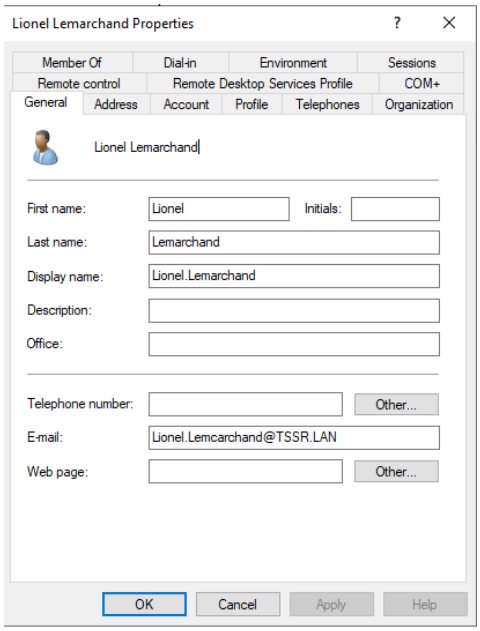
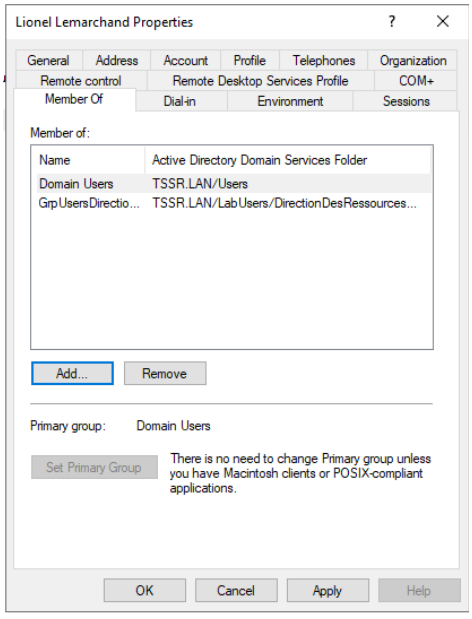
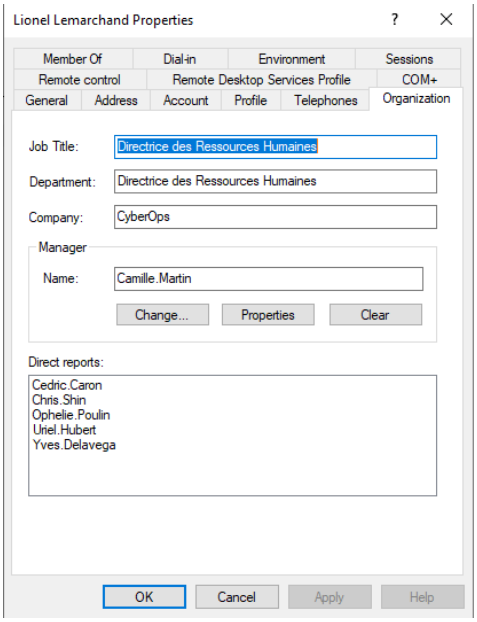
Exercice 1 - VM Windows

Partie 1 - Gestion des utilisateurs

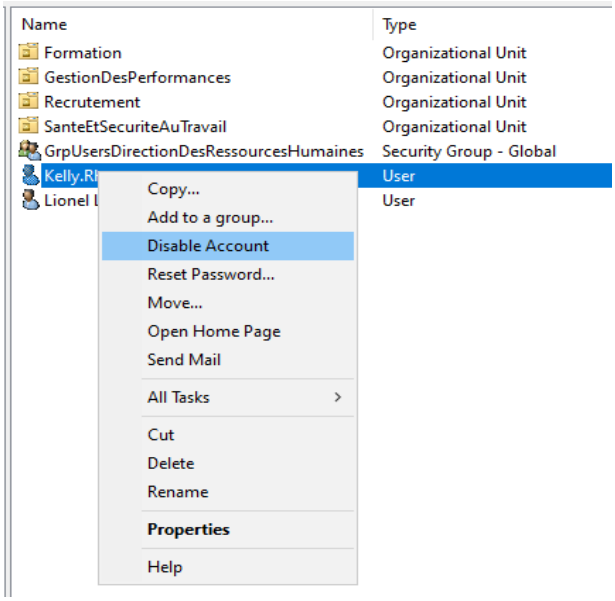
Q.1.1.1 Créer l'utilisateur Lionel Lemarchand avec les même attribut de société que Kelly Rhameur.

