

Exercice 1 - VM Windows

Partie 1 - Gestion des utilisateurs

Q.1.1.1

Il est possible d'utiliser l'option **Copier** pour créer un nouvel utilisateur en conservant les mêmes attributs qu'un utilisateur existant. Cela simplifie la création de Lionel Lemarchand en copiant directement le compte de Kelly Rhameur.

The screenshot shows the 'Lionel Lemarchand Properties' dialog box in the Active Directory Users and Groups console. The 'Organization' tab is selected, showing the following fields:

- Job Title: Directeur des Ressources Humaines
- Department: Direction des Ressources Humaines
- Company: CyberOps
- Manager: Camille.Martin

Below the Manager field are buttons for 'Change...', 'Properties', and 'Clear'. The 'Direct reports:' field is empty.

In the background, the Active Directory Users and Groups console is visible, showing a list of objects:

name	type	Description
Formation	Organizational Unit	
GestionDesPerformances	Organizational Unit	
GrpUsersDirectionDesRessourcesHumaines	Security Group - Global	
Kelly.Rhameur	User	
Lionel Lemarchand	User	
Recrutement	Organizational Unit	
SanteEtSecuriteAuTravail	Organizational Unit	

Organizational Unit

Lionel Lemarchand Properties

Member Of	Dial-in	Environment	Sessions
Remote control	Remote Desktop Services Profile		COM+
General	Address	Account	Profile
	Telephones	Organization	



Lionel Lemarchand

First name: Lionel Initials:

Last name: Lemarchand

Display name: Lionel Lemarchand

Description: Office: Telephone number: Other...

E-mail: Lionel.Lemarchand@TSSR.LAN

Web page: Other...

Q.1.1.2

Action view help

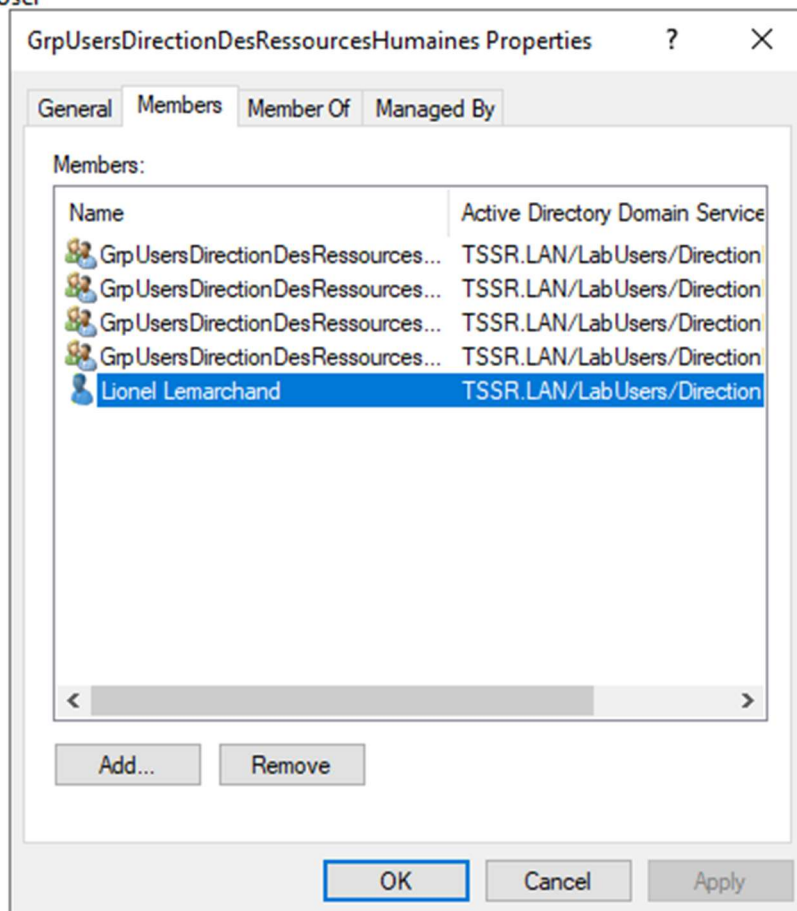
Active Directory Users and Computers [SRVWIN01.TSSR.LAN]	
Name	Type
Kelly.Rhameur	User

Saved Queries
 TSSR.LAN
 > Built-in
 > Computers
 > Domain Controllers
 > ForeignSecurityPrincipals
 > LabComputers
 > LabUsers
 > DeactivatedUsers
 > DirectionCommerciale

