Ubuntu 20.04 and Samba integration with Active Directory using SSSD

Join Ubuntu to Active Directory

```
# install required applications
su@fs:~$ sudo apt -y install realmd sssd sssd-tools libnss-sss libpam-sss
adcli samba-common-bin oddjob oddjob-mkhomedir packagekit

# configure network to use ADDC as DNS server, and to use the FQDN as
default search name
su@fs:~$ sudo vim /etc/netplan/00-installer-config.yaml
network:
  ethernets:
    eth0:
      addresses:
      - 192.168.2.251/24
      gateway4: 192.168.2.1
      nameservers:
        addresses:
        - 192.168.2.2
        search:
        - example.com
  version: 2

# apply the configuration
su@fs:~$ sudo netplan apply

# test if you can discover the domain
su@fs:~$ realm discover example.com
example.com
type: kerberos
realm-name: EXAMPLE.COM
domain-name: example.com
configured: no
...

# join the domain
su@fs:~$ realm join -U administrator example.com
Password for administrator:

# test if you can query the domain
su@fs:~$ id user@example.com
uid=687821651(user@example.com) gid=687800512(user@example.com)
groups=687800512(domain users@example.com)

# additional configuration
```

```
su@fs:~$ sudo vim /etc/sssd/sssd.conf
# set use_fully_qualified_names to false id you want to login using username
only - otherwise you must use user@example.com
# modify fallback_homedir to change user home folder - I prefer /home/%d/%u

# enable auto create of home folders
su@fs:~$ sudo pam-auth-update --enable mkhomedir

# add users to sudo group
su@fs:~$ sudo usermod -aG sudo user@example.com
# or add a domain group to sudoers
su@fs:~$ visudo
# append the line (with the desired group name
%Domain\ admins  ALL=(ALL:ALL) ALL

# login with user
su@fs:~$ su - user@example.com
Creating directory '/home/example.com/user'.
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

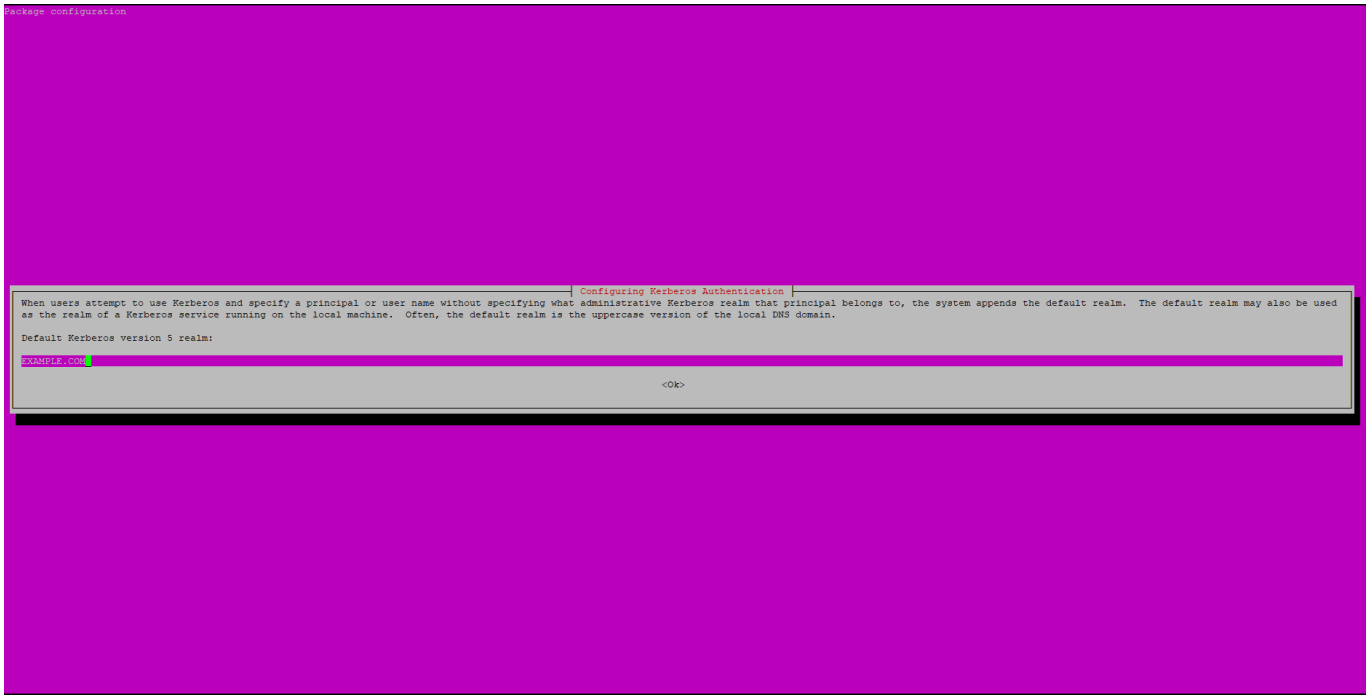
user@example.com@fs:~$ exit
logout
su@fs:~$

# additionally, you can allow only certain users to login
su@fs:~$ sudo realm deny –all
su@fs:~$ sudo realm permit user@example.com user2@example.com
su@fs:~$ sudo realm permit -g 'Domain Admins'
```

