Make a Linux server Active Directory member

The task

An old "real" server **Fujitsu Siemens RX300S3** with one LSI MegaRaid extender with Windows server 2003 was on duty for years mainly as file server for some 2000 users in an AD domain. Windows 2003 would not do it any longer: no working updates, problems to communicate with the (three) domain controllers over several networks after their having been migrated to Windows server 2008 R2.

The concrete task was to make this Windows file server in an AD domain an Ubuntu one. Its name used here for brevity is PD330S respectively PD330s.FB3-MEVA.fh-bochum.de.

Window's failure

Installing Windows server 2008 R2 as full replace of W2003 on PD330S went like charm, keeping its domain membership intact, updating its computer entry with the new OS, keeping all LANs working and configured correctly etc. ... – except for not recognising the LSI MegaRaid extender. No driver found, no remedy.

Enter Ubuntu server 16.04. We knew from other installations it would "raid" without problems. OK it did recognise and use LSI MegaRaid extender(s) automatically, it is stupid with LANs, but this can be handled (as we did on some machines).

Ubuntu's failure

Well after years of Samba advertising – "Linux with Samba can take over the AD DC role" – one would expect making an Ubuntu server an AD domain member computer would be the first simple hopefully automatic step in getting an Ubuntu computer doing work in a domain. It is not.

We followed half a dozen mostly well documented recipes, the common denominator of which is best described by

```
sudo apt install krb5-user samba sssd ntp
```

after having made multiple preparations in /etc/resolv.conf, /etc/hosts, /etc/network/interfaces and partly more of those.

To make it short, none of these approaches worked. And neither did the googled remedies some of them being just unexplained voodoo. Some repairs even insinuated introducing new AD groups for sorting user accounts in. No, we won't! The AD domain in questions has some 300 computer and some 6000 user accounts. We will not touch their structure just for the purpose of adding/replacing a member computer.

We like to keep old servers running for resiliency, and we have some over 15 years old still doing quite well. And we like to introduce Linux/Ubuntu for a bundle of reasons. But here, after days of senseless "samba dancing", we were at a point of putting new hardware and W2008 or W2012 in.
To cite [13]:
"Even armed with that [deep samba] knowledge, this wouldn't always work. Even after hours of editing your /etc/samba/smb.conf file, you found yourself stumped until you simply gave up."
This was written 2010 – no real progress since.

An alternate approach with Ubuntu

[13] describes (2010) an alternative approach called "likewise open". That's gone in between. The company BeyondTrust (www.beyondtrust.com) has taken over the work and offers it as open source version of "PowerBroker Identity Services" (PBIS).
You must fill out a little form to get the download link.

To give them a fair start, we (again) got rid of previous futile trials and made a fresh install with Ubuntu distribution on a DVD burned from downloaded

ubuntu-16.04.1-server-amd64.iso [07.11.2016 699.400.192]

We let install just basics and open-ssh (for being able to use putty in the warm office instead of the cold server room). With the one user (albrecht) made on install we just made the minimal alias and LAN settings (in ~/.bash_aliases and /etc/network/interfaces, cf. [29]). But we made no other changes nor updates so far.

To install PBIS and join the domain do:

```
mkdir Downloads
cd Downloads/
wget https://github.com/BeyondTrust/pbis-
open/releases/download/8.5.2/pbis-open-
8.5.2.265.linux.x86_64.deb.sh  ## three lines are one

chmod 774  pbis-open-8.5.2.265.linux.x86_64.deb.sh
sudo ./pbis-open-8.5.2.265.linux.x86_64.deb.sh
cd /opt/pbis/bin/
sudo domainjoin-cli join --disable ssh fb3-meva.fh-bochum.de
weinert@fb3-meva.fh-bochum.de  ## two lines are one

sudo shutdown -r now
```

The Ubuntu server PD337S has joined the domain. Logged in again as local albrecht

```
getent passwd
```

now shows thousands of AD user accounts. We can login as FB3-MEVA\weinert on a separate putty, but will be disappointed by the ugly sh instead of bash.