Q.1.1.3

maines Security Group - Global

User



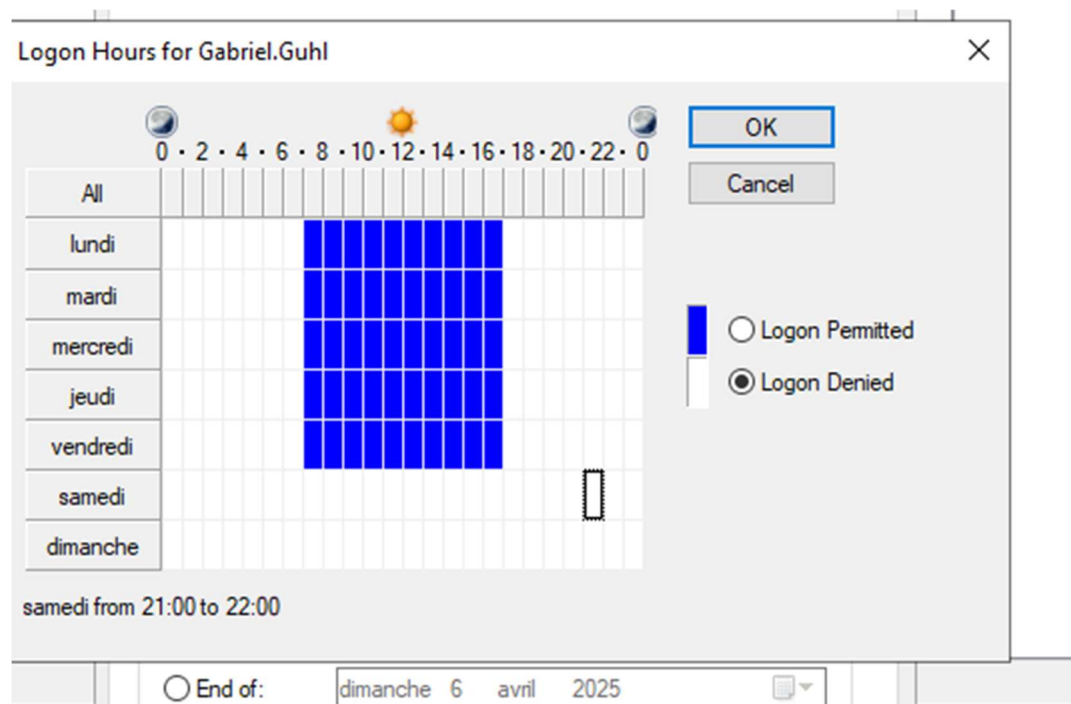
Q.1.1.1.4

> DossiersIndividuels (F:) >

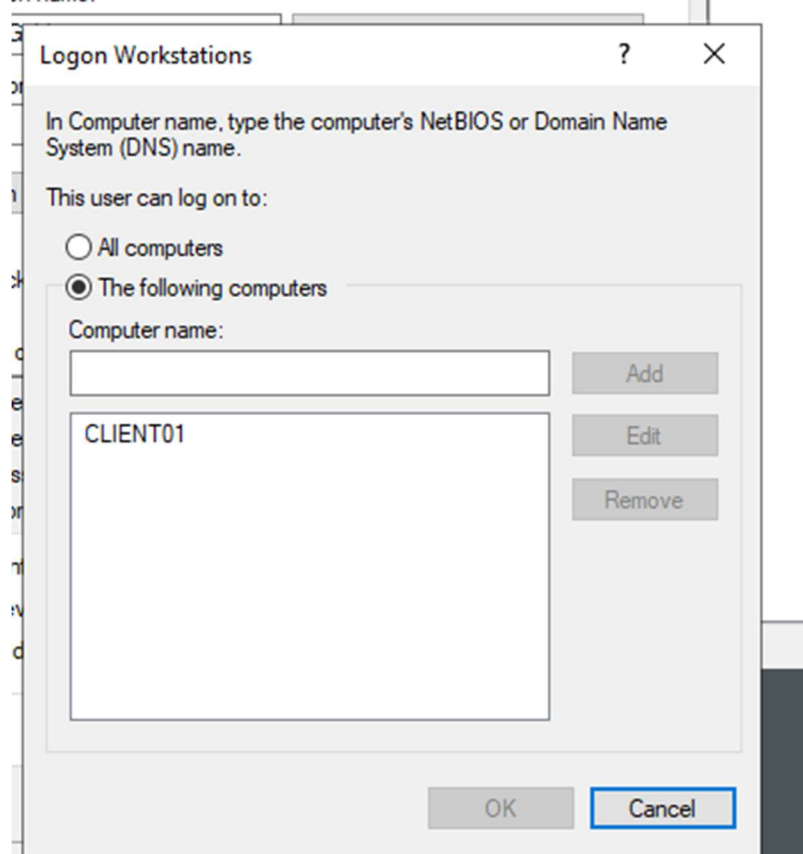
Name	Date modified	Type	Size
kelly.rhameur-ARCHIVE	21/12/2023 12:47	File folder	
Lionel.Lemarchand	07/03/2025 09:31	File folder	

