

# 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 shows two windows side-by-side, both titled "Properties".

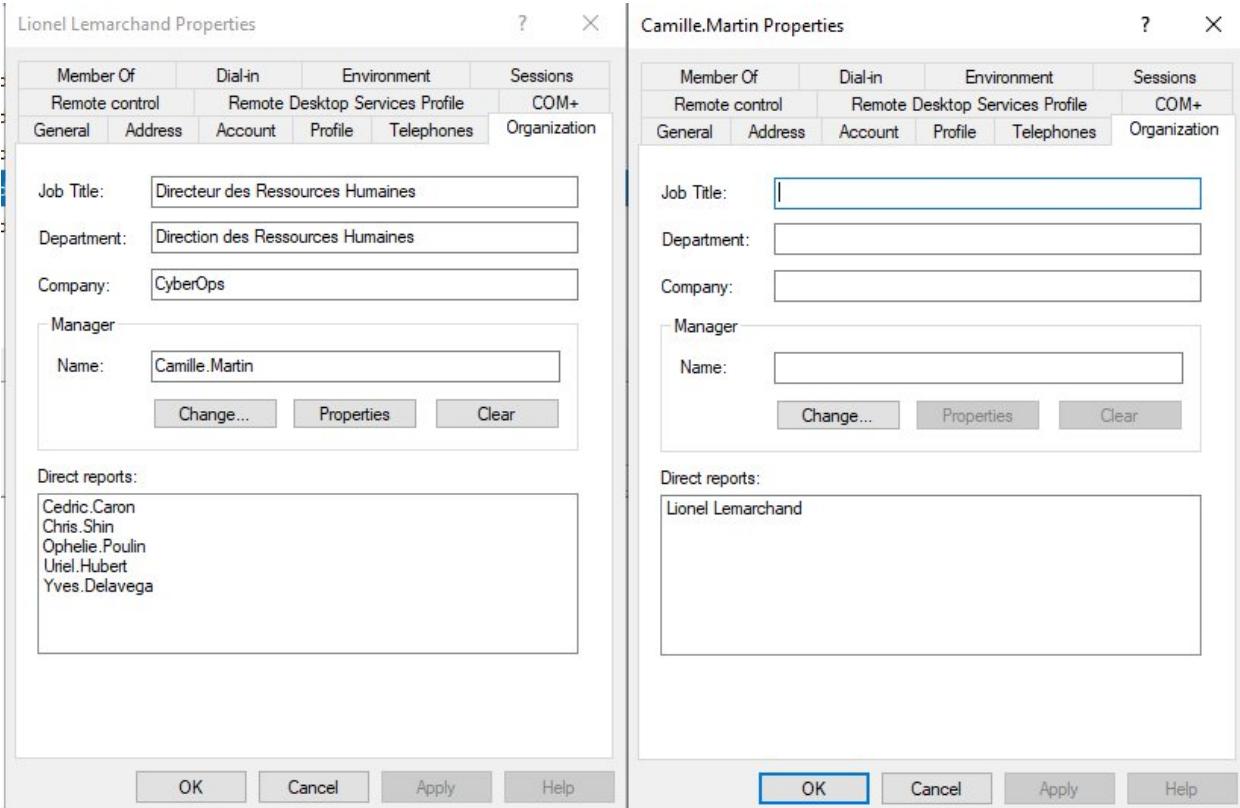
**Lionel Lemarchand Properties:**

- General Tab:**
  - Job Title: Directeur des Ressources Humaines
  - Department: Direction des Ressources Humaines
  - Company: CyberOps
  - Manager:
    - Name: Camille.Martin
  - Buttons: Change..., Properties, Clear
- Direct reports:** (Empty list)
- Buttons at the bottom:** OK, Cancel, Apply, Help

**Kelly.Rhameur Properties:**

- General Tab:**
  - Job Title: Directrice des Ressources Humaines
  - Department: Direction des Ressources Humaines
  - Company: CyberOps
  - Manager:
    - Name: Camille.Martin
  - Buttons: Change..., Properties, Clear
- Direct reports:**
  - Cedric.Caron
  - Chris.Shin
  - Ophelie.Poulin
  - Uriel.Hubert
  - Yves.Delavega
- Buttons at the bottom:** OK, Cancel, Apply, Help

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



### Q.1.1.2

Copie d'écran de l'OU DeactivatedUsers.

