

Compte rendu de travaux pratiques

TP3

Partager des fichiers et maîtriser les journaux

Nom : PACHOT

Prénom : Dorian

Classe : BTS SIO 2e année

Module : Linux avancé

Date de la séance : 9 septembre 2026

1. Objectif

Dans ce TP, je monte un espace de travail partagé sur srv-linux. Le partage est accessible depuis les postes Windows avec Samba, et depuis les serveurs Linux avec NFS.

Je m'occupe ensuite des journaux. Je rends le journal du système persistant, je crée un journal applicatif à part avec rsyslog, je le fais tourner avec logrotate, et je bannis les adresses qui échouent à se connecter en SSH avec fail2ban.

Ces machines viennent du TP1 et servent encore au jour 5. Elles doivent rester en état à la fin de la séance.

2. Environnement de travail

Machine	Système	Adresse IP	Rôle
poste-hote	Windows 11, VMware Workstation Pro 17.6.1	192.168.100.1 / 24 sur VMnet2	Poste étudiant, client Samba
srv-linux	Debian 12 « bookworm »	192.168.100.10 / 24	Serveur Samba, serveur NFS, collecteur de journaux
cli-linux	Debian 12, clone de srv-linux	192.168.100.50 par réservation DHCP	Client Samba et NFS, émetteur de journaux

Le réseau pédagogique est VMnet2, en host-only sur 192.168.100.0/24. Le domaine DNS bts-sio.lan monté au TP1 est toujours en place. Sur ces machines, la carte du réseau pédagogique s'appelle ens33 et non ens37 comme dans l'énoncé.

Avant de commencer, j'ai pris un instantané VMware des deux machines, nommé « Avant TP3 ». La partie D modifie /etc/fstab, et une faute à cet endroit empêche la machine de démarrer.

3. Déroulé

Partie A. Préparer les comptes et l'arborescence

Créer le groupe et les trois comptes

Je crée le groupe formation et les trois comptes. alice et bob sont mis dans formation, carla non. Elle sert à tester un refus.

```
sio@srv-linux:~$ sudo groupadd formation
```

```
sio@srv-linux:~$ sudo useradd -m -s /bin/bash -G formation alice
sio@srv-linux:~$ sudo useradd -m -s /bin/bash -G formation bob
sio@srv-linux:~$ sudo useradd -m -s /bin/bash carla
sio@srv-linux:~$ echo 'alice:...' | sudo chpasswd
sio@srv-linux:~$ echo 'bob:...' | sudo chpasswd
sio@srv-linux:~$ echo 'carla:...' | sudo chpasswd
sio@srv-linux:~$ id alice ; id bob ; id carla
uid=1001(alice) gid=1002(alice) groupes=1002(alice),1001(formation)
uid=1002(bob) gid=1003(bob) groupes=1003(bob),1001(formation)
uid=1003(carla) gid=1004(carla) groupes=1004(carla)
```

Je ne recopie pas les mots de passe. Le id montre que alice et bob ont bien formation en groupe secondaire, et pas carla. Le groupe formation a le GID 1001.

Créer le répertoire commun et poser le bit SGID

```
sio@srv-linux:~$ sudo mkdir -p /srv/samba/commun
sio@srv-linux:~$ sudo chown root:formation /srv/samba/commun
sio@srv-linux:~$ sudo chmod 2770 /srv/samba/commun
sio@srv-linux:~$ ls -ld /srv/samba/commun
drwxrws--- 2 root formation 4096  9 sept. 14:00 /srv/samba/commun
```

Le répertoire est à root et au groupe formation. Le s à la place du x veut dire que le SGID est posé.

Vérifier l'effet du bit SGID

```
sio@srv-linux:~$ sudo -u alice touch /srv/samba/commun/essai-alice.txt
sio@srv-linux:~$ ls -l /srv/samba/commun/
ls: impossible d'ouvrir le répertoire '/srv/samba/commun/': Permission non accordée
sio@srv-linux:~$ sudo ls -l /srv/samba/commun/
total 0
-rw-r--r-- 1 alice formation 0  9 sept. 14:00 essai-alice.txt
sio@srv-linux:~$ sudo ls -ln /srv/samba/commun/
total 0
-rw-r--r-- 1 1001 1001 0  9 sept. 14:00 essai-alice.txt
```

Mon premier ls a raté. C'est normal, mon compte sio n'est pas dans formation. Avec sudo je vois le fichier. Il est à alice mais au groupe formation, alors que le groupe principal d'alice c'est alice. C'est le SGID qui a fait ça. En numérique le GID est 1001, donc formation.

Tester le refus pour carla

```
sio@srv-linux:~$ sudo -u carla ls /srv/samba/commun/
ls: impossible d'ouvrir le répertoire '/srv/samba/commun/': Permission non accordée
```

carla n'est pas dans formation, l'accès lui est refusé.

Partie B. Installer et configurer Samba

Installation et sauvegarde de la configuration d'origine

```
sio@srv-linux:~$ sudo apt update
sio@srv-linux:~$ sudo apt install samba smbclient
sio@srv-linux:~$ sudo cp /etc/samba/smb.conf /etc/samba/smb.conf.origine
```

Le fichier de Debian fait plus de 250 lignes. Je le sauvegarde avant de mettre le mien, plus court.

Écriture du fichier smb.conf

J'ai écrit mon smb.conf à partir du cahier des charges. Le fichier entier est recopié au chapitre 5. Chez moi la carte du réseau pédagogique s'appelle ens33 et pas ens37 comme dans l'énoncé.

