

CHECKPOINT 3

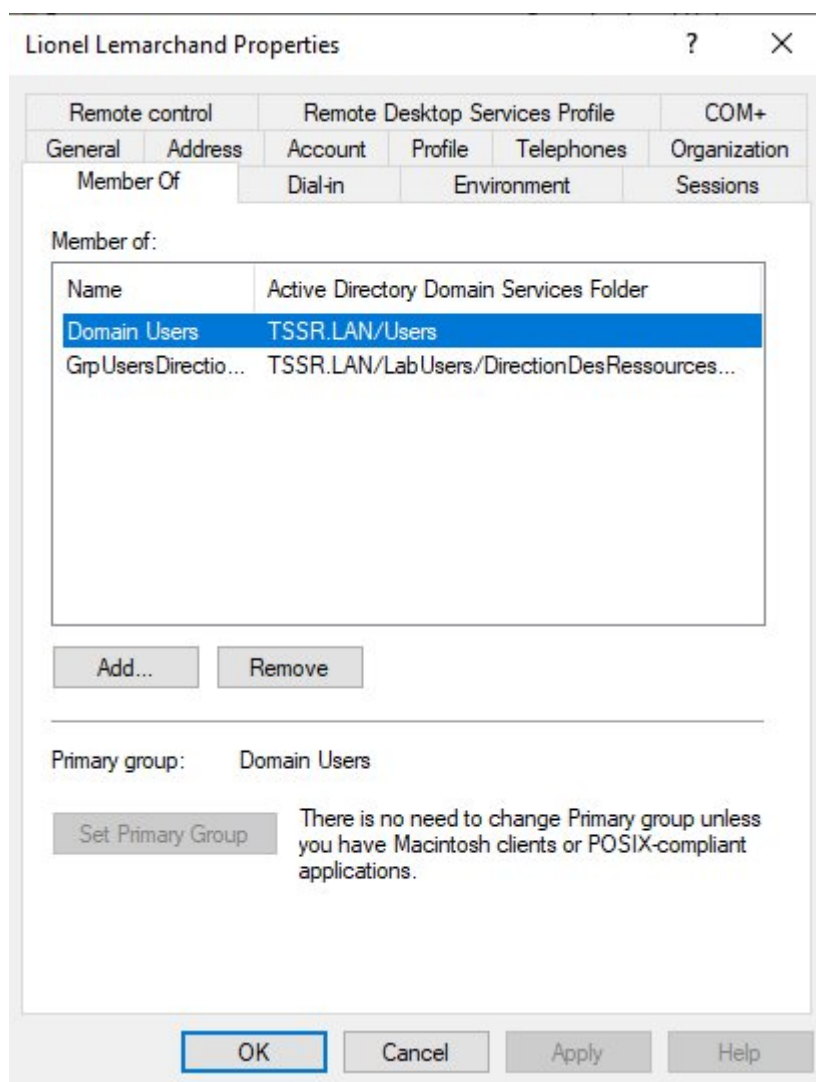
Formulaire réponses

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.

Lionel Lemarchand User

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:

- Cedric.Caron
- Chris.Shin
- Ophelie.Poulin
- Uriel.Hubert
- Yves.Delavega

OK Cancel Apply Help

Q.1.1.2

Copie d'écran de l'OU DeactivatedUsers.

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		
	DesactivatedUsers		
	Managed Service Accounts		
	Users		

Name	Type	Description
Kelly.Rhameur	User	

Q.1.1.3

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

The screenshot displays the 'Active Directory Users and Computers' console tree on the left, showing the hierarchy: Active Directory Users and Computers [SRVWIN01.TSSR.LAN] > Saved Queries > TSSR.LAN > LabUsers. The 'LabUsers' group is expanded, showing a list of subgroups: DirectionCommerciale, DirectionDeLaCommunication, DirectionDesRessourcesHumaines, DirectionDesServiceGeneraux, DirectionDesSystemesDinformation, DirectionExpertiseSecurite, DirectionFinanciere, DirectionGenerale, DirectionJuridique, DirectionMarketing, DirectionQualite, DesactivatedUsers, Managed Service Accounts, and Users. The 'DesactivatedUsers' group is highlighted.

