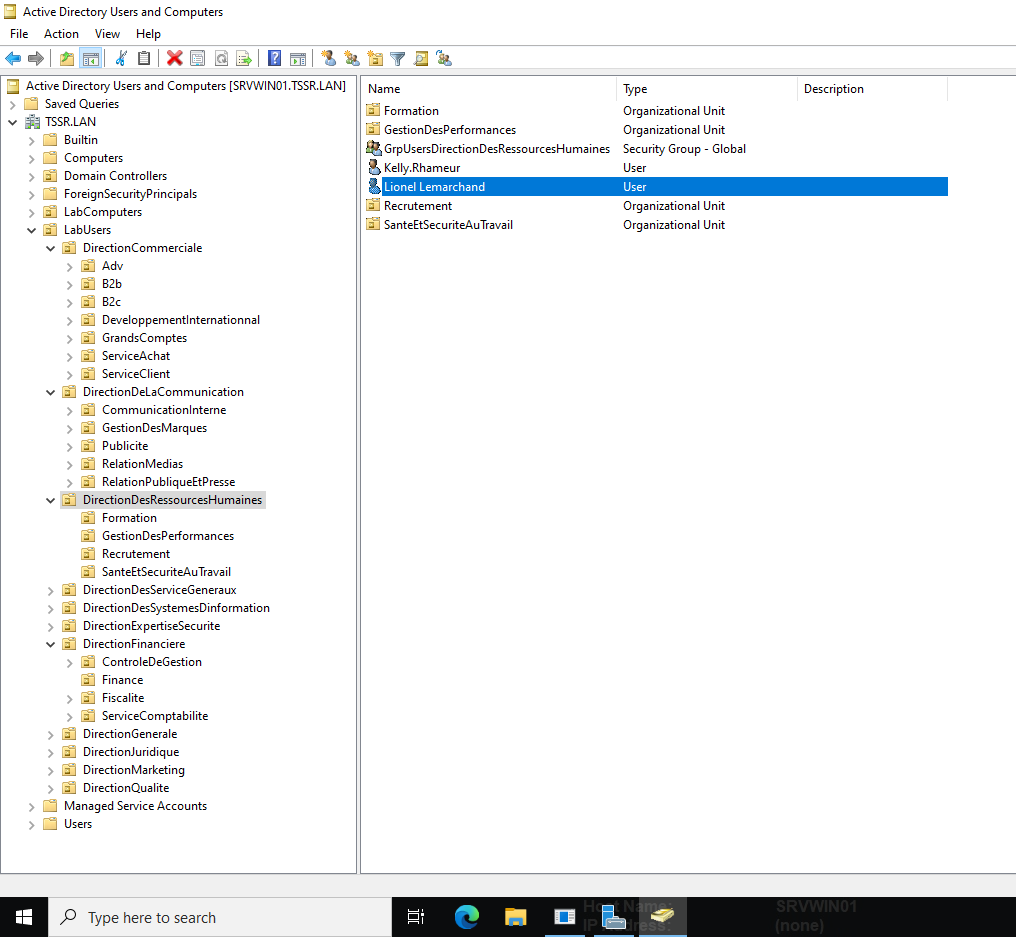
Exercice 1 - VM Windows

Partie 1 - Gestion des utilisateurs

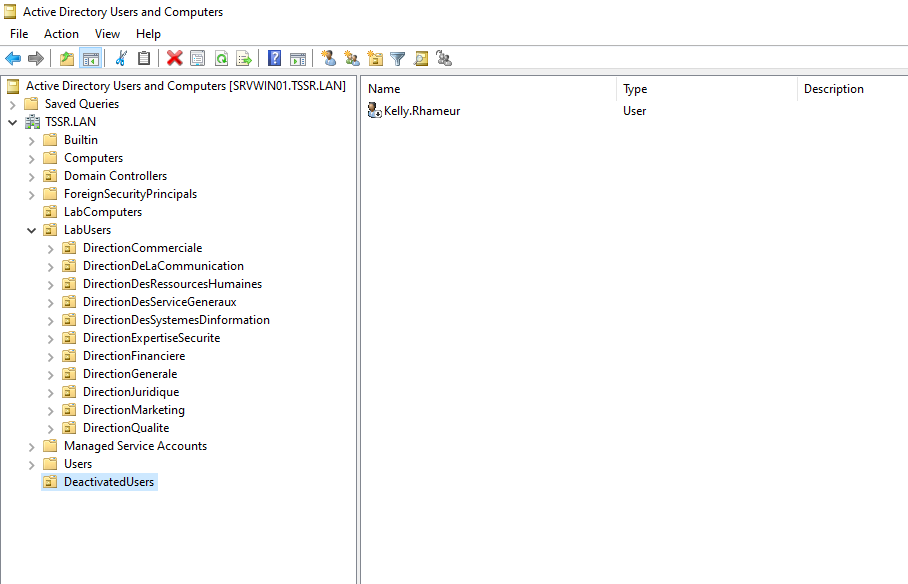
Q.1.1.1

* J'ouvre la console Active Directory Users and Computers en appuiant sur **Windows+r** et avec la comamnde **dsa.msc**.
* Dans l'OU où se trouve Kelly Rhameur, *Direction des Ressources Humaines*, je fais un clic droit sur Kelly Rhameur et je copie son profile.
* Je rensigne les informations de Lionel Lemarchand et en suite en cliquant sur **Next** je définis son mot de passe. Je verifie les informations et je clique sur **OK**.

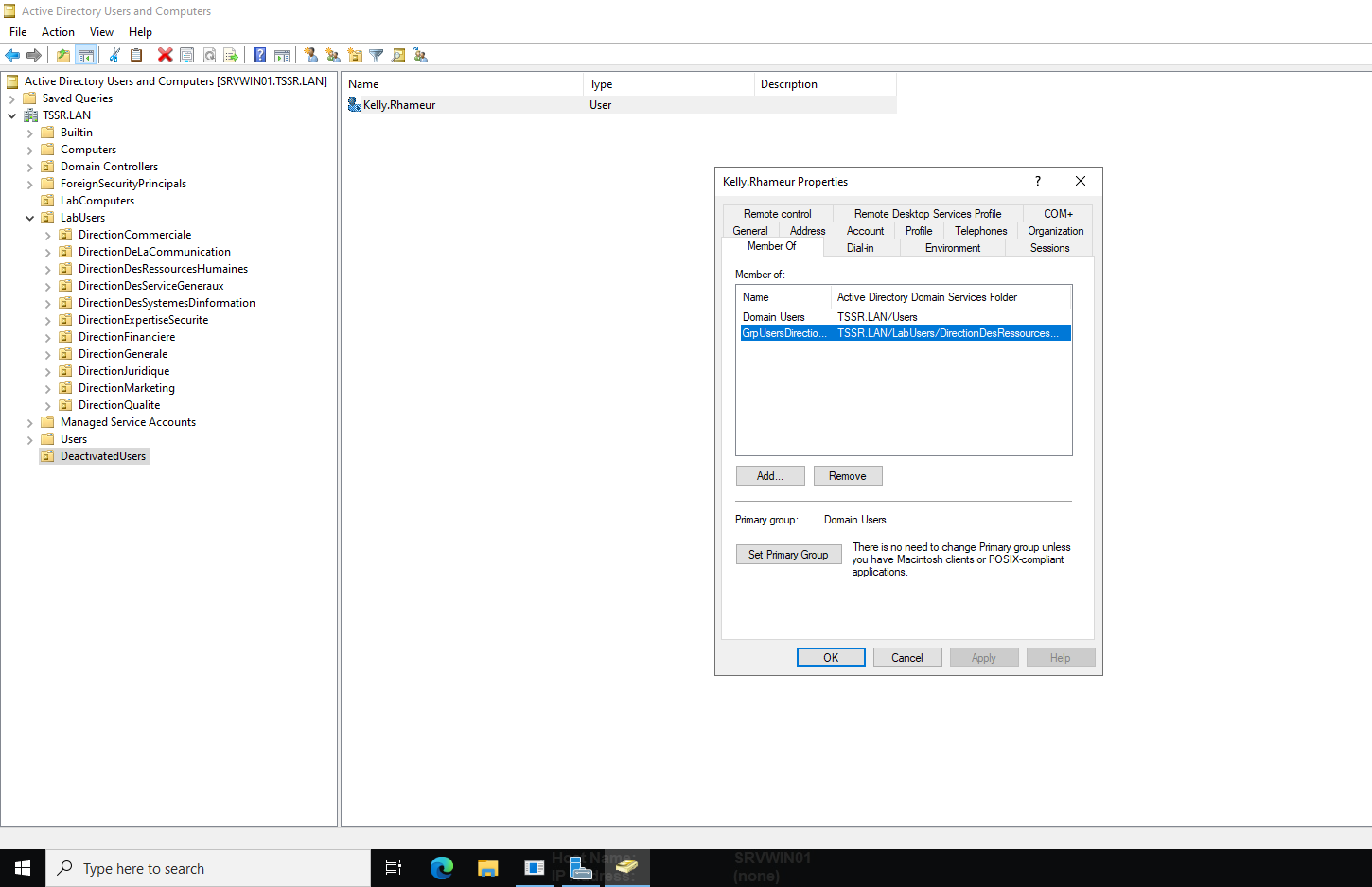


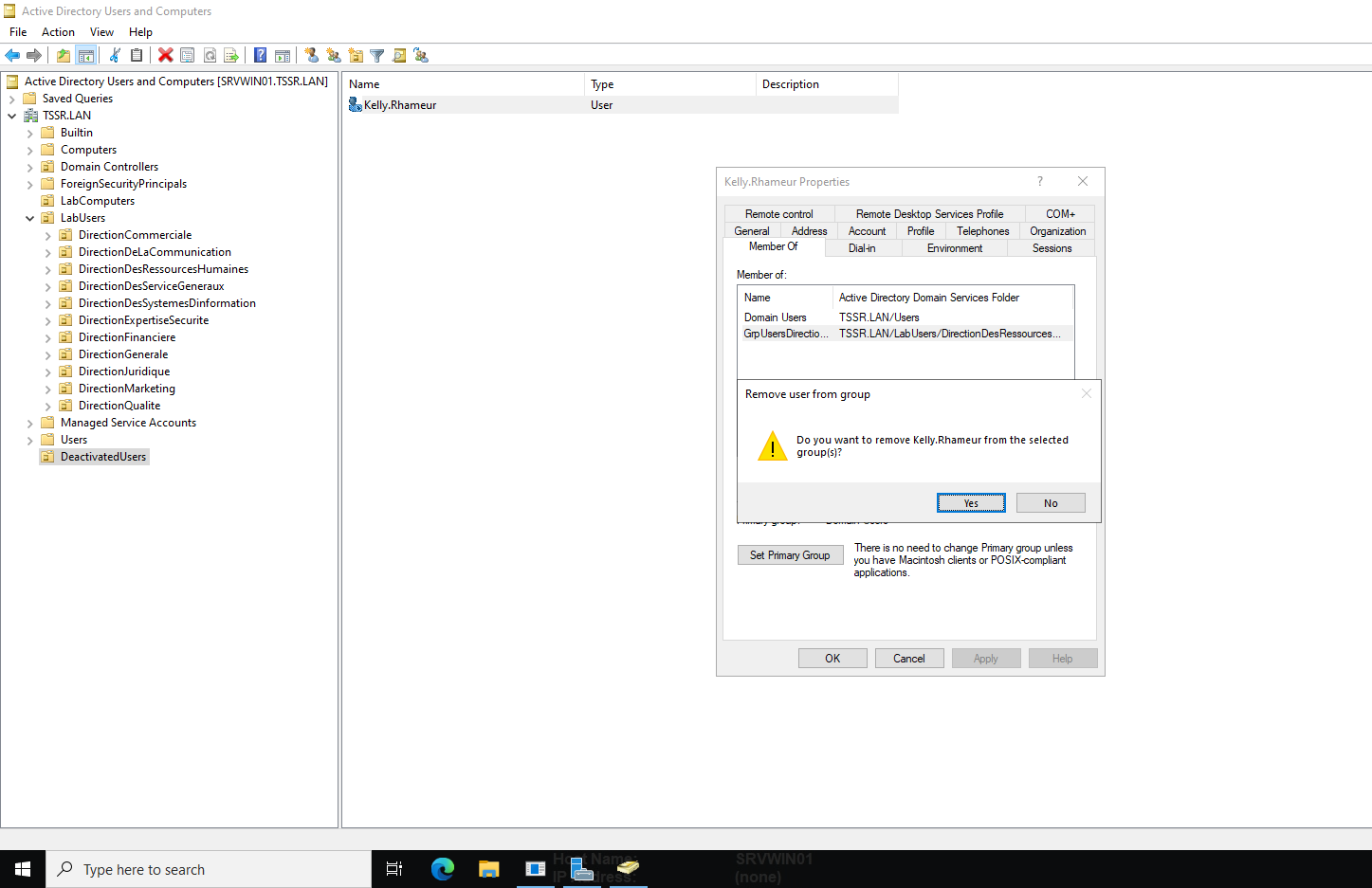
Q.1.1.2

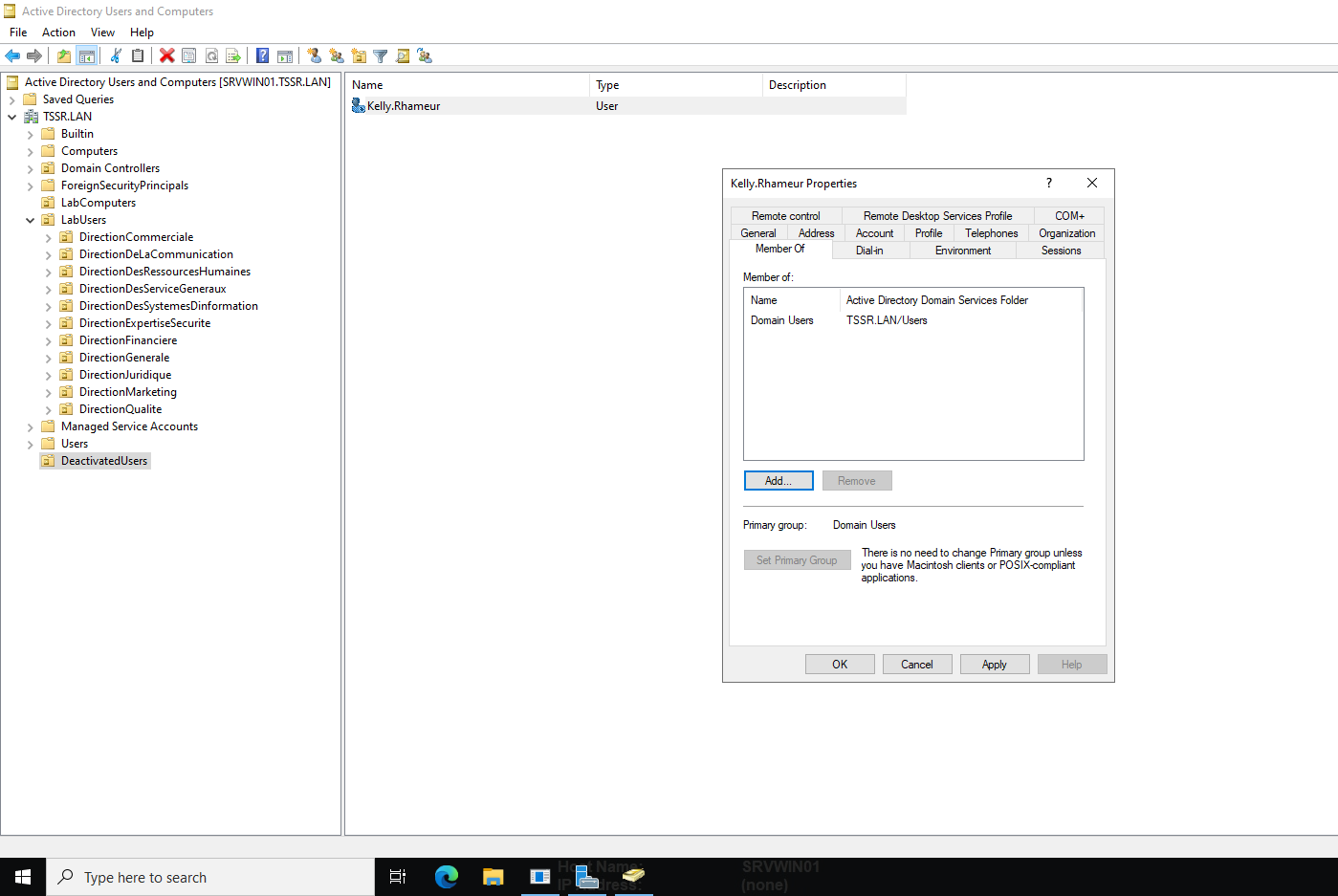
* Dans Active Directory Users and Computer, je sélectionne TSSR.LAN, je fais un clic droit et je sélectionne **New** 🡪 **Organisational Unit** et je l’appelle **DeactivatedUsers.**
* Je retourne sur le compte de Kelly Rhameur, je fais un clic droit sur son compte et je sélectionne **Disable Account**.
* Je refais un clic droit sur le compte de Kelly Rhameur, je sélectionne **Move** et je déplace le compte dan OU **DeactivatedUsers**.



