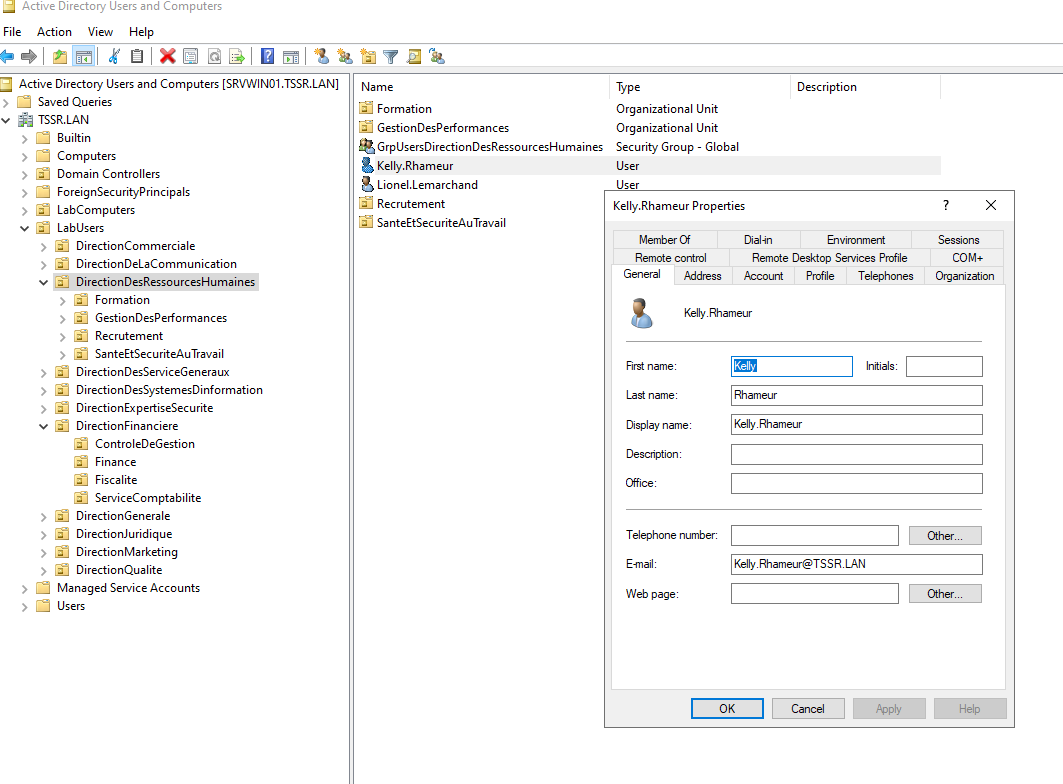
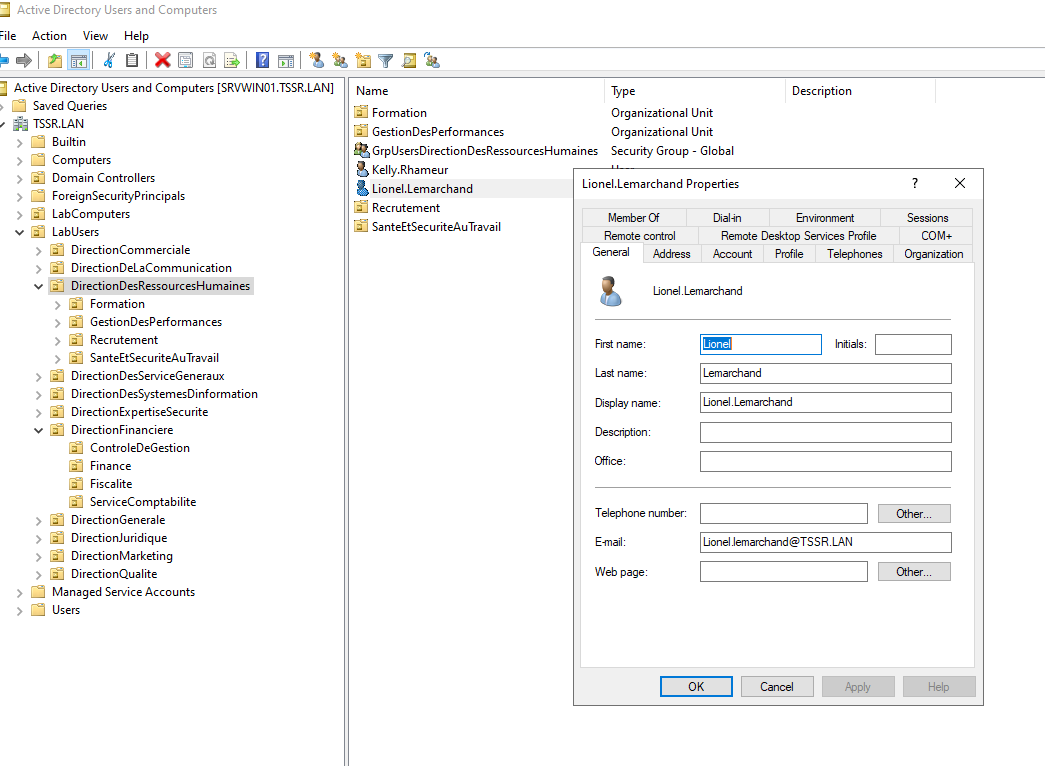
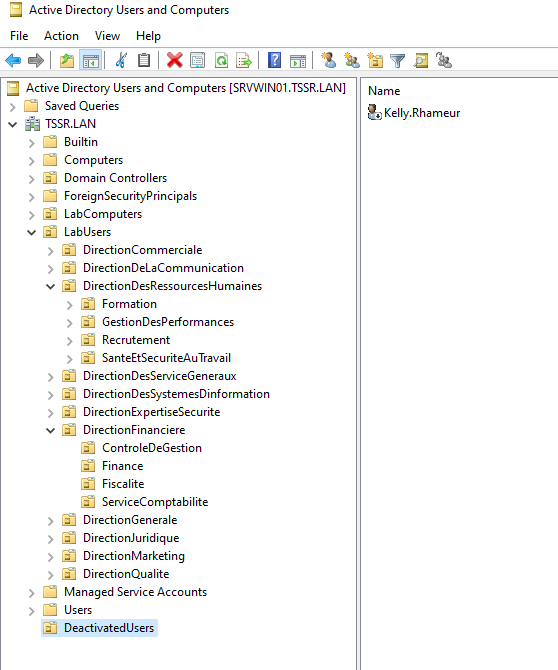
Exercice 1 - VM Windows

