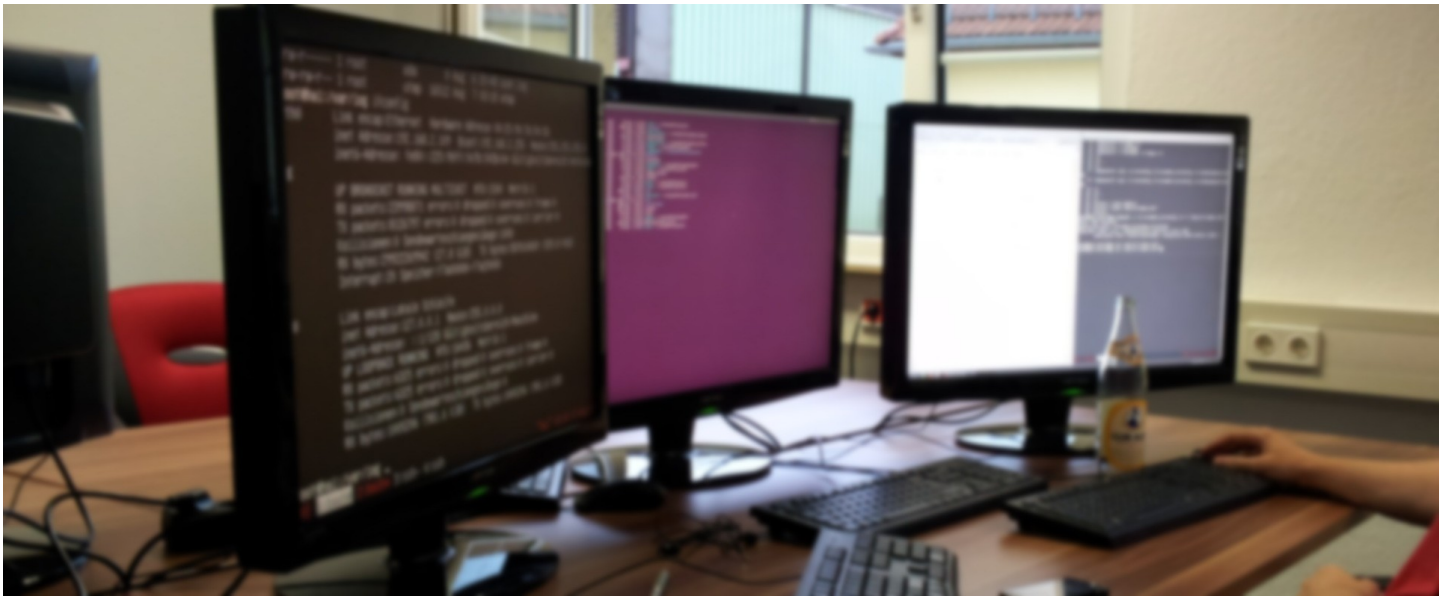

Samba 4 Active Directory controller with Windows 7 roaming profiles + Linux login – The complete guide

Stefan on 02/07/2014 under developer (/categories/developer/)

9 minute read

Out Of Date Warning

This article was published on **02/07/2014**, this means the content may be out of date or no longer relevant. You should **verify that the technical information in this article is still up to date** before relying upon it for your own purposes.

Recently, we decided to rebuild our office setup with Samba 4, which ships with the Ubuntu 14.04 packages. At pludoni, we'd like to create virtual working spaces, so that users can use every computer and have their profile synchronized. Ideally, so that you can set one password and log in to all internal company services. As different users have different requirements, the login should work across Windows PCs (I look at you, MS Office and Adobe Creative Suite), Linux workstations and the developer server. Besides this, various services, like Gitlab and Chat-server should query the same authentication database.

During the last few days, we achieved most of our goals with the setup. I want to record how we progressed with this blog post for future reference and happy Googlers :).