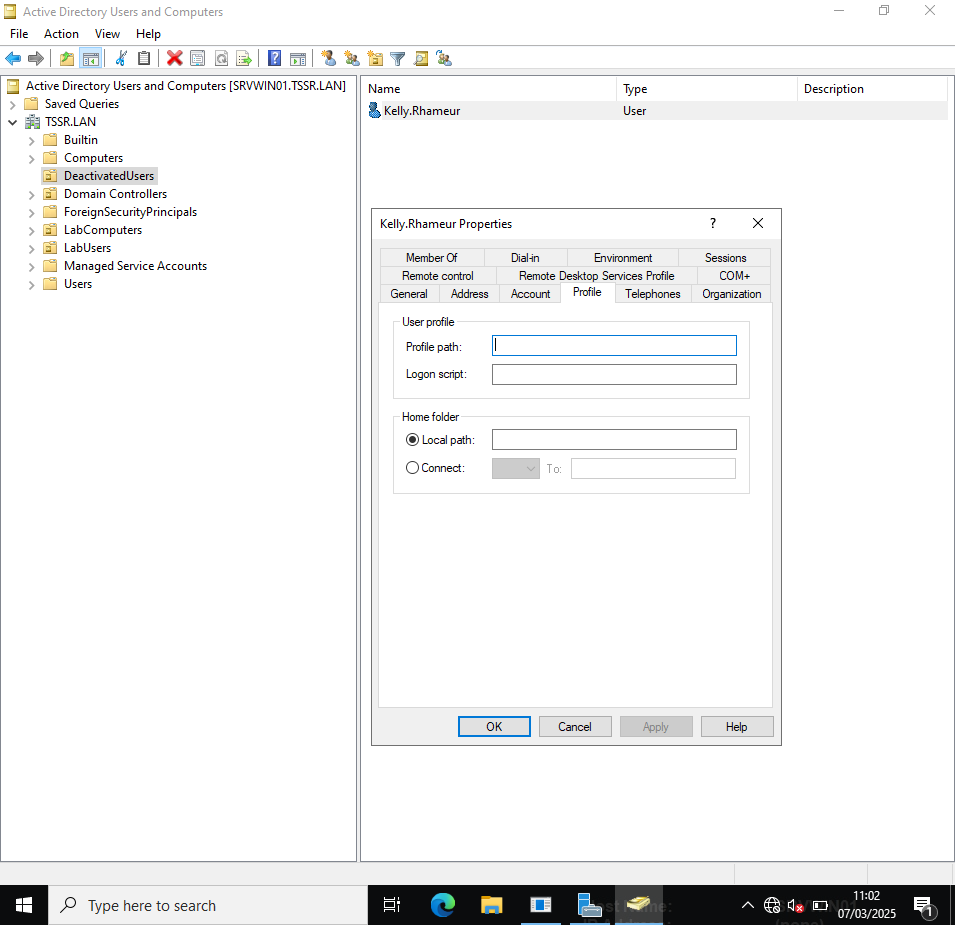
Q.1.1.3

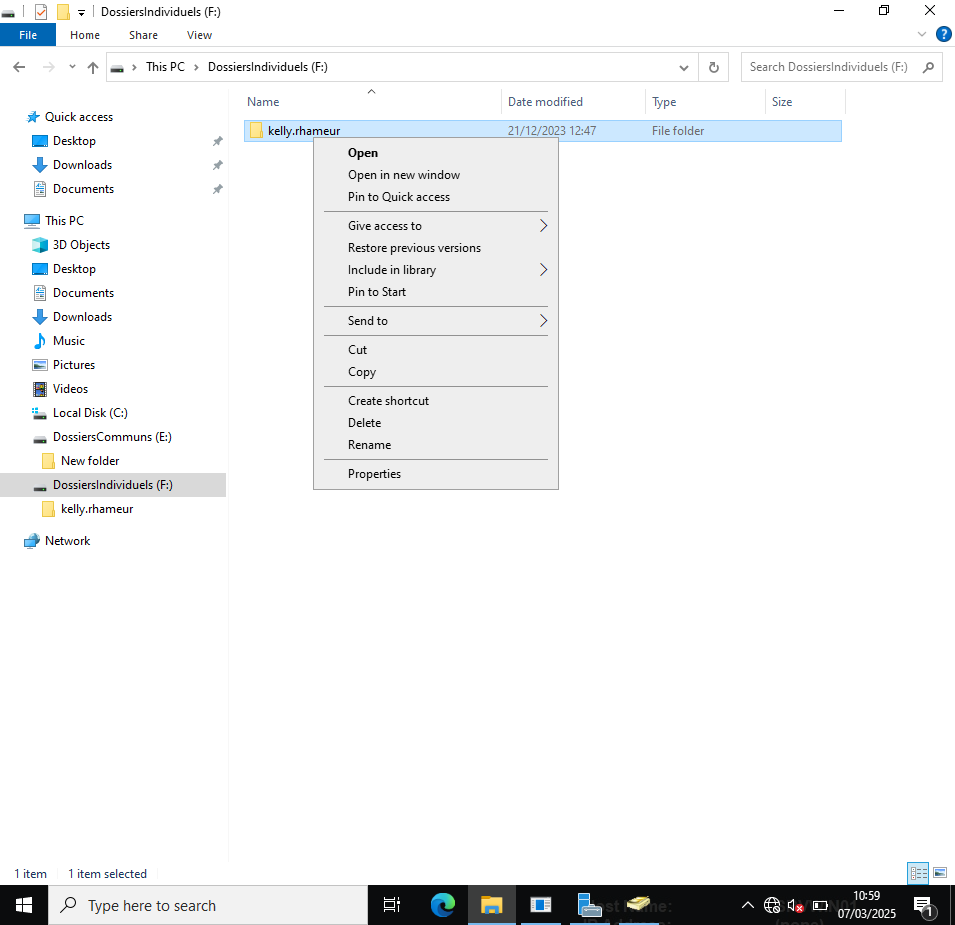


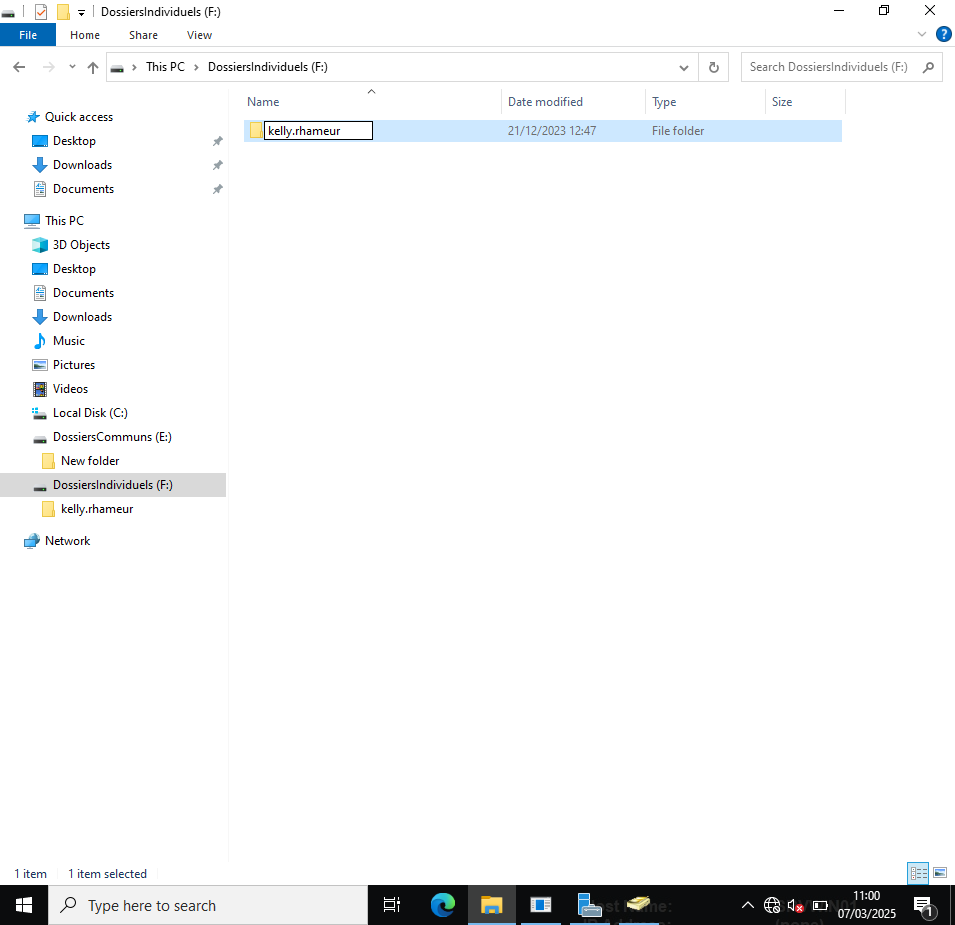


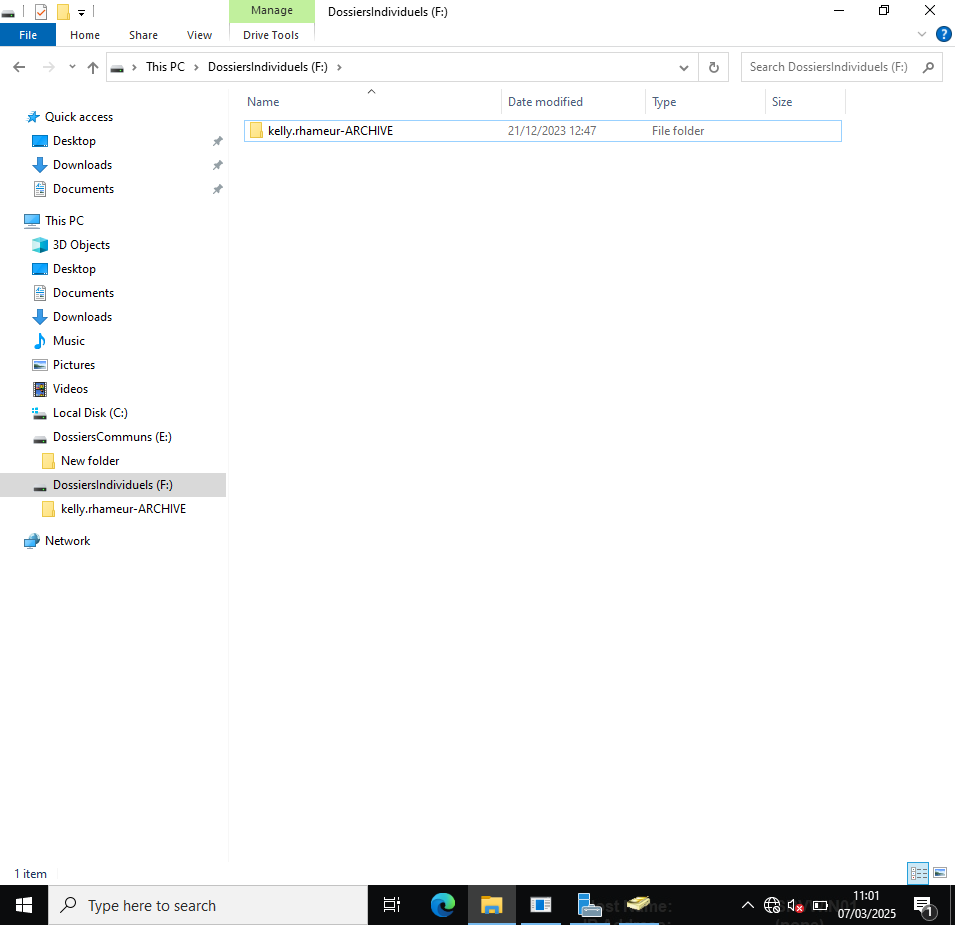


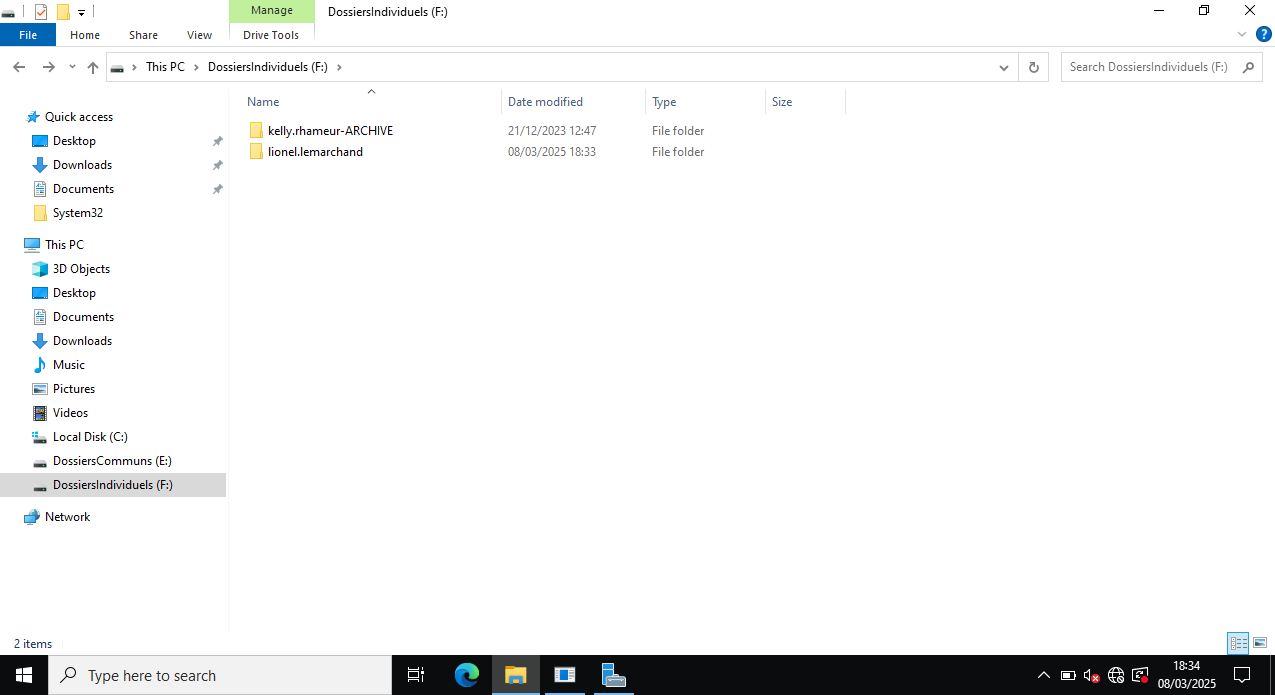
Q.1.1.4





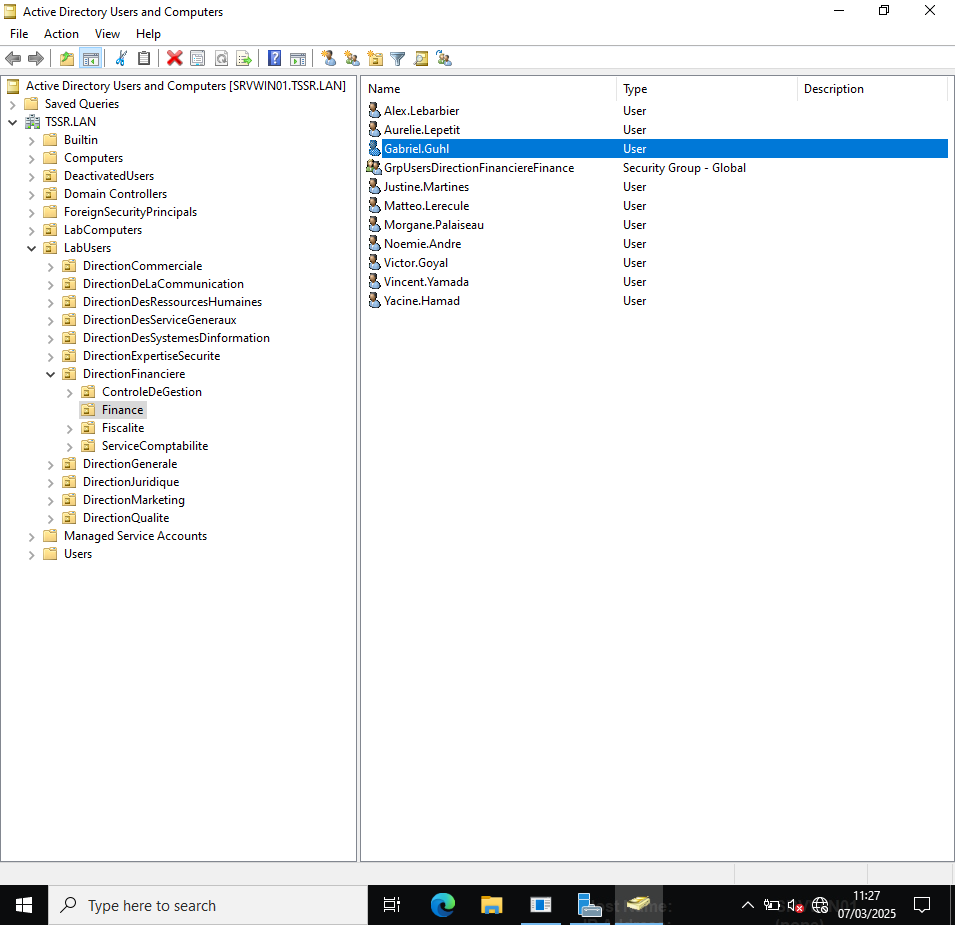


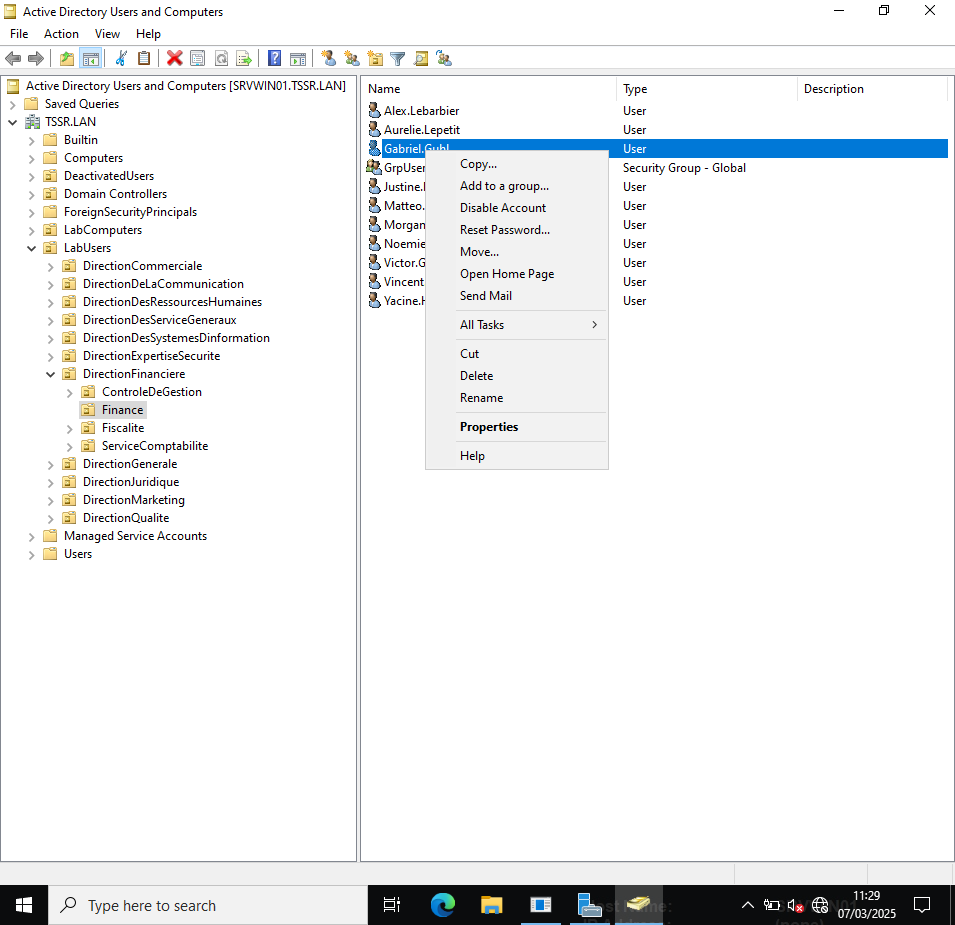


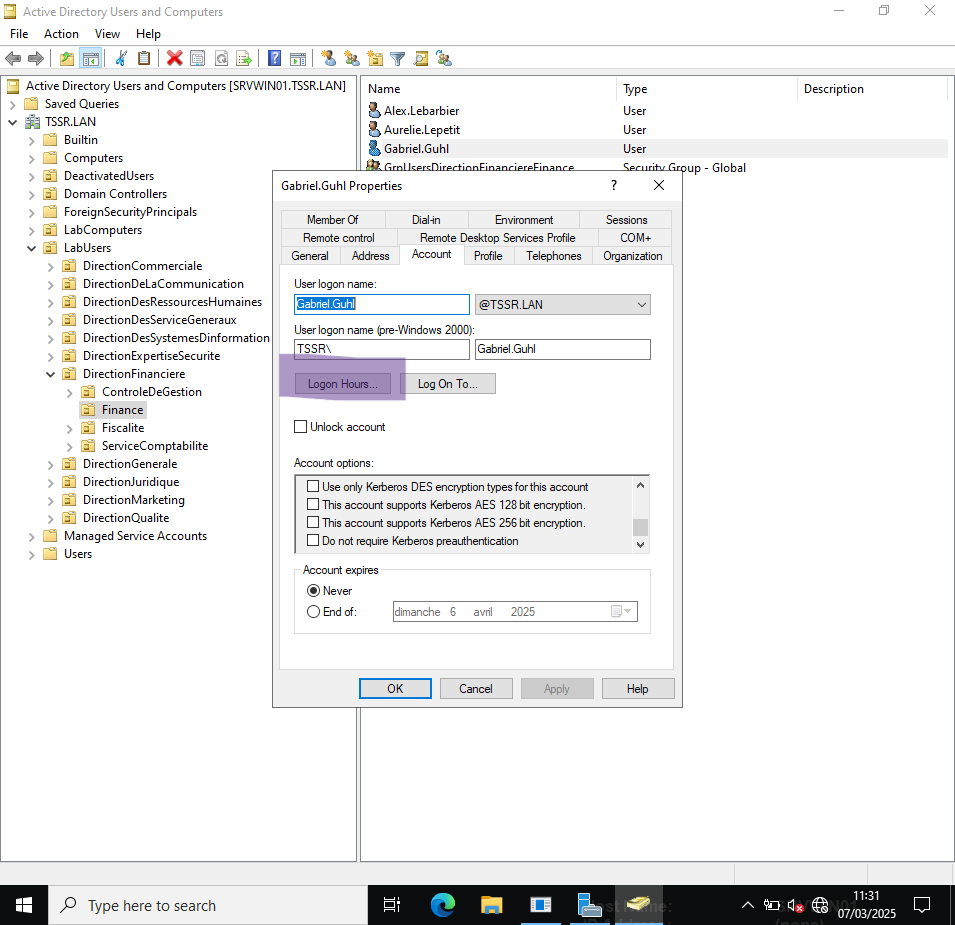


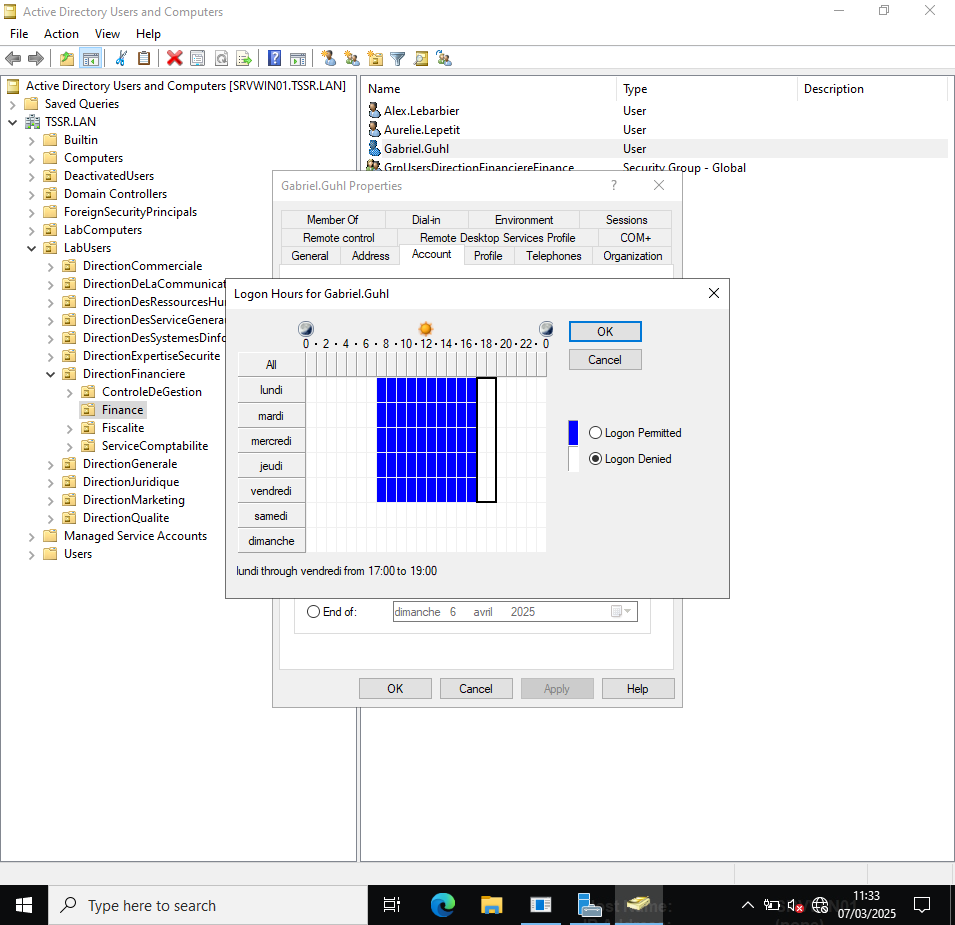
