

CHECKPOINT 3

Formulaire réponses

Exercice 1

Partie 1

Q.1.1.1

Copie(s) d'écran montrant que Lionel Lemarchand a les mêmes attributs de société que Kelly Rhameur.

The image displays two side-by-side screenshots of the 'Properties' dialog boxes for two Active Directory users: Lionel Lemarchand and Kelly Rhameur. Both windows show the 'General' tab, which contains fields for Job Title, Department, Company, Manager, and Direct reports. The 'Company' field for both users is 'CyberOps'. The 'Manager' field for both is 'Camille.Martin'. The 'Direct reports' field for Kelly Rhameur lists Cedric.Caron, Chris.Shin, Ophelie.Poulin, Uriel.Hubert, and Yves.Delavega. The 'OK' button in the Kelly Rhameur window is highlighted with a blue border.

Member Of	Dial-in	Environment	Sessions
Remote control	Remote Desktop Services Profile	COM+	
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:

OK Cancel Apply Help

Copie(s) d'écran montrant le changement coté management.

Lionel Lemarchand Properties

Member Of

Dial-in

Environment

Sessions

Remote control

Remote Desktop Services Profile

COM+

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:

OK

Cancel

Apply

Help

Camille.Martin Properties

Member Of

Dial-in

Environment

Sessions

Remote control

Remote Desktop Services Profile

COM+

General

Address

Account

Profile

Telephones

Organization

Job Title:

Department:

Company:

Manager

Name:

Change...

Properties

Clear

Direct reports:

Lionel Lemarchand

OK

Cancel

Apply

Help

Q.1.1.2

Copie d'écran de l'OU DeactivatedUsers.

Active Directory Users and Computers

File Action View Help

Active Directory Users and Computers [SRVWIN01.TSSR.LAN]

Saved Queries

TSSR.LAN

- Builtin
- Computers
- Domain Controllers
- ForeignSecurityPrincipals
- LabComputers
- LabUsers
 - DirectionCommerciale
 - DirectionDeLaCommunication
 - DirectionDesRessourcesHumaines
 - DirectionDesServiceGeneraux
 - DirectionDesSystemesDinformation
 - DirectionExpertiseSecurite
 - DirectionFinanciere
 - DirectionGenerale
 - DirectionJuridique
 - DirectionMarketing
 - DirectionQualite
 - DeactivatedUsers
- Managed Service Accounts
- Users