Table of Contents

Definitions

In the following guide, we assume these settings:

- `pdc.pludoni.com` - DNS name of the machine dedicated as the **P**rimary **D**omain **C**ontroller. I suggest, using a virtual machine with bridged network (as forwarding the gazillion ports is kind of a hassle) or a dedicated server
- `PDC` - Netbios name of the PDC
- `PDC01` - working group name (has to differ from netbios name)
- Ubuntu 14.04 server edition for Domain controllers
- Ubuntu 14.04 desktop for the Linux clients
- Windows 7 SP2 Professional for Windows clients

Setting up the domain controller

Starting off with a fresh Ubuntu 14.04 server edition, we followed this guide (http://www.server-world.info/en/note?os=Ubuntu_14.04&p=samba&f=4):

Kerberos

```
apt-get install samba krb5-config libpam-smbpass nfs-kernel-server
```

(nfs-kernel-server is not necessary, see later for Ubuntu clients)

Run `kerberos-config` if it didn't show up during installation:

```
dpkg-configure krb5-config
```

Answer the questions:

- Default Kerberos Realm: `PDC.PLUDONI.COM`
- Kerberos servers for your realm: `pdc.pludoni.com`
- Administrative server for your Kerberos realm: `pdc.pludoni.com`

Samba

Run: `samba-tool domain provision`

Answer:

- Real: `PDC.PLUDONI.COM`
- Domain: `PDC01`
- Role: `<Enter>`
- DNS Backend: `<Enter>`
- DNS Forwarder: <Enter your DNS server's IP>
- Admin password (hereafter referenced as `PASSWORD`)
- reboot
- `samba-tool domain level raise --domain-level 2008_R2 --forest-level 2008_R2`
- Password settings, adjust as necessary:

  `samba-tool domain passwordsettings set --complexity=off --min-pwd-length=6 --max-pwd-age=0`

After that, edit `/etc/samba/smb.conf` and add the profiles section. Also increasing the log level might be helpful for debugging if there are problems later on

```
# Global parameters
[global]
        workgroup = PDC01
        realm = PDC.PLUDONI.COM
        netbios name = PDC
        server role = active directory domain controller
        dns forwarder =
log level = 3 # <--- Might want to add this

[netlogon]
        path = /var/lib/samba/sysvol/pdc.pludoni.com/scripts
        read only = No

[sysvol]
        path = /var/lib/samba/sysvol
        read only = No

[profiles] # <---- ADD here
   path = /var/lib/samba/sysvol/pdc.pludoni.com/profiles
   read only = no
```

After a fresh reboot, that's it for the PDC! :) That didn't hurt, did it?

Optional: NFS-exports

Windows has it's roaming profiles. To achieve something similar for the Linux workstations, we just mount a home folder via NFS. As we installed a nfs-kernel-server we added a `/etc/exports` to make it possible for the clients to mount the folder:

```
# /etc/exports

"/ubuntu-homes/" 192.168.2.0/255.255.255.0(rw,async,no_root_squash,insecure)
```

Don't forget to `mkdir /ubuntu-homes && service nfs-kernel-server restart` afterwards.

Setting up Windows clients with roaming profiles

After fiddling around, we successfully applied the following procedure to several clients:

- Install Windows on a client, if not already done
- Add registry entries in `regedit.exe` (source (https://wiki.samba.org/index.php/Registry_changes_for_NT4-style_domains)):

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters]

DomainCompatibilityMode = 1 (dword)

DNSNameResolutionRequired = 0 (dword)
```

- Make sure the DNS-Server in your network settings is the PDC server IP
- Make sure the clock is in sync with the PDC – Login won't work if the difference is too large!
- Join domain:
  - Right click on My Computer in start menu
  - Click on Change Settings in the right bottom
  - Click "Change"
  - Check "Member of": `pdc.pludoni.com` , OK
  - There should be a login prompt, use: Administrator, PASSWORD
  - You should be able to join the domain. If it didn't work, you should check the DNS settings first and then consult the Samba log on the PDC (/var/log/samba/log.*)
  - reboot.

Repeat steps 1 through 5 for every additional windows pc.

Initial Samba profile setup (once)

- Try to reach the samba shares via explorer: `\\pdc.pdc.pludoni.com\`
- You should be able to change the settings of the Profiles folder (Security tab) and set the permissions accordingly (full access/read/write etc.) **this is important, otherwise roaming won't**

work

- Inside profiles, create a folder with the name of user + '.V2' for each user, like: `{username}.V2` , e.g. `stefan.V2`
- Download Microsoft Remote Server Administration Tools http://www.microsoft.com/en-us/download/details.aspx?id=7887 ([Windows 7 Version])
- Install it (takes a long time), and activate it:

