CHECKPOINT 3

Formulaire réponses

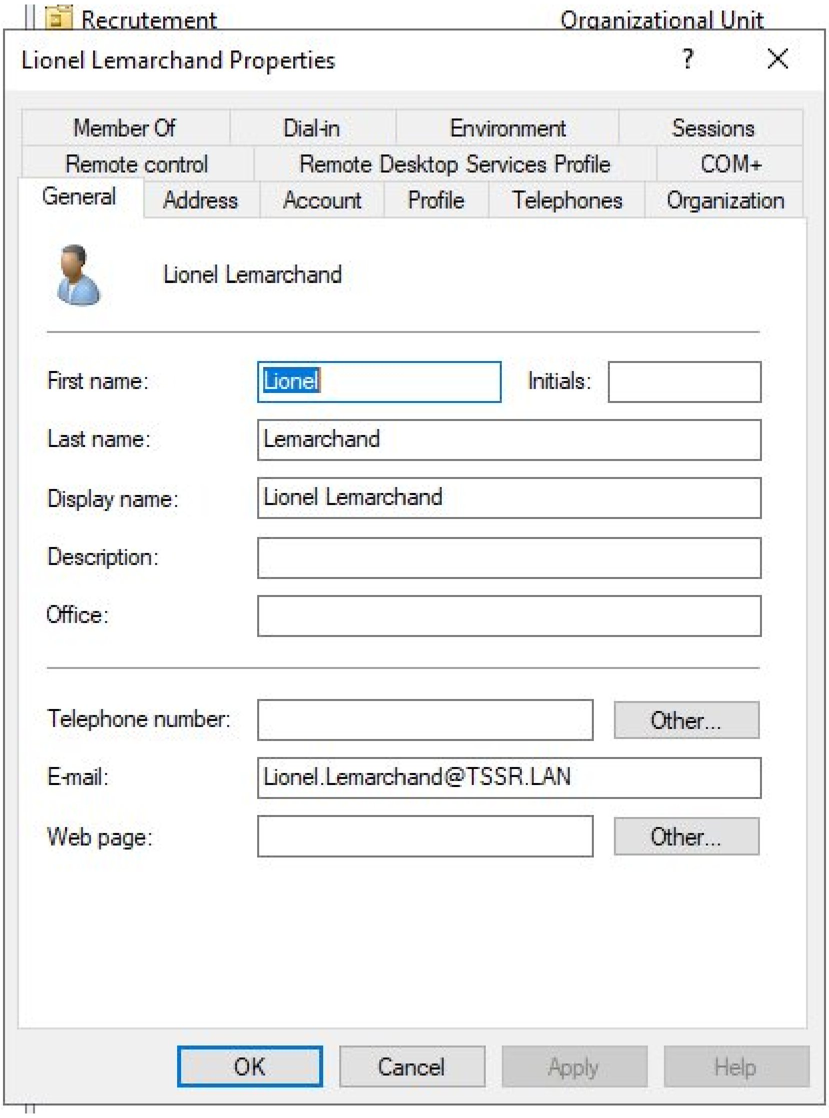
Exercice 1

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



Lionel Lemarchand

First name: Lionel

Initials:

Last name: Lemarchand

Display name: Lionel Lemarchand

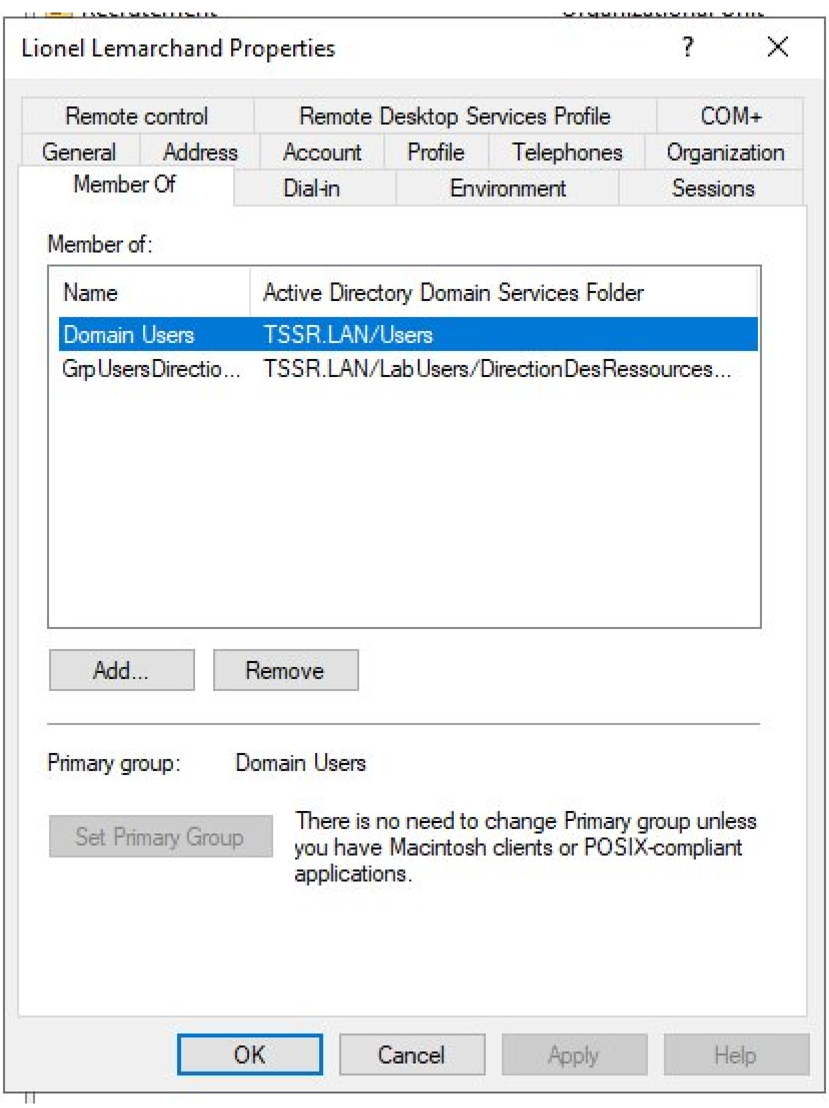
Description:

Office:

Telephone number:

E-mail: Lionel.Lemarchand@TSSR.LAN

Web page:



Member of:

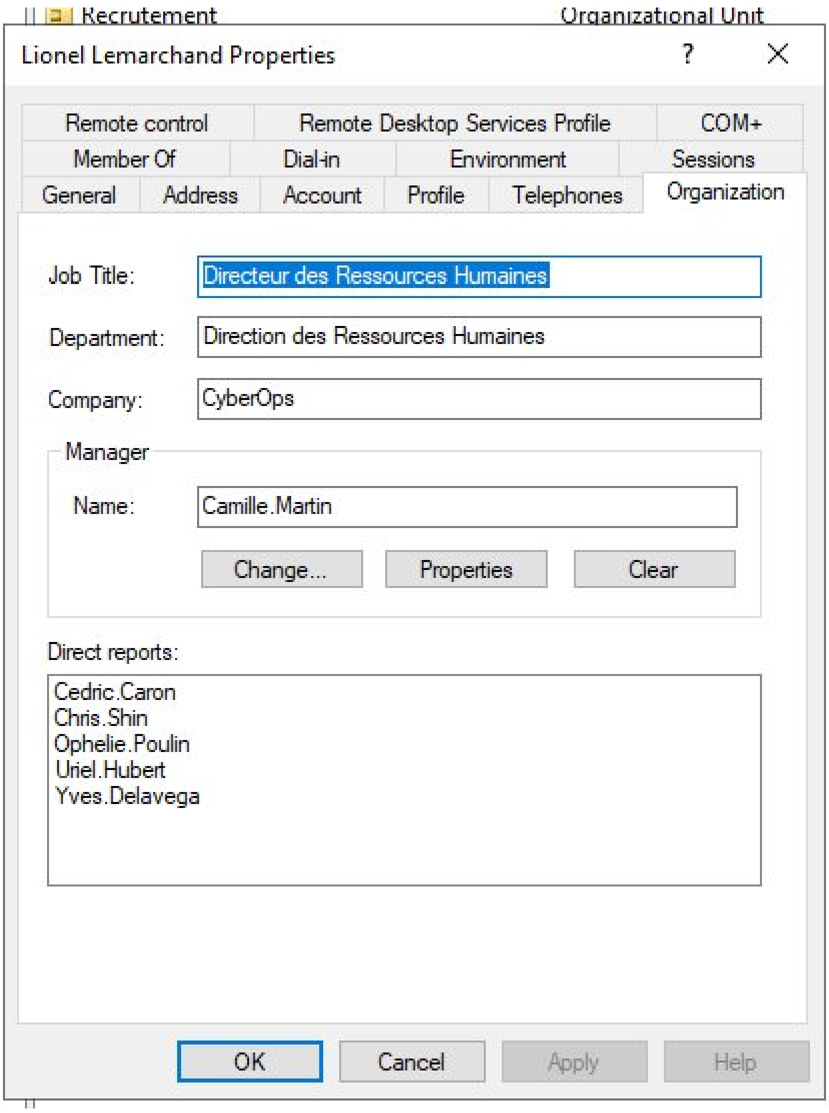
Name	Active Directory Domain Services Folder
Domain Users	TSSR.LAN/Users
GrpUsersDirectio...	TSSR.LAN/LabUsers/DirectionDesRessources...

Primary group: Domain Users

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

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

Copie(s) d'écran



Recrutement Organizational Unit

Lionel Lemarchand Properties

Job Title: Directeur des Ressources Humaines

Department: Direction des Ressources Humaines

Company: CyberOps

Manager

Name: Camille.Martin

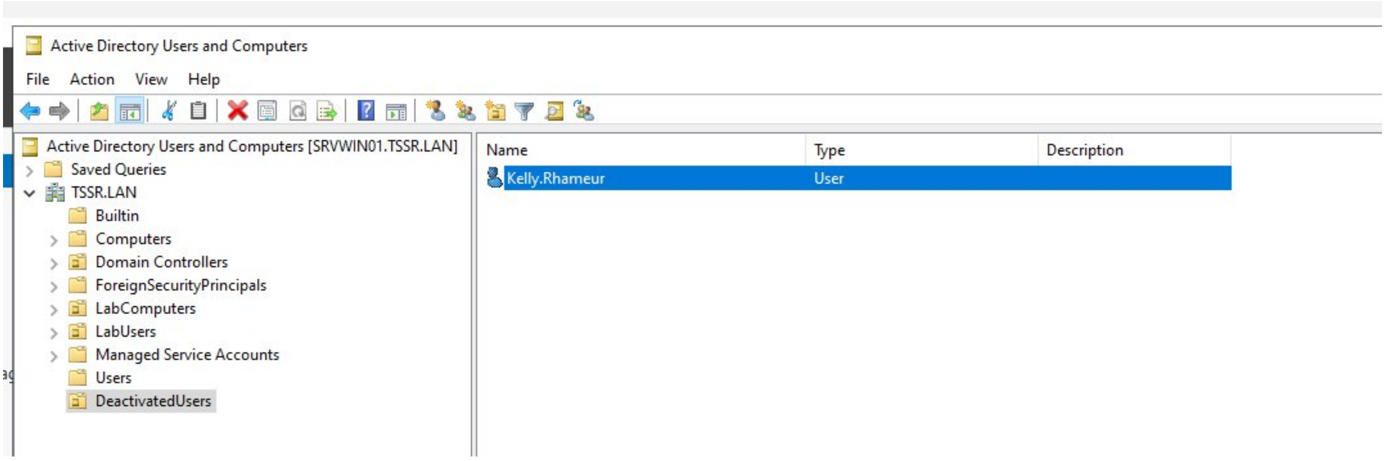
Direct reports:

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

Q.1.1.2

Copie d’écran de l’OU DeactivatedUsers.