Name

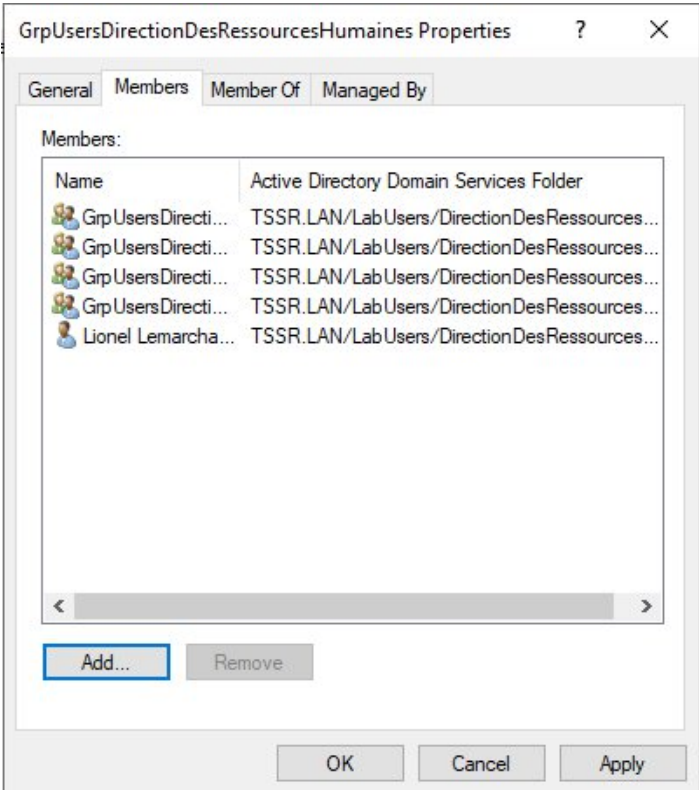
Type

Kelly.Rhameur

User

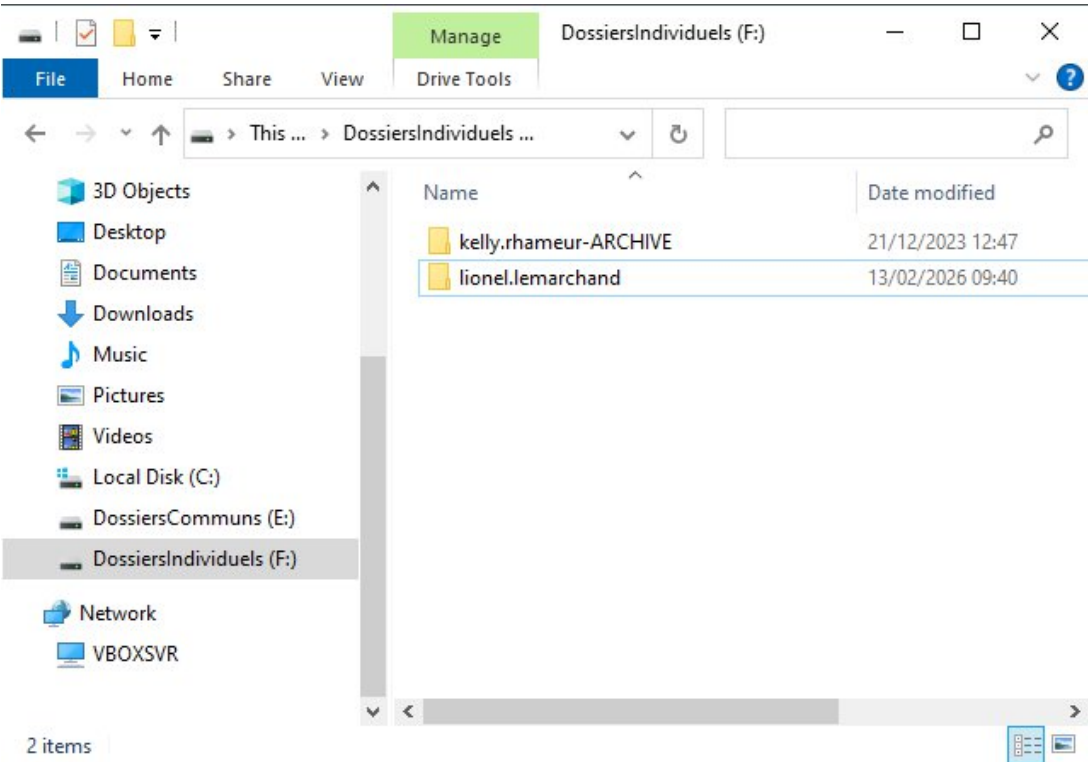
Q.1.1.3

Copie d'écran de l'ancien groupe dans lequel était Kelly Rhameur.



Q.1.1.4

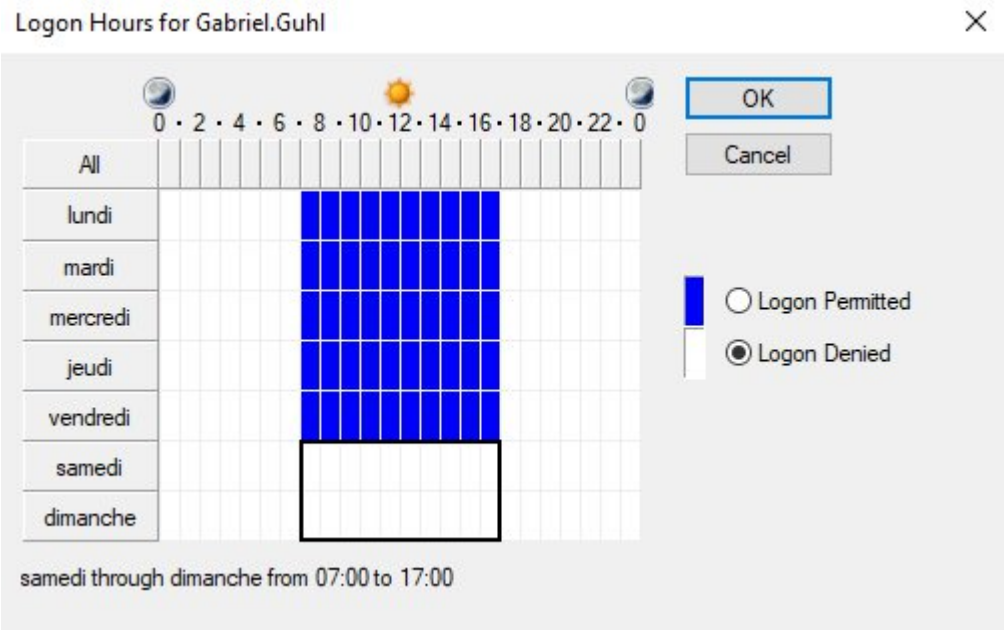
Copie d'écran des dossiers individuels demandés.