Contrôle de la syntaxe avec testparm

```

sio@srv-linux:~$ sudo testparm
Load smb config files from /etc/samba/smb.conf
Loaded services file OK.
Weak crypto is allowed by GnuTLS (e.g. NTLM as a compatibility fallback)

Server role: ROLE_STANDALONE

Press enter to see a dump of your service definitions

# Global parameters
[global]
    bind interfaces only = Yes
    interfaces = lo ens33
    log file = /var/log/samba/log.%m
    logging = file
    max log size = 1000
    security = USER
    server min protocol = SMB2
    server role = standalone server
    server string = Serveur de fichiers %h (Samba %v)
    workgroup = BTSSIO
    idmap config * : backend = tdb
    hosts allow = 127.0.0.1 192.168.100.0/24
    hosts deny = 0.0.0.0/0

[commun]
    comment = Espace commun de l'equipe formation
    create mask = 0660
    directory mask = 02770
    force group = formation
    path = /srv/samba/commun
    read only = No
    valid users = @formation
    write list = @formation

[perso]
    browseable = No
    comment = Repertoire personnel de %U
    create mask = 0600
    directory mask = 0700
    path = /home/%U
    read only = No
    valid users = %U

```

Loaded services file OK, donc pas d'erreur de syntaxe, et mes deux partages sont là.

Création des mots de passe Samba et démarrage des services

```

sio@srv-linux:~$ sudo smbpasswd -a alice
sio@srv-linux:~$ sudo smbpasswd -a bob
sio@srv-linux:~$ sudo smbpasswd -a carla
sio@srv-linux:~$ sudo pdbedit -L
alice:1001:
carla:1003:
bob:1002:

```

Les trois comptes sont bien dans la base Samba, avec les mêmes UID qu'en partie A.

```

sio@srv-linux:~$ sudo systemctl restart smbd nmbd
sio@srv-linux:~$ sudo systemctl enable smbd nmbd
sio@srv-linux:~$ systemctl status smbd --no-pager
● smbd.service - Samba SMB Daemon
    Loaded: loaded (/lib/systemd/system/smbd.service; enabled; preset: enabled)

```

```

Active: active (running) since Wed 2026-09-09 14:24:06 CEST; 14s ago
   Docs: man:smbd(8)
         man:samba(7)
         man:smb.conf(5)
Main PID: 3048 (smbd)
  Status: "smbd: ready to serve connections..."
    Tasks: 3 (limit: 2272)
  Memory: 5.4M
    CPU: 103ms
  CGroup: /system.slice/smbd.service
          └─3048 /usr/sbin/smbd --foreground --no-process-group
            └─3050 /usr/sbin/smbd --foreground --no-process-group
              └─3051 /usr/sbin/smbd --foreground --no-process-group

```

Le service tourne et il est activé au démarrage.

Partie C. Tester depuis le poste Windows hôte

Ouvrir le partage depuis l'Explorateur

J'ai mis \\192.168.100.10\commun dans la barre d'adresse de l'Explorateur et je me suis connecté en SRV-LINUX\alice. J'ai dû mettre le préfixe SRV-LINUX, sinon ça ne passe pas.

Au premier essai j'ai eu le code 0x80070043. C'était le pare-feu du serveur, je l'explique au chapitre 6.

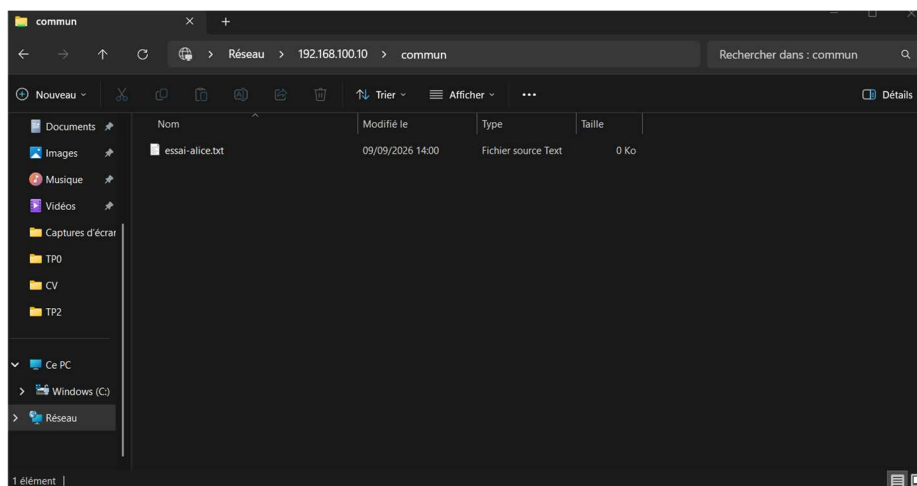


Figure 1 : le partage commun ouvert dans l'Explorateur Windows

Ensuite j'ai créé un fichier texte depuis-windows-alice.txt dans le partage.

Observer le résultat côté Linux

```

sio@srv-linux:~$ sudo ls -l /srv/samba/commun/
total 0
-rw-rw---- 1 alice formation 0  9 sept. 15:03 depuis-windows-alice.txt
-rw-r--r-- 1 alice formation 0  9 sept. 14:00 essai-alice.txt

```

Les deux fichiers ont le même propriétaire et le même groupe, mais pas les mêmes droits. Celui qui vient de Windows est en 660, celui fait avec touch est en 644.

```

sio@srv-linux:~$ sudo ls -l /srv/samba/commun/
total 0
-rw-rw---- 1 alice formation 0  9 sept. 15:03 depuis-windows-alice.txt
-rw-r--r-- 1 alice formation 0  9 sept. 14:00 essai-alice.txt
sio@srv-linux:~$

```

Figure 2 : les deux fichiers au groupe formation

```
sio@srv-linux:~$ sudo smbstatus
```

Samba version 4.17.12-Debian

PID	Username	Group	Machine	Protocol
Version	Encryption		Signing	
3418	alice	alice	192.168.100.1 (ipv4:192.168.100.1:54585)	SMB3_11
-		AES-128-GMAC		

Service	pid	Machine	Connected at	Encryption	Signing
commun	3418	192.168.100.1	mer. sept. 9 14:57:00 2026 CEST	-	AES-128-GMAC

Locked files:

Pid	User(ID)	DenyMode	Access	R/W	Oplock	SharePath	Name
Time							
3418	1001	DENY_NONE	0x100081	RDONLY	NONE		
/srv/samba/commun	.	Wed Sep 9 15:01:16 2026					

La session est en SMB3_11, donc mon server min protocol = SMB2 est respecté.