Partie 1 - Gestion des utilisateurs

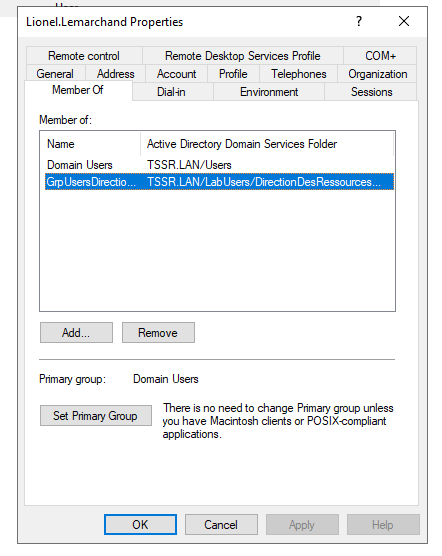
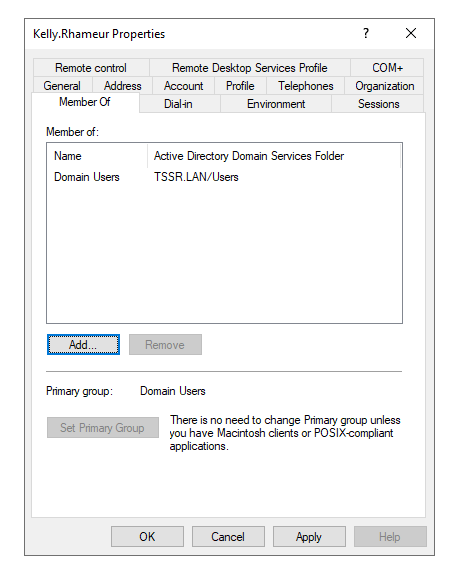
Q.1.1.1

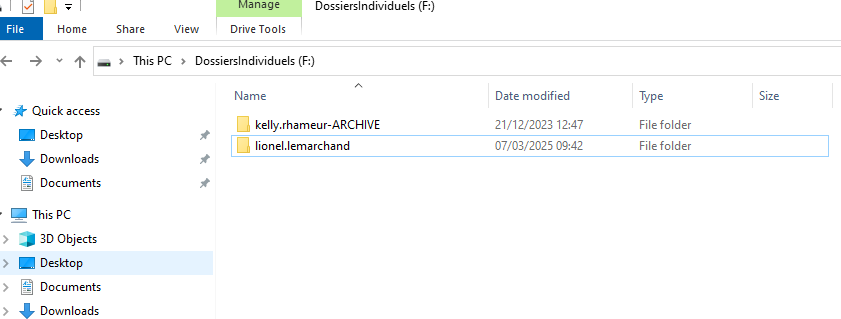
Q.1.1.2

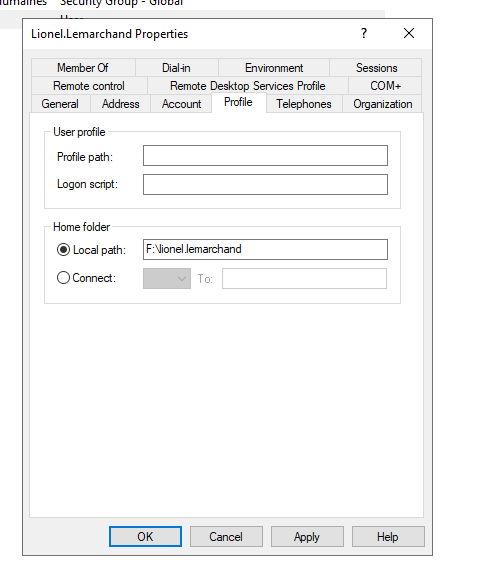
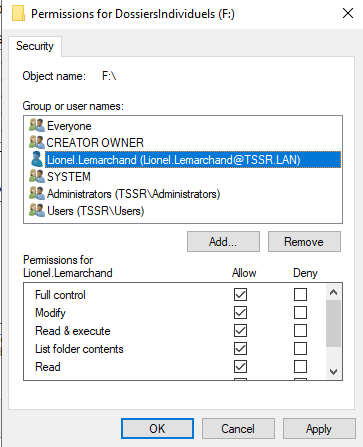