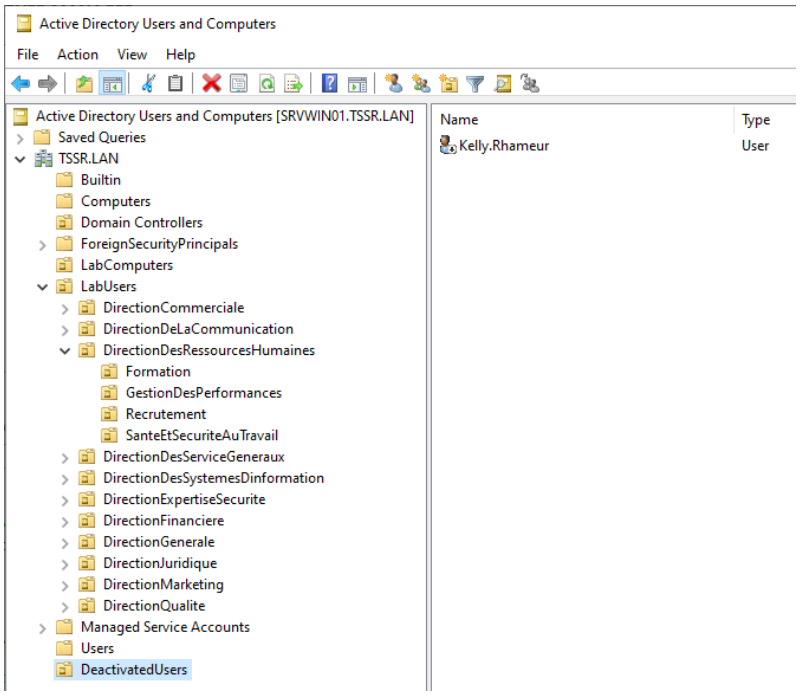




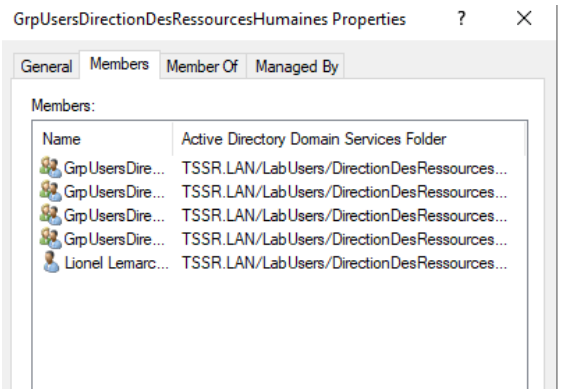


Q.1.1.2 Déplacement du compte désactivé de Kelly Rhameur

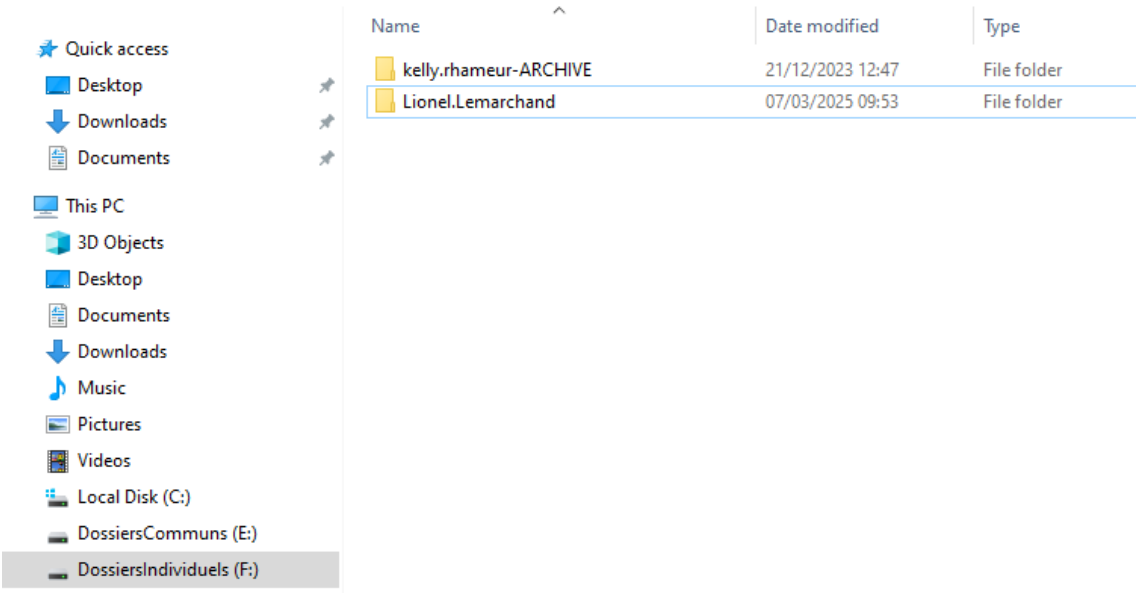




Q.1.1.3 Modifier le groupe de l'OU dans laquelle était Kelly Rhameur en conséquence.

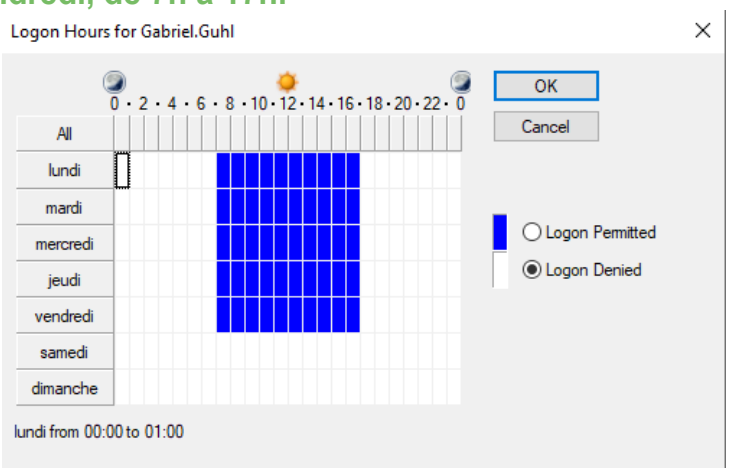


Q.1.1.4 Créer le dossier Individuel du nouvel utilisateur et archive celui de Kelly Rhameur en le suffixant par -ARCHIVE.

