checkpoint3-CORRECTION

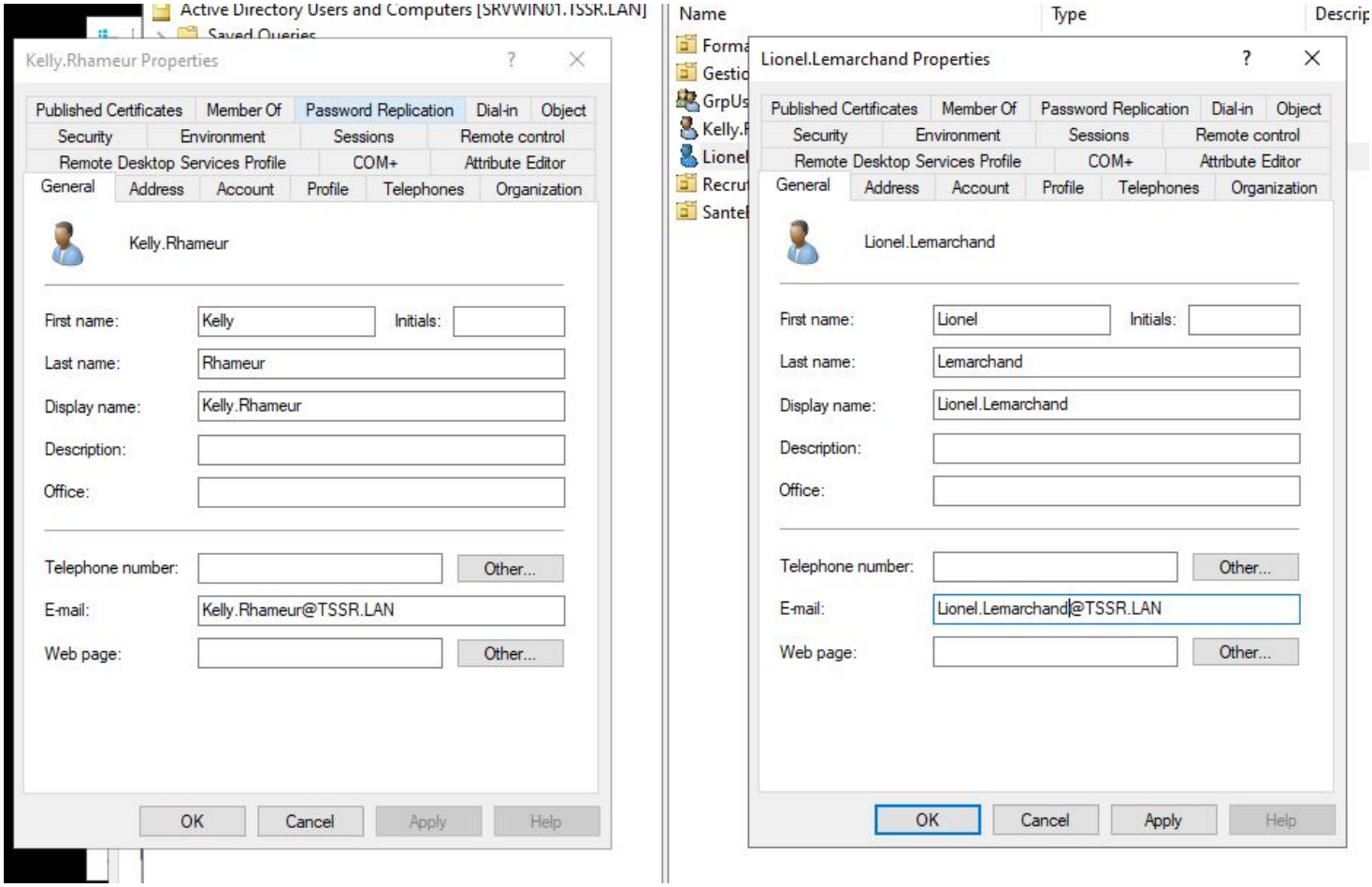
Exercice 1 : Manipulations pratiques sur VM Windows (temps estimé : 1h30)

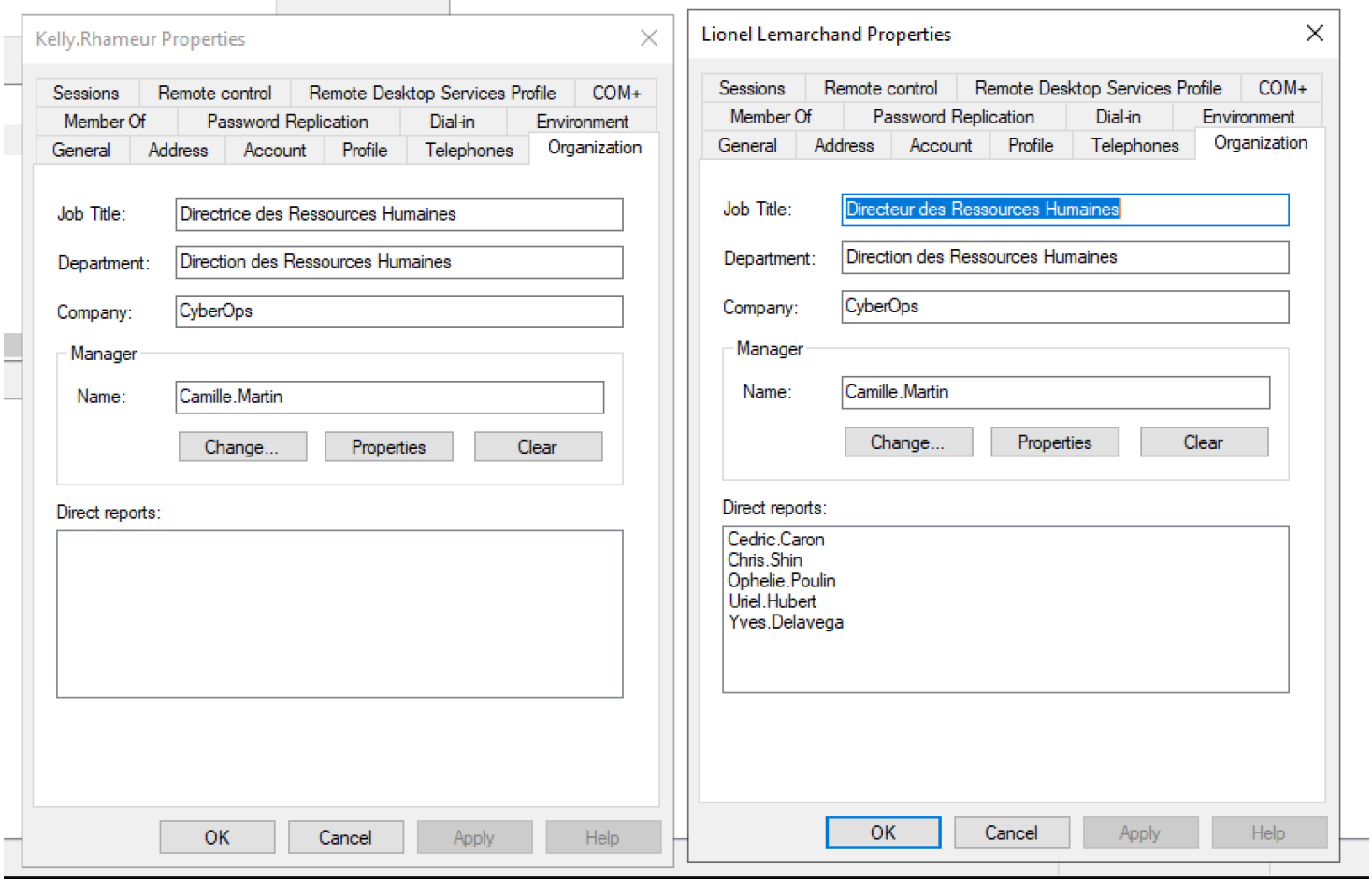
Pour cet exercice tu as besoin de la VM **SRVWIN01**.