Partie 2

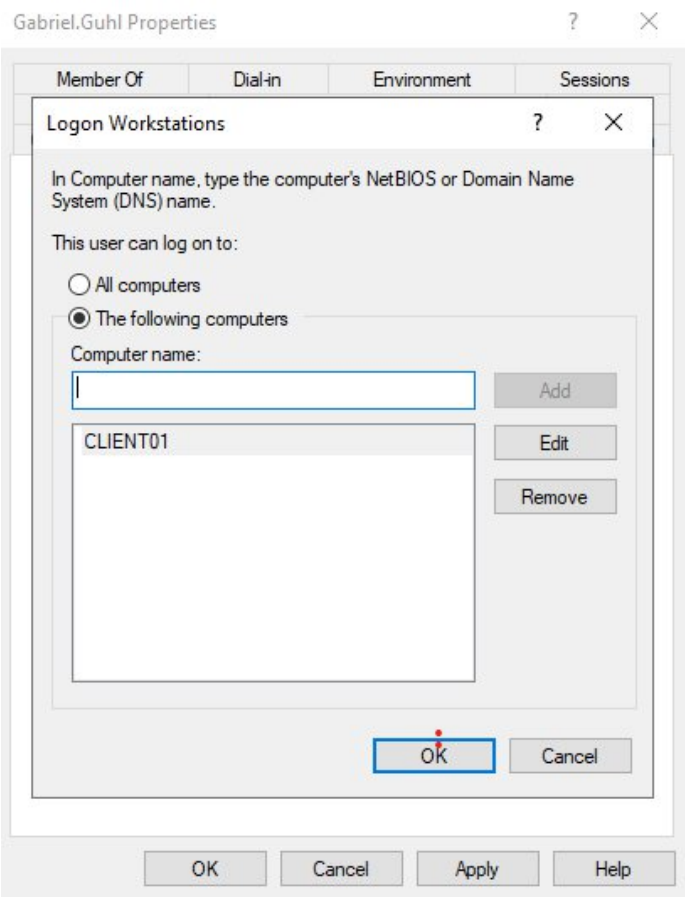
Q.1.2.1

Copies d'écran montrant le paramétrage de la restriction de connexion horaire.



Q.1.2.2

Copie d'écran montrant le paramétrage de la restriction de la connexion machine.



Q.1.2.3

Copies d'écran de la stratégie de mot de passe.

Create Password Settings: Password Policies

TASKS ▾ SECTIONS ▾

Password Settings

Directly Applies To

Precedence: * 15

☒ Enforce minimum password length
Minimum password length (characters): * 15

☒ Enforce password history
Number of passwords remembered: * 12

☒ Password must meet complexity requirements

☐ Store password using reversible encryption

☒ Protect from accidental deletion

Description:

☒ Enforce minimum password age
User cannot change the password within (days): * 7

☒ Enforce maximum password age
User must change the password after (days): * 90

☒ Enforce account lockout policy:
Number of failed logon attempts allowed: * 3
Reset failed logon attempts count after (mins): * 15
Account will be locked out:
☐ For a duration of (mins): * 30
☒ Until an administrator manually unlocks the account

