Mise en place de Samba sur Debian avec les users d'AD pour s'authentifier

I – Configuration de la machine virtuelle Debian 10 pour joindre à un domaine Active Directory.

Les exigences pour ce projet : avoir une machine Debian ou Ubuntu, **un contrôleur de domaine Windows serveur prêts à fonctionner** et des machines Windows 10 client qui sont joint au domaine. Et bien sûr, **les machines doivent pouvoir se communiquer entre-elles,** donc elles se trouvent dans le même réseau ou dans des sous-réseaux différents avec le routage approprié en place.

La première chose que nous ferons est de définir une adresse IP statique sur notre machine virtuelle Debian. On tapera la commande IP -c link show pour savoir le nom de notre interface.

```
util@debian:~$ ip -c link show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT group default qlen
1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP mode DEFAULT group d
efault qlen 1000
    link/ether 08:00:27:6b:69:cb brd ff:ff:ff:ff:ff:ff
```

Ignorez l'interface lo, nous n'avons pas besoin. Ce qu'on utilisera est l'interface 2.

L'étape suivante consiste à ouvrir le fichier d'interfaces et à définir l'adresse IP de l'interface. « sudo nano /etc/network/interfaces » et « sudo /etc/init.d/networking restart » pour actualiser.

```
  GNU nano 3.2                          /etc/network/interfaces

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug enp0s3
iface enp0s3 inet static
address 192.168.1.100
netmask 255.255.255.0
gateway 192.168.1.254
dns-domain apes.local
dns-nameservers 192.168.1.10
util@debian:~$ sudo /etc/init.d/networking restart
[ ok ] Restarting networking (via systemctl): networking.service.
```

Nous allons maintenant mettre à jour notre serveur Debian, « sudo apt -y update && sudo apt -y upgrade »

```
util@debian:~$ sudo apt -y update && sudo apt -y upgrade
Atteint :1 http://security.debian.org/debian-security buster/updates InReleas
Atteint :2 http://deb.debian.org/debian buster InRelease
Atteint :3 http://deb.debian.org/debian buster-updates InRelease
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances
Lecture des informations d'état... Fait
Tous les paquets sont à jour.
```

La prochaine étape consiste à installer SSH, il sera utilisé pour communiquer avec notre contrôleur de domaine. Tapez simplement « sudo apt -y install ssh »

```
util@debian:~$ sudo apt -y install ssh
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances
Lecture des informations d'état... Fait
Les NOUVEAUX paquets suivants seront installés :
  ssh
```

Maintenant que c'est fait, notre allons maintenant configurer le fichier resolve.conf de la VM Debian pour qu'il puisse utiliser le contrôleur de domaine en tant que serveur DNS.

```
util@debian:~$ sudo rm /etc/resolv.conf
util@debian:~$ sudo nano /etc/resolv.conf
```

```
  GNU nano 3.2                                /etc/resolv.conf

nameserver 192.168.1.10
search apes.local
```

Le fichier resolve.conf est géré par le système donc il est possible qu'il revienne au serveur DNS par défaut à chaque redémarrage de la machine. Pour résoudre ce problème, nous allons supprimer le fichier et on créera notre propre resolve.conf avec notre serveur à nous.

Nous limiterons ensuite l'accès à ce fichier pour être sûr.

```
util@debian:~$ sudo chattr +i /etc/resolv.conf
```

Modifions maintenant également le fichier hosts avec la commande « sudo nano etc/hosts ».

```
  GNU nano 3.2                                  /etc/hosts

127.0.0.1       localhost
192.168.1.10    debian debian.apes.local

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

Nous allons utiliser un autre service donc pour éviter d'autres problèmes, on supprimera avahi-daemon.

```
util@debian:~$ sudo apt -y remove avahi-daemon
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances
Lecture des informations d'état... Fait
Le paquet « avahi-daemon » n'est pas installé, et ne peut donc être supprimé
0 mis à jour, 0 nouvellement installés, 0 à enlever et 0 non mis à jour.
```

On installera le service en tapant « wget rebrand.ly/adjoiin -O adjoin.sh ».

