Wie man mit der Endian Firewall Community Edition 2.5 auch ohne die Web-Oberfläche einer Windows Active Directory Domäne beitritt.

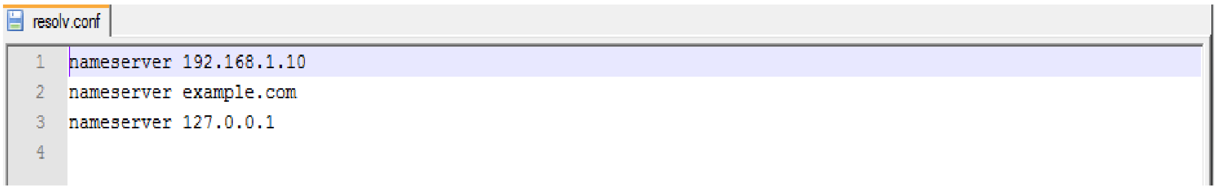
Ich übernehme keine Gewähr und Haftung für entstandene Schäden, und dass das bei jedem funktioniert.

1. Umgebung: -Endian Firewall Community Edition 2.5 auf phys. Server interne IP 192.168.1.3
-Windows AD 2003 Domäne, DC heißt Server1 und hat die IP 192.168.1.10 (IPADRESSE)
-Domäne nenne ich EXAMPLE.COM
-Tools: Putty, WinSCP beide gibt es zum kostenlosen Download
-ACHTUNG: zu ändernde Dateien auf der Firewall stets vorher sichern!

2. Vorgehensweise:

Verbinungstest

Zuerst sollte man testen, ob eine Verbindung zum Server hergestellt werden kann. Dazu öffnet man eine SSH Verbindung mit der Firewall, z. Beispiel mit Putty, und verwendet den Befehl *ping* FQDN (FQDN = Fully Qualified Domain Name z. Beispiel *server1.example.com*). Scheitert man hier schon, hat man ein DNS Problem. Auf dem DNS-Server der Domäne sollte man erst mal die Firewall als statischen Hosteintrag hinzufügen. Dann verbindet man sich per WinSCP oder ähnlichen mit der Firewall (Root Zugangsdaten sollte man haben). Jetzt die Datei **/etc/resolv.conf** sichern. Dann die Datei öffnen, und den DNS der Domäne eintragen. Sieht dann so aus:



```
nameserver 192.168.1.10
nameserver example.com
nameserver 127.0.0.1
```

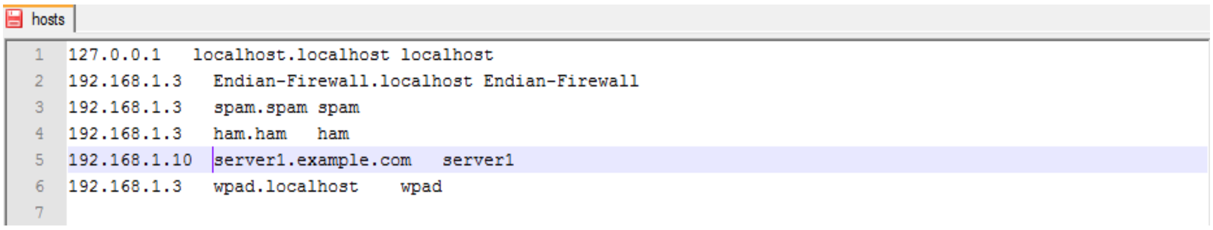
Danach sollte der *ping* FQDN funktionieren.

Zeitabgleich

Anschließend sollte man sicherstellen dass die Zeit auf der Firewall und dem DC gleich ist. Bei Unterschieden von mehr als 2 min können Verbindungsfehler auftreten.

Hosts ändern

Mit WinSCP die Datei **/etc/hosts** öffnen, und folgende Zeilen einfügen:

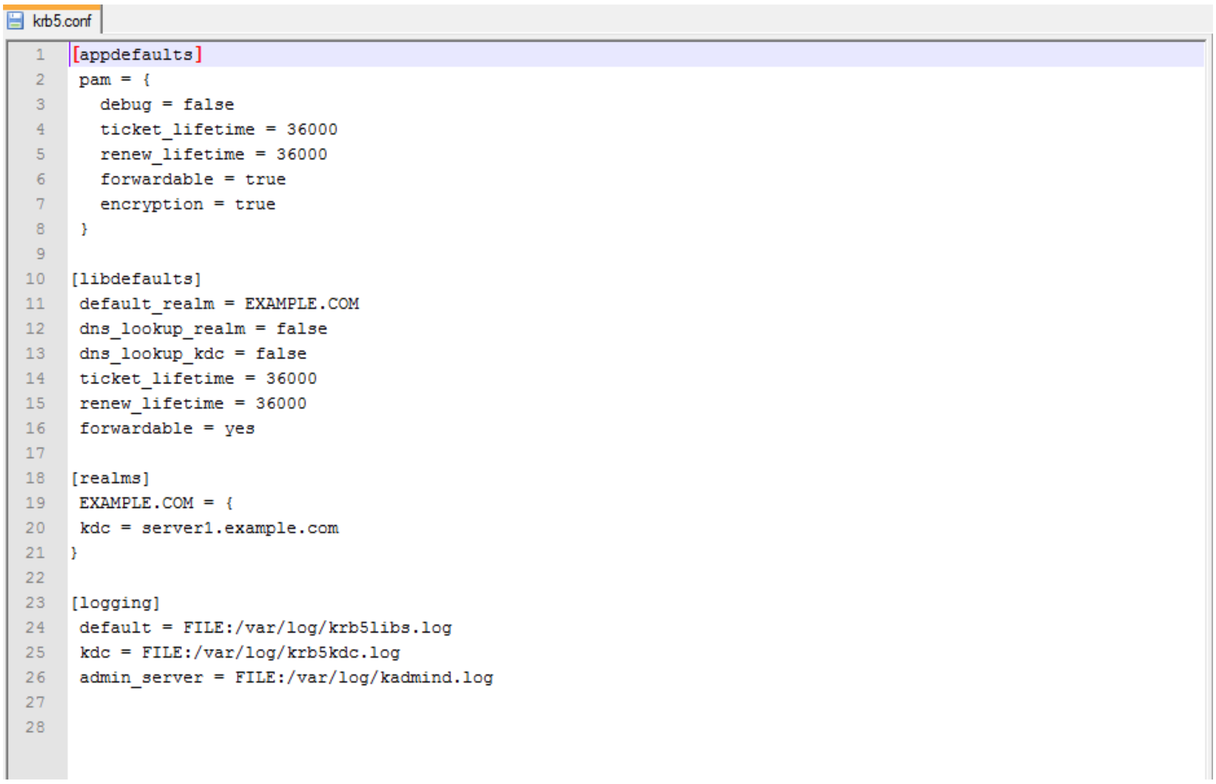


```
127.0.0.1    localhost.localhost localhost
192.168.1.3   Endian-Firewall.localhost Endian-Firewall
192.168.1.3   spam.spam spam
192.168.1.3   ham.ham   ham
192.168.1.10  server1.example.com   server1
192.168.1.3   wpad.localhost    wpad
```

Dies ist wichtig um eine richtige Anmeldung gewährleisten zu können.