Partie 2 - Restriction utilisateurs

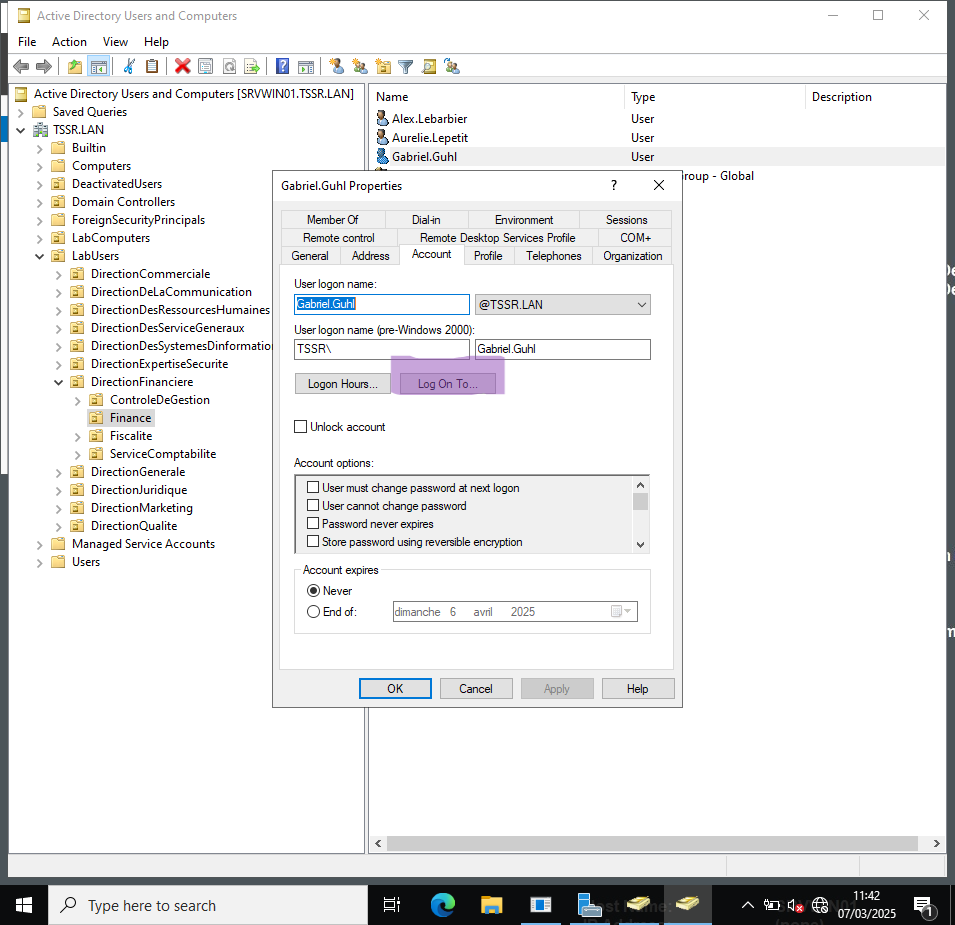
Q.1.2.1

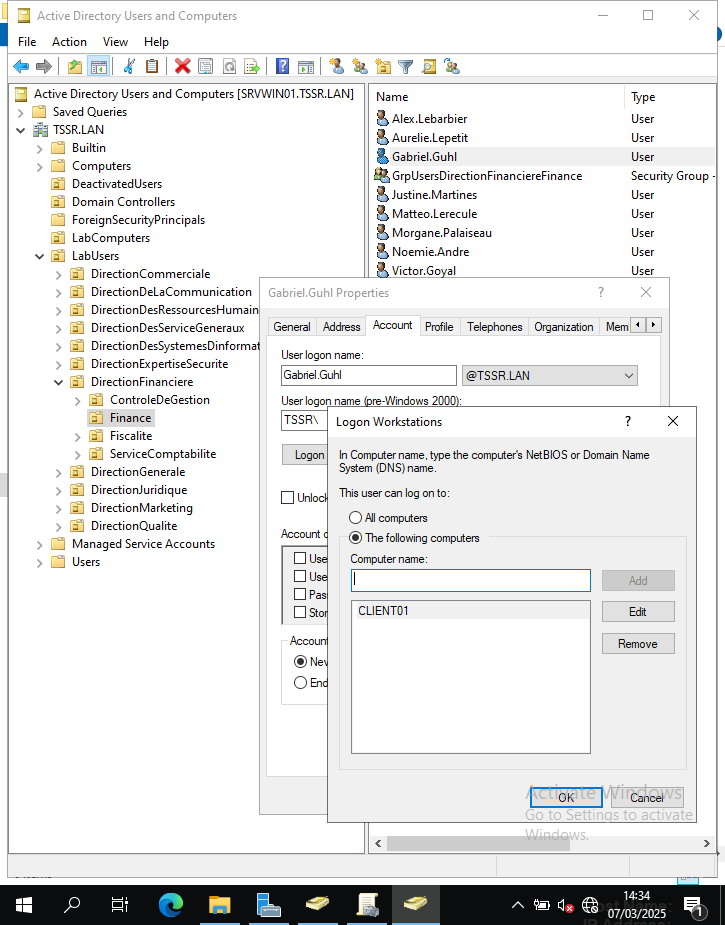




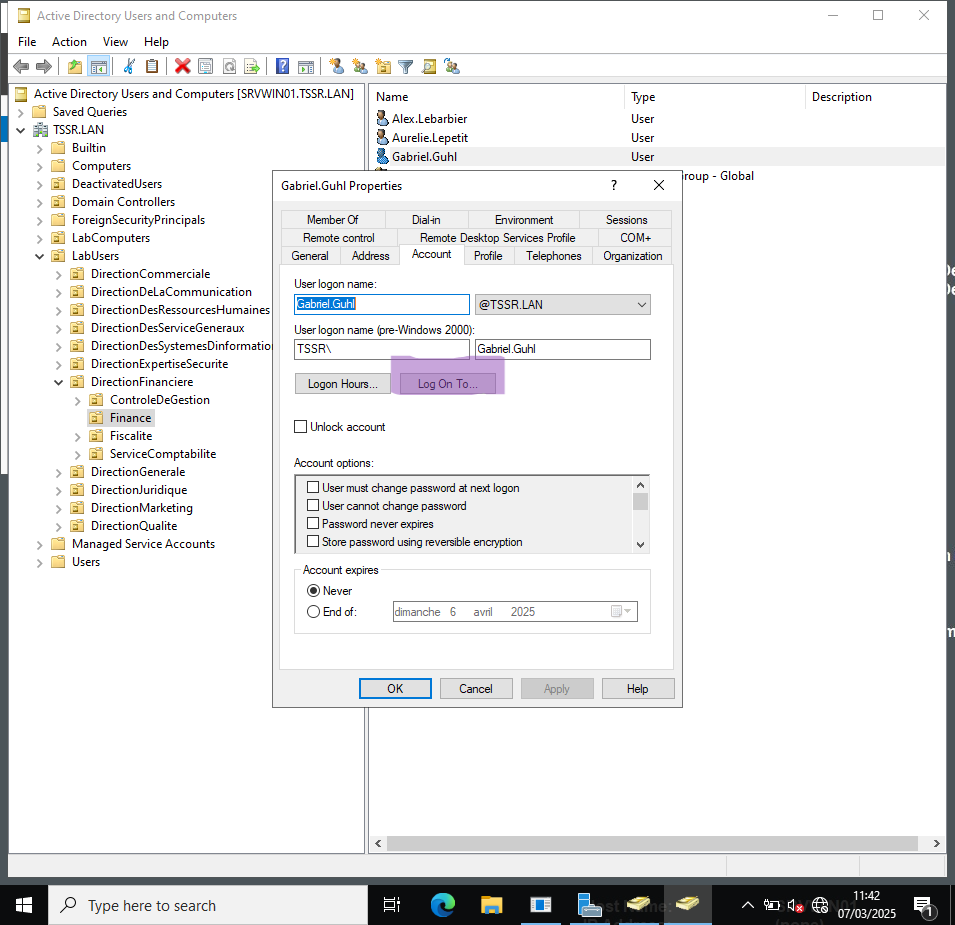


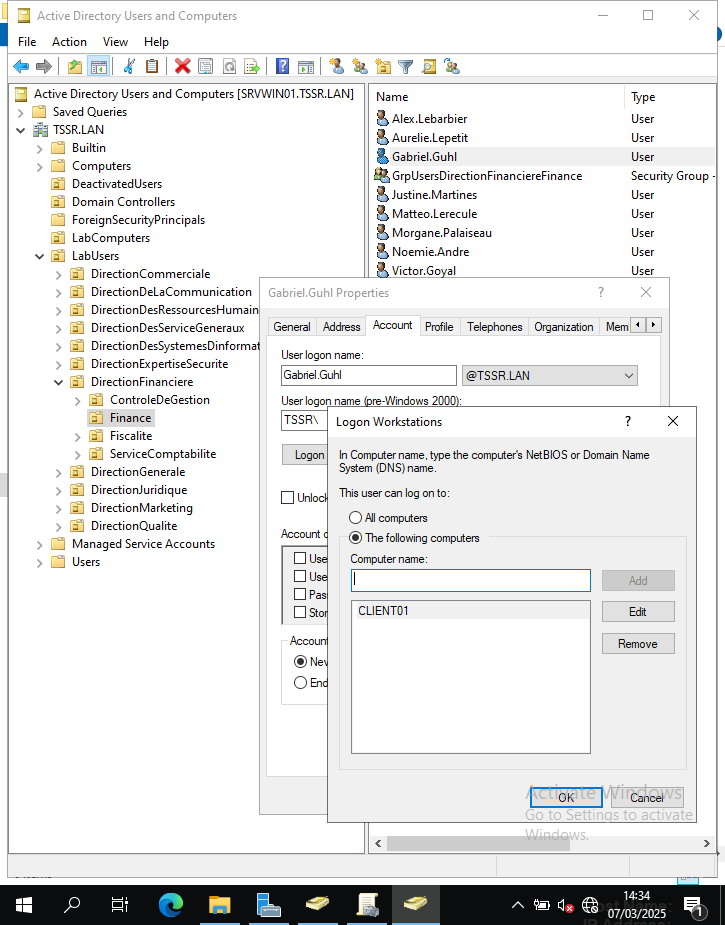




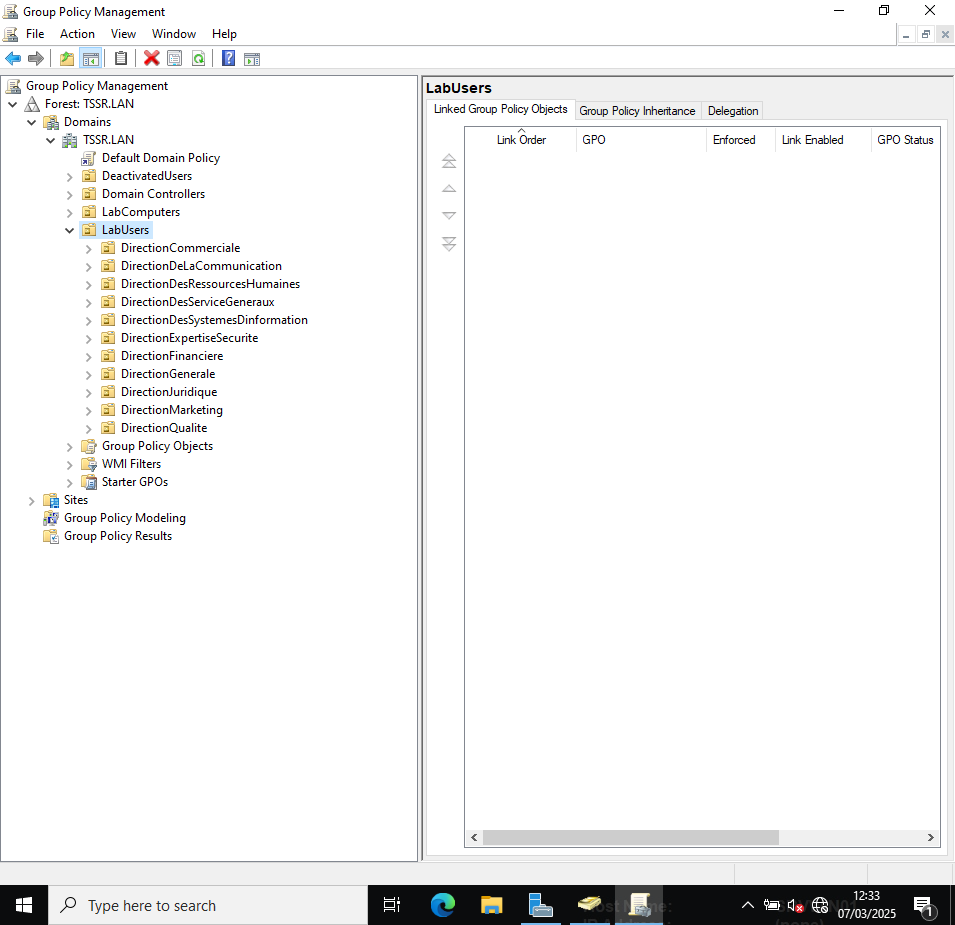


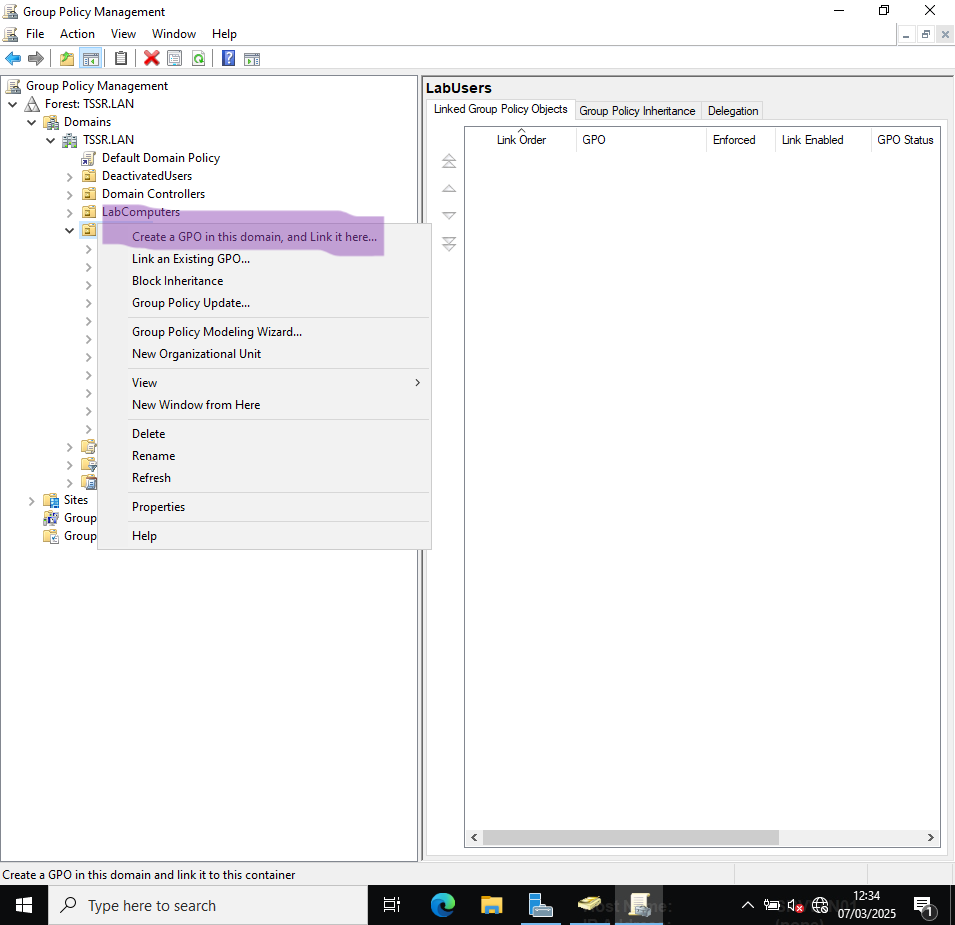
Q.1.2.2

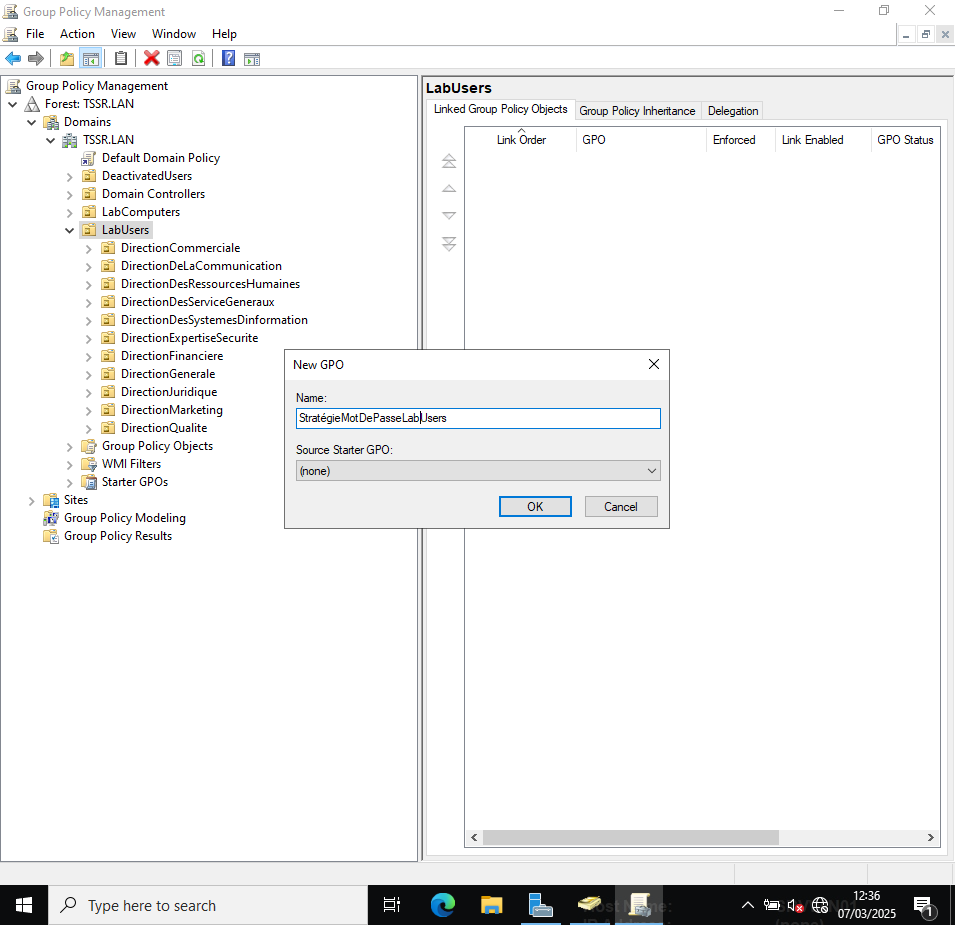


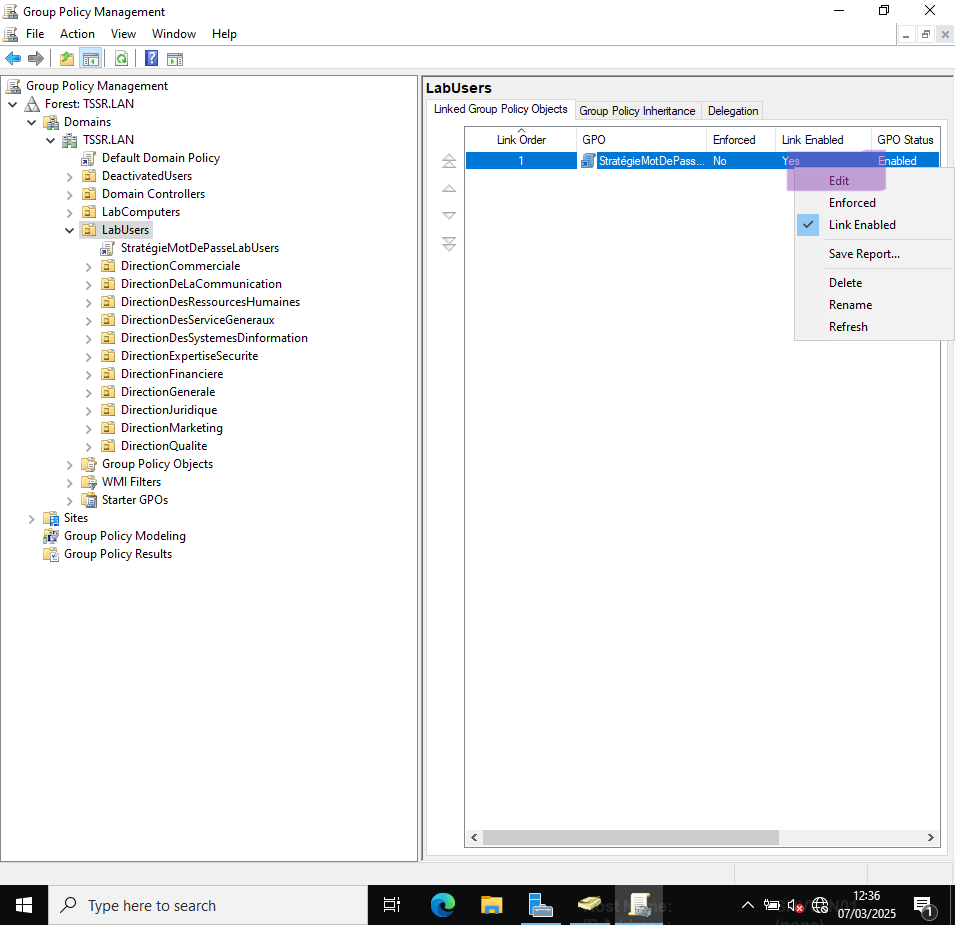