```
util@debian:~$ wget rebrand.ly/adjoin -O adjoin.sh
--2022-04-16 19:17:20--  http://rebrand.ly/adjoin
Résolution de rebrand.ly (rebrand.ly)… 52.44.44.79, 52.206.137.117
Connexion à rebrand.ly (rebrand.ly)|52.44.44.79|:80… connecté.
requête HTTP transmise, en attente de la réponse… 301 Moved Permanently
Emplacement : https://github.com/BeyondTrust/pbis-open/releases/download/9.1.
```

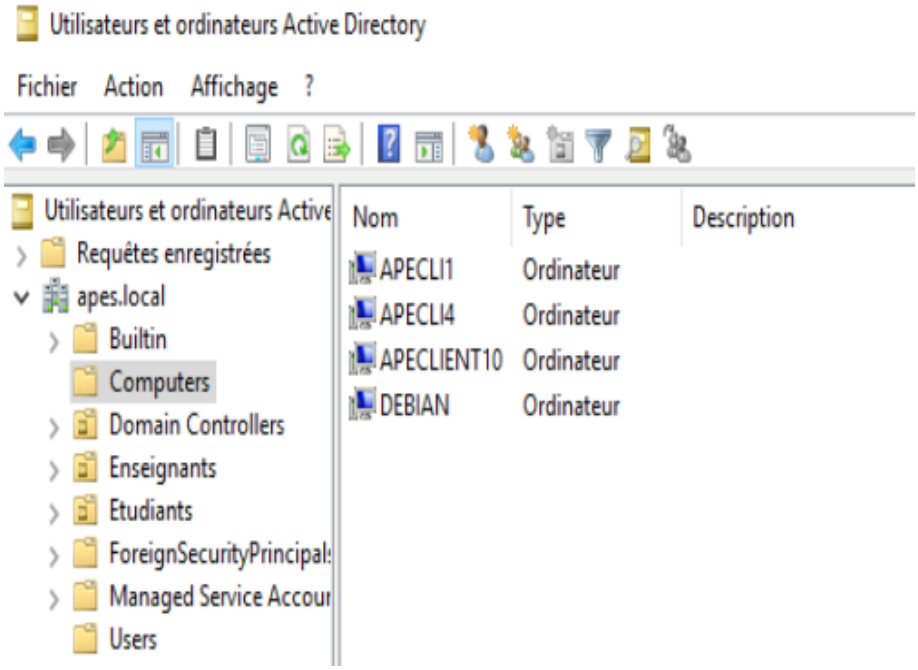
Pour pouvoir l'executer, on tapera la commande « sudo chmod +x adjoin.sh ». Et on lancera avec la commande « sudo ./adjoin.sh »

```
util@debian:~$ sudo chmod +x adjoin.sh
util@debian:~$ sudo ./adjoin.sh
Creating directory pbis-open-9.1.0.551.linux.x86_64.deb
Verifying archive integrity... All good.
Uncompressing pbis-open-9.1.0.551.linux.x86_64.deb.........
Installing packages and old packages will be removed
Sélection du paquet pbis-open-upgrade précédemment désélectionné.
```

Rejoignons maintenant le domaine en tapant simplement « sudo domainjoin-cli join APES.LOCAL ». Si vous avez un message d'erreur concernant le « clock screw », vérifiez que vous avez bien configuré le temps dans les 2 machines.

```
util@debian:~$ date
samedi 16 avril 2022, 19:23:26 (UTC+0200)
util@debian:~$ sudo domainjoin-cli join APES.LOCAL
Username: Administrateur
Joining to AD Domain:   APES.LOCAL
With Computer DNS Name: debian.apes.local

Administrateur@APES.LOCAL's password:
Warning: System restart required
Your system has been configured to authenticate to Active Directory for the first time.  It is
recommended that you restart your system to ensure that all applications recognize the new settings.

SUCCESS
util@debian:~$
```

On peut voir que la machine virtuelle Debian a été joint au domaine.



II – Installation et configuration de Samba pour pouvoir utiliser les users d'Active Directory.

Donc, on installera tous les paquets nécessaires pour le bon fonctionnement de Samba « sudo apt install ntp krb-user samba cifs-utils smbclient winbind libnss-winbind libpam-winbind ». On tapera « Non » pour le WIN DHCP.

Ensuite, on configura le fichier conf de krb5-user « sudo nano /etc/krb5.conf ». Mettez bien l'adresse IP et le nom votre domaine.