Q.1.1.3



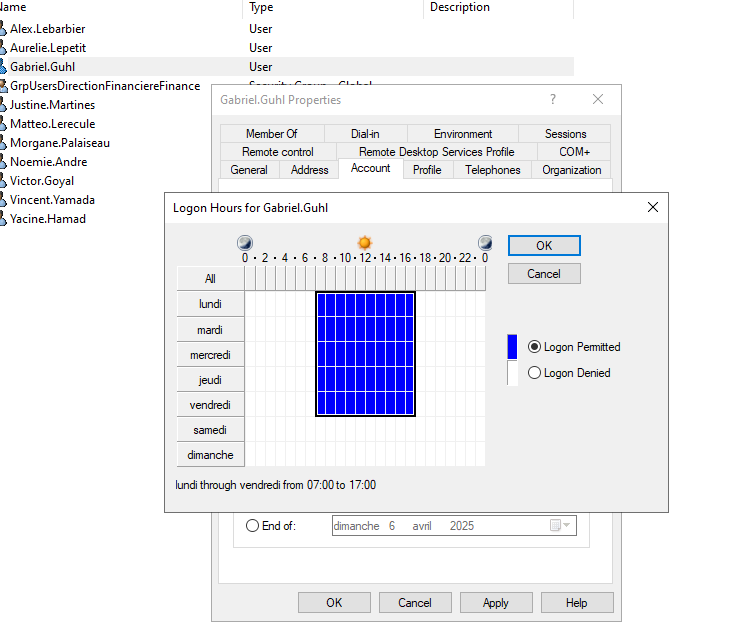
J’ai retiré l’accès de Kelly à GrpUsersDirectiondesressourceshumaines et à contrario, j’ai ajouté Lionel Lemarchand à ce groupe.