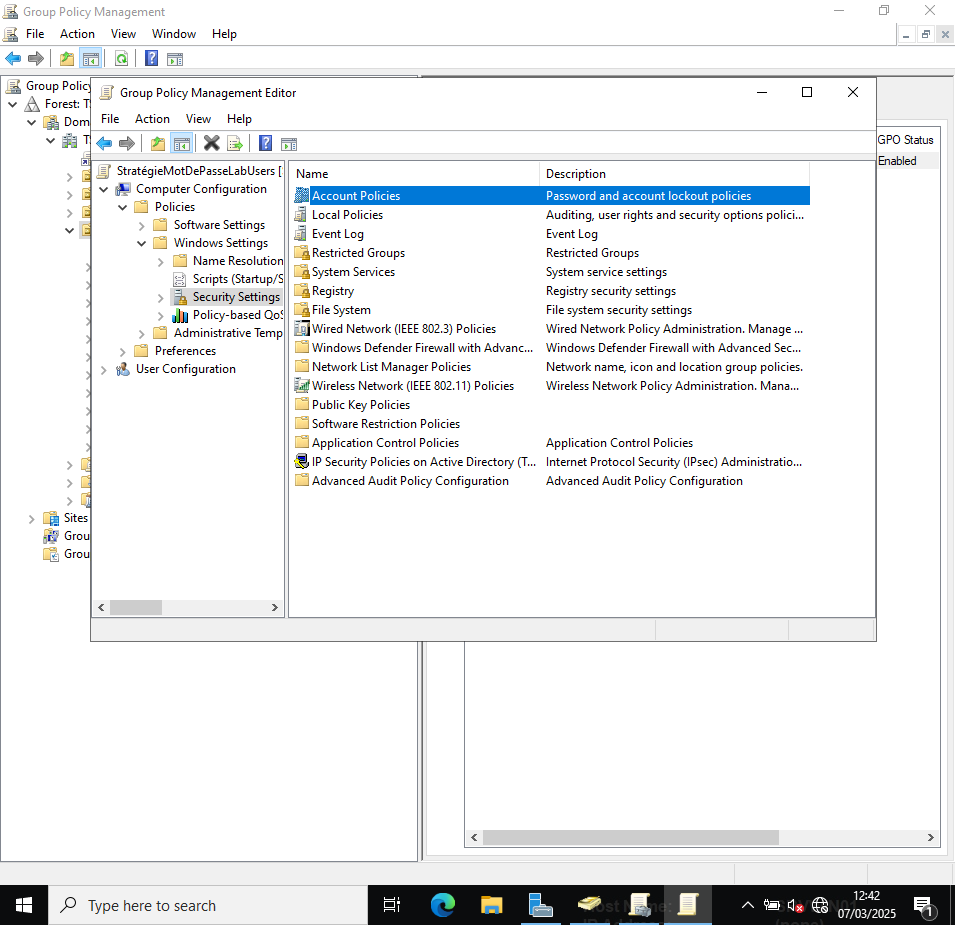
Q.1.2.3

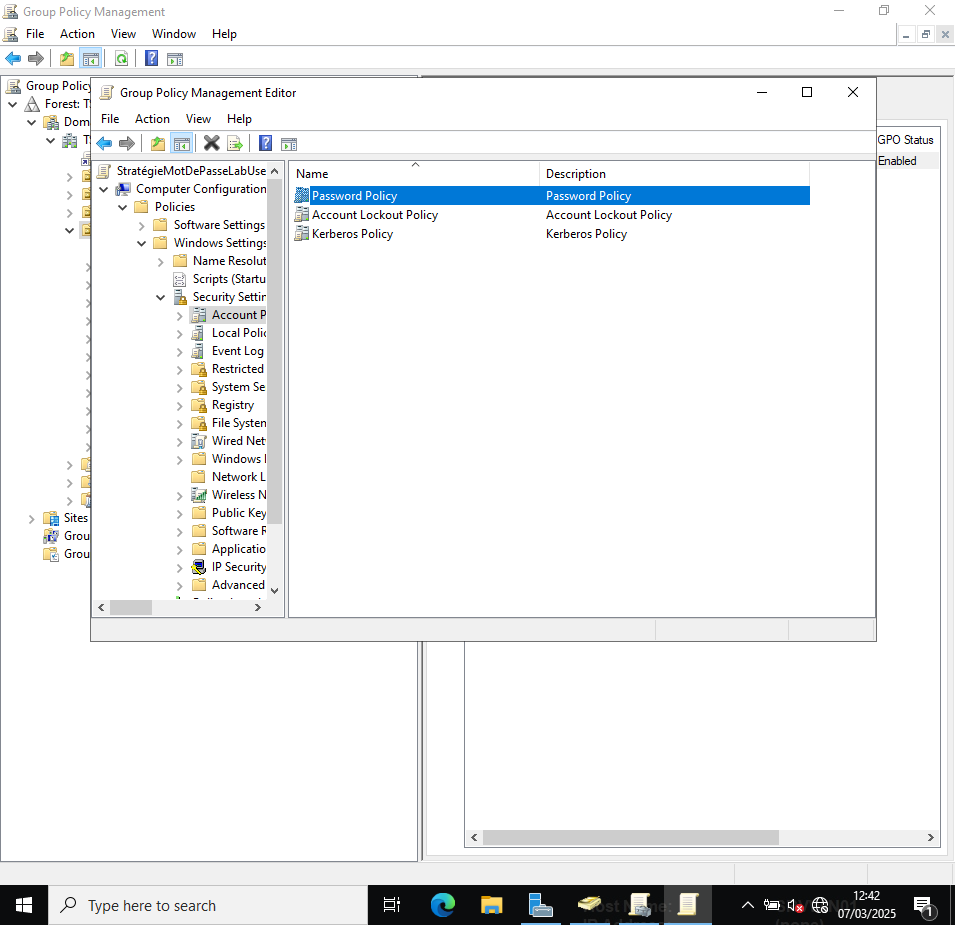


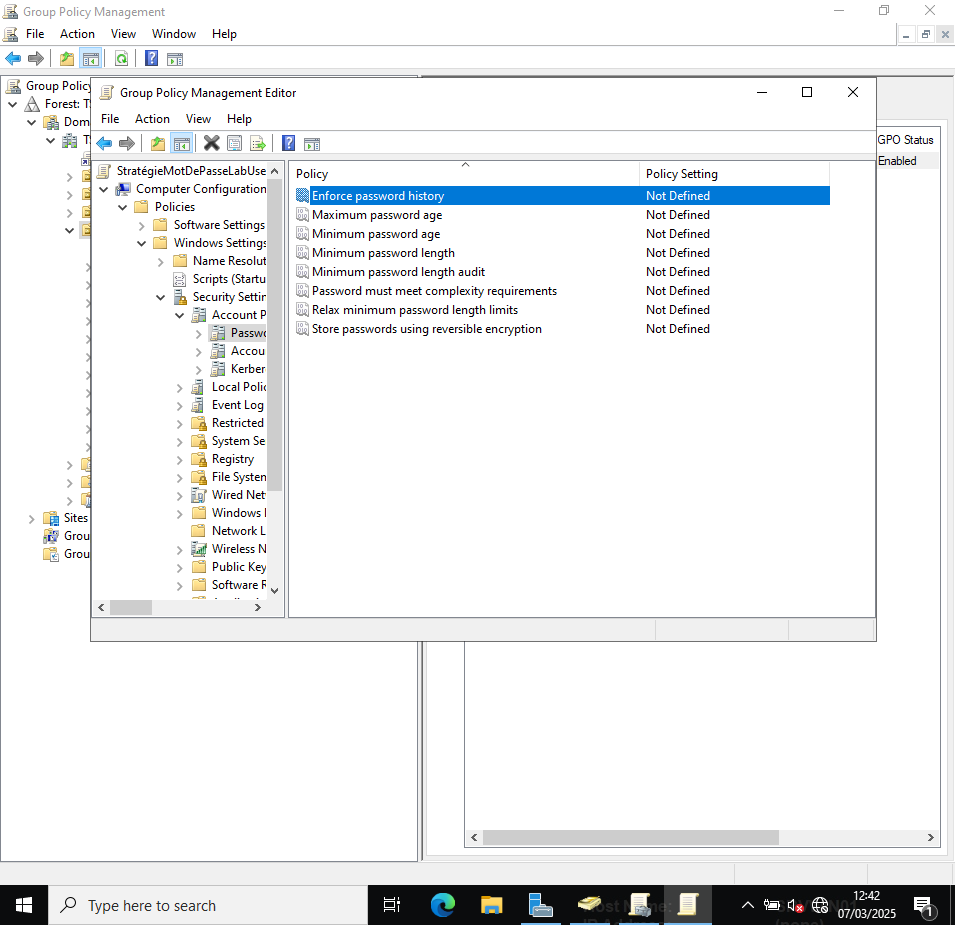


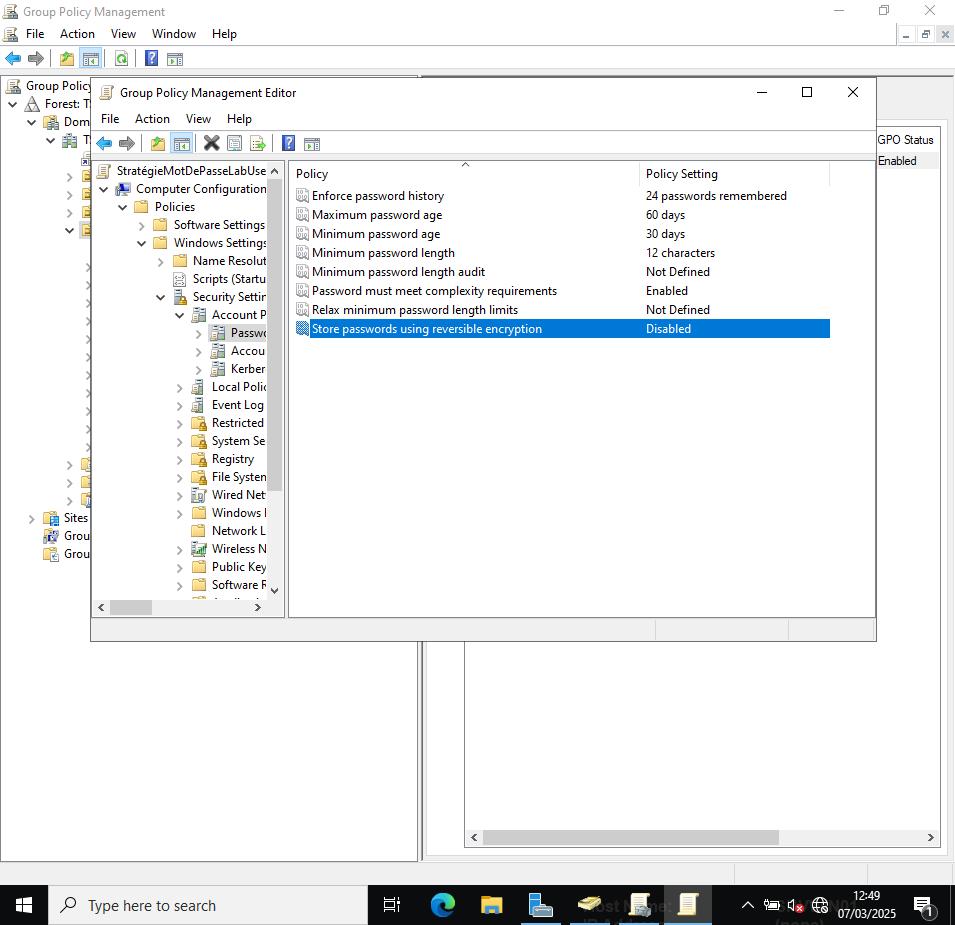






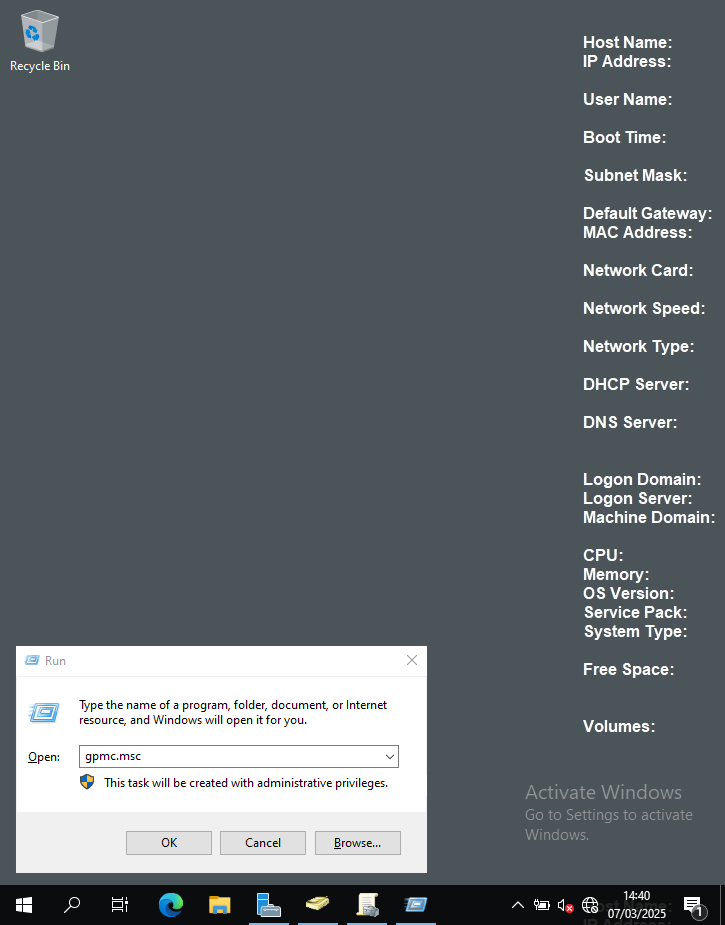


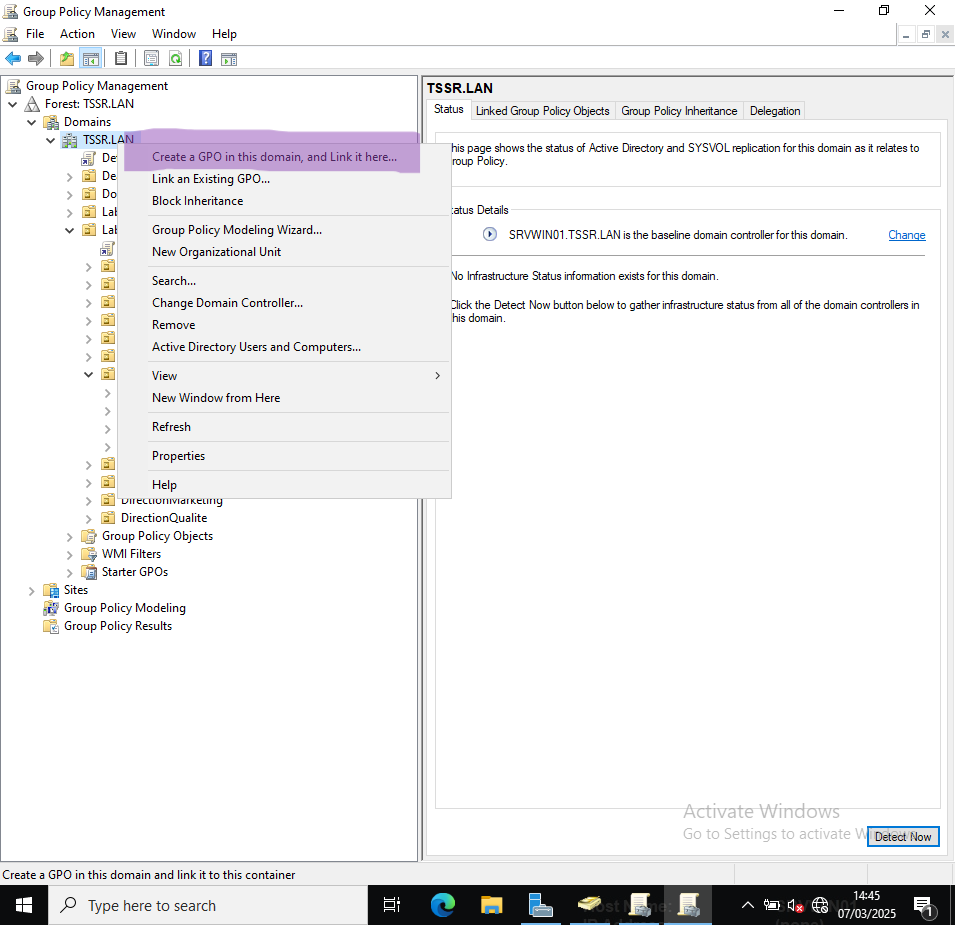


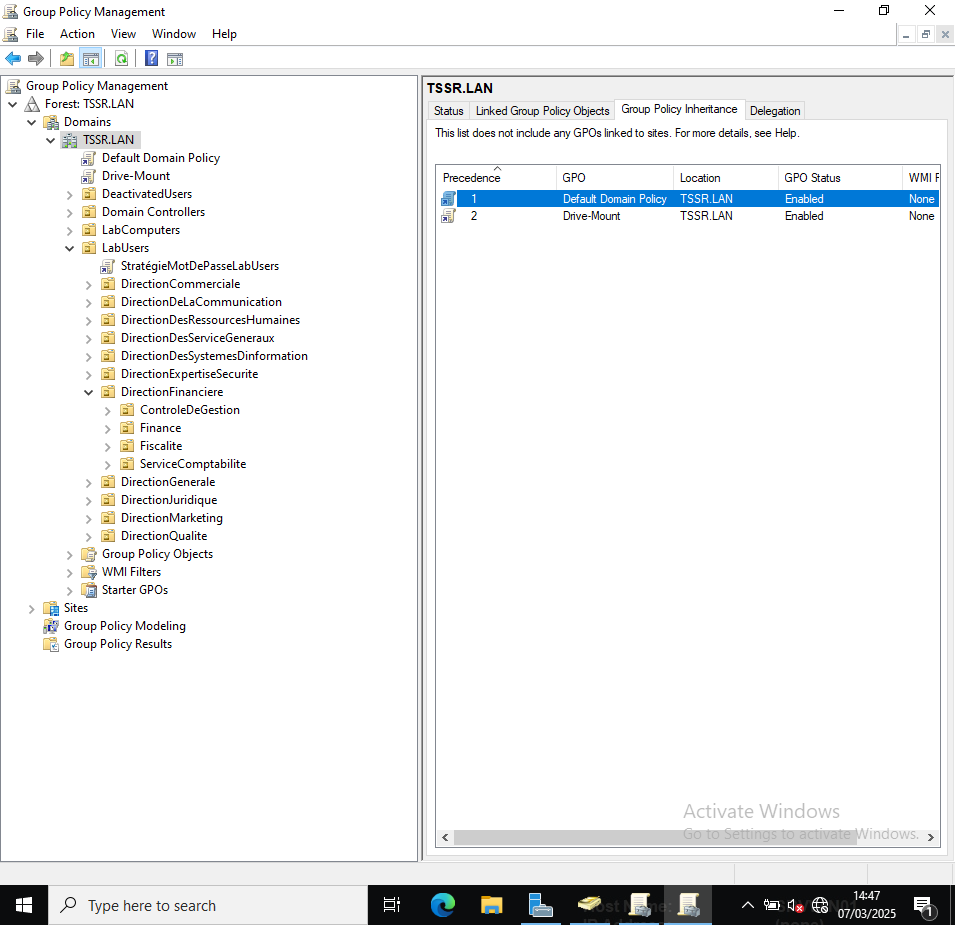


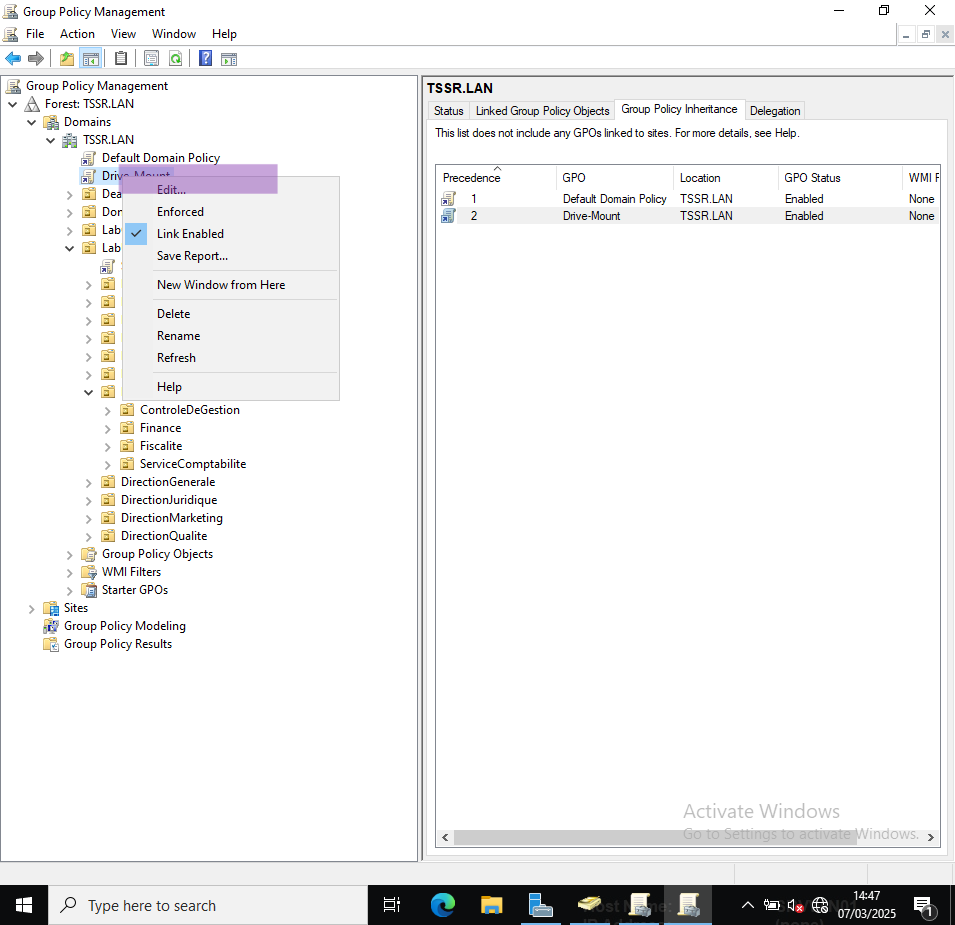
Partie 3 - Lecteurs réseaux