```
[libdefaults]
  ticket_lifetime = 24h
  default_realm = APES.LOCAL
  forwardable = true

[realms]
  APES.LOCAL = {
    kdc = 192.168.1.10
    default_domain = APES.LOCAL
  }

[domain_realm]
  .apes.local = APES.LOCAL
  apes.local = APES.LOCAL

[kdc]
  profile = /etc/krb5kdc/kdc.conf

[appdefaults]
  pam = {
    debug = false
    ticket_lifetime = 36000
    renew_lifetime = 36000
    forwardable = true
    krb4_convert = false
  }

[logging]
  kdc = FILE:/var/log/krb5kdc.log
  admin_server = FILE:/var/log/kadmin.log
  default = FILE:/var/log/krb5lib.log
```

Pour vérifier que le fichier de conf est bien correct, tapez la commande « kinit Administrateur » et « klist ».

```
util@debian:~$ sudo nano /etc/krb5.conf
util@debian:~$ kinit Administrateur
Password for Administrateur@APES.LOCAL:
util@debian:~$ klist
Ticket cache: FILE:/tmp/krb5cc_1000
Default principal: Administrateur@APES.LOCAL

Valid starting       Expires              Service principal
16/04/2022 20:00:12  17/04/2022 06:00:12  krbtgt/APES.LOCAL@APES.LOCAL
        renew until 17/04/2022 20:00:09
util@debian:~$
```

On modifiera également le /etc/nsswitch.conf et /etc/samba/smb.conf pour qu'ils puissent utiliser winbind.

```
 GNU nano 3.2                                  /etc/nsswitch.conf

# /etc/nsswitch.conf
#
# Example configuration of GNU Name Service Switch functionality.
# If you have the `glibc-doc-reference' and `info' packages installed, try:
# `info libc "Name Service Switch"' for information about this file.

passwd:         compat winbind
group:          compat winbind
shadow:         compat winbind
gshadow:        files

hosts:          files dns
networks:       files

protocols:      db files
services:       db files
ethers:         db files
rpc:            db files

netgroup:       nis
```

```
[global]
# No .tld
workgroup = APES
# Active Directory System
security = ads
# With .tld
realm = APES.LOCAL
# Just a member server
domain master = no
local master = no
preferred master = no
# Disable printing error log messages when CUPS is not installed.
printcap name = /etc/printcap
load printers = no
# Works both in samba 3.2 and 3.6.
idmap backend = tdb
idmap uid = 10000-99999
idmap gid = 10000-99999
# no .tld
idmap config EXAMPLE:backend = rid
idmap config EXAMPLE:range = 10000-99999
winbind enum users = yes
winbind enum groups = yes
# This way users log in with username instead of username@example.com
winbind use default domain = yes
# Inherit groups in groups
winbind nested groups = yes
winbind refresh tickets = yes
winbind offline logon = true
# Becomes /home/example/username
template homedir = /home/%D/%U
# No shell access
template shell = /bin/false
client use spnego = yes
client ntlmv2 auth = yes
encrypt passwords = yes
restrict anonymous = 2
log file = /var/log/samba/samba.log
log level = 2
# Full audit
vfs object = full_audit
full_audit:prefix = %u|%I|%m|%S
full_audit:success = mkdir rmdir read pread write pwrite rename unlink
full_audit:failure = connect
full_audit:facility = local7
full_audit:priority = notice
```

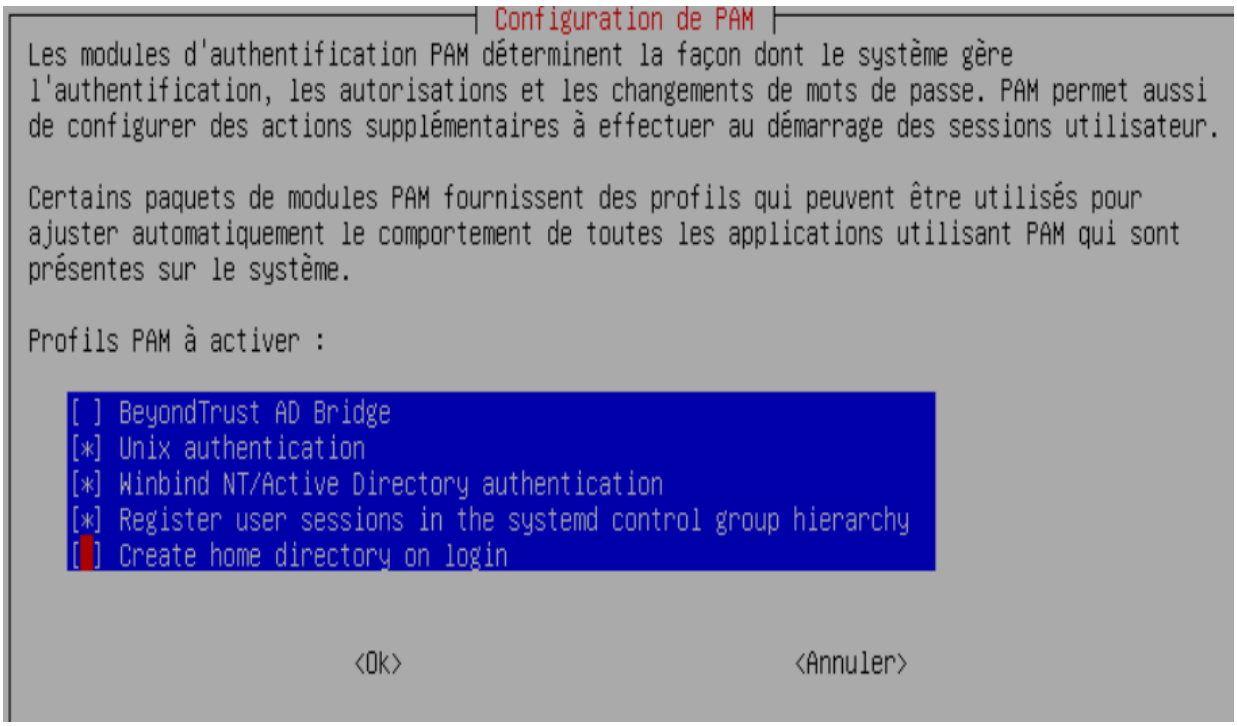
On redémarre les services en tapant “sudo systemctl restart smbd nmbd winbind”.