Q.1.1.4  
 

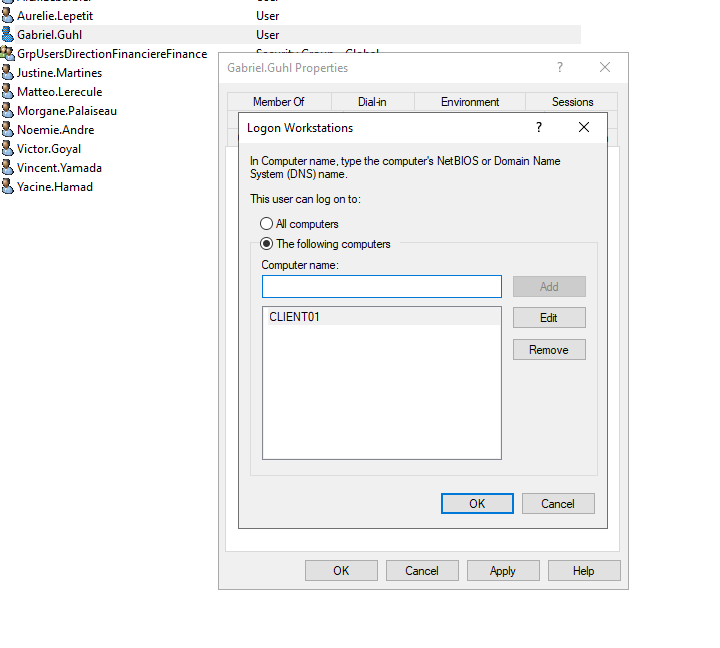


Partie 2 - Restriction utilisateurs

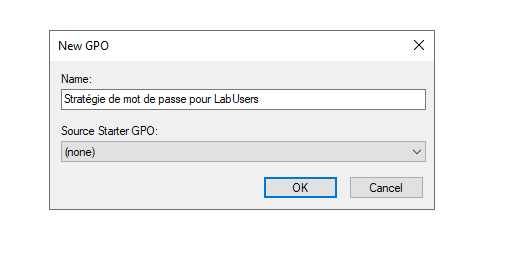
Q.1.2.1

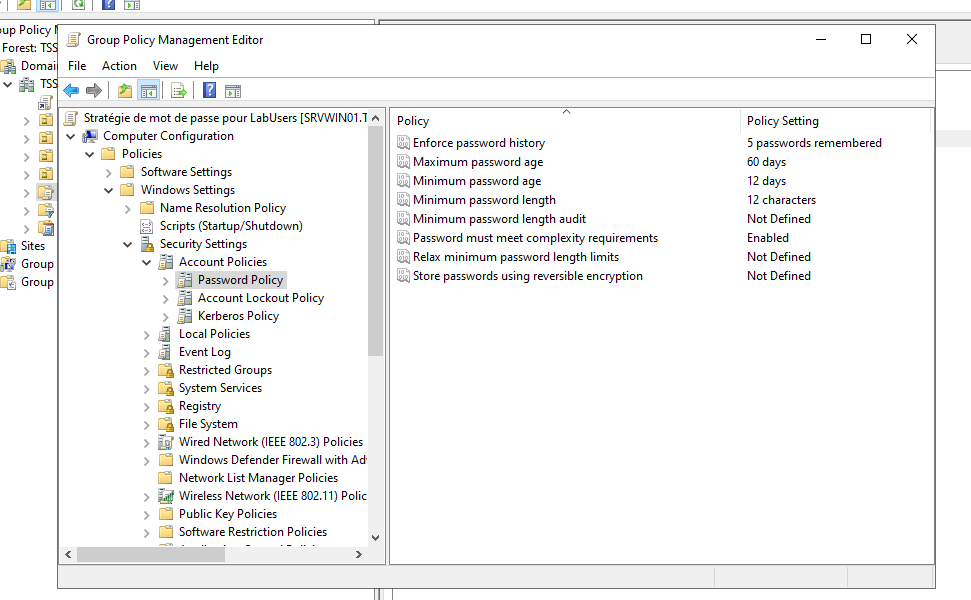


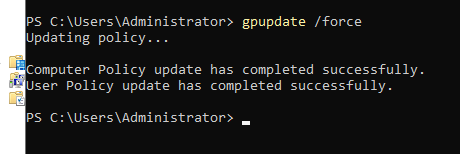
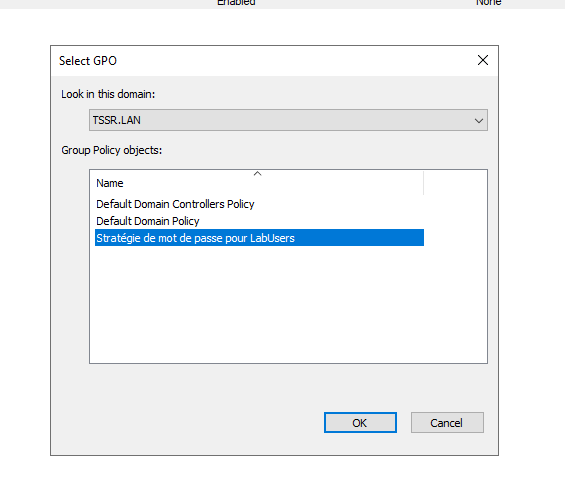
Q.1.2.2