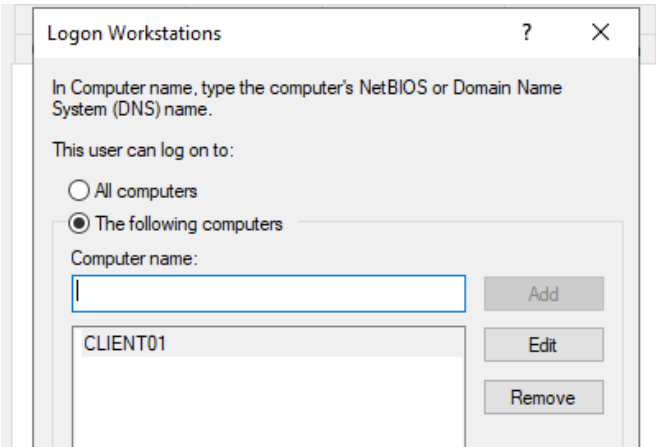


Partie 2 - Restriction utilisateurs

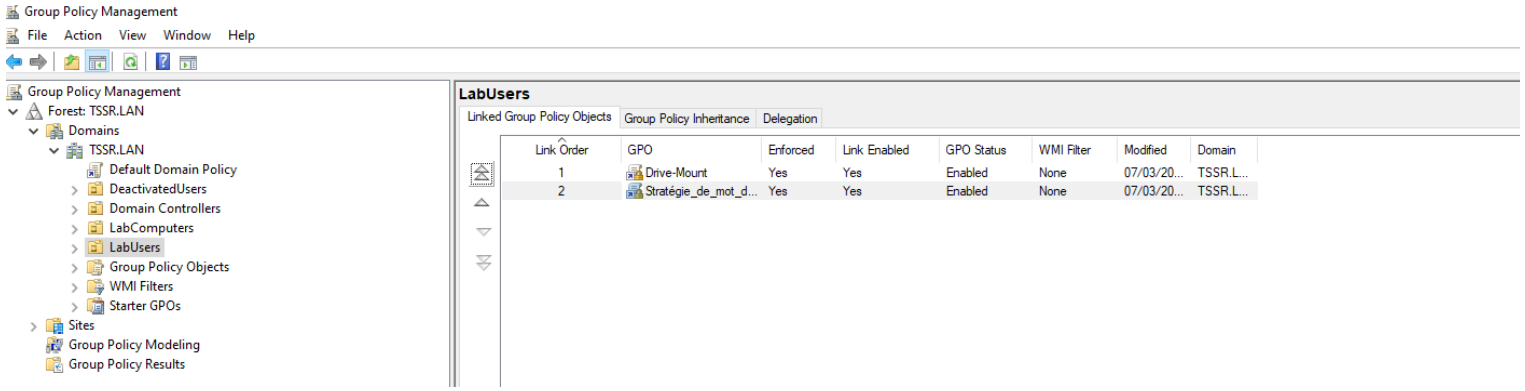
Q.1.2.1 Faire en sorte que l'utilisateur Gabriel Ghul ne puisse se connecter que du lundi au vendredi, de 7h à 17h.



