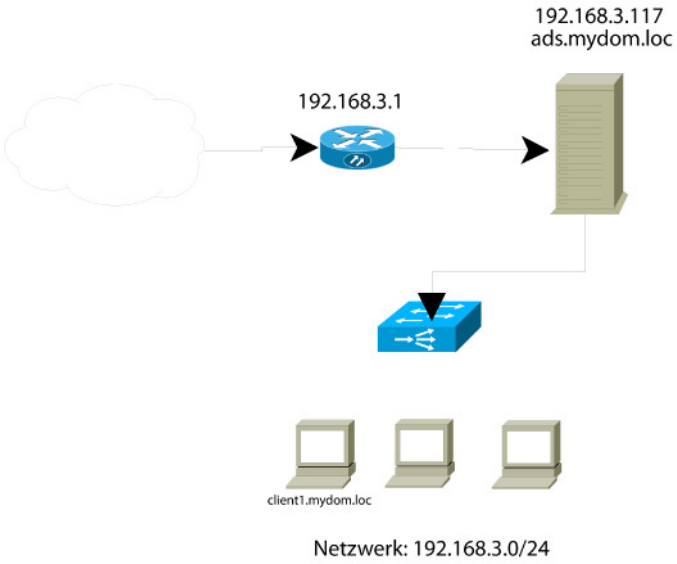
Samba 4

Active Directory Unterstützung mit Samba

Installationsanleitung für Debian ETCH

Michael Mayer
Rudolf-Diesel-Fachschule
2006-2008



Benötigte Abhängigkeiten installieren:
apt-get install attr binutils-doc cpp-doc gcc-4.1-locales make manpages-dev autoconf automake1.9 libtool flex bison gdb gcc-doc gcc-4.1-doc libc6-dev libc-dev libmudflap0-dev rsync bind9 dnsutils

attr = erweiterte Attribute für Dateisysteme **(wichtig!)**

Schritt 1: Download von Samba4

```
cd /root/
rsync -avz samba.org::ftp/unpacked/samba_4_0_test samba4
```

Schritt 2: Kompilieren von Samba4

```
$ cd samba4...test/
$ cd samba4/source
$ # Konfigurieren und Kompilieren
$ ./configure && LD_LIBRARY_PATH=./bin/shared && make proto all
```

Schritt 3: Installieren von Samba4

```
make install
```

Schritt 4: Pfade anpassen

Damit Samba problemlos ausgeführt werden kann, müssen die Pfade für die dynamischen Bibliotheken dem „runtime Linker“ bekannt gemacht werden. Normalerweise werden alle Bibliotheken unter /lib oder /usr/lib installiert. Da wir Samba aber mit *prefix(/usr/local/samba)* installiert haben, findet der Linker die Bibliotheken nicht von selbst.

Fehlermeldung vom provision Skript:
smbscript: error while loading shared libraries: libldb.so.0: cannot open shared object file: No such file or directory

 # Library Path anpassen

```
echo "/usr/local/samba/lib" > /etc/ld.so.conf.d/samba4.conf
```

 # Bibliothekencache neu laden (/etc/ld.so.cache)

```
ldconfig
```

**Der Systempfad muss ebenfalls angepasst werden,
damit ein Aufruf vom smbd aus jedem Pfad heraus möglich ist.**

```
export PATH=$PATH:/usr/local/samba/bin:/usr/local/samba/sbin
```

Achtung!! Sollte noch ein aktueller Samba 3.x installiert sein, kann es zu Verwechslungen kommen (smbd!). Der Pfad sollte auch in der /root/.bashrc und/oder in /etc/profiles angepasst werden, damit er nach einem Reboot des Systems noch vorhanden ist.

Schritt 5: Samba4 konfigurieren

Samba4 beinhaltet ein neues Konfigurationsskript, welches uns eine smb.conf anlegt und die Active Directory Domäne initialisiert.

```
#Legt ein Passwort für den Administrator an.
#Dies ist auch später der Loginname.

./setup/provision --realm mydom.loc --domain=mydom.loc --adminpass=rdf0608 --server-role='domain
controller'
```

Die Ausgabe des Skripts sollte genau verfolgt werden, da es Hinweise auf die nächsten Schritte erteilt.