```
(from the MS site)
 5. In the Programs and Features area, click Turn Windows features on or off.
 6. If you are prompted by User Account Control to enable the Windows Features dialog box to open, click Continue.
 7. In the Windows Features dialog box, expand Remote Server Administration Tools.
 8. Select the remote management tools that you want to install.
```

- Run it, create your users under Users section. Don't forget to add an E-Mail, if you want to log in to Gitlab (and other services which require that field).
- Don't forget to add a profile path, to make use of roaming profiles, e.g.: `\\pdc.pdc.pludoni.com\profiles\%USERNAME%` (USERNAME will be replaced by the interface)

Done with windows! Try to log out and log in with another user to check if roaming profiles work.

Setting up Ubuntu desktop clients

Using samba and not LDAP as the primary authentication backend was a little tricky. After several tries we went with PBIS (http://www.beyondtrust.com/Resources/OpenSourceDocumentation/) (formerly known as Likewise-open), which had a really easy setup **Original Guide (http://community.spiceworks.com/how_to/show/80336-join-ubuntu-14-04lts-to-a-windows-domain-using-pbis-open)** Summary of the guide, for future reference in case of site offline

Download (http://download1.beyondtrust.com/Technical-Support/Downloads/PowerBroker-Identity-Services-Open-Edition/?Pass=True)

```
cd ~
sudo wget http://download.beyondtrust.com/PBISO/8.0.1/linux.deb.x64/pbis-open-8.0.1.2029.linux.x86_64.deb.sh
sudo chmod +x pbis-open-8.0.1.2029.linux.x86_64.deb.sh
sudo ./pbis-open-8.0.1.2029.linux.x86_64.deb.sh

# Answer questions (no, yes)

/opt/pbisdomainjoin-cli join --disable ssh pdc.pludoni.com Administrator
# type Administrator Password
# wait for SUCCESS
sudo /opt/pbis/bin/config UserDomainPrefix PDC01
sudo /opt/pbis/bin/config AssumeDefaultDomian true
sudo /opt/pbis/bin/config LoginShellTemplate /bin/bash
sudo /opt/pbis/bin/config HomeDirTemplate %H/local/%D/%U
```

Change some settings in /etc/pam.d/common-session:

```
sudo vi /etc/pam.d/common-session

# Find the line that states the following:
# session sufficient pam lsass.so
# Replace it with:
# session [success=ok default=ignore] pam_lsass.so
```

Activate manual login for the login screen (Lightdm):

```
# sudo vi /usr/share/lightdm/lightdm.conf.d/50-unity-greeter.conf

allow-guest=false
greeter-show-manual-login=true
```

We had some problems with the greeter. If it doesn't work, create a new file under `/usr/share/lightdm/lighdm.conf.d/99-custom.conf` with the same settings.

Allow "Domain Admins" to use sudo in `/etc/sudoers.d/samba`. Make sure the file has `chmod 0440 /etc/sudoers.d/samba`:

```
%domain^admins ALL=(ALL) ALL
```

We also wanted a kind of roaming profile with Ubuntu, but eventually decided to separate, as we didn't like mixing the two, which results in a folder mess and long Windows log in/out times, as Windows has to sync the whole directory. PBIS doesn't help with that requirement. After fiddling a little with samba-clients, we ran into problems with the permission systems, so we decided to go the easy route: just mount a folder with all the profiles via NFS at boot time, using fstab:

```
pdc.pludoni.com:/ubuntu-homes /home/local/PDC01 nfs rw 0 0
```

Initial mount: `mkdir /home/local/PDC01 && mount /home/local/PDC01`

Warning if using dual boot

If you plan to run Windows and Ubuntu alongside each other on a single machine, make sure, to tell Ubuntu to use local time for the hardware clock. Otherwise, Windows will have the wrong time **and Samba Login won't work because of this**. One way to fix it:

```
# add this line in /etc/default/rcS
UTC=no
```

After reboot, check if `date == hwclock -r`. If it is still in the wrong timezone, running `'ntpdate -u ntp.ubuntu.com && hwclock -w` might help.

Bonus feature: Provide a file bookmark to the Windows roaming profile

New users will have a home folder created from `/etc/skel` on the workstations.