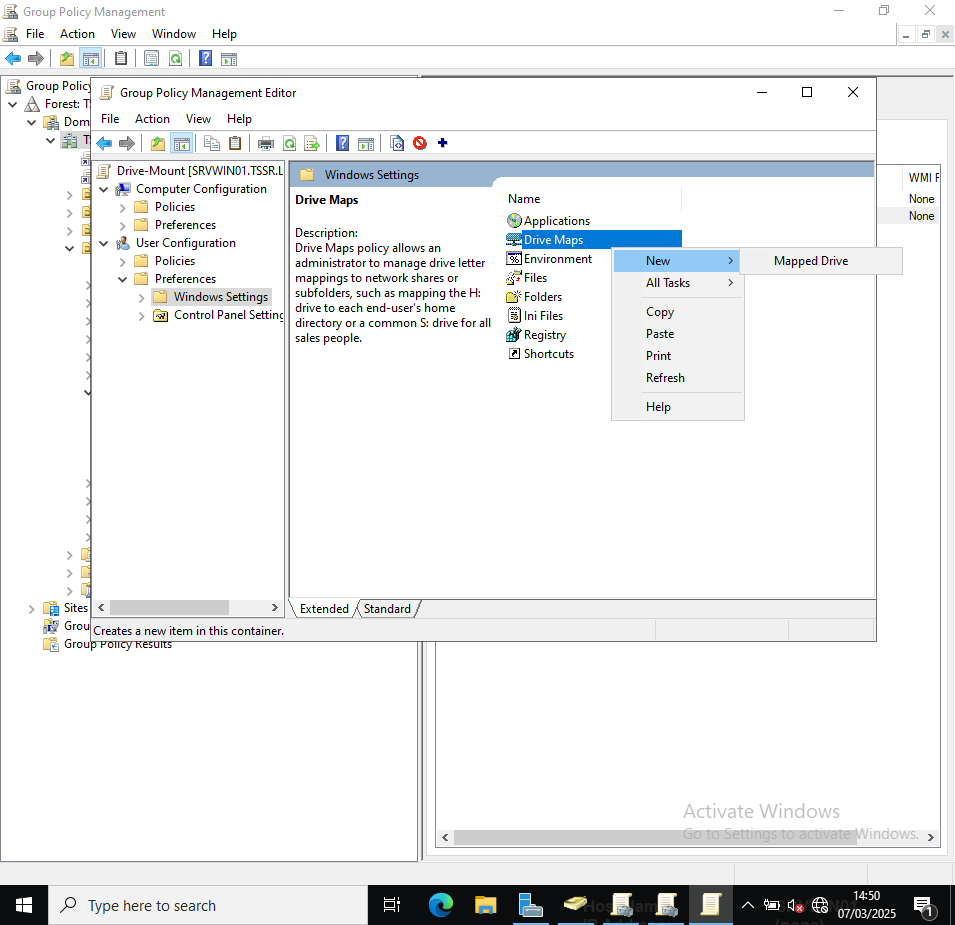
Q.1.3.1

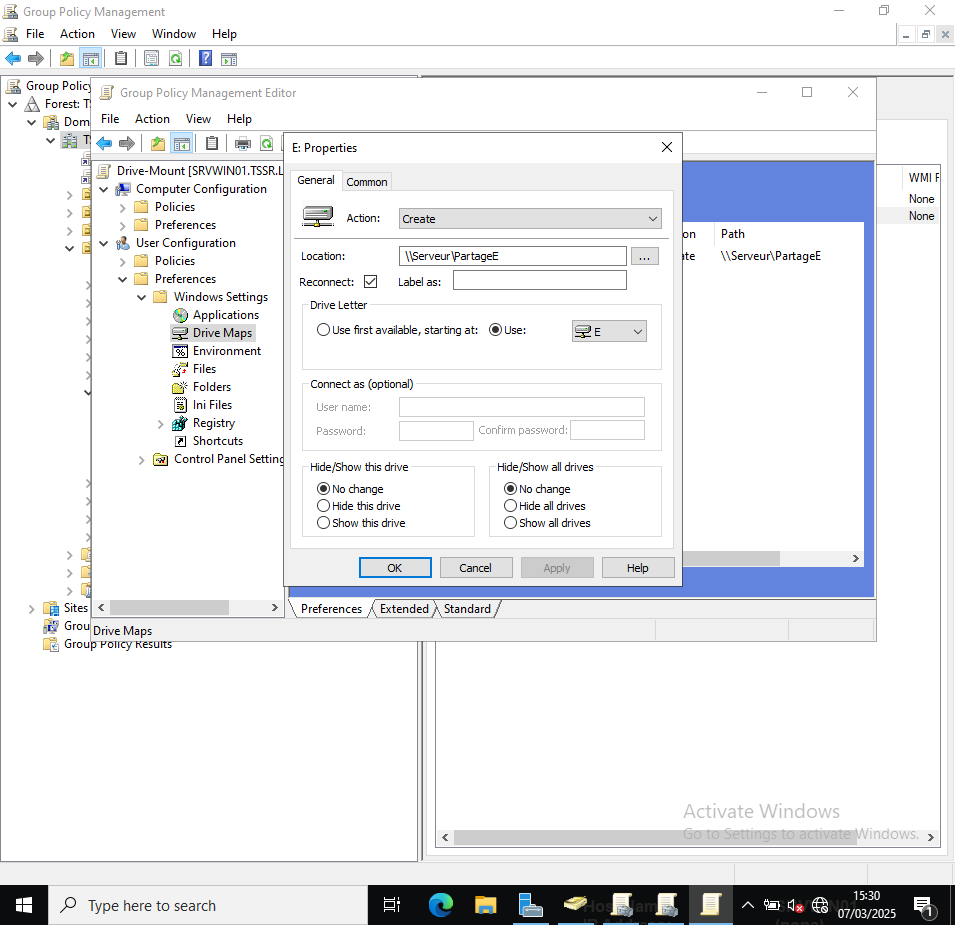


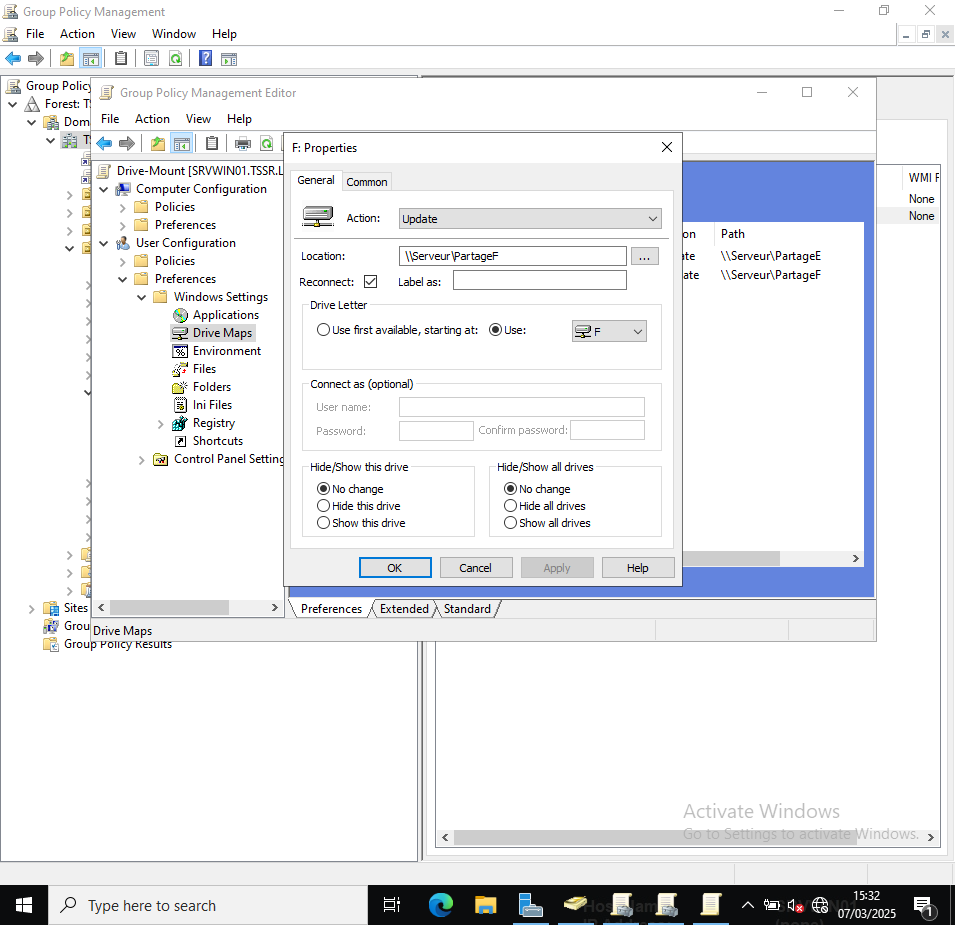


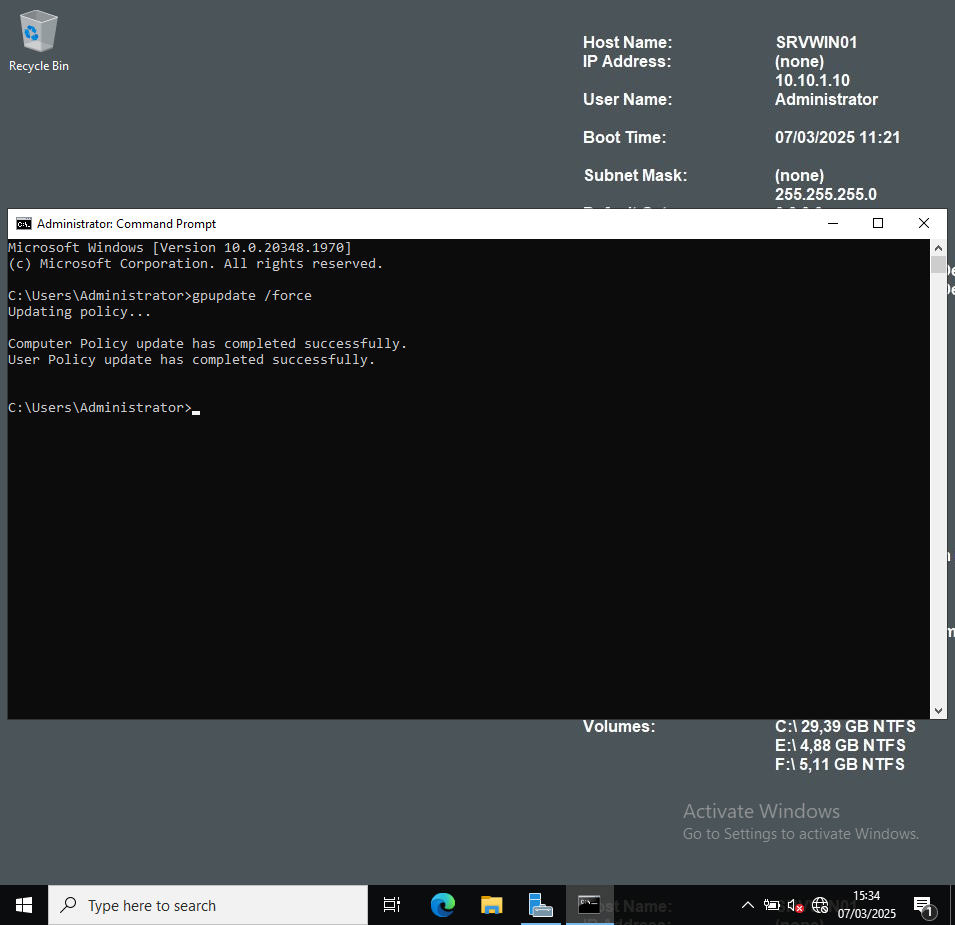












Exercice 2 - VM Linux

Partie 1 - Gestion des utilisateurs

Q.2.1.1

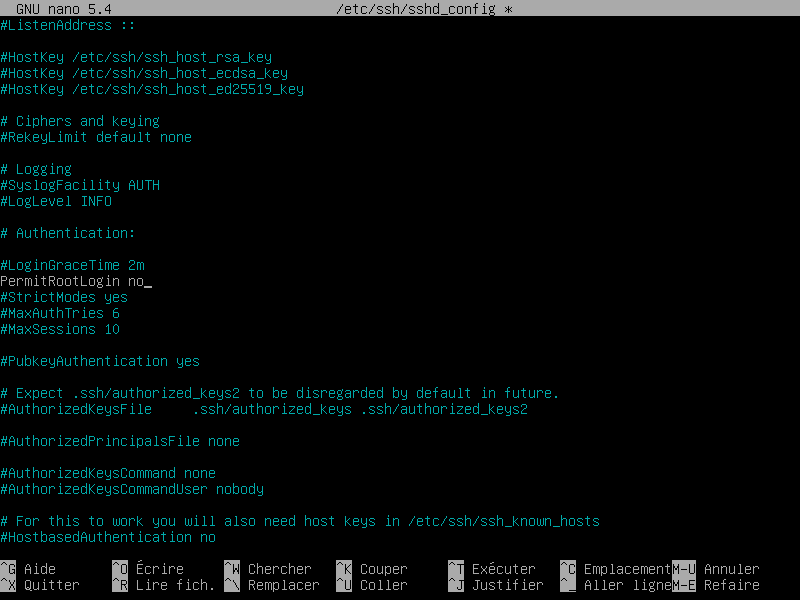


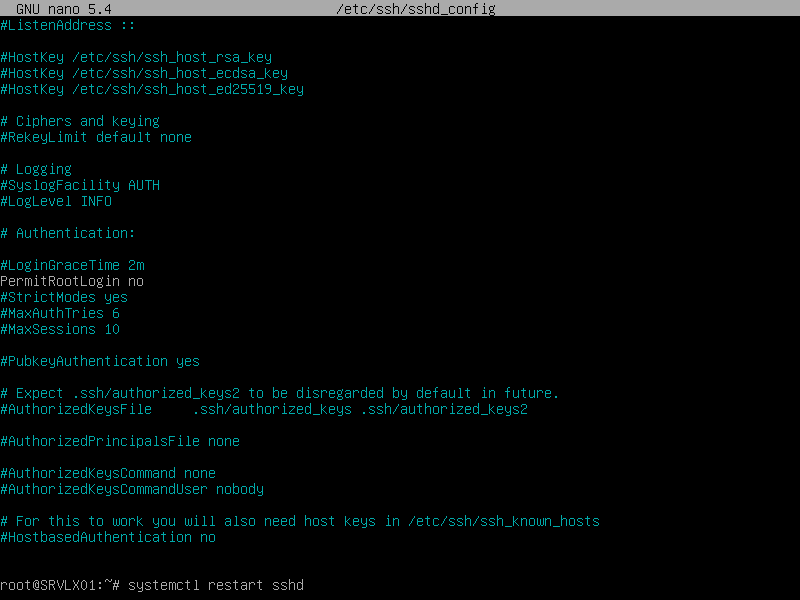
Q.2.1.2

Les préconisations sont : Un mdp fort, privilèges limités, groupe **sudo,** clé SSH, verrouillage de compte en cas d’inactivité, surveillance des activités.

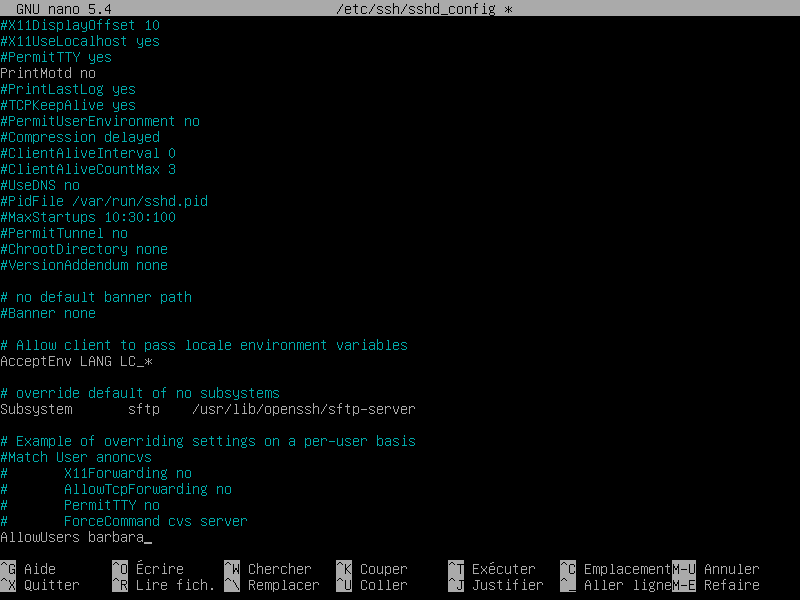
Partie 2 - Configuration de SSH

Q.2.2.1

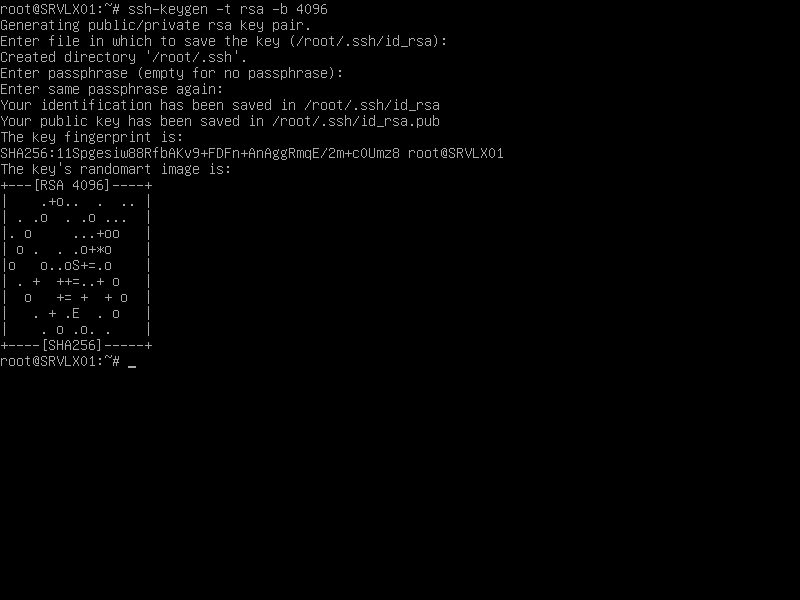


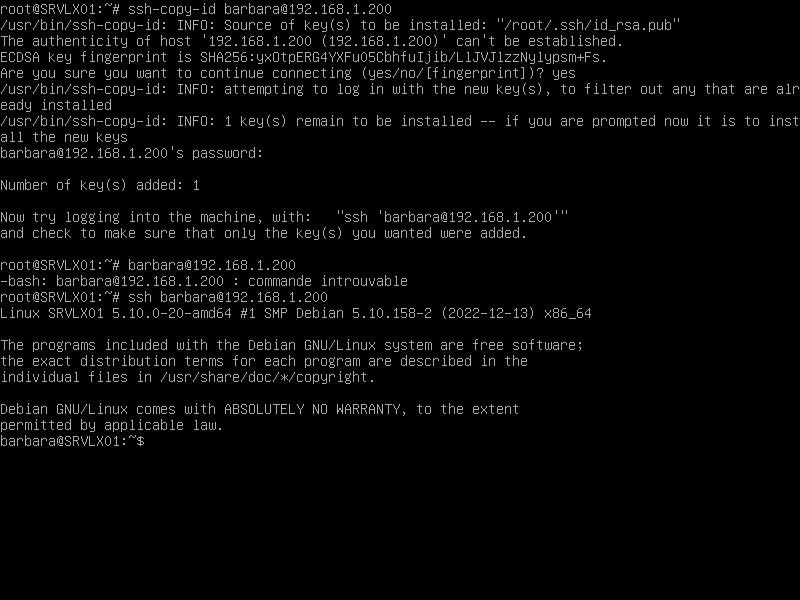


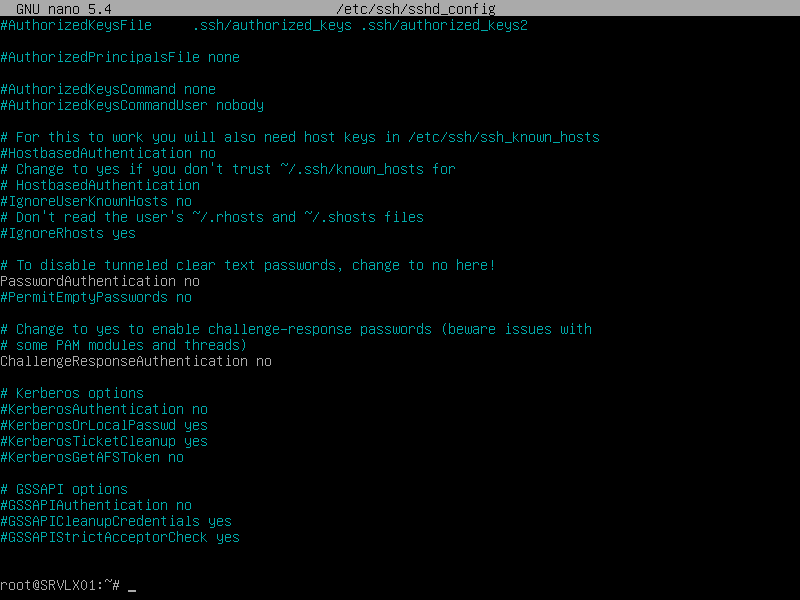
Q.2.2.2

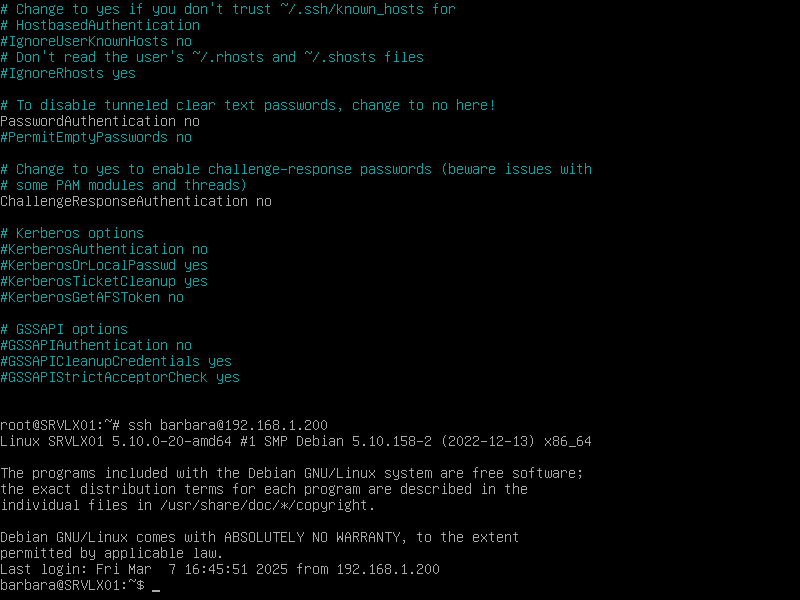


Q.2.2.3





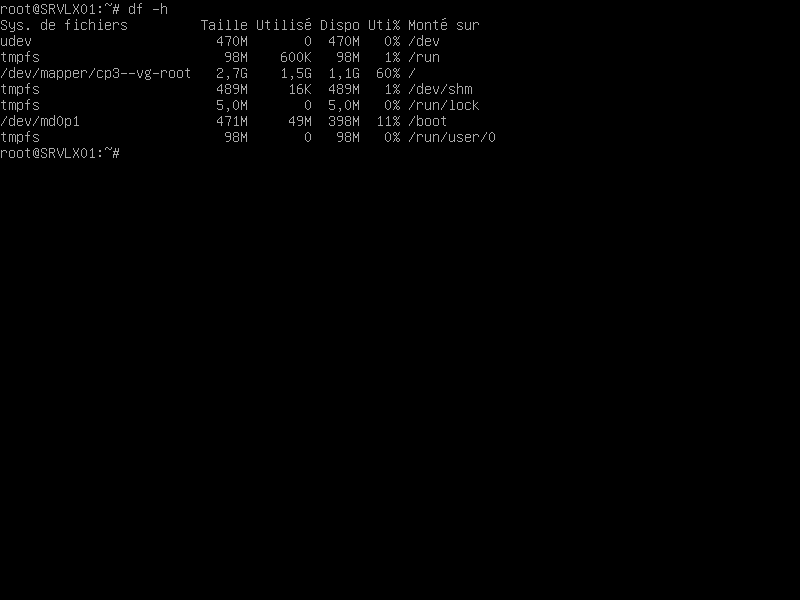