Directly Applies To ? X ^

Name	Mail
Domain Users	

Add... Remove

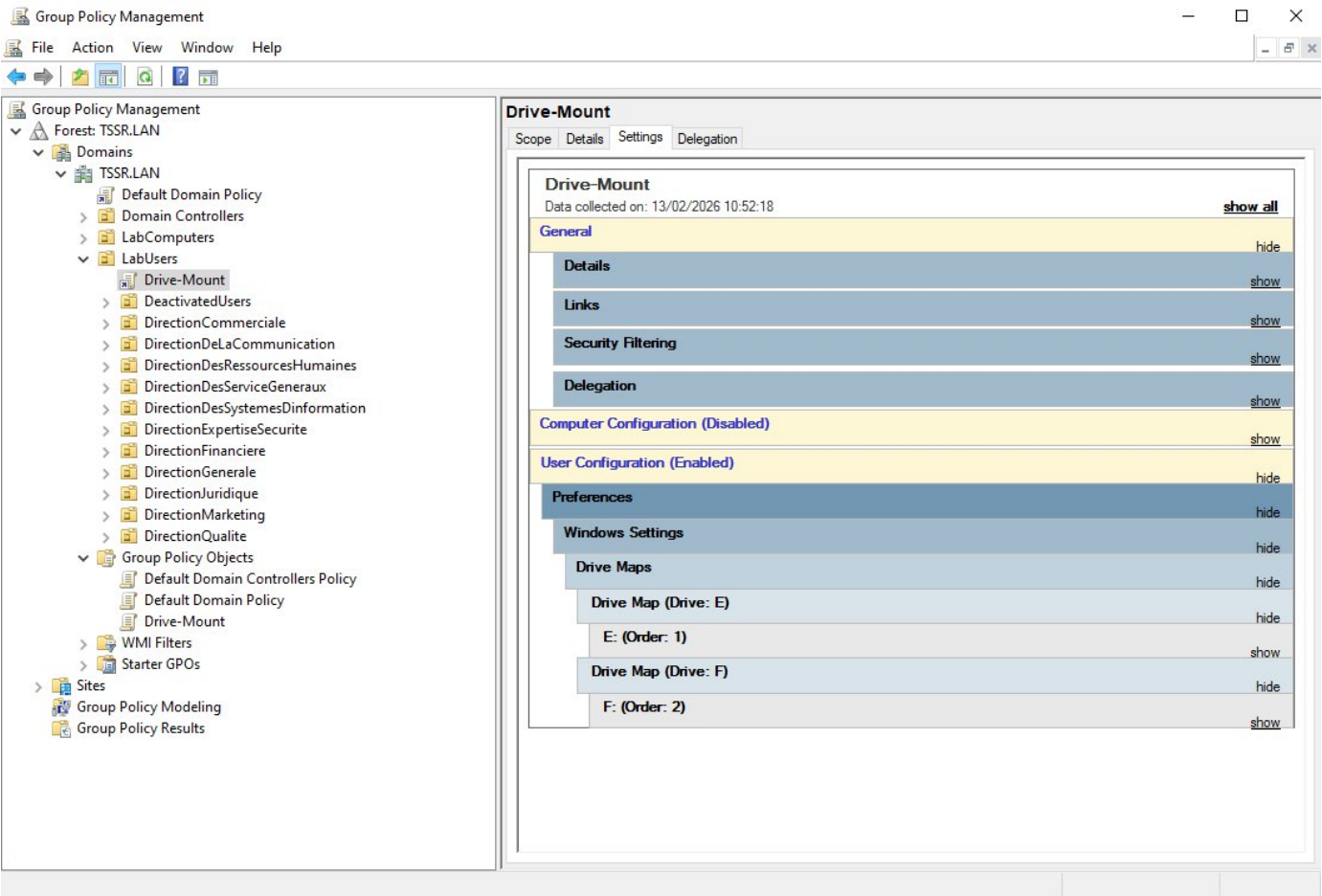
More Information

OK Cancel

Partie 3

Q.1.3.1

Copies d'écran de la GPO de montage de lecteurs.