```
util@debian:~$ sudo nano /etc/samba/smb.conf
util@debian:~$ sudo systemctl restart smb nmbd winbind
```

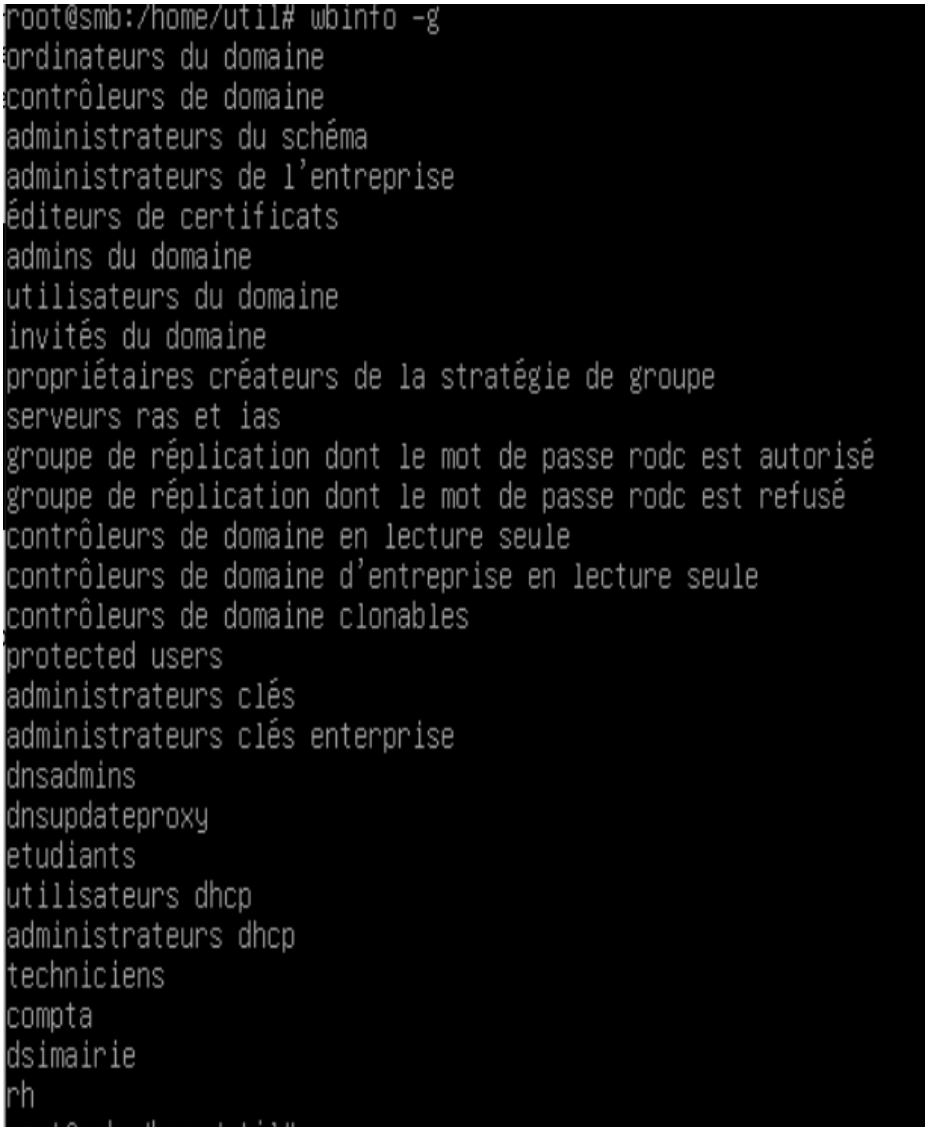
On synchronisera maintenant avec l’Active Directory en tapant « net ads join -U Administrateur ». Si vous avez des erreurs, essayez de taper la commande en tant que root ou vérifiez que le temps est bien configuré sur les deux machines. N’hésitez pas aussi de relancer la commande tout simplement.