Kerberos einrichten

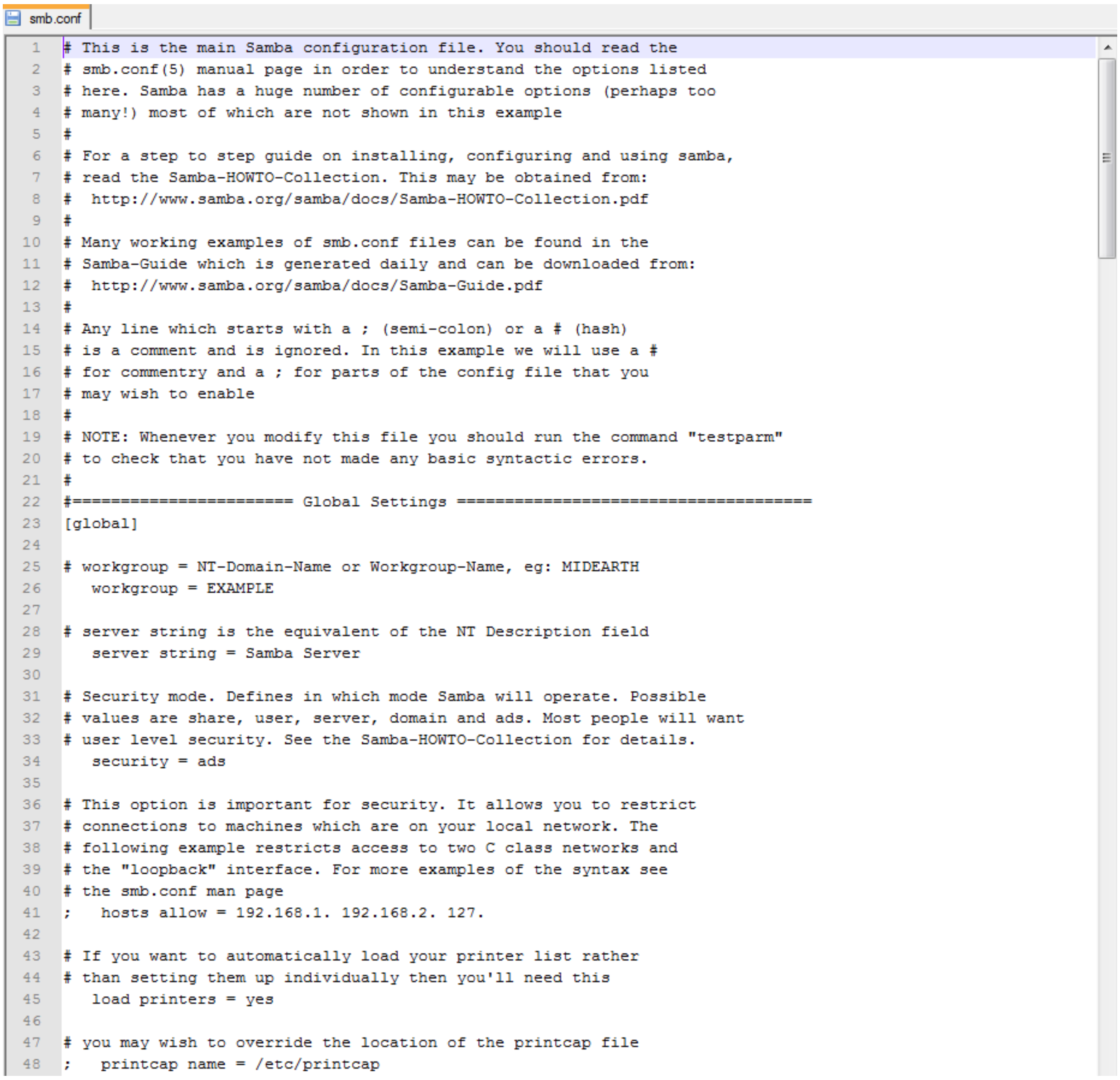
Als erstes den Kerberos Authentifizierungsdienst auf dem Kerberos-Server des Windows-Domänencontroller einstellen. Dazu die Datei **/etc/krb5.conf** öffnen und wie folgt Konfigurieren:



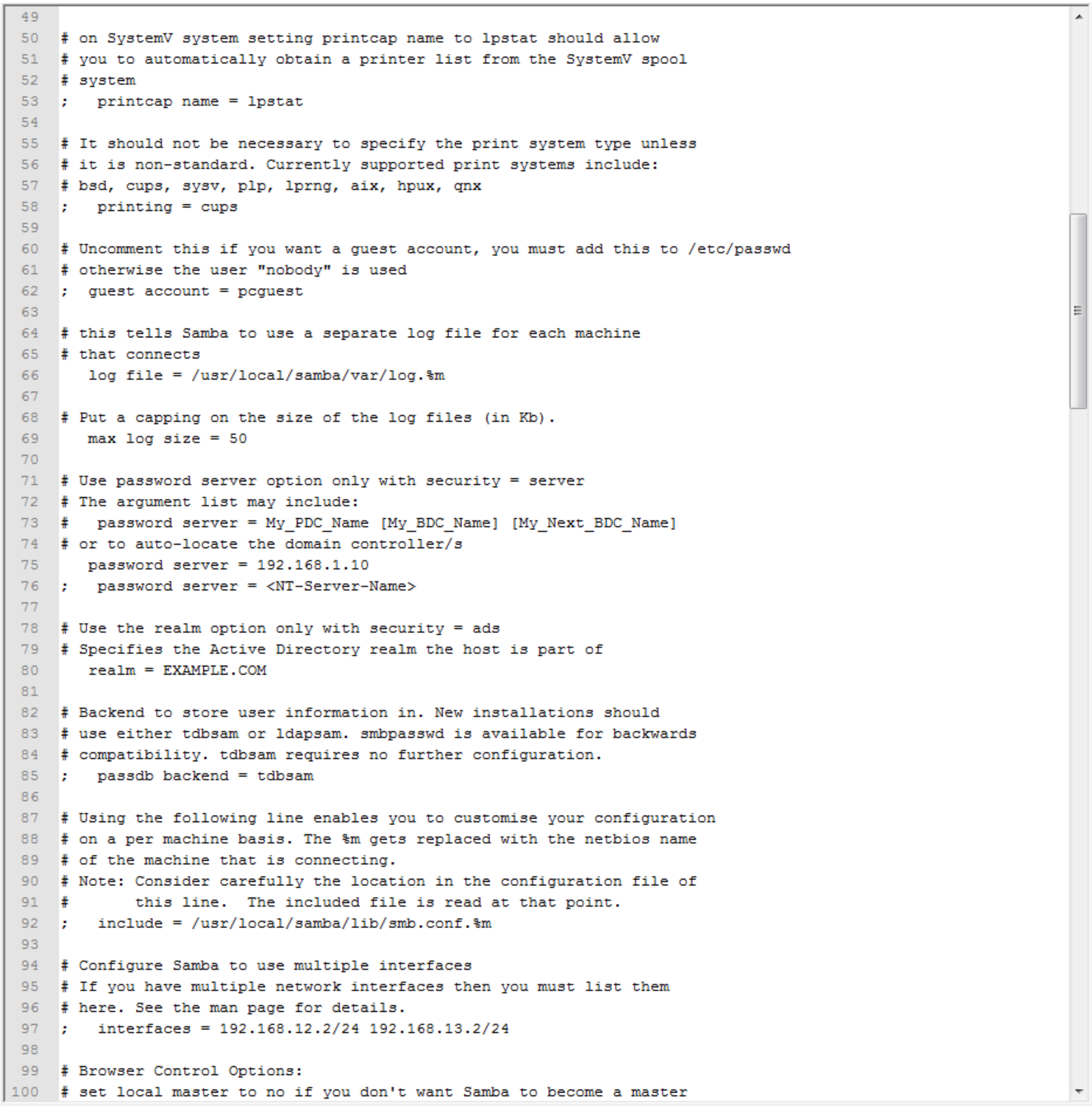
```
[appdefaults]
 pam = {
   debug = false
   ticket_lifetime = 36000
   renew_lifetime = 36000
   forwardable = true
   encryption = true
 }

[libdefaults]
 default_realm = EXAMPLE.COM
 dns_lookup_realm = false
 dns_lookup_kdc = false
 ticket_lifetime = 36000
 renew_lifetime = 36000
 forwardable = yes

[realms]
 EXAMPLE.COM = {
 kdc = server1.example.com
}

[logging]
 default = FILE:/var/log/krb5libs.log
 kdc = FILE:/var/log/krb5kdc.log
 admin_server = FILE:/var/log/kadmind.log
```

