

CHECKPOINT 3

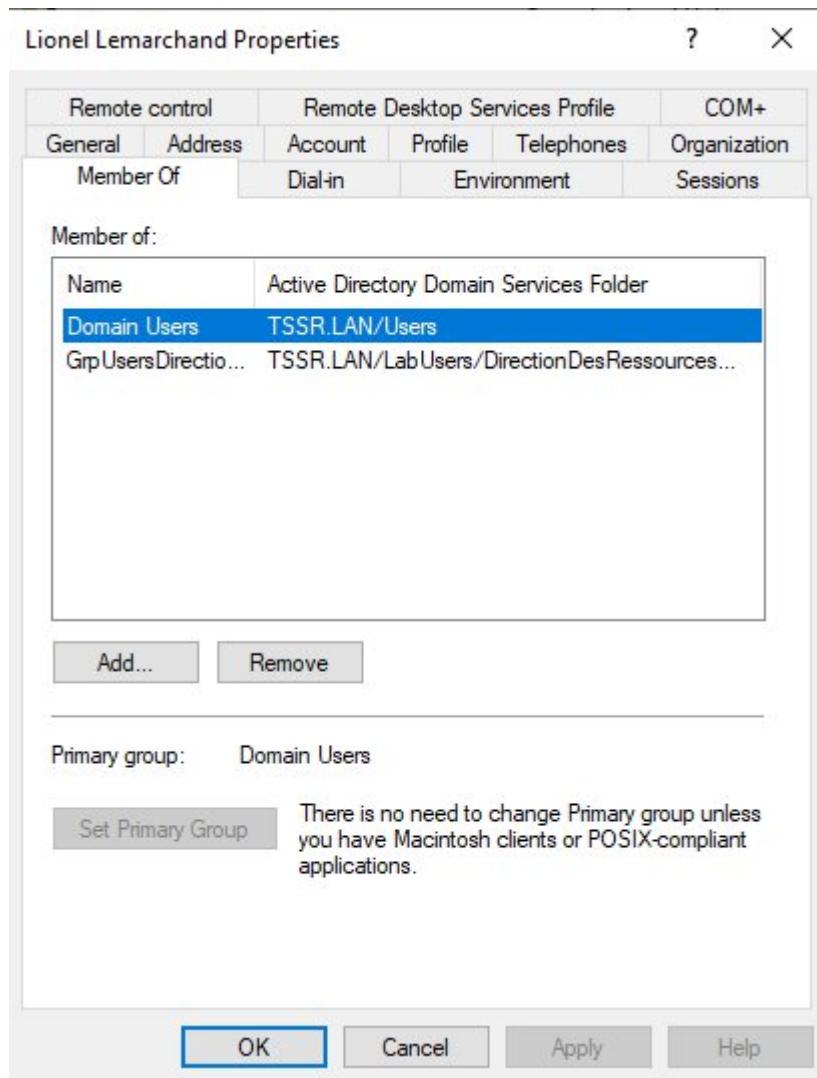
Formulaire réponses

Exercice 1

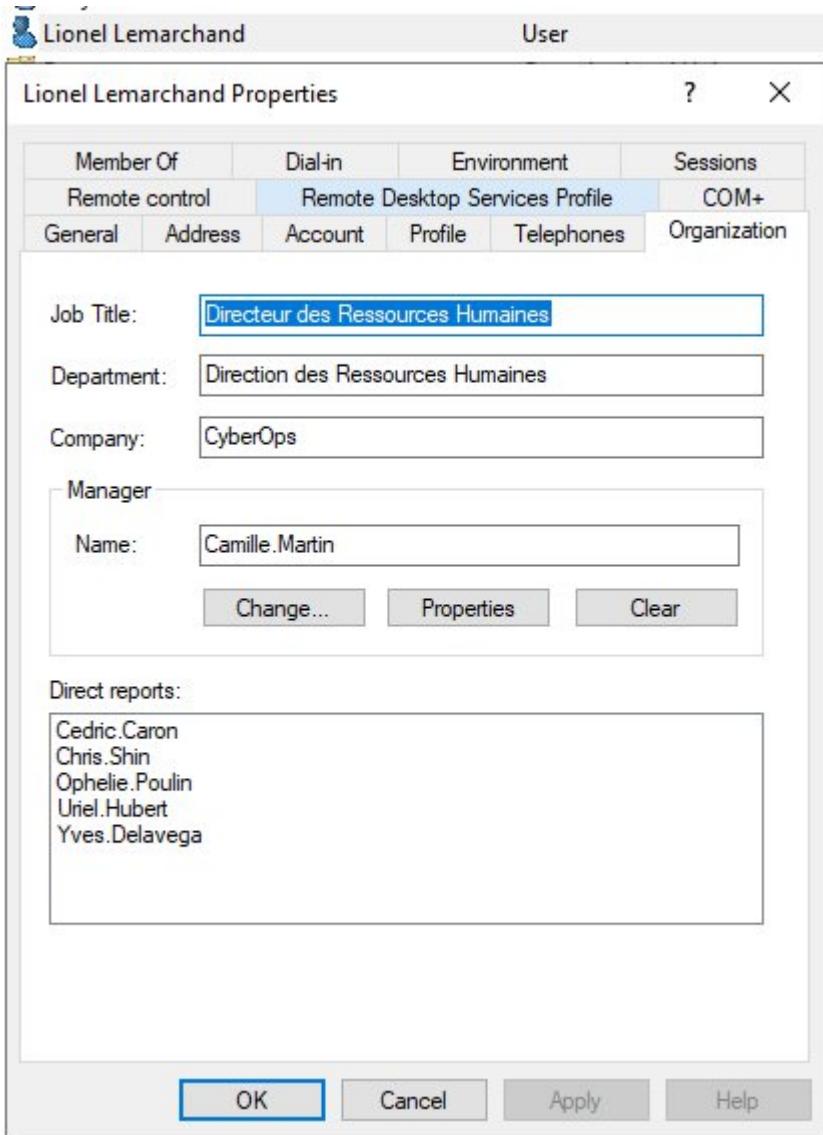
Partie 1

Q.1.1.1

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



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' interface. The left pane shows a tree view of the directory structure under 'TSSR.LAN'. The 'DeactivatedUsers' folder is highlighted. The right pane displays a table of users in the 'LabUsers' container. The table has columns for 'Name', 'Type', and 'Description'. One user, 'Kelly.Rhameur', is listed as a 'User' type.

Name	Type	Description
Kelly.Rhameur	User	

Q.1.1.3

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

The screenshot shows the Windows Active Directory Users and Computers interface. On the left, a tree view of the directory structure is visible, including 'Saved Queries', 'TSSR.LAN' (which is expanded to show 'Builtin', 'Computers', 'Domain Controllers', 'ForeignSecurityPrincipals', 'LabComputers', 'LabUsers' (expanded to show various departmental groups like 'DirectionCommerciale' through 'DirectionQualite'), 'Managed Service Accounts', and 'Users'), and 'DesactivatedUsers'. On the right, the properties