Partie 2 - Restriction utilisateurs









Q.1.2.1

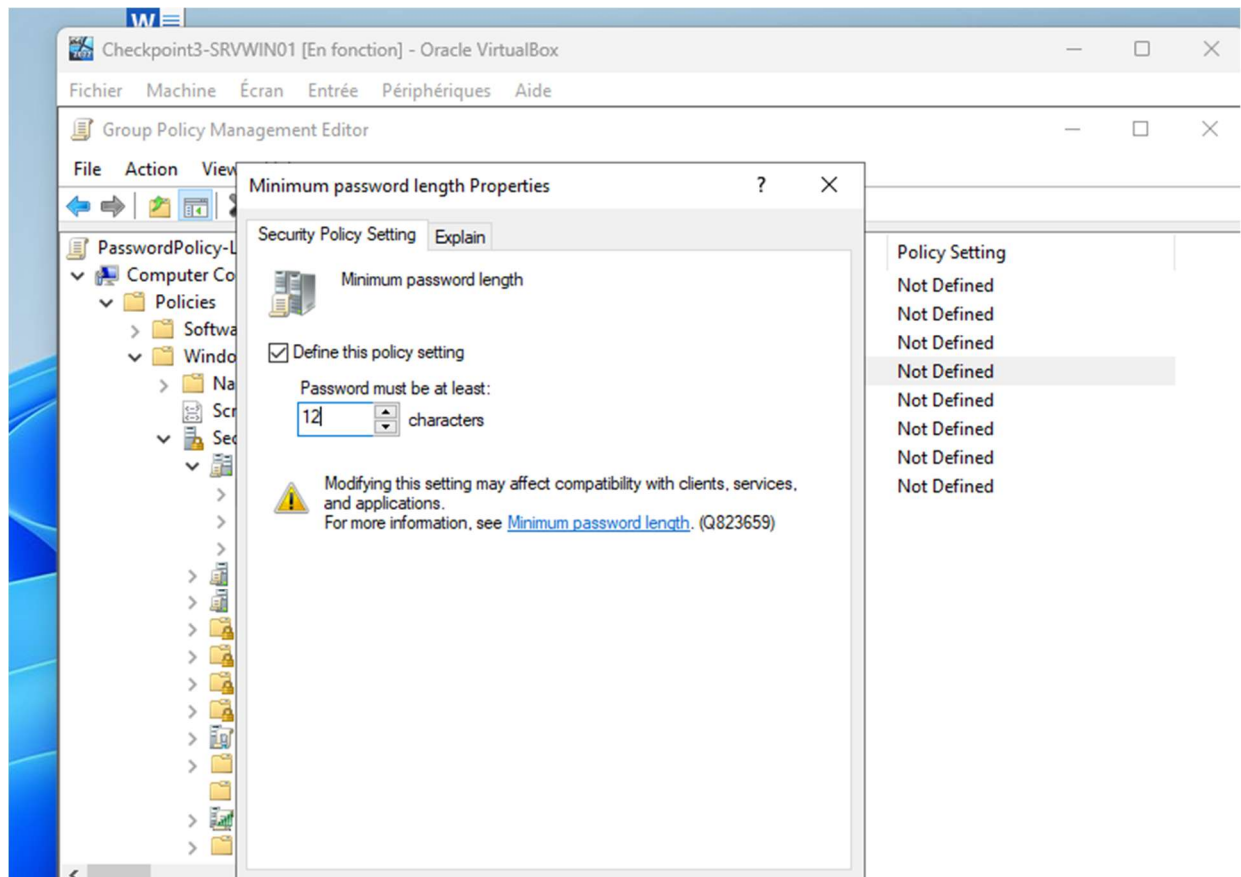


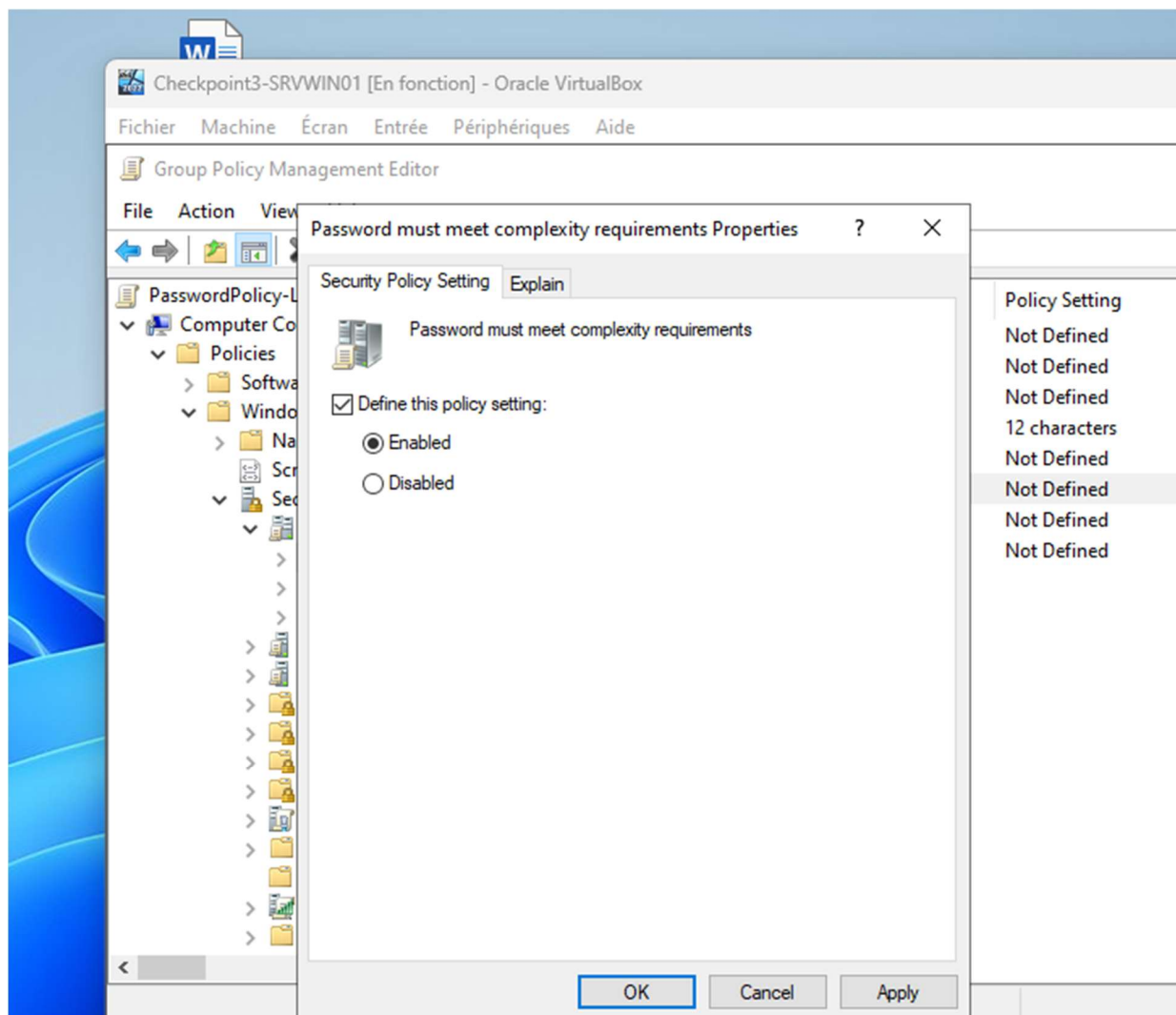
Q.1.2.2

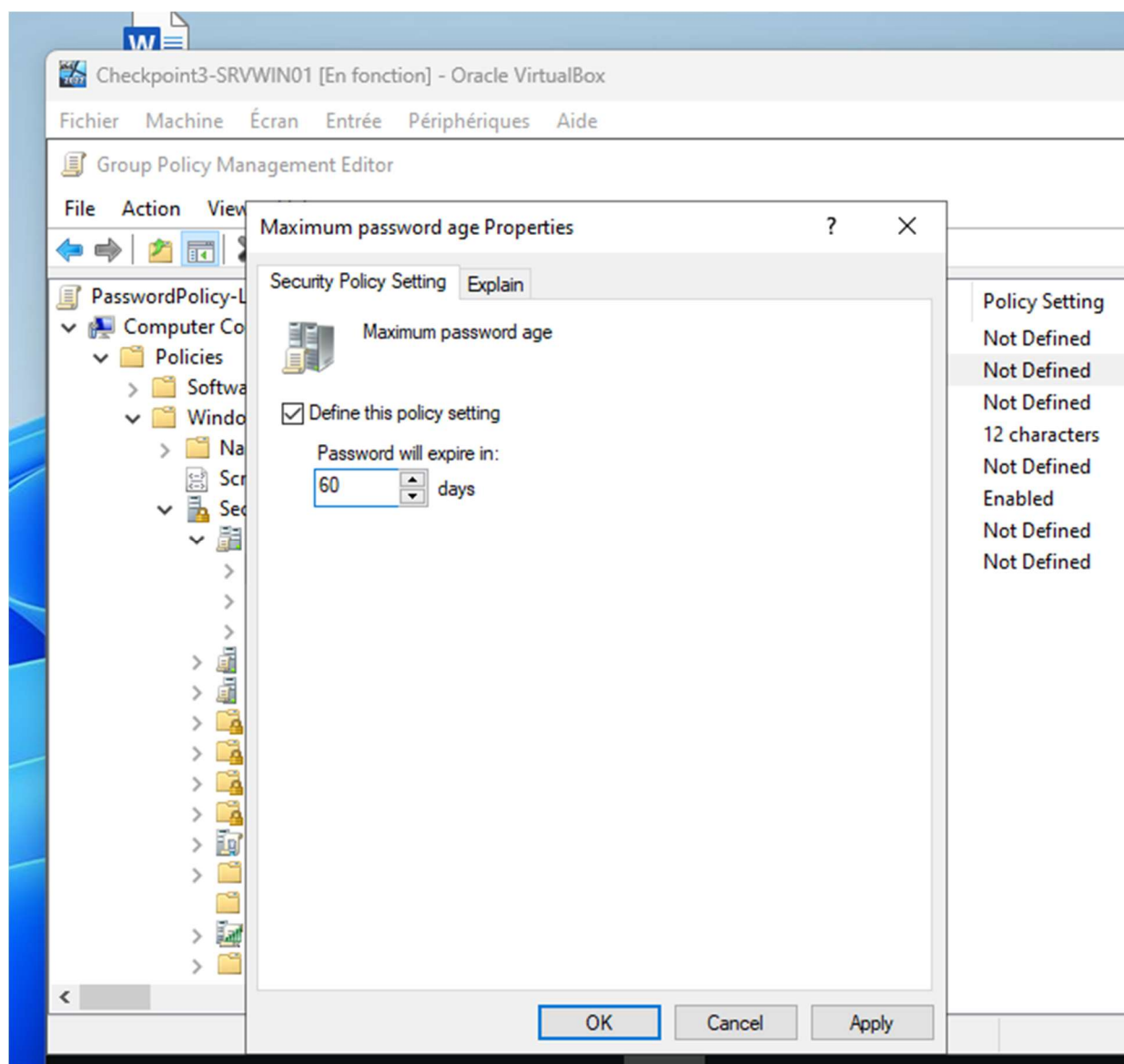


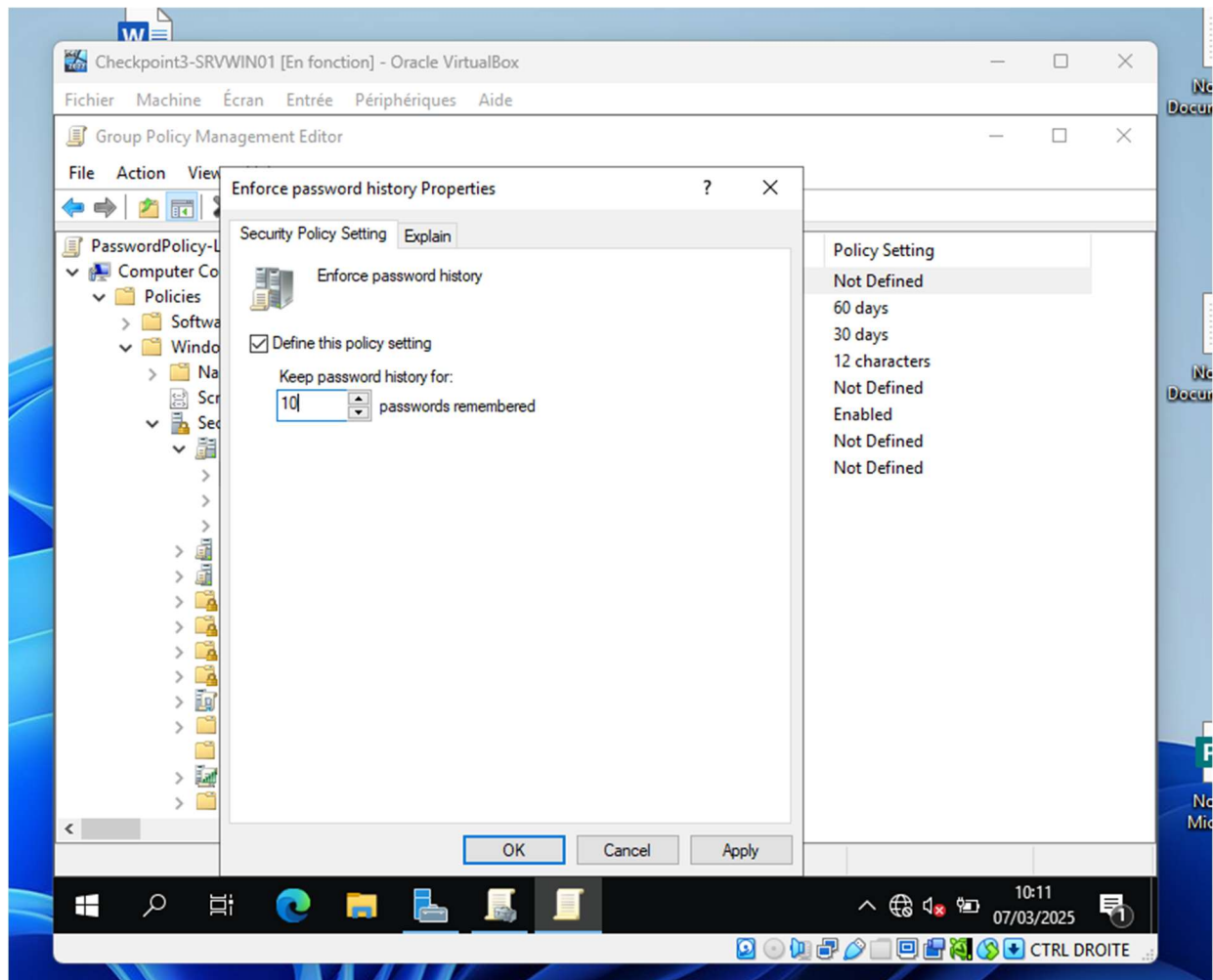
Q.1.2.3

- ▼  TSSR.LAN
 -  Default Domain Policy
 - >  Domain Controllers