Connecter un lecteur réseau permanent

Mon premier essai a raté avec l'erreur 1219.

```
PS C:\Users\doria> net use Z: \\192.168.100.10\commun /user:alice * /persistent:yes
Entrez le mot de passe pour \\192.168.100.10\commun :
L'erreur système 1219 s'est produite.
```

Plusieurs connexions à un serveur ou à une ressource partagée par le même utilisateur, en utilisant plus d'un nom utilisateur, ne sont pas autorisées. Supprimez toutes les connexions précédentes au serveur ou à la ressource partagée et recommencez.

Ma fenêtre d'Explorateur était encore ouverte sur le partage. Je la ferme et je vide les connexions.

```
PS C:\Users\doria> net use * /delete /y
Vous possédez les connexions à distance suivantes :
```

```
\\192.168.100.10\commun
La poursuite de cette opération va rompre les connexions.
```

La commande s'est terminée correctement.

```
PS C:\Users\doria> net use
La liste est vide.
```

```
PS C:\Users\doria> net use Z: \\192.168.100.10\commun /user:alice * /persistent:yes
Entrez le mot de passe pour \\192.168.100.10\commun :
La commande s'est terminée correctement.
```

```
PS C:\Users\doria> net use
```

État	Local	Distant	Réseau
OK	Z:	\\192.168.100.10\commun	Microsoft Windows Network

Le lecteur Z: est monté et il apparaît dans Ce PC. J'ai mis un * à la place du mot de passe pour ne pas l'écrire dans la commande.

```

PS C:\Users\doria> net use Z: \\192.168.100.10\commun /user:alice * /persistent:yes
Entrez le mot de passe pour \\192.168.100.10\commun :
L'erreur système 1219 s'est produite.

Plusieurs connexions à un serveur ou à une ressource partagée par le même utilisateur, en utilisant pl
us d'un nom utilisateur, ne sont pas autorisées. Supprimez toutes les connexions précédentes au serveu
r ou à la ressource partagée et recommencez.

PS C:\Users\doria> net use
Les nouvelles connexions seront mémorisées.

État          Local      Distant          Réseau
-----
OK             \\192.168.100.10\commun  Microsoft Windows Network
La commande s'est terminée correctement.

PS C:\Users\doria>

```

Figure 3 : le lecteur Z: monté sur le partage

Tester le refus avec carla

Je vide d'abord les sessions et les identifiants gardés.

```

PS C:\Users\doria> net use * /delete /y
Vous possédez les connexions à distance suivantes :

Z:                \\192.168.100.10\commun
La poursuite de cette opération va rompre les connexions.
La commande s'est terminée correctement.

PS C:\Users\doria> cmdkey /delete:192.168.100.10
CMDKEY: Élément introuvable.

```

cmdkey ne trouve rien pour 192.168.100.10, je n'ai pas coché Mémoriser mes informations d'identification. Le cache est donc vide.

J'ouvre le partage en SRV-LINUX\carla. Windows me redemande le mot de passe, puis il affiche Accès refusé.

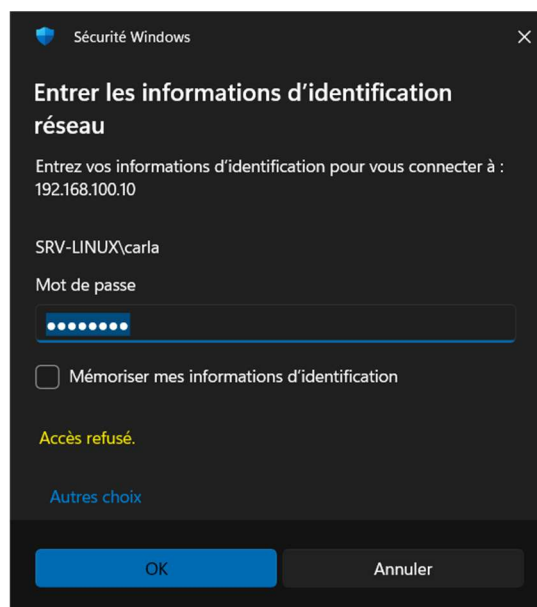


Figure 4 : le refus obtenu avec carla

Vérifier l'écriture partagée avec bob

Je revide les connexions, je me reconnecte en SRV-LINUX\bob et j'ouvre depuis-windows-alice.txt pour écrire une ligne dedans. L'enregistrement marche. bob peut bien modifier le fichier d'alice.

Partie D. Tester le partage depuis cli-linux

Installer le client et lister les partages

L'installation n'est pas passée du premier coup, cli-linux n'a pas d'accès Internet. Je l'explique au chapitre 6.

```
sio@cli-linux:~$ sudo apt install smbclient cifs-utils
sio@cli-linux:~$ smbclient -L //192.168.100.10 -U alice
Password for [WORKGROUP\alice]:

      Sharename      Type            Comment
      -----
      commun         Disk            Espace commun de l'equipe formation
      IPC$           IPC            IPC Service (Serveur de fichiers srv-linux (Samba
4.17.12-Debian))
SMB1 disabled -- no workgroup available
```

Seul commun apparaît. perso n'est pas dans la liste.

Le fichier d'identifiants

J'ai mis dans /etc/samba/credentials les trois lignes username, password et domain. Le fichier est recopié au chapitre 5, sans le mot de passe.

```
sio@cli-linux:~$ sudo chmod 600 /etc/samba/credentials
sio@cli-linux:~$ sudo ls -l /etc/samba/credentials
-rw----- 1 root root 47 10 sept. 09:04 /etc/samba/credentials
```

Le fichier est bien à root et lisible par lui seul.