of a user account named 'Kelly.Rhameur' are displayed. The 'General' tab is selected in the top navigation bar. The 'Member Of' section shows 'Active Directory Domain Services Folder' and 'TSSR.LAN/Users' under 'Domain Users'. A note at the bottom states: 'There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.' At the bottom of the dialog are buttons for 'OK', 'Cancel', 'Apply', and 'Help'.

Q.1.1.4

Copie d'écran des dossiers individuels demandés.

The screenshot shows the 'Active Directory Users and Computers' interface. On the left, a tree view shows the structure of the domain: 'Active Directory Users and Computers [SRVWIN01.TSSR.LAN]', 'Saved Queries', 'TSSR.LAN' (expanded to show 'BuiltIn', 'Computers', 'Domain Controllers', 'ForeignSecurityPrincipals', 'LabComputers'), 'LabUsers' (expanded to show various departmental groups like 'DirectionCommerciale', 'DirectionDeLaCommunication', etc., and 'DesactivatedUsers' which contains 'Kelly.Rhameur-ARCHIVE'), 'Managed Service Accounts', and 'Users'. On the right, a table lists the found object: 'Name' (Kelly.Rhameur-ARCHIVE), 'Type' (User), and 'Description' (empty). The 'Kelly.Rhameur-ARCHIVE' entry is highlighted in blue.