Partie 1 : Gestion des utilisateurs

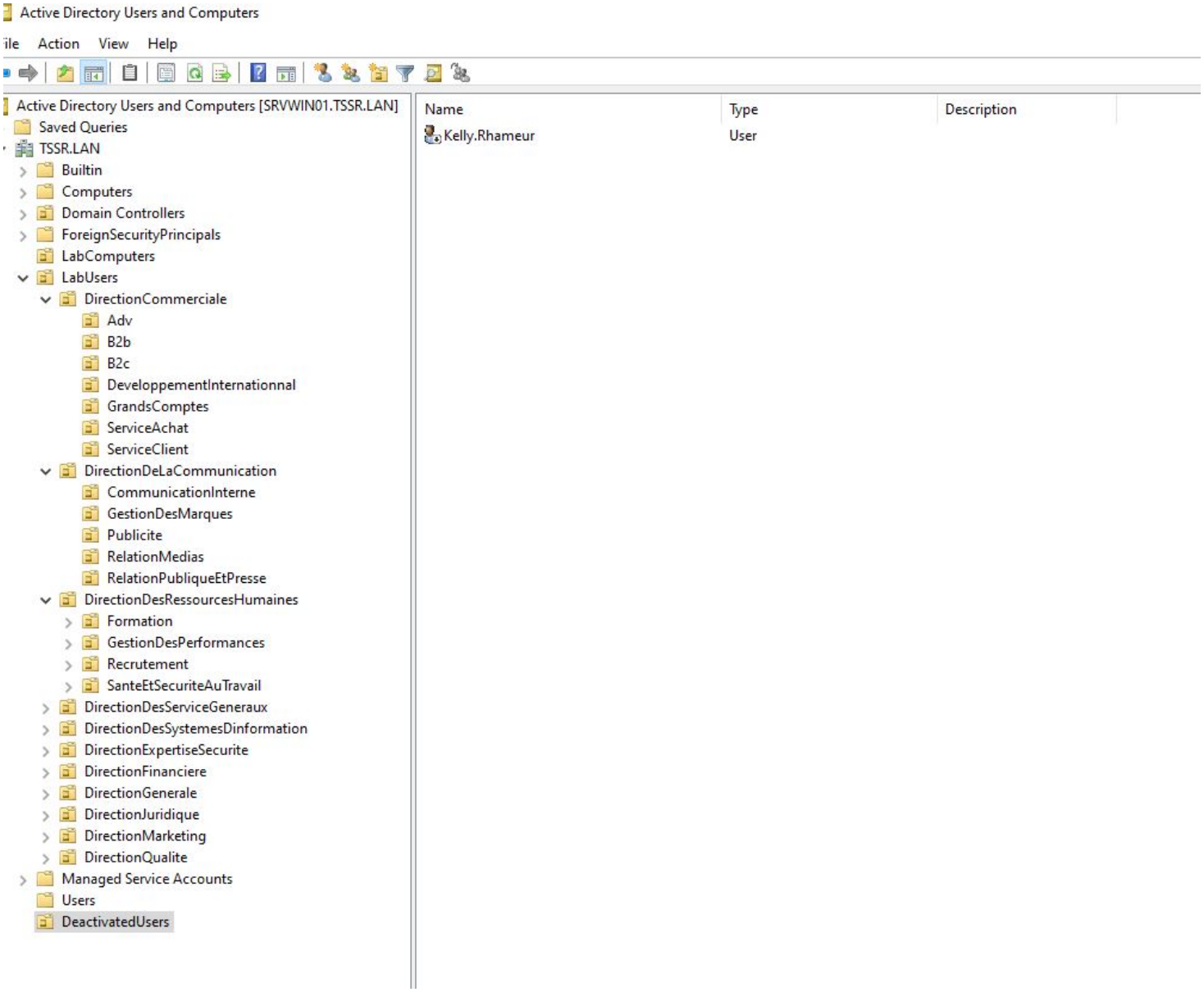
L'utilisateur **Kelly Rhameur** a quitté l'entreprise.
Elle est remplacée par **Lionel Lemarchand**