Q.1.2.2 De même, bloquer sa connexion au seul ordinateur CLIENT01.

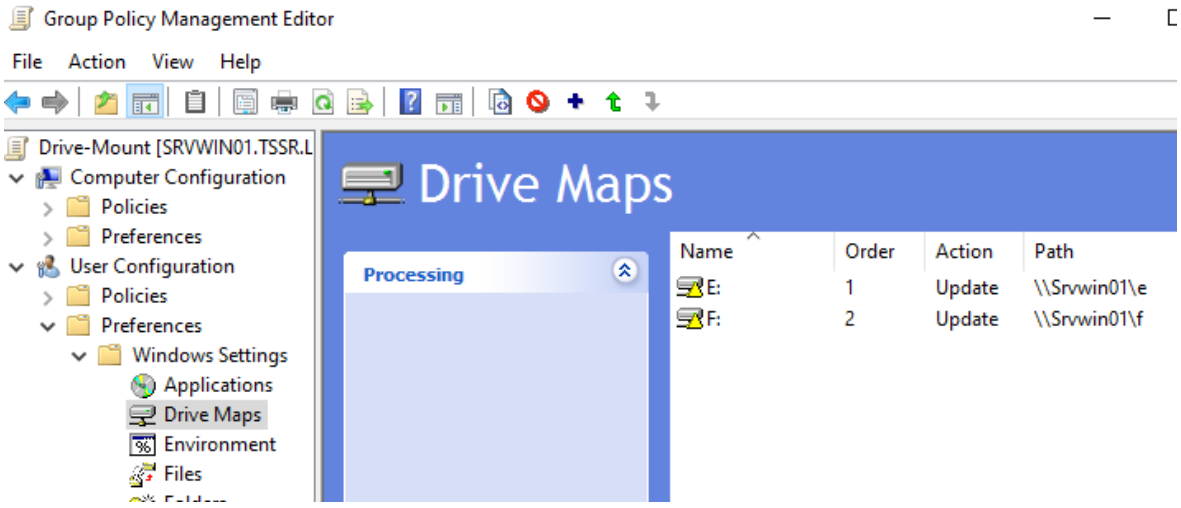


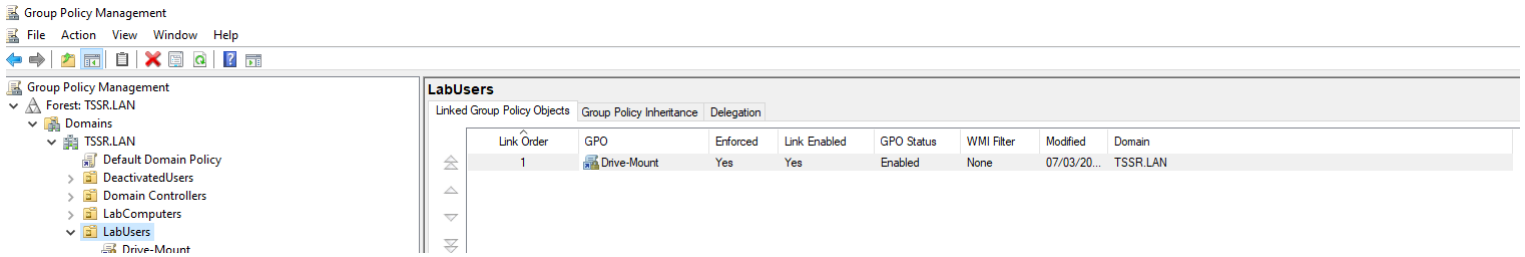
Q.1.2.3 Mettre en place une stratégie de mot de passe pour durcir les comptes des utilisateurs de l'OU LabUsers.



