

How to join or connect UBUNTU Desktop 18.10 Workstation to an Active Directory (AD) Domain, including automatic mounting of CIFS (SMB) shares and home directory

This page describes the results of a small 3 day workshop i threw with a former colleague on how to set up an UBUNTU Desktop 18.10 Workstation that connects to an existing (SAMBA 4 based) Active Directory domain, so that users can use their AD user accounts to graphically logon and have their cifs (or smb) shares and (windows) home directories mounted automatically on login.



NOTE: In this scenario the Linux workstations are supposed to be used as a SINGLE USER workstation only! That means, its not allowed (more precise, its untested) to logon more than one user to the workstation at a time. Since this **may** result in a conflict or collision on auto-mounting, as we do it here.

Scenario / Project Goals:

1. Using a somewhat **modern and popular Linux workstation distro** like UBUNTU 18
2. Connect/Join it to an existing Active Directory (AD) Domain so that **Users can logon to it using their Domain-Accounts** (no need of local linux accounts)
 1. Both, Windows- or Linux based AD Domain-Controllers should work.
 2. We assume a properly set up networking environment with DHCP, DNS and open internet access is given.
3. Have some network **shares mounted automatically** for the user on login (no user interaction required)
 1. Common shared network shares are mounted onto root level filesystem mountpoints like **/xray/** or **/share/** .
 2. Windows-Homedirectory is supposed to be temporarily mounted to **/home/loginName/** .
4. **only one user at a time** will use the workstation (no multiuser)
5. Some sort of "linux login script" should be triggered whenever a user logs in or opens a linux terminal to set up the users shell environment.
6. Do not show a "user picker" on graphical logon. Users are required to enter their login name manually.

Sources and further documentation used:


- <https://help.ubuntu.com/its/serverguide/sssd-ad.html.en>
- Book: SAMBA 4 Praxisbuch für Administratoren
- misc personal historic notes.



NOTE: Contains errors!

Installation and configuration:

1. Install UBUNTU 18.10 from DVD or USB Stick/Drive as **minimal installation** using the whole disk. We recommend to install updates while installation.

1.  **IMPORTANT: When asked for the Hostname make sure you enter the FQDN (that is hostname + local DNS domain name) instead of the short hostname only!** This saves a little additional work and makes sure that later the system will support short hostnames on command line interface and configuration files. However its always recommended to use FQDN, wherever you enter a hostname.
 2. If you missed entering the FQDN on installation time you later will have to add it to your **/etc/hosts** file.

2. Test if important AD specific DNS records are existing:

```
host -t srv _kerberos._tcp.$(hostname -d)
host -t srv _ldap._tcp.$(hostname -d)
host -t srv _kpasswd._tcp.$(hostname -d)
# expected result: no errors
```

3. Install the required packages for kerberos authentication, time synchronisation, [SSSD Layer](#) and local samba (client) components:

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

4. Create or edit **/etc/krb5.conf** to look like this:

[/etc/krb5.conf](#)

```
[libdefaults]
    default_realm = YOUR_FQ_AD_DOMAINNAME.UNI-FREIBURG.DE
    ticket_lifetime = 24h
    renew_lifetime = 7d
```

5. Ensure proper time synchronisation using chrony on our workstation side. It does not matter what you use for time sync. Just make sure your AD Domain Controller and all your workstations use the same timeserver. Therefor create or edit your ntp daemon config file, so it uses your preferred timeserver:

[/etc/chrony/chrony.conf](#)

```
# Welcome to the chrony configuration file. See chrony.conf(5) for
more
.
.
.
# About using servers from the NTP Pool Project in general see
(LP: #104525).
# Approved by Ubuntu Technical Board on 2011-02-08.
# See http://www.pool.ntp.org/join.html for more information.
```

```
#pool ntp.ubuntu.com iburst maxsources 4
#pool 0.ubuntu.pool.ntp.org iburst maxsources 1
#pool 1.ubuntu.pool.ntp.org iburst maxsources 1
#pool 2.ubuntu.pool.ntp.org iburst maxsources 2

# WE DONT WANT FOREIGN TIME SERVERS TO BE USED.
# So we commented out all those "pool" lines.
.
.

server time.uni-freiburg.de
# your time server goes here ^^^^
# it "maybe" is your local AD Domain controller itself, if it runs
a local ntp time server.
```

6. Start/Restart the local time synchronisation service, so we have consistent time with the AD domain controller:

```
systemctl restart chrony.service
```

7. Create or edit your **/etc/samba/smb.conf** so it contains the minimum required configuration to use with "smb client" and kerberos command line tools:

[/etc/samba/smb.conf](#)

```
[global]

workgroup = YOUR_NETBIOS_AD_DOMAINNAME #(short version)
client signing = yes
client use spnego = yes
kerberos method = secrets and keytab
realm = YOUR_FQ_AD_DOMAINNAME.UNI-FREIBURG.DE
security = ads
```

- **NOTE:** We dont want ANY samba shares on the workstation side. Therefor we dont have any example or default samba-shares sections in your smb.conf!
8. Now we configure the SSSD layer, so it knows what frontend and backend services we want it to serve/interface. Create the file if it does not exist just yet.