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

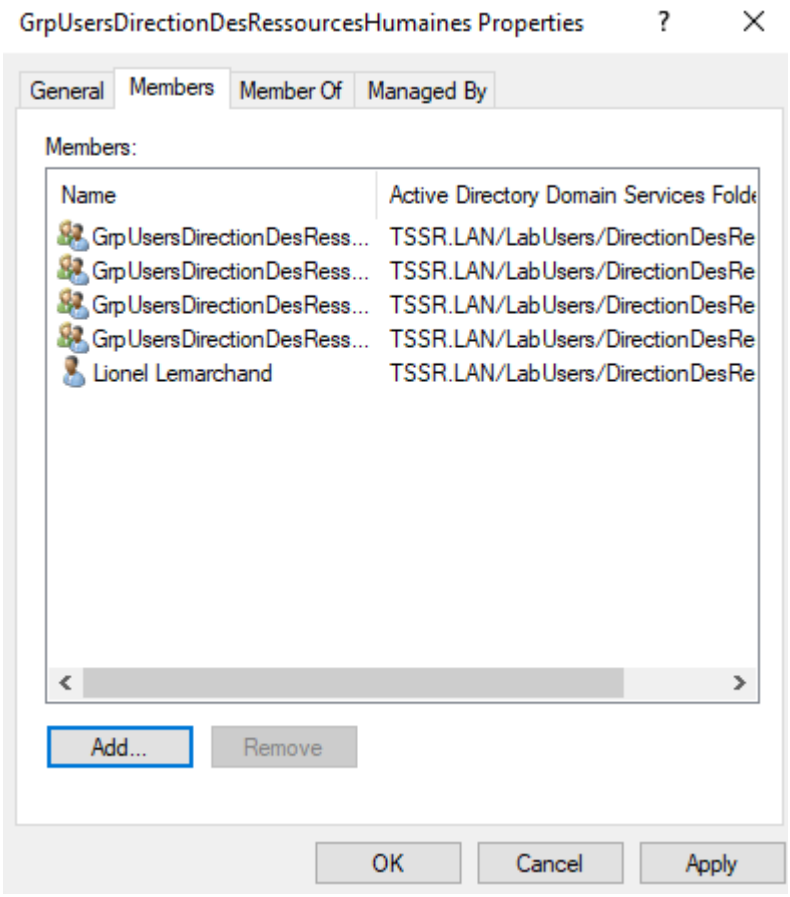



Kelly.Rhameur Properties
Sessions
Remote control
Remote Desktop Services Profile
COM+
Member Of
Password Replication
Dial-in
Environment
General
Address
Account
Profile
Telephones
Organization
Job Title:
Directrice des Ressources Humaines
Department:
Direction des Ressources Humaines
Company:
CyberOps
Manager
Name:
Camille.Martin
Change...
Properties
Clear
Direct reports:
OK
Cancel
Apply
Help
Lionel Lemarchand Properties
Sessions
Remote control
Remote Desktop Services Profile
COM+
Member Of
Password Replication
Dial-in
Environment
General
Address
Account
Profile
Telephones
Organization
Job Title:
Directeur des Ressources Humaines
Department:
Direction des Ressources Humaines
Company:
CyberOps
Manager
Name:
Camille.Martin
Change...
Properties
Clear
Direct reports:
Cedric.Caron
Chris.Shin
Ophelie.Poulin
Uriel.Hubert
Yves.Delavega
OK
Cancel
Apply
Help

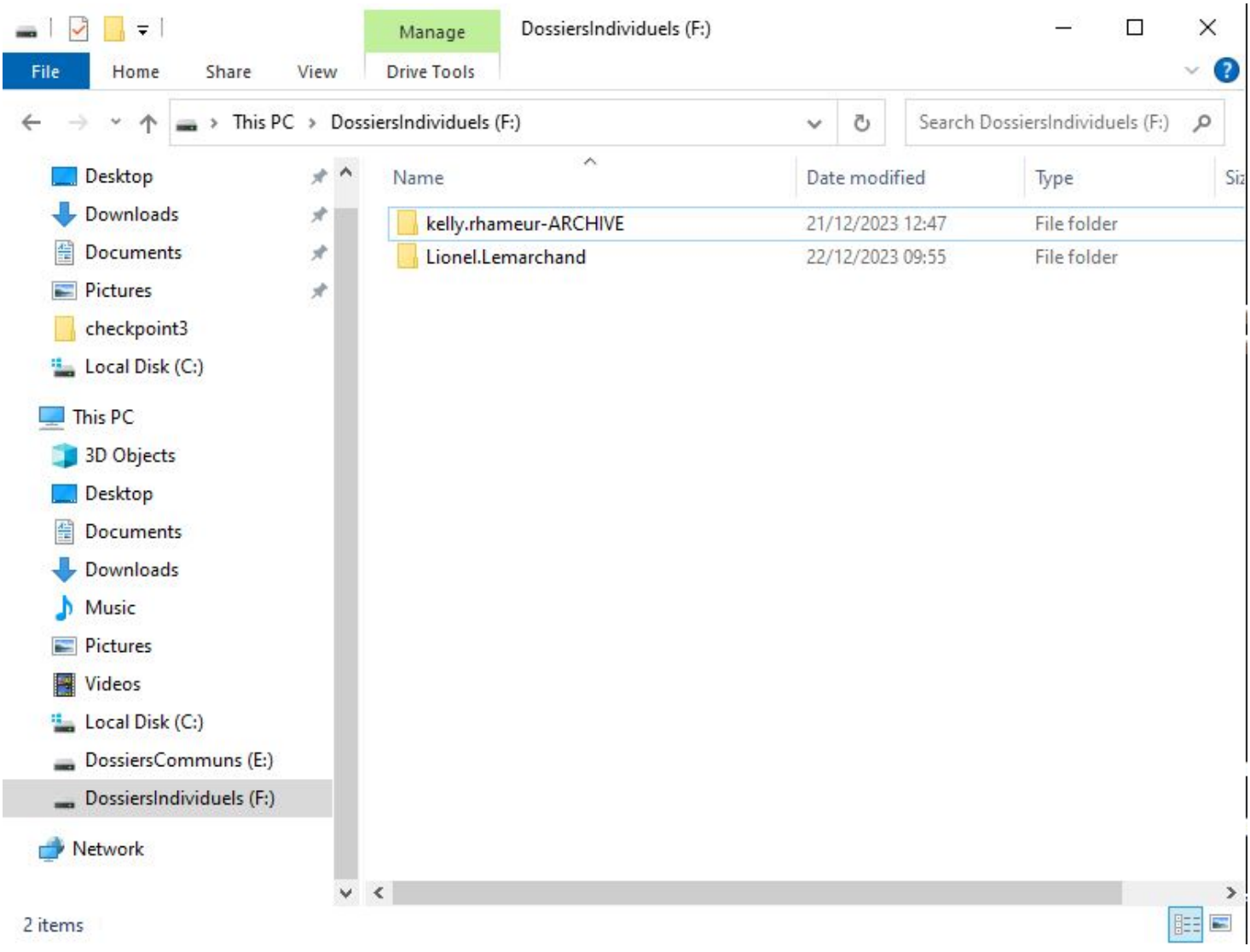
Q.1.1.2 Créer une OU **DeactivatedUsers** et déplace le compte désactivé de **Kelly Rhameur** dedans.