Partie 3 - Lecteurs réseaux

Q.1.3.1 Créer une GPO Drive-Mount qui monte les lecteurs E: et F: sur les clients.





Exercice 2 - VM Linux

Partie 1 - Gestion des utilisateurs

Q.2.1.1 Création d'un compte personnel sur le serveur Debian

```
wilder@SRVLX01:~$ su
Mot de passe :
root@SRVLX01:/home/wilder# sudo adduser ben
Ajout de l'utilisateur « ben » ...
Ajout du nouveau groupe « ben » (1001) ...
Ajout du nouvel utilisateur « ben » (1001) avec le groupe « ben » ...
Création du répertoire personnel « /home/ben »...
Copie des fichiers depuis « /etc/skel »...
Nouveau mot de passe :
Retapez le nouveau mot de passe :
passwd: password updated successfully
Changing the user information for ben
Enter the new value, or press ENTER for the default
        Full Name []: Ben
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Cette information est-elle correcte ? [O/n]o
root@SRVLX01:/home/wilder#
```

Q.2.1.2 Quelles préconisations proposes-tu concernant ce compte ?

Mettre un mot de passe fort , empêcher la connexion en ssh si le compte n'a pas besoin d'accès a distance,

Partie 2 - Configuration de SSH

Q.2.2.1 Désactiver complètement l'accès à distance de l'utilisateur root.

```
#LoginGraceTime 2m
PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
```

Q.2.2.2 Autoriser l'accès à distance à ton compte personnel uniquement.

```
 GNU nano 5.4                          /etc/ssh/sshd_config *

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
PermitRootLogin no
AllowUsers ben
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
```

Q.2.2.3 Mettre en place une authentification par clé valide et désactiver l'authentification par mot de passe

```
root@SRVLX01:/home/wilder# ssh-keygen -t ed25519
Generating public/private ed25519 key pair.
Enter file in which to save the key (/root/.ssh/id_ed25519):
Created directory '/root/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_ed25519
Your public key has been saved in /root/.ssh/id_ed25519.pub
The key fingerprint is:
SHA256:9RqmxhlGUUQgs7DujEfofAssqgHi5D9lHtm9tXBYYLA root@SRVLX01
The key's randomart image is:
+--[ED25519 256]--+
|     . o.+=+     |
|      o +.+      |
|     . .Eo o     |
|    o   . . o    |
|o.. o o S = .    |
|*+ = = + O =     |
|oo* O . = * .    |
|.o.= o . . .     |
|+  .o            |
+----[SHA256]-----+
root@SRVLX01:/home/wilder# _
```

```
# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication no

PubkeyAuthentication yes
```

Partie 3 - Analyse du stockage

Q.2.3.1 Quels sont les systèmes de fichiers actuellement montés ?

```
root@SRVLX01:/home/wilder# df -Th
Sys. de fichiers          Type     Taille Utilisé Dispo Uti% Monté sur
udev                      devtmpfs   470M       0  470M   0% /dev
tmpfs                     tmpfs       98M    632K   98M   1% /run
/dev/mapper/cp3--vg-root  ext4       2,7G    1,9G  691M  74% /
tmpfs                     tmpfs      489M     16K  489M   1% /dev/shm
tmpfs                     tmpfs      5,0M       0  5,0M   0% /run/lock
/dev/md0p1                ext2       471M     88M  360M  20% /boot
tmpfs                     tmpfs       98M       0   98M   0% /run/user/1000
root@SRVLX01:/home/wilder#
```