Copie d'écran



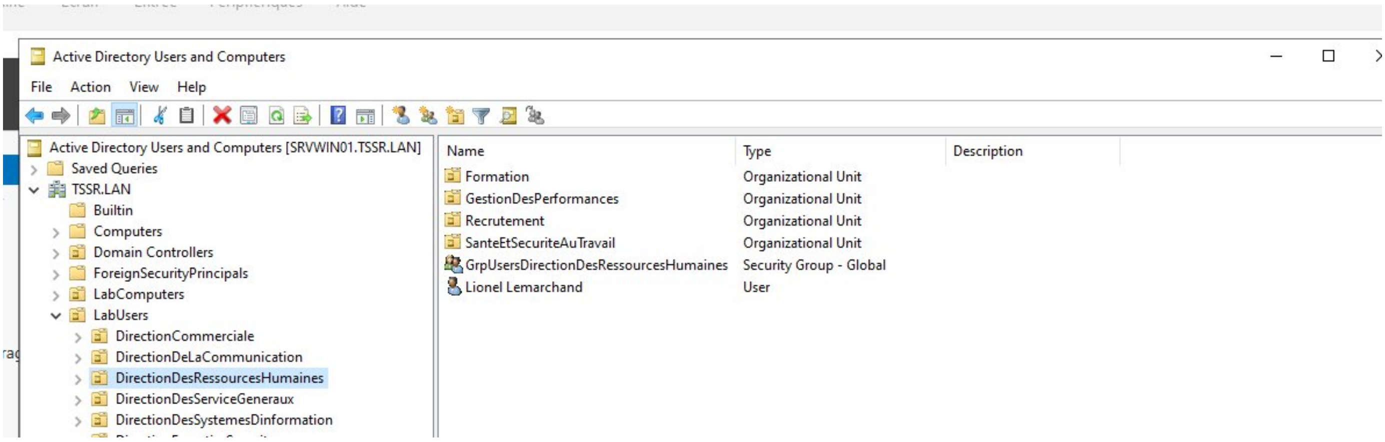
Active Directory Users and Computers

Name	Type	Description
Kelly.Rhameur	User	

Q.1.1.3

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

Copie d'écran



- Active Directory Users and Computers [SRVWIN01.TSSR.LAN]
  - Saved Queries
  - TSSR.LAN
    - Builtin
    - Computers
    - Domain Controllers
    - ForeignSecurityPrincipals
    - LabComputers
    - LabUsers
      - DirectionCommerciale
      - DirectionDeLaCommunication
      - DirectionDesRessourcesHumaines
      - DirectionDesServiceGeneraux
      - DirectionDesSystemesDinformation

Name	Type	Description
Formation	Organizational Unit	
GestionDesPerformances	Organizational Unit	
Recrutement	Organizational Unit	
SanteEtSecuriteAuTravail	Organizational Unit	
GrpUsersDirectionDesRessourcesHumaines	Security Group - Global	
Lionel Lemarchand	User	

Q.1.1.4

Copie d’écran des dossiers individuels demandés.

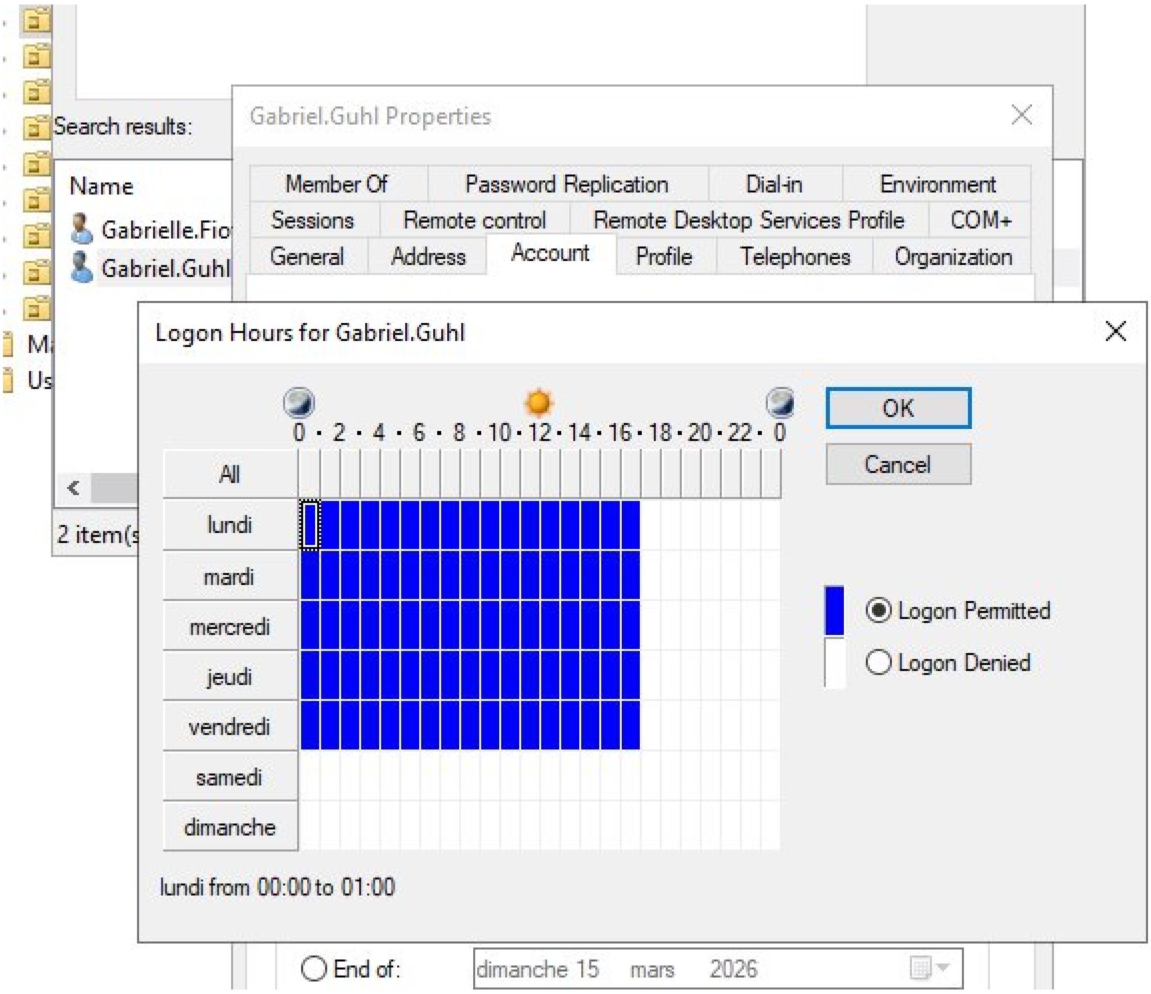
Copie d'écran

Partie 2

Q.1.2.1

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

Copies d'écran



	0	·	2	·	4	·	6	·	8	·	10	·	12	·	14	·	16	·	18	·	20	·	22	·
All																								
lundi	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦							
mardi	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦							
mercredi	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦							
jeudi	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦							
vendredi	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦							
samedi																								
dimanche																								

🟦 ● Logon Permitted

□ ○ Logon Denied

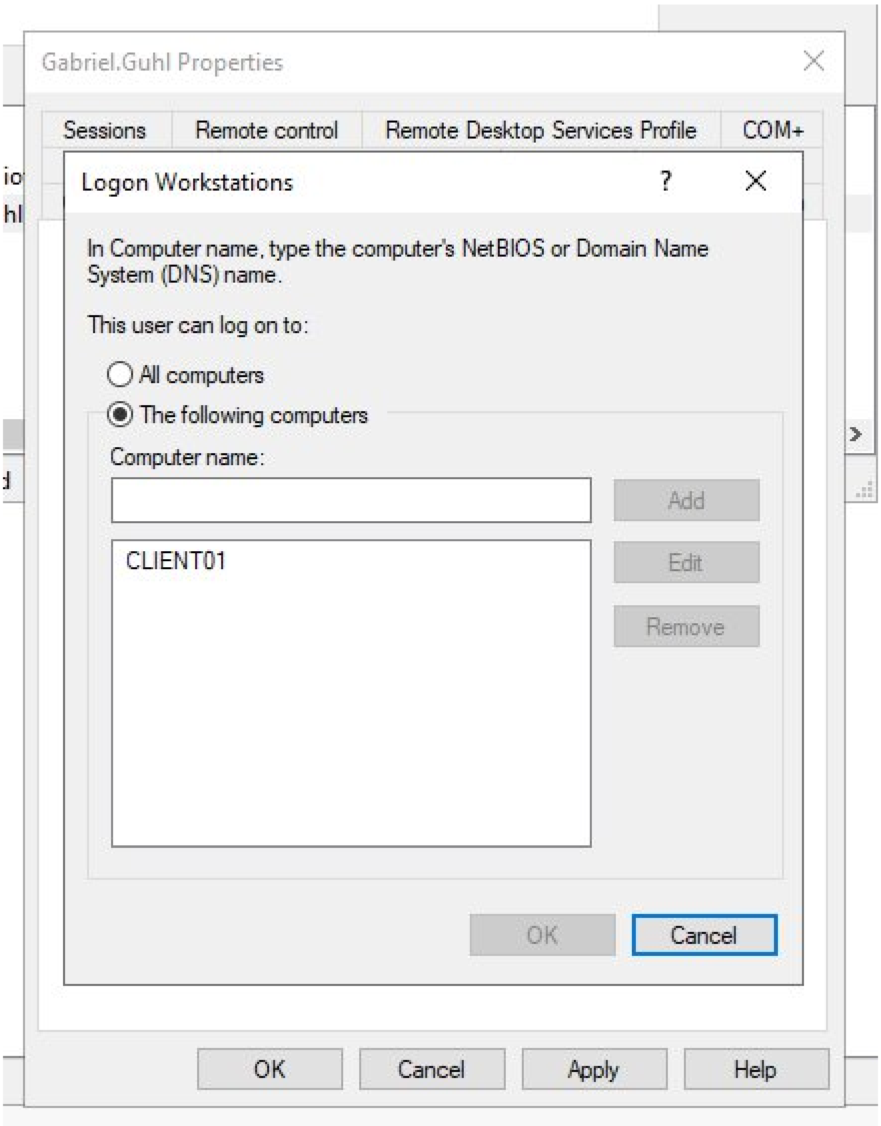
lundi from 00:00 to 01:00

○ End of: dimanche 15 mars 2026

Q.1.2.2

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

Copie d'écran



Gabriel.Guhl Properties

Sessions | Remote control | Remote Desktop Services Profile | COM+

Logon Workstations

In Computer name, type the computer's NetBIOS or Domain Name System (DNS) name.