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

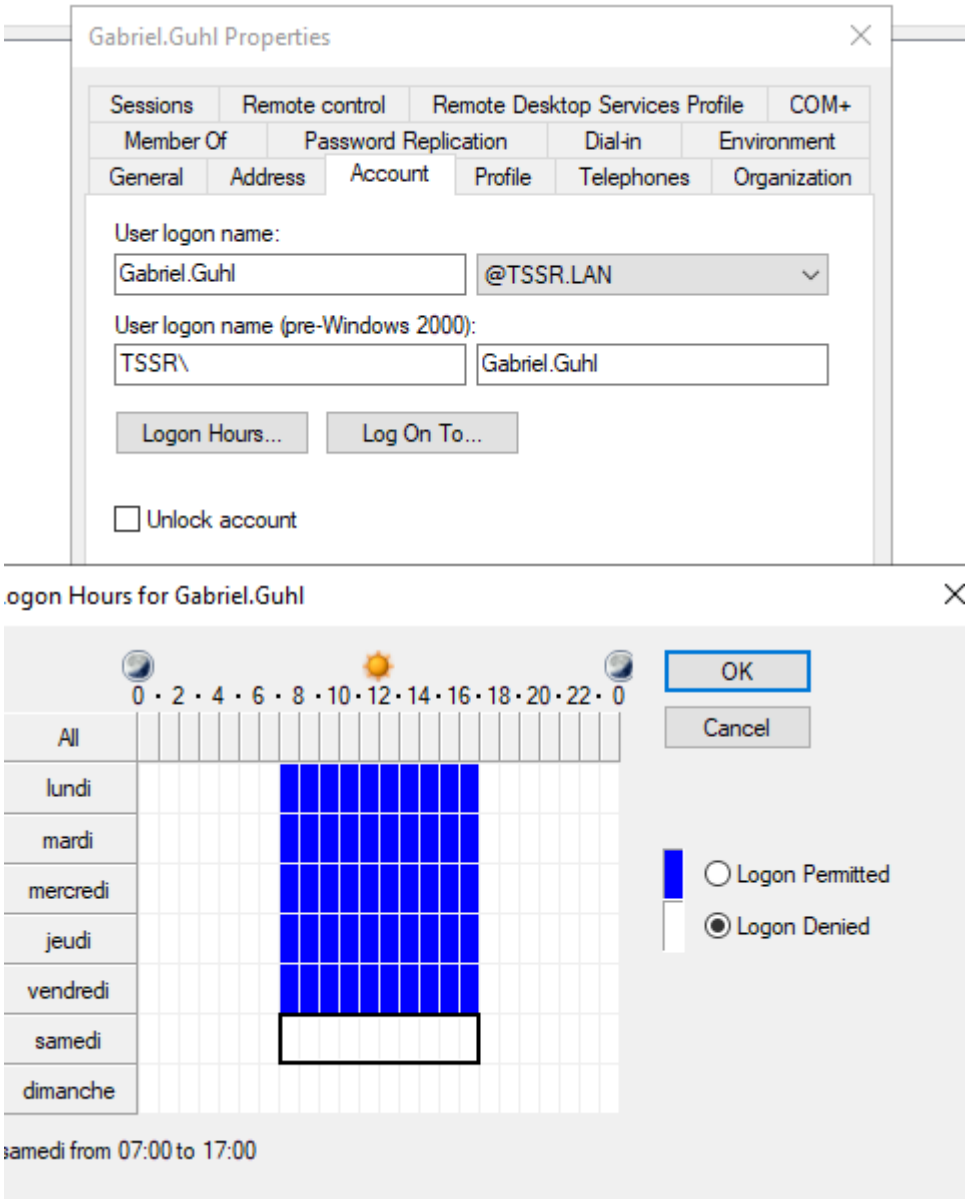


Q.1.1.4 Créer le dossier Individuel du nouvel utilisateur et archive celui de **Kelly Rhameur** en le suffixant par **-ARCHIVE**.