Le montage permanent

J'ai relevé mon UID avec id sio, c'est 1000 pour l'utilisateur comme pour le groupe. Je m'en sers dans la ligne de fstab, qui est recopiée au chapitre 5.

```
sio@cli-linux:~$ sudo mount -a
montage : (astuce) votre fstab a été modifié mais systemd utilise encore
l'ancienne version ; utilisez « systemctl daemon-reload » pour recharger.
sio@cli-linux:~$ findmnt /mnt/commun
TARGET          SOURCE          FSTYPE OPTIONS
/mnt/commun     //192.168.100.10/commun cifs
rw,relatime,vers=3.0,cache=strict,username=alice,domain=BTS
sio@cli-linux:~$ ls -l /mnt/commun/
total 4
-rwxr-xr-x 1 sio sio 11  9 sept. 15:14 depuis-windows-alice.txt
-rwxr-xr-x 1 sio sio  0  9 sept. 14:00 essai-alice.txt
sio@cli-linux:~$ touch /mnt/commun/depuis-cli.txt
sio@cli-linux:~$ ls -l /mnt/commun/
total 4
-rwxr-xr-x 1 sio sio  0 10 sept. 09:06 depuis-cli.txt
-rwxr-xr-x 1 sio sio 11  9 sept. 15:14 depuis-windows-alice.txt
-rwxr-xr-x 1 sio sio  0  9 sept. 14:00 essai-alice.txt
```

Le montage marche et l'écriture aussi. Les fichiers apparaissent en sio alors que sur le serveur ils sont à alice et au groupe formation. Ce sont mes options uid=1000 et gid=1000 qui décident de ce qu'on voit ici.

J'ai ensuite fait le systemctl daemon-reload demandé par mount.

Partie E. Mettre en place le partage NFS

Le serveur

```
sio@srv-linux:~$ sudo apt install nfs-kernel-server
sio@srv-linux:~$ sudo mkdir -p /srv/nfs/partage
sio@srv-linux:~$ sudo chown nobody:nogroup /srv/nfs/partage
sio@srv-linux:~$ sudo chmod 0777 /srv/nfs/partage
```

J'ai ensuite écrit /etc/exports, il est recopié au chapitre 5.

```
sio@srv-linux:~$ sudo exportfs -ra
sio@srv-linux:~$ sudo exportfs -v
/srv/nfs/partage
192.168.100.0/24(sync,wdelay,hide,no_subtree_check,sec=sys,rw,secure,
root_squash,no_all_squash)
sio@srv-linux:~$ sudo showmount -e localhost
Export list for localhost:
/srv/nfs/partage 192.168.100.0/24
```

L'export est en place et root_squash est bien actif. showmount ne marche qu'avec sudo, il est dans /usr/sbin qui n'est pas dans le PATH d'un utilisateur normal.

J'ouvre le port dans le pare-feu tout de suite, pour ne pas retomber sur le problème de la partie C.

```
sio@srv-linux:~$ sudo ufw allow from 192.168.100.0/24 to any port 2049 proto tcp comment 'NFS'
Rule added
sio@srv-linux:~$ sudo ufw allow from 192.168.100.0/24 to any port 111 comment 'rpcbind'
Rule added
```

La règle sur le 2049 sert au montage NFSv4. Celle sur le 111 sert à showmount, qui passe par rpcbind : sans elle, showmount depuis le client restait bloqué sans rien afficher.

Le client

```
sio@cli-linux:~$ sudo showmount -e 192.168.100.10
Export list for 192.168.100.10:
/srv/nfs/partage 192.168.100.0/24
sio@cli-linux:~$ sudo mount -t nfs 192.168.100.10:/srv/nfs/partage /mnt/nfs
sio@cli-linux:~$ sudo -u sio touch /mnt/nfs/essai-cli.txt
sio@cli-linux:~$ ls -ln /mnt/nfs/
total 0
-rw-r--r-- 1 1000 1000 0 10 sept. 2026 essai-cli.txt
```

Le montage marche et l'écriture passe.

J'ai ajouté la ligne NFS dans /etc/fstab, elle est recopiée au chapitre 5.

```
sio@cli-linux:~$ sudo mount -a
sio@cli-linux:~$ sudo systemctl daemon-reload
sio@cli-linux:~$ findmnt -t nfs4
TARGET SOURCE FSTYPE OPTIONS
/mnt/nfs 192.168.100.10:/srv/nfs/partage nfs4
rw,relatime,vers=4.2,rsize=262144,wsiz=262144
```

Le montage est permanent et il négocie du NFSv4.2.

L'expérience sur les UID

Je crée david avec un UID différent sur chaque machine.

```
# Sur srv-linux
sio@srv-linux:~$ sudo useradd -m -u 1601 david
sio@srv-linux:~$ sudo -u david touch /srv/nfs/partage/fichier-de-david.txt

# Sur cli-linux
sio@cli-linux:~$ sudo usermod -u 1701 david
```

```
sio@cli-linux:~$ id david
uid=1701(david) gid=1601(david) groupes=1601(david)
```

Sur cli-linux david existait déjà en 1601, je lui change l'UID avec usermod. Le GID reste à 1601.

```
sio@cli-linux:/mnt/nfs$ ls -l /mnt/nfs/
-rw-r--r-- 1 1601 david 0 10 sept. 09:26 fichier-de-david.txt
sio@cli-linux:/mnt/nfs$ ls -ln /mnt/nfs/
-rw-r--r-- 1 1601 1601 0 10 sept. 09:26 fichier-de-david.txt
sio@cli-linux:/mnt/nfs$ sudo -u david touch /mnt/nfs/depuis-cli-david.txt
touch: impossible de faire un touch '/mnt/nfs/depuis-cli-david.txt': Permission non accordée
```

Le fichier créé par david sur le serveur s'affiche avec le numéro 1601 côté client, parce que plus personne ne porte ce numéro là-bas. Et david ne peut même plus toucher à son propre fichier, vu qu'il est maintenant en 1701.