This user can log on to:

○ All computers

● The following computers

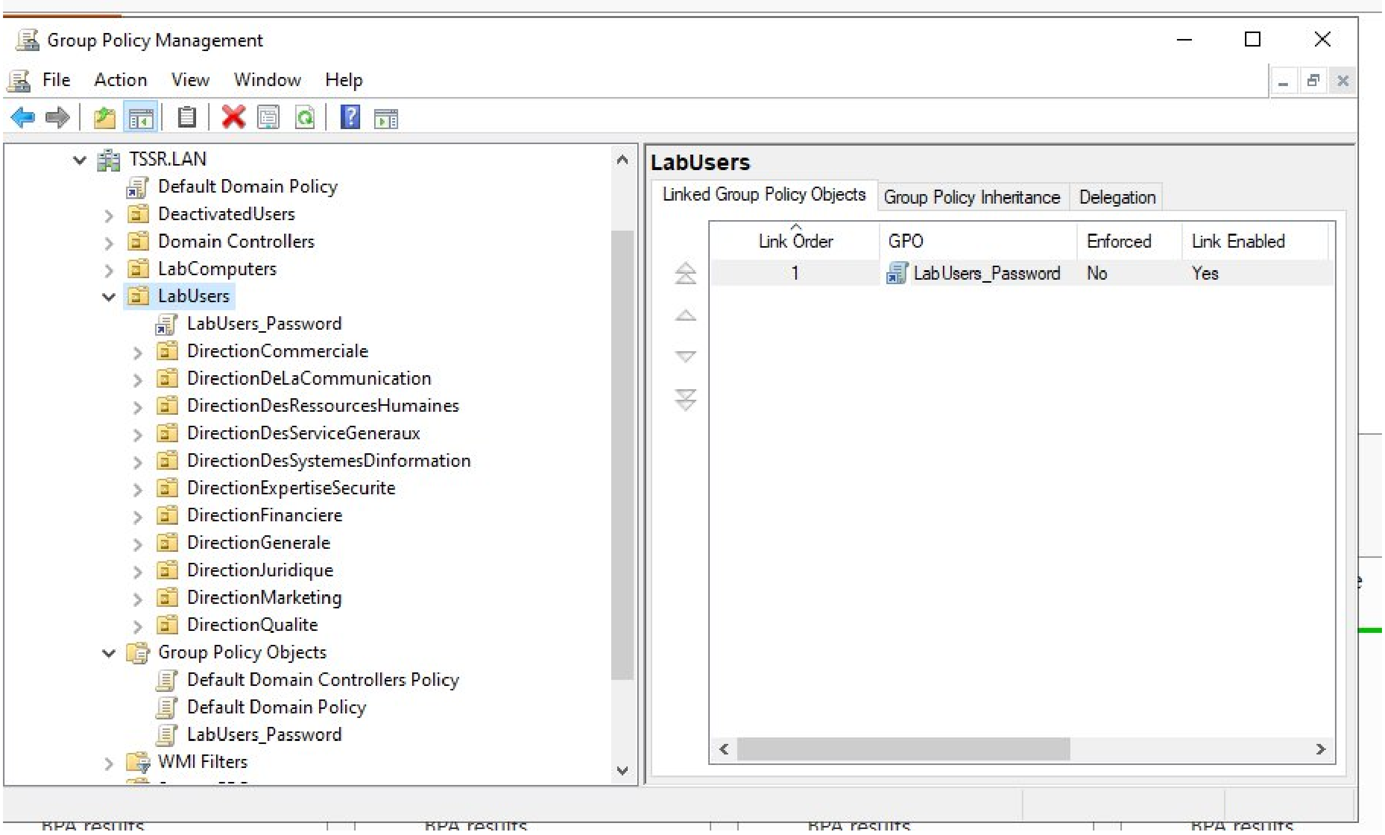
Computer name:

CLIENT01

Q.1.2.3

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

Copies d'écran



Link Order	GPO	Enforced	Link Enabled
1	LabUsers_Password	No	Yes

Partie 3

Q.1.3.1

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

Copies d'écran

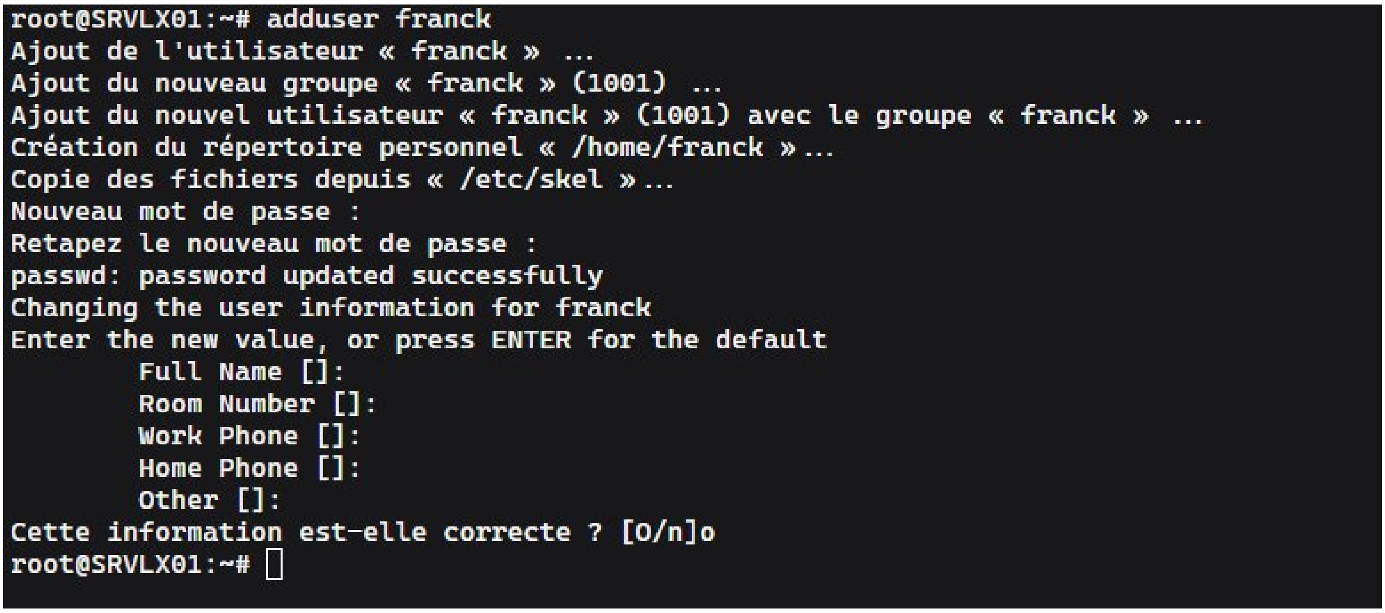
Exercice 2

Partie 1

Q.2.1.1

Copie d’écran de la création de compte.

Copie d'écran

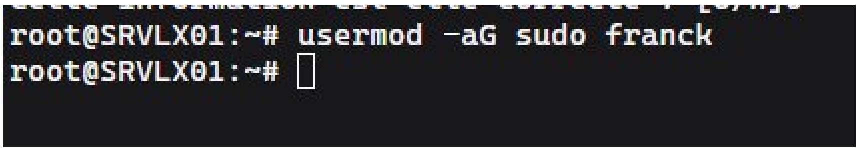


```
root@SRVLX01:~# adduser franck
Ajout de l'utilisateur « franck » ...
Ajout du nouveau groupe « franck » (1001) ...
Ajout du nouvel utilisateur « franck » (1001) avec le groupe « franck » ...
Création du répertoire personnel « /home/franck »...
Copie des fichiers depuis « /etc/skel »...
Nouveau mot de passe :
Retapez le nouveau mot de passe :
passwd: password updated successfully
Changing the user information for franck
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Cette information est-elle correcte ? [O/n]o
root@SRVLX01:~#
```

Q.2.1.2

Copie d’écran du paramétrage du compte.

Copie d'écran



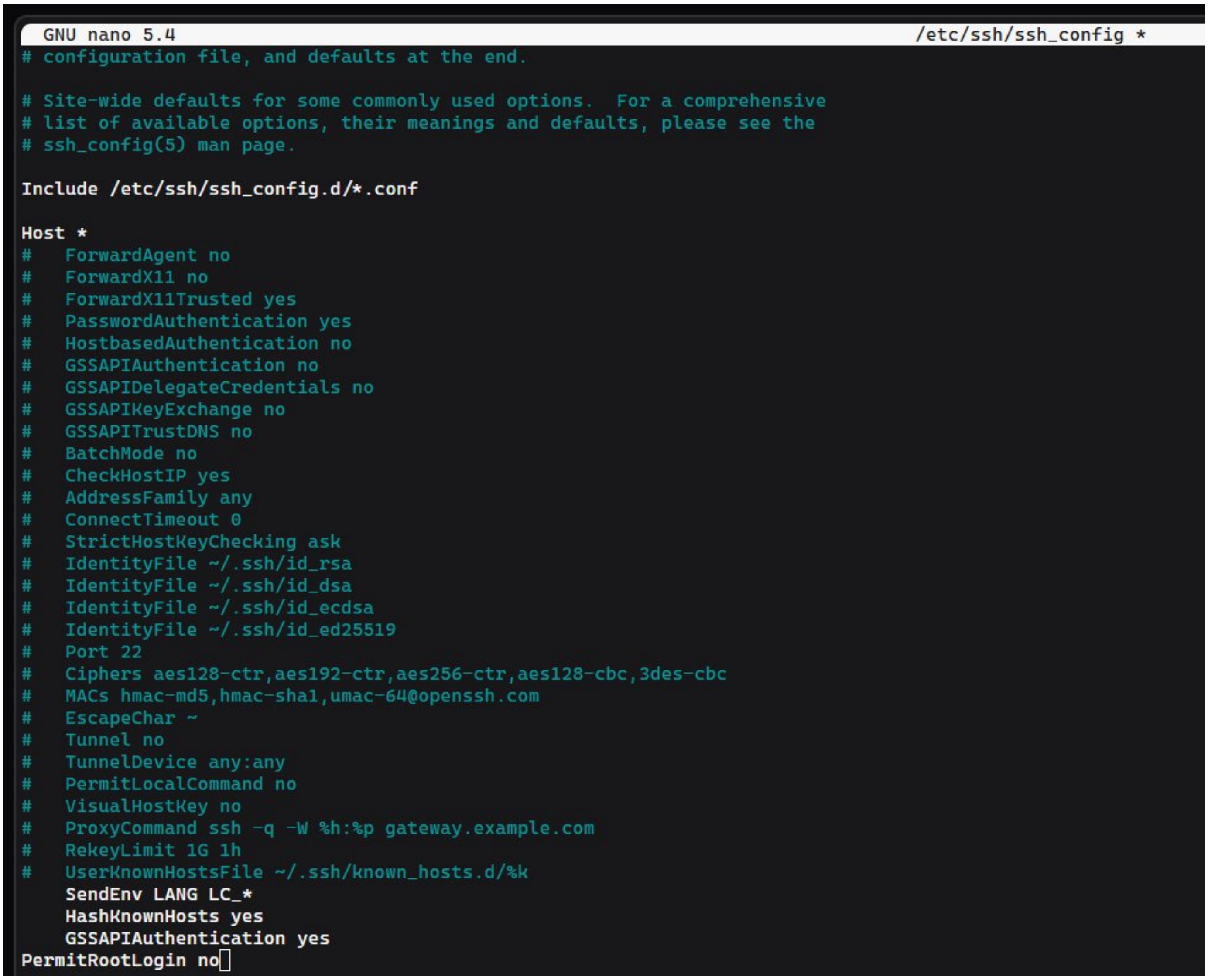
```
Cette information est-elle correcte ? [O/n]o
root@SRVLX01:~# usermod -aG sudo franck
root@SRVLX01:~#
```