[/etc/sss/sss.conf](#)

```
[sss]
services = nss, pam
config_file_version = 2
domains = YOUR_FQ_AD_DOMAINNAME.UNI-FREIBURG.DE

[domain/YOUR_FQ_AD_DOMAINNAME.UNI-FREIBURG.DE]
id_provider = ad
```

```
access_provider = ad

# Use this if users are being logged in at /.
# This example specifies /home/DOMAIN-FQDN/user as $HOME. Use
with pam_mkhomedir.so
#override_homedir = /home/%d/%u
override_homedir = /home/%u

# Uncomment if the client machine hostname doesn't match the
computer object on the DC.
# ad_hostname = mymachine.myubuntu.example.com

# Uncomment if DNS SRV resolution is not working
# ad_server = dc.mydomain.example.com

# Uncomment if the AD domain is named differently than the Samba
domain
# ad_domain = MYUBUNTU.EXAMPLE.COM

# Enumeration is discouraged for performance reasons.
# However, i want to be able to list all available AD user
accounts and groups. So im going to enable this:
enumerate = true
```

9. Make sure the file permissions on **/etc/sss/sssd.conf** are set to a minimum:

```
chown root:root /etc/sss/sssd.conf
chmod 600 /etc/sss/sssd.conf
```

10. Now we are ready to attempt a first AD domain authentication and domain join using the Domain Administrator account:

```
kinit Administrator
# interactively enter the domain administrators password

# see if we received a valid kerberos ticket/token from the DC:
klist

# then try a domain join (add new installed workstation computer to the
windows domain, so the domain controller gets aware of it and allows
user logons from it in the future):
net ads join -k
```

11. NOW that we are known by the AD Domain Controller, we can try to start the local samba and sssd services:

```
systemctl restart smbd.service nmbd.service
systemctl start sssd.service
```



NOTE: The original manual that we first used did this WRONG (too early) and lead to weird unclear error messages in the /var/log/syslog preventing us from successfully starting these local services! At this point in time, after a successful domain join, its supposed to be started without any problems.

12. Test if we now can see/list the AD user accounts and/or AD groups on our workstation side:

```
#syntax: getent passwd adLoginName

getent passwd

# expected result: a whole list of all AD user accounts available.
# Example:
#
werner:*:878801300:878800513:werner:/home/YOUR_FQ_AD_DOMAINNAME.UNI-FREIBURG.DE/werner:

getent group

# expected result: a whole list of all AD groups available.
# Example:
#      .
#      .
#      .
#      domain
guests:*:878800514:student0,student1,student2,student3,student4,student5,student6,student7,student8,student9,someAdUsername,anotherAdUsername,yetAnotherAdUsername,guest
#      some
adGroupName:*:878801198:someAdUsername,anotherAdUsername,yetAnotherAdUsername
domain admins:*:878800512:administrator
#      .
#      .
#      .
```

13. At this stage the AD integration itself is pretty much complete. Now we are going after the automatic mounting of samba (windows-) shares and network-home drive for the local users. For this we decided to use pam_mount. So we need to install some more packages now:

```
apt install cifs-utils libpam-mount -y
```

14. Create or edit **/etc/security/pam_mount.conf.xml** to configure where to mount the users home directory and all the other cifs/smb shares to our local workstation:

[/etc/security/pam_mount.conf.xml](#)

```
<?xml version="1.0" encoding="utf-8" ?>
<!DOCTYPE pam_mount SYSTEM "pam_mount.conf.xml.dtd">
<!--
```

```
See pam_mount.conf(5) for a description.
-->

<pam_mount>

    <!-- debug should come before everything else,
    since this file is still processed in a single pass
    from top-to-bottom -->

<debug enable="1" />

    <!-- Volume definitions -->

    <!-- pam_mount parameters: General tunables -->

<!--
<luserconf name=".pam_mount.conf.xml" />
-->

<!-- Note that commenting out mntoptions will give you the
defaults.
    You will need to explicitly initialize it with the empty
string
    to reset the defaults to nothing. -->
<mntoptions
allow="nosuid,nodev,loop,encryption,fsck,nonempty,allow_root,allow
_other" />
<!--
<mntoptions deny="suid,dev" />
<mntoptions allow="*" />
<mntoptions deny="*" />
-->
<mntoptions require="nosuid,nodev" />

<logout wait="0" hup="0" term="0" kill="0" />

    <!-- pam_mount parameters: Volume-related -->

<mkmountpoint enable="1" remove="true" />

<!--

<volume
fstype="cifs"
server="yourFileServer.AdDomainName.uni-freiburg.de"
path="home"
mountpoint="/home"
options="vers=1.0,sec=ntlmv2,workgroup=YOUR_AD_NETBIOS_NAME" />
```

```
-->

<!--
    WATCH OUT! on UBUNTU 18 the cifs mount option
    "vers=1.0" **may** be required, because of some
    weird bug/feature. See ...
https://bugs.launchpad.net/ubuntu/+source/cifs-utils/+bug/1764778
    For some strange reason, it was not required to
    mount any other network share, other than HOME.
-->

<!--

NOTE: On earlier and other Linux Distro, like openSuse 13 it
seems we have been able to use the ...
    sec=krb5,cuid=%(USERUID)
... mount options to access the network shares. On UBUNTU 18
however, we have been unable so far to achieve that for whatever
reason. But we found out, that it will just work if we replace
these two parameters with ...
    sec=ntlmv2

This might have to do with the fact, that we only had some SAMBA
Server as AD DC and Fileserver, not a real Windows Server.

EXAMPLES that hat seem to work on openSuse 13 :

<volume
fstype="cifs"
server="yourFileServer.AdDomainName.uni-freiburg.de"
path="home"
mountpoint="/home"
options="sec=krb5,cuid=%(USERUID),workgroup=YOUR_AD_NETBIOS_NAME"
/>

<volume
fstype="cifs"
server="yourFileServer.AdDomainName.uni-freiburg.de"
path="xray"
mountpoint="/xray"
options="sec=krb5,cuid=%(USERUID),workgroup=YOUR_AD_NETBIOS_NAME"
/>

-->

<!-- ##### MOUNT USERS HOME DRIVE ##### -->
```

```
<volume
fstype="cifs"
server="yourFileServer.AdDomainName.uni-freiburg.de"
path="home/$(DOMAIN_USER)"
mountpoint="/home/$(DOMAIN_USER)"
options="vers=1.0,sec=ntlmv2,workgroup=YOUR_AD_NETBIOS_NAME" />

<!--
    WATCH OUT! Login as a domain user **may fail**, if pam_mount
    is unable to properly mount the users home drive to
    /home/adUserName (accepts password and then kicks you out the the
    graphical session, back to the graphical login screen again)

    Make sure at /home is no existing directory with the same name
    (local linux user). If you need local linux users AND AD users
    which share the same login names, you may want to have domain
    users home mounted somewhere else, like
    /home/adDomainName/adLoginname instead.

-->

<!--##### Mount further network shares ##### -->

<volume
fstype="cifs"
server="yourFileServer.AdDomainName.uni-freiburg.de"
path="someNetworkShare"
mountpoint="/someLocalMountpoint"
options="sec=ntlmv2,workgroup=YOUR_AD_NETBIOS_NAME" />

<volume
fstype="cifs"
server="yourFileServer.AdDomainName.uni-freiburg.de"
path="someNetworkShare"
mountpoint="/someLocalMountpoint"
options="sec=ntlmv2,workgroup=YOUR_AD_NETBIOS_NAME" />

<volume
fstype="cifs"
server="yourFileServer.AdDomainName.uni-freiburg.de"
path="someNetworkShare"
mountpoint="/someLocalMountpoint"
options="sec=ntlmv2,workgroup=YOUR_AD_NETBIOS_NAME" />

</pam_mount>
```

15. At last we want to disable the user listing at the graphical login (gdm3), so the users are always required to manually enter their adLoginName :

</etc/gdm3/greeter.dconf-defaults>


```
.  
.   
.   
# uncomment the following two lines within your default file:  
[org/gnome/login-screen]  
disable-user-list=true  
.   
.   
.
```

16. Reboot the system and try the graphical login as a domain user, using the plain username (no domain prefix required). Example AD Login: **werner** , Password: **whatever** . Expected result: Graphical Ubuntu desktop should appear. With your graphical file manager or via Terminal you should be able to find your network home directory and all the additional mounted network shares.
17. If you want to run some sort of Linux login script for each and every user at your workstation, you can add it to the users `~/.bashrc` file, or put it into `/etc/profile` or `/etc/bash.bashrc` to have it available system wide.

Found a bug, error, mistake or have recommendations to improve this documentaton?

Please let me know and send in reports, comments etc by email!! Im happy to learn and improve on it and make it even better and more reliable.

— [Axel Werner](#) 2019-01-05 12:05

[linux](#), [ad](#), [activeDirectory](#), [ubuntu](#), [18.10](#), [18.06](#), [samba](#), [kerberos](#), [cifs](#), [smb](#), [active](#), [directory](#), [smb](#)
[mount](#)

From:
<https://awerner.myhome-server.de/> - Axel Werner's OPEN SOURCE Knowledge Base

Permanent link:
<https://awerner.myhome-server.de/doku.php?id=it-artikel:linux:how-to-join-or-connect-ubuntu-desktop-18.10-workstation-to-an-active-directory-ad-domain-including-automatic-mounting-of-cifs-smb-shares-and-home-directory>

Last update: 2022-08-31 12:30