The screenshot shows the 'Active Directory Users and Computers' snap-in. The left pane displays a tree view of the directory structure under 'TSSR.LAN'. The 'DeactivatedUsers' folder is highlighted in blue. The right pane shows a list of users with their names and types.

**Active Directory Users and Computers**

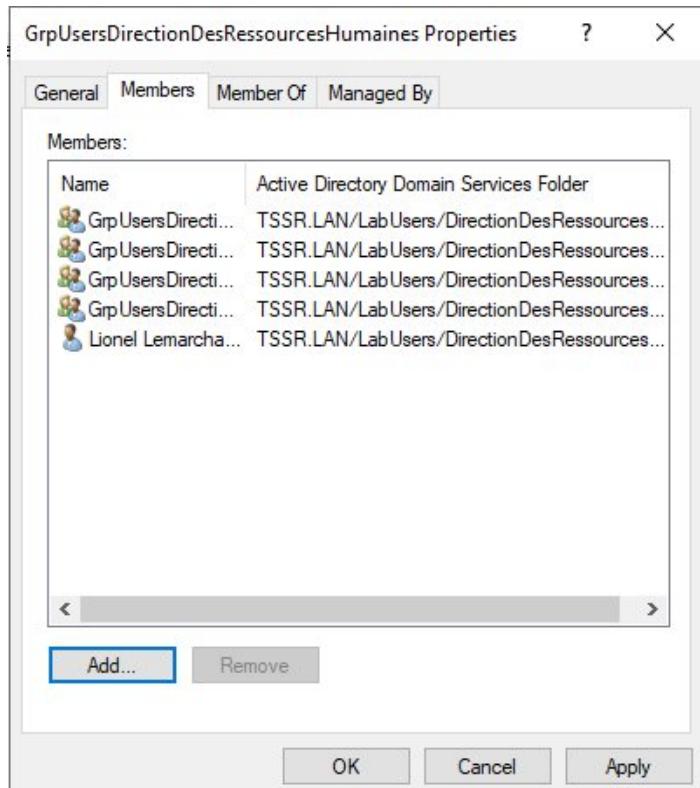
File Action View Help

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

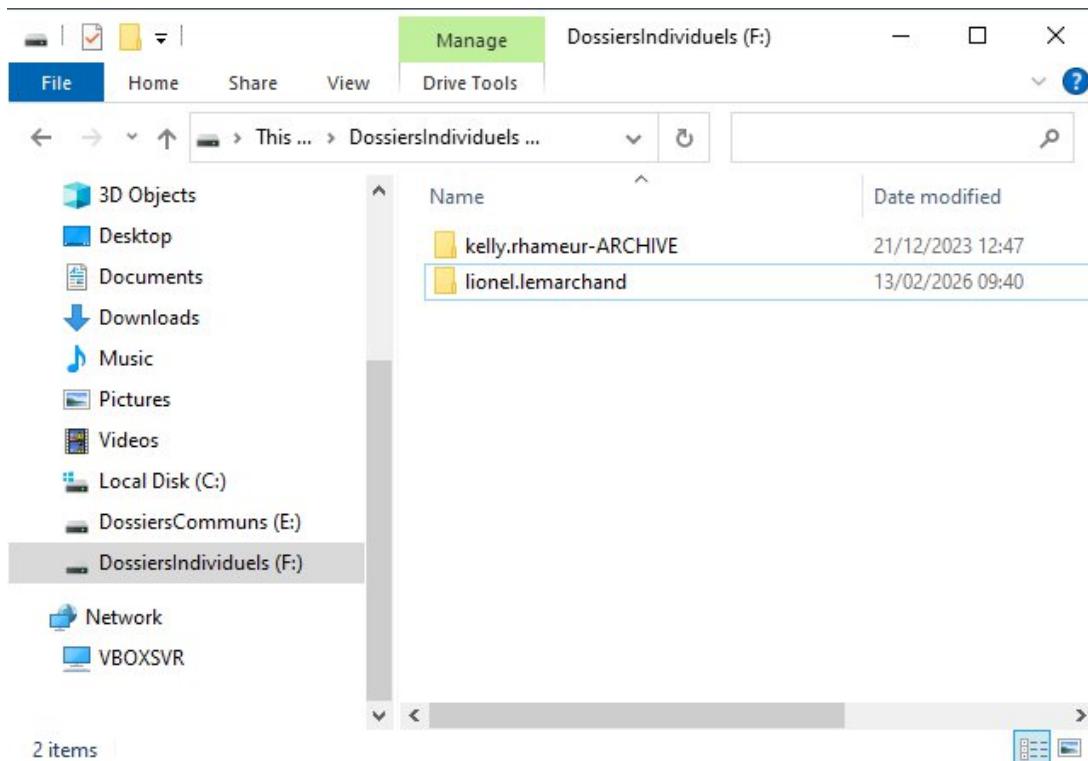
#### Q.1.1.3

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



#### Q.1.1.4

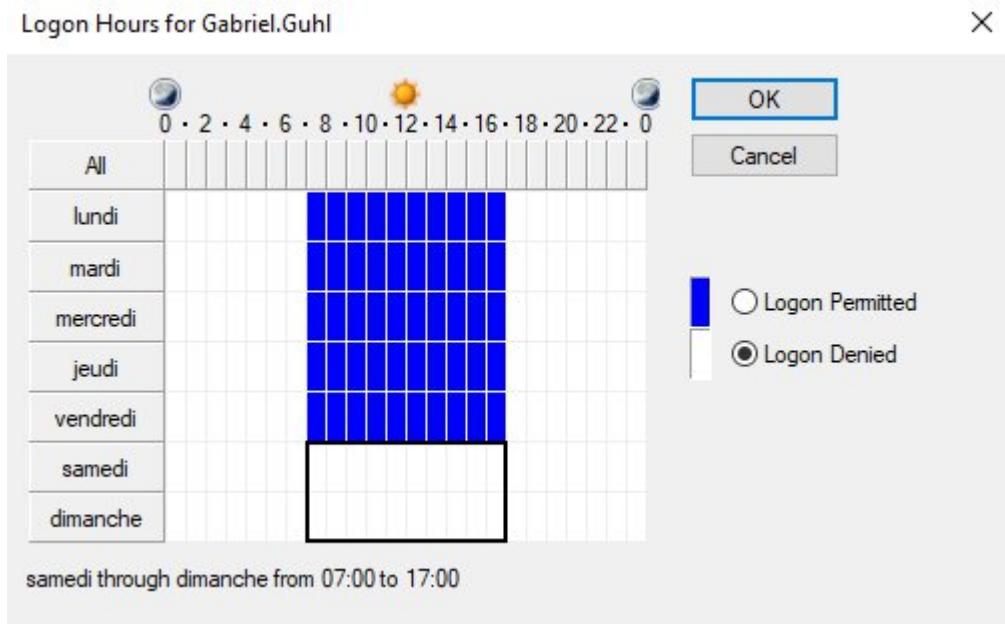
Copie d'écran des dossiers individuels demandés.