Partie 2

Q.2.2.1

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

Copie d'écran

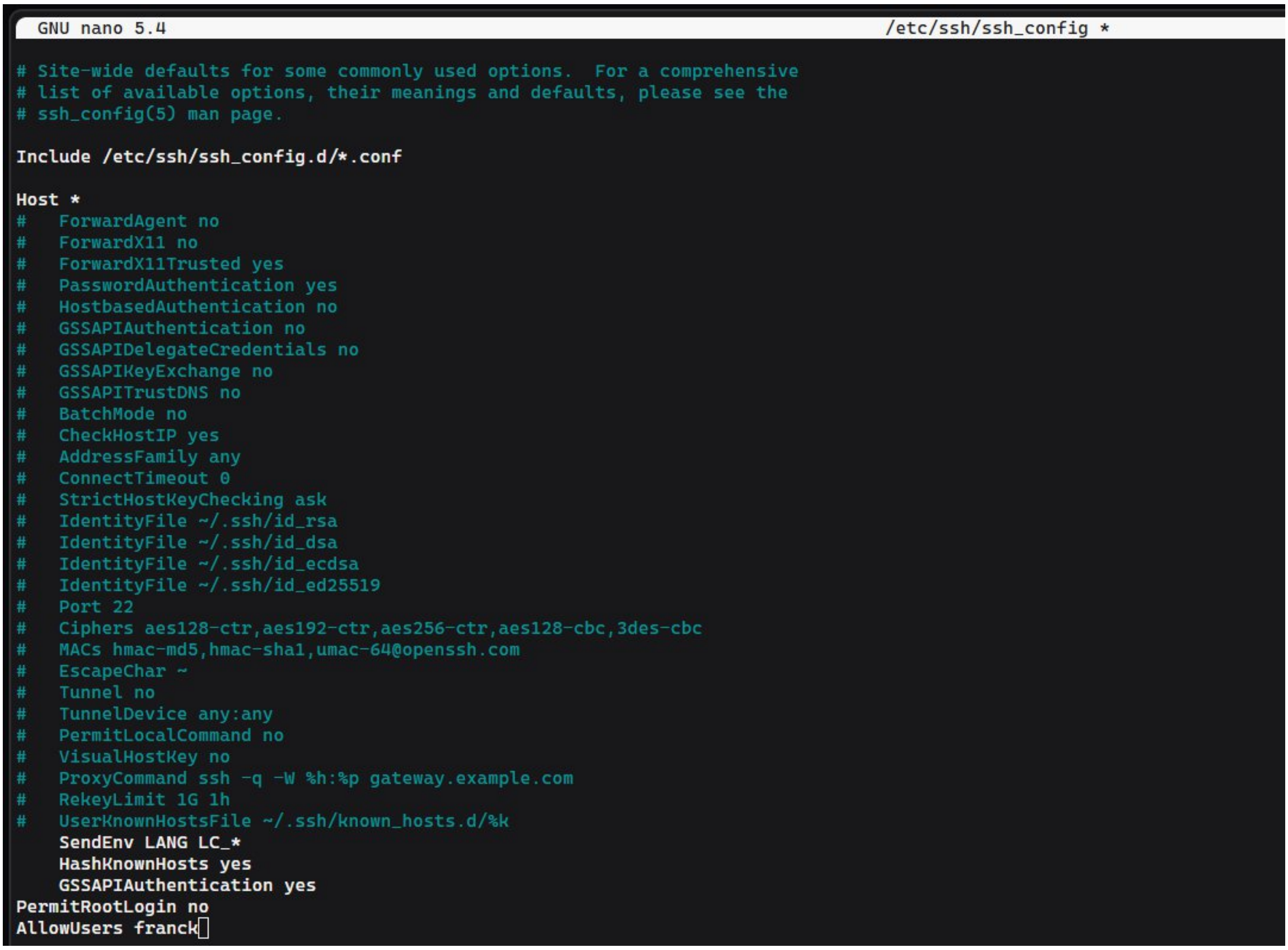


```
  GNU nano 5.4                                                     /etc/ssh/ssh_config *
# configuration file, and defaults at the end.

# Site-wide defaults for some commonly used options.  For a comprehensive
# list of available options, their meanings and defaults, please see the
# ssh_config(5) man page.

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

Host *
#   ForwardAgent no
#   ForwardX11 no
#   ForwardX11Trusted yes
#   PasswordAuthentication yes
#   HostbasedAuthentication no
#   GSSAPIAuthentication no
#   GSSAPIDelegateCredentials no
#   GSSAPIKeyExchange no
#   GSSAPITrustDNS no
#   BatchMode no
#   CheckHostIP yes
#   AddressFamily any
#   ConnectTimeout 0
#   StrictHostKeyChecking ask
#   IdentityFile ~/.ssh/id_rsa
#   IdentityFile ~/.ssh/id_dsa
#   IdentityFile ~/.ssh/id_ecdsa
#   IdentityFile ~/.ssh/id_ed25519
#   Port 22
#   Ciphers aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,3des-cbc
#   MACs hmac-md5,hmac-sha1,umac-64@openssh.com
#   EscapeChar ~
#   Tunnel no
#   TunnelDevice any:any
#   PermitLocalCommand no
#   VisualHostKey no
#   ProxyCommand ssh -q -W %h:%p gateway.example.com
#   RekeyLimit 1G 1h
#   UserKnownHostsFile ~/.ssh/known_hosts.d/%k
    SendEnv LANG LC_*
    HashKnownHosts yes
    GSSAPIAuthentication yes
PermitRootLogin no
```

Q.2.2.2

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

Copie d'écran

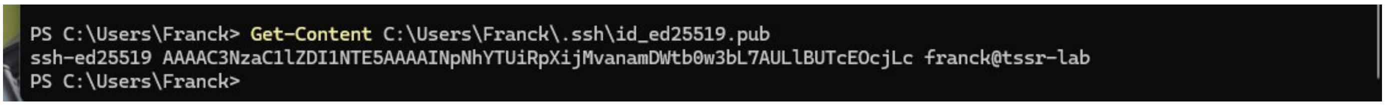


```
  GNU nano 5.4                                                  /etc/ssh/ssh_config *

# Site-wide defaults for some commonly used options.  For a comprehensive
# list of available options, their meanings and defaults, please see the
# ssh_config(5) man page.

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

Host *
#   ForwardAgent no
#   ForwardX11 no
#   ForwardX11Trusted yes
#   PasswordAuthentication yes
#   HostbasedAuthentication no
#   GSSAPIAuthentication no
#   GSSAPIDelegateCredentials no
#   GSSAPIKeyExchange no
#   GSSAPITrustDNS no
#   BatchMode no
#   CheckHostIP yes
#   AddressFamily any
#   ConnectTimeout 0
#   StrictHostKeyChecking ask
#   IdentityFile ~/.ssh/id_rsa
#   IdentityFile ~/.ssh/id_dsa
#   IdentityFile ~/.ssh/id_ecdsa
#   IdentityFile ~/.ssh/id_ed25519
#   Port 22
#   Ciphers aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,3des-cbc
#   MACs hmac-md5,hmac-sha1,umac-64@openssh.com
#   EscapeChar ~
#   Tunnel no
#   TunnelDevice any:any
#   PermitLocalCommand no
#   VisualHostKey no
#   ProxyCommand ssh -q -W %h:%p gateway.example.com
#   RekeyLimit 1G 1h
#   UserKnownHostsFile ~/.ssh/known_hosts.d/%k
    SendEnv LANG LC_*
    HashKnownHosts yes
    GSSAPIAuthentication yes
PermitRootLogin no
AllowUsers franck
```

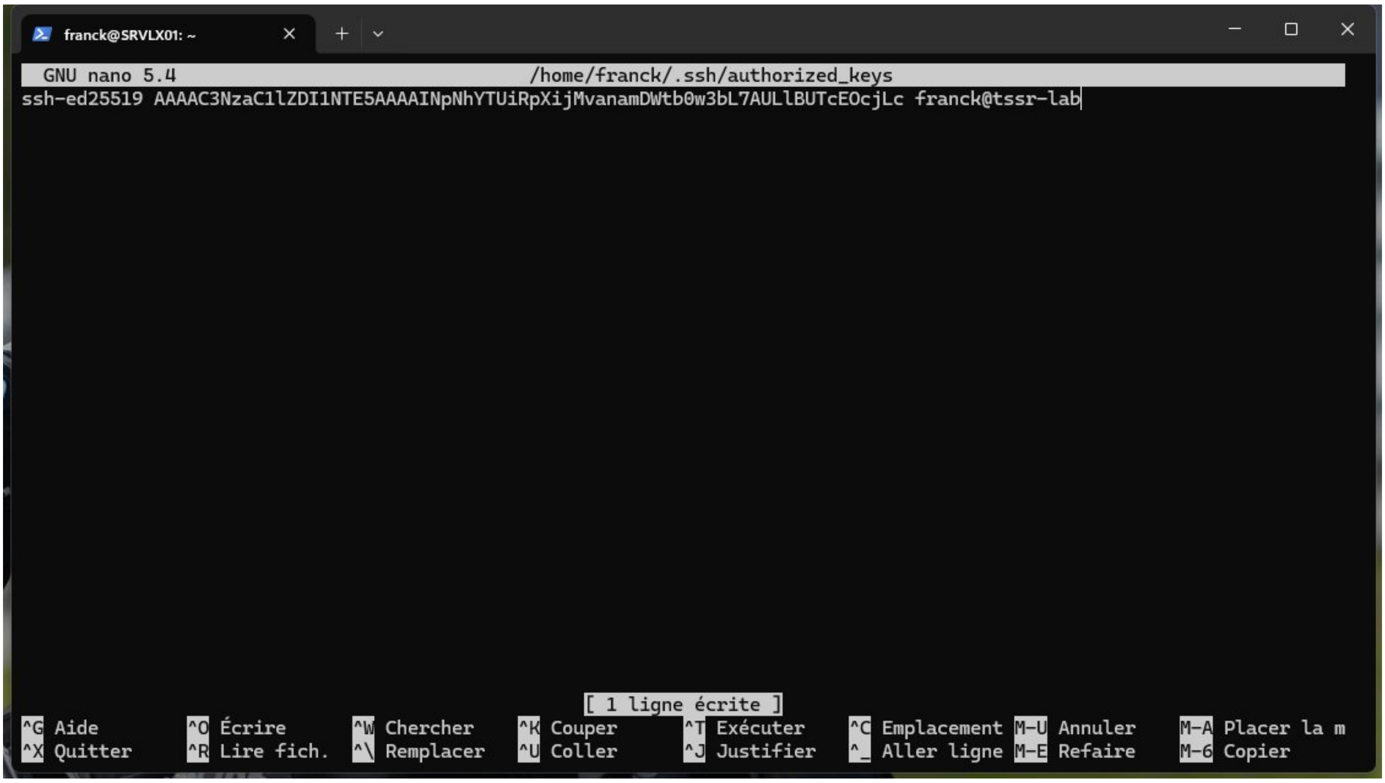
Q.2.2.3

Copies d’écran du paramétrage de l’authentification.