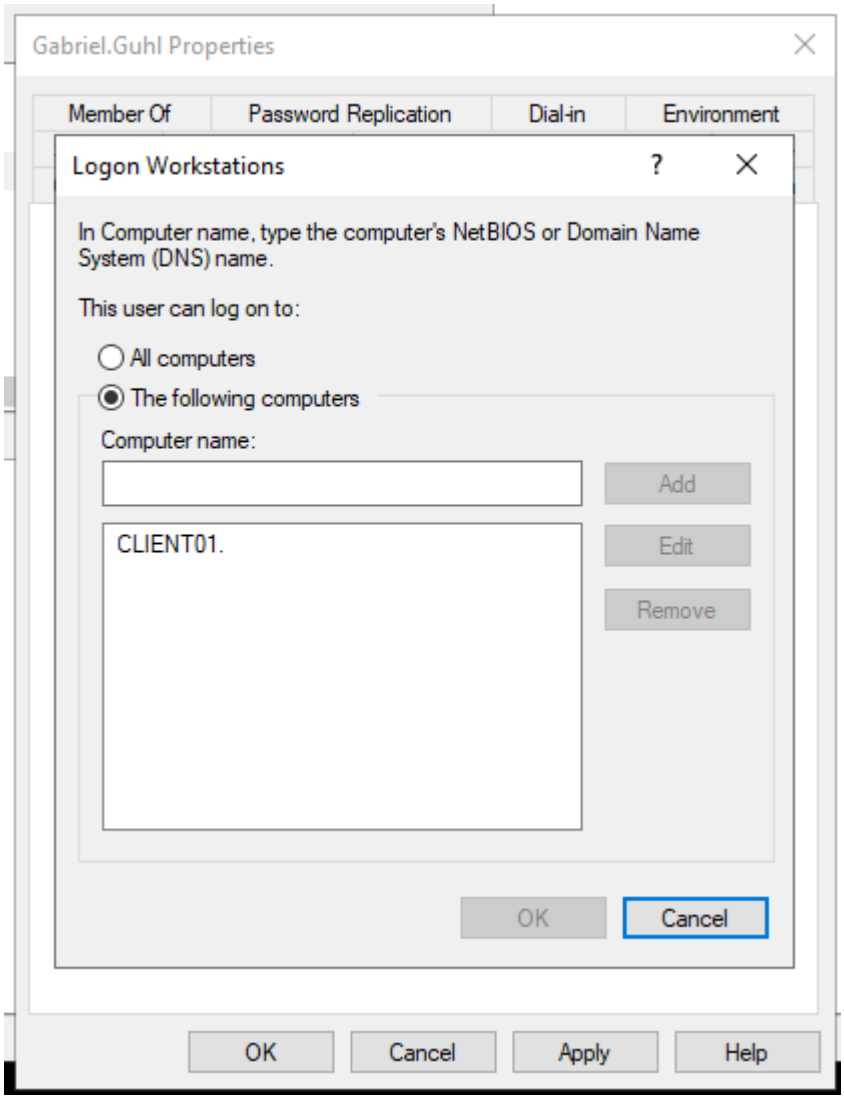


Partie 2 : Restriction utilisateurs

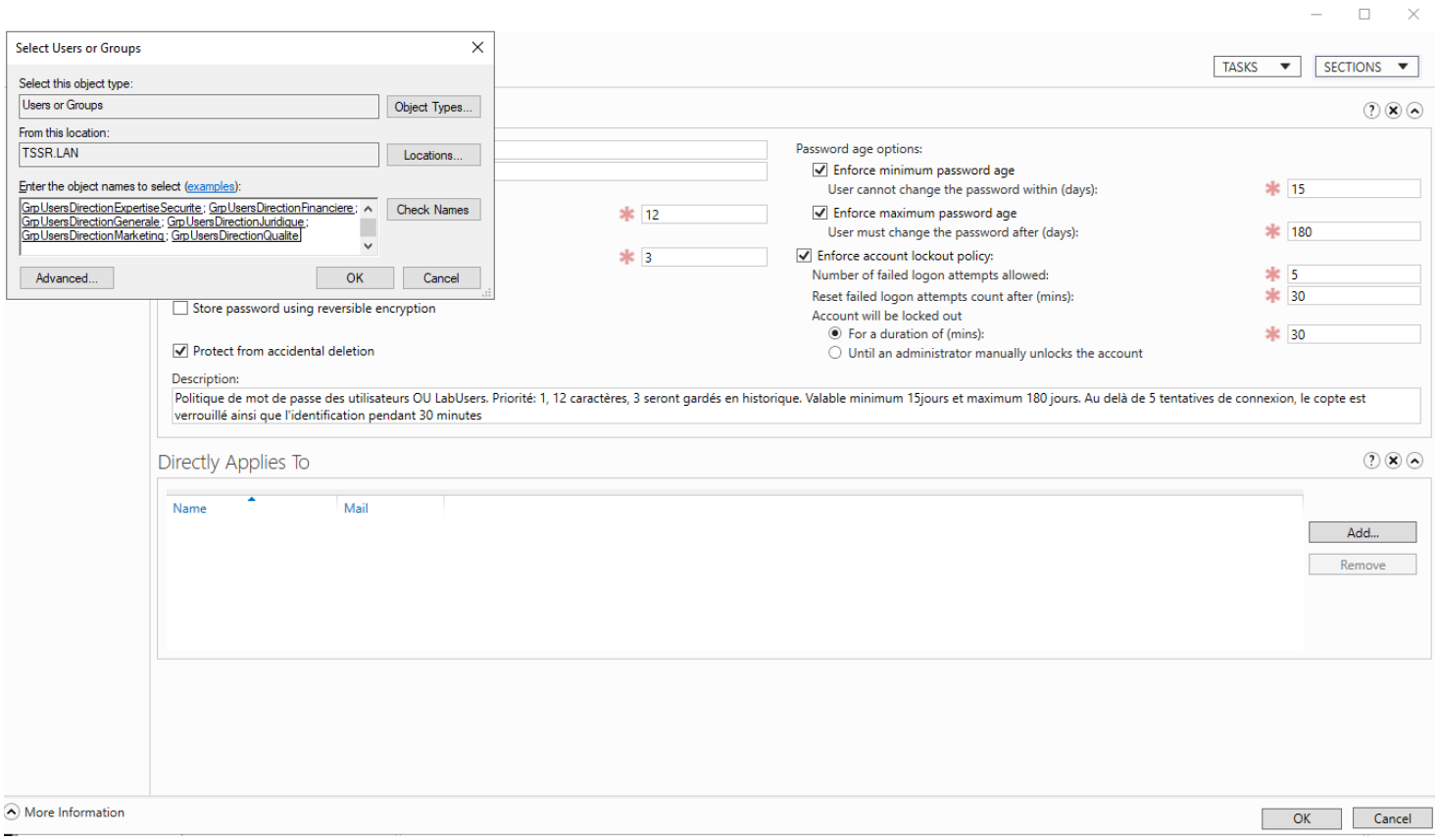
Q.1.2.1 Faire en sorte que l'utilisateur **Gabriel Ghul** ne puisse se connecter que du lundi au vendredi, de 7h à 17h.

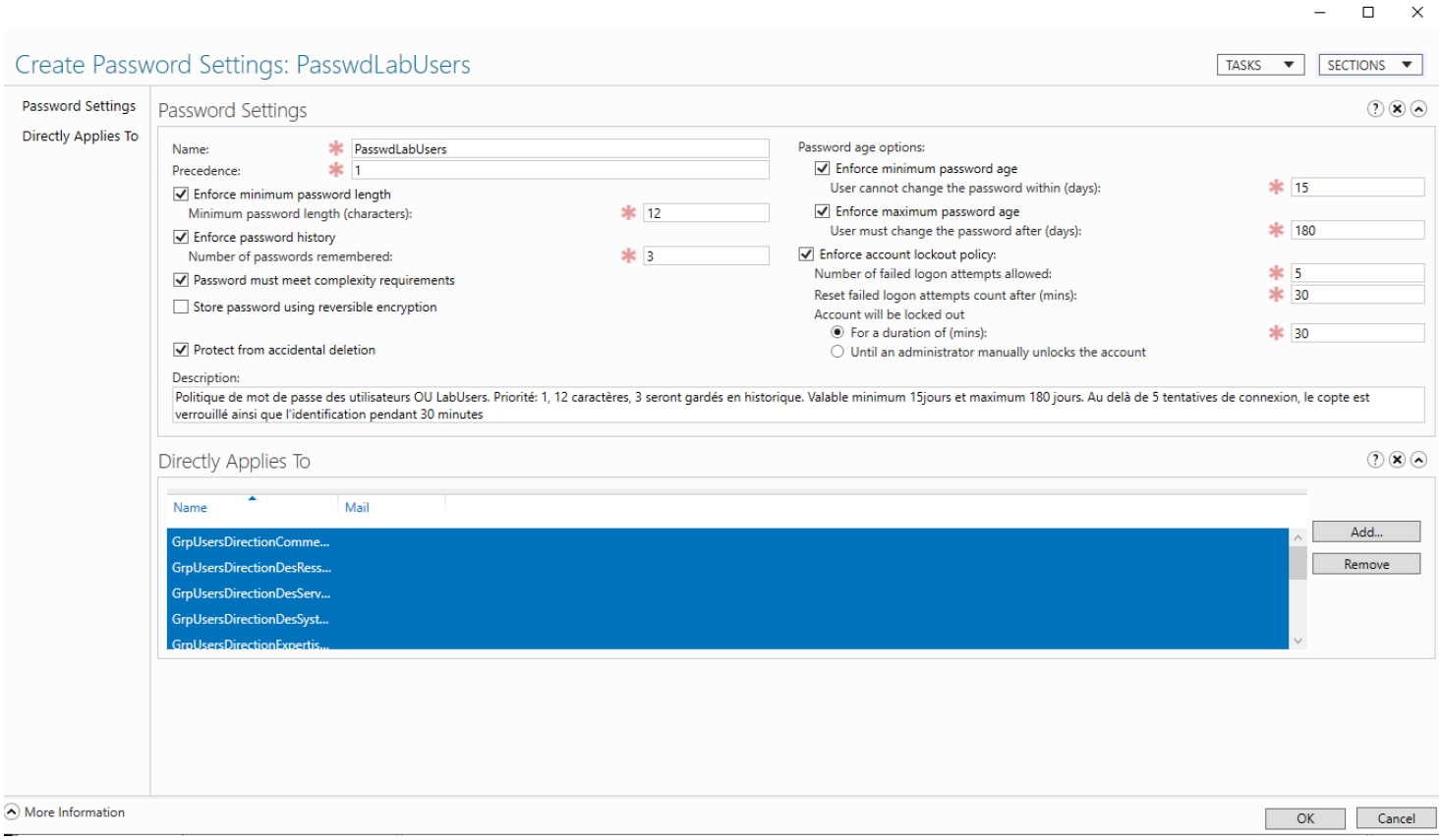


Q.1.2.2 De même, bloquer sa connexion au seul ordinateur **CLIENT01**.