## Partie 2

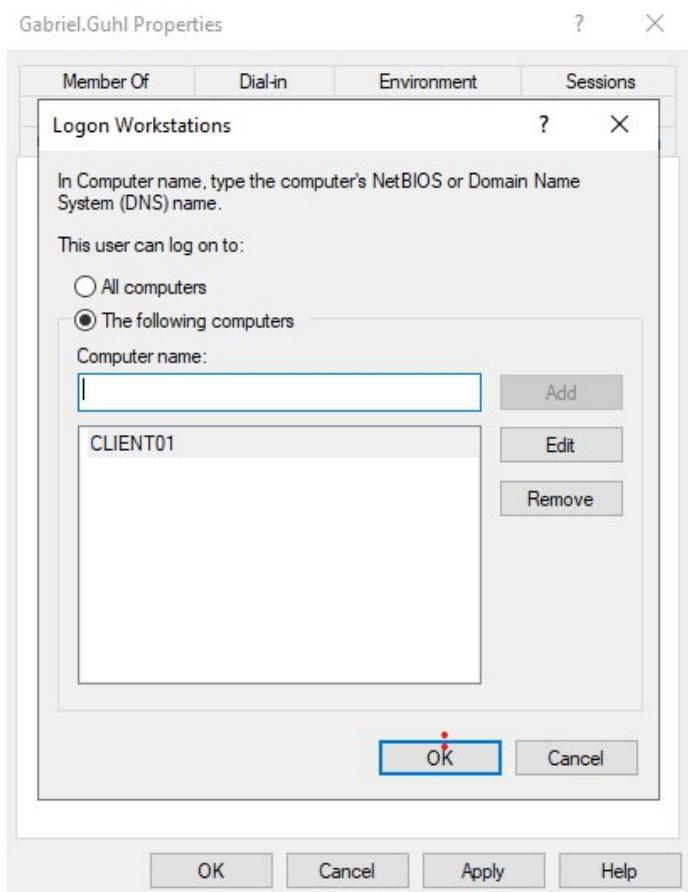
### Q.1.2.1

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

Password Settings		Directly Applies To					
Precedence:	* 15	Enforce minimum password age	User cannot change the password within (days): * 7				
<input checked="" type="checkbox"/> Enforce minimum password length	Minimum password length (characters): * 15	<input checked="" type="checkbox"/> Enforce maximum password age	User must change the password after (days): * 90				
<input checked="" type="checkbox"/> Enforce password history	Number of passwords remembered: * 12	<input checked="" type="checkbox"/> Enforce account lockout policy:	Number of failed logon attempts allowed: * 3				
<input checked="" type="checkbox"/> Password must meet complexity requirements		Reset failed logon attempts count after (mins): * 15	Account will be locked out				
<input type="checkbox"/> Store password using reversible encryption		<input type="radio"/> For a duration of (mins): * 30	<input checked="" type="radio"/> Until an administrator manually unlocks the account				
<input checked="" type="checkbox"/> Protect from accidental deletion							
Description:							
Directly Applies To							
<table border="1"><thead><tr><th>Name</th><th>Mail</th></tr></thead><tbody><tr><td colspan="2">Domain Users</td></tr></tbody></table>		Name	Mail	Domain Users		<input type="button" value="Add..."/>	<input type="button" value="Remove"/>
Name	Mail						
Domain Users							
<input type="button" value="More Information"/>		<input type="button" value="OK"/>	<input type="button" value="Cancel"/>				

# Partie 3

## Q.1.3.1

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

The screenshot shows the Windows Group Policy Management console. On the left, the navigation pane displays the forest structure under 'Forest: TSR.LAN'. The 'Domains' node is expanded, showing 'TSSR.LAN' which contains 'Default Domain Policy', 'Domain Controllers', 'LabComputers', and 'LabUsers'. 'LabUsers' is further expanded to show 'Drive-Mount' and several other policy items. The 'Group Policy Objects' node also contains 'Default Domain Controllers Policy', 'Default Domain Policy', and 'Drive-Mount'. Below these are 'WMI Filters' and 'Starter GPOs'. The 'Sites', 'Group Policy Modeling', and 'Group Policy Results' nodes are also listed. On the right, the main pane is titled 'Drive-Mount' and shows the 'Scope' tab selected. It displays the 'Drive-Mount' policy settings, including 'Computer Configuration (Disabled)' and 'User Configuration (Enabled)'. Under 'User Configuration', the 'Preferences' section is expanded, showing 'Windows Settings' and 'Drive Maps'. The 'Drive Maps' section lists 'Drive Map (Drive: E)' (Order: 1) and 'Drive Map (Drive: F)' (Order: 2). The 'E' entry is currently selected. The 'Details' tab is also visible in the top right of the main pane.