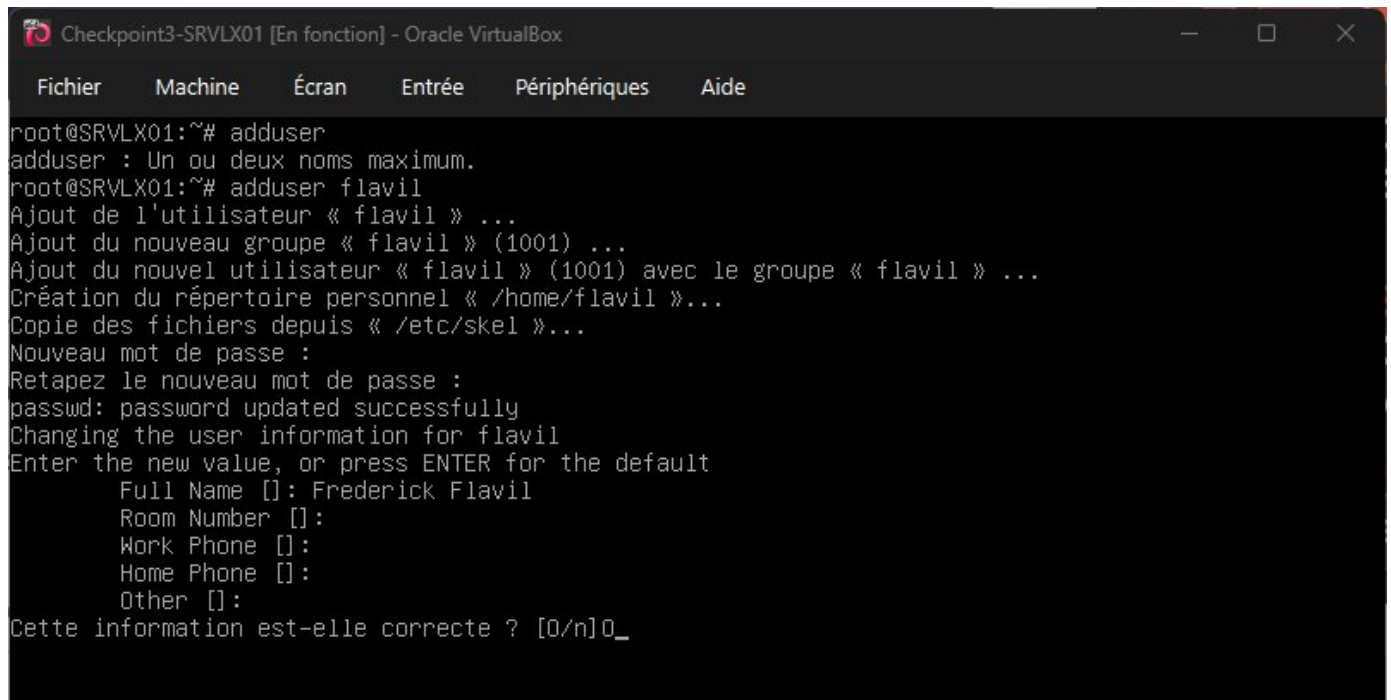


Exercice 2

Partie 1

Q.2.1.1

Copie d'écran de la création de compte.



```
Checkpoint3-SRVLX01 [En fonction] - Oracle VirtualBox
Fichier  Machine  Écran  Entrée  Périphériques  Aide

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

Q.2.1.2

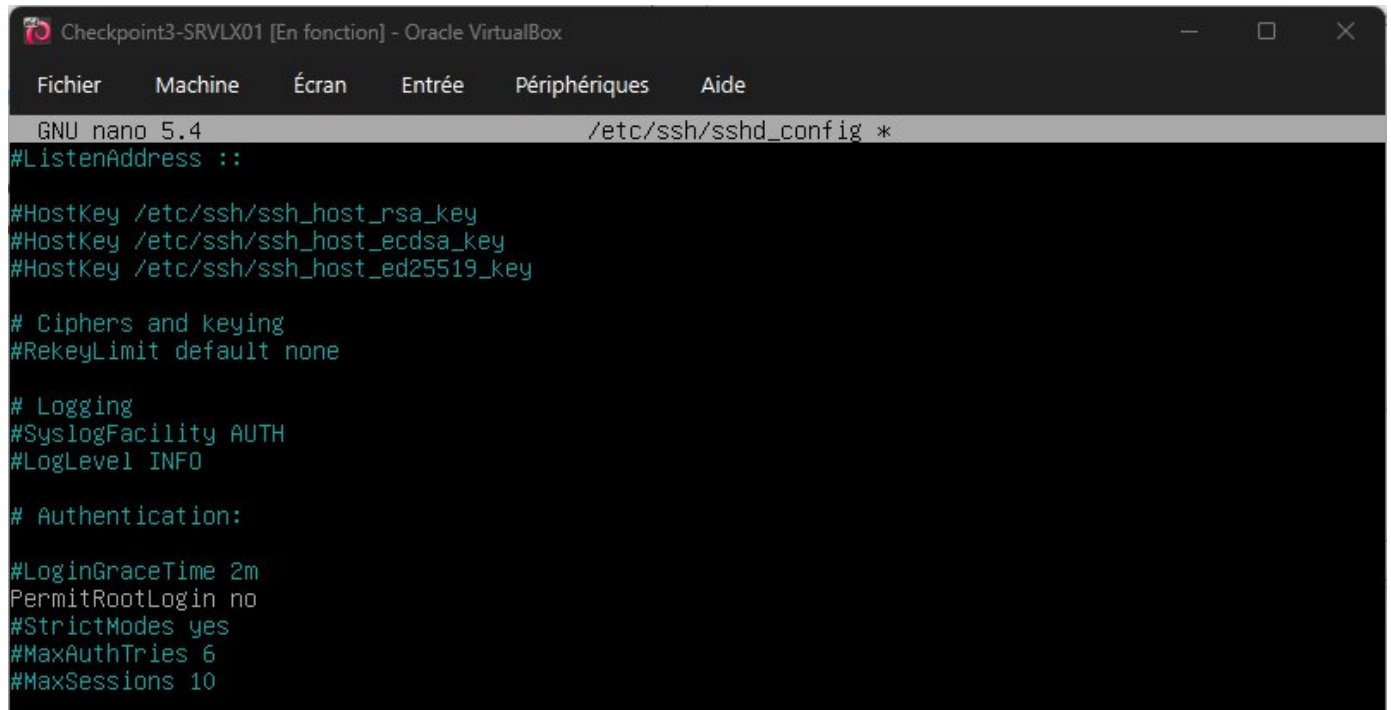
Copie d'écran du paramétrage du compte.

Copie d'écran

Partie 2

Q.2.2.1

Copie d'écran du paramétrage de l'accès distant.



```
Checkpoint3-SRV LX01 [En fonction] - Oracle VirtualBox
Fichier  Machine  Écran  Entrée  Périphériques  Aide
GNU nano 5.4 /etc/ssh/sshd_config *
#ListenAddress ::

#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

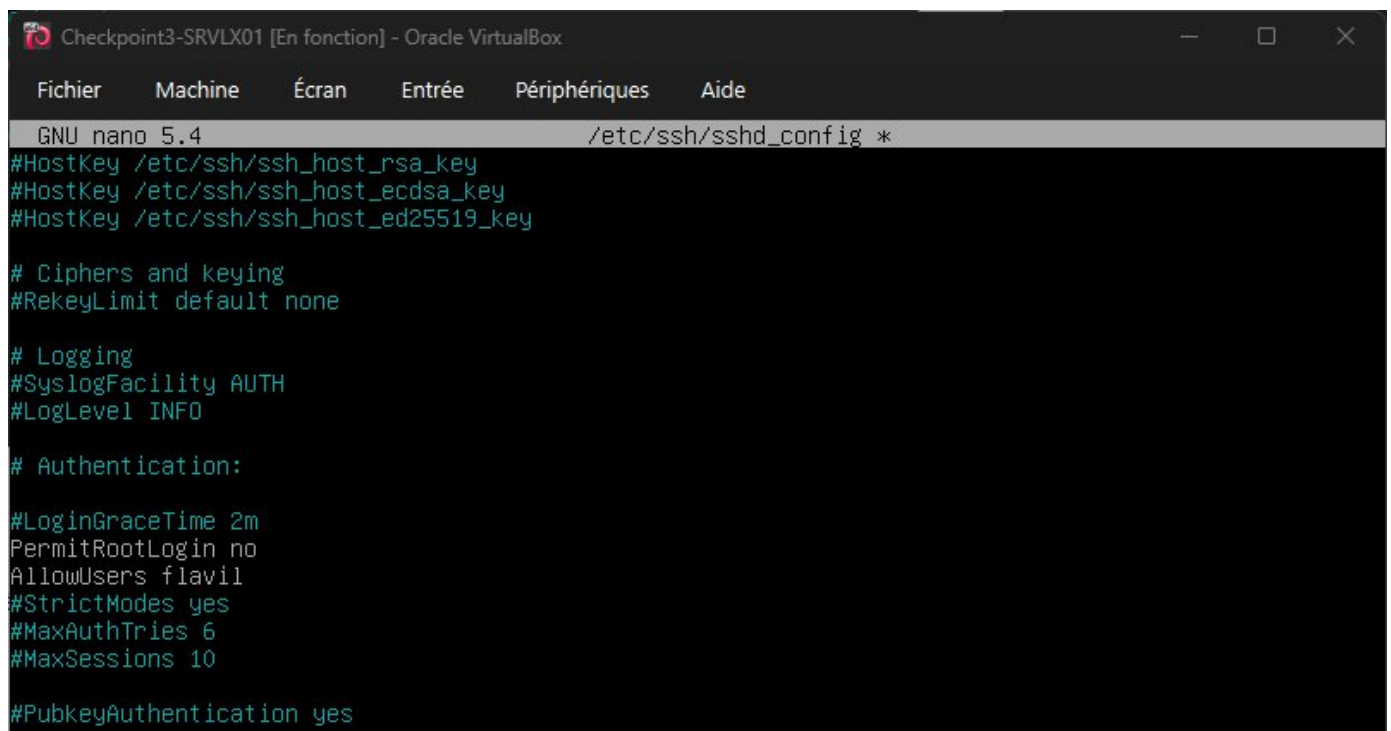
# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