Der Domäne beitreten

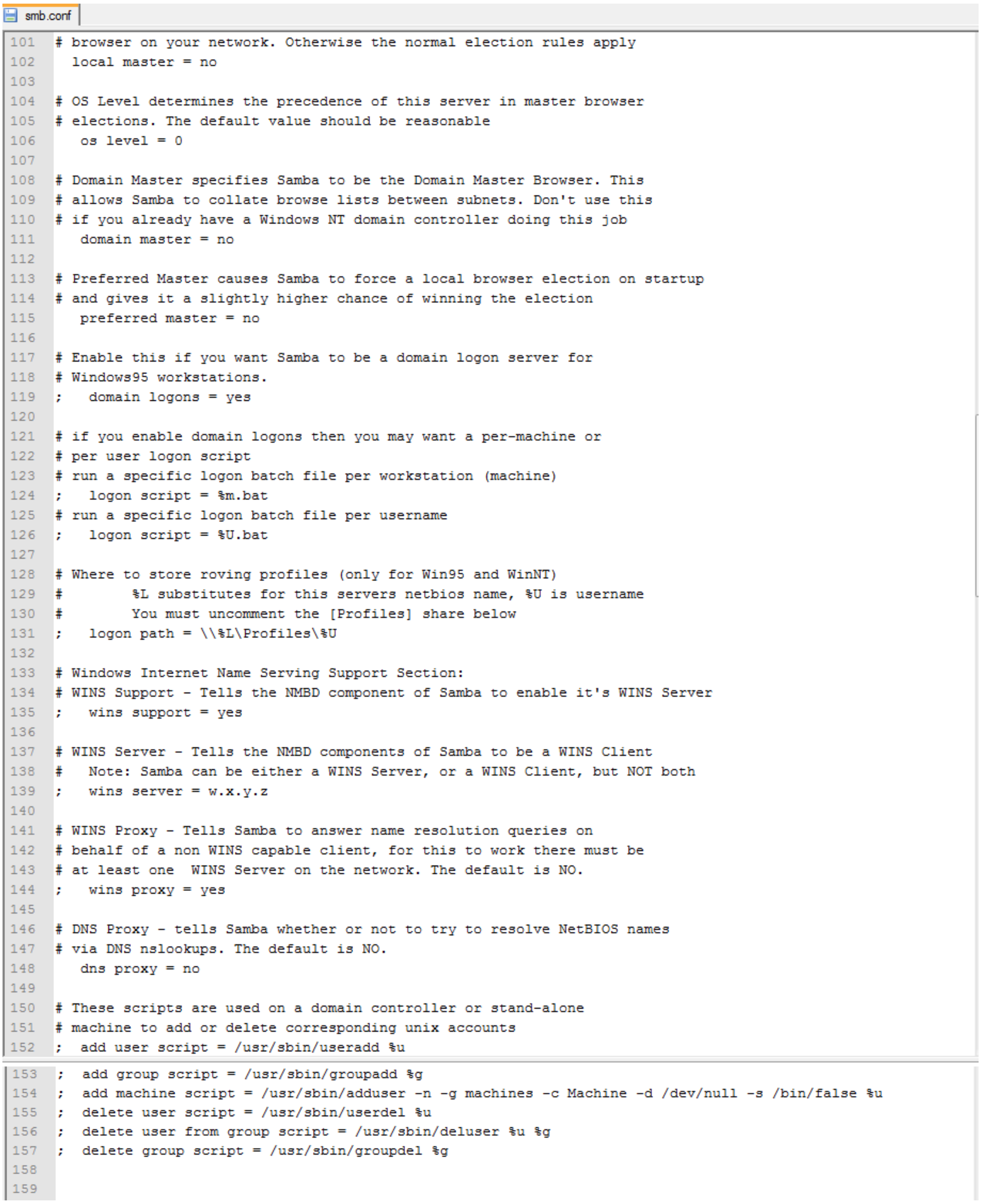
Die Datei **/etc/samba/smb.conf** öffnen und wie nachfolgend Dargestellt anpassen:



```
# This is the main Samba configuration file. You should read the
# smb.conf(5) manual page in order to understand the options listed
# here. Samba has a huge number of configurable options (perhaps too
# many!) most of which are not shown in this example
#
# For a step to step guide on installing, configuring and using samba,
# read the Samba-HOWTO-Collection. This may be obtained from:
#  http://www.samba.org/samba/docs/Samba-HOWTO-Collection.pdf
#
# Many working examples of smb.conf files can be found in the
# Samba-Guide which is generated daily and can be downloaded from:
#  http://www.samba.org/samba/docs/Samba-Guide.pdf
#
# Any line which starts with a ; (semi-colon) or a # (hash)
# is a comment and is ignored. In this example we will use a #
# for commentry and a ; for parts of the config file that you
# may wish to enable
#
# NOTE: Whenever you modify this file you should run the command "testparm"
# to check that you have not made any basic syntactic errors.
#
#======================= Global Settings =====================================
[global]

# workgroup = NT-Domain-Name or Workgroup-Name, eg: MIDEARTH
   workgroup = EXAMPLE

# server string is the equivalent of the NT Description field
   server string = Samba Server

# Security mode. Defines in which mode Samba will operate. Possible
# values are share, user, server, domain and ads. Most people will want
# user level security. See the Samba-HOWTO-Collection for details.
   security = ads

# This option is important for security. It allows you to restrict
# connections to machines which are on your local network. The
# following example restricts access to two C class networks and
# the "loopback" interface. For more examples of the syntax see
# the smb.conf man page
;   hosts allow = 192.168.1. 192.168.2. 127.

# If you want to automatically load your printer list rather
# than setting them up individually then you'll need this
   load printers = yes

# you may wish to override the location of the printcap file
;   printcap name = /etc/printcap
```



```

# on SystemV system setting printcap name to lpstat should allow
# you to automatically obtain a printer list from the SystemV spool
# system
;   printcap name = lpstat

# It should not be necessary to specify the print system type unless
# it is non-standard. Currently supported print systems include:
# bsd, cups, sysv, plp, lprng, aix, hpux, qnx
;   printing = cups

# Uncomment this if you want a guest account, you must add this to /etc/passwd
# otherwise the user "nobody" is used
;  guest account = pcguest

# this tells Samba to use a separate log file for each machine
# that connects
   log file = /usr/local/samba/var/log.%m

# Put a capping on the size of the log files (in Kb).
   max log size = 50

# Use password server option only with security = server
# The argument list may include:
#   password server = My_PDC_Name [My_BDC_Name] [My_Next_BDC_Name]
# or to auto-locate the domain controller/s
   password server = 192.168.1.10
;   password server = <NT-Server-Name>

# Use the realm option only with security = ads
# Specifies the Active Directory realm the host is part of
   realm = EXAMPLE.COM

# Backend to store user information in. New installations should
# use either tdbsam or ldapsam. smbpasswd is available for backwards
# compatibility. tdbsam requires no further configuration.
;   passdb backend = tdbsam