Partie 3 - Analyse du stockage

Q.2.3.1

* udev
* tmpfs (plusieurs instances)
* /dev/mapper/cp3--vg-root (LVM)
* /dev/md0p1 (raid software)



Q.2.3.2

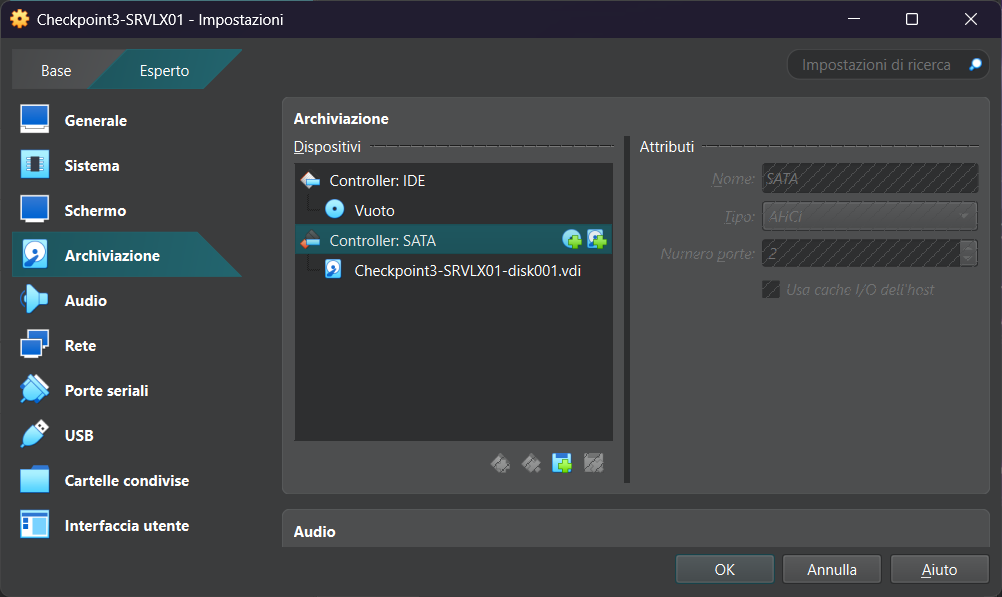
**/dev/mapper/cp3--vg-root** : ce chemin indique l’utilisation de LVM

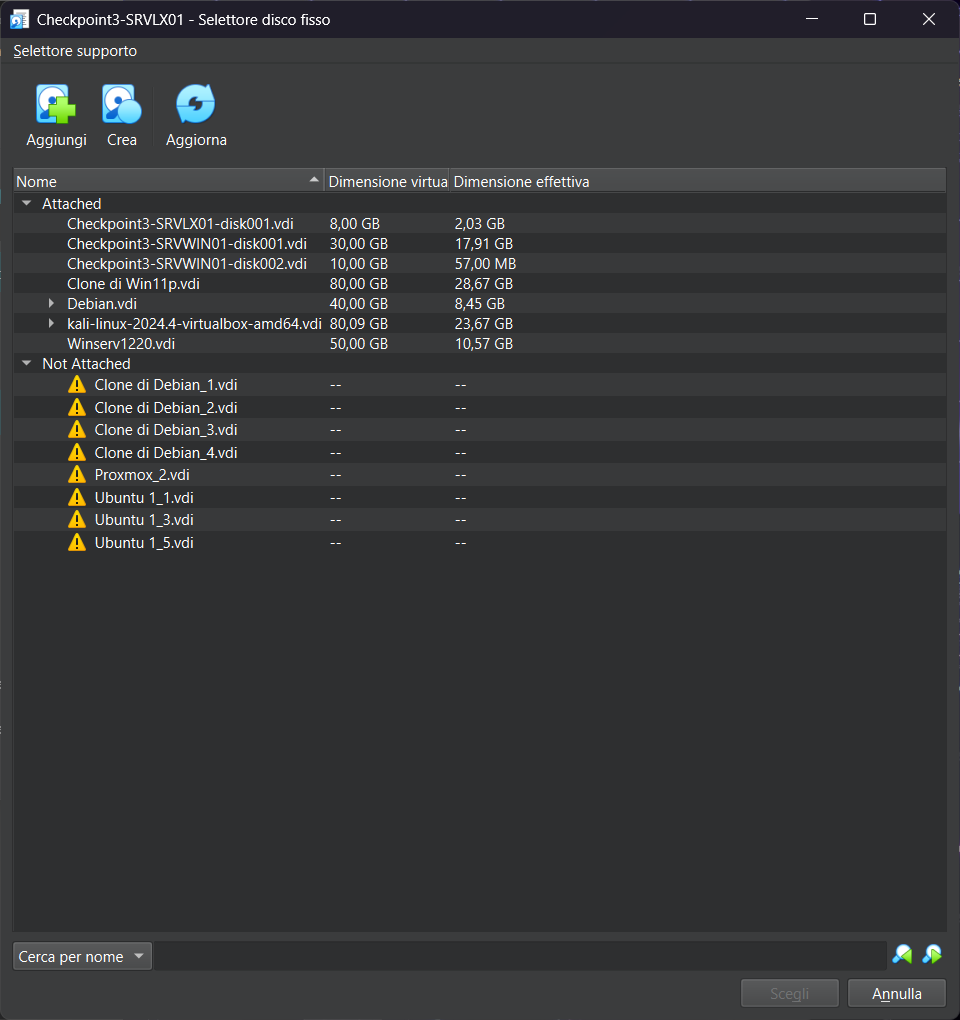
**/dev/md0p1** : ce chemin indique l’utilisation de RAID (md veut dire multiples devices)