Kerberos

If you install krb5-user, your AD users will also get a kerberos ticket upon logging in

```
su@fs:~$ sudo apt install krb5-user
```




```
su@fs:~$ su -l user@example.com
Password:
user@example.com@fs:~$ klist
Ticket cache: FILE:/tmp/krb5cc_1945601295_0twWui
Default principal: user@EXAMPLE.COM

Valid starting       Expires              Service principal
03/29/2021 08:57:32  03/29/2021 18:57:32  krbtgt/EXAMPLE.COM@EXAMPLE.COM
        renew until 03/30/2021 08:57:32
user@example.com@fs:~$ sudo apt install smbclient
user@example.com@fs:~$ smbclient -k -L dc.example.com

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        CertEnroll      Disk      Active Directory Certificate Services
share
        ContentBuilderSCUM Disk
        D$              Disk      Default share
        E$              Disk      Default share
        IPC$            IPC       Remote IPC
        NETLOGON        Disk      Logon server share
        Share           Disk
        ShareSSD        Disk
        SYSVOL          Disk      Logon server share
SMB1 disabled -- no workgroup available
user@example.com@fs:~$  klist
Ticket cache: FILE:/tmp/krb5cc_1945601295_0twWui
Default principal: tplecko-adm@GAMEPIRES.COM

Valid starting       Expires              Service principal
```

```
03/29/2021 08:59:11  03/29/2021 18:59:11  krbtgt/EXAMPLE.COM@EXAMPLE.COM
        renew until 03/30/2021 08:59:11
03/29/2021 08:59:40  03/29/2021 18:59:11  cifs/dc.example.com@EXAMPLE.COM
user@example.com@fs:~$
```

SAMBA integration

This part needs review since it is broken in the fresh versions

```
su@fs:~$ sudo apt install samba cifs-utils libwbclient-sssd
su@fs:~$ sudo vim /etc/samba/smb.conf
[global]
   workgroup = EXAMPLE
   realm = EXAMPLE.COM
   server string = %h server
   #idmap backend = lwopen
   idmap config * : backend = tdb
   idmap config * : range = 10000-199999
   idmap config EXAMPLE : backend = sss
   idmap config EXAMPLE : range = 1000000-19999999
   idmap config EXAMPLE : rangesize = 1000000
   passdb backend = tdbsam
   kerberos method = system keytab
   #secrets
   #secrets and keytab
   dedicated keytab file = /etc/krb5.keytab
   security = ads
   log file = /var/log/samba/log.%m
   max log size = 1000
   logging = file
   panic action = /usr/share/samba/panic-action %d
   server role = member server
   #standalone
   obey pam restrictions = yes
   unix password sync = yes
   passwd program = /usr/bin/passwd %u
   passwd chat = *Enter\snew\s*\spassword:* %n\n *Retype\snew\s*\spassword:*
%n\n *password\supdated\ssuccessfully* .
   pam password change = yes
   map to guest = bad user
   usershare allow guests = yes
   max protocol = SMB3
   min protocol = NT1
[public]
        comment = Public share
        path = /shared/public
        read only = no
        guest ok = no
        browsable = yes
```

```
        writable = yes
        #admin users =
        valid users = Domain\ users\@example.com
        #invalid users =
        #read list =
        write list = Domain\ users\@example.com
        create mask = 0770
        directory mask = 0770
        force create mode = 0770
        force directory mode = 0770


#get your domain SID from powershell with get-addomain example.com
su@fs:~$ sudo net setdomainsid S-1-5-21-111111111-2222222222-33333333
su@fs:~$ sudo systemctl restart smbd nmbd
```

From:
https://wiki.plecko.hr/ - **Eureka Moment**

Permanent link:
https://wiki.plecko.hr/doku.php?id=linux:ad_integration:sssd&rev=1617019889

Last update: **2021/03/29 14:11**