Ausgabe des Skripts:

set DOMAIN SID: S-1-5-21-2165432318-3390051618-3668605479
Provisioning for MYDOM.LOC in realm MYDOM.LOC
Using administrator password: rdf0608
Setting up /usr/local/samba/etc/smb.conf
Setting up share.ldb
Setting up secrets.ldb
Setting up the registry
Setting up templates into /usr/local/samba/private/templates.ldb
Setting up sam.ldb partitions
Setting up sam.ldb attributes
Setting up sam.ldb rootDSE
Erasing data from partitions
Pre-loading the Samba4 and AD schema
Adding DomainDN: DC=mydom,DC=loc (permitted to fail)
Modifying DomainDN: DC=mydom,DC=loc
Adding configuration container (permitted to fail)
Modifying configuration container
Adding schema container (permitted to fail)
Modifying schema container
Setting up sam.ldb Samba4 schema
Setting up sam.ldb AD schema
Setting up sam.ldb configuration data
Setting up display specifiers
Adding users container (permitted to fail)
Modifying users container
Adding computers container (permitted to fail)
Modifying computers container
Setting up sam.ldb data
Setting up sam.ldb users and groups
Setting up self join
Setting up sam.ldb index
Setting up sam.ldb rootDSE marking as syncronized
Setting up phpLDAPadmin configuration
Please install the phpLDAPadmin configuration located at /usr/local/samba/private/phpldapadmin-config.php into /etc/phpldapadmin/config.php
WARNING: probable memory leak in ldb /usr/local/samba/private/sam.ldb - 5224 blocks (startup 650) 172575 bytes
Setting up DNS zone: mydom.loc
Please install the zone located in /usr/local/samba/private/mydom.loc.zone into your DNS server. A sample BIND configuration snippit is at /usr/local/samba/private/named.conf
To reproduce this provision, run with:
--realm='MYDOM.LOC' --domain='MYDOM.LOC' \
--domain-guid='c189a170-fc66-4f8d-b1bc-dc32b4aac97f' \
--host-guid='7600b35d-6db0-44d3-8b24-680487446f88' \
--policy-guid='1a2cbcb8-6ea6-4c56-b75a-e0ef3dc13bdb' --host-name='ads' --host-ip='192.168.3.177' \
--invocationid='f000cbda-c005-49b1-b0f3-e0a012a635bf' \
--adminpass='rdf0608' --krbtgtpass='7VhXwoE,03uA' \
--machinepass='TOJ#A9aGuuu0' --dnspass='aKf6v4wn7Ll3' \
--root='root' --nobody='nobody' --nogroup='nogroup' \
--wheel='root' --users='users' --server-role='domain controller' \
--aci='# no aci for local ldb' \
All OK

Schritt 6: DNS Konfiguration

DNS ist ein Wichtiger Bestandteil von Active Directory. Hier erfolgt die Anpassung:

Kopieren der von provision erstellten Zonendatei und der named.conf.

```
cp  /usr/local/samba/private/mydom.loc /etc/bind
cat  /usr/local/samba/private/named.conf >> /etc/bind/named.conf.local
```

Anpassen der Konfigurationsdatein

 # /etc/bind/named.conf.local

```
# Diese Zeilen auskommentieren
# tkey-gssapi-credential "DNS/mydom.loc";
# tkey-domain "MYDOM.LOC";

# Diese Zeile suchen und mit dem kompletten Pfad ersetzen:
  file "/etc/bind/mydom.loc.zone";
```

 # /etc/resolv.conf

```
echo "nameserver 127.0.0.1" >> /etc/resolv.conf
```

 # /etc/init.d/bind

```
KRB5_KTNAME=/usr/local/samba/private/dns.keytab
```

Schritt 7: Anpassen des Dateisystems (für ext3 geeinget!)