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

Q.2.2.2

Copie d'écran du paramétrage distant avec le compte personnel.



```
Checkpoint3-SRV LX01 [En fonction] - Oracle VirtualBox
Fichier  Machine  Écran  Entrée  Périphériques  Aide
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

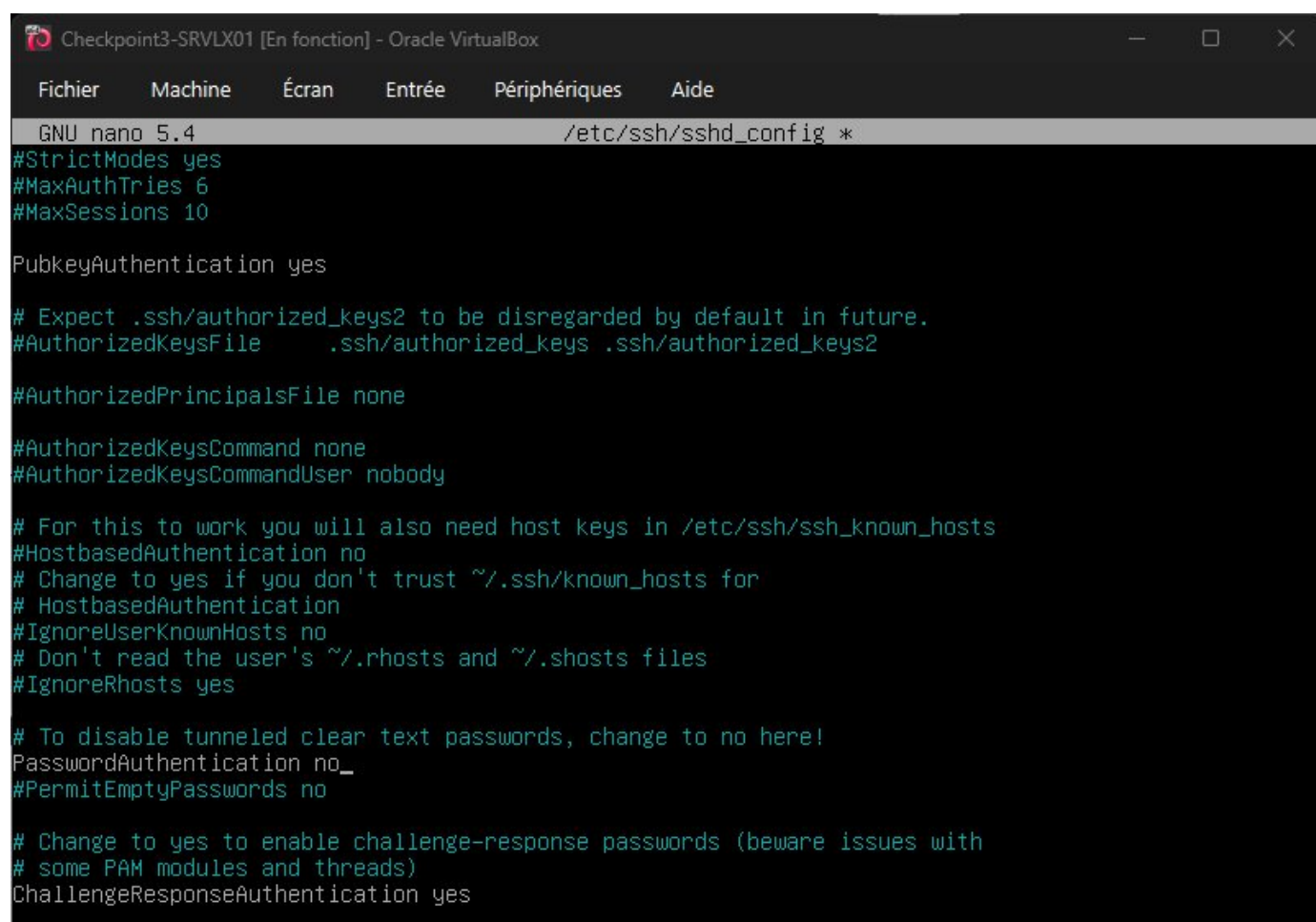
# Authentication:

#LoginGraceTime 2m
PermitRootLogin no
AllowUsers flavi1
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes
```