# Exercice 2

## Partie 1

### Q.2.1.1

Copie d'écran de la création de compte.

```
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

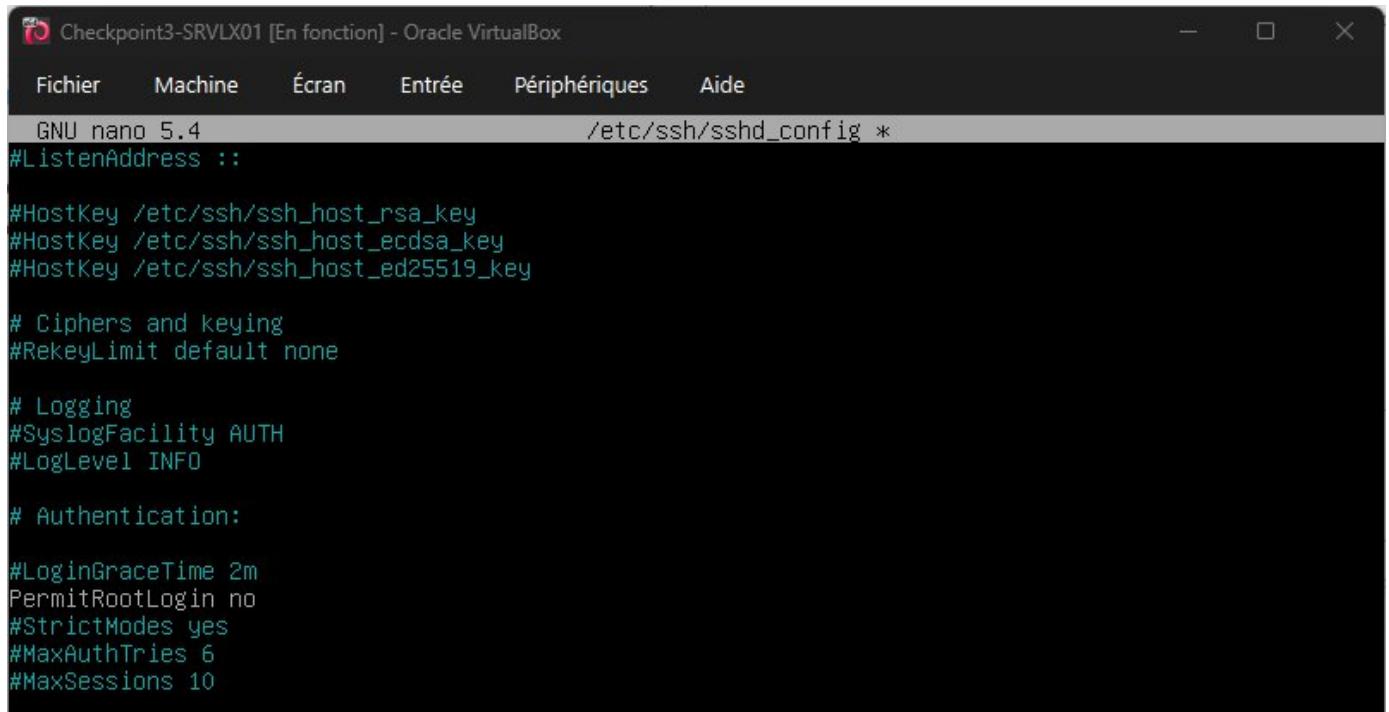
Copie d'écran du paramétrage du compte.

```
root@SRVLX01:~# usermod -aG sudo flavil
root@SRVLX01:~# id flavil
uid=1001(flavil) gid=1001(flavil) groupes=1001(flavil),27(sudo)
root@SRVLX01:~#
```

## Partie 2

### Q.2.2.1

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



The screenshot shows a terminal window titled "Checkpoint3-SRVLX01 [En fonction] - Oracle VirtualBox". The menu bar includes "Fichier", "Machine", "Écran", "Entrée", "Périphériques", and "Aide". The main area displays the contents of the /etc/ssh/sshd\_config file, which is being edited with the GNU nano 5.4 text editor. The configuration includes sections for host keys, ciphers, logging, authentication, and root login settings.