```
mkdir -p /etc/skel/.config/autostart
vim /etc/skel/.config/autostart/mount_windows.desktop
```

```
[Desktop Entry]
Type=Application
Exec=/usr/local/bin/mount_windows
Hidden=false
NoDisplay=false
X-GNOME-Autostart-enabled=true
Name[de_DE]=Automount windows
Name=Automount windows
Comment[de_DE]=
Comment=
```

And create a executable file under `/usr/local/bin/mount_windows` :

```
#!/bin/bash
sleep 5
echo "file://$HOME/Dokumente
file://$HOME/Musik
file://$HOME/Bilder
file://$HOME/Videos
file://$HOME/Downloads
smb://pdc.pdc.pludoni.com/profiles/$USER.V2 Windows-Profil on pdc
" > ./.config/gtk-3.0/bookmarks
```

This will reset the user's bookmarks to the default (here German!) + a Samba share. Adjust to your needs :). You can also put apps into the Autostart for each user the same way (e.g. Chat-App or time-tracker)

Connecting various services via LDAP

Besides using Samba for authentication, you can use plain LDAP to connect different services, e.g. ejabberd, Gitlab, Jenkins, Bugtracker, CRM, ...

The command `ldapsearch` helps to find out necessary fields and filters:

```
ldapsearch -h pdc.pludoni.com -D 'cn=Administrator,cn=Users,dc=pdc,dc=pludoni,dc=com' -x -W -b 'cn=Users,dc=pdc,dc=pludoni,dc=com'
```

For opportunistic Googlers and future reference, here are the configurations for some services we use:

Gitlab

Gitlab needs an e-Mail for each user. Make sure it is provided in the Active Directory Users & Groups.

```
# Gitlab gitlab.yml
host: 'pdc.pludoni.com'
base: 'cn=Users,dc=pdc,dc=pludoni,dc=com'
port: 389
uid: 'samaccountname'
method: 'plain'
bind_dn: 'cn=Administrator,cn=Users,dc=pdc,dc=pludoni,dc=com'
password: 'PASSWORD'
```

ejabberd

```
# ejabberd.cfg
{auth_method, ldap}.
{ldap_servers, ["pdc.pludoni.com"]}.
{ldap_encrypt, none}.
{ldap_port, 389}.
{ldap_rootdn, "cn=Administrator,cn=Users,dc=pdc,dc=pludoni,dc=com"}.
{ldap_password, "PASSWORD"}.
{ldap_base, "cn=Users,dc=pdc,dc=pludoni,dc=com"}.
{ldap_uids, [{"sAMAccountName", "%u"}]}.
{ldap_filter, "(objectClass=person)"}.
```

Errbit