Dans l'autre sens, un fichier créé par david depuis le client :

```
sio@cli-linux:/mnt/nfs$ sudo -u david touch /mnt/nfs/david-uid1701.txt

# Sur srv-linux
sio@srv-linux:~$ ls -l /srv/nfs/partage/
-rw-r--r-- 1 1701 david 0 10 sept. 10:48 david-uid1701.txt
-rw-r--r-- 1 david david 0 10 sept. 09:26 fichier-de-david.txt
```

Le problème est symétrique. Le fichier venu du client apparaît en 1701 sur le serveur, où personne ne porte ce numéro.

L'effet de root_squash

```
sio@cli-linux:/mnt/nfs$ sudo touch /mnt/nfs/fichier-cree-par-root.txt
sio@cli-linux:/mnt/nfs$ ls -l /mnt/nfs/fichier-cree-par-root.txt
-rw-r--r-- 1 nobody nogroup 0 10 sept. 09:28 /mnt/nfs/fichier-cree-par-root.txt
sio@cli-linux:/mnt/nfs$ ls -ln /mnt/nfs/
-rw-r--r-- 1 65534 65534 0 10 sept. 09:28 fichier-cree-par-root.txt
```

J'ai créé le fichier en root depuis le client, et il appartient à nobody sur le serveur, en numéro 65534. C'est root_squash qui fait ça.

Le démontage

```
sio@cli-linux:/mnt/nfs$ sudo umount /mnt/nfs
umount.nfs4: /mnt/nfs: device is busy
sio@cli-linux:/mnt/nfs$ sudo fuser -vm /mnt/nfs
sudo: fuser : commande introuvable
sio@cli-linux:/mnt/nfs$ cd /
sio@cli-linux:/$ sudo umount /mnt/nfs
sio@cli-linux:/$ sudo mount -a
```

Le démontage a été refusé parce que mon shell était dans le répertoire. fuser n'est pas installé sur cette machine, mais le coupable était moi. Je suis sorti avec cd / et le démontage est passé.

Partie F. Explorer, rendre persistants et centraliser les journaux

Exploration de journalctl

Mes premières commandes ne montraient presque rien, avec le message « You are currently not seeing messages from other users and the system ». Mon compte sio n'est pas dans le groupe adm, journalctl ne me montrait donc que mes propres messages. J'ai tout refait avec sudo.

```
sio@srv-linux:~$ sudo journalctl -b -p err --no-pager
sept. 09 13:35:46 srv-linux kernel: [Firmware Bug]: cpu 0, try to use APIC520 ...
```

```

sept. 10 09:15:26 srv-linux blkmapd[4719]: open pipe file /run/rpc_pipefs/nfs/blocklayout
failed
sept. 10 09:48:51 srv-linux sshd[5262]: error: kex_exchange_identification: Connection
closed

sio@srv-linux:~$ sudo journalctl -u smbd -n 20 --no-pager
sept. 09 14:20:04 srv-linux systemd[1]: Starting smbd.service - Samba SMB Daemon...
sept. 09 14:24:06 srv-linux systemd[1]: Stopped smbd.service - Samba SMB Daemon.
sept. 10 09:04:42 srv-linux systemd[1]: Reloaded smbd.service - Samba SMB Daemon.

sio@srv-linux:~$ journalctl --disk-usage
Archived and active journals take up 8.0M in the file system.

```

Le -p err ne garde que les erreurs, le -u smbd ne garde que le service demandé. On y retrouve bien mes redémarrages de Samba de la partie B.

Rendre le journal persistant

Avant de toucher à quoi que ce soit, je relève le nombre de démarrages mémorisés.

```

sio@srv-linux:~$ journalctl --list-boots
IDX BOOT ID FIRST ENTRY LAST ENTRY
-7 ba87f9053d954f66ac96f006b93583a0 Mon 2026-09-07 14:40:05 CEST Mon 2026-09-07 15:43:22
CEST
-6 f45b2aefda924524982a3772f45e999e Mon 2026-09-07 16:06:41 CEST Mon 2026-09-07 16:25:58
CEST
-5 bf94299e8d114405ae649458d8223d96 Tue 2026-09-08 08:51:50 CEST Tue 2026-09-08 09:00:30
CEST
-4 1a15d54c5d6e4732a126512a66061436 Tue 2026-09-08 09:06:25 CEST Tue 2026-09-08 11:14:17
CEST
-3 bfbe3491c8fb430c97dd82eb1f267176 Tue 2026-09-08 11:14:50 CEST Tue 2026-09-08 13:33:57
CEST
-2 3037d286fd884ad9968497d8a18b493e Tue 2026-09-08 13:49:11 CEST Tue 2026-09-08 15:55:49
CEST
-1 a7075656faaf4b4cb497509314bc5b7a Wed 2026-09-09 08:49:50 CEST Wed 2026-09-09 09:47:41
CEST
0 2ada292f174045718ac454e7292533c4 Wed 2026-09-09 13:51:16 CEST Thu 2026-09-10 10:00:32
CEST

sio@srv-linux:~$ ls -ld /var/log/journal
drwxr-sr-x+ 3 root systemd-journal 4096 7 sept. 14:30 /var/log/journal

```

Huit démarrages sont listés, du 7 au 10 septembre, et /var/log/journal existe déjà depuis le 7. Mon journal était donc déjà persistant, ça date du TP1.