First user settings

```
getent passwd | grep weinert
```

reveals the shell problem.

```
FB3-MEVA\weinert:PBIS:1943012371:1943011841:Albrecht
Weinert:/home/local/FB3-MEVA/weinert:/bin/sh
```

```
sudo usermod -s /bin/bash  FB3-MEVA\weinert ## don't try this
```

will NOT work with PBIS.
Little searching puts us to PBIS' config tools where the shell can be changed for all users by:

```
sudo /opt/pbis/bin/config LoginShellTemplate /bin/bash
```

Now logging in as FB3-MEVA\weinert gets the nice bash. But being a AD admin means nothing, yet. weinert gets punished when trying sudo. The remedy is (caution!) visudo to make either all AD admins (as %group) sudoable or do so for single (admin) users. For the latter add something like

```
# Domain admin weinert may gain root privileges
FB3-MEVA\\weinert ALL=(ALL) ALL
```

to /etc/sudoers (using sudo visudo).

One might be tempted to set

```
sudo /opt/pbis/bin/config   UserDomainPrefix 'FB3-MEVA'
sudo /opt/pbis/bin/config  AssumeDefaultDomain true
```

for the comfort to type weinert instead of FB3-MEVA\weinert on logon. It works for logon but spills later sudo commands (then assuming a non existent local user, perhaps).

Hence, to keep the sudo privileges, the simple repair is set AssumeDefaultDomain false again by:

```
sudo /opt/pbis/bin/config  AssumeDefaultDomain false
```

On the other hand, with some applications (samba e.g.) and circumstances default domain settings are strongly recommended. To keep the exemplary FB3-MEVA\weinert sudo two more steps are required or, to put it cautiously, worked in our installation: Put pure weinert in local group sudo

```
sudo usermod -aG sudo weinert
```

and duplicate the suborders entry for weinert:

```
# Domain admin weinert may gain root privileges
FB3-MEVA\\weinert ALL=(ALL) ALL
weinert ALL=(ALL) ALL
```

Regarding the RAID drives inherited from the late W2003 file server

```
sudo lsblk -f
```
yields

```
NAME   FSTYPE LABEL        UUID                                 MOUNTPOINT
fd0
sda
└─sda1 ntfs   F:ileservice 6C90958D90955F00
sdb
└─sdb1 ntfs   E:xtra       70C4073AC4070258
sdc
└─sdc1 ntfs   H:ome        4A98C6E798C6D11D
sdd
├─sdd1 ext4               c685a218-1b69-4b71-bb13-ece220a52036 /
├─sdd2
└─sdd5 swap               c822db43-14fb-4931-8f31-c41fa117417d [SWAP]
sr0
```

We see sdd being the drive (also RAID and within the server compartment) having been formatted for the Ubuntu installation, having been formerly drives C: and S: (labelled "C:ystem" and "S:wap"). An we recognise sda, sdb and sdc as the former drives F:, E: and H: (by their clever label), still NTFS and old W2003 file system intact (located in the LSI megaRAID extender rack).

We check having NTSF support by (which we normally do):

```
dir /lib/modules/  ## see the numbers and use then en lieu de 63
ls /lib/modules/4.4.0-63-generic/kernel/fs | grep nt
```

Make three mount points for the LSI MegaRAID extender, here re-using the old Windows labels F:ileservice, E:xtra and H:ome without colon:

```
sudo mkdir /megaRaid
sudo mkdir /megaRaid/Extra
sudo mkdir /megaRaid/Fileservice
sudo mkdir /megaRaid/Home
```

Make one preliminary test mount:

```
sudo mount -t ntfs-3g /dev/sdc1 /megaRaid/Home/
dir /megaRaid/Home/home/weinert/eq.list
```

```
-rwxrwxrwx 2 root root 15716 2002-11-18 megaRaid/Home/home/weinert/eq.list
```

We see the mount working but no AD ACLs displayed.

