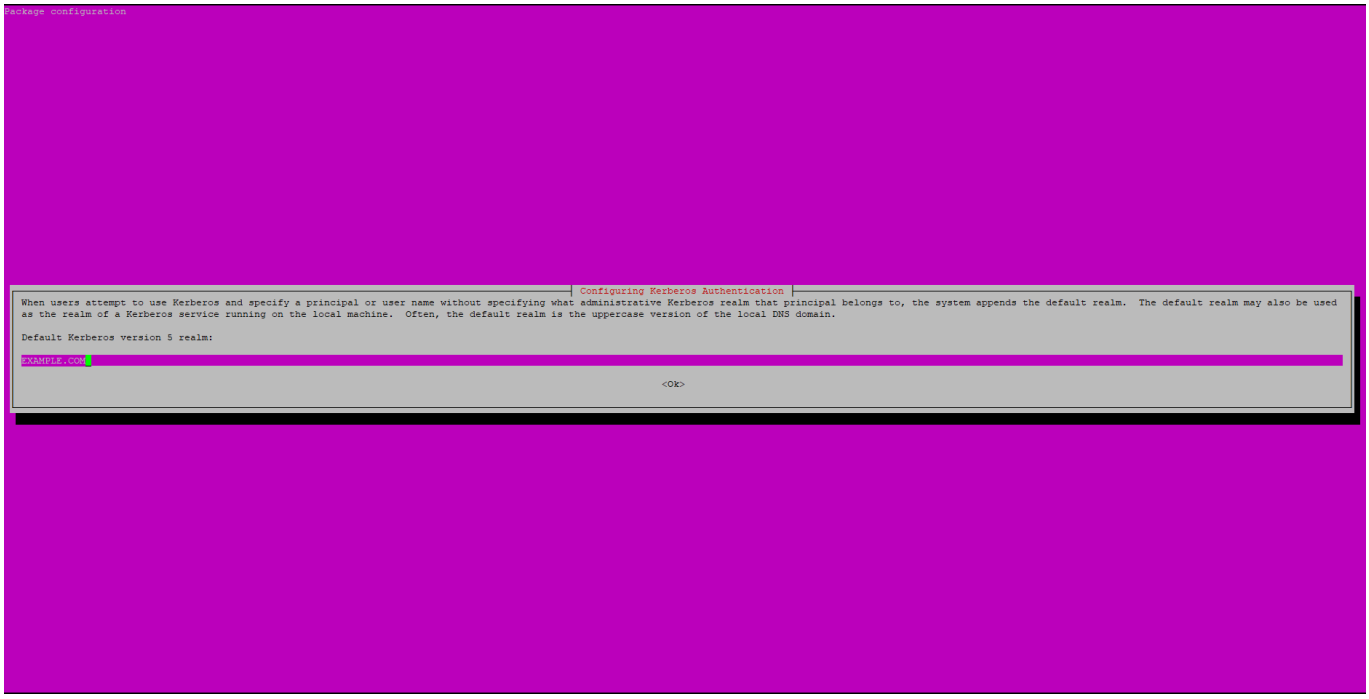
Ubuntu 20.04 and Samba integration with Active Directory using Winbind

Install required programs

```
su@fs:~$ sudo apt -y install winbind libpam-winbind libnss-winbind krb5-config samba-dsdb-modules samba-vfs-modules
```



Configure everything

```
su@fs:~$ sudo vim /etc/samba/smb.conf
   workgroup = EXAMPLE
   realm = EXAMPLE.COM
   security = ads
   idmap config * : backend = tdb
   idmap config * : range = 3000-7999
   idmap config EXAMPLE : backend = rid
   idmap config EXAMPLE : range = 10000-999999
   template homedir = /home/%U
   template shell = /bin/bash
   winbind use default domain = true
   winbind offline logon = false

su@fs:~$ sudo vim /etc/nsswitch.conf
passwd:         files systemd winbind
group:          files systemd winbind
```

```
su@fs:~$ sudo vim /etc/pam.d/common-session
# add to the end if you need (auto create a home directory at initial login)
session optional        pam_mkhomedir.so skel=/etc/skel umask=077

# change DNS setting to refer to AD
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
```

Join Ubuntu to Active Directory

```
# join in domain ( net ads join -U [AD's Administrative user])
su@fs:~$ sudo net ads join -U Administrator
Enter Administrators password:
Using short domain name -- EXAMPLE
Joined 'SMB' to dns domain 'example.com'
su@fs:~$ sudo systemctl restart winbind
# show domain info
su@fs:~$ sudo net ads info
LDAP server: 192.168.2.2
LDAP server name: dc.example.com
Realm: EXAMPLE.COM
Bind Path: dc=EXAMPLE,dc=COM
LDAP port: 389
Server time: Mon, 29 Mar 2021 13:30:41 UTC
KDC server: 192.168.2.2
Server time offset: -116
Last machine account password change: Mon, 29 Mar 2021 11:28:46 UTC

# show AD user list
su@fs:~$ sudo wbinfo -u
administrator
guest
krbtgt
user
```

```
mssql
ldapusers

# verify to login with an AD user
su@fs:~$ su -l user@example.com
Password:
Welcome to Ubuntu 20.04 LTS (GNU/Linux 5.4.0-26-generic x86_64)

.....
.....

Creating directory '/home/user'.
user@fs:~$ id
uid=11295(user) gid=10513(domain users) groups=10513(domain
users),3000(BUILTIN\administrators),3001(BUILTIN\users),10512(domain
admins),10518(schema admins),10519(enterprise admins),10572(denied rodc
password replication group),11028(dhcp
administrators),11130(dnsadmins),11295(user)

user@fs:~$ exit

# 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
```

SAMBA integration

```
su@fs:~$ sudo apt install samba
su@fs:~$ vim /etc/samba/smb.conf
[global]
   workgroup = EXAMPLE
        realm = EXAMPLE.COM
        security = ads
        idmap config * : backend = tdb
        idmap config * : range = 3000-7999
        idmap config EXAMPLE : backend = rid
        idmap config EXAMPLE : range = 10000-999999
        template homedir = /home/%U
        template shell = /bin/bash
        winbind use default domain = true
        winbind offline logon = false
        winbind refresh tickets = yes
   server string = %h server (Samba, Ubuntu)
   log file = /var/log/samba/log.%m
   max log size = 1000
   logging = file
```

```
   panic action = /usr/share/samba/panic-action %d
   server role = standalone server
#   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
[public]
        comment = Public share
        path = /shared/public
        read only = no
        guest ok = no
        browsable = yes
        writable = yes
        #admin users =
        valid users = @"EXAMPLE\Domain users"
        #invalid users =
        #read list =
        write list = @"EXAMPLE\Domain users"

        create mask = 0770
        force create mode = 0770

        security mask = 0770
        force security mask = 0770

        directory mask = 0770
        force directory mode = 0770

        directory security mask = 0770
        force directory security mode = 0770

        inherit acls = no
```

Also, make sure to mount the volume holding the shares with **noacl** in fstab, and do not set **obey pam restrictions = yes**, else security, create and directory mode directives are ignored