Authentication of client Ubuntu20 on ActiveDirectory of a nethServer7

Difficulté
Moyen

This works for a real machine and for a VM.
It seems not to work for an **unprivileged** container!! (no login possible)
⇒ Must be tested for a privileged container.

Main source:
https://community.nethserver.org/t/howto-for-neth-7-as-ad-pdc-and-file-server-with-ubuntu-and-windows-clients/8685

Assuming that the ActiveDirectory of the NethServer is running properly:

- domain:“domain.tld”
- domain for the ActiveDirectory: “ad.domain.tld” (must be configured into the DNS resolver of the domain)
- server for the ActriveDirectory of the NethServer: “host.ad.domain.tld”

Packages:

Install following packages on Ubuntu:

```
# apt-get install realmd ntp adcli sssd libsss-sudo libpam-mount cifs-utils
samba-common smbclient krb5-user sssd-tools packagekit
```

```
Default Kerberos version 5 realm: => AD.DOMAIN.TLD
Kerberos servers for your realm: => host.ad.domain.tld
Administrative server for your Kerberos realm: => host.ad.domain.tld
```

Kerberos

- discover the ad domain:

```
# realm discover host.ad.domain.tld
ad.domain.tld
  type: kerberos
  realm-name: AD.DOMAIN.TLD
  domain-name: ad.domain.tld
  configured: no
  server-software: active-directory
  client-software: sssd
  required-package: sssd-tools
  required-package: sssd
```

```
  required-package: libnss-sss
  required-package: libpam-sss
  required-package: adcli
  required-package: samba-common-bin
```

- join the domain

```
# realm -v join -U administrator host.ad.domain.tld   #### and
enter the password of "admin" of the NethServer
```

- check

```
# realm list
ad.domain.tld
  type: kerberos
  realm-name: AD.DOMAIN.TLD
  domain-name: ad.domain.tld
  configured: kerberos-member
  server-software: active-directory
  client-software: sssd
  required-package: sssd-tools
  required-package: sssd
  required-package: libnss-sss
  required-package: libpam-sss
  required-package: adcli
  required-package: samba-common-bin
  login-formats: %U@ad.domain.tld
  login-policy: allow-realm-logins
```

sssd

Modidy the conf file of sssd:

```
# nano /etc/sssd/sssd.conf
and modify following:
"default_shell" => "override_shell"
"fallback_homedir = /home/%u@%d" => "override_homedir = /home/%u"
"use_fully_qualified_names = True" => "use_fully_qualified_names = False"
add at the end: "access_provider = permit"
```

```
# systemctl restart sssd
# systemctl status sssd
followinf message seem to be "normal":
tkey query failed: GSSAPI error: Major = Unspecified GSS failure.  Minor
code may provide more information, Minor = Server not found in Kerberos
database.
```

```
# systemctl enable sssd
```

/home

For the create of the /home folder:

```
# pam-auth-update --enable mkhomedir
```

lightdm

With greeter “lightdm” (e.g. for Xubuntu) ⇒ nothing to do. The login via GUI works.

Fine tuning: create /etc/lightdm/lightdm.conf.d/00-hide-user-list.conf and insert:

```
[SeatDefaults]
greeter-hide-users=true
greeter-show-manual-login=true
allow-guest=false
```

pam_mount

Auto mount of distant folders:

- install

  ```
  # apt-get install nfs-common
  ```

  if access of nfs-shares is needed.

- Add following into /etc/security/pam_mount.conf.xml after `<!– Volume definitions –>`. Don't forget to adjust `<mntoptions>` at the end of the file.
  - for a samba shared folder:

    ```
    <volume          fstype="cifs"
                     server="samba-host.domain.tld"
                     path="the_share"
                     mountpoint="/media/samba-host/shared_folder1"
                     user="*"
                     options="rw,auto,iocharset=utf8" />
    ```

  - for the home-folder:

    ```
    <volume          fstype="cifs"
                     server="samba-host.domain.tld"
    ```

```
                path="%(DOMAIN_USER)"
                mountpoint="/media/samba-host/home_%(DOMAIN_USER)"
                user="*"
                options="rw,auto,iocharset=utf8" />
```

- for a nfs share:

```
<volume         fstype="nfs"
                server="nfs-host.domain.tld"
                path="/the/path/of/the/shared/folder"
                mountpoint="/media/nfs-host/nfs_shared_folder1"
                user="*"
                options="rw" />
```

- for the auto creation of the mount points: add at the end:

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

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

Despite this `media/samba-host` and `/media/nfs-host` must be created by hand and get `chmod 777`

Unmount by logout

LXDE

The logout doesn't unmout the shares automatically mounted at login ⇒ the next user can access them inspite he doesn't have the needed permissions.
In order to avoid this:

- add at the end of `/etc/lxdm/lxdm.conf`

```
session-cleanup-script = /etc/lxdm/post-session.sh
```

- create `/etc/lxdm/post-session.sh` and insert in it:

```
#!/bin/bash
umount /media/samba-host/*
exit 0
```

- give the needed permissions:

```
sudo chmod 774 /etc/lxdm/post-session.sh
```

```
sudo chown root:root /etc/lxdm/post-session.sh
```

Forr Xubuntu (XFCE): enter “lightdm” instead of “lxdm” for all commands and parameters

Gnome

```
# nano /etc/gdm/PostSession/Default     ### and add into it:
umount /media/samba-host/*
```