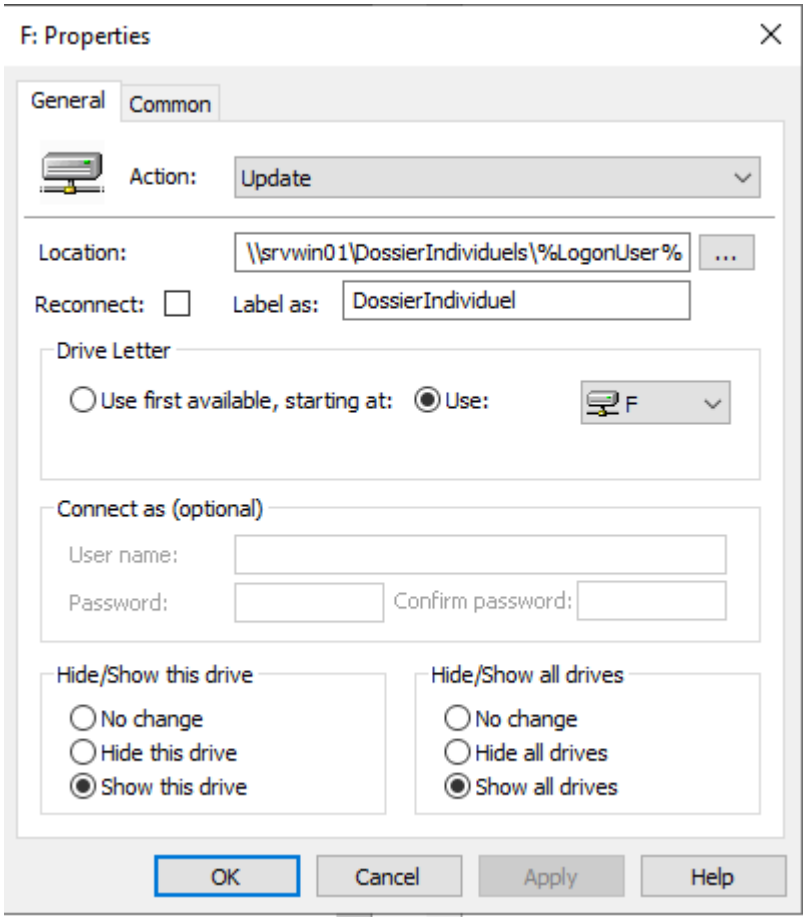
Q.1.2.3 Mettre en place une stratégie de mot de passe pour durcir les comptes des utilisateurs de l'OU **LabUsers**.

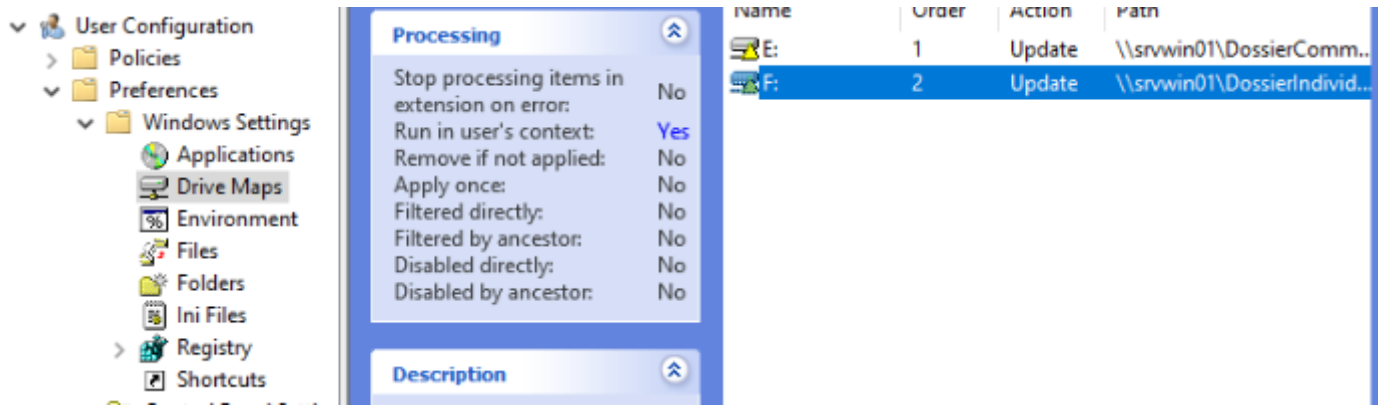




Partie 3 : Lecteurs réseaux

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





Exercice 2 : Manipulations pratiques sur VM Linux (temps estimé : 2h30)

Pour cet exercice tu as besoin de la VM **SRVLX01**.

Partie 1 : Gestion des utilisateurs

Q.2.1.1 Sur le serveur, créer un compte pour ton usage personnel.
Utilisation de la commande `adduser` :

```
root@cp3:~# adduser wilder2
Ajout de l'utilisateur « wilder2 » ...
Ajout du nouveau groupe « wilder2 » (1001) ...
Ajout du nouvel utilisateur « wilder2 » (1001) avec le groupe « wilder2 » ...
Création du répertoire personnel « /home/wilder2 »...
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 wilder2
Enter the new value, or press ENTER for the default
Full Name []:
Room Number []:
Work Phone []:
Home Phone []:
Other []:
Cette information est-elle correcte ? [O/n]o
```

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

```
Mot de passe complexe : Mot de passe d'au moins 12 caractères, avec au moins :
• 1 caractère spécial
• 1 majuscule
• 1 minuscule
• 1 chiffre
Les autorisation sont également à configurer
```

Partie 2 : Configuration de SSH

Un serveur SSH est lancé sur le port par défaut.
Il est possible de s'y connecter avec n'importe quel compte, y compris le compte root.

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

```
# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented. Uncommented options override the
# default value.

Include /etc/ssh/sshd_config.d/*.conf

PermitRootLogin no

Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
```

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

```
# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented. Uncommented options override the
# default value.

Include /etc/ssh/sshd_config.d/*.conf
```

```
PermitRootLogin no
AllowUsers wilder

Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
```

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

```
wilder@LapBuntu:~$ ssh-keygen
Generating public/private ed25519 key pair.
Enter file in which to save the key (/home/wilder/.ssh/id_ed25519): keylab
Enter passphrase (empty for no passphrase):
Enter same passphrase again:

[...]

The key's randomart image is:
+---[ED25519 256]---+
|                   |
|                   |
|                   |
| . . .             |
| o . S o.. . o     |
|+o.= o+o oO+o      |
|B=+. o+ o.++.o|    |
|B Eo ..o o + =     |
|*+ ...=* o..o|     |
+----[SHA256]------+
```

Copie de la clé publique sur le serveur avec `ssh-copy-id -p 22 -i keylab.pub wilder@192.168.1.84`

```
# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented. Uncommented options override the
# default value.

Include /etc/ssh/sshd_config.d/*.conf

PermitRootLogin no
AllowUsers wilder

PasswordAuthentication no
PubkeyAuthentication yes

Port 22
#AddressFamily any
```

```
#ListenAddress 0.0.0.0
#ListenAddress ::
```

Partie 3 : Analyse du stockage

Q.2.3.1 Quels sont les systèmes de fichiers actuellement montés ?
`df` affiche les systèmes de fichiers montés :

```
root@SRVLX01:~# df -hT
Sys. de fichiers         Type     Taille Utilisé Dispo Uti% Monté sur
udev                     devtmpfs   470M       0  470M   0% /dev
tmpfs                    tmpfs       98M    604K   98M   1% /run
/dev/mapper/cp3--vg-root ext4       2,7G    1,5G  1,1G  59% /
tmpfs                    tmpfs      489M     16K  489M   1% /dev/shm
tmpfs                    tmpfs      5,0M       0  5,0M   0% /run/lock
/dev/md0p1               ext2       471M     49M  398M  11% /boot
tmpfs                    tmpfs       98M       0   98M   0% /run/user/1000
```

Donc **ext4** et **ext2**.

