner: CN=NTDS Settings,CN=SAMBA4-1,CN=Servers,\
   CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=example,DC=net
SchemaMasterRole owner: CN=NTDS Settings,CN=SAMBA4-1,CN=Servers,\
   CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=example,DC=net
```

Alle Rollen werden hier aufgeführt. Im Beispiel sehen Sie, dass der DC *samba4-1* der *PDC-Master* ist. Nur auf diesem DC dürfen Sie Gruppenrichtlinen und Logonskripte ändern und erstellen. Alle anderen DC erhalten später die Informationen über `rsync`.

- Einrichten von `rsync` auf dem *PDC-Master*
  Auf dem PDC-Master brauchen Sie neben dem Programm `rsync` auch noch den `xinetd` um den *rsync-Server* starten zu können. Installieren sie das Paket `rsync` und `xinetd` auf dem entsprechenden DC über `apt-get install rsync xinetd`. Anschließend müssen Sie für den *xinetd* eine Konfigurationsdatei rsync im Verzeichnis /etc/xinetd.d erstellen. Im folgenden Listing sehen Sie den Inhalt dieser Datei:

```
service rsync
{
   disable         = no
   only_from       = 192.168.123.171     # Restrict to your DCs
   socket_type     = stream
   wait            = no
   user            = root
   server          = /usr/bin/rsync
   server_args     = --daemon
   log_on_failure += USERID
}
```

Im nächsten Schritt müssen Sie `rsync` konfigurieren. Diese Konfiguration führen Sie über die Datei /etc/rsyncd.conf durch. Wenn diese Datei nicht vorhanden ist, erstellen Sie diese Datei. Die Datei muss den folgenden Inhalt haben:

```
[sysvol]
path = /var/lib/samba/sysvol/
comment = Samba sysvol
uid = root
gid = root
read only = yes
auth users = sysvol-repl
secrets file = /etc/samba/rsync.secret
```

In die Datei /etc/samba/rsync.secret tragen Sie den Benutzer ein, den Sie in dieser Datei als `auth user` eingetragen haben und das Passwort das dieser Benutzer verwenden soll. Ein Beispiel dafür sehen Sie in dem nächsten Listing:

```
sysvol-repl:geheim
```

Der Benutzername und dessen Passwort werden durch einen Doppelpunkt getrennt. Sorgen Sie dafür, dass *others* keinen Zugriff auf die Datei hat.
Starten Sie anschließend den *xinetd* neu. In der Datei /var/log/syslog finden Sie die folgenden Meldungen:

```
Jul 29 11:46:50 samba4-1 xinetd[4565]: xinetd Version 2.3.14 started with libwrap\
                loadavg options compiled in.
Jul 29 11:46:50 samba4-1 xinetd[4565]: Started working: 1 available service
Jul 29 11:51:27 samba4-1 xinetd[4565]: Exiting...
Jul 29 11:51:28 samba4-1 xinetd[4652]: Reading included configuration file:
                /etc/xinetd.d/chargen [file=/etc/xinetd.conf] [line=14]
Jul 29 11:51:28 samba4-1 xinetd[4652]: Reading included configuration file:\
                /etc/xinetd.d/daytime [file=/etc/xinetd.d/daytime] [line=28]
Jul 29 11:51:28 samba4-1 xinetd[4652]: Reading included configuration file:\
                /etc/xinetd.d/discard [file=/etc/xinetd.d/discard] [line=26]
Jul 29 11:51:28 samba4-1 xinetd[4652]: Reading included configuration file:\
                /etc/xinetd.d/echo [file=/etc/xinetd.d/echo] [line=25]
Jul 29 11:51:28 samba4-1 xinetd[4652]: Reading included configuration file:\
                /etc/xinetd.d/rsync [file=/etc/xinetd.d/rsync] [line=26]
Jul 29 11:51:28 samba4-1 xinetd[4652]: Reading included configuration file:\
                /etc/xinetd.d/time [file=/etc/xinetd.d/time] [line=11]
Jul 29 11:51:28 samba4-1 xinetd[4652]: removing chargen
Jul 29 11:51:28 samba4-1 xinetd[4652]: removing chargen
Jul 29 11:51:28 samba4-1 xinetd[4652]: removing daytime
Jul 29 11:51:28 samba4-1 xinetd[4652]: removing daytime
Jul 29 11:51:28 samba4-1 xinetd[4652]: removing discard
Jul 29 11:51:28 samba4-1 xinetd[4652]: removing discard
Jul 29 11:51:28 samba4-1 xinetd[4652]: removing echo
Jul 29 11:51:28 samba4-1 xinetd[4652]: removing echo
Jul 29 11:51:28 samba4-1 xinetd[4652]: removing time
Jul 29 11:51:28 samba4-1 xinetd[4652]: removing time
Jul 29 11:51:28 samba4-1 xinetd[4652]: xinetd Version 2.3.14 started with\
                libwrap loadavg options compiled in.
Jul 29 11:51:28 samba4-1 xinetd[4652]: Started working: 1 available service
```

Hier sehen Sie, das die Datei zur Konfiguration des *rsyncd* abgearbeitet wurde. Mit dem Kommando `netstat` können Sie dann noch testen, ob der Port auch erreichbar ist. Im folgenden Listing sehen Sie diesen Test:

```
root@samba4-1:/etc/xinetd.d# netstat -tlp
Aktive Internetverbindungen (Nur Server)
Proto Recv-Q Send-Q Local Address    Foreign Address    State   PID/Program name
.
.
.
tcp    0   0 *:rsync          *:*              LISTEN      4652/xinetd
.
.
.
```

Das zeigt, dass der *rsync* über den *xinetd* erreichbar ist.

- Konfiguration aller anderen DCs
  Auf allen weiteren DCs müssen Sie ebenfalls *rsync* installieren, den *xinetd* benötigen Sie dort nicht, da es sich hierbei immer nur um einen rsync-Client handelt.
  Nach der Installation von *rsync* erstellen Sie eine Datei, in der das Passwort für den Zugriff auf den rsync-Server abgelegt wird. Hier im Beispiel soll es die Datei /etc/samba/rsync.pass sein. Achten Sie hier auch wieder darauf, dass *others* keinen Zugriff auf die Datei hat.
  Jetzt können Sie die Replikation testen. Verwenden Sie beim testen auf jeden Fall den Parameter `--dry-run` damit verhindern Sie, dass die Replikation wirklich durchgeführt wird. Erst wenn das Ergebnis des Tests stimmt sollten Sie die Replikation starten. Im folgenden Listing sehen Sie den Test der Replikation:

```
root@samba4-2:~# rsync --dry-run -XAavz --delete-after\
```

```
                --password-file=/etc/samba/rsync.pass\
                rsync://sysvol-repl@samba4-1/sysvol/ /var/lib/samba/sysvol/
receiving file list ... done
./
example.net/
example.net/Policies/
example.net/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/
example.net/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/GPT.INI
example.net/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/
example.net/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/USER/
example.net/Policies/{6AC1786C-016F-11D2-945F-00C04FB984F9}/
example.net/Policies/{6AC1786C-016F-11D2-945F-00C04FB984F9}/GPT.INI
example.net/Policies/{6AC1786C-016F-11D2-945F-00C04FB984F9}/MACHINE/
example.net/Policies/{6AC1786C-016F-11D2-945F-00C04FB984F9}/USER/
example.net/scripts/
example.net/scripts/alle.bat

sent 102 bytes  received 874 bytes  1952.00 bytes/sec
total size is 75  speedup is 0.08 (DRY RUN)
```

Hier sehen Sie, dass alle Gruppenrichtlinen und das Logonskript übertragen wurden.

Warnung !

Achten Sie darauf, dass die Pfade alle korrekt sind, bei der Replikation werden später alle alten Einträge gelöscht und die neuen geschrieben. Stimmen hier die Pfade nicht, können Sie Ihr System unbrauchbar machen.

Jetzt können Sie den Parameter `--dry-run` aus der Befehlszeile entfernen und die erste Replikation durchführen. So wie Sie es im folgenden Listing sehen können:

```
root@samba4-2:~# rsync  -XAavz --delete-after\
                --password-file=/etc/samba/rsync.pass\
                rsync://sysvol-repl@samba4-1/sysvol/ /var/lib/samba/sysvol/
receiving file list ... done
./
example.net/
example.net/Policies/
example.net/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/
example.net/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/GPT.INI
example.net/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/
example.net/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/USER/
example.net/Policies/{6AC1786C-016F-11D2-945F-00C04FB984F9}/
example.net/Policies/{6AC1786C-016F-11D2-945F-00C04FB984F9}/GPT.INI
example.net/Policies/{6AC1786C-016F-11D2-945F-00C04FB984F9}/MACHINE/
example.net/Policies/{6AC1786C-016F-11D2-945F-00C04FB984F9}/USER/
example.net/scripts/
example.net/scripts/alle.bat

sent 166 bytes  received 2304 bytes  1646.67 bytes/sec
total size is 75  speedup is 0.03
```

Prüfen Sie, ob alle Verzeichnisse und Dateien übertragen wurden. Wenn alle Dateien übertragen wurden, können Sie mit dem nächsten Schritt fortfahren.

- Einrichtung eins *cron-jobs* für die Replikation

17.2.7 Einrichten des cron

Damit Sie die Replikation nicht immer von Hand durchführen müssen, sollten Sie an dieser Stelle einen *cron-job* als Benutzer *root* einrichten, der regelmäßig die Replikation durchführt.

Im Beispiel soll die Replikation alle fünf Minuten durchgeführt werden.

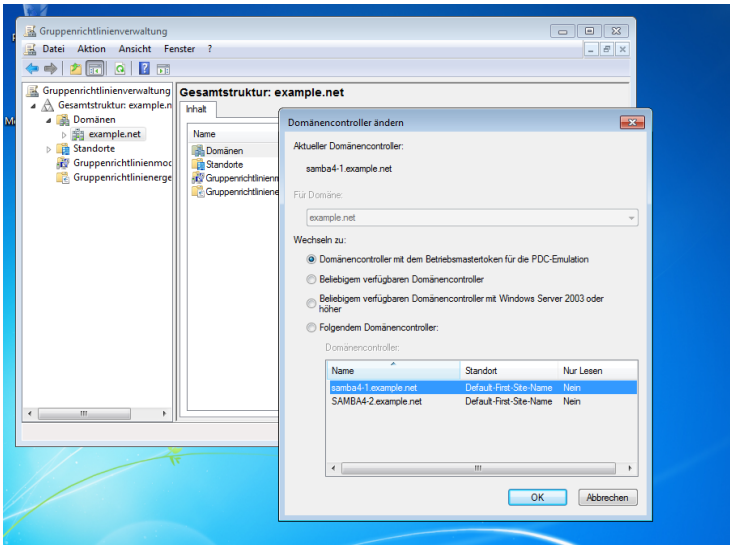
```
*/5 * * * * rsync  -XAavz --delete-after\
            --password-file=/etc/samba/rsync.pass\
            rsync://sysvol-repl@samba4-1/sysvol/ /var/lib/samba/sysvol/
```

Die Zeit für die Replikation ist immer davon abhängig, wie viele Änderungen Sie an den Gruppenrichtlinen und den Logonskripten vornehmen. Damit ist die Replikation des zweiten DCs abgeschlossen. Wenn Sie noch weitere DCs in Ihrer Domäne haben, müssen Sie diesen Schritt auf allen weiteren DCs durchführen.

- Anpassen der smb.conf Auf den Client-DCs der Replikation sollten Sie die Freigabe sysvol auf *read-only* setzen, dass hier niemand über das Netzwerk Änderungen vornehmen kann. Passen Sie hierfür die Datei /etc/samba/smb.conf wie im folgenden Listing zu sehen an:

  ```
  [sysvol]
          path = /var/lib/samba/sysvol
          read only = Yes
  ```

- Einstellung für die Gruppenrichtlinen
  Jetzt müssen Sie nur noch dafür sorgen, dass das RSAT für die Verwaltung der Gruppenrichtlinien nur noch auf dem entsprechenden Server mit der *fsmo*-Rolle *PDC-Master*. Starten Sie hierfür das RSAT `Gruppenrichtlinenverwaltung` suchen auf der linken Seite Ihre Domäne, klicken Sie mit der rechten Maustaste auf die Domäne und wählen Sie dann den Punkt *`Domänencontroller ändern...`* aus. Es öffnet sich ein neues Fenster, in diesem Fenster markieren Sie den Punkt *`Domänencontroller mit dem Betriebsmastertoken für die PDC-Emulation`* aus. Der Entsprechenden DC aus der Liste wird daraufhin im unteren Teil des Fensters markiert. In der folgen Abbildung sehen Sie die entsprechende Einstellung:



Bestätigen Sie die Einstellung mit einem Klick auf *`OK`*. Ab sofort werden alle Änderungen an den Gruppenrichtlinen nur noch auf dem entsprechenden DC durchgeführt.

17.2.8 Aufgaben

- Richten Sie den rsync-Server auf dem DC ein, der die PDC-fsmo-Rolle hat.
- Konfigurieren Sie auf dem anderen DC den rsync-Client und testen Sie die Replikation.
- Erstellen Sie einen cron-Job der regelmäßig die Replikation durchführt.

18 Migration von Samba3

Nicht immer starten Sie mit einer neuen Domäne, in den meisten Fällen werden Sie von einer Samba3-Domäne auf eine samba4-Domäne migrieren wollen. In diesem Abschnitt geht es genau um dieses Thema. Bei diesem Thema müssen Sie zwischen zwei Szenarien unterscheiden, einmal kann der Samba3 PDC mit dem tdb-Backend arbeiten, oder aber Sie haben eine Kombination aus Samba3 und openLDAP.
Im ersten Teil geht es um die Umstellung einer Samba3-Domäne die mit dem tdb-Backend arbeitet. Im zweiten Teil dann um die Migration einer Samba3-Domäne mit openLDAP als Datenbank-Backend.
Bei der Migration gibt es immer zwei Wege die Sie gehen können, da wäre einmal eine *In Place*-Migration, also auf dem selben Server auf dem der Samba3 läuft, oder aber eine Migration auf eine neue Maschine. Die Migration auf eine neu Maschine ist immer der *In Place*-Migration vorzuziehen, da Sie dann immer noch die Möglichkeit haben, die alte Domäne wieder herzustellen. Hier soll nur die Migration auf einen neue Maschine besprochen werden.
Ein weiterer Punkt den Sie berücksichtigen müssen, ist die Umstellung der Windows-Clients. Nach der Migration von Samba3 auf samba4 können Sich die Benutzer direkt wieder an Ihren Maschinen anmelden, ein *re-join* der Maschinen ist nicht notwendig. Nur wenn die Maschinen einmal von einer Samba3- auf eine samba4-Domäne umgestellt sind, gibt es keinen Weg mehr zurück, außer ein *re-join*.
Wenn Sie die Möglichkeit haben, testen Sie die Migration vorher in einem virtuellen Netz.
Bei der Migration auf einen neuen Server müssen Sie darauf achten, dass Sie den alten Samba3-PDC sofort nach der Migration abschalten. Bei der Migration wird die gesamte Konfiguration übernommen, auch die NetBIOS-Namen des Servers. Wenn Sie also den alten PDC nicht vom Netz nehmen, kommt es anschließend zu einem Adressenkonflikt.

18.1 Migration einer tdb-Backend Domäne

Bei der Migration soll es hier nur um die Migration der Benutzerverwaltung gehen, nicht um die Migration etwaiger Daten auf dem Server. Wenn Sie auf Ihrem Samba3-PDC auch Freigaben eingerichtet haben, empfiehlt es sich, diese auf einen eigenen Fileserver zu migrieren um dem Problem des ID-Mappings aus dem Weg zu gehen.

18.2 Vorbereiten der Migration

Setzen Sie einen neuen samba4-Server auf und installieren Sie die SerNet-samba4-Pakete. Stellen Sie die benötigten Informationen zusammen die sie brauchen um die AD-Domäne einrichten zu können. Zu den Informationen gehören der Domänenname, der realm für Kerberos und die DNS-Informationen. Führen Sie an dieser Stelle auf gar keinen Fall das *Provisioning* durch. Erst müssen die Datenbanken vom Samba3-Server kopiert werden.
Sammeln Sie alle Informationen des alten Servers, prüfen Sie die Benutzer, Gruppen und Hosts in der alten Domäne. Erstellen Sie sich eine Liste um später zu prüfen, ob alle Objekte übernommen wurden. Führen Sie eine Sicherung durch.
Die Datei smb.conf auf dem Samba3-Server sollte die folgenden Informationen enthalten:

```
[global]
        workgroup = sambadom
        domain master = yes
        domain logons = yes
        netbios name = samba3
        os level = 99
        wins support = yes
```

```
        winbind enum users = yes
        winbind enum groups = yes
```

Sie sehen hier, dass der Samba3-Server auch als WINS durch den Parameter `wins support = yes` eingerichtet ist. Sollte der PDC bis zu diesem Zeitpunkt nicht der WINS-Server in der Domäne sein, macht es Sinn, den Server vor der Migration zum WINS-Server zu machen. Dadurch wird bei der Migration die WINS-Datenbank gleich ausgelesen und in die neue Domäne übernommen. Prüfen Sie mit `pdbedit -Lv administrator` ob Ihr Administrator den RID=500 hat. Wenn nicht, dann passen Sie den RID mit dem Kommando `pdbedit -U 500 -u administrator` an, da es sonst bei der Migration zu Fehlermeldungen kommt.

18.2.1 Kopieren aller benötigten Daten

Jetzt müssen Sie die Datenbanken und die Datei smb.conf des Samba3-Servers auf den neuen samba4-Server kopieren. Im folgenden Listing sehen Sie den Kopiervorgang:

```
root@samba3:~# scp /etc/samba/smb.conf root@192.168.123.181:/root/samba3/
root@192.168.123.181's password:
smb.conf

root@samba3:~# scp -r /var/lib/samba root@192.168.123.181:/root/samba3/
root@192.168.123.181's password:
secrets.tdb
share_info.tdb
schannel_store.tdb
group_mapping.tdb
wins.tdb
account_policy.tdb
wins.dat
passdb.tdb
registry.tdb

root@samba3:~# scp /etc/group root@192.168.123.181:/root
root@192.168.123.181's password:
group
```

Wie sie sehen, sind das alles .tdb-Dateien. Jetzt haben Sie alle Daten der alten Domäne auf den neuen Server kopiert. Passen Sie jetzt die kopierte Version der *smb.conf* hinsichtlich der NetBIOS-Namen an die neue Umgebung an. In den meisten Fällen wollen Sie die alten Namen behalten, dann müssen Sie an dieser Stelle nichts ändern. Die Datei /etc/group benötigen Sie, um die Gruppenzugehörigkeiten wiederherstellen zu können.
Wenn Sie aber die alten Namen behalten, denke Sie daran, den alten Server rechtzeitig, vor dem Start der neuen Domäne, anzuhalten.

18.2.2 Migration der Datenbanken

Jetzt kommt der Schritt, in dem Sie die Migration starten. Für die Migration kommt wieder das Kommando `samba-tool` zum Einsatz. Im folgenden Listing sehen Sie diesen Vorgang:

```
root@samba4:~# samba-tool domain classicupgrade --dbdir=/root/samba3/samba \
               --use-xattrs=yes --realm=example.net /root/samba3/smb.conf
Reading smb.conf
Provisioning
```

```
Exporting account policy
Exporting groups
Ignoring group 'samba3alle' S-1-5-21-244948763-3797424407-11963266-1005 listed but\
         then not found: Unable to enumerate group members, (-1073741722,No such group)
Ignoring group 'Domainadmins' S-1-5-21-244948763-3797424407-11963266-512 listed but\
         then not found: Unable to enumerate group members, (-1073741722,No such group)
Ignoring group 'Domainhosts' S-1-5-21-244948763-3797424407-11963266-515 listed but\
         then not found: Unable to enumerate group members, (-1073741722,No such group)
Ignoring group 'Domainusers' S-1-5-21-244948763-3797424407-11963266-513 listed but\
         then not found: Unable to enumerate group members, (-1073741722,No such group)
Ignoring group 'samba3buch' S-1-5-21-244948763-3797424407-11963266-1003 listed but\
         then not found: Unable to enumerate group members, (-1073741722,No such group)
Ignoring group 'samba3verw' S-1-5-21-244948763-3797424407-11963266-1004 listed but\
         then not found: Unable to enumerate group members, (-1073741722,No such group)
Ignoring group 'Domainguests' S-1-5-21-244948763-3797424407-11963266-514 listed but\
         then not found: Unable to enumerate group members, (-1073741722,No such group)
Exporting users
  Skipping wellknown rid=500 (for username=administrator)
Ignoring group memberships of 'samba3ktom' S-1-5-21-244948763-3797424407-11963266-1002:\
         Unable to enumerate group memberships, (-1073741724,No such user)
Ignoring group memberships of 'samba3stka' S-1-5-21-244948763-3797424407-11963266-1001:\
         Unable to enumerate group memberships, (-1073741724,No such user)
Ignoring group memberships of 'samba3win7$' S-1-5-21-244948763-3797424407-11963266-1006:\
         Unable to enumerate group memberships, (-1073741724,No such user)
Next rid = 1007
Exporting posix attributes
Reading WINS database
Looking up IPv4 addresses
Looking up IPv6 addresses
Setting up share.ldb
Setting up secrets.ldb
Setting up the registry
Setting up the privileges database
Setting up idmap db
Setting up SAM db
Setting up sam.ldb partitions and settings
Setting up sam.ldb rootDSE
Pre-loading the Samba 4 and AD schema
Adding DomainDN: DC=example,DC=net
Adding configuration container
Setting up sam.ldb schema
Setting up sam.ldb configuration data
Setting up display specifiers
Modifying display specifiers
Adding users container
Modifying users container
Adding computers container
Modifying computers container
Setting up sam.ldb data
Setting up well known security principals
Setting up sam.ldb users and groups
Setting up self join
Setting acl on sysvol skipped
Adding DNS accounts
Creating CN=MicrosoftDNS,CN=System,DC=example,DC=net
Creating DomainDnsZones and ForestDnsZones partitions
Populating DomainDnsZones and ForestDnsZones partitions
Setting up sam.ldb rootDSE marking as synchronized
```

```
Fixing provision GUIDs
A Kerberos configuration suitable for Samba 4 has been generated at \
          /var/lib/samba/private/krb5.conf
Setting up fake yp server settings
Once the above files are installed, your Samba4 server will be ready to use
Admin password:        gzQPi>p),Bh@EC
Server Role:           active directory domain controller
Hostname:              samba3
NetBIOS Domain:        SAMBADOM
DNS Domain:            example.net
DOMAIN SID:            S-1-5-21-244948763-3797424407-11963266
Importing WINS database
Importing Account policy
Importing idmap database
Cannot open idmap database, Ignoring: [Errno 2] No such file or directory
Importing groups
Group already exists sid=S-1-5-21-244948763-3797424407-11963266-512,\
      groupname=Domainadmins existing_groupname=Domain Admins, Ignoring.
Group already exists sid=S-1-5-21-244948763-3797424407-11963266-515,\
      groupname=Domainhosts existing_groupname=Domain Computers, Ignoring.
Group already exists sid=S-1-5-21-244948763-3797424407-11963266-513,\
      groupname=Domainusers existing_groupname=Domain Users, Ignoring.
Group already exists sid=S-1-5-21-244948763-3797424407-11963266-514,\
      groupname=Domainguests existing_groupname=Domain Guests, Ignoring.
Importing users
Adding users to groups
```

Hinweis !

Notieren Sie sich das neue Passwort für den Administrator der neuen Domäne!

Jetzt wurden alle Daten aus der alten Domäne übernommen. Die Meldungen mit dem Hinweis `Unable to enumerate group members` können Sie ignorieren, das sind lediglich Hinweise das die RIDs der Benutzer nicht in UIDs umgesetzt werden können. Die Migration ist trotzdem erfolgreich.

18.2.3 Testen der Benutzer und Gruppen

Wenn Sie jetzt die Benutzer und Gruppen überprüfen, werden Sie feststellen, dass zwar alle Benutzer und Gruppen vorhanden sind, aber die Gruppenmitgliedschaften der Benutzer nicht übernommen wurden. Das können Sie im nachfolgenden Listing sehen:

```
oot@samba4:~# samba-tool group list
.
.
.
Domain Users
Replicator
IIS_IUSRS
samba3alle
samba3buch
samba3verw
DnsAdmins
Guests
Users

root@samba4:~# samba-tool user list
Administrator
```

```
samba3ktom
samba3stka
krbtgt
Guests

root@samba4:~# samba-tool group listmembers samba3alle
```

Die Übernahme der Mitglieder in die neuen Gruppen ist so auch nicht möglich, da bei Samba3 die Mitglieder der Gruppen über die Linux-Gruppen gesteuert werden. Die Mitglieder der Gruppen werden in der Datei /etc/group verwaltet. Diese haben Sie ja vorher schon auf dem neuen samba4-Server kopiert. Bevor Sie jetzt das nachfolgende Skript erstellen und ausführen, bereinigen Sie die Kopie der Datei group, so dass nur noch die Gruppen übrig bleiben, die auch Mitglieder haben und die migriert wurden. Mit dem folgenden Skript können Sie die Mitglieder der Gruppen auswerten und in die neuen Gruppen auf dem DC eintragen:

```
# Datei group als Parameter uebergeben
cat $1 | awk -F: '
$3>100 {
       printf("/usr/bin/samba-tool group addmembers %s %s\n", $1, $4);
}' | /bin/sh
```

Wenn Sie jetzt erneut die Mitgliederliste der Gruppen prüfen, werden Sie wie im folgenden Listing sehen, dass alle Mitglieder wieder den Gruppen hinzugefügt wurden:

```
root@samba4:~# samba-tool group listmembers samba3alle
samba3ktom
samba3stka
```

Mit diesem Schritt ist die Migration der Benutzer und Gruppen aus der alten Samba3-Domäne abgeschlossen. Wenn sich jetzt ein Benutzer an einer Arbeitsstationen in der Domäne anmeldet, wird er sich sofort am neuen DC anmelden. Denken Sie daran, dass eine Workstation die einmal in die neue Domäne gewechselt ist nicht ohne weiteres in die alte Domäne zurück kann. Testen Sie die Umgebung ausgiebig, bevor Sie alle Clients endgültig umstellen.

18.3 Migration der Benutzer und Gruppen aus einem openLDAP

Bei der Migration aus einem *openLDAP* gehen Sie nicht viel anders vor, als bei der Migration aus den tdb-Dateien. Das Kommando `samba-tool domain classicupgrade` ließt aus der Datei smb.conf des Samba3-Servers die Adresse des openLDAP-Server aus, verbindet sich mit dem Server und ließt alle Konten aus dem openLDAP aus und legt diese im neuen AD an. Aber auch hier müssen Sie gewisse Vorarbeiten treffen, bevor die eigentlich Migration stattfinden kann.

18.3.1 Doppelte SIDs und Benutzername == Gruppenname

Einer der Schritte die Sie vornehmen müssen, ist die Überprüfung ob doppelte SIDs in Ihrem openLDAP vorhanden sind. Sollte das der Fall sein, müssen Sie die SIDs vor der Migration ändern. Sollte es doppelte SIDs geben, erhalten Sie während der Migration die folgende Fehlermeldung:

```
ERROR(<class 'samba.provision.ProvisioningError'>): uncaught exception - \
      ProvisioningError: Please remove duplicate user sid entries before upgrade.
```

Für die Prüfung auf doppelte SIDs können Sie das folgende Python-Skript einsetzen:

```
#!/usr/bin/python
# A quick and dirty python script that checks for duplicat SID's using slapcat.
import os

data = os.popen("slapcat | grep sambaSID", 'r')
line = []

def anydup(thelist):
        dups = list(set([x for x in thelist if thelist.count(x) > 1]))
        for i in dups:
                print "Duplicate id: ", i

for each_line in data:
        line.append(each_line.strip())

anydup(line)
```

Nachdem Sie sicher sind, dass es keine doppelten SIDs in Ihrem LDAP-Baum gibt, müssen Sie noch prüfen, ob es Gruppen gibt, deren Name gleich dem eines Benutzers sind. Sollte das der Fall sein, erhalten Sie während der Migration die folgende Fehlermeldung:

```
ERROR(<class 'samba.provision.ProvisioningError'>): uncaught exception -\
      ProvisioningError: Please remove common user/group names before upgrade
```

18.3.2 Kopieren der benötigten Daten

Auch hier müssen Sie die tdb-Dateien und die smb.conf Datei wieder auf den neuen Server kopieren. In den tdb-Dateien befinden sich jetzt keine Benutzerinformationen, aber die gesamte Konfiguration des Samba3-Servers. Diese wollen Sie komplett auf den neuen Server migrieren. Die Datei /etc/group benötigen Sie hier nicht, da die Mitgliedschaften in den Gruppen im LDAP verwaltet werden. Im folgenden Listing sehen Sie wieder das Kopieren der Daten:

```
root@openldap:~# scp -r /var/lib/samba root@192.168.123.181:/root/samba3/
root@192.168.123.181's password:
secrets.tdb
share_info.tdb
schannel_store.tdb
group_mapping.tdb
wins.tdb
account_policy.tdb
passdb.tdb
registry.tdb

root@openldap:~# scp /etc/samba/smb.conf root@192.168.123.181:/root/samba3/
root@192.168.123.181's password:
smb.conf
```

18.3.3 Start der Migration

Jetzt können Sie mit der Migration beginnen. Im folgenden Listing sehen Sie die Migration mit dem Kommando `samba-tool`:

```
root@samba4:~# samba-tool domain classicupgrade --dbdir=/root/samba3/samba \
               --use-xattrs=yes --realm=example.net /root/samba3/smb.conf
Reading smb.conf
Provisioning
Exporting account policy
Exporting groups
Exporting users
  Skipping wellknown rid=500 (for username=administrator)
Ignoring group memberships of 'skania' S-1-5-21-2364478241-1785271800-285767775-21002:\
     Unable to enumerate group memberships, (-1073741596,NT_STATUS_INTERNAL_DB_CORRUPTION)
Ignoring group memberships of 'ktom' S-1-5-21-2364478241-1785271800-285767775-21004:\
     Unable to enumerate group memberships, (-1073741596,NT_STATUS_INTERNAL_DB_CORRUPTION)
Ignoring group memberships of 'ptau' S-1-5-21-2364478241-1785271800-285767775-21006:\
     Unable to enumerate group memberships, (-1073741596,NT_STATUS_INTERNAL_DB_CORRUPTION)
Next rid = 21016
Exporting posix attributes
Reading WINS database
Cannot open wins database, Ignoring: [Errno 2] No such file or directory:\
     '/root/samba3/samba/wins.dat'
Looking up IPv4 addresses
Looking up IPv6 addresses
Setting up share.ldb
Setting up secrets.ldb
Setting up the registry
Setting up the privileges database
Setting up idmap db
Setting up SAM db
Setting up sam.ldb partitions and settings
Setting up sam.ldb rootDSE
Pre-loading the Samba 4 and AD schema
Adding DomainDN: DC=example,DC=net
Adding configuration container
Setting up sam.ldb schema
Setting up sam.ldb configuration data
Setting up display specifiers
Modifying display specifiers
Adding users container
Modifying users container
Adding computers container
Modifying computers container
Setting up sam.ldb data
Setting up well known security principals
Setting up sam.ldb users and groups
Setting up self join
Setting acl on sysvol skipped
Adding DNS accounts
Creating CN=MicrosoftDNS,CN=System,DC=example,DC=net
Creating DomainDnsZones and ForestDnsZones partitions
Populating DomainDnsZones and ForestDnsZones partitions
Setting up sam.ldb rootDSE marking as synchronized
Fixing provision GUIDs
A Kerberos configuration suitable for Samba 4 has been generated at \
           /var/lib/samba/private/krb5.conf
Setting up fake yp server settings
Once the above files are installed, your Samba4 server will be ready to use
Admin password:        jODFpCjX=8mE99P6(S)eDh#
Server Role:           active directory domain controller
Hostname:              samba4
```

```
NetBIOS Domain:        SAMBA3
DNS Domain:            example.net
DOMAIN SID:            S-1-5-21-2364478241-1785271800-285767775
Importing WINS database
Importing Account policy
Importing idmap database
Cannot open idmap database, Ignoring: [Errno 2] No such file or directory
Importing groups
Group already exists sid=S-1-5-21-2364478241-1785271800-285767775-512,\
      groupname=domainadmins existing_groupname=Domain Admins, Ignoring.
Group already exists sid=S-1-5-21-2364478241-1785271800-285767775-513,\
      groupname=domainusers existing_groupname=Domain Users, Ignoring.
Group already exists sid=S-1-5-21-2364478241-1785271800-285767775-514,\
      groupname=domainguests existing_groupname=Domain Guests, Ignoring.
Group already exists sid=S-1-5-21-2364478241-1785271800-285767775-515,\
      groupname=domainhosts existing_groupname=Domain Computers, Ignoring.
Importing users
Adding users to groups
```

Hinweis !

Notieren Sie sich das neue Passwort für den Administrator der neuen Domäne!

Damit ist die Migration aus dem LDAP abgeschlossen.

18.3.4 Testen der neuen Domäne

Auch hier sollten Sie ausgiebig testen, ob alle Benutzer und Gruppen übernommen wurden. Im folgenden Listing sehen Sie auch hier die entsprechenden Tests:

```
root@samba4:~# samba-tool user list
Administrator
krbtgt
skania
Guest
ktom
ptau

root@samba4:~# samba-tool group list
Allowed RODC Password Replication Group
Enterprise Read-Only Domain Controllers
.
.
.
Domain Users
Replicator
IIS_IUSRS
samba3alle
samba3buch
samba3verw
DnsAdmins
Guests
Users

root@samba4:~# samba-tool group listmembers samba3alle
ktom
ptau
skania
```

Wie Sie hier sehen, werden jetzt alle Gruppenmitgliedschaften direkt übernommen. Damit ist auch diese Migration abgeschlossen. Achten Sie auch hier darauf, dass der alte Samba-Server nicht länger im Netz aktiv ist, da es sonst zu Adressenkonflikten kommt.

19 Migration eins Windows 2003 Servers

In diesem Abschnitt geht es darum, einen alten Windows 2003 Domänencontroller auf samba4 zu migrieren. Bevor Sie den samba4-Server in die Domäne aufnehmen, stellen Sie sicher, dass sich die AD-Domäne auf dem Windows-Server im *2003 Betriebsmodus* befindet. Das können Sie im Programm *Active Directory-Benutzer und -Computer* auf dem Windows-DC prüfen und gegebenenfalls umstellen. Die Standardeinstellung ist dort *2000 Betriebsmodus*. Samba4 benötigt aber mindestens den *2003 Betriebsmodus*.
Sorgen Sie dafür, dass auf dem DNS-Server im AD eine *reverse*-Zone vorhanden ist, da diese für die Replikation der DCs benötigt wird. Installieren Sie einen neuen samba4-Server und nehmen Ihn so wie im Abschnitt 17.2 beschrieben, in die bestehenden Domäne als DC auf.

19.1 DNS-Einträge erstellen und prüfen

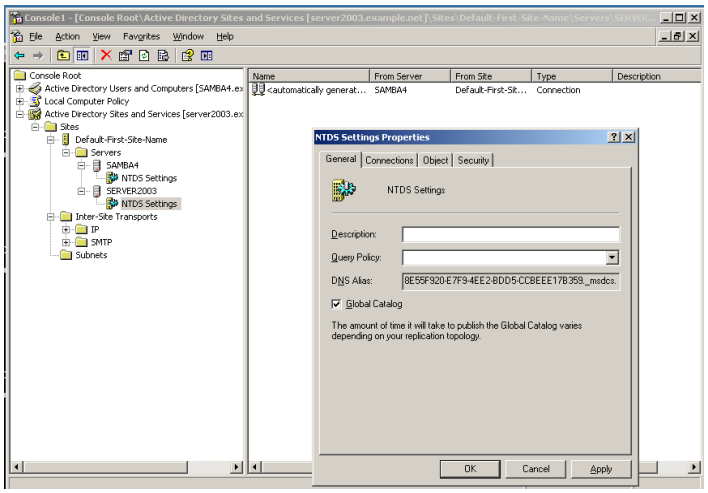
Starten Sie jetzt den DNS-Manager auf dem Windows-Server und fügen Sie den samba4-Server als DNS-Server zur Domäne hinzu. Prüfen Sie, ob eine *reverse*-Zone auf dem samba4-Server erzeugt wurde. Wenn das nicht der Fall ist, legen Sie eine neue *reverse*-Zone auf dem samba4-Server an. Anschießend führen Sie das Kommando `samba_dnsupdate --all-names --verbose` aus. Dabei werden alle Informationen zwischen den beiden DNS-Servern ausgetauscht. Interessant sind die ersten beiden Meldungen, die Sie im folgenden Listing sehen:

```
Skipping PDC entry (SRV _ldap._tcp.pdc._msdcs.${DNSDOMAIN}\
                    ${HOSTNAME} 389) as we are not a PDC
Skipping PDC entry (SRV _ldap._tcp.pdc._msdcs.${DNSFOREST}\
                    ${HOSTNAME} 389) as we are not a PDC
```

Hier sehen Sie, dass der samba4-Server noch nicht die *fsmo*-Rolle *PDC* besitzt. Wie auch alle anderen *fsmo*-Rollen noch auf dem Windows-Server vorhanden sind. Diese müssen noch auf den samba4-Server migriert werden.

19.2 Global Catalog umziehen

Bevor Sie die Rollen übergeben können, müssen Sie als erstes den *global catalog* auf den neuen samba4-Server verschieben und anschließend vom Windows-server entfernen. Bevor Sie den *global catalog* vom Windows-Server entfernen, prüfen Sie, ob der samba4-Server diese Funktion übernommen hat. In den *NTDS-Setting* muss der Haken bei *Global Catalog* gesetzt sein. Entfernen Sie den *global catalog* über das Werkzeug `Activ Directory Sites and Services` in dem Sie bei dem Windows-Server in den *NTDS-Settings* den Haken bei *Global Catalog* entfernen. In der folgenden Abbildung sehen Sie die Einstellung:



Jetzt ist der samba4-Server der *global-catalog*-Server.

19.3 Übertragung der *fsmo*-Rollen

Bevor Sie die *fsmo*-Rollen übertragen, prüfen Sie auf dem samba4-Server welcher Server in der Domäne die Rollen hält. Im folgenden Listing sehen Sie diesen Test mit den entsprechenden Ergebnissen:

```
root@samba4:/etc# samba-tool fsmo show
InfrastructureMasterRole owner: CN=NTDS Settings,CN=SERVER2003,CN=Servers,\
            CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=example,DC=net
RidAllocationMasterRole owner: CN=NTDS Settings,CN=SERVER2003,CN=Servers,\
            CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=example,DC=net
PdcEmulationMasterRole owner: CN=NTDS Settings,CN=SERVER2003,CN=Servers,\
            CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=example,DC=net
DomainNamingMasterRole owner: CN=NTDS Settings,CN=SERVER2003,CN=Servers,\
            CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=example,DC=net
SchemaMasterRole owner: CN=NTDS Settings,CN=SERVER2003,CN=Servers,\
            CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=example,DC=net
```

Alle *fsmo*-Rollen werden noch auf dem Windows-Server gehalten. Jetzt können Sie die Rollen auf den samba4-Server übernehmen. Das folgenden Listing zeigt wie Sie die Rollen übernehmen:

```
root@samba4:/etc# samba-tool fsmo transfer --role=all
FSMO transfer of 'rid' role successful
FSMO transfer of 'pdc' role successful
FSMO transfer of 'naming' role successful
FSMO transfer of 'infrastructure' role successful
FSMO transfer of 'schema' role successful
```

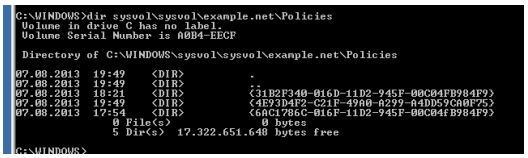
Hier werden dann gleich alle Rollen auf einmal auf den samba4-Server verschoben. Ein weiterer Test zeigt dann im folgenden Listing, dass der samba4-Server jetzt alle *fsmo*-Rollen hält:

```
root@samba4:/etc# samba-tool fsmo show
InfrastructureMasterRole owner: CN=NTDS Settings,CN=SAMBA4,CN=Servers,\
              CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=example,DC=net
RidAllocationMasterRole owner: CN=NTDS Settings,CN=SAMBA4,CN=Servers,\
```

```
              CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=example,DC=net
PdcEmulationMasterRole owner: CN=NTDS Settings,CN=SAMBA4,CN=Servers,\
              CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=example,DC=net
DomainNamingMasterRole owner: CN=NTDS Settings,CN=SAMBA4,CN=Servers,\
              CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=example,DC=net
SchemaMasterRole owner: CN=NTDS Settings,CN=SAMBA4,CN=Servers,\
              CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=example,DC=net
```

19.4 Prüfen der Gruppenrichtlinien

Als letztes bleibt nur noch zu prüfen, ob alle Gruppenrichtlinien vom Windows-DC auf dem samba4-DC übertragen wurden. Listen Sie, auf dem Windows-Server, das Verzeichnis mit dem Gruppenrichtlinen auf. So wie Sie es in der folgenden Abbildung sehen:



Jetzt lassen Sie sich die Gruppenrichtlinen auf dem samba4-DC wie im folgenden Listing anzeigen:

```
root@samba4:/etc# samba-tool gpo listall
GPO          : {31B2F340-016D-11D2-945F-00C04FB984F9}
display name : Default Domain Policy
path         : \\example.net\sysvol\example.net\Policies\\
               {31B2F340-016D-11D2-945F-00C04FB984F9}
dn           : CN={31B2F340-016D-11D2-945F-00C04FB984F9},\
               CN=Policies,CN=System,DC=example,DC=net
version      : 65539
flags        : NONE

GPO          : {4E93D4F2-C21F-49A0-A299-A4DD59CA0F75}
display name : systemsteuerung
path         : \\example.net\SysVol\example.net\Policies\\
               {4E93D4F2-C21F-49A0-A299-A4DD59CA0F75}
dn           : CN={4E93D4F2-C21F-49A0-A299-A4DD59CA0F75},\
               CN=Policies,CN=System,DC=example,DC=net
version      : 65536
flags        : NONE

GPO          : {6AC1786C-016F-11D2-945F-00C04fB984F9}
display name : Default Domain Controllers Policy
path         : \\example.net\sysvol\example.net\Policies\\
               {6AC1786C-016F-11D2-945F-00C04fB984F9}
dn           : CN={6AC1786C-016F-11D2-945F-00C04fB984F9},\
               CN=Policies,CN=System,DC=example,DC=net
version      : 1
flags        : NONE
```

Prüfen Sie ob alle Gruppenrichtlinen vorhanden sind. Wenn alle Gruppenrichtlinen vorhanden sind, ist die Migration abgeschlossen und Sie können den alten Windows-DC vom Netz nehmen. Sollten noch Gruppenrichtlinen fehlen, kopieren Sie diese von Hand.

20 Datensicherung

In diesem Abschnitt geht es nicht um die Sicherung der Daten, sondern um die Sicherung und Wiederherstellung der Konfiguration des DC. Also wie können Sie die Informationen des LDAP und der anderen Datenbanken, die für den Betrieb der Domäne und des Samba4-Servers relevant sind, sicher. Denn auch hinsichtlich eines Desaster Recoveries müssen Sie sich beim samba4 mehr Gedanken machen als vielleicht noch beim Samba3.

20.1 Sicherung der Datenbanken

In den Quellen von samba4 finden Sie das Skript source4/scripting/bin/samba_backup. Mithilfe dieses Skriptes können Sie alle relevanten Daten des Domaincontrollers sichern. Das Skript ist aber auf die Umgebung eines selbst kompilierten samba4 ausgelegt. Das Skript müssen Sie auf jeden Fall noch an die Umgebung der samba4-Installation aus den SerNet-Paketen anpassen: Im folgenden Listing sehen Sie das Skript für die Sicherung der Datenbanken mit den entsprechenden Anpassungen für diese Umgebung:

```
#!/bin/sh
#
# Copyright (C) Matthieu Patou <mat@matws.net> 2010-2011
#
# This program is free software; you can redistribute it and/or modify
# it under the terms of the GNU General Public License as published by
# the Free Software Foundation; either version 3 of the License, or
# (at your option) any later version.
#
# This program is distributed in the hope that it will be useful,
# but WITHOUT ANY WARRANTY; without even the implied warranty of
# MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
# GNU General Public License for more details.
#
# You should have received a copy of the GNU General Public License
# along with this program.  If not, see <http://www.gnu.org/licenses/>.
#

/etc/init.d/samba4 stop > /dev/null 2>&1
/etc/init.d/bind9 stop > /dev/null 2>&1

s=$(/usr/local/samba/sbin/samba -V)
version="$(echo $s |cut -d' ' -f2)"

mkdir -p /usr/local/backups/samba_$version
chmod 750 /usr/local/backups/samba_$version

FROMWHERE=/usr/local/samba
WHERE=/usr/local/backups/samba_$version
if [ -n "$1" ] && [ "$1" = "-h" -o "$1" = "--usage" ]; then
        echo "samba_backup [provisiondir] [destinationdir]"
        echo "Will backup your provision located in provisiondir to archive stored in destinationdir"
        echo "Default provisiondir: $FROMWHERE"
        echo "Default destinationdir: $WHERE"
        exit 0
fi
```

```
[ -n "$1" -a -d "$1" ]&&FROMWHERE=$1
[ -n "$2" -a -d "$2" ]&&WHERE=$2

DIRS="private etc sysvol"
#Number of days to keep the backup
DAYS="90"
WHEN=`date +%d%m%y`

if [ ! -d $WHERE ]; then
        echo "Missing backup directory $WHERE"
        exit 1
fi

if [ ! -d $FROMWHERE ]; then
        echo "Missing or wrong provision directory $FROMWHERE"
        exit 1
fi

cd $FROMWHERE
for d in $DIRS;do
        relativedirname=`find . -type d -name "$d" -prune`
        n=`echo $d | sed 's/\//_/g'`
        if [ "$d" = "private" ]; then
                find $relativedirname -name "*.ldb.bak" -exec rm {} \;
                for ldb in `find $relativedirname -name "*.ldb"`; do
                        tdbbackup $ldb
                        if [ $? -ne 0 ]; then
                                echo "Error while backuping $ldb"
                                exit 1
                        fi
                done
                tar cjf ${WHERE}/${n}.${WHEN}.tar.bz2  $relativedirname --exclude=*.ldb >/dev/null 2>&1
                if [ $? -ne 0 ]; then
                        echo "Error while archiving ${WHERE}/${n}.${WHEN}.tar.bz2"
                        exit 1
                fi
                find $relativedirname -name "*.ldb.bak" -exec rm {} \;
        else
                tar cjf ${WHERE}/${n}.${WHEN}.tar.bz2  $relativedirname >/dev/null 2>&1
                if [ $? -ne 0 ]; then
                        echo "Error while archiving ${WHERE}/${n}.${WHEN}.tar.bz2"
                        exit 1
                fi
        fi
done

/etc/init.d/bind9 start > /dev/null 2>&1
/etc/init.d/samba4 start > /dev/null 2>&1

find $WHERE -name "*.tar.bz2" -mtime +$DAYS -exec rm  {} \; > /dev/null 2>&1
```

Hinweis !

Das Skript wurde von Matthieu Patou erstellt und von Armin Breier an die SerNet-Pakete angepasst und verbessert und in einer Produktivumgebung getestet.

Wichtig ist, dass Sie die beiden Variablen `FROMWHERE` und `WHERE` richtig setzen. Achten Sie darauf, dass Sie das Verzeichnis in dem die Datensicherung gespeichert werden soll auch vor der Sicherung angelegt haben. Nach der lokalen Sicherung der Daten, sollten Sie auch noch dafür sorgen, dass

die Daten auch auf einen anderen Server kopiert werden, für den Fall, dass der Server vollständig ausfällt.
Auf dem Verzeichnis /var/lib/samba/sysvol befinden sich neben den Unix-Dateisystemrechten auch noch ACLs, die nicht mit *tar* gesichert werden können, die aber für den ordnungsgemäßen Betrieb des Domaincontrollers wichtig sind. Diese ACLs können Sie mit dem Kommando `getfacl` sichern. Im folgenden Listing sehen Sie ein Auflistung aller ACLs und einer anschließenden Sicherung der ACLs in eine Datei:

```
root@samba4-1:/var/lib/samba# getfacl -R sysvol/
# file: sysvol/
# owner: root
# group: 3000000
user::rwx
user:root:rwx
group::rwx
group:3000000:rwx
group:3000001:r-x
group:3000002:rwx
group:3000003:r-x
mask::rwx
other::---
default:user::rwx
default:user:root:rwx
default:group::---
default:group:3000000:rwx
default:group:3000001:r-x
default:group:3000002:rwx
default:group:3000003:r-x
default:mask::rwx
default:other::---

# file: sysvol//example.net
# owner: root
# group: 3000000
user::rwx
user:root:rwx
group::rwx
group:3000000:rwx
group:3000001:r-x
group:3000002:rwx
group:3000003:r-x
mask::rwx
other::---
default:user::rwx
default:user:root:rwx
default:group::---
default:group:3000000:rwx
default:group:3000001:r-x
default:group:3000002:rwx
default:group:3000003:r-x
default:mask::rwx
default:other::---

# file: sysvol//example.net/Policies
# owner: root
# group: 3000000
user::rwx
user:root:rwx
```

```
group::rwx
group:3000000:rwx
group:3000001:r-x
group:3000002:rwx
group:3000003:r-x
group:EXAMPLE\134Group\040Policy\040Creator\040Owners:rwx
mask::rwx
other::---
default:user::rwx
default:user:root:rwx
default:group::---
default:group:3000000:rwx
default:group:3000001:r-x
default:group:3000002:rwx
default:group:3000003:r-x
default:group:EXAMPLE\134Group\040Policy\040Creator\040Owners:rwx
droot@samba4-1:/var/lib/samba# getfacl -R sysvol/
# file: sysvol/
# owner: root
# group: 3000000
user::rwx
user:root:rwx
group::rwx
group:3000000:rwx
group:3000001:r-x
group:3000002:rwx
group:3000003:r-x
mask::rwx
other::---
default:user::rwx
default:user:root:rwx
default:group::---
default:group:3000000:rwx
default:group:3000001:r-x
default:group:3000002:rwx
default:group:3000003:r-x
default:mask::rwx
default:other::---

# file: sysvol//example.net
# owner: root
# group: 3000000
user::rwx
user:root:rwx
group::rwx
group:3000000:rwx
group:3000001:r-x
group:3000002:rwx
group:3000003:r-x
mask::rwx
other::---
default:user::rwx
default:user:root:rwx
default:group::---
default:group:3000000:rwx
default:group:3000001:r-x
default:group:3000002:rwx
default:group:3000003:r-x
```