Next we make three mounts permanent in etc/fstab by adding three lines at the end:

```
UUID=6C90958D90955F00  /megaRaid/Fileservice  ntfs-3g
defaults,windows_names,locale=de_DE.utf8  0 0

UUID=70C4073AC4070258  /megaRaid/Extra  ntfs-3g
defaults,windows_names,locale=de_DE.utf8  0 0

UUID=4A98C6E798C6D11D  /megaRaid/Home  ntfs-3g
defaults,windows_names,locale=de_DE.utf8  0 0
```

It works for all three drives (now mounts) as it should. But all is still root:root. And risk a reboot.

Having shares for AD users (samba)

Sofar the Ubuntu server machine PD337S is a domain member computer again in a Windows AD domain. We have all LSI megaRAID drives again with NTFS. We don't see the AD/NTFS ACLs there (yet?, just root:root).

To have PD337S again as file server – with or without the NTFS drives in their current state – we need shares, working and aware of AD user and group account. To get there we substantially follow [14].

To start we just install samba (+ nothing else!) and integrate it in PBIS:

```
cd /opt/pbis/bin/
dir
sudo ./samba-interop-install --install
sudo apt-get install samba
./samba-interop-install --check-version
sudo ./samba-interop-install --install
dir /etc/samba/
cp   /etc/samba/smb.conf  /etc/samba/smb.conf.orig
testparm
sudo nano   /etc/samba/smb.conf   ## make/re-make smb.conf
testparm
```

We expected additional problems when when sharing linked/mounted NTSF raid drives. So, we follow [14]'s recommendation to use a simple home-made (test) share, as not to complicate the basic file share function. In most (non LSI RAID, non NTFS) cases more is seldom required. With the last but one command above, we make an according smb.conf:

```
# Samba configuration file for PD337S in domain FB3-MEVA
# Beyond Trust, Albrecht Weinert              22.02.2017
# Whenever you modify this file you should run the command "testparm"
# to check that you have not made any basic syntactic errors.

[global]
 security = ADS
 workgroup = FB3-MEVA
 realm = PD337S.FB3-MEVA
 netbios name = pd337s
 machine password timeout = 0

# server string is the equivalent of the NT Description field
 server string = %h server (Samba, Ubuntu)

# This will prevent nmbd to search for NetBIOS names through DNS.
```

```
 dns proxy = no

 log file = /var/log/samba/log.%m
 max log size = 1000
 logging =
 server role = standalone server

# testshare will be the share's visible name (Freigabename)
# On a Windows machine make it available by something like
# net use t: \\192.168.89.15\testshare
# net use t: \\192.168.89.15\testshare * /USER:FB3-MEVA\otto
[testshare]
 comment = This is a test share
 path = /share
 browseable = yes
 read only = no
 valid users = FB3-MEVA\weinert
 writeable = yes
```

Make the share by

```
sudo mkdir /share
sudo chmod a+rx /share
dir /
sudo chown -H  weinert:domänen-benutzer /share/
dir /
sudo chmod 777 /share/
cp etc/samba/smb.conf /share/  # populate it
dir / # check population and ownership
```

When manipulating/populating a share on the Ubuntu machine, best do it logged in as the AD-user=owner. Otherwise access or read/only restrictions may occur.
Use the share on a Windows machine by:

```
net use t: \\192.168.89.15\testshare
```

It worked – hopefully will with you, too.

Remark 1: In all the years, we fell in the habit of using only IP addresses with "net use". This always worked like charm, while using DNS names, often produced funny errors, at once – or worse after a while or when using a second or third share.

Remark 2: If such share won't work, before panicking or doing complicated trouble shooting, repeating the commands

```
cd /opt/pbis/bin/
./samba-interop-install --check-version
sudo ./samba-interop-install --install
sudo domainjoin-cli join --disable ssh fb3-meva.fh-bochum.de
weinert@fb3-meva.fh-bochum.de
```

```
sudo  service smbd restart
```

never hurts, but was a remedy after installations or removes.

And ... risk a re-boot if your first share works.