> On peut aussi utiliser `lsblk -f`

Q.2.3.2 Quel type de système de stockage ils utilisent ?
`lsblk` affiche la liste de tous les dispositifs de bloc disponibles et leurs points de montage (structure du montage des disques et des partitions) :

```
root@SRVLX01:~# 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    397,3M
10% /boot
    ├─md0p2
    └─md0p5    LVM2_m LVM2        tlCGJ2-LG5u-kWGc-8kuO-wAiU-icBu-07BEcN
      ├─cp3--vg-root
      │        ext4   1.0         bbc31a37-8e49-47fe-8fad-a3fe18919fdd        1G
55% /
      └─cp3--vg-swap_1
               swap   1           8220bf51-2675-4203-91af-1c149f717652
[SWAP]
sr0
```

Donc systèmes de stockage utilisés : **RAID** et **LVM**.

Q.2.3.3 Ajouter un nouveau disque de 8,00 Gio au serveur et réparer le volume RAID
Vérifier l'état du RAID :
Méthode 1 :

```
root@SRVLX01:~# cat /proc/mdstat
Personalities : [raid1] [linear] [multipath] [raid0] [raid6] [raid5] [raid4]
[raid10]
md0 : active raid1 sda1[0]
      8381440 blocks super 1.2 [2/1] [U_]

unused devices: <none>
```

==> md0 = RAID1 avec 1 seul disque `sda1[0]`
`[2/1] [U_]` indique 1 seul disque fonctionnel

Méthode 2 :

```
root@SRVLX01:~# 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 : 1
       Persistence : Superblock is persistent

       Update Time : Thu Dec 21 15:46:25 2023
             State : clean, degraded
    Active Devices : 1
   Working Devices : 1
    Failed Devices : 0
     Spare Devices : 0

Consistency Policy : resync

              Name : cp3:0
              UUID : 32332561:cf16c858:703517e8:81dd5c10
            Events : 2434

    Number   Major   Minor   RaidDevice State
       0       8        1        0      active sync   /dev/sda1
       -       0        0        1      removed
```

On voit le statut dégradé avec `State : clean, degraded`

Après ajout du disque de 8 Go (vdi) sur virtualbox et l'attachement à la machine debian, liste des disques :

```
root@SRVLX01:~# fdisk -l
Disque /dev/sda : 8 GiB, 8589934592 octets, 16777216 secteurs
Modèle de disque : VBOX HARDDISK
Unités : secteur de 1 × 512 = 512 octets
```

```
Taille de secteur (logique / physique) : 512 octets / 512 octets
taille d'E/S (minimale / optimale) : 512 octets / 512 octets
Type d'étiquette de disque : dos
Identifiant de disque : 0x92c7c8b1

Périphérique Amorçage Début Fin Secteurs Taille Id Type
/dev/sda1 *
2048 16775167 16773120 8G fd RAID Linux autodétecté

Disque /dev/md0 : 7,99 GiB, 8582594560 octets, 16762880 secteurs
Unités : secteur de 1 × 512 = 512 octets
Taille de secteur (logique / physique) : 512 octets / 512 octets
taille d'E/S (minimale / optimale) : 512 octets / 512 octets
Type d'étiquette de disque : dos
Identifiant de disque : 0x5d8af9d6

Périphérique Amorçage Début Fin Secteurs Taille Id Type
/dev/md0p1
2 1000109 1000108 488,3M 83 Linux
/dev/md0p2
1000110 16762679 15762570 7,5G 5 Étendue
/dev/md0p5
1000112 16762679 15762568 7,5G 8e LVM Linux

Disque /dev/mapper/cp3--vg-root : 2,77 GiB, 2973761536 octets, 5808128 secteurs
Unités : secteur de 1 × 512 = 512 octets
Taille de secteur (logique / physique) : 512 octets / 512 octets
taille d'E/S (minimale / optimale) : 512 octets / 512 octets

Disque /dev/mapper/cp3--vg-swap_1 : 976 MiB, 1023410176 octets, 1998848 secteurs
Unités : secteur de 1 × 512 = 512 octets
Taille de secteur (logique / physique) : 512 octets / 512 octets
taille d'E/S (minimale / optimale) : 512 octets / 512 octets

Disque /dev/sdb : 8 GiB, 8589934592 octets, 16777216 secteurs
Modèle de disque : VBOX HARDDISK
Unités : secteur de 1 × 512 = 512 octets
Taille de secteur (logique / physique) : 512 octets / 512 octets
taille d'E/S (minimale / optimale) : 512 octets / 512 octets
```

Création d'une partition sur le disque de 8 Go

```
root@SRVLX01:~# fdisk /dev/sdb

Bienvenue dans fdisk (util-linux 2.36.1).

Les modifications resteront en mémoire jusqu'à écriture.
Soyez prudent avant d'utiliser la commande d'écriture.

Le périphérique ne contient pas de table de partitions reconnue.
Création d'une nouvelle étiquette pour disque de type DOS avec identifiant de
disque 0x77a24756.
```

```
Commande (m pour l'aide) : p
Disque /dev/sdb : 8 GiB, 8589934592 octets, 16777216 secteurs
Modèle de disque : VBOX HARDDISK
Unités : secteur de 1 × 512 = 512 octets
Taille de secteur (logique / physique) : 512 octets / 512 octets
taille d'E/S (minimale / optimale) : 512 octets / 512 octetsType d'étiquette de
disque : dos
Identifiant de disque : 0x77a24756

Commande (m pour l'aide) : n
Type de partition
p primaire (0 primaire, 0 étendue, 4 libre)
e étendue (conteneur pour partitions logiques)
Sélectionnez (p par défaut) :
Numéro de partition (1-4, 1 par défaut) :
Premier secteur (2048-16777215, 2048 par défaut) :
Dernier secteur, +/-secteurs ou +/-taille{K,M,G,T,P} (2048-16777215, 16777215 par
défaut) :

Une nouvelle partition 1 de type « Linux » et de taille 8 GiB a été créée.

Commande (m pour l'aide) : p
Disque /dev/sdb : 8 GiB, 8589934592 octets, 16777216 secteurs
Modèle de disque : VBOX HARDDISK
Unités : secteur de 1 × 512 = 512 octets
Taille de secteur (logique / physique) : 512 octets / 512 octets
taille d'E/S (minimale / optimale) : 512 octets / 512 octets
Type d'étiquette de disque : dos
Identifiant de disque : 0x77a24756

Périphérique Amorçage Début Fin Secteurs Taille Id Type
/dev/sdb1
2048 16777215 16775168 8G 83 Linux

Commande (m pour l'aide) : w
La table de partitions a été altérée.
Appel d'ioctl() pour relire la table de partitions.
Synchronisation des disques.
```