Partie 2

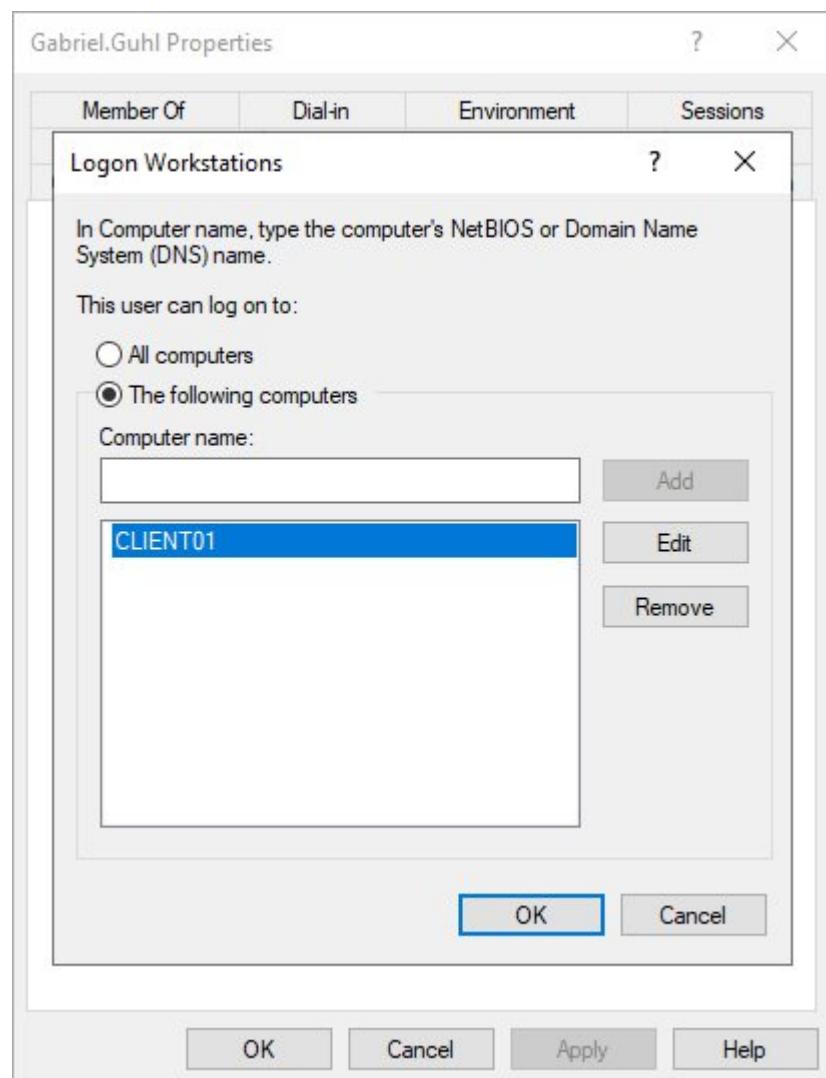
Q.1.2.1

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

The screenshot shows the 'Logon Hours for Gabriel.Guhl' dialog box. At the top, there's a title bar with 'Logon Hours for Gabriel.Guhl' and a close button ('X'). Below the title bar is a horizontal timeline from 0 to 24 hours, with icons for night (blue circle) and day (orange sun) at the ends. The timeline has tick marks every 2 hours (0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 0). To the right of the timeline are 'OK' and 'Cancel' buttons. A legend below the timeline indicates that blue squares represent 'Logon Permitted' and white squares represent 'Logon Denied'. On the left, a vertical list shows days of the week: 'All', 'lundi', 'mardi', 'mercredi', 'jeudi', 'vendredi', 'samedi', and 'dimanche'. The 'lundi' row has a blue square at the 00:00 position, indicating a logon restriction from 00:00 to 01:00. At the bottom left, the text 'lundi from 00:00 to 01:00' is displayed.

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.

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

Name	Type	Description
DesactivatedUsers	Organizational Unit	
DirectionCommerciale	Organizational Unit	
DirectionDeLaCommunication	Organizational Unit	
DirectionDesRessourcesHumaines	Organizational Unit	
DirectionDesServiceGeneraux	Organizational Unit	
DirectionDesSystemesDinformation	Organizational Unit	
DirectionExpertiseSecurite	Organizational Unit	
DirectionFinanciere	Organizational Unit	
DirectionGenerale	Organizational Unit	
DirectionJuridique	Organizational Unit	
DirectionMarketing	Organizational Unit	
DirectionQualite	Organizational Unit	
GrpUsersPasswordRestricted	Security Group - Global	

PSOUsersPasswordRestricted Properties

General Members Member Of Managed By

Members:

Name	Active Directory Domain Services Folder
Arav Kuznet...	TSSR.LAN/Lab Users/DirectionExpertiseSecurite
Aaron.Roche...	TSSR.LAN/Lab Users/DirectionDesSystemesDin...
Adam.Edison...	TSSR.LAN/Lab Users/DirectionExpertiseSecurite
Adrian.Schultz...	TSSR.LAN/Lab Users/DirectionDeLaCommunica...
Adrien.Foll...	TSSR.LAN/Lab Users/DirectionDesSystemesDin...
Ahmed.Ali...	TSSR.LAN/Lab Users/DirectionFinanciere/Servi...
Alan.Meunier...	TSSR.LAN/Lab Users/DirectionDesSystemesDin...
Alban.Dumas...	TSSR.LAN/Lab Users/DirectionDeLaCommunica...
Alejandro.Sury...	TSSR.LAN/Lab Users/DirectionQualite/Laborato...
Alex.Lebarlier...	TSSR.LAN/Lab Users/DirectionFinanciere/Finan...
Alexandre.Ch...	TSSR.LAN/Lab Users/DirectionDeLaCommunica...
Alexis.Flemmard...	TSSR.LAN/Lab Users/DirectionGenerale/Directi...
Alice.Hussein...	TSSR.LAN/Lab Users/DirectionCommerciale/Advi...

OK Cancel Apply

Password Settings

Name: PSOUsersPasswordRestricted
Precedence: 1

Enforce minimum password length
Minimum password length (characters): 12

Enforce password history
Number of passwords remembered: 5

Password must meet complexity requirements

Store password using reversible encryption

Protect from accidental deletion

Directly Applies To

Name	Mail
GrpUsersPasswordRestrict...	

Add... Remove

More Information

Partie 3

Q.1.3.1

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

The screenshot shows the Group Policy Management console. On the left, the navigation pane displays the forest 'TSSR.LAN' and various GPOs under 'Domains'. The 'PROD_Users_Drive-Mount' GPO is selected. The main pane shows the 'PROD_Users_Drive-Mount' properties. Under the 'Scope' tab, it lists 'Links' to 'TSSR LAN' and 'LabUsers'. A table shows the link settings for 'LabUsers': Location (LabUsers), Enforced (No), Link Enabled (Yes), and Path (TSSR.LAN/LabUsers). Under the 'Security Filtering' tab, it specifies that the settings apply to 'Authenticated Users'.

Two 'New Drive Properties' dialog boxes are shown side-by-side. Both boxes have the 'General' tab selected. They both have 'Action' set to 'Update' and 'Location' set to '\\SRVWIN01\LecteurE' and '\\SRVWIN01\LecteurF' respectively. The 'Reconnect' checkbox is unchecked. The 'Label as:' field contains 'Lecteur E' for the left box and 'Lecteur F' for the right box. In the 'Drive Letter' section, both use 'Use:' and select drive letter 'E' for the left and 'F' for the right. In the 'Connect as (optional)' section, both have empty 'User name' and 'Password' fields, and an empty 'Confirm password' field. In the 'Hide/Show this drive' section, both choose 'No change'. In the 'Hide/Show all drives' section, both choose 'No change'. At the bottom, both have 'OK', 'Cancel', 'Apply', and 'Help' buttons.

PROD_Users_Drive-Mount [SRVWIN01.TSSR.LAN] Policies

- Computer Configuration
 - Policies
 - Preferences
- User Configuration
 - Policies
 - Preferences
 - Windows Settings
 - Applications
 - Drive Maps
 - Environment
 - Files
 - Folders
 - Ini Files
 - Registry
 - Shortcuts
 - Control Panel Settings

Drive Maps

Name	Order	Action	Path	Reconnect
E:	1	Update	\SRVWIN01\LecteurE	No
F:	2	Update	\SRVWIN01\LecteurF	No

Processing

Description

No policies selected

Exercice 2

Partie 1

Q.2.1.1

Copie d'écran de la création de compte.

```
root@SRVLX01:~# useradd sami
root@SRVLX01:~# cat /etc/passwd | grep "sami"
sami:x:1001:1001::/home/sami:/bin/sh
root@SRVLX01:~#
```

Q.2.1.2

Copie d'écran du paramétrage du compte.

```
root@SRVLX01:~# usermod -aG sudo sami
root@SRVLX01:~# passwd sami
Nouveau mot de passe :
Retapez le nouveau mot de passe :
passwd: password updated successfully
root@SRVLX01:~#
```