 - >  LabComputers
 - ▼  LabUsers
 -  PasswordPolicy-Labusers
 - >  DeactivatedUsers
 - >  Discontin...





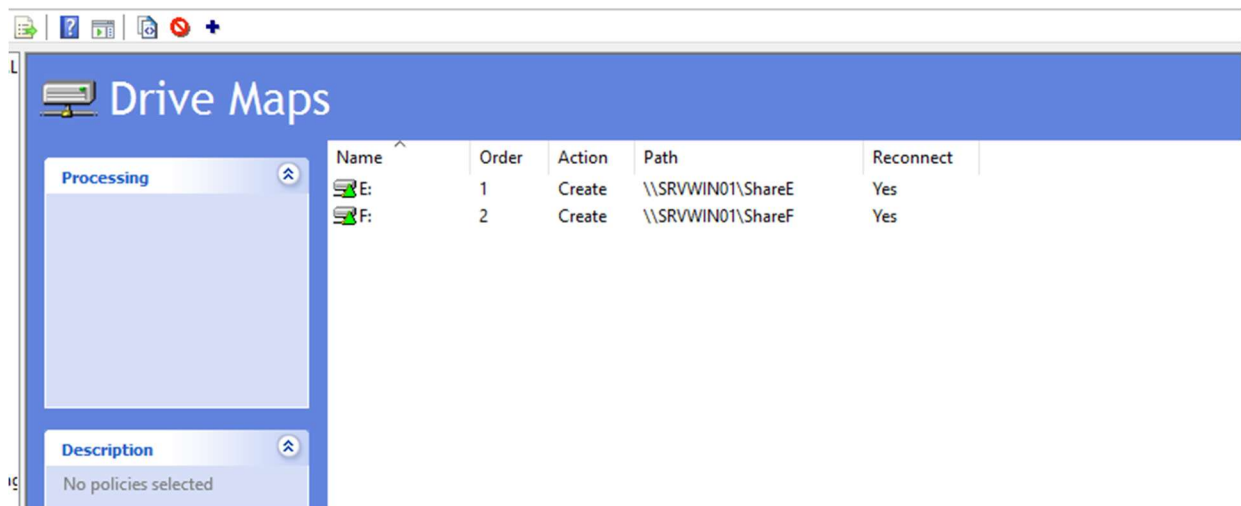




Pour finir on fait un
gpupdate /force
gpresult /r

Partie 3 - Lecteurs réseaux

Q.1.3.1



```
gpupdate /force
gpreresult /r
```

Exercice 2 - VM Linux

Partie 1 - Gestion des utilisateurs

Q.2.1.1

On commence par faire un apt update && apt upgrade -y

```
root@SRVLX01:~# adduser xavier
Ajout de l'utilisateur « xavier » ...
Ajout du nouveau groupe « xavier » (1001) ...
Ajout du nouvel utilisateur « xavier » (1001) avec le groupe « xavier » ...
Création du répertoire personnel « /home/xavier »...
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 xavier
Enter the new value, or press ENTER for the default
    Full Name []: xavierM
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
Cette information est-elle correcte ? [0/n]o
root@SRVLX01:~# _
```