Q.2.3.2 Quel type de système de stockage ils utilisent ?

```
root@SRVLX01:/home/wilder# lsblk -f
NAME             FSTYPE FSVER LABEL UUID                                 FSAVAIL FSUSE% MOUNTPOINT
sda
└─sda1           linux_ 1.2   cp3:0 32332561-cf16-c858-7035-17e881dd5c10
  └─md0
    ├─md0p1      ext2   1.0         9bba6d48-3e4b-42a6-bccc-12836de215ec    359,2M    18% /boot
    ├─md0p2
    └─md0p5      LVM2_m LVM2        tlCGJ2-LG5u-kWGc-8kuO-wAiU-icBu-07BEcN
      ├─cp3--vg-root
      │          ext4   1.0         bbc31a37-8e49-47fe-8fad-a3fe18919fdd    690,6M    69% /
      └─cp3--vg-swap_1
                 swap   1           8220bf51-2675-4203-91af-1c149f717652                  [SWAP]
sr0
root@SRVLX01:/home/wilder#
```

Q.2.3.3 Ajouter un nouveau disque de 8,00 Gio au serveur et réparer le volume RAID

```
root@SRVLX01:/home/wilder# lsblk
NAME                    MAJ:MIN RM   SIZE RO TYPE  MOUNTPOINT
sda                       8:0    0     8G  0 disk
└─sda1                    8:1    0     8G  0 part
  └─md0                   9:0    0     8G  0 raid1
    ├─md0p1             259:0    0 488,3M  0 part  /boot
    ├─md0p2             259:1    0     1K  0 part
    └─md0p5             259:2    0   7,5G  0 part
      ├─cp3--vg-root    253:0    0   2,8G  0 lvm   /
      └─cp3--vg-swap_1  253:1    0   976M  0 lvm   [SWAP]
sdc                       8:32   0     8G  0 disk
└─sdc1                    8:33   0     8G  0 part
  └─md0                   9:0    0     8G  0 raid1
    ├─md0p1             259:0    0 488,3M  0 part  /boot
    ├─md0p2             259:1    0     1K  0 part
    └─md0p5             259:2    0   7,5G  0 part
      ├─cp3--vg-root    253:0    0   2,8G  0 lvm   /
      └─cp3--vg-swap_1  253:1    0   976M  0 lvm   [SWAP]
sr0                      11:0    1  1024M  0 rom
root@SRVLX01:/home/wilder# _
```

```
root@SRVLX01:/home/wilder# cat /proc/mdstat
Personalities : [raid1] [linear] [multipath] [raid0] [raid6] [raid5] [raid4] [raid10]
md0 : active raid1 sdc1[2] sda1[0]
      8381440 blocks super 1.2 [2/2] [UU]

unused devices: <none>
root@SRVLX01:/home/wilder# sudo mdmadm --detail /dev/md0
sudo: mdmadm : commande introuvable
root@SRVLX01:/home/wilder# sudo mdadm --detail /dev/md0
/dev/md0:
           Version : 1.2
     Creation Time : Tue Dec 20 10:02:28 2022
        Raid Level : raid1
        Array Size : 8381440 (7.99 GiB 8.58 GB)
     Used Dev Size : 8381440 (7.99 GiB 8.58 GB)
      Raid Devices : 2
     Total Devices : 2
       Persistence : Superblock is persistent

       Update Time : Fri Mar  7 12:17:38 2025
             State : clean
    Active Devices : 2
   Working Devices : 2
    Failed Devices : 0
     Spare Devices : 0

Consistency Policy : resync

              Name : cp3:0
              UUID : 32332561:cf16c858:703517e8:81dd5c10
            Events : 3097

    Number   Major   Minor   RaidDevice State
       0       8        1        0      active sync   /dev/sda1
       2       8       33        1      active sync   /dev/sdc1
root@SRVLX01:/home/wilder#
```

