Samba - Server

- Kurzakte –

Server:

Installation	
• samba (nach /usr/sbin/smbd und /usr/sbin/nmbd), samba-client, samba-doc	
Besondere Kennzeichen	
• verwendet die Protokolle SMB (Server Message Block) und NBT (NetBIOS over TCP/IP) • smbd lauscht auf den Ports TCP: 139 (netbios-ssn) 445 (microsoft-ds ohne NetBIOS)) • nmbd lauscht auf den Ports TCP: 137 (netbios-ns) UDP: 138 (netbios-dgm)	
Konfiguration	
/etc/samba/smb.conf	• Hauptkonfigurationsdatei • über „include“ können weitere Dateien hinzugefügt werden
/etc/passwd	• Sambabenutzer müssen auch als Linux-User angelegt sein • ein Passwort und eine eigene Shell sind unnötig
/etc/samba/smbpasswd	• enthält Samba-Benutzerkonten und verschlüsselte Win-Passwörter • Anlegen mit Programm `smbpasswd –a username` • nochmals: Benutzer müssen zuvor im System angelegt sein
/etc/lmhosts	• Mapping von NetBIOS-Namen auf IP-Adressen • nur als Notlösung, wenn NetBIOS-Namensauflösung nicht funktoniert • empfohlen ist der Einsatz eines WINS-Servers
/etc/samba/smbusers	• Account-Verwaltung für Samba • hier werden Windows-Benutzer auf bereits bestehende Saba-User gemappt (z. B. Administrator wird root gleichgestellt)
/etc/hosts	• Zuordnung eines Namens zur IP-Adresse für Fernzugriff auf einen Windows-Rechner z.B. als WINS-Server
/etc/fstab	• Eintrag spezieller Samba-Mountparamater (erfolgt durch Samba) `... ext3 acl,user_xattr 1 1` • `acl` aktiviert ACLs im Dateisystem • `user_xattr` zur Unterstützung frei erweiterbarer Dateiattribute (EA) z. B. für Windows-Dateirechte *Vererbung* und *Geschützt* sowie *hidden*, *archive* u. *system* als Ersatz für das x-Recht-Mapping Anzeigen und Ändern der EA mit `setfattr` und `getfattr`
Start als Stand-Alone-Dienst	
/etc/init.d/smb /etc/init.d/nmb rcsmb und rcnmb (S.u.S.E.)	• start | stop | restart | reload | status - Skript startet/stoppt Dämonen smbd und nmbd manuell
insserv smb insserv nmb	• automatischer Start des Samba-Servers • alternativ mit Runleveleditor im Yast
Funktionsprüfung	
testparm	• syntaktische Prüfung der smb.conf • durch Umleitung in eine neue Datei können alle Kommentare entfernt werden
smbclient –L "samba" –U Benutzer	• zeigt alle einem angegebenen Benutzer (-U) zugänglichen Ressourcen des Samba-Servers • sowohl lokal als auch remote ausführbar
smbstatus	• zeigt verbundene Benutzer (-b) und Zugriffe auf Shares an
netstat –a	• für TCP muss netbios-ssn auf LISTEN stehen
nmblookup –d2 *	• welche Rechner antworten auf NetBIOS-Anfragen (mit Debuglevel 2)
smbclient //server/freigabe	• Verbinden mit einer Freigabe auf dem Sambaserver • vom smb> Prompt aus können nun ftp-ähnliche Kommandos wie cd, dir, put oder get abgesetzt werden
smbd –S –F –i –d 5	• Anzeige, mit welchen Optionen Samba kompiliert wurde
tdbdump [datei.tdb]	• Anzeige der Dateien des Samba-internen Datenbankformats im Klartext • *.tdb-Dateien liegen unter /var/lib/samba
Dokumentation	
man: smbd (8), nmbd (8), swat (8), tdbbackup (8), tdbdump (8), smbpasswd (5), smbstatus (1), testprns (1),	

Linux-Client:

Installation	
• Paket samba-client	
Aktionen	
smbmount	• abgespeckte Version von smbclient zum Mounten von Windows-Freigaben: `smbmount //<WindowsServer>/Freigabename /Mountpoint -o username=paul,password=geheim,ip=192.168.1.1` Achtung: über history der bash kann das Passwort nachgelesen werden! • auch möglich: `mount –t smbfs ...`