```
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

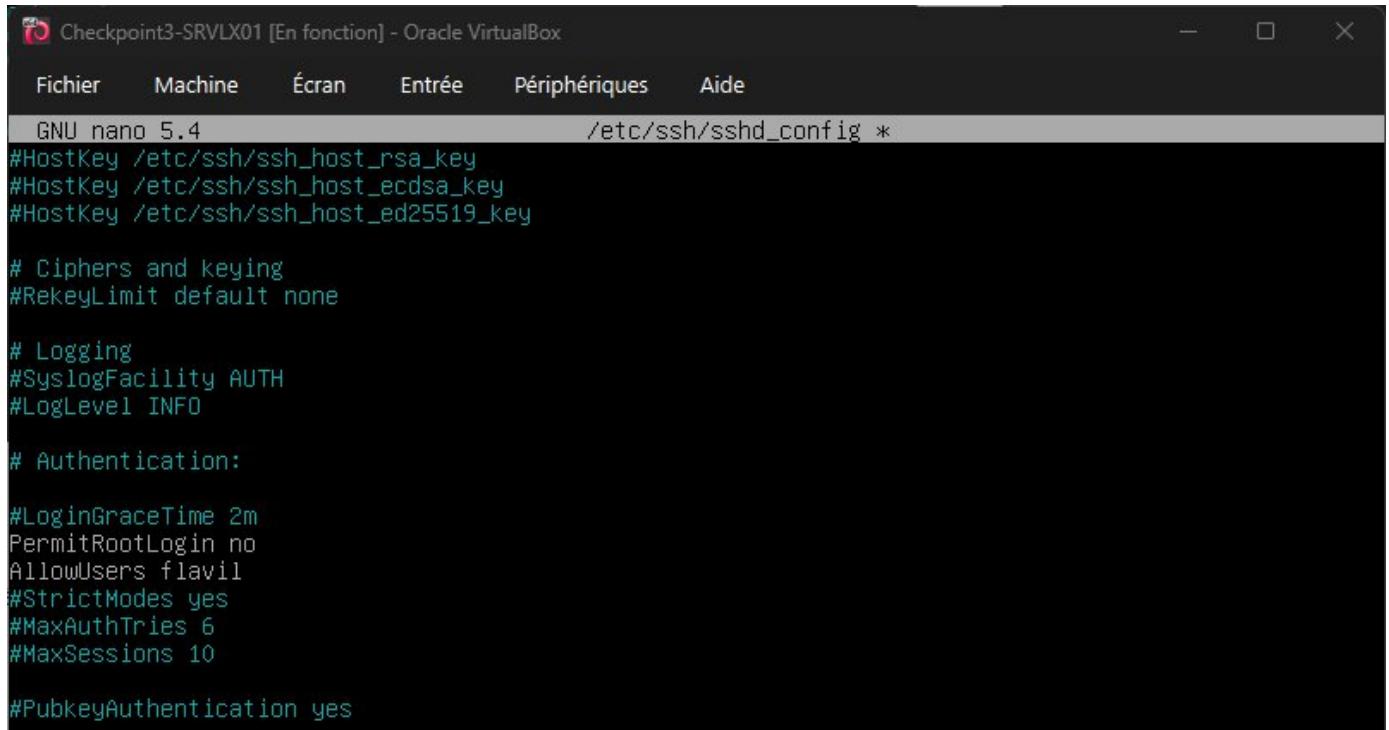
# Logging
#SyslogFacility AUTH
#LogLevel INFO

# 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.



The screenshot shows a terminal window titled "Checkpoint3-SRVLX01 [En fonction] - Oracle VirtualBox". The menu bar includes "Fichier", "Machine", "Écran", "Entrée", "Périphériques", and "Aide". The main area displays