Q.1.2.3

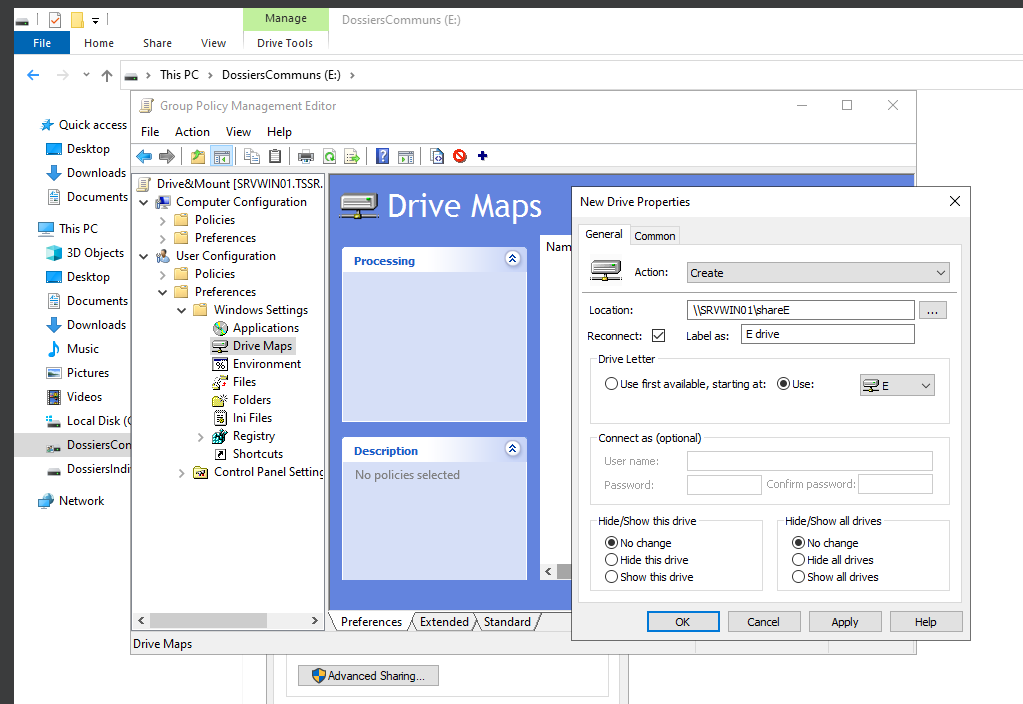


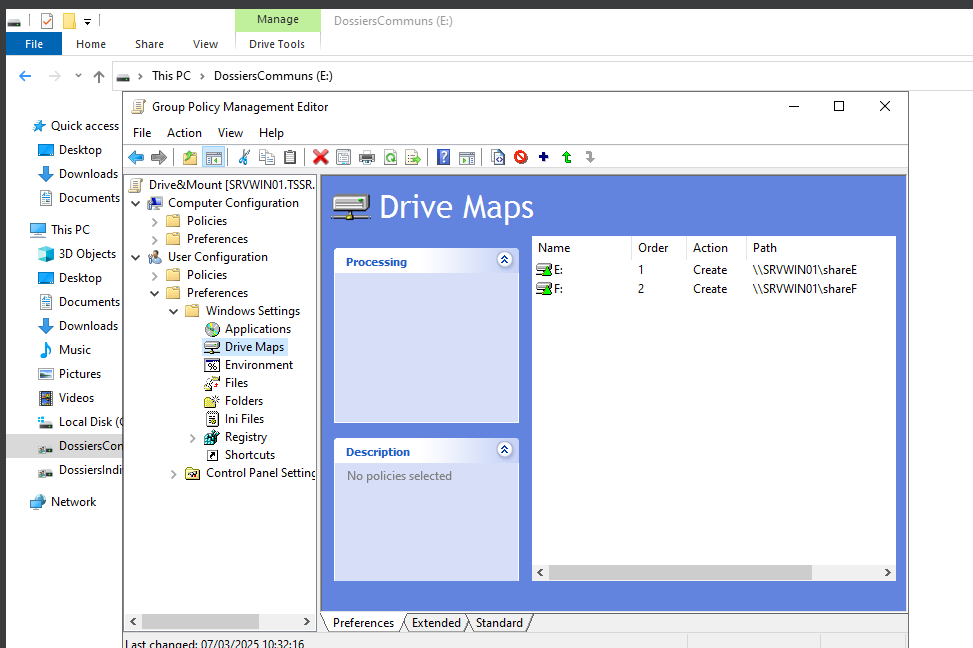


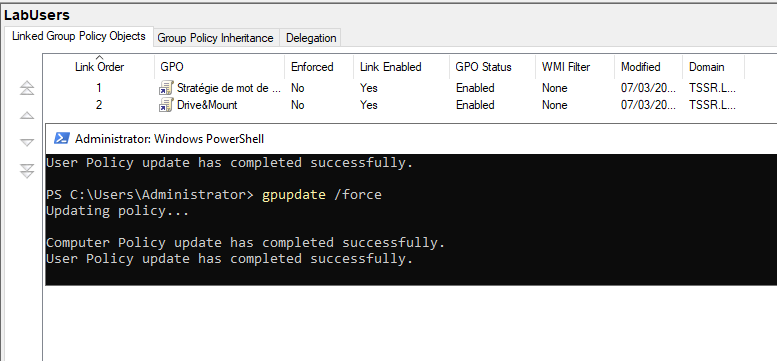


Partie 3 - Lecteurs réseaux

Q.1.3.1



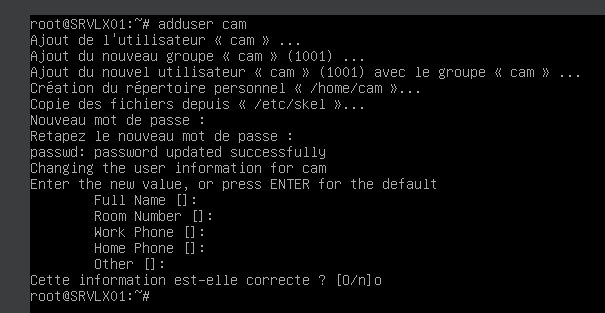




Exercice 2 - VM Linux

Partie 1 - Gestion des utilisateurs

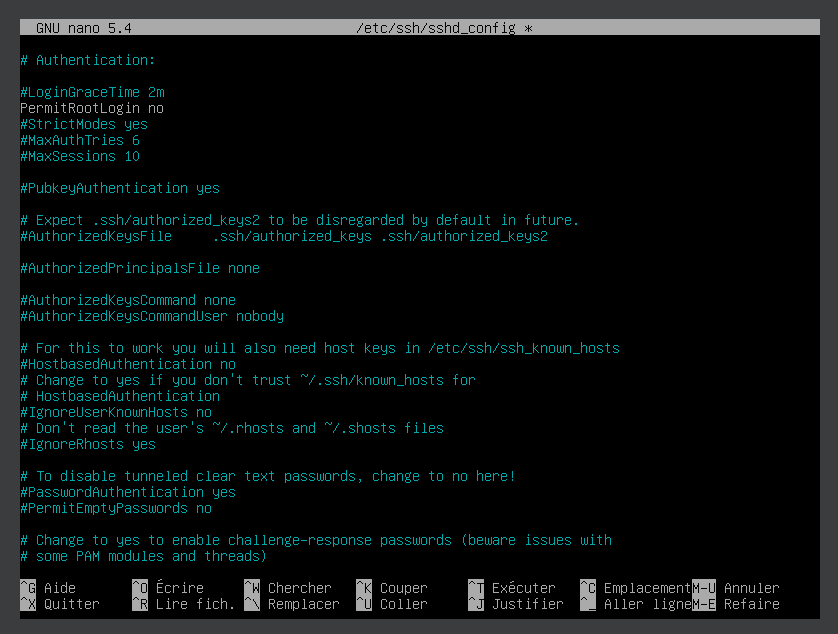
Q.2.1.1



Q.2.1.2   
  
Concernant ce compte personnel, je préconiserais dans un premier temps de choisir un mot de passe fort pour le sécurisé. Ensuite d’utiliser sudo au lieu de root pour les tâches administratives et donc d’accorder des permissions sudo. On peut configurer l’accès SSH pour le sécurisé par exemple en utilisant des clés SSH au lieu de mots de passe pour l'authentification. (On peut aussi limiter les adresses IP autorisées à se connecter via SSH (avec un pare-feu ou dans le fichier SSH config)). On peut aussi mettre régulièrement à jour le système et enfin, on peut utiliser des outils pour scanner notre système, en prévention ! (pour détecter des intrusions potentielles par exemple)