 # /etc/fstab anpassen

```
# user_xattr hinzufügen für sambadateisystem
/dev/ROOT       /       ext3    defaults,user_xattr,errors=remount-ro 1       1
```

 # Partition remounten

```
# mount -o remount,rw /
```

7.1) Test des Dateisystemes:

Zunächst führen wir einen Test durch, ob die Einrichtung der erweiterten Attribute für unser ext3 Dateisystem funktioniert hat.

```
# cd /tmp
 # touch test.txt
 # setfattr -n user.test -v test test.txt
 # setfattr -n security.test -v test2 test.txt
 # getfattr -d test.txt
 # getfattr -n security.test -d test.txt
```

Ausgabe der oben genannten Befehle:

```
ads:/tmp# getfattr -d test.txt
# file: test.txt
user.test="test"

ads:/tmp# getfattr -n security.test -d test.txt
# file: test.txt
security.test="test2"
```

Troubleshooting:

Falls die Tests fehlschlagen, muss überprüft werden, ober der Kernel xattr unterstützt. Am einfachsten geht dies über /proc/config.gz (falls in den Kernel kompiliert)

```
$ zgrep CONFIG_EXT3_FS /proc/config.gz

CONFIG_EXT3_FS_XATTR=y
CONFIG_EXT3_FS_SECURITY=y
```

Wenn das nichts nützt, der smb.conf folgenden Eintrag hinzufügen um die xattr zu simulieren:

```
  posix:eadb = /usr/local/samba/eadb.tdb
```

Schritt 8: Testen von Samba

In /usr/local/samba/etc/smb.conf für wir einen Eintrag für ein Verzeichnis hinzu:

```
[test]
       path = /tmp/test
       read only = no

mkdir /tmp/test
chmod 777 /tmp/test
```

Dann testen wir, ob Samba funktionsfähig ist.

```
smbclient //localhost/test -Uadministrator%rdf0608
```

Nach allen Tests und Fertigstellung von Samba kann dieser Ordner wieder gelöscht und aus der Konfiguration entfernt werden

Einrichten der Windows Clients:

Schritt 1: Windows Netzwerkeinstellungen

Wir weisen dem Client, falls es keinen DHCP Server im Netzwerk gibt, eine entsprechende IP-Adresse und Subnetmask zu, z.B. 192.168.3.180/24. Dann geben wir als primären DNS-Server unseren neuen ADS an (192.168.3.177).

Da wir den Bind bis jetzt nicht als **Forwarder** konfiguriert haben, richten wir als sekundären DNS-Server den unseres Providers oder unseres Gateways ein (falls dort DNS läuft).

Schritt 2: Konnektivitätstest zwischen Client und Server

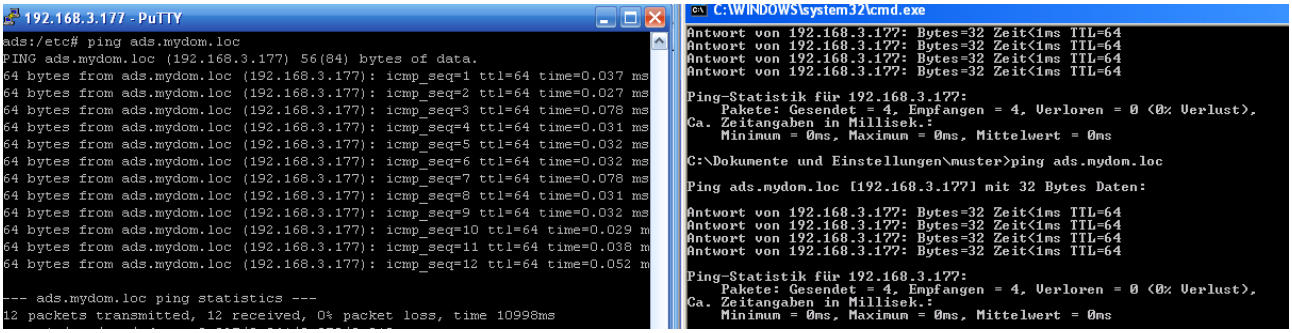
Als Ersten Schritt versuchen wir einen Pingtest vom Server aus an sich selbst.
Über den Namen – nicht über Loopback!

```
ping ads.mydom.loc
```

Wenn wir eine Antwort bekommen, heißt dies, das unser DNS Server funktionsfähig ist und die Domäne aufgelöst werden kann.