Q.2.2.3

Copies d'écran du paramétrage de l'authentification.



```
Checkpoint3-SRVLX01 [En fonction] - Oracle VirtualBox
Fichier  Machine  Écran  Entrée  Périphériques  Aide
GNU nano 5.4 /etc/ssh/sshd_config *
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile .ssh/authorized_keys .ssh/authorized_keys2

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

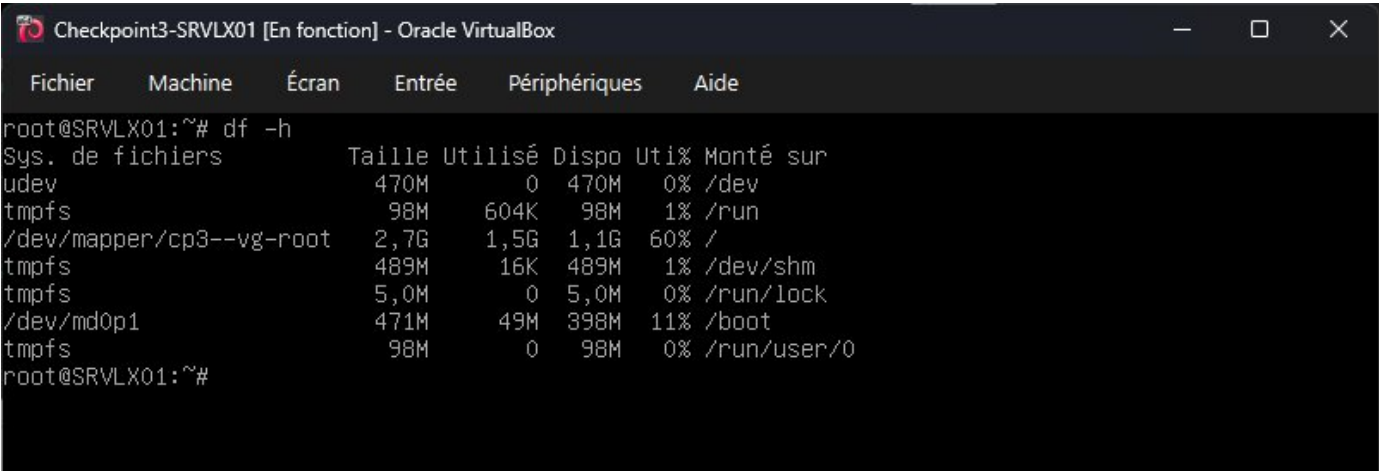
# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication no_
#PermitEmptyPasswords no

# Change to yes to enable challenge-response passwords (beware issues with
# some PAM modules and threads)
ChallengeResponseAuthentication yes
```