On the right, the 'Kelly.Rhameur Properties' dialog box is open, showing the 'General' tab. The 'Name' field contains 'Kelly.Rhameur' and the 'Type' field contains 'User'. The 'Member Of' section shows a list of groups: 'Domain Users' (TSSR.LAN/Users). The 'Primary group' is set to 'Domain Users'. The 'Add...' button is highlighted.

Remote control		Remote Desktop Services Profile		COM+	
General	Address	Account	Profile	Telephones	Organization
Member Of		Dial-in	Environment	Sessions	

Member of:

Name	Active Directory Domain Services Folder
Domain Users	TSSR.LAN/Users

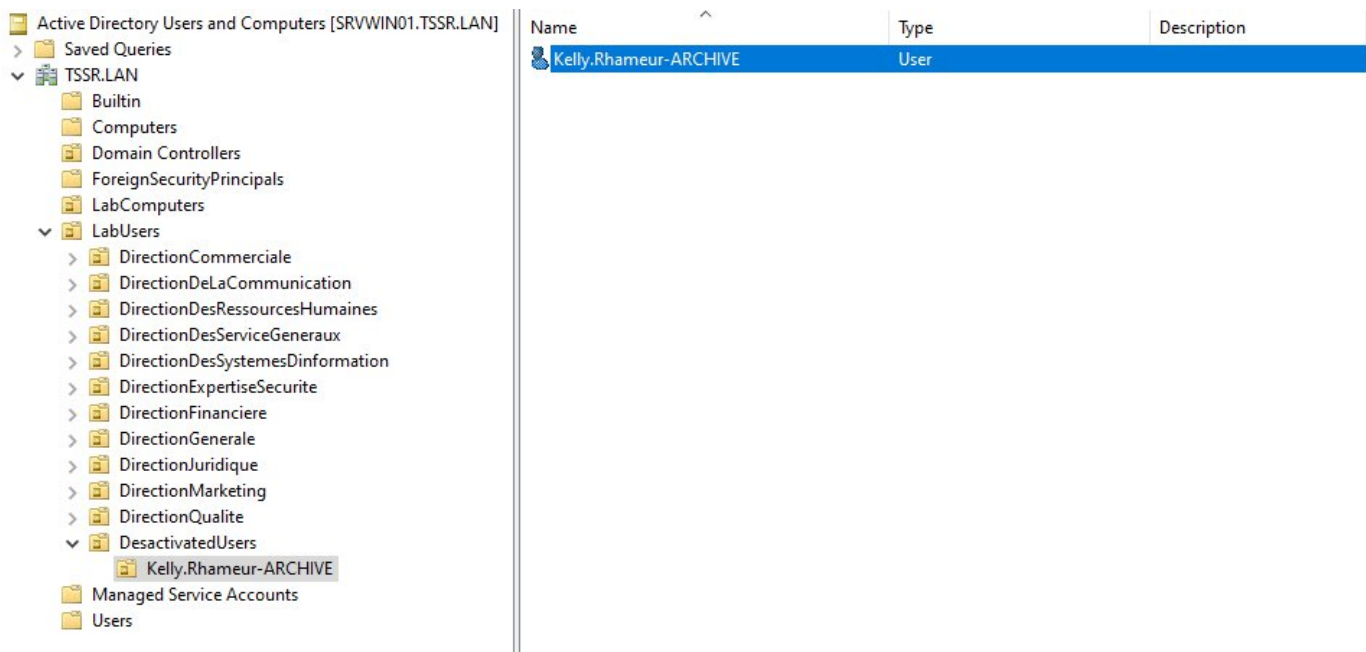
Primary group: Domain Users

Set Primary Group: There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

Buttons: OK, Cancel, Apply, Help

Q.1.1.4

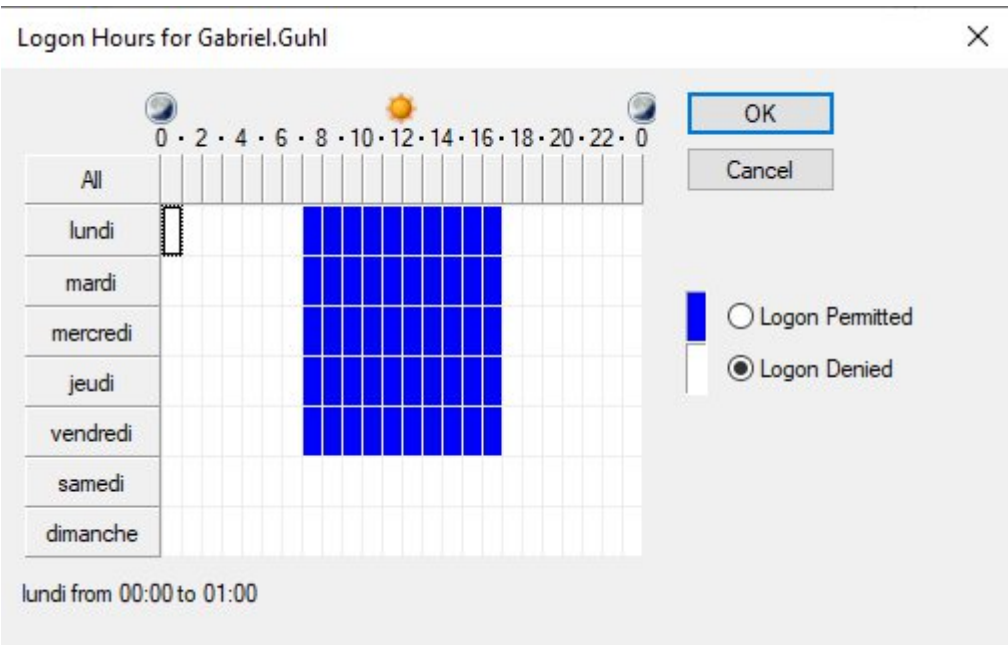
Copie d'écran des dossiers individuels demandés.



Partie 2

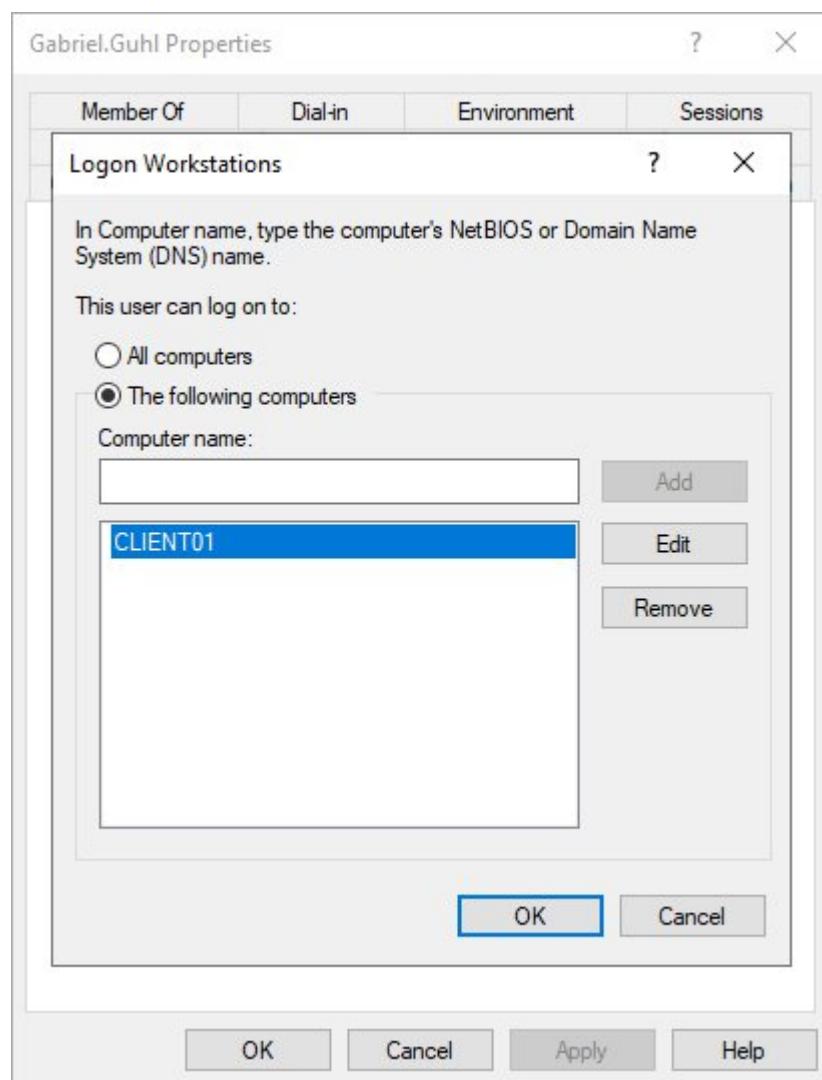
Q.1.2.1

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.