/etc/fstab	• automatisches Mounten einer SMB-Freigabe
	`/windowsswerver/freigabename /mnt/samba smbfs noauto,user,gid=users,credentials=/etc/samba/benutzerdaten 0 0`
	• in der nur für root lesbaren Datei stehen Login-Daten in folgender Form:
	`username=paul`
	`password=geheim`

smbclient	• macht Windows-Ressourcen im Netz sichtbar:
	`smbclient –L windowsserver`
	• verbindet Linux-Clients mit Windows-Freigaben:
	`smbclient //windowsserver/freigabe -U paul%geheim`
	• Verschicken von Popup-Nachrichten:
	`echo hallo | smbclient –M winrechner`
	• Drucken :
	`smbclient -U paul%geheim print Datei`
	• Anlegen, Öffnen, Bearbeiten, Speichern und Löschen von Dateien und Verzeichnissen
	• interaktive Backups von Freigaben

net	• Zusammenfassung vieler Funktionen in einem Befehl (Nachfolger von smbclient) • Beispielsabfrage nach dem Masterbrowser der Domäne TESTDOM net -S windowsserver -U paul%geheim lookup master testdom
smbtree (!!!)	• zeigt in Baumstruktur alle Domänen/Arbeitsgruppen mit den Servern und Freigaben `smb -b` Suche nach allen Domain-Masterbrowsern `smb –D` zeigt nur die Arbeitsgruppen- und Domänennamen an `smb –S` Anzeige aller Server ohne die Freigaben
rpcclient	• Zugriff auf Microsoft-RPCs • interaktiv oder online mit Option `–c Befehlsstring` • Beispielsabfrage nach der Domain-SID: `rpcclient windowsserver -U paul%geheim -c lsaquery`
smbtar	• Shellskript zum Erzeugen eines Backups einer SMB-Freigabe mit dem Namen tar.out `smbtar –s Server –x Freigabe –u Benutzer –p Passwort`
nmblookup	• Auflösung eines NetBIOS-Namens in eine IP-Adresse
Dokumentation	
man: editreg (1), findsmb (1), nmblookup (1), nmbstatus (1), profiles (1), rpcclient (1), smbcacls (1), smbclient (1), smbcontrol (1), smbcquotas (1), smbget (1), smbsh (1), smbtar (1), smbtree (1), testparm (1), lmhosts (5), smb.conf (5), smbgetrc (5), mount.cifs (8), net (8), pdbedit (8), smbmnt (8), smbmount (8), smbpasswd (8), smbspool (8), smbumount (8),	

Windows-Client:

Installation und Voraussetzungen	
• Installation und Einrichtung von TCP/IP und Aktivierung von NetBIOS über TCP/IP • Installation des Clients für Microsoft-Netzwerke	
Aktionen	
Explorer	• Zugriff auf eine SMB-Freigabe über Netzwerkumgebung oder • Eingabe in Adressleiste: username:passwort//Server/Freigabe
net	• eierlegende Wollmilchsau des Microsoft-Netzwerks • Bsp.: Erstellen eines Netzlaufwerks zu einer SMB-Freigabe `net use Laufwerksbuchstabe: //Server/Freigabename`
nbtstat	• Namens- (Option –a) pzw. IP-Adress-Auflösung (Option –A) • entspricht dem Kommando nmblookup von Samba
netsh	• Kommandozeileneditor für die Netzwerkkonfiguration von Win2000/XP • Anzeige der kompletten Konfiguration: `netsh dump all`

SWAT: (Samba Web Administration Tool)

- Kurzakte –

Server:

Installation	
• Bestandteil des Samba-Pakets (nach /usr/sbin/swat) • Start über inetd oder xinetd	
Konfiguration Normalzugang bei inetd (veraltet) oder xinetd	
/etc/services	• Kommentarzeichen entfernen vor Zeile: • swat 901/tcp
/etc/inetd.conf	• bei der Nutzung von inetd • Kommentarzeichen entfernen vor Zeile: • swat stream tcp nowait.400 root /usr/sbin/swat swat
/etc/xinetd.conf	• Hauptkonfigurationsdatei von xinetd • bei Vorhandensein der Zeile "includedir /etc/xinetd.d" liest xinetd alle zusätzlichen Dateien dieses Verzeichnisses