Partie 2

Q.2.2.1

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

```
GNU nano 5.4                               sshd_config
#      $OpenBSD: sshd_config,v 1.103 2018/04/09 20:41:22 tj Exp $

# This is the sshd server system-wide configuration file. See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/bin:/bin:/usr/sbin:/sbin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented. Uncommented options override the
# default value.

Include /etc/ssh/sshd_config.d/*.conf

GNU nano 5.4                               checkpoint3.conf *
# Création fichier checkpoint3.conf pour ajouter les configurations demandées par les questions :

# 2.2.1 Désactivation accès à distance de l'utilisateur root_
PermitRootLogin no
```

Q.2.2.2

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

```
GNU nano 5.4                               checkpoint3.conf *
# Création fichier checkpoint3.conf pour ajouter les configurations demandées par les questions :

# 2.2.1 Désactivation accès à distance de l'utilisateur root
PermitRootLogin no

# 2.2.2 Autorisation de l'utilisateur sami uniquement
AllowUsers sami
```

Q.2.2.3

Copies d'écran du paramétrage de l'authentification.

Réponse incomplète car problème de connexion. Partage de connexion au réseau mobile au lieu d'une connexion via une box.

```
GNU nano 5.4                               checkpoint3.conf *
# Création fichier checkpoint3.conf pour ajouter les configurations demandées par les questions :

# 2.2.1 Désactivation accès à distance de l'utilisateur root
PermitRootLogin no

# 2.2.2 Autorisation de l'utilisateur sami uniquement
AllowUsers sami

# 2.2.3 Authentification par clé et désactivation du mot de passe
PubkeyAuthentication yes
PasswordAuthentication no_
```

Partie 3

Q.2.3.1

Copie d'écran montrant les systèmes de fichiers montés.

```
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]
sr0
```

Q.2.3.2

Copie d'écran montrant les systèmes de stockage utilisés.

NAME	MAJ:MIN	RM	SIZE	RO	TYPE	MOUNTPOINT	TYPE
sda	8:0	0	8G	0	disk		disk
└─sda1	8:1	0	8G	0	part		part
└─md0	9:0	0	8G	0	raid1		raid1
├─md0p1	259:0	0	488,3M	0	part	/boot	part
├─md0p2	259:1	0	1K	0	part		part
├─md0p5	259:2	0	7,5G	0	part		part
│ ├─cp3--vg-root	253:0	0	2,8G	0	lvm	/	lvm
│ └─cp3--vg-swap_1	253:1	0	976M	0	lvm	[SWAP]	lvm
sr0	11:0	1	1024M	0	rom		rom

Q.2.3.3

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

```
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
sdc            8:32   0     2G  0 disk
sr0           11:0    1 1024M 0 rom
root@SRVLX01:~#
```

```
root@SRVLX01:~# cat /proc/mdstat
Personalities : [raid1] [linear] [multipath] [raid0] [raid6] [raid5] [raid4] [raid10]
md0 : active raid1 sda1[0]
      8381440 blocks super 1.2 [2/1]  [U_]

unused devices: <none>
```

```
root@SRVLX01:~# mdadm /dev/md0 -a /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 = 31.0% (2601472/8381440) finish=0.4min speed=216789K/sec

unused devices: <none>
```

```
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 [2/2]  [UU]

unused devices: <none>
```

Q.2.3.4

Copies d'écran montrant les différentes étapes de configuration.

```
root@SRVLX01:~# vgs
  VG      #PV #LV #SN Attr   VSize VFree
  cp3-vg   1   2   0 wz--n- 7,51g <3,79g
```

Ne sais plus.

Q.2.3.5

Copie d'écran montrant l'espace disponible.

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	
└─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]
sdc	8:32	0	2G	0	disk	
sr0	11:0	1	1024M	0	rom	

Sans le LVM.

Partie 4

Q.2.4.1

Réponse à la question

Partie 5

Q.2.5.1

Réponse à la question

Q.2.5.2

SSH autorisé

ICMP autorisé

ICMP IPv6 autorisé

Q.2.5.3

Réponse à la question

Q.2.5.4

Réponse à la question

Partie 6

Q.2.6.1

```
tail -n 10 /var/log/auth.log | grep "FAILED LOGIN"
```