Q.2.3.4 Ajouter un nouveau volume logique LVM de 2 Gio qui servira à héberger des sauvegardes. Ce volume doit être monté automatiquement à chaque démarrage dans l'emplacement par défaut : `/var/lib/bareos/storage`

```
root@SRVLX01:/home/wilder# sudo vgs
  VG     #PV #LV #SN Attr   VSize VFree
  cp3-vg   1   2   0 wz--n- 7,51g <3,79g
root@SRVLX01:/home/wilder# sudo lvcreate -L 2G  -n cp3-vg
  No command with matching syntax recognised.  Run 'lvcreate --help' for more information.
  Nearest similar command has syntax:
  lvcreate --type error -L|--size Size[m|UNIT] VG
  Create an LV that returns errors when used.

root@SRVLX01:/home/wilder# sudo lvcreate -L 2G -n backtoback cp3-vg
  Logical volume "backtoback" created.
root@SRVLX01:/home/wilder# sudo mkfs.ext4 /dev/cp3-vg/backtoback
mke2fs 1.46.2 (28-Feb-2021)
Creating filesystem with 524288 4k blocks and 131072 inodes
Filesystem UUID: e9154c9f-bc23-471c-b60c-e7470af5dd4c
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376, 294912

Allocating group tables: done
Writing inode tables: done
Creating journal (16384 blocks): done
Writing superblocks and filesystem accounting information: done
```

```
# /etc/fstab: static file system information.
#
# Use 'blkid' to print the universally unique identifier for a
# device; this may be used with UUID= as a more robust way to name devices
# that works even if disks are added and removed. See fstab(5).
#
# systemd generates mount units based on this file, see systemd.mount(5).
# Please run 'systemctl daemon-reload' after making changes here.
#
# <file system> <mount point>   <type>  <options>       <dump>  <pass>
/dev/mapper/cp3--vg-root /               ext4    errors=remount-ro 0       1
# /boot was on /dev/md0p1 during installation
UUID=9bba6d48-3e4b-42a6-bccc-12836de215ec /boot           ext2    defaults        0       2
/dev/mapper/cp3--vg-swap_1 none            swap    sw              0       0
/dev/sr0        /media/cdrom0   udf,iso9660 user,noauto     0       0
/dev/cp3-vg/backtoback /var/lib/bareos/storage ext4 defaults 0 2
```

Q,2,3,5 Combien d'espace disponible reste-t-il dans le groupe de volume ?

```
root@SRVLX01:~# df -h
Sys. de fichiers                Taille Utilisé Dispo Uti% Monté sur
udev                              470M       0  470M   0% /dev
tmpfs                              98M    676K   98M   1% /run
/dev/mapper/cp3--vg-root          2,7G    1,9G  691M  74% /
tmpfs                             489M     16K  489M   1% /dev/shm
tmpfs                             5,0M       0  5,0M   0% /run/lock
/dev/md0p1                        471M     88M  360M  20% /boot
tmpfs                              98M       0   98M   0% /run/user/1000
tmpfs                              98M       0   98M   0% /run/user/0
/dev/mapper/cp3--vg-backtoback    2,0G     24K  1,8G   1% /var/lib/bareos/storage
root@SRVLX01:~# nano /etc/fstab
root@SRVLX01:~# df -h
Sys. de fichiers                Taille Utilisé Dispo Uti% Monté sur
udev                              470M       0  470M   0% /dev
tmpfs                              98M    676K   98M   1% /run
/dev/mapper/cp3--vg-root          2,7G    1,9G  691M  74% /
tmpfs                             489M     16K  489M   1% /dev/shm
tmpfs                             5,0M       0  5,0M   0% /run/lock
/dev/md0p1                        471M     88M  360M  20% /boot
tmpfs                              98M       0   98M   0% /run/user/1000
tmpfs                              98M       0   98M   0% /run/user/0
/dev/mapper/cp3--vg-backtoback    2,0G     24K  1,8G   1% /var/lib/bareos/storage
root@SRVLX01:~#
```

Partie 4 - Sauvegardes

Q.2.4.1 Expliquer succinctement les rôles respectifs des 3 composants bareos installés sur la VM.

- **bareos-dir** : Gère et planifie les sauvegardes.
- **bareos-sd** : Gère le stockage des sauvegardes.
- **bareos-fd** : Collecte les données à sauvegarder sur les clients.