Partie 2 - Configuration de SSH

Q.2.2.1



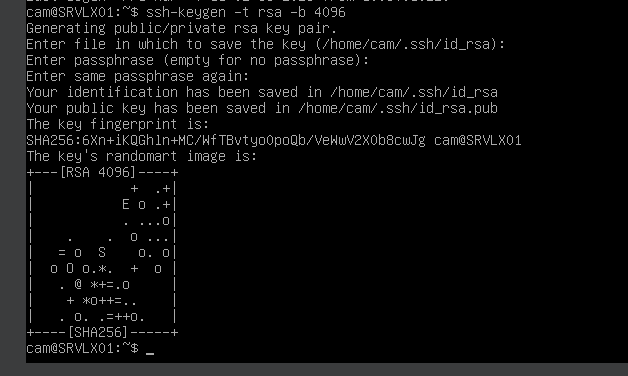


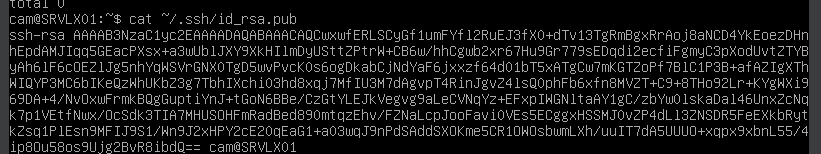
Q.2.2.2



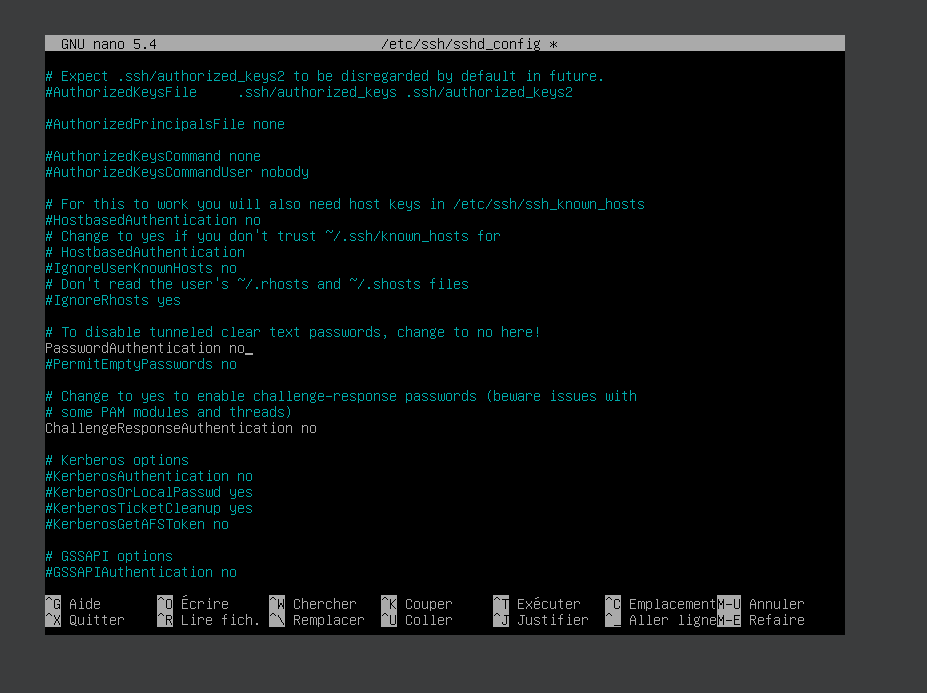


Q.2.2.3

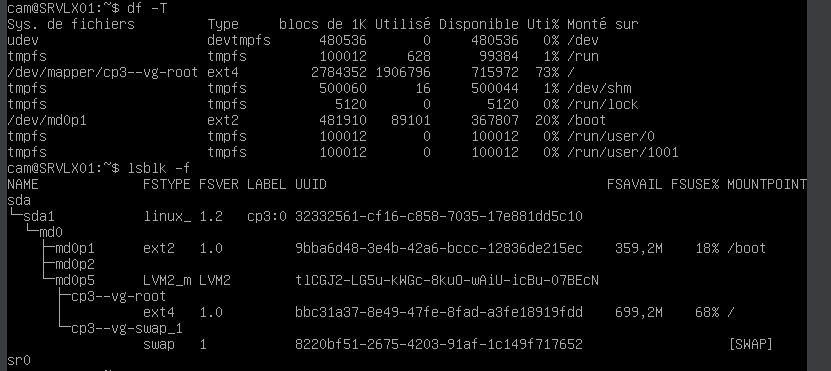




il faut rentrer la clé généré dans le fichier sudo nano ~/.ssh/authorized\_keys ( je n’ai pas réussi car le copier-coller ne marche pas et je n’avais pas le temps de tout recopier à la main)

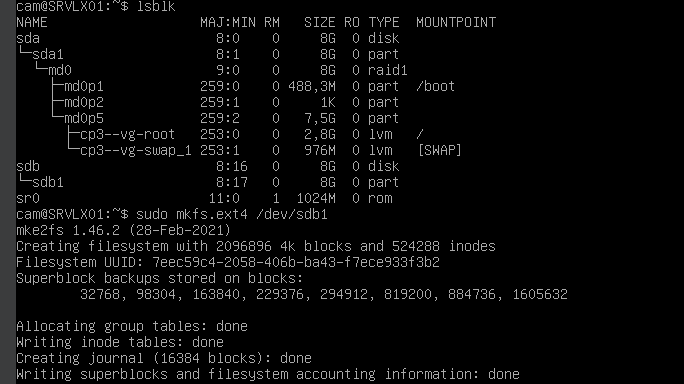
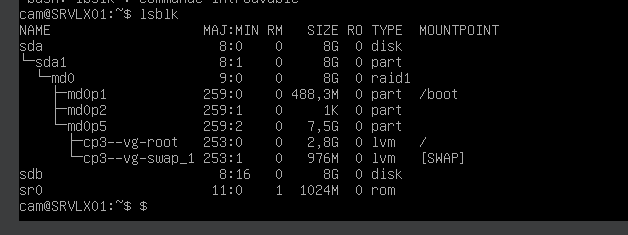