the contents of the /etc/ssh/sshd\_config file, which is being edited with the GNU nano 5.4 text editor. In addition to the standard configuration, it includes a section allowing users named "flavil" to log in via SSH.

```
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

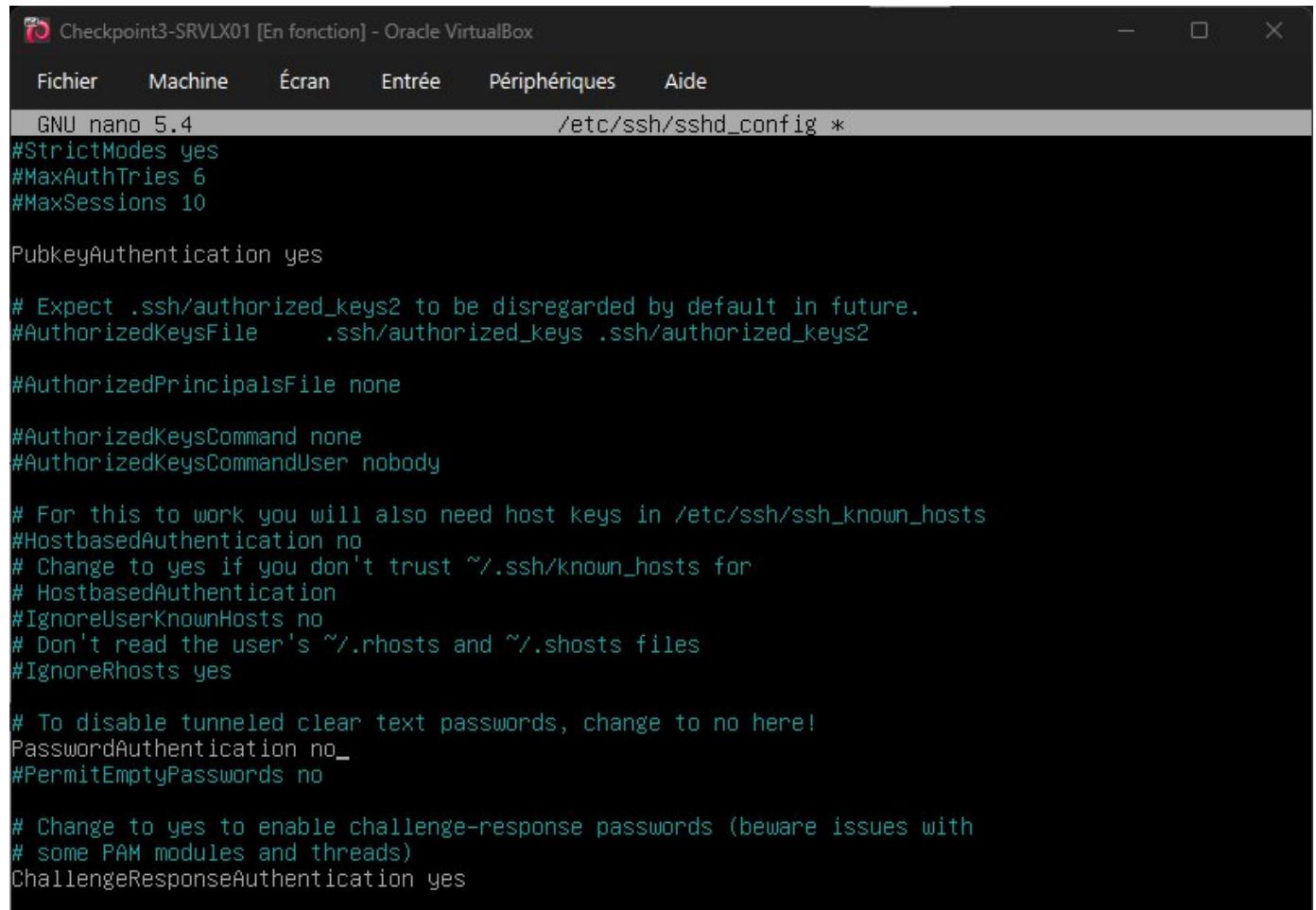
# Authentication:

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

#PubkeyAuthentication yes
```