```
# Errbit error tracking
production:
  host: pdc.pludoni.com
  port: 389
  attribute: sAMAccountName
  base: cn=Users,dc=pdc,dc=pludoni,dc=com
  admin_user: cn=Administrator,cn=Users,dc=pdc,dc=pludoni,dc=com
  admin_password: 'PASSWORD'
  # group_base:
  ssl: false
  uid: "sAMAccountName"
```

Jenkins

- Server: `pdc.pludoni.com`
- Root-DN: `dc=pdc,dc=pludoni,dc=com`
- Users: `cn=Users`
- Filter: `samaccountname={0}`
- Group: `(empty)`
- Manager-DN: `cn=Administrator,cn=Users,dc=pdc,dc=pludoni,dc=com`

Troubleshooting

If login or joining a domain doesn't work:

- Make sure, DNS works: `nslookup pdc.pludoni.com` has meaningful result
- Check the clocks
- Make sure Profile folders are accessible via samba (e.g. on Windows just enter `\\pdc.pdc.pludoni.com\profiles\` , also might want to check the Windows access rights again.
- Check the PDC logs (`tail -f /var/logs/samba/log.samba` and `tail -f /var/logs/samba/log.smbd`)

Possible improvements

Add security. If you don't trust your users very much, enable LDAP encryption, think about Samba access rules, and add a manager account instead of using the Administrator account for the services.

In future, we'd like to add more things:

- Configure e-mail server to use LDAP (maybe using Zarafa)
- Add (Open)VPN to enable remote login
- Think about regular backup of the roaming-profiles and NFS-homes

This guide was developed from sweat and tears by my collegue Akos Toth (https://www.xing.com/profile/Akos_Toth2) and me.

---

server (/categories/server/) windows (/categories/windows/) linux (/categories/linux/) office (/categories/office/) pludoni (/categories/pludoni/) guide (/categories/guide/)

Related posts

Gitlab CI with Docker - Test and deploy Rails apps (/blog/2015/11/07/gitlab-ci-with-docker-starting-guide/) *07/11/2015* — rails, gitlab, docker, server, pludoni, guide

How to replace soft RAID1 hard drive (Hetzner) (/blog/2014/07/10/how-to-replace-soft-raid1-hard-drive-hetzner/) *10/07/2014* — server, guide

Fix anoying message with vagrant ubuntu base box related to en_ZM.UTF-8 locale (/blog/2012/07/06/fix-anoying-message-with-vagrant-ubuntu-base-box-related-to-en-zm-dot-utf-8-locale/) *06/07/2012* — vagrant, server, linux, english

Easy Website-Performance Tests mit ab (/blog/2010/11/04/easy-website-performance-tests-mit-ab/) *04/11/2010* — server, linux, german

Batch umbenennen mit Unix/Linux Standardprogramm rename (/blog/2010/11/04/batch-umbenennen-mit-unix-linux-standardprogramm-rename/) *04/11/2010* — linux, bash, server, tools, german

---

← Side project: Hackingchinese Resources (/blog/2014/06/11/side-project-hackingchinese-resources/) 11/06/2014

How to replace soft RAID1 hard drive (Hetzner) → (/blog/2014/07/10/how-to-replace-soft-raid1-hard-drive-hetzner/) 10/07/2014

Wintermute • a year ago

We are using the Zentyal implementation of Samba4, to authenticate linux ubuntu 14.04 and Windows 7 clients desktops.

Recently a major issue came up : an usual ubuntu user had to log into a Windows 7 box. It worked, but the next day, the main user for the Windows 7 box just saw his user account was reset : no more desktop shortcuts, files etc... just a default user setting and that's all. Please be aware that the user reset happened for a different user than the linux one who logged in the Windows box. The same day, the linux user, some hours later, just saw his own user account reset ... ! Roaming profiles shouldn't be involved since they are only applied to specific Ubuntu desktops, that are none of the desktops involved in this case.

A week has almost passed and still we have no answers. Neither Google nor Zentyal offers any help. The Zentyal IRC is a time wasting joke. I'm running out of options. Do you have an idea of what could be wrong ?

1 • Reply • Share ›

thealbino raven Wintermute • a year ago

yes, in that case it is called a 'restore'. These magical things called 'restores' can be found on your tape backups of the roaming profiles directory that are usually done nightly with a process called an incremental backup. Believe it or not, even in an all windows universe roaming profiles are 'eaten' by accident often enough that there are vendors out there that offer backup solutions to wave the magical wand of "restore".

• Reply • Share ›

jk • 2 years ago

I can also say that this guide is a marvelous masterpiece!!!

1 • Reply • Share ›

Stefan Wienert Mod jk • 2 years ago

Thanks! :)

• Reply • Share ›

Jay's Geek Shop • 2 years ago

This is exactly the guide I was looking for. I've recently added a couple of laptops to my home network for the kids to use, and my wife and I use multiple computers. Thank you so much for this guide!

1 • Reply • Share ›

Kromonos • a year ago

Subsonic works also great with LDAP:
LDAP URL: ldap://pdc.pludoni.com:389/cn=Users,dc=pdc,dc=pludoni,dc=com
Searchfilter: samaccountName={0}
LDAP Manager DN: pdc01\Administrator

• Reply • Share ›

iawes • 2 years ago

and that dns ip should be config first?

• Reply • Share ›

iawes • 2 years ago

After a fresh reboot, that's it for the PDC! :) That didn't hurt, did it?

before this line, it is all ok

• Reply • Share ›

iawes • 2 years ago

server role = 'active directory domain controller' not compatible with running smbd standalone.

when I start smbd on my ubuntu 14.04, this error occur, I have no idear about that , please help me,thx

• Reply • Share ›

Jonas • 2 years ago

This looks like a great guide, hope it will help me along the way. Just wanted to mention, there is no SP2 for Win7.