```
root@smb:/home/util# net ads join -U Administrateur
Enter Administrateur's password:
Using short domain name -- APES
Joined 'SMB' to dns domain 'apes.local'
root@smb:/home/util# _
```

Ensuite, on tapera pam-auth-update ou /usr/sbin/pam-auth-update pour activer « Winbind/NT Active Directory authentification ». (espace = sélectionner | entrée = confirmer)



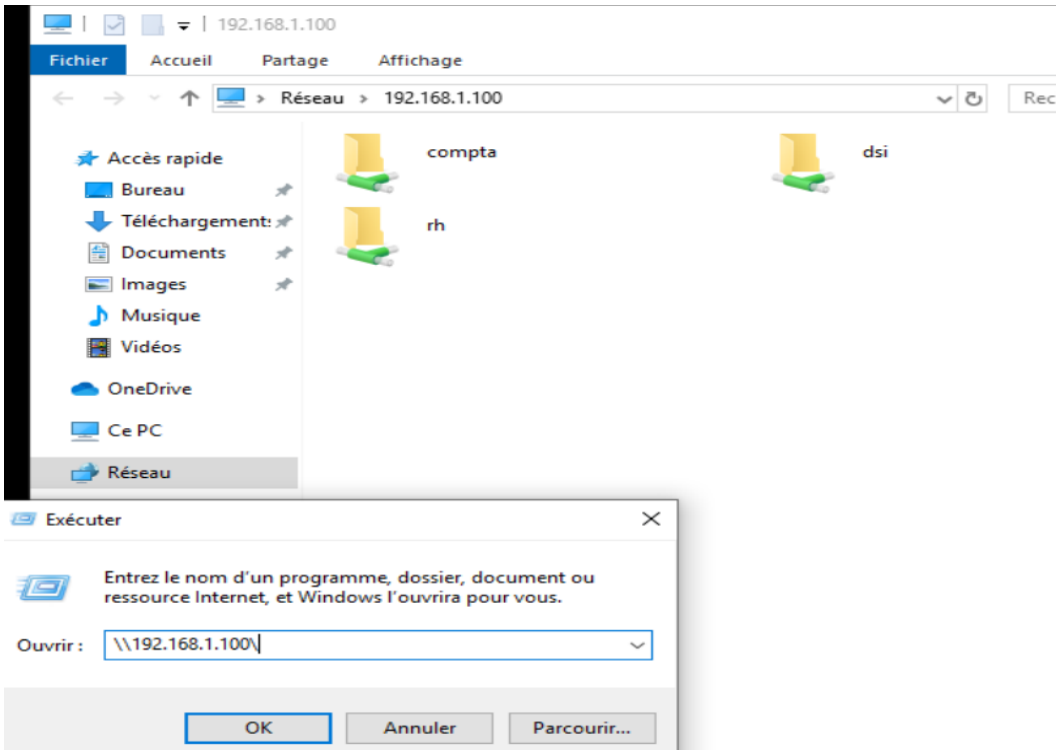
Enfin, pour voir si tout a été bien configuré, on tape wbinfo -u ou wbinfo -g, et on verra normalement tous les utilisateurs/groupes dans notre Active Directory !



Maintenant pour partager un dossier avec Samba et faire l'authentification avec les comptes de l'Active Directory, on mettra simplement « valid users = @APES\NomduGroupe », le même pour admin users. Pour sauver du temps et du code, j'ai décidé de mettre les utilisateurs dans un groupe. Le « path » doit bien exister donc pensez à créer d'abord les dossiers : mkdir et cetera…