J'ai quand même mis les deux directives dans /etc/systemd/journald.conf, elles sont recopiées au chapitre 5, puis j'ai redémarré.

```

sio@srv-linux:~$ journalctl --list-boots
-8 ba87f9053d954f66ac96f006b93583a0 Mon 2026-09-07 14:40:05 CEST Mon 2026-09-07 15:43:22
CEST
...
-1 2ada292f174045718ac454e7292533c4 Wed 2026-09-09 13:51:16 CEST Thu 2026-09-10 14:05:55
CEST
0 50ff0eebcfa9482bb8f3cf3f3ca37f74 Thu 2026-09-10 14:06:30 CEST Thu 2026-09-10 14:06:30
CEST

```

Neuf démarrages maintenant. Le nouveau, c'est mon reboot, pas ma modification.

Le journal applicatif

```

sio@srv-linux:~$ sudo mkdir -p /var/log/sio
sio@srv-linux:~$ sudo chown root:adm /var/log/sio
sio@srv-linux:~$ sudo chmod 0750 /var/log/sio
sio@srv-linux:~$ ls -ld /var/log/sio

```

```
drwxr-x--- 2 root adm 4096 10 sept. 14:08 /var/log/sio
```

Le répertoire est à root, au groupe adm, et fermé aux autres.

rsyslog n'était pas installé sur cette Debian, j'ai dû le poser avant d'écrire ma règle. Le fichier 30-sio.conf est recopié au chapitre 5.

```
sio@srv-linux:~$ sudo rsyslogd -N1
rsyslogd: version 8.2302.0, config validation run (level 1), master config
/etc/rsyslog.conf
rsyslogd: End of config validation run. Bye.
sio@srv-linux:~$ sudo systemctl restart rsyslog
sio@srv-linux:~$ logger -p local1.info -t sauvegarde "Debut du traitement"
sio@srv-linux:~$ logger -p local1.err -t sauvegarde "Echec de connexion a la base"
sio@srv-linux:~$ sudo tail -n 5 /var/log/sio/application.log
2026-09-10T14:11:26.781764+02:00 srv-linux sauvegarde: Debut du traitement
2026-09-10T14:11:26.784425+02:00 srv-linux sauvegarde: Echec de connexion a la base
sio@srv-linux:~$ sudo grep -c sauvegarde /var/log/syslog
0
```

Les deux messages sont bien arrivés dans mon fichier, et le grep sur syslog renvoie 0. Le & stop a fait son travail, les messages ne sont pas dupliqués.

La centralisation

Le collecteur sur srv-linux et l'émetteur sur cli-linux sont recopiés au chapitre 5. rsyslog n'était pas installé sur cli-linux non plus.

```
sio@srv-linux:~$ sudo ss -lntp | grep 514
LISTEN 0 25 0.0.0.0:514 0.0.0.0:* users:(("rsyslogd",pid=1536,fd=8))
LISTEN 0 25 [::]:514 [::]:* users:(("rsyslogd",pid=1536,fd=9))
sio@srv-linux:~$ sudo ss -lnup | grep 514
UNCONN 0 0 0.0.0.0:514 0.0.0.0:* users:(("rsyslogd",pid=1536,fd=6))
UNCONN 0 0 [::]:514 [::]:* users:(("rsyslogd",pid=1536,fd=7))
sio@srv-linux:~$ sudo ufw allow from 192.168.100.0/24 to any port 514 comment 'rsyslog'
Rule added
```

Le collecteur écoute bien sur le 514 en TCP et en UDP. En TCP l'état est LISTEN, en UDP c'est UNCONN, c'est normal, l'UDP n'établit pas de connexion. J'ouvre le port dans le pare-feu, sinon rien n'arriverait.

```
sio@cli-linux:/$ logger -t test-centralisation "Bonjour depuis cli-linux"

# Sur srv-linux
sio@srv-linux:~$ sudo ls -R /var/log/distant/
/var/log/distant/:
cli-linux

/var/log/distant/cli-linux:
rsyslogd.log sudo.log systemd.log test-centralisation.log
sio@srv-linux:~$ sudo tail -n 5 /var/log/distant/cli-linux/test-centralisation.log
2026-09-10T14:15:19+02:00 cli-linux test-centralisation: Bonjour depuis cli-linux
```

Le message parti de cli-linux est bien rangé dans un dossier à son nom, et dans un fichier au nom du programme. Les autres fichiers du dossier viennent des services de cli-linux qui écrivent aussi dans son journal.

Partie G. Faire tourner le journal applicatif

J'ai écrit /etc/logrotate.d/sio-application, il est recopié au chapitre 5, puis je l'ai protégé et simulé avant de forcer la rotation.

```
sio@srv-linux:~$ sudo chown root:root /etc/logrotate.d/sio-application
```

```
sio@srv-linux:~$ sudo chmod 644 /etc/logrotate.d/sio-application
sio@srv-linux:~$ sudo logrotate -d /etc/logrotate.d/sio-application
reading config file /etc/logrotate.d/sio-application
Reading state from file: /var/lib/logrotate/status
```

Handling 1 logs

```
rotating pattern: /var/log/sio/*.log after 1 days (7 rotations)
empty log files are not rotated, old logs are removed
considering log /var/log/sio/application.log
  Now: 2026-09-10 14:27
  Last rotated at 2026-09-10 14:00
  log does not need rotating (log has already been rotated)
```

Le mode -d ne fait qu'afficher ce qu'il ferait, il n'écrit rien. Il confirme ma configuration : rotation quotidienne, 7 générations, pas de rotation si le fichier est vide.

```
sio@srv-linux:~$ sudo logrotate -f /etc/logrotate.d/sio-application
sio@srv-linux:~$ sudo ls -l /var/log/sio/
total 8
-rw-r----- 1 root adm  0 10 sept. 14:27 application.log
-rw-r----- 1 root adm 78 10 sept. 14:27 application.log.1
-rw-r----- 1 root adm 126 10 sept. 14:11 application.log.2.gz
```