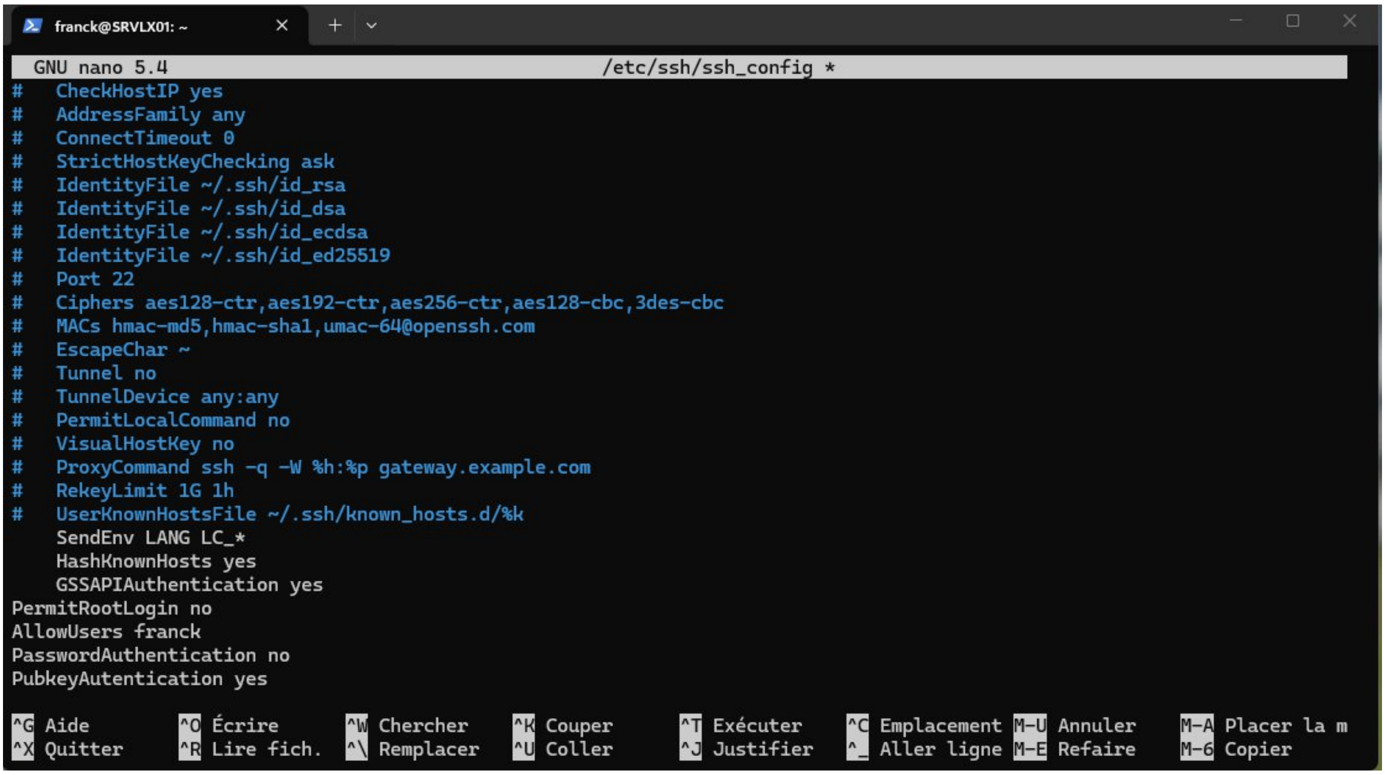
Copies d'écran



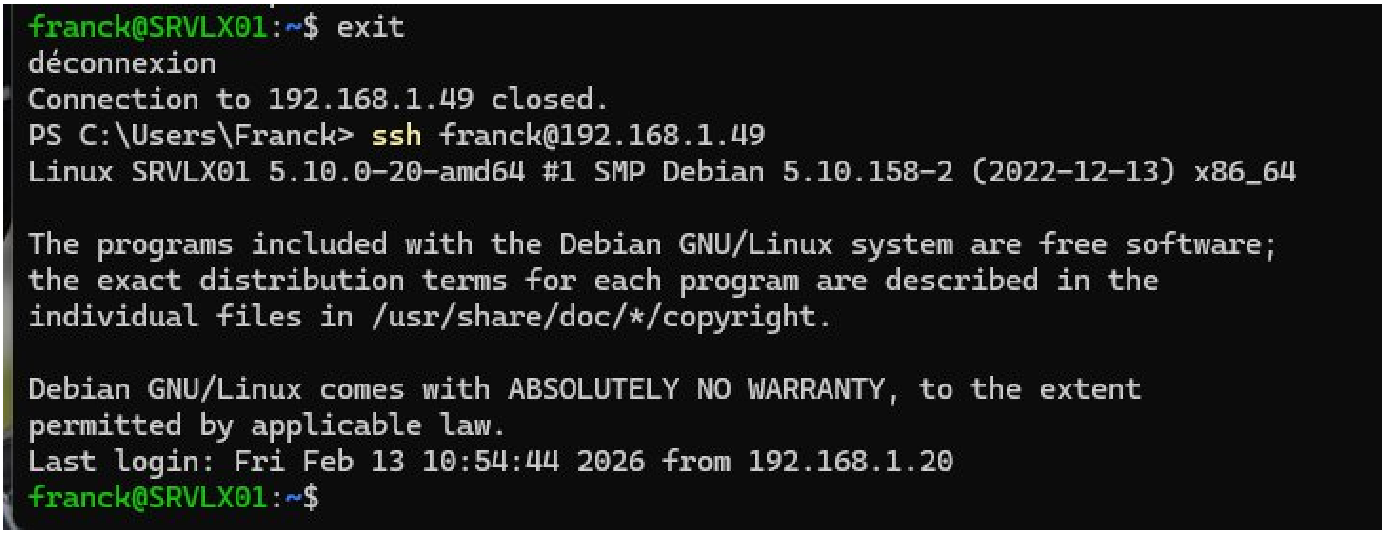
```
PS C:\Users\Franck> Get-Content C:\Users\Franck\.ssh\id_ed25519.pub
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAINpNhYTUiRpXijMvanamDWtb0w3bL7AULlBUTcEOcjLc franck@tssr-lab
PS C:\Users\Franck>
```



```
 GNU nano 5.4                              /home/franck/.ssh/authorized_keys
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAINpNhYTUiRpXijMvanamDWtb0w3bL7AULlBUTcEOcjLc franck@tssr-lab








                                        [ 1 ligne écrite ]
^G Aide       ^O Écrire     ^W Chercher   ^K Couper     ^T Exécuter   ^C Emplacement M-U Annuler    M-A Placer la m
^X Quitter    ^R Lire fich. ^\ Remplacer  ^U Coller     ^J Justifier  ^_ Aller ligne M-E Refaire    M-6 Copier
```



```
 GNU nano 5.4                                  /etc/ssh/ssh_config *
#   CheckHostIP yes
#   AddressFamily any
#   ConnectTimeout 0
#   StrictHostKeyChecking ask
#   IdentityFile ~/.ssh/id_rsa
#   IdentityFile ~/.ssh/id_dsa
#   IdentityFile ~/.ssh/id_ecdsa
#   IdentityFile ~/.ssh/id_ed25519
#   Port 22
#   Ciphers aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,3des-cbc
#   MACs hmac-md5,hmac-sha1,umac-64@openssh.com
#   EscapeChar ~
#   Tunnel no
#   TunnelDevice any:any
#   PermitLocalCommand no
#   VisualHostKey no
#   ProxyCommand ssh -q -W %h:%p gateway.example.com
#   RekeyLimit 1G 1h
#   UserKnownHostsFile ~/.ssh/known_hosts.d/%k
    SendEnv LANG LC_*
    HashKnownHosts yes
    GSSAPIAuthentication yes
PermitRootLogin no
AllowUsers franck
PasswordAuthentication no
PubkeyAutentication yes

^G Aide       ^O Écrire     ^W Chercher   ^K Couper     ^T Exécuter   ^C Emplacement M-U Annuler    M-A Placer la m
^X Quitter    ^R Lire fich. ^\ Remplacer  ^U Coller     ^J Justifier  ^_ Aller ligne M-E Refaire    M-6 Copier
```



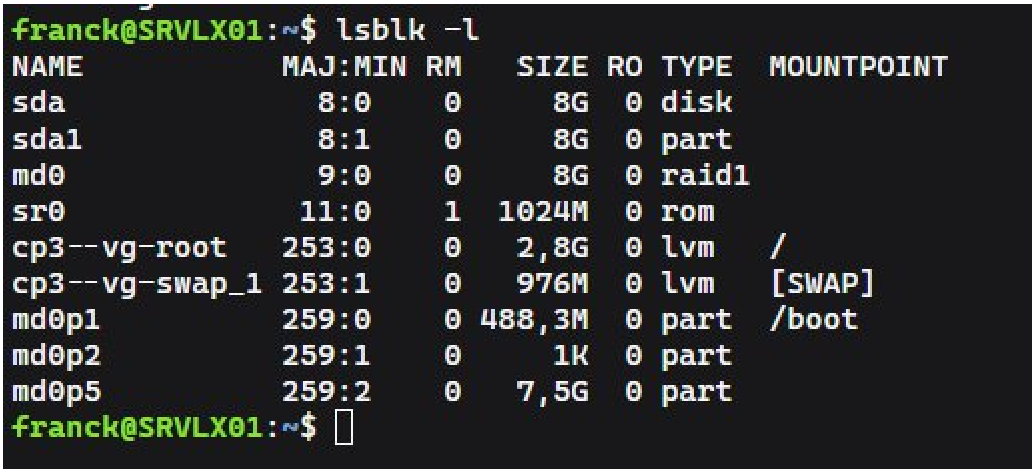
```
franck@SRVLX01:~$ exit
déconnexion
Connection to 192.168.1.49 closed.
PS C:\Users\Franck> ssh franck@192.168.1.49
Linux SRVLX01 5.10.0-20-amd64 #1 SMP Debian 5.10.158-2 (2022-12-13) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Feb 13 10:54:44 2026 from 192.168.1.20
franck@SRVLX01:~$
```

Partie 3

Q.2.3.1

Copie d’écran montrant les systèmes de fichiers montés.