```
default:mask::rwx
default:other::---
.
.
.
root@samba4-1:/var/lib/samba# getfacl -R sysvol/ > /tdb-backup/sysvol-acl.back
```

Neben den tdb-Dateien, der Freigabe sysvol und den ACLs sollten Sie auch noch die Konfigurationsdatei /etc/samba/smb.conf sichern. Wenn Sie Ihre Freigaben nicht mehr in der Datei smb.conf sichern, sollten Sie auf jeden Fall die *Registry* mit den entsprechenden Einträgen mit dem Kommando `net registry export hklm\software\samba /tdb-backup/share-reg.back` sichern. Damit haben Sie alle Daten gesichert um einen ausgefallen Domaincontroller wiederherstellen zu können.

20.2 Wiederherstellung der Datenbanken

ACHTUNG !

Sollten Sie noch einen laufenden Domaincontroller haben, stellen Sie niemals die Daten eines Domaincontrollers aus dem Backup wieder her. Nehmen Sie den Server neu in die Domäne auf, damit sich die Daten dann von dem noch laufenden Domaincontroller automatisch replizieren. Ein Backup der Daten würde die bestehenden Datenbanken auf anderen Domaincontrollern unbrauchbar machen und die Domäne wäre im schlimmsten Fall verloren.

Die folgenden Punkte sollten Sie für den Fall einer Wiederherstellung berücksichtigen:

1. Führen Sie niemals ein Upgrade auf eine neue samba4 Version und die Wiederherstellung gleichzeitig durch.
2. Verwenden Sie immer die selbe IP-Adresse und den selben Hostname für das neue System. Anderenfalls bekommen Sie Problem mit dem DNS und Kerberos.
3. Verwenden Sie möglichst die selbe Distribution wie bei dem alten Server, das die Pfade in den verschieden Distributionen oft unterschiedlich sind.

Bevor Sie an dieser Stelle weiter machen, nochmal der Hinweis: Es darf kein weiterer Domaincontroller mehr in der Domäne vorhanden sein!
Installieren Sie einen neuen Domaincontroller anschließend stoppen Sie den samba4-Dienst und löschen die folgenden Dateien und Verzeichnisse:

```
root@samba4-1:~#rm  /etc/samba/smb.conf
root@samba4-1:~#rm -rf /var/lib/samba/private
root@samba4-1:~#rm -rf /var/lib/samba/sysvol
```

Entpacken Sie die Datensicherungen in die original Verzeichnisse:

```
root@samba4-1:~#tar -jxf samba4_private.{Timestamp}.tar.bz2 -C /var/lib/samba/
root@samba4-1:~#tar -jxf sysvol.{Timestamp}.tar.bz2 -C /var/lib/samba/
```

Stellen Sie die ACLs für das Verzeichnis sysvol wieder her:

```
root@samba4-1:~#/var/lib/samba# setfacl --restore=/tdb-backup/sysvol-acl.back
sysvol/: *,*
sysvol//example.net: *,*
sysvol//example.net/Policies: *,*
sysvol//example.net/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}: *,*
sysvol//example.net/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/GPT.INI: *,*
sysvol//example.net/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE: *,*
sysvol//example.net/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/USER: *,*
sysvol//example.net/Policies/{7774A3DB-4B0B-41F9-9359-D3782D9ED1B1}: *,*
sysvol//example.net/Policies/{7774A3DB-4B0B-41F9-9359-D3782D9ED1B1}/GPT.INI: *,*
sysvol//example.net/Policies/{7774A3DB-4B0B-41F9-9359-D3782D9ED1B1}/User: *,*
sysvol//example.net/Policies/{7774A3DB-4B0B-41F9-9359-D3782D9ED1B1}/User/Registry.pol: *,*
sysvol//example.net/Policies/{7774A3DB-4B0B-41F9-9359-D3782D9ED1B1}/Machine: *,*
sysvol//example.net/Policies/{6AC1786C-016F-11D2-945F-00C04FB984F9}: *,*
sysvol//example.net/Policies/{6AC1786C-016F-11D2-945F-00C04FB984F9}/GPT.INI: *,*
sysvol//example.net/Policies/{6AC1786C-016F-11D2-945F-00C04FB984F9}/MACHINE: *,*
sysvol//example.net/Policies/{6AC1786C-016F-11D2-945F-00C04FB984F9}/USER: *,*
sysvol//example.net/scripts: *,*
sysvol//example.net/scripts/alle.bat: *,*
```

Bei der Sicherung der Datenbanken im Verzeichnis private wurde bei den ldb-Dateien immer die Endung .back angehängt, diese Endung müssen Sie jetzt wieder entfernen:

```
root@samba4-1:~# find /var/lib/samba/private -type f -name '*.ldb.bak' -print0 |\
                 while read -d $'\0' f ; do mv "$f" "${f%.bak}" ; done
```

Sollten Sie vergessen haben, die ACLs des Verzeichnis sysvol zu sichern, können Sie die ACLs mit dem Kommando `samba-tool ntacl sysvolreset` wiederherstellen.
Natürlich können Sie auch einzelne Datenbanken wiederherstellen, denken Sie nur daran, dass die verschieben Datenbanken oft Abhängigkeiten untereinander haben.
Wenn Sie die Skripte zur Sicherung der AD-Datenbanken regelmäßig durchführen und auf einen anderen Server verschieben, sind Sie für den Fall eines Totalausfalls ihrer Domäne gerüstet und können die Datenbanken wiederherstellen. Auf jeden Fall ist es eine gute Idee, immer mindestens zwei Domänencontroller in der Domäne zu haben.

21 Samba4 als Printserver

Auch die Funktion des Printserver kann samba4 wieder übernehmen. Da die File- und Printservices direkt aus Samba3 übernommen wurden, hat sich bei der Konfiguration eines Printservers hier nichts geändert. Sie können über einen zentralen Printserver die Drucker in Ihrer Domäne verwalten und die Druckertreiber an die Clients verteilen, genau wie bei einem Windows-Printserver. Sie können die Treiber bis zur Version 3 bereitstellen, dass sind Treiber bis Windows7. Die Treiber für Windows8 sind Treiber der Version 4, diese werden momentan von Samba noch nicht unterstützt.
Den Printserver sollten Sie, wenn es möglich ist, immer auf einem Fileserver installieren und nicht auf einem Domaincontroller. Sie sollten auch immer dafür sorgen, dass das Verzeichnis /var eine eigene Partition ist, denn dort wird das *Spooling* der Druckaufträge gespeichert.

21.1 Vorbereitungen

Damit Sie überhaupt Drucker über samba4 bereitstellen können, müssen Sie das *CUPS*-Drucksystem installieren. Denn *CUPS* verwaltet die Drucker und sendet die Druckaufträge an die Drucker. Samba nutzt die Drucker im *CUPS* um diese den Windows-Clients zur Verfügung zu

stellen. Alle Drucker müssen zuerst unter *CUPS* installiert werden, damit Samba die Drucker erkennen kann.
Bei älteren Samba-Versionen gab es einen Parameter `printer admin = user,@gruppe`, diesen Parameter gibt es heute so nicht mehr. Die Rechte zur Verwaltung von Druckern hängen heute an einem Windows-Privileg. Diese Privilegien geben Benutzern oder Gruppen Systemrechte. Welche Gruppen und Benutzer welche Systemprivilegien haben können Sie sich wie im folgenden Listing anzeigen lassen:

```
 root@fileserver:~# net rpc rights list accounts -Uadministrator
Enter administrator's password:
BUILTIN\Print Operators
SeLoadDriverPrivilege
SeShutdownPrivilege
SeInteractiveLogonRight

BUILTIN\Account Operators
SeInteractiveLogonRight

BUILTIN\Backup Operators
SeBackupPrivilege
SeRestorePrivilege
SeShutdownPrivilege
SeInteractiveLogonRight

BUILTIN\Administrators
SeSecurityPrivilege
SeBackupPrivilege
SeRestorePrivilege
SeSystemtimePrivilege
SeShutdownPrivilege
SeRemoteShutdownPrivilege
SeTakeOwnershipPrivilege
SeDebugPrivilege
SeSystemEnvironmentPrivilege
SeSystemProfilePrivilege
SeProfileSingleProcessPrivilege
SeIncreaseBasePriorityPrivilege
SeLoadDriverPrivilege
SeCreatePagefilePrivilege
SeIncreaseQuotaPrivilege
SeChangeNotifyPrivilege
SeUndockPrivilege
SeManageVolumePrivilege
SeImpersonatePrivilege
SeCreateGlobalPrivilege
SeEnableDelegationPrivilege
SeInteractiveLogonRight
SeNetworkLogonRight
SeRemoteInteractiveLogonRight

BUILTIN\Server Operators
SeBackupPrivilege
SeSystemtimePrivilege
SeRemoteShutdownPrivilege
SeRestorePrivilege
SeShutdownPrivilege
SeInteractiveLogonRight
```

```
BUILTIN\Pre-Windows 2000 Compatible Access
SeRemoteInteractiveLogonRight
SeChangeNotifyPrivilege
```

Ein Benutzer oder eine Gruppe, die später die Druckertreiber auf dem Server installieren können soll, muss das Privileg `SePrintOperatorPrivileg` besitzen. Dieses Privileg müssen Sie erst noch vergeben. Am besten ist es, wenn Sie dieses Privileg der Gruppe der Domänenadmins geben. Da in den meisten Fällen die Mitglieder dieser Gruppe die Printserver verwalten werden. Im folgenden Listing sehen Sie, wie sie dieses Privileg an die Gruppe vergeben und anschließen prüfen, ob das Privileg auch richtig gesetzt wurde:

```
root@fileserver:~# net rpc rights grant 'example\Domain Admins' SePrintOperatorPrivilege\
                   -Uadministrator
Enter administrator's password:
Successfully granted rights.

root@fileserver:~# net rpc rights list 'example\Domain Admins' -Uadministrator
Enter administrator's password:
SePrintOperatorPrivilege
```

Erst mit diesem Privileg ist die Gruppe der Domänenadministratoren berechtigt die Druckertreiber von einem Windows-Client aus zu installieren.

21.2 Einrichten der Freigaben

Für den Printserver benötigen Sie zwei Freigaben. Einmal die Freigabe printers und die Freigabe print$. Die Freigabe printers ist die Freigabe in der die Druckaufträge gespoolt werden und in der Freigabe print$ werden die Druckertreiber für die Netzwerkinstallation auf den Clients abgelegt. Für die Freigabe printers müssen Sie als erstes ein Verzeichnis für das Spooling anlegen und dann die entsprechenden Freigabe einrichten. Im folgenden Listing sehen Sie die einzelnen Schritt:

```
root@fileserver:~# mkdir /var/spool/samba

root@fileserver:~# chmod 777 /var/spool/samba/

root@fileserver:~# net conf addshare printers /var/spool/samba/ writeable=y guest_ok=n\
                   "Druckerspooling"

root@fileserver:~# net conf setparm printers "browsable" "yes"

root@fileserver:~# net conf setparm printers "printable" "yes"

root@fileserver:~# net conf setparm printers "create mask" "0700"
```

Das das Verzeichnis dem Benutzer *root* gehört, müssen sie *others* auch alle Rechte an dem Verzeichnis geben. Damit nicht jeder Benutzer einfach die Druckaufträge anderer Benutzer löschen kann, sollten Sie in der Freigabe `priners`, den Parameter `create mask = 0700` setzen, dadurch hat nur der Besitzer eines Druckauftrages Rechte an dem Eintrag.
Ohne den Parameter `browsable = yes` wären die Drucker später in der Netzwerkumgebung der Clients nicht sichtbar und ein Benutzer könnte sich nicht mit den Druckern verbinden.
Die Druckertreiber müssen in einer von Windows fest vorgegebenen Verzeichnisstruktur abgelegt werden. Diese wurde bei der Installation der samba4-Pakete bereits mit angelegt. Sie finden

die Verzeichnisse unter /var/lib/samba/drivers. In dem Verzeichnis finden Sie verschiedene Unterverzeichnisse, die nach verschiedenen Systemarchitekturen benannt sind. Im Moment sind diese Verzeichnisse noch leer. Beim späteren Einspielen der Druckertreiber werden dort weiter Unterverzeichnisse für die verschiedenen Treiberversionen angelegt. Sie müssen jetzt nur die entsprechende Freigabe wie im folgenden Listing anlegen:

```
root@fileserver:~# net conf addshare 'print$' /var/lib/samba/drivers/ writeable=y\
                   guest_ok=n "Druckertreiber"

root@fileserver:~# net conf setparm 'print$' "create mask" "0775"

root@fileserver:~# net conf setparm 'print$' "inherit permissions" "yes"
```

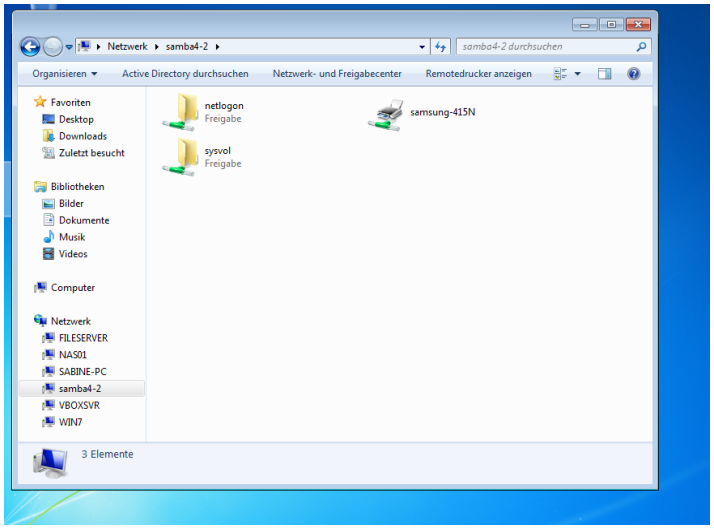
Über den Parameter `create mask = 0775` stellen Sie sicher, dass bei allen Dateien die später auf den Server kopiert werden, dass Execute-Recht gesetzt ist. Einige Treiber benötigen diese Recht um die Installation auf dem Client durchführen zu können. Da einige Treiber auch noch Unterverzeichnis erzeugen, sorgt der Parameter `inherit permissions = yes` dafür, dass die Rechte auch in den Unterverzeichnissen richtig gesetzt sind. Damit die Domänenbenutzer auch auf die Treiber zugreifen können, setzen Sie den Parameter `valid users = @domain users`. Der Parameter `admin users = @domain admins` sorgt dafür, dass die Gruppe der Domänenadministratoren das Schreibrecht am Verzeichnis bekommen, wenn Sie Druckertreiber installieren.

21.3 Hochladen der Drucktreiber

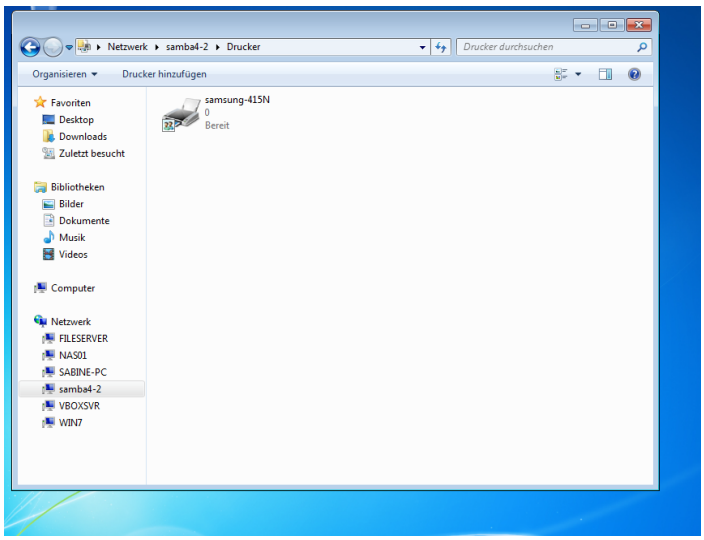
Hinweis !

Besorgen Sie sich als erstes die Druckertreiber für Ihren Drucker, sollten die Treiber gepackt sein, dann müssen Sie diese als erstes entpacken.

Die Druckertreiber lassen sich am einfachsten über einen Windows-Client hoch laden. Dazu melden Sie sich am Client als Domänenadministrator an, dieser hat über die Gruppe der Domänenadministratoren das entsprechende Privilegien. Jetzt starten Sie den *Explorer* und suchen über die Netzwerkumgebung den Server, auf dem Sie den Printserver installiert haben. Markieren Sie den Server durch einen einfachen Klick. Daraufhin erscheinen auf der rechten Seite alle Freigaben und Drucker, so wie Sie es in der folgenden Abbildung sehen:



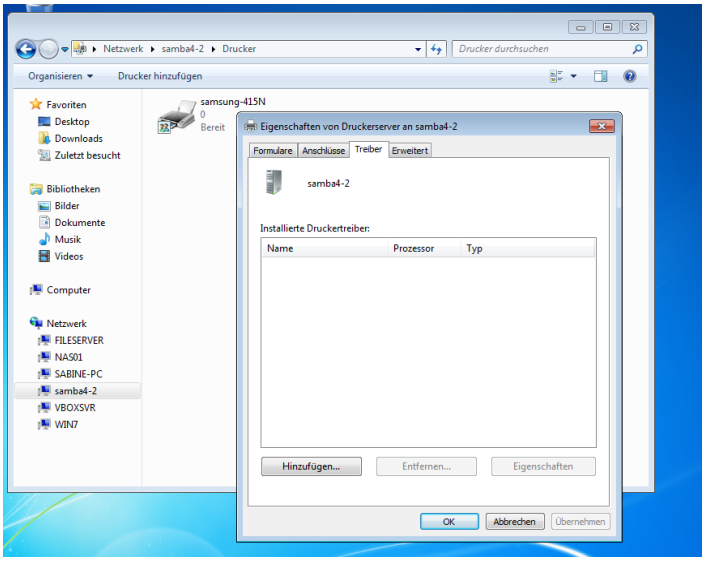
Klicken Sie jetzt, im Menü oberhalb der Freigaben und der Drucker, auf den Punkt *Remotedrucker Anzeigen*. Daraufhin sehen Sie jetzt nur noch die Drucker, die auf dem entsprechenden Server eingerichtet wurden. Sehen Sie dazu auch die folgende Abbildung:



Hinweis !

An dieser Stelle dürfen Sie auf keinen Fall auf den Drucker klicken für den Sie den Treiber installieren wollen. Denn dann würden Sie den Treiber lokal auf dem Client installieren und nicht auf dem Printserver.

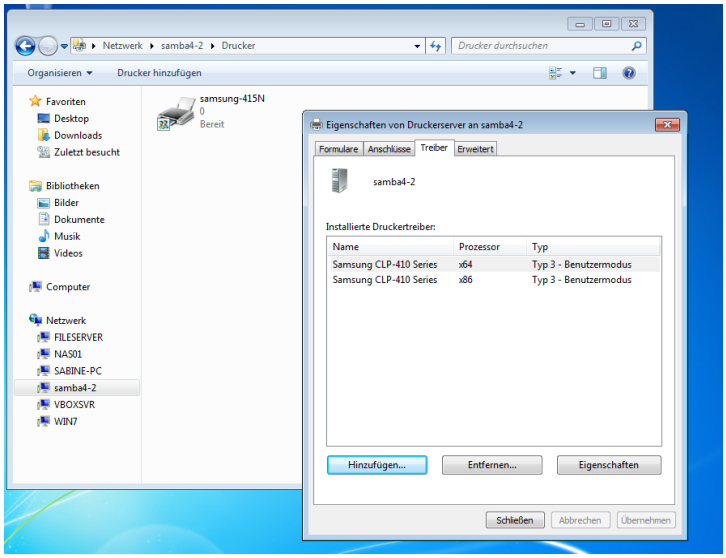
Klicken Sie jetzt irgendwo im Fenster auf der rechten Seite mit der rechten Maustaste. Es erscheint ein Kontextmenü. In diesem Kontextmenü wählen Sie den Punkt *Servereigenschaften...* aus. Daraufhin öffnet sich das Eigenschaftenfenster des Printservers. Klicken Sie hier auf *Treiber*. In der folgenden Abbildung sehen Sie das entsprechenden Fenster:



Klicken Sie anschließend auf *Hinzufügen* und folgen Sie den Assistenten. Im Anschluss sehen Sie, wie in der folgenden Abbildung, den gerade installierten Druckertreiber.

Hinweis !

Sollte die Schaltfläche*Hinzufügen* nicht aktiv sein, fehlt dem Benutzer auf dem Server das Privileg `SePrintOperatorPrivilege`.



Sie sehen hier, dass sowohl die Treiber für 64-Bit System als auch für 32-Bit System installiert wurde. Prüfen Sie vor der Installation, ob Sie beide Versionen benötigen und installieren Sie nur die Versionen, für die entsprechenden Betriebssysteme in Ihrer Umgebung. Jetzt können alle Benutzer auf den Drucker über das Netzwerk zugreifen und den Treiber vom Server installieren.

21.4 Zuordnung des Druckertreibers

Damit die Windows-Clients später eine *Point'n'Print* Treiber Installation durchführen können, muss der Druckertreiber noch dem entsprechenden Drucker zugeordnet werden. Ohne diese Zuordnung wir zwar der Drucker auf dem Printserver gefunden, aber der entsprechende Druckertreiber kann bei der *Point'n'Print* Treiber Installation durch den Benutzer nicht gefunden werden. Als erstes müssen Sie den genauen Name des Druckers und des Druckertreibers kennen. Dazu suchen Sie auf dem Server nach dem Drucker mit dem Kommando `smbclient`. Im folgenden Listing sehen Sie die Suche:

```
root@samba4-2:~# smbclient -L localhost -Uadministrator
Enter administrator's password:
Domain=[EXAMPLE] OS=[Unix] Server=[Samba 4.0.7-SerNet-Debian-5.wheezy]

        Sharename       Type      Comment
        ---------       ----      -------
        IPC$            IPC       IPC Service (Samba 4.0.7-SerNet-Debian-5.wheezy)
        sysvol          Disk
        netlogon        Disk
        samsung-415N    Printer
        print$          Disk      Druckertreiber
Domain=[EXAMPLE] OS=[Unix] Server=[Samba 4.0.7-SerNet-Debian-5.wheezy]

        Server               Comment
        ---------            -------
```

```
        Workgroup            Master
        ---------            -------
```

Der Name des Druckers der jetzt mit einen Treiber verbunden werden soll lautet *samsung-415N*. Jetzt müssen Sie noch den genauen Namen des Treiber für diesen Drucker kennen. Alle Treiber die Sie auf dem Printserver installiert haben, sehen Sie mit dem Kommando `rpcclient`. Im folgenden Listing sehen Sie das Ergebnis des Kommandos:

```
root@samba4-2:~# rpcclient localhost -Uadministrator -c 'enumdrivers'
Enter administrator's password:

[Windows NT x86]
Printer Driver Info 1:
        Driver Name: [Samsung CLP-410 Series]


[Windows x64]
Printer Driver Info 1:
        Driver Name: [Samsung CLP-410 Series]
```

Jetzt müssen Sie den Druckertreiber den Drucker zuweisen, so wie Sie es im folgenden Listing sehen können:

```
root@samba4-2:~# rpcclient localhost -U administrator -c 'setdriver "samsung-415N"\
                           "Samsung CLP-410 Series"'
Enter administrator's password:
Successfully set samsung-415N to driver Samsung CLP-410 Series.
```

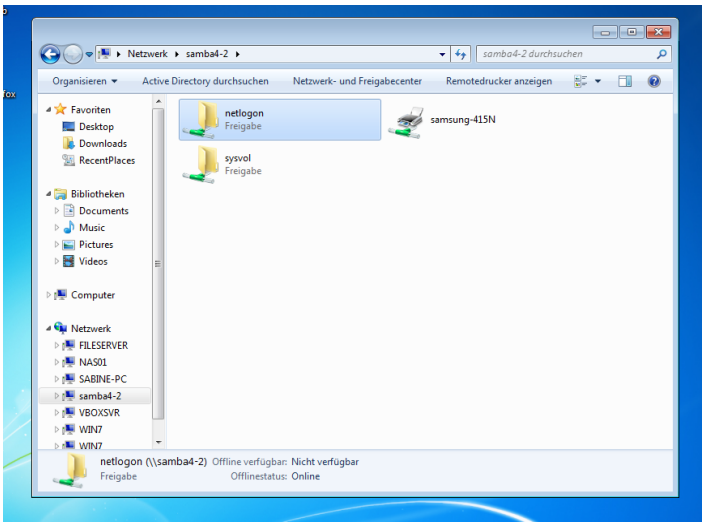
Jetzt können Sie die Zuordnung noch wie im folgenden Listing zu sehen ist, überprüfen:

```
root@samba4-2:~# rpcclient localhost -Uadministrator -c 'enumprinters'
Enter administrator's password:
        flags:[0x800000]
        name:[\\LOCALHOST\samsung-415N]
        description:[\\LOCALHOST\samsung-415N,Samsung CLP-410 Series,]
        comment:[]
```

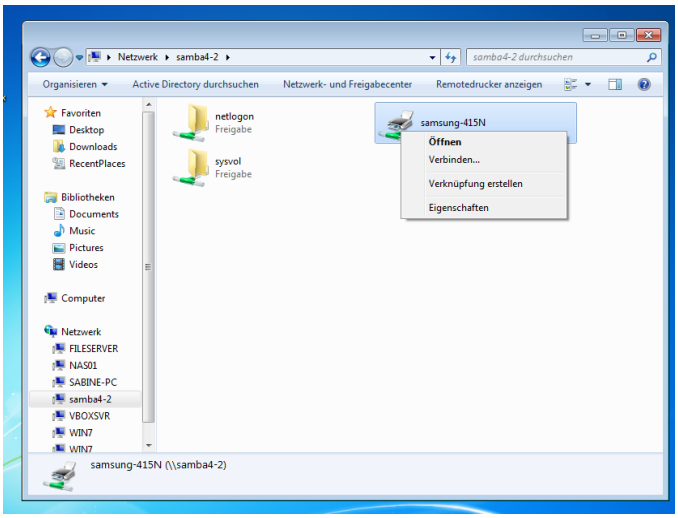
Damit ist jetzt der Druckertreiber dem Drucker zugeordnet und jeder Benutzer der Domäne kann sich mit dem Drucker verbinden und den Treiber für sich installieren, ohne über weiter Rechte im System zu verfügen.

21.5 Verbinden mit dem Drucker

Melden Sie sich jetzt als Benutzer (Nicht als Administrator) an einem Windows-Client an und starten den Explorer. Suchen Sie nach Ihrem Printserver. Der Freigegeben Drucker wird Ihnen, wie in der folgenden Abbildung, angezeigt:



Klicken Sie mit der rechten Maustaste auf den Drucker und es erscheint, so wie in der folgenden Abbildung, ein Kontextmenü:



Klicken Sie dort auf *Verbinden...*. Der Treiber wird sofort gesucht und im System eingebunden. Jetzt können Sie den Drucker nutzen.

22 Firewalls und Samba4

Im Gegensatz zu Samba3 müssen Sie bei samba4 einen etwas größeren Aufwand treiben hinsichtlich von Firewalls. Denn es werden zusätzliche Ports für die Kommunikation benötigt. Sie müssen unterscheiden, ob Ihr samba4-Server als Domaincontroller oder als Fileserver betrieben wird, davon ist abhängig, welche Ports Sie öffnen müssen. In der folgenden Tabelle sehen Sie, welche Ports für eine Domaincontroller geöffnet werden müssen:

Service	Port	Protocol
DNS	53	tcp/udp
Kerberos	88	tcp/udp
End Point Mapper (DCE/RPC Locator Service)	135	tcp
NetBIOS Nameservice	137	tcp
NetBIOS Datagramm	138	tcp
NetBIOS Session	139	tcp
LDAP	389	tcp
SMB over TCP	445	tcp
Kerberos kpasswd	464	tcp/udp
LDAPS (nur wenn "tls enabled = yes")	636	tcp
Dynamic RPC Ports	1024 - 5000	tcp
Global Cataloge	3268	tcp
Global Cataloge SSL (nur wenn "tls enabled = yes")	3269	tcp
Multicast DNS	5353	tcp/udp

Alle Ports können Sie mit dem Kommando `netstat` wie im folgenden Listing auflisten lassen.

```
root@samba4-1:~# netstat -tulpn | egrep "samba|smbd|nmbd"
tcp        0      0 0.0.0.0:464             0.0.0.0:*               LISTEN      2666/samba
tcp        0      0 0.0.0.0:53              0.0.0.0:*               LISTEN      2675/samba
tcp        0      0 0.0.0.0:88              0.0.0.0:*               LISTEN      2666/samba
tcp        0      0 0.0.0.0:636             0.0.0.0:*               LISTEN      2663/samba
tcp        0      0 0.0.0.0:445             0.0.0.0:*               LISTEN      2662/smbd
tcp        0      0 0.0.0.0:1024            0.0.0.0:*               LISTEN      2659/samba
tcp        0      0 0.0.0.0:3268            0.0.0.0:*               LISTEN      2663/samba
tcp        0      0 0.0.0.0:3269            0.0.0.0:*               LISTEN      2663/samba
tcp        0      0 0.0.0.0:389             0.0.0.0:*               LISTEN      2663/samba
tcp        0      0 0.0.0.0:135             0.0.0.0:*               LISTEN      2659/samba
tcp        0      0 0.0.0.0:139             0.0.0.0:*               LISTEN      2662/smbd
tcp6       0      0 :::464                  :::*                    LISTEN      2666/samba
tcp6       0      0 :::53                   :::*                    LISTEN      2675/samba
tcp6       0      0 :::88                   :::*                    LISTEN      2666/samba
tcp6       0      0 :::636                  :::*                    LISTEN      2663/samba
tcp6       0      0 :::445                  :::*                    LISTEN      2662/smbd
tcp6       0      0 :::1024                 :::*                    LISTEN      2659/samba
tcp6       0      0 :::3268                 :::*                    LISTEN      2663/samba
tcp6       0      0 :::3269                 :::*                    LISTEN      2663/samba
tcp6       0      0 :::389                  :::*                    LISTEN      2663/samba
tcp6       0      0 :::135                  :::*                    LISTEN      2659/samba
tcp6       0      0 :::139                  :::*                    LISTEN      2662/smbd
udp        0      0 192.168.123.170:464     0.0.0.0:*                           2666/samba
udp        0      0 0.0.0.0:464             0.0.0.0:*                           2666/samba
udp        0      0 0.0.0.0:53              0.0.0.0:*                           2675/samba
udp        0      0 192.168.123.170:88      0.0.0.0:*                           2666/samba
udp        0      0 0.0.0.0:88              0.0.0.0:*                           2666/samba
udp        0      0 192.168.123.170:137     0.0.0.0:*                           2660/samba
udp        0      0 192.168.123.255:137     0.0.0.0:*                           2660/samba
udp        0      0 0.0.0.0:137             0.0.0.0:*                           2660/samba
udp        0      0 192.168.123.170:138     0.0.0.0:*                           2660/samba
udp        0      0 192.168.123.255:138     0.0.0.0:*                           2660/samba
udp        0      0 0.0.0.0:138             0.0.0.0:*                           2660/samba
udp        0      0 192.168.123.170:389     0.0.0.0:*                           2664/samba
udp        0      0 0.0.0.0:389             0.0.0.0:*                           2664/samba
udp6       0      0 2003:5c:ad0d:a701:a:464 :::*                                2666/samba
udp6       0      0 :::464                  :::*                                2666/samba
```

```
udp6       0      0 :::53                   :::*                                2675/samba
udp6       0      0 2003:5c:ad0d:a701:a0:88 :::*                                2666/samba
udp6       0      0 :::88                   :::*                                2666/samba
udp6       0      0 2003:5c:ad0d:a701:a:389 :::*                                2664/samba
udp6       0      0 :::389                  :::*                                2664/samba
```

Auf einem Fileserver werden erheblich weniger Ports benötigt, da hier keine Authentifizierung der Benutzer durchgeführt wird. In der folgenden Tabelle sehen Sie alle Ports, die für einen Fileserver geöffnet sein müssen:

Service	Port	Protocol
End Point Mapper (DCE/RPC Locator Service)	135	tcp
NetBIOS Nameservice	137	tcp
NetBIOS Datagramm	138	tcp
NetBIOS Session	139	tcp
SMB over TCP	445	tcp

Auch hier können Sie sich die verwendeten Ports wieder mit dem Kommando `netstat`, wie im folgenden Listing, anzeigen lassen:

```
root@fileserver:~# netstat -tulpn | egrep "samba|smbd|nmbd"
tcp        0      0 0.0.0.0:445             0.0.0.0:*         LISTEN      2463/smbd
tcp        0      0 0.0.0.0:139             0.0.0.0:*         LISTEN      2463/smbd
tcp6       0      0 :::445                  :::*              LISTEN      2463/smbd
tcp6       0      0 :::139                  :::*              LISTEN      2463/smbd
udp        0      0 192.168.123.255:137     0.0.0.0:*                     2420/nmbd
udp        0      0 192.168.123.172:137     0.0.0.0:*                     2420/nmbd
udp        0      0 0.0.0.0:137             0.0.0.0:*                     2420/nmbd
udp        0      0 192.168.123.255:138     0.0.0.0:*                     2420/nmbd
udp        0      0 192.168.123.172:138     0.0.0.0:*                     2420/nmbd
udp        0      0 0.0.0.0:138             0.0.0.0:*                     2420/nmbd
```

Die Verwendung der Ports stimmt mit der von Windows überein, da bei samba4 alle Dienste des AD umgesetzt wurden. Die Anzahl der geöffneten `smb`-Ports ist abhängig von den Verbindungen zum Fileserver, da für jede Verbindung ein eigener *smb-Prozess* gestartet wird.

23 Anhang

Im Anhang wird die Installation von samba4 aus den Quellen und die Installation des swat2 besprochen. Hierbei wird auch auf die Möglichkeit eingegangen, einen eigen *bind9*-Nameserver anstelle des internen Nameservers von samba4 zu verwenden. Beides ist nur aus Vollständigkeitsgründen in der Unterlage enthalten und nicht Bestandteil dieses Seminars.

24 Entwicklungsumgebung installieren

Wenn Sie samba4 aus den Quellen installieren wollen, benötigen Sie auf Ihrem System die Entwicklungsumgebung um die Pakete zu erstellen. Dazu müssen einige Pakete zusätzlich installiert werden. Die Installation der Pakete führen Sie mit dem Kommando im folgenden Listing aus:

```
root@samba4-1:~# apt-get install build-essential libacl1-dev libattr1-dev libblkid-dev\
                 libgnutls-dev libreadline-dev python-dev python-dnspython
                 gdb pkg-config libpopt-dev libldap2-dev libbsd-dev attr krb5-user\
                 docbook-xsl libcups2-dev\newline git acl checkinstall gettext
```

Während der Installation des *krb5-user*-Paketes werden Sie nach dem *REALM* für Ihre Kerberos-Domäne gefragt, geben Sie hier bitte den Namen Ihrer DNS-Domäne ein. In dieser Unterlage ist das `EXAMPLE.NET`. Achten Sie hier auf die Großschreibung. Dann werden Sie noch nach dem Kerberos-Server für den *REALM* und dem Admin-Server für den *REALM* gefragt. Geben Sie hier den fqdn Ihres samba4 Servers an, da der erste samba4-Server die Rolle des Kerberos-Servers übernehmen wird. In dieser Unterlage ist das jeweils der Name *samba4-1.example.net*.

25 Installation von Samba4 aus den Quellen

Nach dem Sie die Entwicklungsumgebung installiert haben kann die Installation von samba4 beginnen. Die aktuellen Quellen lassen sich am besten mit `git` herunterladen. Dazu verwenden Sie das folgende Kommando:

```
root@samba4-1:~# git clone -b v4-0-stable git://git.samba.org/samba.git samba4
Cloning into samba4...
remote: Counting objects: 1114939, done.
remote: Compressing objects: 100% (252154/252154), done.
remote: Total 1114939 (delta 862962), reused 1108089 (delta 857032)
Receiving objects: 100% (1114939/1114939), 217.35 MiB | 1.29 MiB/s, done.
Resolving deltas: 100% (862962/862962), done.
```

25.1 Kompilieren und bauen der Pakete

Jetzt haben Sie ein Verzeichnis samba4 in Ihrem aktuellen Verzeichnis in dem sich die Quellen für den samba4 befinden. Jetzt gibt es zwei Möglichkeiten Samba zu installieren. Die erste ist, Sie können den normalen Linux-Dreikampf aus `configure`, `make` und `make install` durchführen. Das hat den Nachteil, dass die Pakete nicht über die Paketdatenbank verwaltet werden und eine Deinstallation etwas aufwendiger ist. Bei der zweiten Möglichkeit verwenden Sie das Programm `checkinstall`. Das hat den Vorteil, dass Sie hierbei ein .deb-Paket erstellen, das Sie dann mit `dpkg -i <paket>` installieren und auch wieder deinstallieren können. In dieser Unterlage wird der Weg über `checkinstall` erklärt. Hier folgen jetzt die einzelnen Schritte bis zur Installation. Alle Schritte werden immer im Verzeichnis samba4 durchgeführt:

25.2 Erstellen der Konfiguration mit`configure`

Vor dem ersten Schritt wechseln Sie in das neue Verzeichnis ./samba4. Im ersten Schritt wir die Konfiguration für Ihr System ermittelt. Das geschieht mit dem Kommando `./configure --enable-debug --enable-selftest`. Je nach Rechenleistung Ihrer Maschine kommt nach einiger Zeit die Meldung `'configure' finished successfully (2m55.086s)`. Im Verzeichnis samba4 befindet sich jetzt die Datei Makefile

25.3 Kompilieren der Quellen mit `make`

Jetzt werden die Quellen mit `make` kompiliert. Auch hier ist die Dauer wieder abhängig von der Leistungsfähigkeit Ihres Systems. Am Ende des Kompilierungsprozesses erhalten Sie die Meldung `'build' finished successfully (24m45.647s)`

25.4 Bauen der Pakete mit `checkinstall`

Jetzt können Sie die Pakete mit `checkinstall` bauen. Bei der Ausführung von `checkinstall` werden einige Fragen zur Paketerstellung gestellt. Sie können die Informationen anpassen oder einfach übernehmen. Am Ende des Prozesses haben Sie dann ein .deb-Paket.
Die Erstellung von Paketen mittels `checkinstall` ist nicht geeignet um Pakete für verschieden System oder Debian-Distributionen zu bauen. Die Pakete die Sie hiermit erstellen sind genau auf das System angepasst und lassen sich nicht unbedingt überall installiere. Wenn Sie samba4 aus den Quellen bauen wollen und diese Pakete anschließend auf verschiedenen Systemen zum Einsatz bringen wollen, dann sollten Sie sich genauer mit der Erstellung von Debian-Paketen befassen und eventuell ein eigenes Repository für die Pakete erstellen. so können Sie nach einem update der Pakete alle System aktualisieren.

25.5 Installation des **.deb**-Paket mit `dpkg`

Jetzt können Sie das Paket mit `dpkg -i <paketname.deb>` installieren. Wenn Sie sich im Anschluss die Liste der Installierten Dateien mit `dpkg -L samba4` ansehen, stellen Sie fest, dass alle Dateien nach /usr/local installiert wurden. Nach der Installation der Pakete sollten Sie darauf achten, dass die Verzeichnisse /usr/local/samba/bin und /usr/local/samba/sbin in der Variablen `$PATH` enthalten sind.

25.6 Verlinkung der winbind-Libraries

Damit später die Gruppen und Benutzer mit `getent` angezeigt werden können, müssen die Libraries für den *winbind* noch im System bekannt gemacht werden. Wie Sie die Libraries in Ihrem System bekannt machen, sehen Sie im folgenden Listing:

```
root@samba4-1:~/samba4# ln -s /usr/local/samba/lib/libnss_winbind.so /usr/lib
root@samba4-1:~/samba4# ln -s /usr/local/samba/lib/libnss_winbind.so.2 /usr/lib
root@samba4-1:~/samba4# ln -s /usr/local/samba/lib/libwbclient.so.* /usr/lib
```

Damit ist die Installation der Pakete aus den Quellen abgeschlossen.

26 Konfiguration des Domaincontrollers mit einem *Bind9*

Jetzt beginnt die Konfiguration des *Domaincontrollers (dc)*. Dazu wird das Kommando `samba-tool domain provision` verwendet. Während der Installation haben Sie die Möglichkeit den von samba4 mitgelieferten DNS-Server zu nutzen, oder aber eine *Bind9*-Nameserver zu verwenden. Wenn Sie den von samba4 bereitgestellten DNS-Server verwenden, haben Sie den Vorteil, dass Sie die gesamte Administration des DNS später über die Windows-Tools realisieren können.
In der Unterlage werden beide Installationen beschrieben, bei der Installation aus den Quellen aber nur die Installation mit dem *bind9*-Nameserver. Achten Sie darauf, dass wenn Sie *Bind9*

verwenden wollen, dass Sie eine Version ab 9.8.x verwenden. Sollten Sie beim Versuch den *dc* zu konfigurieren die folgende Fehlermeldung nach der Eingabe des Kommandos `samba-tool domain provision` erhalten:

```
 root@samba4-1:~/samba4# samba-tool domain provision
Realm [EXAMPLE.NET]: EXAMPLE.NET
 Domain [EXAMPLE]: EXAMPLE
 Server Role (dc, member, standalone) [dc]: dc
 DNS backend (SAMBA_INTERNAL, BIND9_FLATFILE, BIND9_DLZ, NONE)\
      [SAMBA_INTERNAL]: BIND9_DLZ
 DNS forwarder IP address (write 'none' to disable forwarding)\
      [127.0.0.1]: 192.168.123.102
Administrator password:
Retype password:
Looking up IPv4 addresses
Looking up IPv6 addresses
ERROR(<type 'exceptions.OSError'>): uncaught exception - [Errno 2] \
      No such file or directory: '/usr/local/samba/var/locks'
  File "/usr/local/samba/lib/python2.6/site-packages/samba/netcmd/__init__.py",\
line 175, in _run
    return self.run(*args, **kwargs)
  File "/usr/local/samba/lib/python2.6/site-packages/samba/netcmd/domain.py",\
line 398, in run
    use_rfc2307=use_rfc2307, skip_sysvolacl=False)
  File "/usr/local/samba/lib/python2.6/site-packages/samba/provision/__init__.py",\
line 2019, in provision
    os.mkdir(paths.state_dir)
```

Dann fehlt das Verzeichnis /usr/local/samba/var/. Erzeugen Sie das Verzeichnis und starten Sie das Programm erneut.
Wenn das Verzeichnis vorhanden ist, läuft die Konfiguration des samba4 so ab, wie Sie es im folgenden Listing sehen:

```
root@samba4-1:~/samba4# samba-tool domain provision
Realm [EXAMPLE.NET]:
Domain [EXAMPLE]:
Server Role (dc, member, standalone) [dc]:
DNS backend (SAMBA_INTERNAL, BIND9_FLATFILE, BIND9_DLZ, NONE)\
      [SAMBA_INTERNAL]: BIND9_DLZ
Administrator password:
Retype password:
Looking up IPv4 addresses
Looking up IPv6 addresses
Setting up secrets.ldb
Setting up the registry
Setting up the privileges database
Setting up idmap db
Setting up SAM db
Setting up sam.ldb partitions and settings
Setting up sam.ldb rootDSE
Pre-loading the Samba 4 and AD schema
Adding DomainDN: DC=example,DC=net
Adding configuration container
Setting up sam.ldb schema
Setting up sam.ldb configuration data
Setting up display specifiers
Modifying display specifiers
```

```
Adding users container
Modifying users container
Adding computers container
Modifying computers container
Setting up sam.ldb data
Setting up well known security principals
Setting up sam.ldb users and groups
Setting up self join
Adding DNS accounts
Creating CN=MicrosoftDNS,CN=System,DC=example,DC=net
The zone reload and thaw was successful.
See /usr/local/samba/private/named.conf for an example configuration\
    include file for BIND
and /usr/local/samba/private/named.txt for further documentation required\
    for secure DNS updates
Setting up sam.ldb rootDSE marking as synchronized
Fixing provision GUIDs
A Kerberos configuration suitable for Samba 4 has been generated at\
    /usr/local/samba/private/krb5.conf
Once the above files are installed, your Samba4 server will be ready to use
Server Role:           active directory domain controller
Hostname:              samba4-1
NetBIOS Domain:        EXAMPLE
DNS Domain:            example.net
DOMAIN SID:            S-1-5-21-3856655574-465959103-413947164
```

Hinweis !

Bei der Vergabe des Passworts achten Sie darauf, mindesten 7 Zeichen anzugeben. Das Passwort muss Buchstaben, Zahlen und Sonderzeichen enthalten.

Überprüfen Sie nach der Installation, ob der richtige Nameserver und die richtige Domäne in Ihrer /etc/resolv.conf eingetragen sind. Sie sehen hier, dass bei der Konfiguration des Nameservers der interne DNS-Server vom samba4 vorgeschlagen wird. Dieses wurde an der Stelle durch Angabe des Wertes `BIND9_DLZ` geändert. Dadurch wird der interne DNS-Server nicht konfiguriert, sondern nur die benötigten Zonen-Dateien für den *bind9* erstellt.

27 Konfiguration des DNS-Servers für Samba4

Jetzt kann der DNS-Server mit den vorbereiteten Konfigurationsdateien konfiguriert werden. Im vorherigen Schritt bei der Konfiguration des *dc*, sehen die die beiden Zeilen:

```
See /usr/local/samba/private/named.conf for an example configuration include file for BIND
and /usr/local/samba/private/named.txt for further documentation required for secure\
    DNS updates
```

In der Datei named.conf finden Sie die Konfiguration der beiden DNS-Zonen und in der Datei named.txt finden Sie Informationen zur Konfiguration des *Bind9*. In den nachfolgenden Schritten sehen Sie die Vorgehensweise für die Konfiguration des *Bind9*:

27.1 Setzen der Umgebungsvariablen

Damit Bind auf die Kerberos .keytab-Datei des Samba-Servers zugreifen kann, müssen zwei Variablen in der Datei /etc/default/bind9 gesetzt werden:

```
KEYTAB_FILE="/usr/local/samba/private/dns.keytab"
KRB5_KTNAME="/usr/local/samba/private/dns.keytab"
export KEYTAB_FILE
export KRB5_KTNAME
```

mit dem Kommando `chown bind:bind /usr/local/samba/private/dns.keytab` sorgen Sie dafür, dass der DNS-Server den Zugriff auf die Dateien erhält.

27.2 Anpassen der Datei /etc/bin/named.conf.options

Zwei Zeilen für die Anpassung an den Kerberos müssen in der Datei named.conf.options hinzugefügt werden:

```
tkey-gssapi-credential "DNS/samba4-1.example.net";
tkey-domain "EXAMPLE.NET";
```

Achten Sie bei den Einträgen auf die Großschreibung. Zusätzlich müssen Sie noch einen `forwarders`-Eintrag für Ihr Netzwerk erstellen, das Anfragen außerhalb Ihres Netzwerkes auch aufgelöst werden können.

27.3 Anpassen der Datei /etc/bind/named.conf.local

In der Datei /usr/local/samba/private/named.conf finden Sie die Einträge sowohl für die forward-Zone als auch für die reverse-Zone. Kopieren Sie die entsprechenden Inhalte in die Datei /etc/bind/named.conf.local oder binden Sie die Datei einfach in die named.conf.local über eine `include`-Anweisung ein. Natürlich können Sie die Zonendateien auch in das Standardverzeichnis des *bind9* kopieren. Dann müssen Sie nur die Pfade der Zonendateien entsprechend anpassen.
In der Datei /usr/local/samba/private/named.conf sehen Sie, dass die reverse-Zone auskommentiert ist und nicht automatisch eine Zonendateien erzeugt wird. Wenn Sie die Reverse-Auflösung in Ihrem Netzwerk einrichten wollen, müssen Sie die entsprechende Zonendatei im Verzeichnis /var/cache/bind erzeugen.

27.4 Einrichten einer reverse-Zone

Im folgenden Listing finden Sie eine Zonendatei für die reverse-Zone

```
$TTL 1800
@ IN SOA samba4-1.example.net. root.samba4-1.example.net. (
2013042500
600
200
604800
1800 )

;Nameserver
IN NS samba4-1.example.net.

;Hosts
150 IN PTR samba4-1.example.net.
```

27.5 Anpassen der Datei /etc/resolv.conf

Jetzt muss noch die Datei /etc/resolv.conf so angepasst werden, dass der Samba-Server auch den gerade eingerichteten Nameserver als erstes abfragt. Da der Nameserver auf dem selben Host wie der samba4-Server läuft. Können Sie in der Datei die IP-Adresse `127.0.0.1` verwenden.
Jetzt können Sie den DNS-Server neu starten. Anschließend sehen Sie mit dem Kommando `netstat -tlpn`, dass der Port 953 zusätzlich zum Port 53 vom DNS-Server bereitgestellt wird.

27.6 Testen des DNS-Servers

Neben der Auflösung für die Hosts, muss der DNS-Server in einem AD auch die *SRV*-Einträge auflösen können. Sie sollten unbedingt testen, ob diese Einträge auch aufgelöst werden. Mit dem Kommando `host` können Sie die *SRV*-Einträge testen. Beispiele sehen Sie im folgenden Listing:

```
root@samba4-1:~/samba4# host -t SRV _ldap._tcp
_ldap._tcp.example.net has SRV record 0 100 389 samba4-1.example.net.

root@samba4-1:~/samba4# host -t SRV _kerberos._tcp
_kerberos._tcp.example.net has SRV record 0 100 88 samba4-1.example.net.
```

Testen Sie auch, ob alle Ports die für den Betrieb des Domaincontrollers benötigt werde bereitgestellt werden. Nutzen Sie das Kommandos `netstat -tlpn` um die Ports des DNS-Server zu testen. Im folgenden Listing sehen Sie diesen Test:

```
root@samba4-1:~/samba4# netstat -tlpn | grep named
tcp        0      0 192.168.123.150:53      0.0.0.0:*       LISTEN      16929/named
tcp        0      0 127.0.0.1:53            0.0.0.0:*       LISTEN      16929/named
tcp        0      0 127.0.0.1:953           0.0.0.0:*       LISTEN      16929/named
tcp6       0      0 :::53                   :::*            LISTEN      16929/named
tcp6       0      0 ::1:953                 :::*            LISTEN      16929/named
```

Damit ist die Konfiguration des Nameservers abgeschlossen.

28 Kerberos-Einstellungen übernehmen

Während der Konfiguration hat Samba4 eine Datei /usr/local/samba/private/krb5.conf erstellt. Die ursprüngliche Konfigurationsdatei /etc/krb5.conf müssen Sie durch die von Samba4 erzeugt ersetzen. Für den Fall, dass Sie die Konfiguration wieder rückgängig machen wollen, sollten Sie die original Datei sichern. Prüfen Sie, ob in der Datei /etc/krb5.conf Der richtige *REALM* eingetragen ist. Der *REALM* ist der Name Ihrer Domäne in Großbuchstaben. Hier in der Unterlage ist es `EXAMPLE.NET`

29 Erster Start von samba4 aus den Quellen

Jetzt ist es so weit, Sie können den samba4-Server das erste mal starten. Dazu geben Sie das Kommando `samba` ein. Jetzt finden Sie mit `ps ax | grep samba` den Samba-Prozess. Sollten Sie den Prozess nicht sehen und auch keine Fehlermeldung erhalten, versuchen Sie das Kommando `samba -i -M single`. Wenn Sie dann die folgende Meldung erhalten:

```
root@samba4-1:~# samba -i -M single
samba version 4.0.5 started.
Copyright Andrew Tridgell and the Samba Team 1992-2012
ERROR: can't open /usr/local/samba/var/run/samba.pid: Error was No such file or directory
```

fehlt bei Ihnen das Verzeichnis /usr/local/samba/var/run/. Wenn Sie das Verzeichnis anlegen, startet dann auch der Samba-Server.
Wenn Sie jetzt den samba4-Server starten, sehen sie die Samba-Prozesse mit `ps ax | grep samba`. Jetzt können Sie den Samba mit dem Programm `smbclient` testen. Hierbei kann es auch wieder zu einem Fehler kommen, der auf ein fehlendes Verzeichnis zurückzuführen ist. Im folgenden Listing sehen Sie die Fehlermeldungen:

```
root@samba4-1:~/samba4# smbclient -L localhost -U%
session setup failed: NT_STATUS_INVALID_SERVER_STATE
```

Wenn diese Meldung erscheint, sollten Sie alle Samba-Prozesse mit `killall samba` beenden und den Dienst wie folgt neu starten:

```
root@samba4-1:~/samba4# samba -i
samba version 4.0.5 started.
Copyright Andrew Tridgell and the Samba Team 1992-2012
samba: using 'standard' process model
mkdir failed on directory /usr/local/samba/var/lib/winbindd_privileged:\
    No such file or directory
task_server_terminate: [Cannot create winbindd privileged pipe directory]
mkdir failed on directory /usr/local/samba/var/lib/ntp_signd: No such file\
    or directory
task_server_terminate: [Cannot create NTP signd pipe directory:\
    /usr/local/samba/var/lib/ntp_signd]
samba_terminate: Cannot create winbindd privileged pipe directory
```

Hier sehen Sie, das der Prozess Dateien im Verzeichnis /usr/local/samba/var/ ablegen will. Dieses Verzeichnis existiert aber bei der Installation aus den Quellen nicht. Legen Sie das Verzeichnis an und starten Sie jetzt den Dienst mit `samba` neu. Anschließend testen Sie den Samba wieder mit dem Kommando `smbclient` wie im folgenden Listing:

```
root@samba4-1:~/samba4# smbclient -L localhost -U%
Domain=[EXAMPLE] OS=[Unix] Server=[Samba 4.0.5]

        Sharename       Type      Comment
        ---------       ----      -------
        netlogon        Disk
        sysvol          Disk
        IPC$            IPC       IPC Service (Samba 4.0.5)
Domain=[EXAMPLE] OS=[Unix] Server=[Samba 4.0.5]

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
```

29.1 Erstellen eines Init-Skripts für den Samba4 aus den Quellen

Wenn Sie den Samba-Server aus den Quellen installiert habe, müssen Sie den samba4-Server immer per Hand starten, da kein Init-Skript für den samba4 in den Paketen enthalten ist. Sie können das Init-Skript aber mit ein paar Schritten aus dem Internet runter laden und anpassen. Im folgenden Listing sehen Sie die einzelnen Schritt:

```
root@samba4-1:~# wget http://anonscm.debian.org/loggerhead/pkg-samba/samba4/\
  unstable/download/head:\
    /1833%40fc4039ab-9d04-0410-8cac-899223bdd6b0:trunk%252Fsamba4:\
    debian%252Fsamba4.init/samba4.init\ -O /etc/init.d/samba4

root@samba4-1:~/init# sed -i 's|/usr/sbin|/usr/local/samba/sbin|g' samba4

root@samba4-1:~/init# sed -i 's|/etc/samba|/usr/local/samba/etc|g' samba4

root@samba4-1:~/init# chmod 755 /etc/init.d/samba4

root@samba4-1:~/init# update-rc.d samba4 defaults
update-rc.d: using dependency based boot sequencing
```

Im ersten Schritt wird das Paket heruntergeladen, anschließend werden mit den nächsten zwei Kommandos die Pfade im Init-Skript an die Umgebung angepasst. Dann müssen Sie die Berechtigungen am Skript noch auf `755` setzen und dann mit `update-rc.d samba4 defaults` Samba aktivieren. Anschließend können Sie den Samba mit dem Kommando:
`service samba4 start|stop|restart` starten oder stoppen.

30 Konfiguration von swat2

Vielleicht kennen und nutzen sie den SWAT schon unter Samba3 für die Konfiguration des Samba3. Mit samba4 ist der alte SWAT nicht mehr vorhanden, es gibt nur noch die neue Version *swat2*, dieser ist aber standardmäßig deaktiviert. Der neue *swat2* basiert jetzt auf *python* und kann sowohl als standalone Server oder zusammen mit Samba gestartet werden. Wobei der Start als `service` von Samba bis jetzt noch nicht funktioniert. Im Moment wird der neue swat nicht weiterentwickelt, es sieht so aus, als würde er in Zukunft komplett verschwinden. Die Verwaltung der Konfiguration ist mit dem *swat2* schon nicht mehr möglich. Mit dem swat2 haben Sie nur noch die Möglichkeit, Benutzer und Gruppen im AD zu verwalten. Trotzdem soll hier der *swat2* installiert werden um zu zeigen, was mit dem Werkzeug möglich ist und was nicht.
Für die Installation müssen als erstes eine Reihe an Python-Paketen nachinstalliert werden. Diese Pakete installieren Sie mit dem Kommando:

```
apt-get install python-pylons python-yaml python-repoze.who-plugins python-repoze.who\
             python-paste python-pam python-authkit libjs-mootools python-setuptools
```

anschließend können Sie mit den folgenden Schritten den *swat2* konfigurieren.

30.1 Herunterladen und patchen von swat2

Mittels *git* können Sie die aktuelle Version von swat2 herunterladen. Nutzen Sie hierzu das Kommando `git clone git://git.samba.org/jelmer/swat.git`.

Für die aktuelle Version des swat2 gibt es ein Patch das Sie auf jeden Fall noch einspielen müssen. Laden Sie das Patch mit dem Kommando:
`wget http://lists.samba.org/pipermail/samba-technical/attachments/20121230/1e4f6ec5/attachment.patch`.
Speichern Sie das Patch im Verzeichnis vom swat. Anschließend wenden Sie das Patch mit dem Kommando `patch -p1 <attachment.patch` an.

30.2 Setzen der Pfade für Python

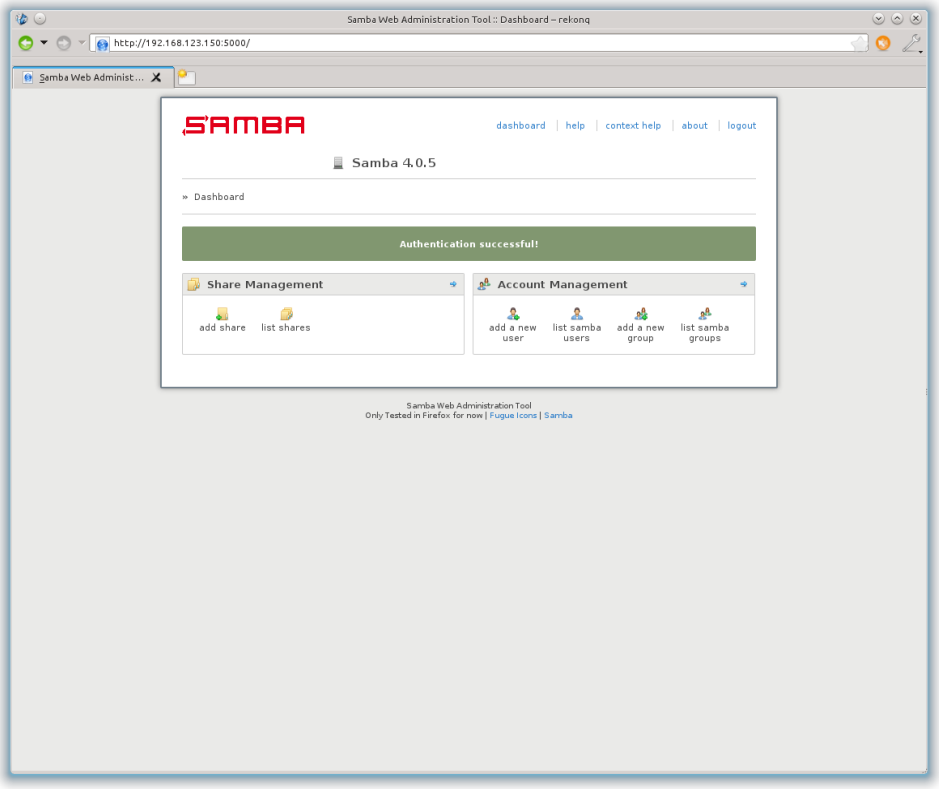
Für Python müssen Sie den Pfad zu dem Python-Libraries anpassen. Dazu geben Sie das Kommando `export PYTHONPATH=/usr/local/samba/lib/python2.7/site-packages` ein. Denken Sie daran, diese Einträge später permanent zu machen.

30.3 Setup des swat2

Vor dem ersten Start, müssen Sie den swat2 noch auf Ihre Umgebung anpassen. Das erreichen Sie durch denn Aufruf von `./setup.py install` im Verzeichnis swat.
In der Datei swat/development.ini müssen Sie die IP-Adresse auf der der swat erreichbar sein soll anpassen. Der Standardwert ist die 127.0.0.1. Auch den Port über den der swat2 erreichbar sein soll, können Sie hier anpassen.

30.4 Starten von swat2

Jetzt können Sie den swat2 mit dem Kommando `paster serve development.ini` starten und über den Browser erreichen. Nach dem Start können Sie sich am swat mit dem Benutzer *administrator* und dessen Passwort anmelden. Nach der Anmeldung erhalten Sie das folgende Bild:



Leider lässt sich der swat2 nicht über den samba4 starten, daher gibt es zwei Möglichkeiten, wie Sie den swat nutzen können:

1. Starten per Hand
   Jedes mal wenn Sie den swat nutzen möchten, starten Sie den Dienst auf dem Server von Hand.

2. Erstellen eines init-Skripts
   Sie können ein Init-Skript für den swat erstellen und den Dienst dann automatisch starten lassen. Im folgenden Listing finden Sie ein Beispiel für ein Init-Skript für den swat:

```
#! /bin/sh
### BEGIN INIT INFO
# Provides:          swat2
# Required-Start:    $network $remote_fs $syslog $samba4
# Required-Stop:     $remote_fs $syslog
# Default-Start:     2 3 4 5
# Default-Stop:      0 1 6
# Short-Description: swat2 web-admin tool
# Description:       This file is use to start and stop
#                    the samba web administration tool 2
#                    for Samba4
### END INIT INFO

# Author: Stefan Kania <stefan@kania-online.de>
#
```

```
# Do NOT "set -e"

# PATH should only include /usr/* if it runs after the mountnfs.sh script
PATH=/sbin:/usr/sbin:/bin:/usr/bin:/usr/local/samba/swat2
export PYTHONPATH=/usr/local/samba/lib/python2.7/site-packages
DESC="swat2 for Samba4"
NAME=swat2
SCRIPTNAME=/etc/init.d/$NAME
PID_FILE=/var/run/$NAME.pid

# Load the VERBOSE setting and other rcS variables
. /lib/init/vars.sh

# Define LSB log_* functions.
# Depend on lsb-base (>= 3.2-14) to ensure that this file is present
# and status_of_proc is working.
. /lib/lsb/init-functions