Le fichier courant est vide et recréé en 0640 root adm, comme demandé. L'archive la plus récente n'est pas compressée.

```
sio@srv-linux:~$ logger -p local1.info -t sauvegarde "Message apres rotation"
sio@srv-linux:~$ sudo tail -n 3 /var/log/sio/application.log
2026-09-10T14:27:03.176931+02:00 srv-linux sauvegarde: Message apres rotation
```

Le message émis après la rotation arrive bien dans le nouveau fichier.

```
sio@srv-linux:~$ sudo logrotate -f /etc/logrotate.d/sio-application
sio@srv-linux:~$ sudo ls -l /var/log/sio/
total 12
-rw-r----- 1 root adm  0 10 sept. 14:28 application.log
-rw-r----- 1 root adm 78 10 sept. 14:28 application.log.1
-rw-r----- 1 root adm 96 10 sept. 14:27 application.log.2.gz
-rw-r----- 1 root adm 126 10 sept. 14:11 application.log.3.gz
```

L'ancienne .1 est devenue .2.gz. C'est ça, delaycompress : la compression est décalée d'une rotation.

```
sio@srv-linux:~$ systemctl list-timers logrotate.timer
NEXT                LEFT    LAST                PASSED            UNIT
Fri 2026-09-11 00:00:00 CEST 9h left Thu 2026-09-10 08:52:35 CEST 5h 34min ago
logrotate.timer
```

Sur Debian 12, logrotate est déclenché par un timer systemd, tous les jours à minuit.

Partie H. Bannir automatiquement avec fail2ban

J'ai installé fail2ban et écrit /etc/fail2ban/jail.local, jamais jail.conf. Le fichier est recopié au chapitre 5. J'ai gardé la console VMware de srv-linux ouverte pendant tout le test.

```
sio@srv-linux:~$ sudo systemctl restart fail2ban
sio@srv-linux:~$ sudo fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| |- Currently failed: 0
| |- Total failed: 0
| `-- Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM=sshd
`- Actions
   |- Currently banned: 0
   |- Total banned: 0
   `-- Banned IP list:
```

La prison sshd est active et elle lit le journal systemd, comme demandé par backend = systemd.

Provoquer le bannissement

```
sio@cli-linux:/$ ssh inexistant@192.168.100.10
inexistent@192.168.100.10: Permission denied (publickey).
```

La connexion est refusée tout de suite, sans demander de mot de passe. C'est le durcissement SSH du TP1 : l'authentification par mot de passe est coupée, seule la clé est acceptée. Chaque tentative compte quand même comme un échec pour fail2ban. J'ai répété quatre fois.

```
sio@srv-linux:~$ sudo fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| |- Currently failed: 1
| |- Total failed: 4
| \- Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM=sshd
\-- Actions
   |- Currently banned: 1
   |- Total banned: 1
   \- Banned IP list: 192.168.100.50
```

```
sio@srv-linux:~$ sudo fail2ban-client status sshd
sudo nft list ruleset | grep -A6 f2b
Status for the jail: sshd
|- Filter
| |- Currently failed: 1
| |- Total failed: 4
| \- Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM=sshd
\-- Actions
   |- Currently banned: 1
   |- Total banned: 1
   \- Banned IP list: 192.168.100.50
# Warning: table ip filter is managed by iptables-nft, do not touch!
meta l4proto tcp tcp dport 22 counter packets 5 bytes 532 jump f2b-sshd
counter packets 1576 bytes 2265240 jump ufw-before-logging-input
counter packets 1576 bytes 2265240 jump ufw-before-input
counter packets 65 bytes 11052 jump ufw-after-input
counter packets 0 bytes 0 jump ufw-after-logging-input
counter packets 0 bytes 0 jump ufw-reject-input
counter packets 0 bytes 0 jump ufw-track-input
--
chain f2b-sshd {
    ip saddr 192.168.100.50 counter packets 0 bytes 0 reject
    counter packets 5 bytes 532 return
}
table ip6 filter {
    chain ufw6-before-logging-input {
# Warning: table ip6 filter is managed by iptables-nft, do not touch!
sio@srv-linux:~$
```

Figure 6 : l'adresse de cli-linux bannie et la règle dans le pare-feu

```
sio@srv-linux:~$ sudo nft list ruleset | grep -A6 f2b
meta l4proto tcp tcp dport 22 counter packets 5 bytes 532 jump f2b-sshd

chain f2b-sshd {
    ip saddr 192.168.100.50 counter packets 0 bytes 0 reject
    counter packets 5 bytes 532 return
}
```

fail2ban a créé sa propre chaîne f2b-sshd, branchée sur le port 22, avec une règle reject sur l'adresse de cli-linux.

```
sio@cli-linux:/$ ssh inexistant@192.168.100.10
ssh: connect to host 192.168.100.10 port 22: Connection refused
```

Le message a changé. Avant le bannissement, le serveur répondait et refusait l'authentification. Maintenant la connexion elle-même est refusée.

Débannir

```
sio@srv-linux:~$ sudo fail2ban-client set sshd unbanip 192.168.100.50
```

```

1
sio@srv-linux:~$ sudo fail2ban-client status sshd
`- Actions
  | - Currently banned: 0
  | - Total banned:    1
  `-- Banned IP list:
sio@srv-linux:~$ sudo nft list ruleset | grep -A6 f2b-sshd
      chain f2b-sshd {
          counter packets 19 bytes 1596 return
      }

```

L'adresse a disparu de la liste et la règle reject n'est plus dans le pare-feu. Il ne reste que le return.

4. Réponses aux questions

Partie A

Q1. *Donnez la sortie de `ls -ld /srv/samba/commun`. Que signifie le s qui apparaît à la place du x des droits du groupe ?*

```

sio@srv-linux:~$ ls -ld /srv/samba/commun
drwxrws--- 2 root formation 4096  9 sept. 14:00 /srv/samba/commun

```

Le s à la place du x c'est le bit SGID. Il impose aux fichiers et sous-répertoires créés à l'intérieur d'appartenir au groupe du répertoire et pas à celui du créateur.