# Using the following line enables you to customise your configuration
# on a per machine basis. The %m gets replaced with the netbios name
# of the machine that is connecting.
# Note: Consider carefully the location in the configuration file of
#       this line.  The included file is read at that point.
;   include = /usr/local/samba/lib/smb.conf.%m

# Configure Samba to use multiple interfaces
# If you have multiple network interfaces then you must list them
# here. See the man page for details.
;   interfaces = 192.168.12.2/24 192.168.13.2/24

# Browser Control Options:
# set local master to no if you don't want Samba to become a master
```



```
# browser on your network. Otherwise the normal election rules apply
  local master = no

# OS Level determines the precedence of this server in master browser
# elections. The default value should be reasonable
   os level = 0

# Domain Master specifies Samba to be the Domain Master Browser. This
# allows Samba to collate browse lists between subnets. Don't use this
# if you already have a Windows NT domain controller doing this job
   domain master = no

# Preferred Master causes Samba to force a local browser election on startup
# and gives it a slightly higher chance of winning the election
   preferred master = no

# Enable this if you want Samba to be a domain logon server for
# Windows95 workstations.
;   domain logons = yes

# if you enable domain logons then you may want a per-machine or
# per user logon script
# run a specific logon batch file per workstation (machine)
;   logon script = %m.bat
# run a specific logon batch file per username
;   logon script = %U.bat

# Where to store roving profiles (only for Win95 and WinNT)
#        %L substitutes for this servers netbios name, %U is username
#        You must uncomment the [Profiles] share below
;   logon path = \\%L\Profiles\%U

# Windows Internet Name Serving Support Section:
# WINS Support - Tells the NMBD component of Samba to enable it's WINS Server
;   wins support = yes

# WINS Server - Tells the NMBD components of Samba to be a WINS Client
#   Note: Samba can be either a WINS Server, or a WINS Client, but NOT both
;   wins server = w.x.y.z

# WINS Proxy - Tells Samba to answer name resolution queries on
# behalf of a non WINS capable client, for this to work there must be
# at least one  WINS Server on the network. The default is NO.
;   wins proxy = yes

# DNS Proxy - tells Samba whether or not to try to resolve NetBIOS names
# via DNS nslookups. The default is NO.
   dns proxy = no

# These scripts are used on a domain controller or stand-alone
# machine to add or delete corresponding unix accounts
;  add user script = /usr/sbin/useradd %u
;  add group script = /usr/sbin/groupadd %g
;  add machine script = /usr/sbin/adduser -n -g machines -c Machine -d /dev/null -s /bin/false %u
;  delete user script = /usr/sbin/userdel %u
;  delete user from group script = /usr/sbin/deluser %u %g
;  delete group script = /usr/sbin/groupdel %g


```

Die Share Definitions lassen wir hier mal außen vor.

Winbind-Dienst neu starten und ADS beitreten

Nach jeder Änderung an der smb.conf Datei, im Konsoleneingabefenster (Putty), den Befehl **/etc/init.d/winbind restart** eingeben. Anschließend **net ads join –U Administrator@EXAMPLE.COM** eingeben, Passwort eingeben und fertig („Administrator“ steht für einen User mit Rechten den Domänenbeitritt auszuführen). Sollte hier ein Fehler alla „malformed …“ auftreten, dann das @EXAMPLE.COM weglassen.

Test

Der Befehl **wbinfo –g** sollte eine Liste der Domaingruppen ausgeben, und **wbinfo –u** der Domainbenutzer. Bekommt man die Fehlermeldung *Error looking up domain groups* dann Winbind nochmal neu starten.

Mit den richtigen Angaben der Server unter dem Punkt Proxy ->Authentifizierung kann man dann bei den Zugriffsrichtlinien seine AD-Benutzer und Gruppen auswählen. Fertig!