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

The screenshot displays the Windows Security console with the 'PSOUsersPasswordRestricted' policy selected. The 'Password Settings' section is expanded, showing various password requirements. To the right, the 'GrsUsersPasswordRestricted Properties' dialog box is open, showing the 'Members' tab with a list of users and groups.

PSOUsersPasswordRestricted

Password Settings

Directly Applies To

Extensions

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

Description:

Passoword age options:

☒ Enforce minimum password age

User cannot change the password withi... * 1

☒ Enforce maximum password age

User must change the password after (... * 90

☒ Enforce account lockout policy:

Number of failed logon attempts allowed: * 3

Reset failed logon attempts count after (m... * 15

Account will be locked out

☒ For a duration of (mins): * 15

☐ Until an administrator manually unlocks the account

Directly Applies To

Name Mail

GrsUsersPasswordRestrict...

Add...

Remove

More Information

OK Cancel

GrsUsersPasswordRestricted Properties

General Members Member Of Managed By

Members:

Name	Active Directory Domain Services Folder
Aarav 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 La...	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 Suny	TSSR.LAN/Lab/Users/DirectionQualite/Laborato
Alex Lebarbier	TSSR.LAN/Lab/Users/DirectionFinanciere/Finan
Alexandre Ch...	TSSR.LAN/Lab/Users/DirectionDeLaCommunica
Alexis Flemmar	TSSR.LAN/Lab/Users/DirectionGenerale/Directic
Alice Hussein	TSSR.LAN/Lab/Users/DirectionCommerciale/Adh...

Add... Remove

OK Cancel Apply

Partie 3

Q.1.3.1

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

Group Policy Management

Forest: TSSR.LAN

Domains

TSSR.LAN

Default Domain Policy

Domain Controllers

LabComputers

LabUsers

PROD_Users_Drive-Mount

DesactivatedUsers

DirectionCommerciale

DirectionDeLaCommunication

DirectionDesRessourcesHumaines

DirectionDesServiceGeneraux

DirectionDesSystemesDinformation

DirectionExpertiseSecurite

DirectionFinanciere

DirectionGenerale

DirectionJuridique

DirectionMarketing

DirectionQualite

Group Policy Objects

Default Domain Controllers Policy

Default Domain Policy

PROD_Users_Drive-Mount

WMI Filters

Starter GPOs

Sites

Group Policy Modeling

Group Policy Results

PROD_Users_Drive-Mount

Scope Details Settings Delegation Status

Links

Display links in this location: TSSR.LAN

The following sites, domains, and OUs are linked to this GPO:

Location	Enforced	Link Enabled	Path
LabUsers	No	Yes	TSSR.LAN/LabUsers

Security Filtering

The settings in this GPO can only apply to the following groups, users, and computers:

Authenticated Users

New Drive Properties

General Common

Update

Location: \\SRVWIN01\LecteurE

Reconnect: ☐ Label as: Lecteur E

Drive Letter

☐ Use first available, starting at: ☒ Use: E

Connect as (optional)

User name: Password: Confirm password:

Hide/Show this drive

☒ No change ☐ Hide this drive ☐ Show this drive

Hide/Show all drives

☒ No change ☐ Hide all drives ☐ Show all drives

OK Cancel Apply Help

New Drive Properties

General Common

Update

Location: \\SRVWIN01\LecteurF

Reconnect: ☐ Label as: Lecteur F

Drive Letter

☐ Use first available, starting at: ☒ Use: F

Connect as (optional)

User name: Password: Confirm password:

Hide/Show this drive


☒ No change ☐ Hide this drive ☐ Show this drive

Hide/Show all drives

☒ No change ☐ Hide all drives ☐ Show all drives

OK Cancel Apply Help

- PROD_Users_Drive-Mount [SRVWIN01.TSSR.LAN] Po
- 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

Processing

Description

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

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
└─ sr0
```

Q.2.3.2

Copie d'écran montrant les systèmes de stockage utilisés.

```
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
```

```
TYPE
disk
part
raid1
part
part
part
lvm
lvm
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:~# 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.

```
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
├─ 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"
```