Copie d'écran

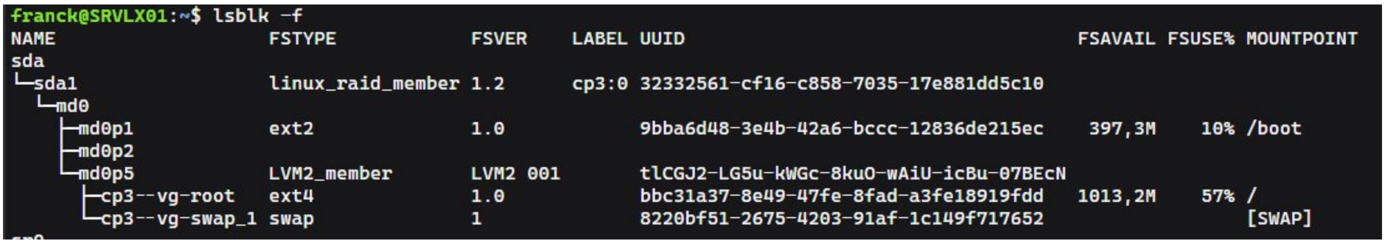


```
franck@SRVLX01:~$ lsblk -l
NAME              MAJ:MIN RM   SIZE RO TYPE  MOUNTPOINT
sda                 8:0    0     8G  0 disk
sda1                8:1    0     8G  0 part
md0                 9:0    0     8G  0 raid1
sr0                11:0    1  1024M  0 rom
cp3--vg-root      253:0    0   2,8G  0 lvm   /
cp3--vg-swap_1    253:1    0   976M  0 lvm   [SWAP]
md0p1             259:0    0 488,3M  0 part  /boot
md0p2             259:1    0     1K  0 part
md0p5             259:2    0   7,5G  0 part
franck@SRVLX01:~$
```

Q.2.3.2

Copie d’écran montrant les systèmes de stockage utilisés.

Copie d'écran

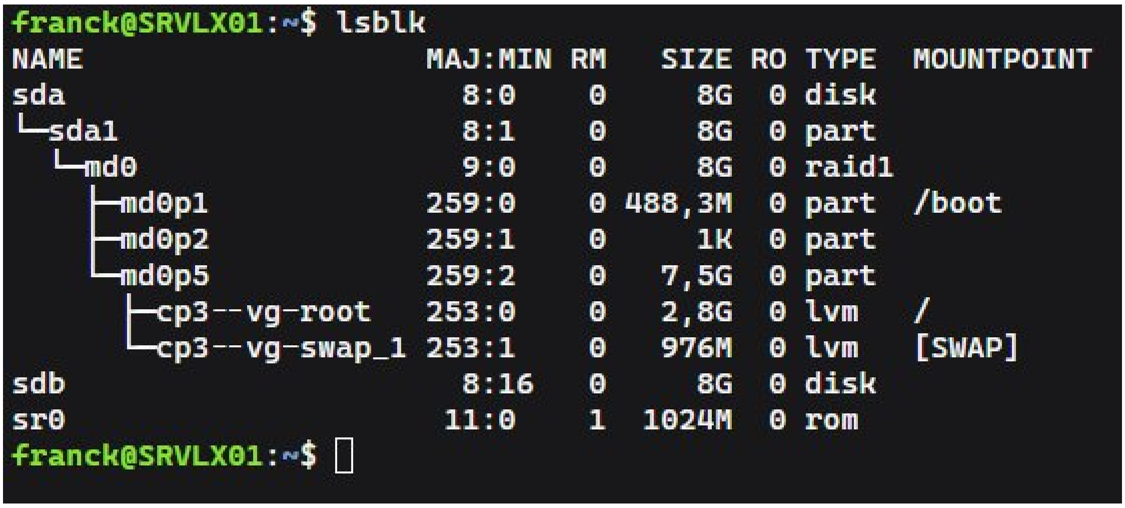


```
franck@SRVLX01:~$ lsblk -f
NAME                   FSTYPE            FSVER    LABEL UUID                                   FSAVAIL FSUSE% MOUNTPOINT
sda
└─sda1                 linux_raid_member 1.2      cp3:0 32332561-cf16-c858-7035-17e881dd5c10
  └─md0
    ├─md0p1            ext2              1.0            9bba6d48-3e4b-42a6-bccc-12836de215ec    397,3M    10% /boot
    ├─md0p2
    └─md0p5            LVM2_member       LVM2 001       tlCGJ2-LG5u-kWGc-8kuO-wAiU-icBu-07BEcN
      ├─cp3--vg-root   ext4              1.0            bbc31a37-8e49-47fe-8fad-a3fe18919fdd   1013,2M    57% /
      └─cp3--vg-swap_1 swap              1              8220bf51-2675-4203-91af-1c149f717652                  [SWAP]
```