Partie 3

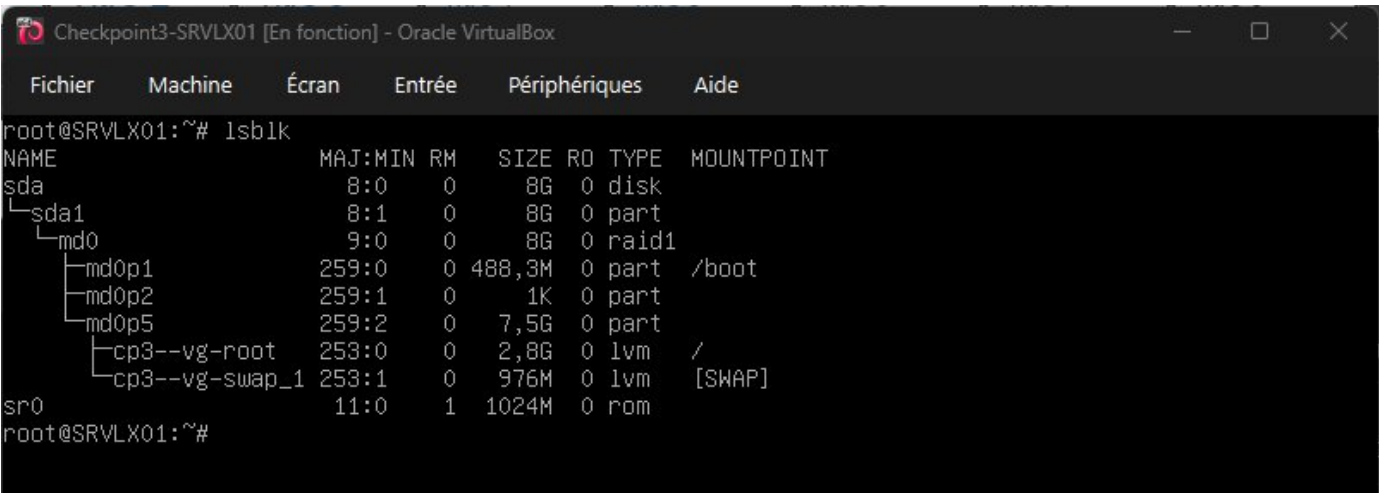
Q.2.3.1

Copie d'écran montrant les systèmes de fichiers montés.



Q.2.3.2

Copie d'écran montrant les systèmes de stockage utilisés.



Q.2.3.3

Copies d'écran montrant les différentes étapes pour la réparation du volume RAID.

```
Checkpoint3-SRV LX01 [En fonction] - Oracle VirtualBox
Fichier  Machine  Écran  Entrée  Périphériques  Aide

root@SRVLX01:~# root
-bash: root : commande introuvable
root@SRVLX01:~# 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]
sdb                                  8:16    0    8G  0 disk
sr0                                 11:0    1 1024M  0 rom
```

```
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) : p
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) : t
Partition 1 sélectionnée
Code Hexa ou synonyme (taper L pour afficher tous les codes) :FD
Type de partition « Linux » modifié en « Linux raid autodetect ».

Commande (m pour l'aide) : w_
```

```
Checkpoint3-SRV LX01 [En fonction] - Oracle VirtualBox
Fichier  Machine  Écran  Entrée  Périphériques  Aide

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                    ext2    1.0    9bba6d48-3e4b-42a6-bccc-12836de215ec
│       └─md0p5                    LVM2_m  LVM2    t1CGJ2-LG5u-KWGc-8ku0-wAiU-icBu-07BEcN
│           ├─cp3--vg-root          ext4    1.0    bbc31a37-8e49-47fe-8fad-a3fe18919fdd    1G        56% /
│           └─cp3--vg-swap_1        swap    1        8220bf51-2675-4203-91af-1c149f717652    [SWAP]
sdb
├─sdb1                              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                    ext2    1.0    9bba6d48-3e4b-42a6-bccc-12836de215ec
│       └─md0p5                    LVM2_m  LVM2    t1CGJ2-LG5u-KWGc-8ku0-wAiU-icBu-07BEcN
│           ├─cp3--vg-root          ext4    1.0    bbc31a37-8e49-47fe-8fad-a3fe18919fdd    1G        56% /
│           └─cp3--vg-swap_1        swap    1        8220bf51-2675-4203-91af-1c149f717652    [SWAP]
sr0
root@SRVLX01:~#
```

```
Checkpoint3-SRVLX01 [En fonction] - Oracle VirtualBox
Fichier  Machine  Écran  Entrée  Périphériques  Aide

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 : 2
    Persistence : Superblock is persistent

    Update Time : Fri Feb 13 12:02:21 2026
    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 : 2889

    Number  Major  Minor  RaidDevice State
     0         8        1         0  active sync  /dev/sda1
     2         8       17         1  active sync  /dev/sdb1
root@SRVLX01:~#
```

Q.2.3.4

Copies d'écran montrant les différentes étapes de configuration.

Copies d'écran

Q.2.3.5

Copie d'écran montrant l'espace disponible.

Copie d'écran

Partie 4

Q.2.4.1

Alors voici la configuration des 3 machines :

- **bareos-dir (director)** est installé sur le serveur de sauvegarde.
- **bareos-sd (storage daemon)** est installé sur le stockage (ex : un stockage isolé)
- **bareos-fd (file daemon)** est installé sur le serveur de fichiers (ou machines à sauvegarder), c'est un agent.

Le director va communiquer avec le file daemon à l'aide d'une configuration lui permettant d'ordonner la connexion entre le fd et le sd afin de lancer le processus en utilisant une périodicité définie pour les sauvegardes complètes, incrémentielles ou différentielle.

Partie 5

Q.2.5.1

Les règles de filtrages sont :

- **ct state established, related accept** : Autorise les paquets des connexions établies
- **ct state invalid drop** : Rejet des paquets de connexion invalide
- **iifname « lo » accept** : Doit certainement autoriser une machine « lo »
- **tcp dport 22 accept** : Pour autoriser les connexions SSH via la port par défaut (22)
- **ip protocol icmp accept** : Pour autoriser le protocole ICMP IPv6
- **ip6 nexthdr ipv6-icmp accept** : Pour autoriser le protocole ICMP IPv6

Q.2.5.2

La communication SSH via le port 22 en TCP.

Q.2.5.3

Tout ce qui n'est pas autorisé comme énoncé dans la réponse 2.5.1 est systématiquement rejeté par rapport à la politique de filtrage « policy drop ».

Q.2.5.4

Réponse à la question

Partie 6

Q.2.6.1

Réponse à la question