Réparer le RAID :Ajouter le disque sdb (avec la partition sdb1) au RAID :

```
root@SRVLX01:~# mdadm --add /dev/md0 /dev/sdb
mdadm: added /dev/sdb
```

Vérification de la reconstruction du RAID

```
root@SRVLX01:~# mdadm -D /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 : Wed Jan 11 01:50:35 2023
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 : 1861
Number Major Minor RaidDevice State
0
8
1
0 active sync /dev/sda1
2
8
17
1 active sync /dev/sdb1
```

==> state en "clean" donc ok

Dernière vérif possible :

```
root@SRVLX01:~# cat /proc/mdstat
Personalities : [raid1] [linear] [multipath] [raid0] [raid6] [raid5] [raid4]
[raid10]
md0 : active raid1 sdb1[2] sda1[0]
8381440 blocks super 1.2 [2/2] [UU]
unused devices: <none>
```

==> 2 disques sda (avec la partition sda1) et sdb (avec la partition sdb1) ok sur le RAID1

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`.
Affichage des infos LVM avec la commande `vgdisplay`, le nom du VG est `cp3-vg`.

Avec le nom du VG "cp3-vg", je regarde si je peux créer un disque logique de 2 Go :

```
root@SRVLX01:~# vgdisplay cp3-vg | grep "Free"
Free PE / Size           970 / <3,79 GiB
```

Oui c'est possible car il reste 3.79 Go.

Création du volume logique de 2 Go

```
root@SRVLX01:~# lvcreate --name LVMBackup --size 2G cp3-vg
Logical volume "LVMBackup" created.
```

Formatage du volume logique (ici en ext4) :

```
root@SRVLX01:~# mkfs.ext4 /dev/cp3-vg/LVMBackup
mke2fs 1.46.2 (28-Feb-2021)
Creating filesystem with 524288 4k blocks and 131072 inodes
Filesystem UUID: 2bb2922a-244e-446d-beb0-bbc1a8b02050
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
```

Vérification existence du répertoire de montage par défaut **/var/lib/bareos/storage** :

```
root@SRVLX01:~# ls -d /var/lib/bareos/storage
/var/lib/bareos/storage
```

Montage dans l'emplacement par défaut **/var/lib/bareos/storage** :

```
root@SRVLX01:~# mount /dev/cp3-vg/LVMBackup /var/lib/bareos/storage/
```

Montage automatique à chaque démarrage :

```
# Editer le fichier /etc/fstab
root@SRVLX01:~# nano /etc/fstab
GNU nano 5.4
/etc/fstab *
# /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
/dev/mapper/cp3--vg-swap_1 none
swap sw
0
0
/dev/sr0
/media/cdrom0 udf,iso9660 user,noauto 0
0
/dev/cp3-vg/LVMBackup /var/lib/bareos/storage ext4 defaults
0
0
```

Ajouter la ligne `/dev/cp3-vg`, enregistrer et fermer le fichier

Q.2.3.5 Combien d'espace disponible reste-t-il dans le groupe de volume ?

```
root@SRVLX01:~# vgdisplay
2--- Volume group ---
VG Name                cp3-vg
System                 ID
Format                 lvm2
Metadata Areas         1
Metadata Sequence No   4
VG Access              read/write
VG Status              resizable
MAX LV                 0
Cur LV                 3
Open LV                3
Max PV                 0
Cur PV                 1
Act PV                 1
VG Size                7,51 GiB
PE Size                4,00 MiB
Total PE               1923
Alloc PE / Size        1465 / 5,72 GiB
Free PE / Size         458 / <1,79 GiB
VG UUID                BMardR-vLO6-CToa-ad0f-XVh0-ODeS-cX7Obt
```

Il reste moins de 1,79 Go

Partie 4 : Sauvegardes

Le logiciel bareos est installé sur le serveur.
Les composants `bareos-dir`, `bareos-sd` et `bareos-fd` sont installés avec une configuration par défaut.

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

Bareos-dir (*Director*): Composant central qui gère la configuration, la planification des travaux de sauvegarde
Bareos-sd (*Storage Daemon*): Responsable du stockage physique des données de sauvegarde sur les supports de stockage qu'il reçoit des clients.
Bareos-fd (*File Daemon*): C'est l'agent installé sur chaque client qui permet à Bareos-dir de gérer les sauvegardes.

Partie 5 : Filtrage et analyse réseau

Q.2.5.1 Quelles sont actuellement les règles appliquées sur Netfilter ?
Dans le fichier `/etc/network/interfaces` on voit un fichier `/root/nftables/config.nft`.
Contenu de ce fichier :

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

flush 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 ssh accept
                ip protocol icmp accept
                ip6 nexthdr icmpv6 accept
        }
}
```

> ou la commande `nft list ruleset`

Q.2.5.2 Quels types de communications sont autorisées ?
`fluch ruleset` supprime toutes les règles existantes. Seules celles indiquées ici seront validées par le système.
Dans cette règle, la politique est que tout paquet qui ne correspond pas à la règle sera rejeté (`drop`).
Est accepté :

- `ct state established, related accept` : les connexions déjà établies
- `iifname lo accept` : trafic de bouclage
- `tcp dport ssh accept` : ssh
- `ip protocol icmp accept` : ping (icmp)
- `ip6 nexthdr icmpv6 accept` : ping6 (icmpv6)

Q.2.5.3 Quels types sont interdit ?

- `ct state invalid drop` : paquets ne pouvant pas être identifiés
- Tout le reste

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.

```
Rappel : Bareos utilise les ports TCP 9101 à 9103 pour la communication entre ses différents composants.
```

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

flush 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 ssh accept
                ip protocol icmp accept
                ip6 nexthdr icmpv6 accept

                # Ajout des règles pour Bareos
                tcp dport { 9101-9103 } ct state new accept
        }
}
```

Ou ajout d'une table séparée dans la même table :

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

flush 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 ssh accept
                ip protocol icmp accept
                ip6 nexthdr icmpv6 accept

                # Bareos
                tcp dport { 9101-9103 } ct state new accept
        }

        chain input {
        type filter hook input priority filter; policy drop;
        tcp dport 9101 accept
```

```
        tcp dport 9102 accept
        tcp dport 9103 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 :

- La date et l'heure de la tentative
- L'adresse IP de la machine ayant fait la tentative

Plusieurs possibilités :

- `lastb` : affiche le connexions en échec
- `journalctl -t sshd | grep 'Failed' | tail -n 10` : échecs de connexion ssh
- `journalctl -u ssh | grep 'Failed password' | tail -n 10` : échec sur les mots de passe ssh