Q.2.1.2

Pour ce compte on applique une politique de mot de passe fort

Droits limités : Ne pas ajouter l'utilisateur au groupe sudo sauf si nécessaire.

Accès SSH restreint : Limiter l'accès SSH à cet utilisateur spécifique.

Authentification par clé SSH : Désactiver l'authentification par mot de passe.

Partie 2 - Configuration de SSH

Q.2.2.1

```
root@SRVLX01:~# nano /etc/ssh/sshd_config
```

```
# Authentication:
#LoginGraceTime 2m
PermitRootLogin no_
#StrictModes yes
#MaxAuthTries 6
```

Q.2.2.2

```
root@SRVLX01:~# nano /etc/ssh/sshd_config
```

```
# ForceCommand cvs server
AllowUsers xavier_
```

[« AllowUsers » non trouvé]

Q.2.2.3

```
xavier@SRVLX01:~$ ssh-keygen -t rsa -b 4096
Generating public/private rsa key pair.
Enter file in which to save the key (/home/xavier/.ssh/id_rsa):
Created directory '/home/xavier/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/xavier/.ssh/id_rsa
Your public key has been saved in /home/xavier/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:6NPPmMy8/UFhcvaA+CLptZswYlwG13HIHwepCULF9D0 xavier@SRVLX01
The key's randomart image is:
+----[RSA 4096]-----+
|
|..+0...00
|.000+0...
|..0.0+E00 *
|0 .00.0 = +
| = S . . .
|. + + 0 .
| + * 0 .
|.. B 0 .
| X.+..
+----[SHA256]-----+
```

```
root@SRVLX01:~# nano /etc/ssh/sshd_config
```

```
# To disable tunneled clear text p
PasswordAuthentication no
#PermitEmptyPasswords no
```

```
PubkeyAuthentication yes_
```

Partie 3 - Analyse du stockage

Q.2.3.1

```
root@SRVLX01:/home/xavier# df -Th
Sys. de fichiers      Type      Taille Utilisé Dispo Uti% Monté sur
udev                  devtmpfs  470M      0   470M   0% /dev
tmpfs                 tmpfs     98M      600K   98M    1% /run
/dev/mapper/cp3--vg-root ext4      2,7G    1,6G  1008M   61% /
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/1001
root@SRVLX01:/home/xavier# _
```

Q.2.3.2

```

root@SRVLX01:/home/xavier# lsblk -f
NAME                                FSTYPE FSVER LABEL UUID                                 FSAVAIL FSUSE% MOUNTPOINT
sda
├─ sda1                             linux_  1.2   cp3:0 323332561-cf16-c858-7035-17e881dd5c10
│   └─ md0
│       ├─ md0p1                    ext2    1.0     9bba6d48-3e4b-42a6-bccc-12836de215ec    397,3M    10% /boot
│       ├─ md0p2
│       └─ md0p5                    LVM2_m  LVM2     t1CGJ2-LG5u-kWgc-8ku0-wAiU-icBu-07BEcN
│           ├─ cp3--vg-root          ext4    1.0     bbc31a37-8e49-47fe-8fad-a3fe18919fdd    1007,9M    57% /
│           └─ cp3--vg-swap_1        swap    1        8220bf51-2675-4203-91af-1c149f717652
│                                   [SWAP]
sr0
root@SRVLX01:/home/xavier#

```

Ce système utilise donc une combinaison de **RAID logiciel (md0)**, **LVM pour la gestion des volumes**, et **des partitions temporaires en tmpfs/devtmpfs**.