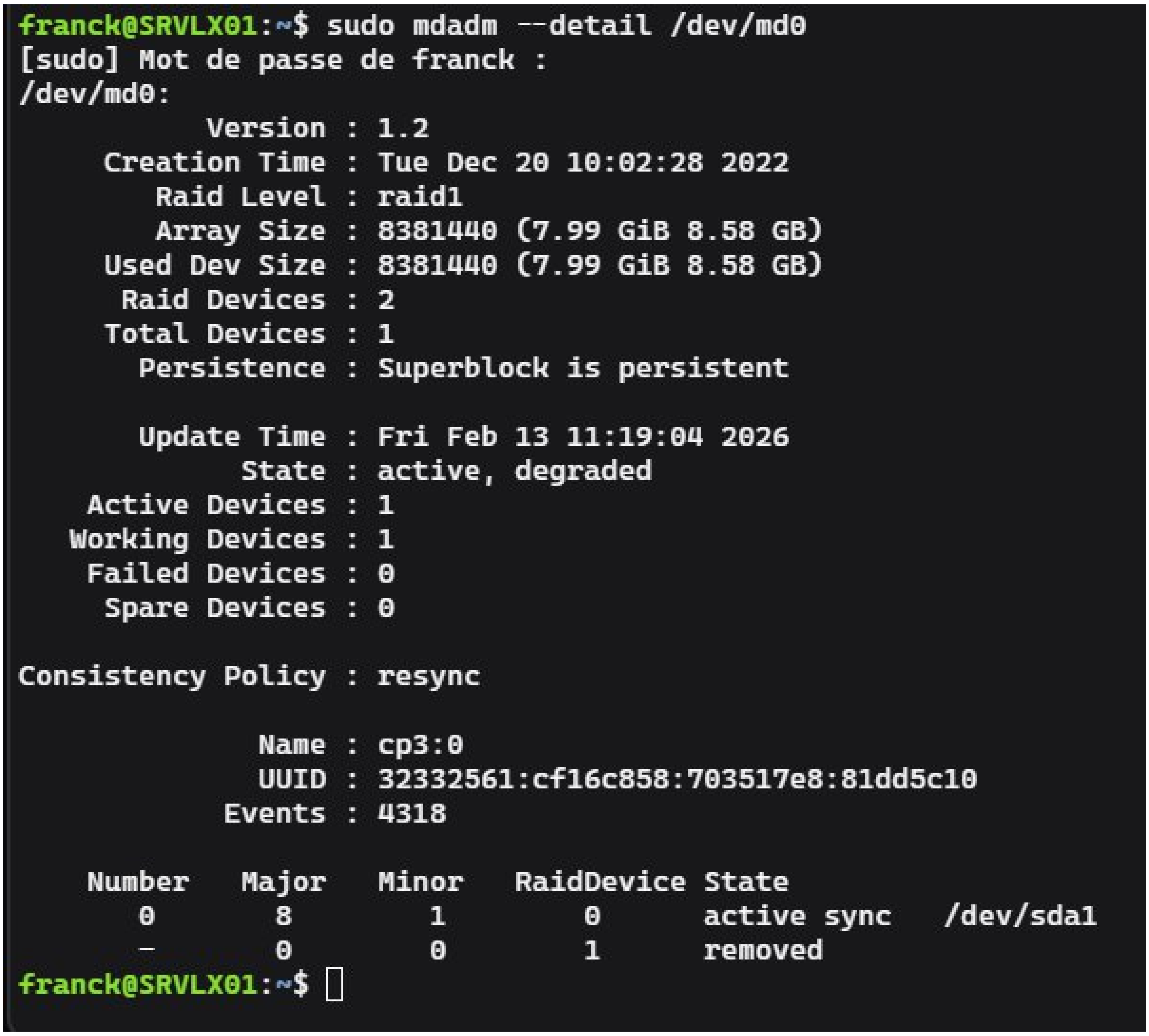
Q.2.3.3

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

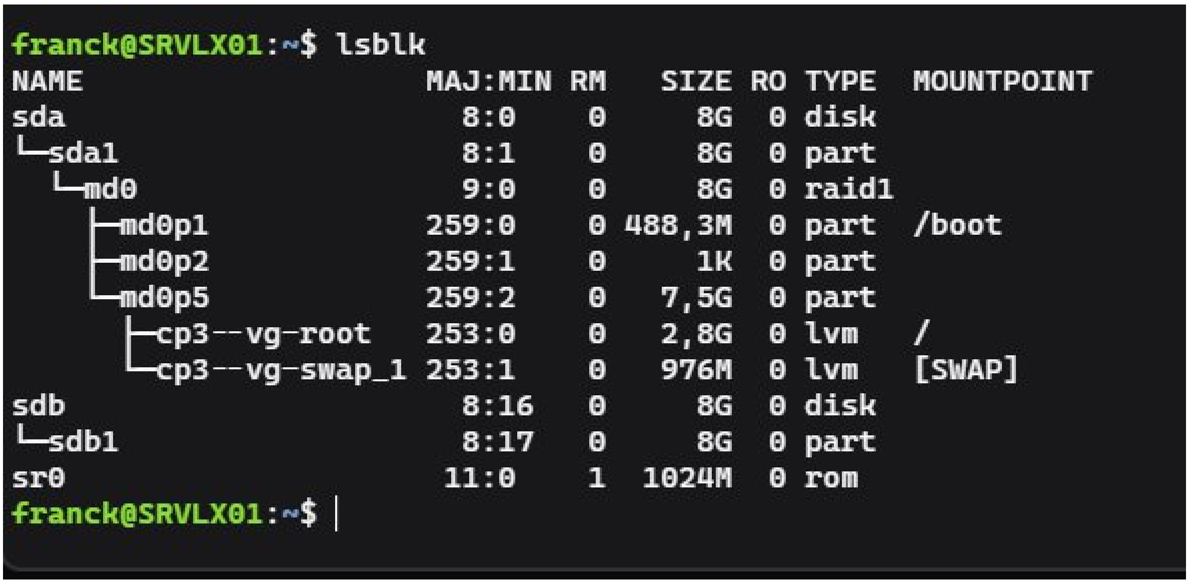
Copies d'écran



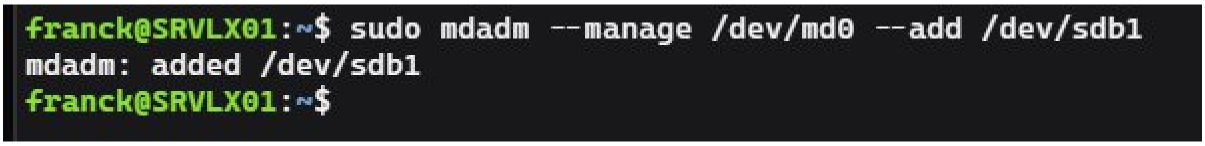
```
franck@SRVLX01:~$ lsblk
NAME                      MAJ:MIN RM   SIZE RO TYPE  MOUNTPOINT
sda                         8:0    0     8G  0 disk
└─sda1                      8:1    0     8G  0 part
  └─md0                     9:0    0     8G  0 raid1
    ├─md0p1               259:0    0 488,3M  0 part  /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
franck@SRVLX01:~$ 
```



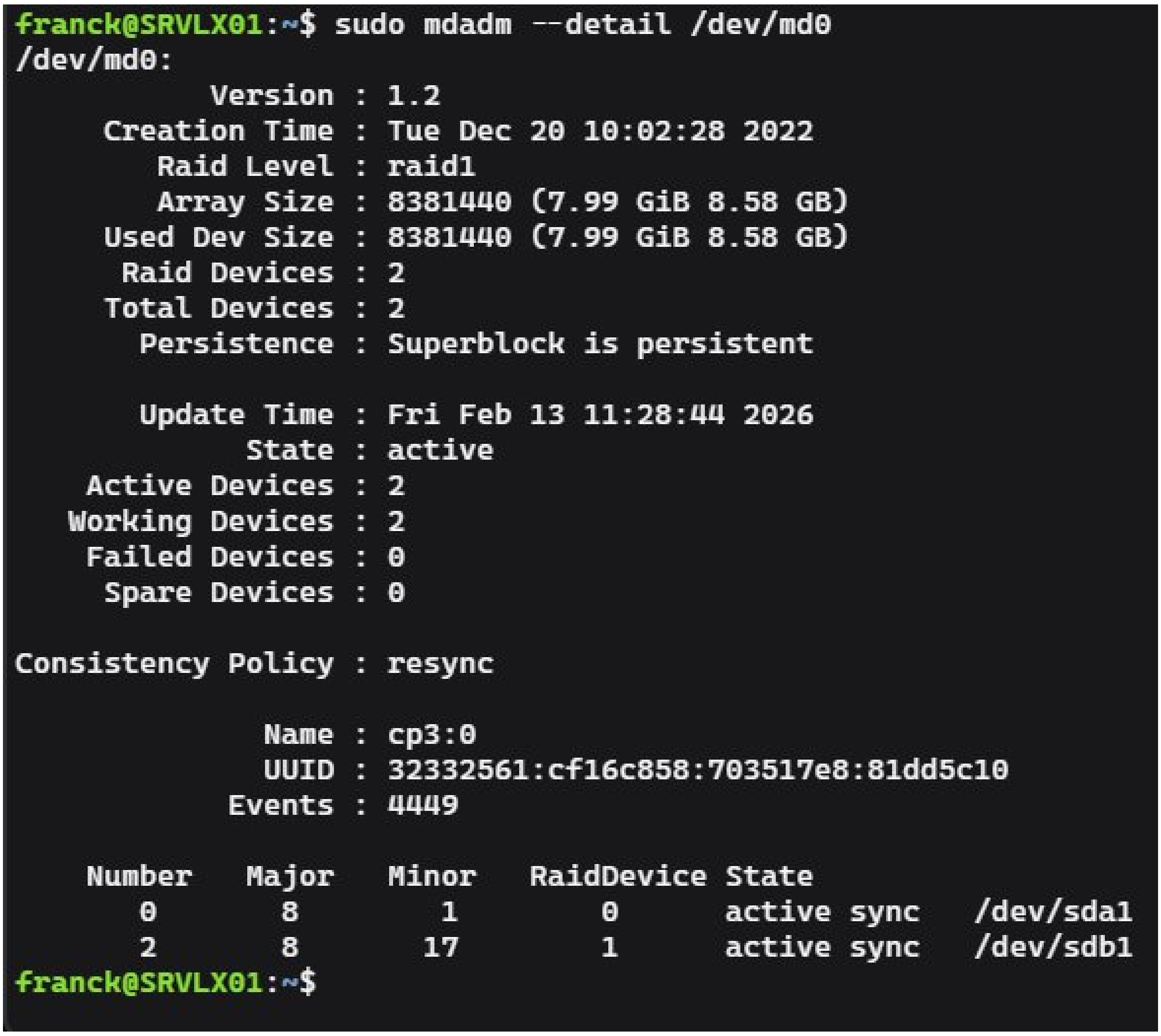
```
franck@SRVLX01:~$ sudo mdadm --detail /dev/md0
[sudo] Mot de passe de franck :
/dev/md0:
           Version : 1.2
     Creation Time : Tue Dec 20 10:02:28 2022
        Raid Level : raid1
        Array Size : 8381440 (7.99 GiB 8.58 GB)
     Used Dev Size : 8381440 (7.99 GiB 8.58 GB)
      Raid Devices : 2
     Total Devices : 1
       Persistence : Superblock is persistent

       Update Time : Fri Feb 13 11:19:04 2026
             State : active, degraded
    Active Devices : 1
   Working Devices : 1
    Failed Devices : 0
     Spare Devices : 0

Consistency Policy : resync

              Name : cp3:0
              UUID : 32332561:cf16c858:703517e8:81dd5c10
            Events : 4318

    Number   Major   Minor   RaidDevice State
       0       8        1        0      active sync   /dev/sda1
       -       0        0        1      removed
franck@SRVLX01:~$ 
```



```
franck@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
└─sdb1                      8:17   0     8G  0 part
sr0                        11:0    1  1024M  0 rom
franck@SRVLX01:~$ |
```



```
franck@SRVLX01:~$ sudo mdadm --manage /dev/md0 --add /dev/sdb1
mdadm: added /dev/sdb1
franck@SRVLX01:~$
```

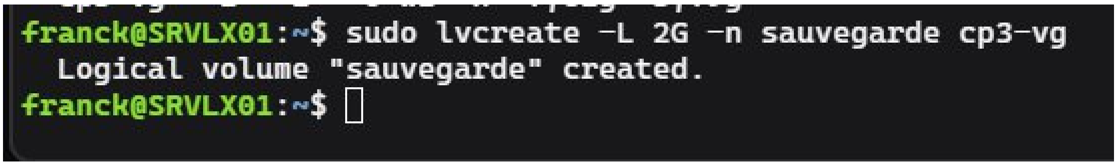


```
franck@SRVLX01:~$ sudo mdadm --detail /dev/md0
/dev/md0:
           Version : 1.2
     Creation Time : Tue Dec 20 10:02:28 2022
        Raid Level : raid1
        Array Size : 8381440 (7.99 GiB 8.58 GB)
     Used Dev Size : 8381440 (7.99 GiB 8.58 GB)
      Raid Devices : 2
     Total Devices : 2
       Persistence : Superblock is persistent

       Update Time : Fri Feb 13 11:28:44 2026
             State : active
    Active Devices : 2
   Working Devices : 2
    Failed Devices : 0
     Spare Devices : 0

Consistency Policy : resync

              Name : cp3:0
              UUID : 32332561:cf16c858:703517e8:81dd5c10
            Events : 4449

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

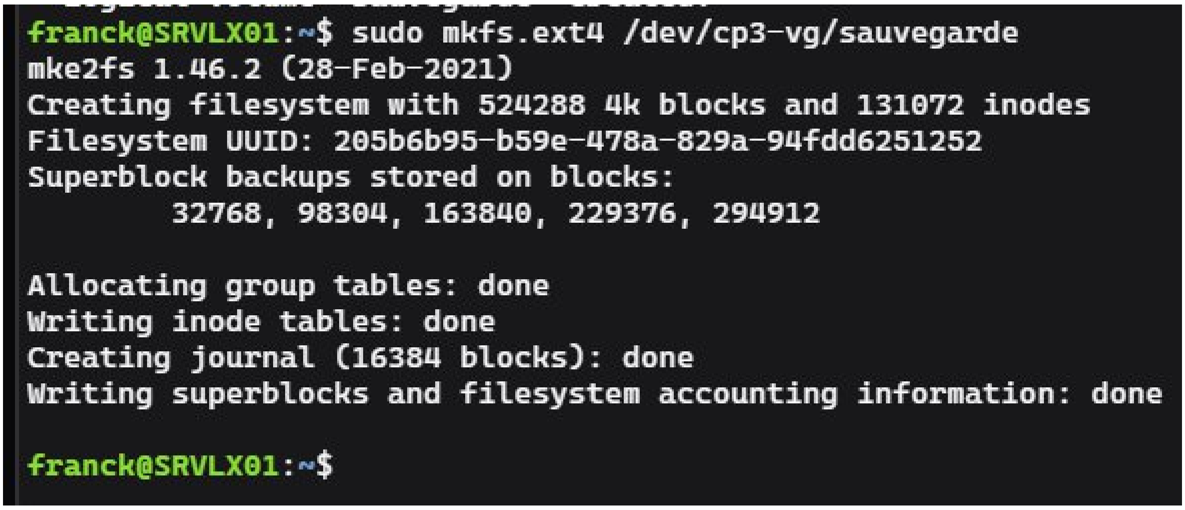
Q.2.3.4

Copies d’écran montrant les différentes étapes de configuration.

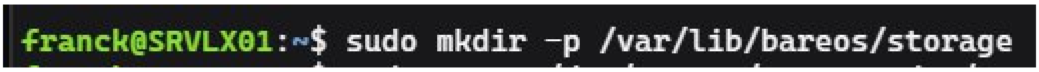
Copies d'écran



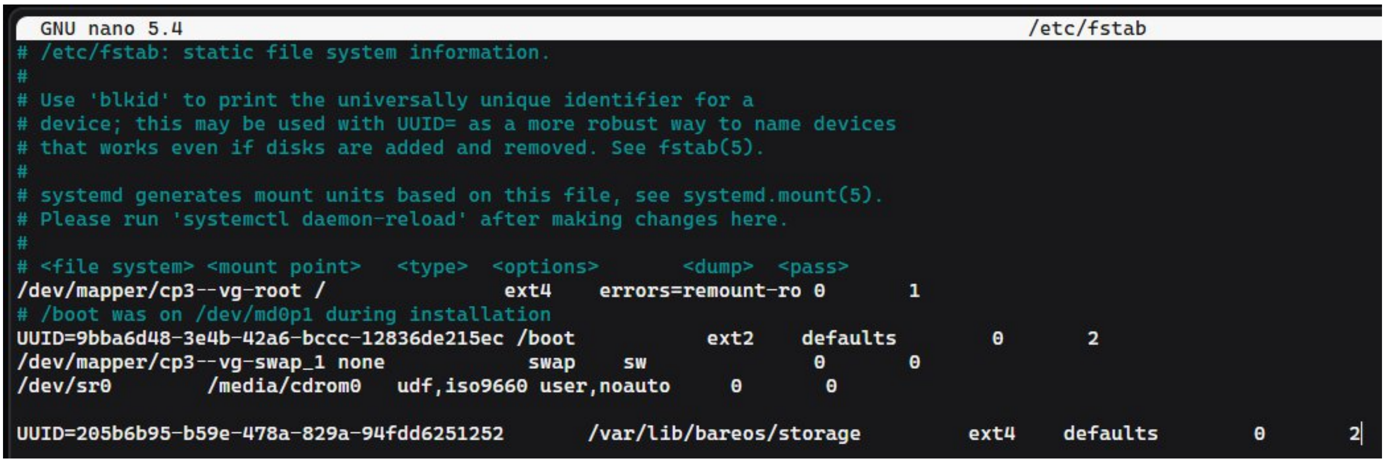
```
franck@SRVLX01:~$ sudo lvcreate -L 2G -n sauvegarde cp3-vg
  Logical volume "sauvegarde" created.
franck@SRVLX01:~$ 
```