/etc/xinetd.d/swat	• Vorhandensein der Datei swat im Verzeichnis /etc/xinetd.d
	`{`
	`port = 901`
	`socket_type = stream`
	`wait = no`
	`#only_from = localhost`
	`user = root`
	`server = /usr/sbin/swat`
	`log_on_failure += USERID`
	`disable = no`
	`}`
	• Aktivierung durch Anpassen der Zeile "disable ="
	• soll SWAT von einem entferntem Rechner aus genutzt werden, muss die Zeile "only_from" angepasst werden

Start durch xinetd	
/etc/init.d/xinetd rcxinetd (S.u.S.E.)	• start | stop | restart | reload | status - Skript startet/stoppt xinetd manuell • auch mit >kill –HUP `cat /var/run/xinetd.pid`
insserv xinetd	• startet xinetd automatisch beim Systemstart • alternativ mit Runleveleditor im Yast
Wichtiger Hinweis!!!	
• bei Änderungen mit Hilfe von SWAT wird die smb.conf komplett neu geschrieben • dabei werden auch alle Kommentarzeilen entfernt • alle Zeilen, die der Default-Einstellung entsprechen, werden gelöscht • Parameter include und copy werden einfach entfernt!!! • Parameterwerte in Anführungszeichen werden ab dem ersten " gelöscht	
Dokumentation	
man: swat (8)	

Client:

Aufruf von SWAT
• über die Adressleiste eines Web-Browsers: - http://<SambaServer-Name oder IP-Adresse>:901 bei Fernzugriff - http://localhost:901 bei lokalem Zugriff
verschlüsselte Remote-Verbindung aufbauen
• die gesamte Datenübertragung zwischen Browser und Samba-Server erfolgt unverschlüsselt • Tunneln über SSH: - Linux-Workstation: `ssh –L 9999:SambaSerer:901 SambaServer` - Windows-PC: `plink –ssh SambaServer –L 9999:SambaSerer:901` • Verwendung von Webmin als Verwaltungstool, - es bringt SSL von Hause aus mit - es entfernt auch keine Kommentarzeilen der smb.conf

Authentifizierungsmöglichkeiten bei Samba

Authentifizierung auf Freigabeebene

Zugriff für alle gestatten

```
[global]
    security = share
[share]
    guest ok = yes
```

Zugriff nur für diese Benutzer gestatten

```
[global]
    security = share
[share]
    guest ok = no
    only user = yes
    username = user1, user2
```

Authentifizierung auf Benutzerebene

Zugriff nur für eingerichtete Benutzer

```
[global]
    security = user
[share]
    guest ok = no
```

Alle unbekannten Benutzer werden zum Gast

```
[global]
    security = user
[share]
    guest ok = no
    map to guest = yes
```

Authentifizierung über einen eingerichteten Windowsrechner oder -server

Windowsserver (NT4) darf Benutzer mit falschem Passwort nicht zum Gast machen

```
[global]
    security = server
    password server = rechner1, rechner2
    encrypt passwords = yes
    paranoid server security = yes
    add user script = /usr/sbin/useradd –m –s /bin/false –d /home/sambauser/%u %u
```

Authentifizierung über das NT4-Domain-Sicherheitsprotokoll an einem PDC/BDC

Benutzer des PDC werden von Samba bei der Anmeldung übernommen (Samba ist Member-Server)

```
[global]
    security = domain
    workgroup = NT4Domainname
    password server = NT_PDC, NT_BDC1, NT_BDC2
    encrypt passwords = yes
    allow trusted domains = no                    (vermeidet doppelte Benutzer)
    add user script = /usr/sbin/useradd –m –s /bin/false –d /home/sambauser/%u %u
    delete user script = userdel –r % u
    machine password timeout = 604800   (Maschinenpasswörter wöchentlich geändert) [share]
    profile acls = yes                            (ab Win2000 SP3)
```

Beitritt von Samba in die Windows-Domäne

```
net join –l –u Administrator
```

Authentifizierung als Mitglied einer ADS-Domäne an einem Win200x-Server

```
[global]
    security = ads
    workgroup = win200X          (vorderer Teil des DNS-Domainnamens)
    password server = *
    realm = win200X.top          (kompletter DNS-Domainname von ADS für Kerberos)
[share]
    guest ok = no
```