Q.2.3.3

```

root@SRVLX01:~# mdadm --add /dev/md0 /dev/sdb
mdadm: added /dev/sdb
root@SRVLX01:~# cat /proc/mdstat
Personalities : [raid1] [linear] [multipath] [raid0] [raid6] [raid5] [raid4] [raid10]
md0 : active raid1 sdb[2] sda1[0]
      8381440 blocks super 1.2 [2/1] [U_]
      [===>.....] recovery = 23.1% (1939008/8381440) finish=0.7min speed=149154K/sec

unused devices: <none>

```

Q.2.3.4

Créer une partition sur le disque

```

fdisk /dev/sdc
n nouvelle partiton
Primaire
Type : 8e lvm
W valider

```

Créer le volume physique
 pvcreate /dev/sdc1

Trouver le nom de la VG
 vgdisplay pour savoir le nom du VG

Ajouter au groupe de volumes
 vgextend cp3-vg /dev/sdc1

Créer le volume logique

```
lvcreate -L 2G -n backup_lv cp3-vg
```

Formater et monter automatiquement
 sudo mkfs.ext4 /dev/cp3-vg/backup_lv sudo mkdir -p /var/lib/bareos/storage echo
 "/dev/cp3-vg/backup_lv /var/lib/bareos/storage ext4 defaults 0 2" | tee -a
 /etc/fstab sudo mount -a

Q.2.3.5

```
VG SIZE          <3,51 GiB
PE Size          4,00 MiB
Total PE         2434
Alloc PE / Size  1465 / 5,72 GiB
Free PE / Size   969 / <3,79 GiB
VG UUID          BMardR-vL06-CToa-ad0f-XVh0-0DeS-cX70bt
root@SRVLX01:~#
```

Partie 4 - Sauvegardes

Q.2.4.1

```
ls -l /etc/bareos/
```

Explication des composants Bareos

bareos-dir (Director) : Gère les sauvegardes, planifications et restaurations.

bareos-sd (Storage Daemon) : Stocke et gère les fichiers sauvegardés.

bareos-fd (File Daemon) : Installe sur les machines clientes, envoie les fichiers au serveur.

Partie 5 - Filtrage et analyse réseau

Q.2.5.1

```
root@SRVLX01:~# 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

- Trafic correspondant à des connexions déjà établies ou reliées (ct state established,related)
- Tout trafic sur l'interface loopback (iifname "lo")
- Connexions entrantes sur le port TCP 22 (SSH)
- Protocole ICMP (pings et autres messages de diagnostic réseau IPv4)
- Protocole ICMPv6 (version IPv6 des pings et messages de diagnostic réseau)

Q.2.5.3

D'après la sortie de nftables, les types de communications interdites sont:

1. Trafic avec un état de connexion "INVALID" (ct state invalid drop)
2. Tout autre trafic entrant qui ne correspond pas aux règles spécifiquement autorisées (en raison de la politique par défaut "policy drop" sur la chaîne d'entrée)

Q.2.5.4

Déterminez d'abord l'interface réseau et l'adresse du réseau local :

```
ip a
```

ip route

Ajouter les règles nécessaires pour autoriser Bareos

```
root@SRVLX01:~# nft add rule inet inet_filter_table in_chain ip saddr 192.168.1.0/24 tcp dport {9101, 9102, 9103} accept
```

```
root@SRVLX01:~# nft add rule inet inet_filter_table in_chain_t ip saddr 192.168.1.0/24 tcp dport {9101, 9102, 9103} accept
```

```
root@SRVLX01:~# 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
        ip saddr 192.168.1.0/24 tcp dport { 9101, 9102, 9103 } accept
        ip6 saddr fe80::/10 tcp dport { 9101, 9102, 9103 } accept
    }
}
```

Partie 6 - Analyse de logs

Q.2.6.1

J'ai testé cette commande

```
grep "Failed password" /var/log/auth.log | tail -n 10 | awk '{print $1, $2, $3, $11}'
```

mais rien ne sort en résultats

```
root@SRVLX01:/var/log# ls
alternatives.log      bareos          debug           faillog         lastlog         syslog
alternatives.log.1    btmp            debug.1         fichierlog.txt  messages        syslog.1
alternatives.log.2.gz btmp.1          debug.2.gz      installer       messages.1       syslog.2.gz
apt                   daemon.log      debug.3.gz      journal         messages.2.gz   syslog.3.gz
auth.log              daemon.log.1    debug.4.gz      kern.log        messages.3.gz   syslog.4.gz
auth.log.1            daemon.log.2.gz dpkg.log        kern.log.1      messages.4.gz   sysstat
auth.log.2.gz         daemon.log.3.gz dpkg.log.1      kern.log.2.gz  postgresql      user.log
auth.log.3.gz         daemon.log.4.gz dpkg.log.2.gz   kern.log.3.gz  private         wtmp
auth.log.4.gz         dbconfig-common exim4           kern.log.4.gz  runit
root@SRVLX01:/var/log# cd faillog
bash: cd: faillog: N'est pas un dossier
```

Il y a plusieurs auth.log

ok : /24

nr :

faux :