Partie 5 - Filtrage et analyse réseau

Q.2.5.1 Quelles sont actuellement les règles appliquées sur Netfilter ?

```
root@SRVLX01:~# sudo nft list ruleset
table inet inet_filter_table {
        chain in_chain {
                type filter hook input priority filter; policy drop;
                ct state established,related accept
                ct state invalid drop
                iifname "lo" accept
                tcp dport 22 accept
                ip protocol icmp accept
                ip6 nexthdr ipv6-icmp accept
        }
```

Q.2.5.2 Quels types de communications sont autorisées ?

```
# Accepter les paquets dans les connexions établies ou liées (réponses aux paquets sortants) ct state established,related accept

# Accepter les paquets venant de l'interface loopback (localhost) iifname "lo" accept

# Accepter les connexions SSH (port 22) tcp dport 22 accept

# Accepter les requêtes ICMP (ping) pour IPv4 ip protocol icmp accept

# Accepter les requêtes ICMP pour IPv6 ip6 nexthdr ipv6-icmp accept
```

Q.2.5.3 Quels types sont interdit ?

```
 # Tout le trafic qui n'est pas explicitement autorisé par une règle est interdit
```

Q.2.5.4 Sur nftables, ajouter les règles nécessaires pour autoriser bareos à communiquer avec les clients bareos potentiellement présents sur l'ensemble des machines du réseau local sur lequel se trouve le serveur.

```
#!/usr/sbin/nft -f

flush ruleset

table inet inet_filter_table {
    chain in_chain {
        type filter hook input priority filter; policy drop;

        # Accepter les paquets dans les connexions établies ou liées
        ct state established,related accept

        # Rejeter les paquets avec un état de connexion invalide
        ct state invalid drop

        # Accepter les paquets venant de l'interface loopback (localhost)
        iifname "lo" accept

        # Accepter SSH (port 22)
        tcp dport 22 accept

        # Accepter ICMP pour IPv4 et IPv6 (ping)
        ip protocol icmp accept
        ip6 nexthdr ipv6-icmp accept

        # Autoriser la communication entre le serveur Bareos et les clients sur le port 9101 (bareo
        tcp dport 9101 accept

        # Autoriser la communication entre le serveur Bareos et le stockage sur le port 9103 (bareo
        tcp dport 9103 accept

        # Autoriser les communications entre le serveur Bareos (192.168.1.200) et les clients dans
        ip daddr 192.168.1.200 ip saddr 192.168.1.0/24 accept
    }
```

Partie 6 - Analyse de logs

Q.2.6.1 Lister les 10 derniers échecs de connexion ayant eu lieu sur le serveur en indiquant pour chacun :

```
root@SRVLX01:~# sudo grep "Failed password" /var/log/auth.log | tail -n 10
Mar  7 14:10:25 SRVLX01 sudo:     root : TTY=pts/0 ; PWD=/root ; USER=root ; COMMAND=/usr/bin/grep Failed password /var/log/auth.log
root@SRVLX01:~# sudo grep "authentication failure" /var/log/auth.log | tail -n 10
Mar  7 11:12:54 SRVLX01 su: pam_unix(su:auth): authentication failure; logname=wilder uid=1000 euid=0 tty=tty1 ruser=wilder rhost=  user=root
Mar  7 11:13:33 SRVLX01 su: pam_unix(su:auth): authentication failure; logname=wilder uid=1000 euid=0 tty=tty1 ruser=wilder rhost=  user=root
Mar  7 11:26:48 SRVLX01 sudo: pam_unix(sudo:auth): authentication failure; logname=wilder uid=1000 euid=0 tty=/dev/tty1 ruser=wilder rhost=  user=wilder
Mar  7 14:10:46 SRVLX01 sudo:     root : TTY=pts/0 ; PWD=/root ; USER=root ; COMMAND=/usr/bin/grep authentication failure /var/log/auth.log
root@SRVLX01:~# sudo grep "Failed password" /var/log/auth.log | awk '{print $1, $2, $3, $11}' | tail -n 10
Mar 7 14:10:25 ;
Mar 7 14:11:18 ;
root@SRVLX01:~#
```

```
root@SRVLX01:~# sudo nft list ruleset
table inet inet_filter_table {
        chain in_chain {
                type filter hook input priority filter; policy drop;
                ct state established,related accept
                ct state invalid drop
                iifname "lo" accept
                tcp dport 22 accept
                ip protocol icmp accept
                ip6 nexthdr ipv6-icmp accept
                tcp dport 9101 accept
                tcp dport 9103 accept
                ip daddr 192.168.1.200 ip saddr 192.168.1.0/24 accept
        }
}
```

ok : /24
nr :
faux :