• Reply • Share ›

Jonas Hallgren • 2 years ago

Brilliant! Thank you! My only trouble following this guide on a new Linux client (Ubuntu 14.04 desktop) was to fix resolve.conf and running sudo resolvconf -u

• Reply • Share ›

Jonas Hallgren Jonas Hallgren • 2 years ago

Also, a couple of typos, here are the corrections I found (under the Ubuntu client part!)
/opt/pbis/bin/domainjoin-cli join --disable ssh pdc.pludoni.com Administrator
sudo /opt/pbis/bin/config AssumeDefaultDomain true
# session sufficient pam_lsass.so
Thank you again!

• Reply • Share ›

Troy Wolfe • 2 years ago

The server I have set up gave me one small issue and it took me forever to figure it out.
Before the issue though, I would like to add that:
samba-tool domain provision
requires that /etc/samba/smb.conf that is generated by installing samba be renamed.

My issue was that when I installed Ubuntu 14.04.1 my network interface was named to em1 instead of eth0

As a result I would get the error in this linux questions thread:
http://www.linuxquestions.org/...

(my thread btw)

I solved the issue by adding the line:
interfaces = 127.0.0.0/8 em1
into the smb.conf file

Otherwise, this is an awesome tutorial!

• Reply • Share ›

Tim Porter • 2 years ago

Awesome article and many thanks! However, I am consistently getting an error when trying to provision. It will pickup my domain name and complain its not a valid NetBIOS name! I'm tried it many times from other builds as well. Same results. What am I missing here? Any help would be tremendously appreciated!
Thanks

• Reply • Share ›

ardukar Tim Porter • 2 years ago

Hi Tim,
did you follow the name conventions for NetBIOS names (your domain)?
Your domain name must not be longer than 15 characters. And you are not allowed to use the characters "/\?:*<>|

• Reply • Share ›

ardukar • 2 years ago

Great guide! Easily set up the DC so far, ubuntu clients work like a charm.
Struggeling to get the Windows clients up and running. Joining the domain was no problem at all.
But after reboot, how do I proceed? I logged into the machine with my local user&password. I can find profiles folder on the server via \\server.domain.lan\ but
cannot find secutitytab neither can I enter the profiles folder to add user profiles.. can anybody point me to some idea?

• Reply • Share ›

Troy Wolfe ardukar • 2 years ago

I believe you need to login as a domain user.

1 • Reply • Share ›

Muthukkumar • 2 years ago

Hi All,

I just did samba 4.1 AD 15 day's back everything working is fine now. i joined the one more machine (windows 7) to domain i'm getting the error "The security ID Structure is invalid" and also i try to browse the server in administrator user the same error occured, when i try to open RSAT tool "RPC server is unavailable" existing node

kindly help me to solve this issue

• Reply • Share ›

ZAJDAN ➚ Muthukkumar • 2 years ago

I am facing same problem "RPC server is unavailable" but so far I do not know what makes the problem....if somebody know, please say how to solve it...thnx

• Reply • Share ›

Siddu • 2 years ago

very good doc ....

• Reply • Share ›

jk • 2 years ago

Stefan, it should be said, that the server that you want the AD to run on, should point to itself when it comes to resolving hostnames. In resolv.conf:

nameserver 127.0.0.1

• Reply • Share ›

jk ➚ jk • 2 years ago

I would also recommend adding information on how to set the permissions for profiles folder on the samba server for the roaming profiles to work properly

• Reply • Share ›

jk • 2 years ago

Question: does unlocking screensaver on ubuntu desktop work with samba stored passwords?

• Reply • Share ›

Stefan Wienert Mod ➚ jk • 2 years ago

I didn't test it right now, but yes, all authentication dialogues (including sudo/admin confirmation) are using the same credentials

• Reply • Share ›

Jking369 • 2 years ago

I was just wondering how its working out?

• Reply • Share ›

Stefan Wienert Mod ➚ Jking369 • 2 years ago

We are running this setup more or less in our office for 3 months now. Granted, we are only about 6 people. We had one or two outages, but that might be related to the virtualization or with the NFS + hard drive speed.

• Reply • Share ›

joebell • 2 years ago

Can Samba 4 be easily seen in the Microsoft Network by its network name? I read a lot of articles there was no NetBIOS browsing support (network neighborhood)
available. Is this correct?

• Reply • Share ›

keV ➚ joebell • 2 years ago

I've used Samba4 as a DC and it is easily connected to using its hostname or FQDN.
Just \\hostname into explorer and all the shares are there.
In active directory administration tools it shows as W2K8 R2, even though it's Linux and Samba4

I think the articles mean that when you click on Network (network neighborhood) then it doesn't show up when then network is "scanned"
Mine does not show, but it may just be a configuration issue, I'm not sure.
If you know the hostname, it's much quicker to just type that in anyway.
And once you've accessed it then it does show in the network list on that PC.

• Reply • Share ›

Stefan Wienert Mod keV • 2 years ago

Thanks for the answer. I am usually not waiting for the windows clients to show up in the network, as it might take a long time and be an issue with the router and/or DNS config.
Putting the name into the explorer worked every single time, so it is a much better way of describing what to do in a guide like this.

• Reply • Share ›