

# Samba 4 - Active Directory

```
apt-get update
```

```
aptitude install apache2 libapache2-mod-php5 phpldapadmin dnsutils
```

```
// Account anlegen:
```

```
https://portal.enterprisesamba.com/
```

```
// Sernet List eintragen
```

```
nano /etc/apt/sources.list/sources.list.d/samba4.list
```

```
deb https://Serverman:hzMQrqWEBkvhBNb6pRIOvSqlNucO6TRD@download.sernet.de/packages/samba/4.1/debian wheezy main
```

```
deb-src https://Serverman:hzMQrqWEBkvhBNb6pRIOvSqlNucO6TRD@download.sernet.de/packages/samba/4.1/debian wheezy main
```

```
// Keyring holen.
```

```
wget http://ftp.sernet.de/pub/sernet-samba-keyring_1.4_all.deb
```

```
// Zusätzlichen apt https Transport aktivieren
```

```
apt-get install apt-transport-https
```

```
// Priority anpassen
```

```
nano /etc/apt/preferences.d/samba-sernet.pref
```

```
Package: *
```

```
Pin: origin "download.sernet.de"
```

```
Pin-Priority: 991
```

```
Package: *
```

```
Pin: origin "ftp.de.debian.org"
```

```
Pin-Priority: 100
```

```
// Installation
```

```
apt-get update
```

```
apt-get install sernet-samba sernet-samba-ad sernet-samba-client
```

```
// Konfiguration neuer Domain
```

```
root@ad:~# cd /etc/samba/
```

```
root@ad:/etc/samba# rm smb.conf
```

```
root@ad:/etc/samba# /usr/bin/samba-tool domain provision --use-rfc2307 --interactive
```

```
Realm [SERVERMAN.DE]:
```

```
Domain [SERVERMAN]:
```

```
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) [localhost]: 192.168.0.1
```

```
Administrator password:
```

```
Retype password:
```

```
Looking up IPv4 addresses
```

```
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=serverman,DC=de  
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=serverman,DC=de  
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  
Server Role: active directory domain controller  
Hostname: ad  
NetBIOS Domain: SERVERMAN  
DNS Domain: serverman.de  
DOMAIN SID: S-1-5-21-4171150359-1055942391-1325825047

// Samba bereitstellen

```
mkdir /var/run/samba
```

// nano /etc/default/samba

dc einstellen

// samba starten

```
/etc/init.d/sernet-samba-ad restart
```

// testen

```
root@ad:/etc/samba# smbclient //localhost/netlogon -UAdministrator -c 'ls'
```

Seite 2 / 6

Enter Administrator's password:

Domain=[SERVERMAN] OS=[Unix] Server=[Samba 4.1.13-SerNet-Debian-9.wheezy]

. D 0 Tue Nov 11 14:34:59 2014

.. D 0 Tue Nov 11 14:35:04 2014

63325 blocks of size 262144. 54830 blocks available

// Kerberos testen

root@ad:/etc/samba# kinit administrator@SERVERMAN.DE

Password for administrator@SERVERMAN.DE:

Warning: Your password will expire in 41 days on Tue Dec 23 14:55:47 2014

// Servergespeicherte Profile

mkdir -p /home/profiles

nano /etc/samba/smb.conf

[global]

workgroup = SERVERMAN

realm = SERVERMAN.DE

netbios name = AD

server role = active directory domain controller

dns forwarder = 192.168.0.1

idmap\_ldb:use rfc2307 = yes

logon path = \\%L\profiles\%U

[netlogon]

path = /var/lib/samba/sysvol/serverman.de/scripts

read only = No

[sysvol]

path = /var/lib/samba/sysvol

read only = No

[Profiles]

path = /home/profiles/

read only = no

store dos attributes = Yes

create mask = 0600

directory mask = 0700

profile acls = yes

csc policy = disable

[Demo]

path = /home/demo/

read only = no

// samba reload

smbcontrol all reload-config

```

// nano /etc/network/interfaces

# The primary network interface
auto eth0
iface eth0 inet static
    address 192.168.0.67
    netmask 255.255.255.0
    network 192.168.0.0
    broadcast 192.168.0.255
    gateway 192.168.0.1
    # dns-* options are implemented by the resolvconf package, if installed
    dns-nameservers 192.168.0.67
    dns-search serverman.de

// nano /etc/resolv.conf

domain serverman.de
nameserver 192.168.0.67

// ldap testen

root@ad:/etc/samba# host -t SRV _ldap._tcp.serverman.de
_ldap._tcp.serverman.de has SRV record 0 100 389 ad.serverman.de.

// kerberos testen

root@ad:/etc/samba# host -t SRV _kerberos._udp.serverman.de
_kerberos._udp.serverman.de has SRV record 0 100 88 ad.serverman.de.

// Host Auflösung testen

root@ad:/etc/samba# host -t A ad.serverman.de
ad.serverman.de has address 192.168.0.67

// Kerberos Konfiguration von Samba einbinden

root@ad:/etc/samba# mv /etc/krb5.conf /etc/krb5.conf_orig
root@ad:/etc/samba# ln -sf /var/lib/samba/private/krb5.conf /etc/krb5.conf

// Kerberos testen - wichtig DOMAIN großschreiben:

root@ad:~# kinit administrator@SERVERMAN.DE
Password for administrator@SERVERMAN.DE:
Warning: Your password will expire in 41 days on Tue Dec 23 16:55:49 2014

root@ad:~# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: administrator@SERVERMAN.DE

Valid starting Expires Service principal
11.11.2014 16:58:53 12.11.2014 02:58:53 krbtgt/SERVERMAN.DE@SERVERMAN.DE
renew until 12.11.2014 16:58:48

root@ad:~# smbclient -L ad.serverman.de -U%
Domain=[SERVERMAN] OS=[Unix] Server=[Samba 4.1.13-SerNet-Debian-9.wheezy]

```

```
Sharename Type Comment
```

Seite 4 / 6

```
-----  ----  -----
netlogon   Disk
sysvol     Disk
IPC$       IPC    IPC Service (Samba 4.1.13-SerNet-Debian-9.wheezy)
Domain=[SERVERMAN] OS=[Unix] Server=[Samba 4.1.13-SerNet-Debian-9.wheezy]
```

```
Server      Comment
-----
Workgroup   Master
-----
```

```
root@ad:~# smbclient //localhost/netlogon -U 'administrator'
Enter administrator's password:
Domain=[SERVERMAN] OS=[Unix] Server=[Samba 4.1.13-SerNet-Debian-9.wheezy]
smb: \>
```

```
apt-get install ntp
```

```
mv /etc/ntp.conf /etc/ntp.conf_org
```

```
nano /etc/ntp.conf
```

```
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/lib/samba/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
```

```
// Rechte ändern
```

```
chgrp ntp /var/lib/samba/ntp_signd
```

```
// Windows Client bei Microsoft
http://www.microsoft.com/de-de/download/details.aspx?id=7887
```

```
// Servergespeicherte Profile
```

- RAST installieren
- mit Domain verbinden als Domänen Admin
- Domänen User Profil: \\SERVERMAN\profiles\%USERNAME%

```
danach:
```

- cmd mit Adminrechten aufmachen

gpupdate /force

- admin password reset:

samba-tool user setpassword Administrator

Eindeutige ID: #1150

Verfasser: n/a

Letzte Änderung: 2015-10-26 21:05