```
[DSI]
comment = Le dossier de DSI
path = /shares/private
valid users = @APES\DSIMairie
admin users = @APES\DSIMairie
force group = "utilisateurs du domaine"
writable = yes
read only = no
force create mode = 0660
create mask = 0777
directory mask = 0777
force directory mode = 0770
access based share enum = yes
hide unreadable = yes
```

Pour vérifier si le dossier « DSI » est bien partagé, on ouvre une session avec un compte qui fait partie du groupe « DSIMairie » sur la machine Windows 10 client qui est joint au domaine. Pour savoir comment joindre une machine Windows 10 à un domaine, veuillez voir mon rapport sur Windows serveur ou cherchez sur Internet.



On activera la journalisation de Samba en ajoutant ces lignes dans « /etc/samba/smb.conf ».

```
[global]

    ... other stuff ...

    # Full audit
    vfs object = full_audit
    full_audit:prefix = %u|%I|%m|%S
    full_audit:success = mkdir rmdir read pread write pwrite rename unlink
    full_audit:failure = connect
    full_audit:facility = local7
    full_audit:priority = notice
```

On modifiera le fichier conf de rsyslog pour qu'il n'envoi pas les logs dans /var/log/syslog. Ensuite, on ajoutera ces lignes pour que les logs puissent se retrouver dans ce fichier « samba-audit.log »

```
# Change this line
*.*;auth,authpriv.none              -/var/log/syslog

# To
*.*;auth,authpriv.none,local7.none -/var/log/syslog
```

```
# Add this line
local7.notice                              /var/log/samba-audit.log
```

Pour compresser ou rotate les logs chaque semaine, ajoutez ces lignes dans /etc/logrotate.d/samba. Enfin, faites un « sudo systemctl restart rsyslog smbd ».

```
/var/log/samba-audit.log {
    weekly
    missingok
    rotate 7
    postrotate
        reload rsyslog > /dev/null 2>&1 || true
    endscript
    compress
    notifempty
}
```

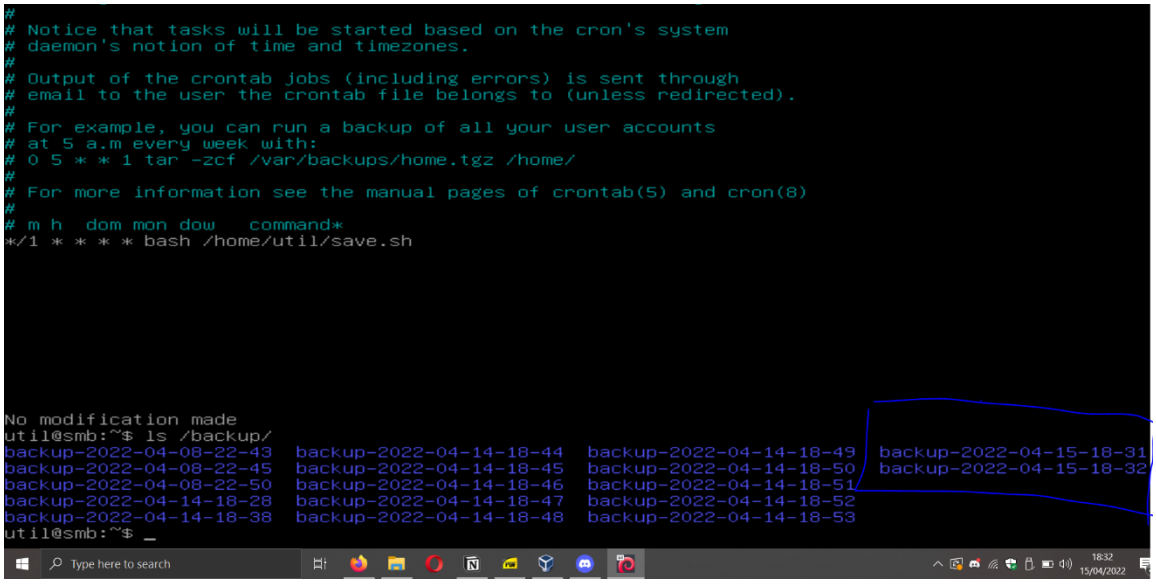
Il suffit de créer des dossiers, supprimer des fichiers dans les dossiers partagés pour voir si les logs de Samba sont bien activé.