```
franck@SRVLX01:~$ sudo mkfs.ext4 /dev/cp3-vg/sauvegarde
mke2fs 1.46.2 (28-Feb-2021)
Creating filesystem with 524288 4k blocks and 131072 inodes
Filesystem UUID: 205b6b95-b59e-478a-829a-94fdd6251252
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376, 294912

Allocating group tables: done
Writing inode tables: done
Creating journal (16384 blocks): done
Writing superblocks and filesystem accounting information: done

franck@SRVLX01:~$
```



```
franck@SRVLX01:~$ sudo mkdir -p /var/lib/bareos/storage
```

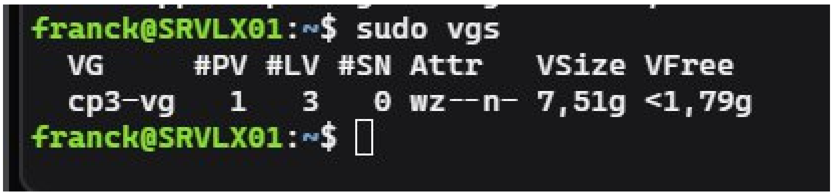


```
  GNU nano 5.4                                                  /etc/fstab
# /etc/fstab: static file system information.
#
# Use 'blkid' to print the universally unique identifier for a
# device; this may be used with UUID= as a more robust way to name devices
# that works even if disks are added and removed. See fstab(5).
#
# systemd generates mount units based on this file, see systemd.mount(5).
# Please run 'systemctl daemon-reload' after making changes here.
#
# <file system> <mount point>   <type>  <options>       <dump>  <pass>
/dev/mapper/cp3--vg-root /               ext4    errors=remount-ro 0       1
# /boot was on /dev/md0p1 during installation
UUID=9bba6d48-3e4b-42a6-bccc-12836de215ec /boot           ext2    defaults        0       2
/dev/mapper/cp3--vg-swap_1 none            swap    sw              0       0
/dev/sr0        /media/cdrom0   udf,iso9660 user,noauto     0       0

UUID=205b6b95-b59e-478a-829a-94fdd6251252       /var/lib/bareos/storage         ext4    defaults        0       2
```

Q.2.3.5

Copie d’écran montrant l’espace disponible.

Copie d'écran



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

Partie 4

Q.2.4.1

Réponse à la question

Partie 5

Q.2.5.1

Réponse à la question

Ct state established, relate accept

Ct state invalid drop

Iiffname lo accept

Tcp dport 22 accept

Ip protocol icmp accept

Ip6 nexthdr ipv6-icmp accept

Q.2.5.2

Réponse à la question

Iiffname lo accept communication locale sur interface loopback

Tcp dport 22 accept communication Port 22 TCP pour SSH

Ip protocol icmp accept Communication pour le ping IPV4 ICMP

Ip6 nexthdr ipv6-icmp accept Communication pour le ping IPV6 ICMP

Ct state established, relate accept Communication au connexions sortantes

Q.2.5.3

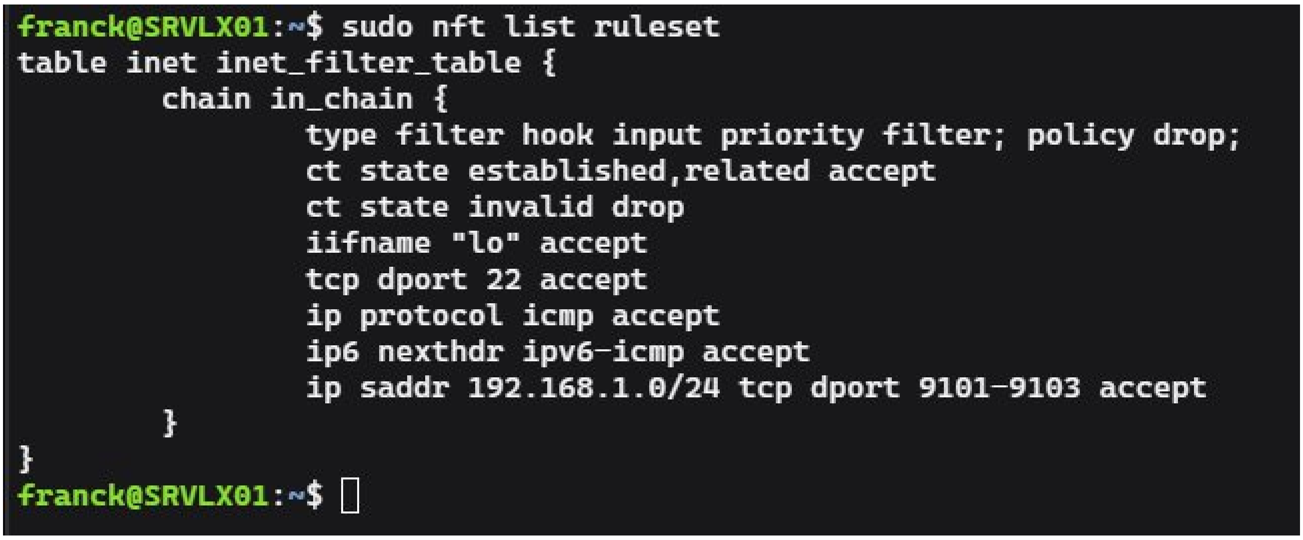
Réponse à la question

Ct state invalid Touts les paquets avec etat invalide

Drop Tout le reste du trafic entrant

Q.2.5.4

Réponse à la question

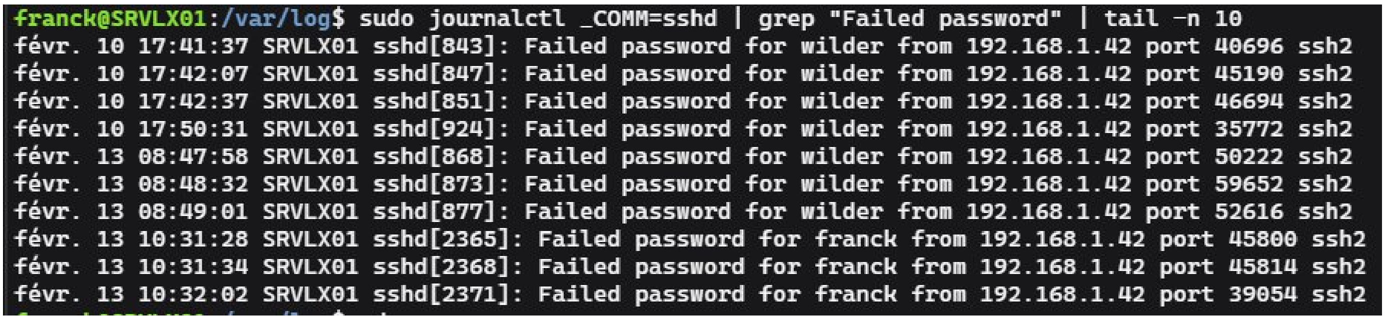


```
franck@SRVLX01:~$ sudo nft list ruleset
table inet inet_filter_table {
        chain in_chain {
                type filter hook input priority filter; policy drop;
                ct state established,related accept
                ct state invalid drop
                iifname "lo" accept
                tcp dport 22 accept
                ip protocol icmp accept
                ip6 nexthdr ipv6-icmp accept
                ip saddr 192.168.1.0/24 tcp dport 9101-9103 accept
        }
}
franck@SRVLX01:~$ 
```

Partie 6

Q.2.6.1

Réponse à la question



```
franck@SRVLX01:/var/log$ sudo journalctl _COMM=sshd | grep "Failed password" | tail -n 10
févr. 10 17:41:37 SRVLX01 sshd[843]: Failed password for wilder from 192.168.1.42 port 40696 ssh2
févr. 10 17:42:07 SRVLX01 sshd[847]: Failed password for wilder from 192.168.1.42 port 45190 ssh2
févr. 10 17:42:37 SRVLX01 sshd[851]: Failed password for wilder from 192.168.1.42 port 46694 ssh2
févr. 10 17:50:31 SRVLX01 sshd[924]: Failed password for wilder from 192.168.1.42 port 35772 ssh2
févr. 13 08:47:58 SRVLX01 sshd[868]: Failed password for wilder from 192.168.1.42 port 50222 ssh2
févr. 13 08:48:32 SRVLX01 sshd[873]: Failed password for wilder from 192.168.1.42 port 59652 ssh2
févr. 13 08:49:01 SRVLX01 sshd[877]: Failed password for wilder from 192.168.1.42 port 52616 ssh2
févr. 13 10:31:28 SRVLX01 sshd[2365]: Failed password for franck from 192.168.1.42 port 45800 ssh2
févr. 13 10:31:34 SRVLX01 sshd[2368]: Failed password for franck from 192.168.1.42 port 45814 ssh2
févr. 13 10:32:02 SRVLX01 sshd[2371]: Failed password for franck from 192.168.1.42 port 39054 ssh2
```