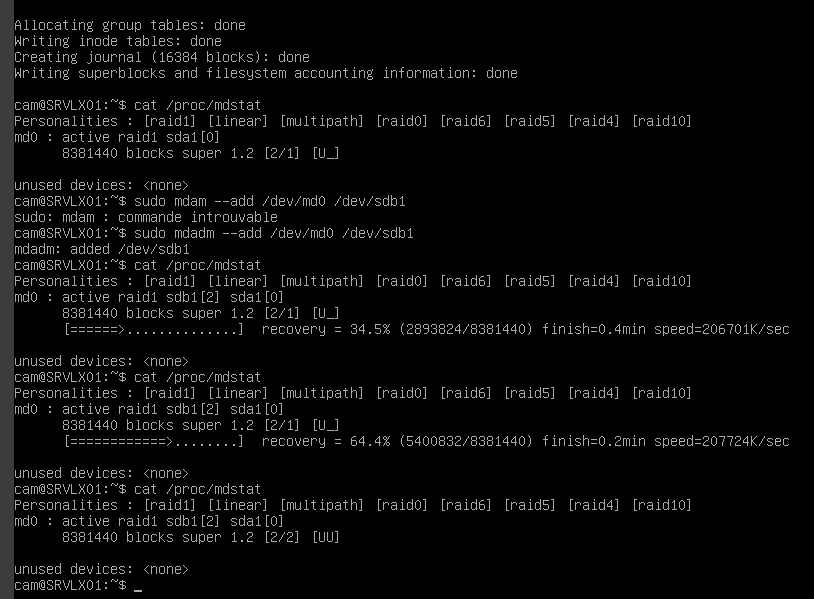
Partie 3 - Analyse du stockage

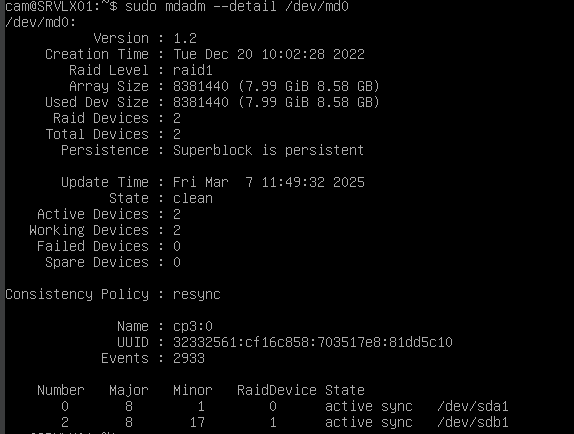
Q.2.3.1   
  
Les systèmes de fichiers actuellement montés sont sda1, md0p1 et md0p5, cp3 vg root cp3 vg swap :  


Q.2.3.2   
Ils utilisent les systèmes de stockage swap, ext2, LVM ext4 et Linux

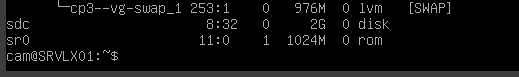
Q.2.3.3

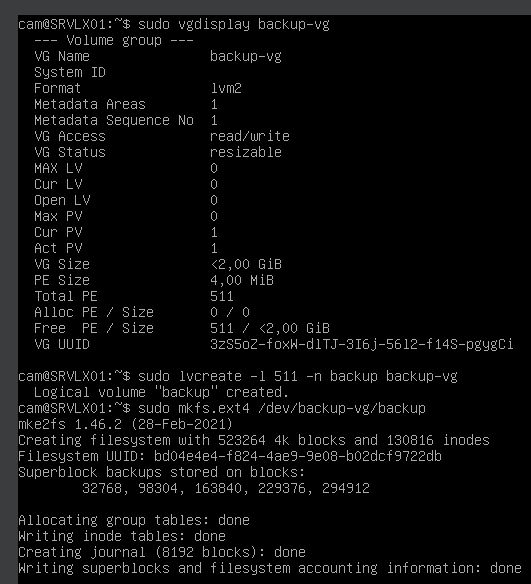


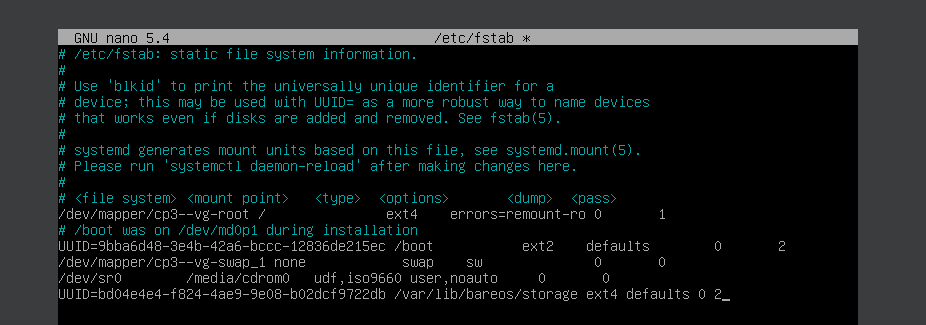


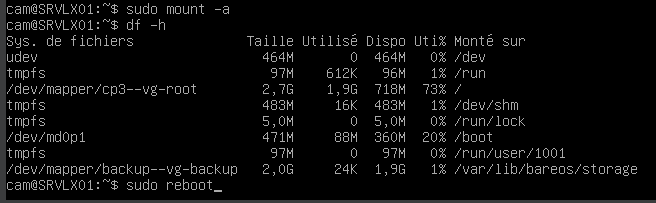


Q.2.3.4



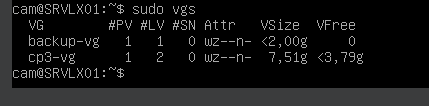








Q.2.3.5



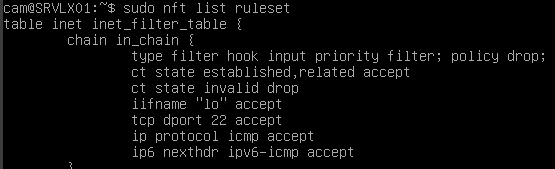
Sur backup vg je n’ai plus de place, il semble me rester de la place pour cp3-vg , environ 3,79 G

Partie 4 - Sauvegardes

Q.2.4.1

**bareos-dir**: il orchestre et contrôle tout le processus de sauvegarde Il Planifie les sauvegardes Gère les clients (File Daemons) et les périphériques de stockage (Storage Daemons).Il surveille l’état des sauvegardes et des restaurations.  
**bareos-sd**: Il Gère les supports de stockage, écrit les sauvegardes, il reçoit les données des clients (via le File Daemon).  
**bareos-fd** : c’est justement l’agent client, envoie les données à sauvegarder. Il envoie les fichiers au Storage Daemon selon les ordres du Director. Peut aussi gérer la restauration de fichiers sur la machine source.