```
util@smb:~$ sudo cat /var/log/samba-audit.log
Apr  8 22:24:15 smb smbd_audit: APES\muchiha|192.168.1.101|lamairiep01|DSI|unlink|ok|/shares/private/Nouveau document texte.tx
t
Apr  8 22:24:20 smb smbd_audit: APES\muchiha|192.168.1.101|lamairiep01|DSI|mkdir|ok|Nouveau dossier
Apr  8 22:25:36 smb smbd_audit: APES\muchiha|192.168.1.101|lamairiep01|DSI|rename|ok|/shares/private/Nouveau dossier|/shares/p
rivate/DSI_Ressources
Apr 14 15:45:19 smb smbd_audit: APES\sbelkhir|192.168.1.101|lamairiep01|COMPTA|mkdir|ok|Nouveau dossier
Apr 14 15:45:41 smb smbd_audit: APES\sbelkhir|192.168.1.101|lamairiep01|COMPTA|rename|ok|/shares/public/Nouveau dossier|/share
s/public/Ressources_Compta
Apr 14 15:51:18 smb smbd_audit: APES\muchiha|192.168.1.101|lamairiep01|COMPTA|rename|ok|/shares/public/Ressources_Compta|/shar
es/public/Compta_Ressources
Apr 14 17:58:52 smb smbd_audit: APES\muchiha|192.168.1.101|lamairiep01|DSI|rename|ok|/shares/private/Nouveau document texte.tx
t|/shares/private/@IPdetoutlesimprimantes.txt
Apr 14 17:59:48 smb smbd_audit: APES\muchiha|192.168.1.101|lamairiep01|DSI|rename|ok|/shares/private/Nouveau document texte.tx
t|/shares/private/test.txt.txt
Apr 14 18:21:59 smb smbd_audit: APES\muchiha|192.168.1.101|lamairiep01|DSI|unlink|ok|/shares/private/test.txt.txt
Apr 14 18:22:10 smb smbd_audit: APES\muchiha|192.168.1.101|lamairiep01|DSI|rename|ok|/shares/private/@IPdetoutlesimprimantes.t
xt|/shares/private/DSI_Ressources/@IPdetoutlesimprimantes.txt
Apr 14 18:26:56 smb smbd_audit: APES\muchiha|192.168.1.101|lamairiep01|DSI|rename|ok|/shares/private/Nouveau document texte.tx
t|/shares/private/delete.txt
Apr 14 18:26:58 smb smbd_audit: APES\muchiha|192.168.1.101|lamairiep01|DSI|unlink|ok|/shares/private/delete.txt
```

Pour finir, j'ai décidé de mettre en place un script de sauvegarde pour les dossiers partagés, le script s'exécutera chaque jour de manière automatique.

```
util@smb:~$ sudo cat save.sh
[sudo] Mot de passe de util :
#!/bin/bash

# date du jour + minute et seconde
backupdate=$(date +%Y-%m-%d-%H-%M)

#répertoire de backup
dirbackup=/backup/backup-$backupdate

# création du répertoire de backup
/bin/mkdir $dirbackup

# tar -cjf /destination/fichier.tar
# créé une archive tar
# sauvegarde de /home
/bin/tar -czvf $dirbackup/shares-$backupdate.tar.gz /shares
```

Ceci est un test pour voir si le crontab fonctionne correctement.



Documentation réalisée par Aaron PESCASIO.