Having come so far, we add the following at the end of /etc/samba/smb.conf just made above:

```
# net use m: \\192.168.89.15\megaRaid * /USER:FB3-MEVA\weinert
[megaRaid]
 comment = three LSI megaRAID drives
 path = /megaRaid
 browseable = yes
 read only = no
 valid users = FB3-MEVA\weinert
 writeable = yes

# net use z: \\192.168.89.15\%u * /USER:FB3-MEVA\%u
# e.g. use z: \\192.168.89.15\sfb72433 * /USER:FB3-MEVA\sfb72433
[homes]
 comment = student user's home in RAID
 path = /megaRaid/Fileservice/fb3stud/%u
 browseable = yes
 read only = no
 writeable = yes
```

After the change getting effective we have [megaRAID] as an administrative access to all NTFS drives and files in the LSI megaRAID rack. Samba's [homes] trick gives easy access for all (some 5000) student users to their file server shares formerly under F:\fb3stud\ by using:

```
net use y: \\192.168.89.15\sfb30917 * /USER:FB3-MEVA\sfb30917
```

and entering sfb30917's domain password.

By some Windows restrictions to the client this "use" cannot combined with any other shares got by other user names, like e.g.

```
net use t: \\192.168.89.15\testshare * /USER:FB3-MEVA\emil
```

triggering the infamous "error 1219" (sorry German, only):

```
Systemfehler 1219 aufgetreten.

Mehrfache Verbindungen zu einem Server oder einer freigegebenen Ressource
von demselben Benutzer unter Verwendung mehrerer Benutzernamen sind nicht
zulässig. Trennen Sie alle früheren Verbindungen zu dem Server bzw. der
freigegebenen Ressource, und versuchen Sie es erneut.
```

As the error massage says

```
net use m: /Y /D
net use t: /Y /D
```

will let it (net use y: ...) happen. The other way out of 1219 is sticking to the rule

"All shares used simultaneously have have to be available to one (1!) user account, being available to the (human) user at the machine in question!"

```
Status       Lokal     Remote                    Netzwerk
OK           M:        \\192.168.89.15\megaRaid  Microsoft Windows Network
OK           Y:        \\192.168.89.15\dfb30017  Microsoft Windows Network
Der Befehl wurde erfolgreich ausgeführt.
```

In most cases it might be easy to meet this condition, if known beforehand. In other cases it becomes an organisational nightmare involving AD accounts, Samba configuration and (automated) login procedures at client workstations. (Have fun!)

Hopefully we and you will always find a configuration trick to avoid f..n 1219 – one of Windows' favourite bitchinesses when it comes to using shares.

Resume

We have made an Ubuntu server join an AD domain and being aware of all domain users using PBIS open. We never got this far with the "krb5-user-samba-sssd" approach.
The OS entry of the member computer PD337S in AD automatically got:

```
name = Ubuntu;
version = 16.04;
ServicePack = PBIS Open 8.5.265.265.
```

We have (Samba) shares for an AD users.

We've mounted all former W2003 file server NTSF drives (LSI megaRAID) intact.
Still to do: See if we can revive those files AD/NTFS ACLs anyhow.

References and Abbreviations

Please find those in
[29] Albrecht Weinert, Ubuntu for remote services, Report, November 2016,
(the full story): a-weinert.de/pub/ubuntu4remoteServices.pdf

We keep those in one (the biggest Ubuntu server) document for consistency, so far. Also, see the policy on "Using names" there in the Abstract.

If you see this in print you may look at
[28] Albrecht Weinert, Make a Linux server Active Directory member, Report, February 2017,
This paper (the last actual version): a-weinert.de/pub/makeUbuntuServerADmember.pdf

Table of Content

Dr. Albrecht Weinert is computer science professor at
Bochum University of Applied Sciences or Hochschule Bochum.
He is founder and director of
MEVA-Lab – Laboratory for versatile distributed applications –
as well as of the service provider weinert - automation.
albrecht@a-weinert.de

Rev. 06 03.03.2017