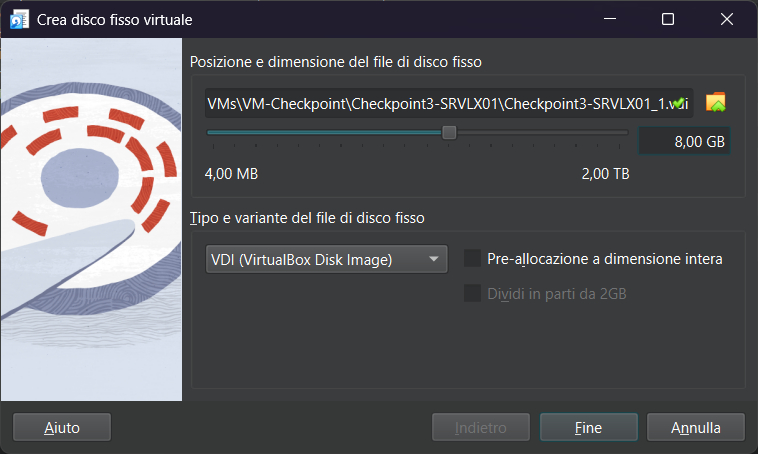
**Udev** : est un système de fichiers virtuel utilisé pour la gestion dynamique des périphériques dans le répertoire /dev

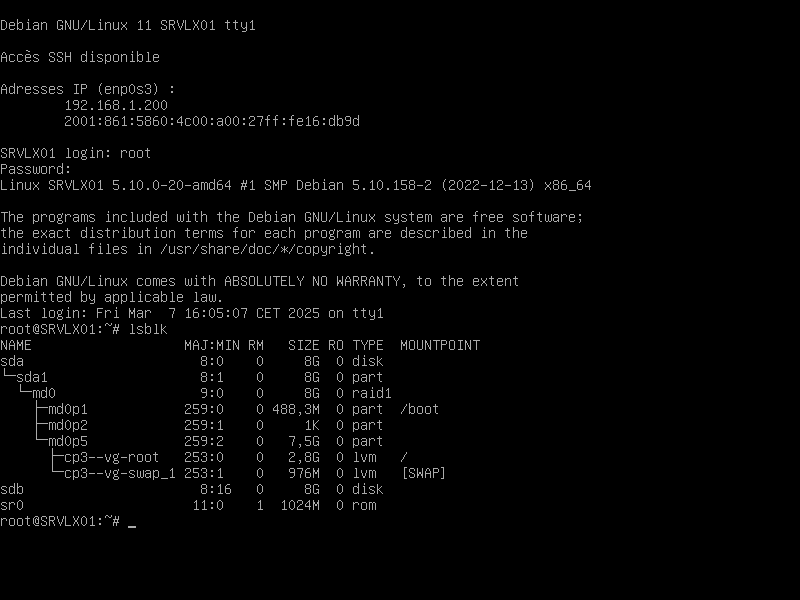
**tmpfs** : un système de fichiers temporaire stocké en RAM.

Q.2.3.3

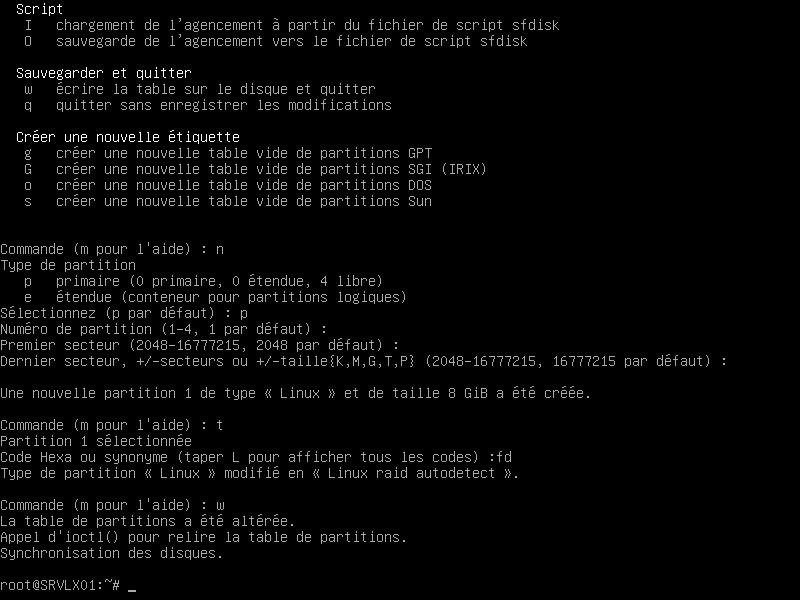






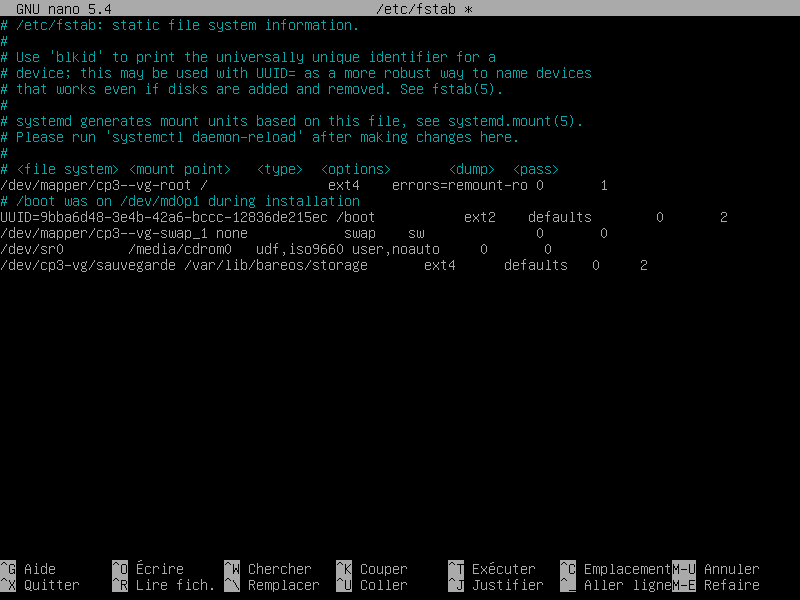


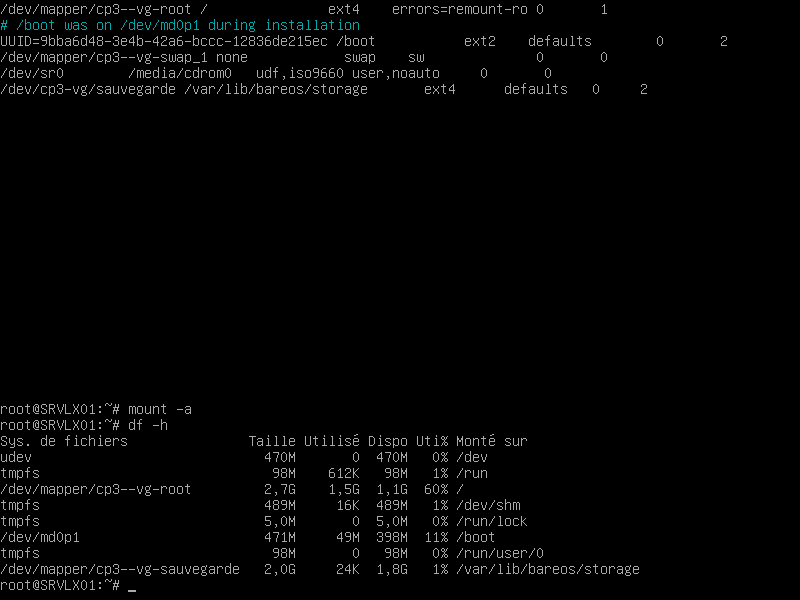
sudo fdisk /dev/sdb



Q.2.3.4







**Q.2.3.5**

Avec la commande **vgs** je peux bien voirqu’il reste 1.79 GB

Q.2.4.1

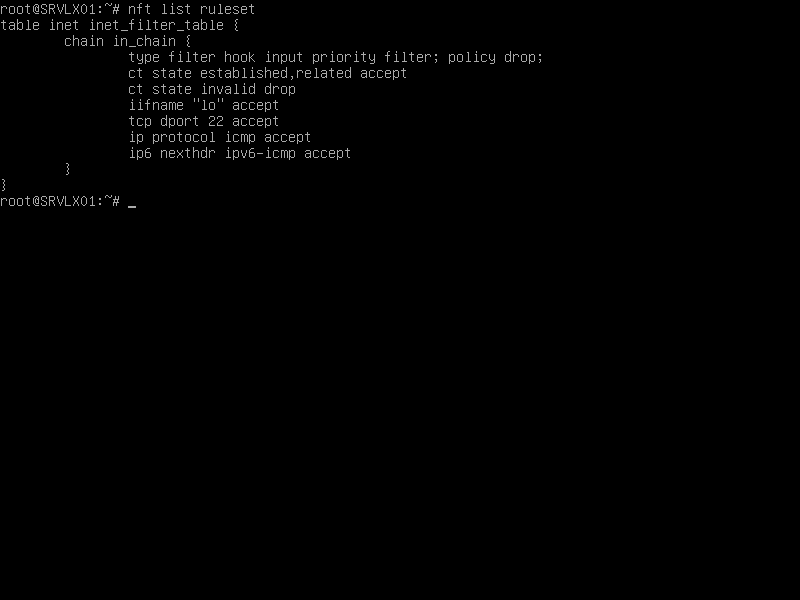
**Bareos-dir** a un rôle de contrôle. C’est le cerveau de Bareos. Il est responsable de la planification et de la gestion de sauvegarde et de restauration.

**Bareos-sd** a dans ses mains la gestion du stockage. Il est reponsable de la gestion des péripheriques de stockage, il reçoit les données à sauvegarder et les écrit sur les supports de stockage et il gére leur restauration à partir du support de stockage.

**Bareos-fd** communique avec bareos-dir et bareos-sd pour exécuter les tâches de sauvegarde et de restauration.

Partie 5 - Filtrage et analyse réseau

Q.2.5.1



Q.2.5.2

- Autorise les connexions établies et les connexions liées

- Autorise tout le trafic provenant de l'interface loopback (lo)

-Autorise le trafic TCP entrant sur le port 22 (SSH)

-Autorise le trafic ICMP (ping) IPv4

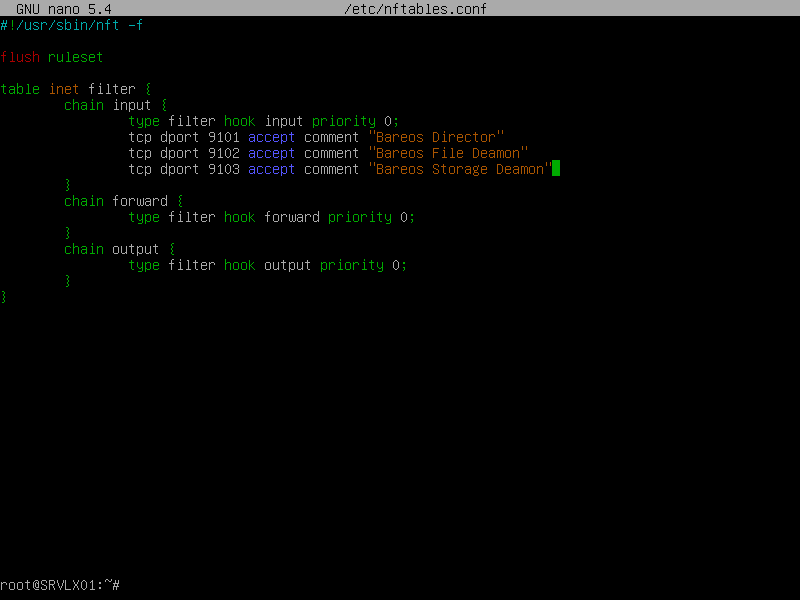
-Autorise le trafic ICMP IPv6

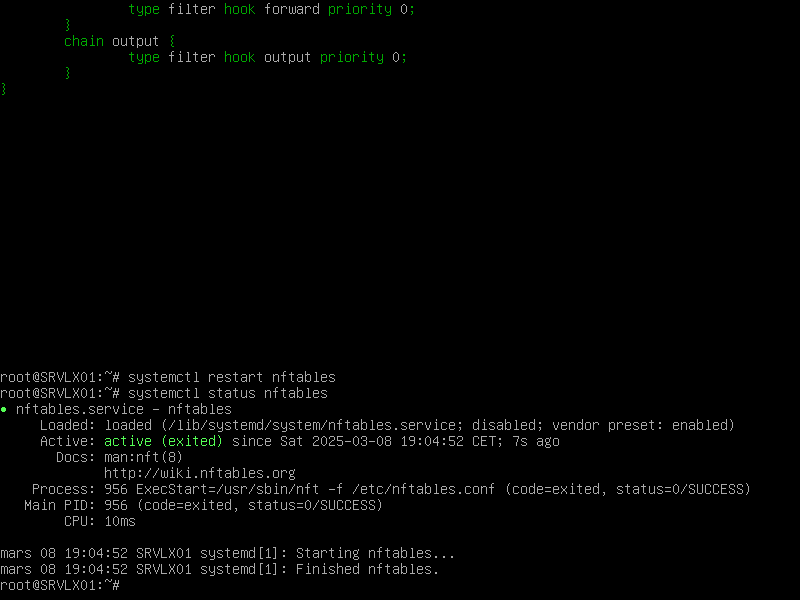
Q.2.5.3

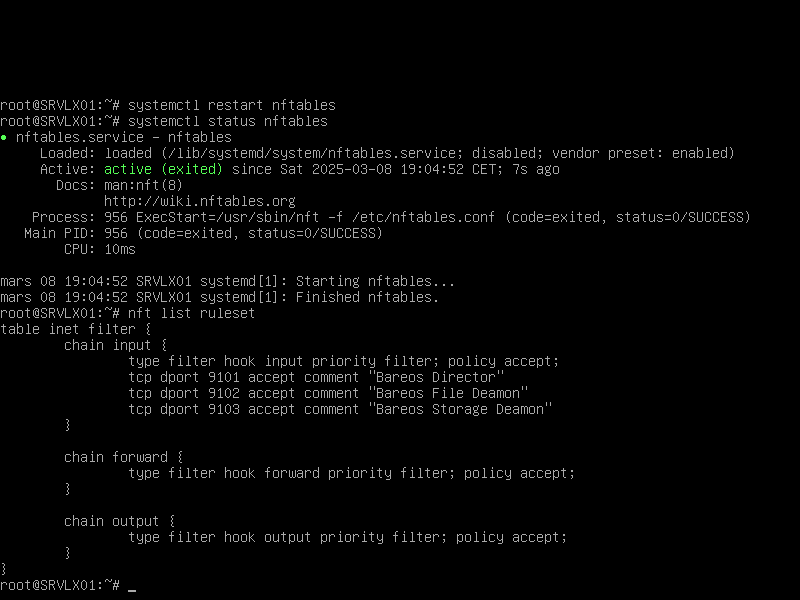
- Tout trafic non explicitement autorisé est bloqué

-Les paquets invalides sont bloqués

Q.2.5.4







Partie 6 - Analyse de logs

Q.2.6.1