case "$1" in
  start)
        paster serve /usr/local/samba/swat2/development.ini &
        ps ax | grep /usr/local/samba/swat2/development.ini | head -n 1  |\
        awk '{ print $1 }' > $PID_FILE
        ;;
  stop)
        PID=`cat $PID_FILE`
        kill $PID
        ;;
  *)
        echo "Usage: $SCRIPTNAME {start|stop}" >&2
        exit 3
        ;;
esac
```

Das Skript können Sie dann, wie schon zuvor das Init-Skript für den Samba, mit dem Kommando `update-rc.d swat2 defaults` in Ihr System einbinden.

Damit läuft der swat und Sie können Freigaben und Benutzer mit dem swat verwalten.

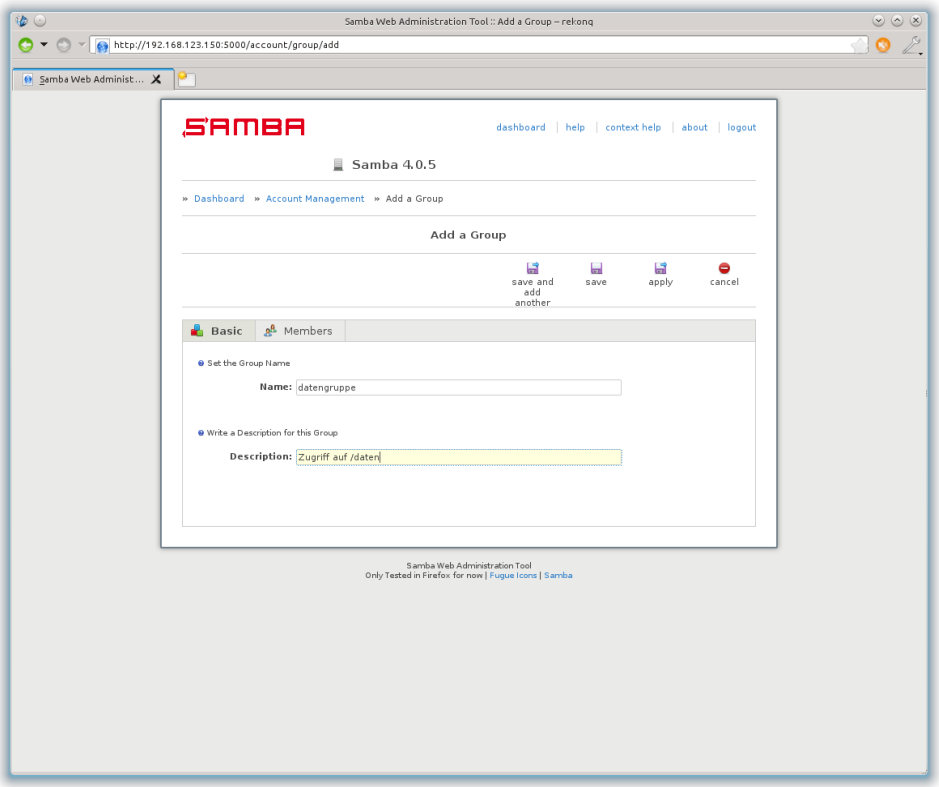
30.5 Benutzer- und Gruppenverwaltung mit dem *swat2*

Wie Sie schon bei der Installation des *swat2* gesehen haben, können Sie mit dem neuen swat jetzt Benutzer und Gruppen verwalten. Im folgenden sehen Sie Screenshots zu den Verschiedenen Themen. Nach der Anmeldung am *swat2* landen Sie auf dem *Dashboard* des swat. Von hieraus können Sie die einzelnen Administrationspunkte auswählen.

30.5.1 Verwaltung von Gruppen mittels *swat2*

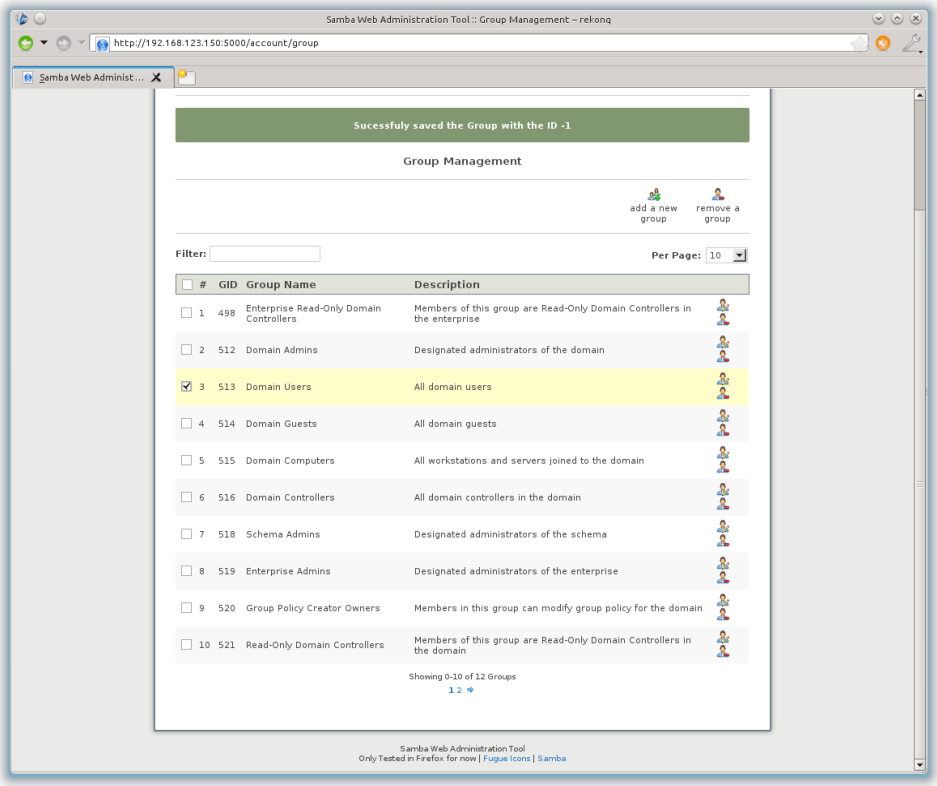
Wie schon am Anfang der Gruppen- und Benutzerverwaltung angesprochen, steht der swat2 für die Verwaltung der Gruppen und Benutzer zur Verfügung. Obwohl es im Moment so aussieht, dass der swat2 nicht weiter gepflegt wird, sollen an dieser Stelle die derzeitigen Möglichkeiten des swat2 angesprochen werden. Den Anfang macht wieder die Verwaltung der Gruppen.

- Gruppen hinzufügen
  Klicken Sie auf die Schaltfläche `textitadd a new group` um eine neue Gruppe zum System hinzuzufügen.



  Leider lassen sich mit dem *swat2* noch keine Mitglieder zu den Gruppen hinzufügen. Das wird hoffentlich, in einer der nächsten Versionen möglich sein.

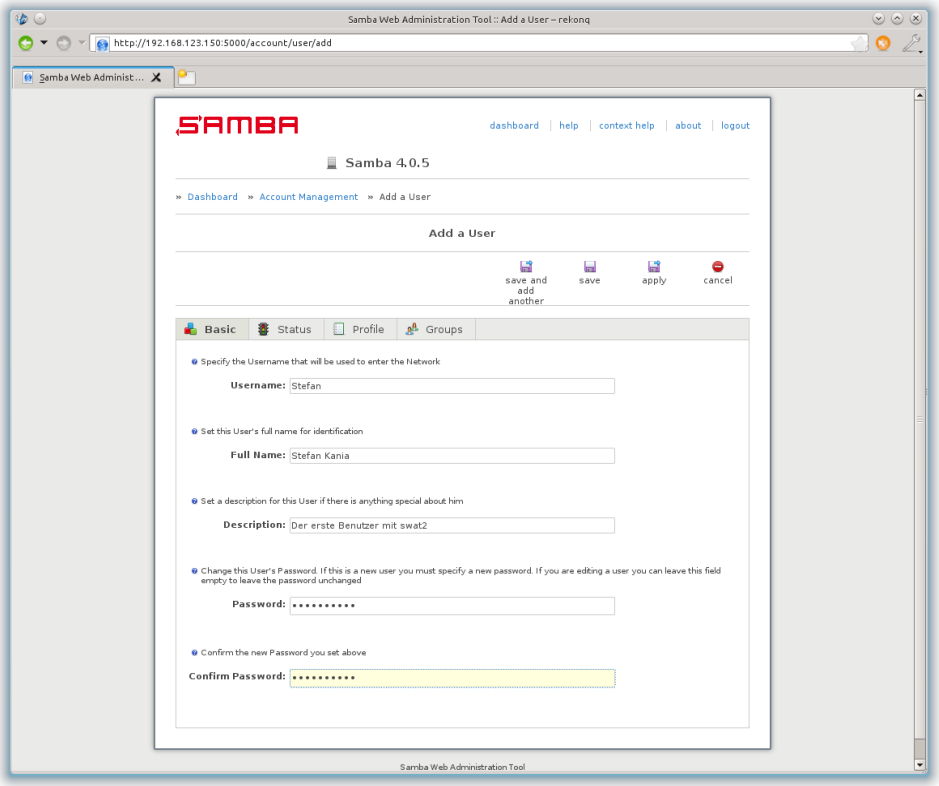
- Auflisten der Gruppen
  durch eine Klick auf *`list samba groups`* im *Dashboard* des *swat2* können Sie sich alle Gruppen auflisten lassen und verwalten. Soweit eine Verwaltung mit dem *swat2* schon möglich ist.



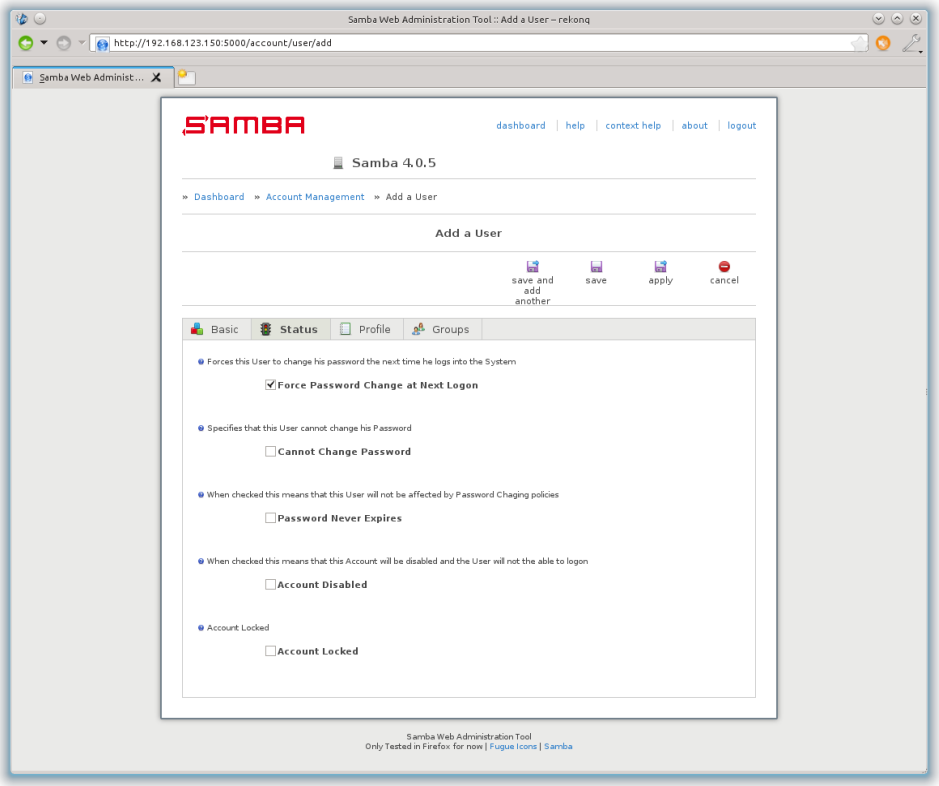
30.5.2 Verwaltung von Benutzern mittels *swat2*

Auch die Verwaltung der Benutzer ist mit dem *swat2* noch sehr eingeschränkt, aber Sie können schon neue Benutzer mit bestimmten Eingenschaften anlegen und verwalten. Auch können Sie die Gruppenzugehörigkeit der Benutzer hier verwalten.

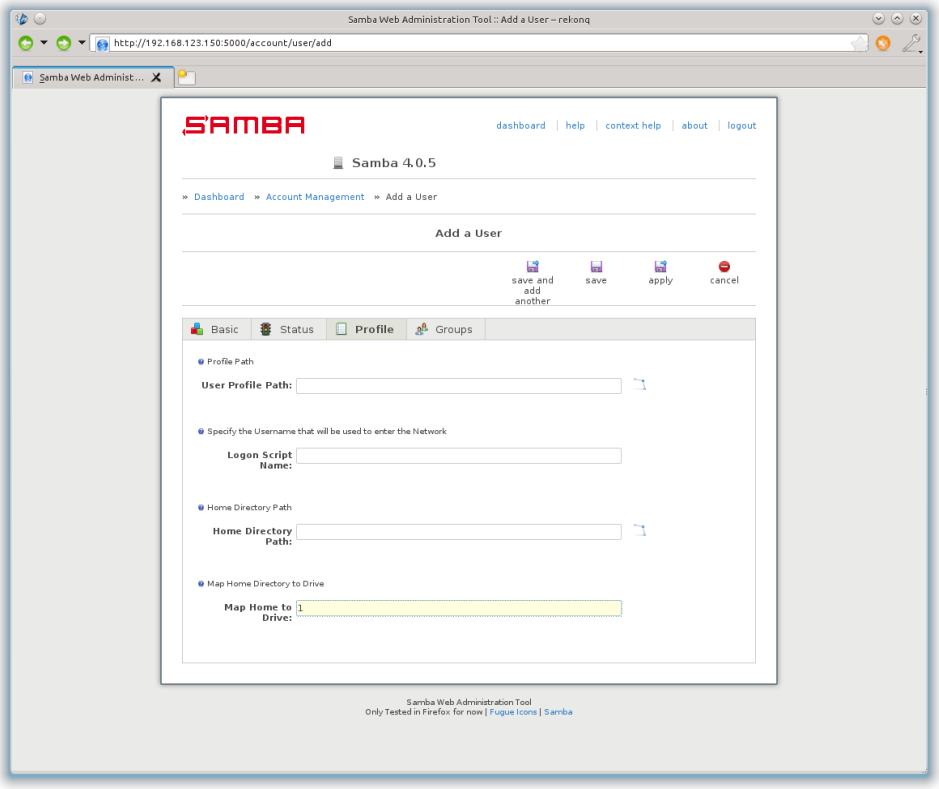
- Den Anfang macht wieder das Anlegen einen neuen Benutzers:



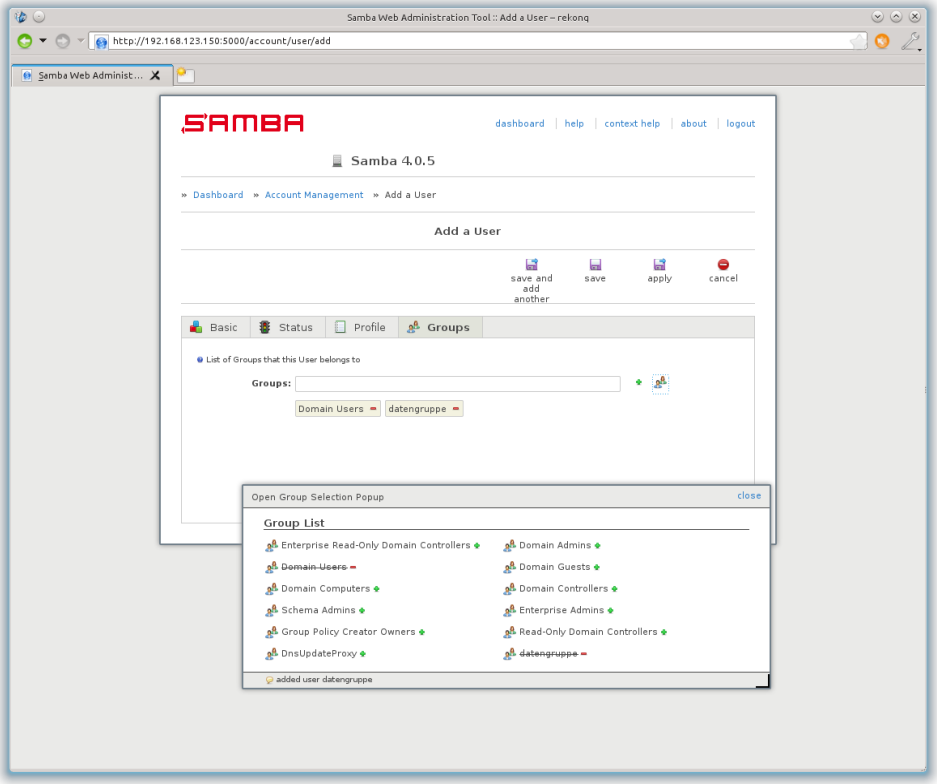
- Auf der Seite *Basic* nehmen Sie die Grundeinstellung für den Benutzer vor. Nach einem Klick auf *Status* können Sie die Kontoeinstellungen des Benutzers ändern. Zum Beispiel können Sie hier einstellen, ob ein Benutzer bei der ersten Anmeldung sein Passwort ändern muss.
  Auf der Seite können Sie auch ein Konto deaktiviere und aktivieren.



- Wenn Sie jetzt auf *`Profile`* klicken, können Sie die Umgebung des Benutzers anpassen. Für die Einträge `User Profile Path` und `Home Directory Path` sehen Sie neben den Feldern ein Symbol eines Verzeichnisbaumes, wenn Sie auf das Symbol klicken, öffnet sich ein weiteres Fenster, in dem Sie eine Verzeichnis auswählen können. Es werden hier aber nur lokale Verzeichnisse angezeigt. Mit der Option `Map Home to Drive:` können Sie festlegen, ob ein Benutzer sein Home-Verzeichnis gleich ein Netzwerklaufwerk zugeordnet bekommen soll wenn er sich am Windows anmeldet. Ein wert von `-1` erzeugt kein Netzwerklaufwerk und ein Wert von `1` erzeugt ein Netzwerklaufwerk

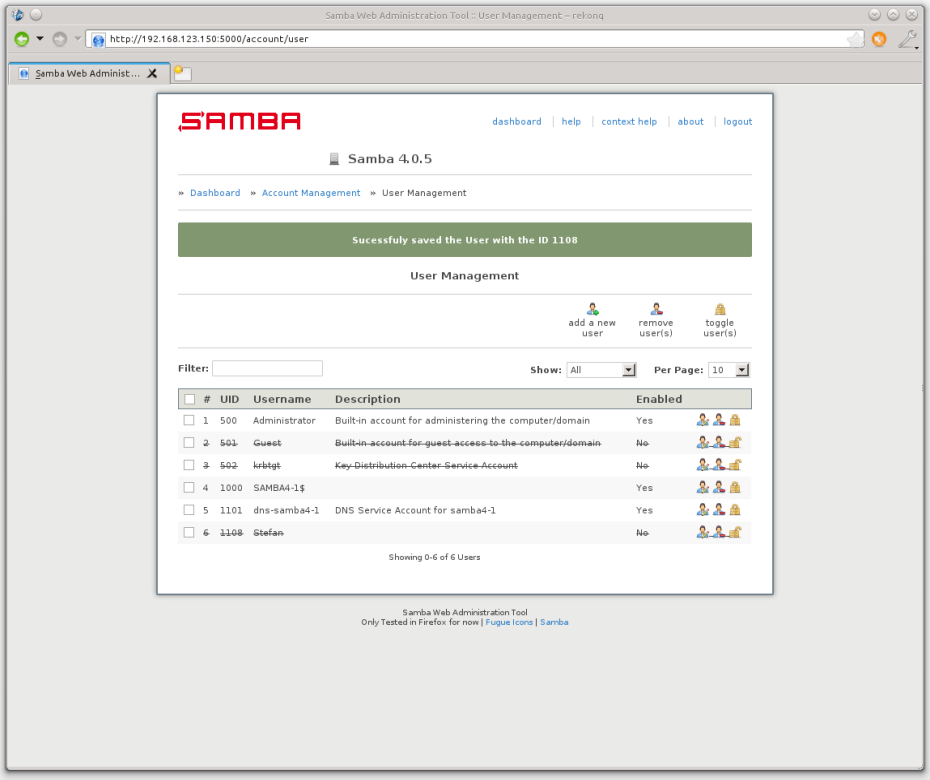


- Wenn Sie jetzt noch auf *Groups* klicken, können Sie dem Benutzer noch Gruppen zuweisen. Klicken Sie auf das Symbol rechts von der Liste und es erscheint ein Fenster aus dem Sie die Gruppen auswählen können.

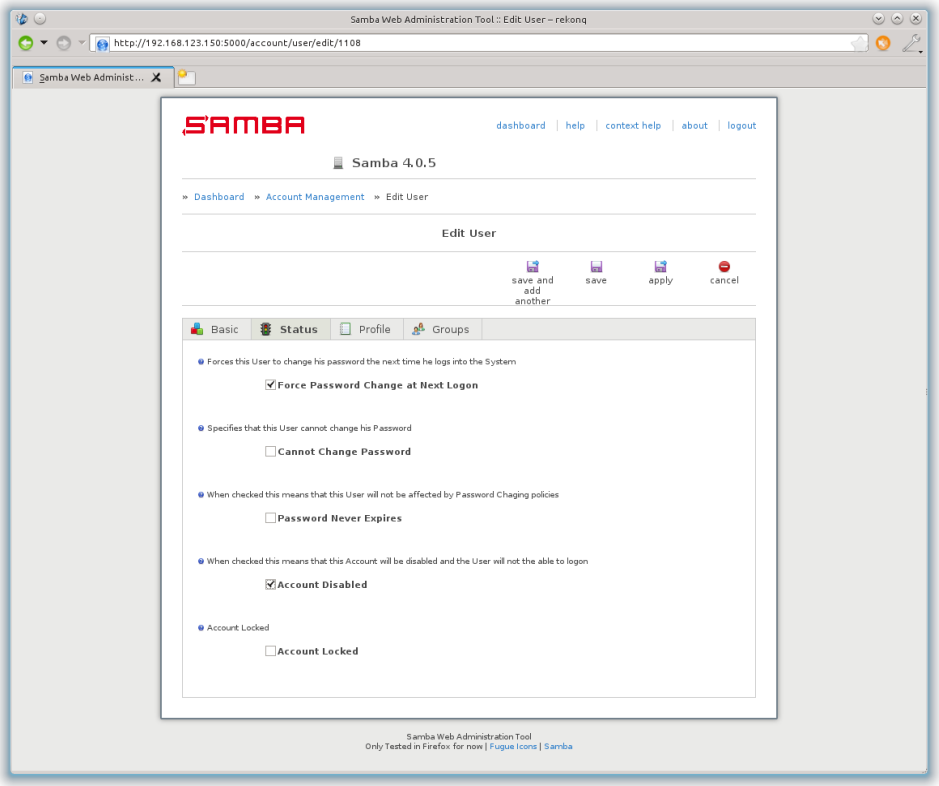


Speichern Sie jetzt den neuen Benutzer über die Schaltfläche *save*.

- Nach dem Speichern kommen Sie zurück auf die Übersichtsseite des swat. Hier sehen Sie, dass der gerade angelegte Benutzer durchgestrichen ist.



Beim Anlegen des Benutzers wird das Konto vom swat erst immer als deaktiviert gespeichert. Sie müssen das Konto erst wieder editiere und unter der Schaltfläche *`Status`* aktivieren.



Speichern Sie die Änderung über die Schaltfläche *save*. Anschließend ist der Benutzer in der Liste nicht mehr durchgestrichen.

Jetzt haben Sie die Möglichkeit die Benutzer für samba4 mittels des SWAT2 zu verwenden.

Index