Auf dem Client versuchen wir das Gleiche:

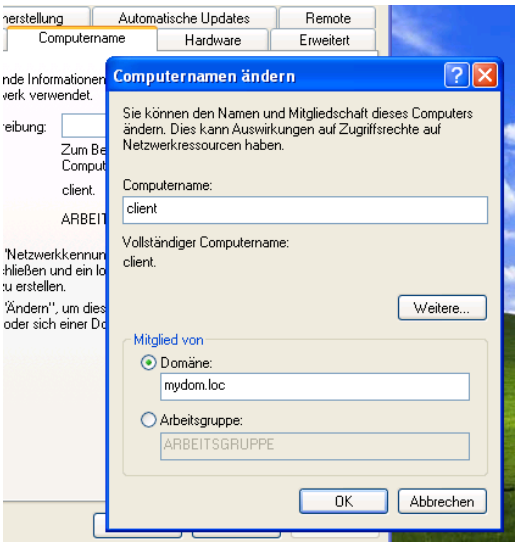
```
ping ads.mydom.loc
```



Gegenüberstellung: Test auf dem Server (links) und Test auf dem Client (rechts)

Rechte Maus auf Arbeitsplatz -> Eigenschaften -> Karteireiter Computername -> Ändern

Hier wählen wir Domäne und Bestätigen.
Wenn wir nach dem Administratorpasswort gefragt werden, geben wir es entsprechend ein.



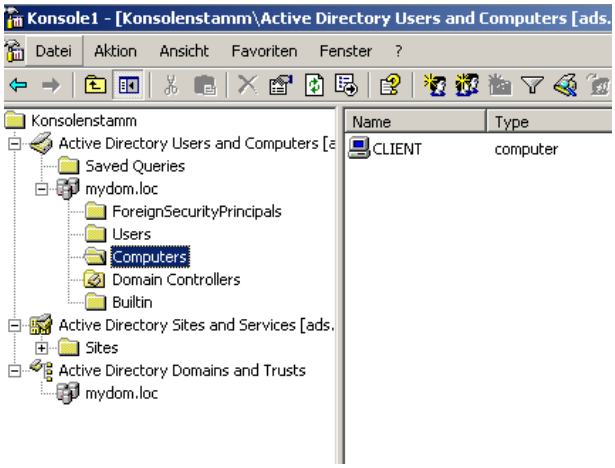
!! Wir sind drin... :-)

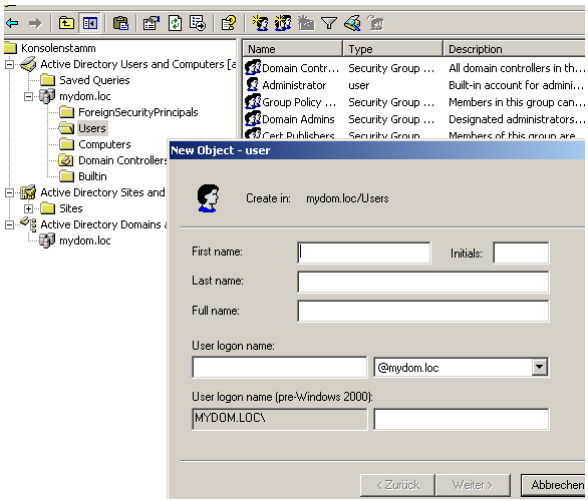
Administration von Active-Directory:

Siehe Skript v. Herrn Hollering 1. und 2. Semester...

Der Linux Server kann über den WindowsXP Client und die zugehörigen Administrationstools, welche WindowsServer2003 standardmäßig bereitstellt Administriert werden.

Für Windows XP benötigt man Addons für die mmc (Ausführen->mmc):
z.B. Active Directory Users and Computers, Sites and Services.....





Adminpack:
http://www.microsoft.com/downloads/details.aspx?FamilyID=c16ae515-c8f4-47ef-a1e4-a8dcbacff8e3&displaylang=en

Support tools:
http://download.microsoft.com/download/3/e/4/3e438f5e-24ef-4637-abd1-981341d349c7/WindowsServer2003-KB892777-SupportTools-x86-ENU.exe

Quellen:
http://wiki.samba.org/index.php/Samba4/HOWTO.