### Q.2.2.3

Copies d'écran du paramétrage de l'authentification.



The screenshot shows a terminal window titled "Checkpoint3-SRVLX01 [En fonction] - Oracle VirtualBox". The menu bar includes "Fichier", "Machine", "Écran", "Entrée", "Périphériques", and "Aide". The main area displays the contents of the /etc/ssh/sshd\_config file, which is being edited with the nano text editor. The configuration includes various SSH authentication settings like StrictModes, MaxAuthTries, MaxSessions, PubkeyAuthentication, AuthorizedKeysFile, AuthorizedPrincipalsFile, AuthorizedKeysCommand, and HostbasedAuthentication. It also covers password authentication options such as PasswordAuthentication, PermitEmptyPasswords, and ChallengeResponseAuthentication.

```
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.

```
Fichier Machine Écran Entrée Périphériques Aide
root@SRVLX01:~# df -h
Sys. de fichiers Taille Utilisé Dispo Utile Monté sur
udev 470M 0 470M 0% /dev
tmpfs 98M 604K 98M 1% /run
/dev/mapper/cp3--vg-root 2,7G 1,5G 1,1G 60% /
tmpfs 489M 16K 489M 1% /dev/shm
tmpfs 5,0M 0 5,0M 0% /run/lock
/dev/md0p1 471M 49M 398M 11% /boot
tmpfs 98M 0 98M 0% /run/user/0
root@SRVLX01:~#
```

## Q.2.3.2

Copie d'écran montrant les systèmes de stockage utilisés.

```
Fichier Machine Écran Entrée Périphériques Aide
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]
sr0 11:0 1 1024M 0 rom
root@SRVLX01:~#
```

### Q.2.3.3

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

The screenshot shows a terminal window titled "Checkpoint3-SRVLX01 [En fonction] - Oracle VirtualBox". The terminal displays the following steps:

```
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_

```

The terminal window has a dark theme and includes a toolbar at the bottom with icons for file operations like copy, paste, and search.

The screenshot shows a terminal window titled "Checkpoint3-SRVLX01 [En fonction] - Oracle VirtualBox". The terminal displays the output of the "lsblk -f" command, showing the final state of the RAID volume:

```
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        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
    ├─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:~#
```

```
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 deamon)** est installé sur le stockage (ex : un stockage isolé)
- **bareos-fd (file deamon)** est installé sur le serveur de fichiers (ou machines à sauvegarder), c'est un agent.

Le director va communiquer avec le file deamon 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