Partie 5 - Filtrage et analyse réseau

Q.2.5.1   


Q.2.5.2

Les types de communication autorisées sont :  
- **Connexions déjà établies ou liées** (réponses aux connexions initiées par le serveur).

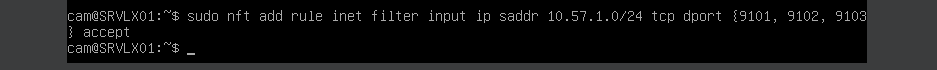
* **Le trafic local** (entre les processus sur le serveur lui-même via l’interface lo).
* **SSH (port 22)** — accès distant pour l’administration.
* **ICMP (ping, etc.)** pour IPv4 et IPv6 — permet les tests de connectivité réseau.

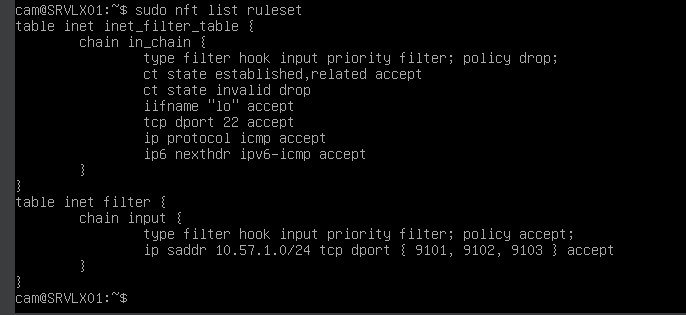
Q.2.5.3   
Les types de connexions interdites sont les suivantes du coup :  
- **Les nouvelles connexions entrantes** (autres que celles sur le port 22).

- **Le trafic Bareos** (ports 9101, 9102 et 9103) — ce qui signifie que le serveur ne pourra pas encore communiquer avec les clients Bareos.

- **Tout service ou port** non spécifiquement autorisé, comme HTTP, HTTPS, ou d'autres protocoles.

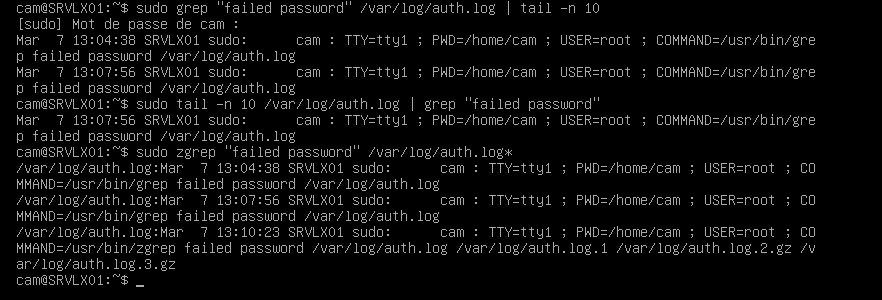
Q.2.5.4

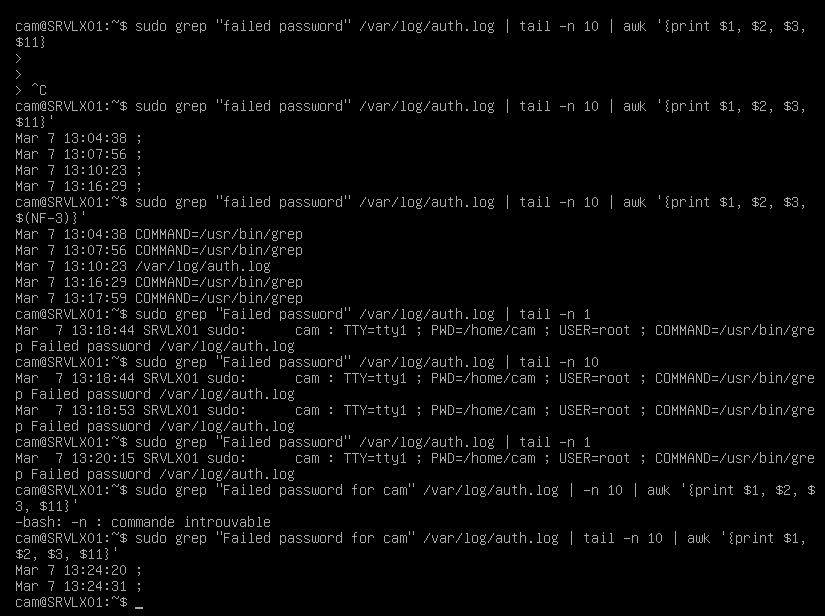




Partie 6 - Analyse de logs

Q.2.6.1



- La tentative à été faite le 07/03/2025 à 13 :04 (il y a d’autres entrée car j’ai fait d’autre test)  
- l’adresse IP n’apparait pas, j’ai tenté d’autre commande mais je n’ai rien..   


ok : /24

nr :

faux :