Anpassen der /etc/resolv.conf (oder zumindest Eintrag des ADS-Servers in /etc/hosts für Kerberos)

```
    search win200X.top
    nameserver <IP-des-ADS-Servers>
```

für Kerberostickets lokale Uhrzeit mit dem ADS-Server synchronisieren

```
    ntpdate <IP-des-ADS-Servers>
```

Anpassen der Kerberos-Konfigdatei /etc/krb5.conffür Heimdal (SuSE) oder MIT-Kerberos (Red Hat)

```
[libdefaults]
    default_realm = win200X.top
[realms]
    win200X.top = {
        kdc = <IP-des-ADS-Servers>
        }
```

Beitritt von Samba in die ADS-Domäne

```
net ads join –l –u Administrator
```

Samba als PDC einrichten

- Samba ist nicht nur Ressourcenlieferant, sondern dient auch als zentraler Anmeldeserver
- weitere Samba- oder Windows-Server werden als Member-Server in die Domäne integriert

1. smb.conf editieren

```
# Date: 2003/07/04 09:52:31
#Samba 2.2.7 als PDC
#
[global]
      workgroup = SAMBADOMAIN    (Domain-Name)
      netbios name = SAMBAPDC    (Name des Servers in der Netzwerkumgebung)
      interfaces = 192.168.38.157/255.255.255.0    (nur für diese Netzkarte, falls Router)
      encrypt passwords = Yes    (verschlüsselte Passwortübertragung)
      time server = Yes          (Samba soll als Zeit-Server fungieren)
      deadtime = 30              (Verbindung wird nach 30 min Inaktivität getrennt)
      domain logons = Yes        (Samba wird Domain-Controller)
      domain master = Yes        (PDC muss gleichzeitig DMB sein)
      os level = 65   # Samba wird Local Masterbrowser (Win2000-Server hat Wert 32)
   ?  add machine script = /usr/sbin/useradd  –s  /bin/false  %u
      logon drive = h:           (Laufwerksbuchstabe zum Heimatverzeichnis)
      logon script = logon.cmd   (liegt in der Freigabe [netlogon] )
      logon path =  \\%L\profiles\%U   (Ordner für das serverbasierte Benutzerprofil)
      valid users = @leitung, @entwicklung, @verwaltung
      hosts allow = 192.168.38.  # Zugriff nur von dieser Net-ID gestattet
          ...
 [netlogon]
      path = /home/samba/netlogon   # hier liegt das Skript logon.cmd
[profiles]
      path = /home/samba/profiles
      read only = No
      store dos attributes = Yes
      create mask = 0600
      directory mask = 0700
      profile acls = Yes
```

2. Windows-Rechner bei Samba registrieren

Für jeden Windows-Client-PC muss auf dem Samba-Server ein Maschinenkonto existieren.
Dazu richtet man einen System-Linux-Account ein:

```
# useradd –r netbiosname$
```

und erstellt eine Passwortzuordnung (pwd=NetBIOS-Name) in der /etc/samba/smbpasswd:

```
# smbpasswd -a -m netbiosname
```

3. Domainbeitritt am Windows-Rechner

Unter Systemsteuerung --> Netzwerk --> Netzwerkidentifikation muss der Rechner zum Mitglied der eingerichteten Samba-Domäne werden.
Geben Sie nach Aufforderung das Konto und Kennworqt von root des Samba-Servers ein.
Achtung: für den Beitritt muss root ein Konto in der smbpasswd auf dem Samba-Server haben!!!
Win2000: Häkchen bei "Primäres DNS-Suffix bei Domänenänderung ändern" entfernen. (nur bei ADS)

4. Beispiel für logon.script in /data/netlogon/logon.cmd

```
@echo off^M
net use h: \\SAMBAPDC\homes
net time \\SAMBAPDC //set /yes
```

5. Systemrichtlinien unter dem jeweiligen Windows mit poledit.exe erzeugen (*.pol–Datei)

die damit erzeugte Datei NTconfig.pol direkt unter [netlogon] ablegen
(Hinweise unter http://www.heise.de/ct/tipps/adms.shtml)