Q2. *À quel groupe appartient `essai-alice.txt` ? Expliquez précisément pourquoi ce n'est pas le groupe principal d'alice, et ce qui se passerait sans le bit SGID.*

Le fichier `essai-alice.txt` est dans le groupe formation (1001). Sans rien de particulier ça aurait dû être au groupe alice (1002), donc le SGID force tout ce qui est créé dedans à être dans formation, sinon bob ne pourrait pas le modifier.

Q3. *Le troisième chiffre de 2770 vaut 0. Quelles conséquences concrètes cela a-t-il pour carla lorsqu'elle est connectée en local sur le serveur ? Vérifiez-le par une commande et donnez le message obtenu.*

Dans 2770, le dernier chiffre vise les autres, et il vaut 0. carla n'est pas root et son id montre qu'elle n'est pas dans formation. Elle n'est donc ni le propriétaire ni dans le groupe, elle tombe dans les autres, et là elle n'a rien du tout : pas de lecture donc elle ne peut pas lister, pas d'écriture donc elle ne peut rien créer, pas de x donc elle ne peut même pas entrer dans le répertoire.

```

sio@srv-linux:~$ sudo -u carla ls /srv/samba/commun/
ls: impossible d'ouvrir le répertoire '/srv/samba/commun/': Permission non accordée

```

Ici on est en local sur le serveur, Samba n'intervient pas. Le refus vient uniquement des droits POSIX.

Q4. *Relevez les UID d'alice, bob et carla sur srv-linux. Notez-les : ils serviront en partie E.*

Utilisateur	UID	GID principal
alice	1001	1002 (alice)
bob	1002	1003 (bob)
carla	1003	1004 (carla)

Le groupe formation porte le GID 1001.

Partie B

Q5. Recopiez votre section [global] et justifiez en une phrase chacune des directives bind interfaces only, hosts allow et server min protocol.

```
[global]
workgroup = BTSSIO
server string = Serveur de fichiers %h (Samba %v)
netbios name = SRV-LINUX
security = user
map to guest = Never
log file = /var/log/samba/log.%m
max log size = 1000
logging = file
interfaces = lo ens33
bind interfaces only = yes
hosts allow = 127.0.0.1 192.168.100.0/24
hosts deny = 0.0.0.0/0
server min protocol = SMB2
server role = standalone server
passdb backend = tdbsam
unix charset = UTF-8
```

Directive	Justification
bind interfaces only = yes	Sans elle, Samba écoute partout. Avec elle, les sockets ne s'ouvrent que sur les interfaces listées.
hosts allow	Liste blanche puis refus du reste, appliqués avant toute authentification.
server min protocol	Version minimale acceptée. SMB2 interdit SMB1. Non négociable.

Q6. Recopiez votre section [commun]. Quelle directive garantit que le fichier déposé par alice restera modifiable par bob, et pourquoi le bit SGID de la partie A ne suffit-il pas à lui seul ?

```
[commun]
comment = Espace commun de l'equipe formation
path = /srv/samba/commun
browseable = yes
read only = no
guest ok = no
valid users = @formation
write list = @formation
create mask = 0660
directory mask = 2770
force group = formation
```

La directive qui fait que le fichier reste modifiable, c'est create mask = 0660. Et le SGID ne suffit pas parce qu'il ne touche pas aux droits, il s'occupe seulement du groupe.

Q7. Quelle variable de substitution avez-vous employée dans [perso] ? Que vaut-elle lorsque bob se connecte ? Pourquoi browseable = no n'est-il pas une mesure de sécurité ?

La variable c'est %U. Elle vaut bob quand il se connecte. Et browseable = no c'est juste du confort, on peut encore trouver le partage par son nom.

Q8. Exécutez sudo ss -lntp | grep smbd et donnez la sortie. Sur quels ports et quelles adresses smbd écoute-t-il ? Ce résultat est-il cohérent avec vos directives interfaces et bind interfaces only ?

```
sio@srv-linux:~$ sudo ss -lntp | grep smbd
LISTEN 0  50      127.0.0.1:139  0.0.0.0:*  users:(("smbd",pid=3048,fd=31))
LISTEN 0  50      192.168.100.10:139  0.0.0.0:*  users:(("smbd",pid=3048,fd=29))
LISTEN 0  50      192.168.100.10:445  0.0.0.0:*  users:(("smbd",pid=3048,fd=28))
LISTEN 0  50      127.0.0.1:445  0.0.0.0:*  users:(("smbd",pid=3048,fd=30))
LISTEN 0  50      [::1]:139      [::]:*    users:(("smbd",pid=3048,fd=33))
LISTEN 0  50      [::1]:445      [::]:*    users:(("smbd",pid=3048,fd=32))
```

smbd écoute sur les ports 139 et 445, et sur les adresses 127.0.0.1 et 192.168.100.10. Et oui, c'est cohérent avec les directives, car sans bind interfaces only on verrait 0.0.0.0.

Q9. `sudo pdbedit -L` liste les comptes Samba. Pourquoi un compte doit-il exister à la fois en Unix et en Samba ? Que se passe-t-il si l'on oublie `smbpasswd -a` ?

```
sio@srv-linux:~$ sudo pdbedit -L
alice:1001:
carla:1003:
bob:1002:
```

Un compte doit être des deux côtés car Samba ne gère que des mots de passe de comptes Unix existants. Unix donne un UID et c'est ce qui donne l'accès aux fichiers. Si on oublie `smbpasswd -a`, le compte Unix marchera toujours mais Samba renvoie `NT_STATUS_LOGON_FAILURE`.

Partie C

Q10. Quel est le propriétaire et quel est le groupe du fichier `depuis-windows-alice.txt` vu depuis Linux ? Quels sont ses droits en octal ? Reliez chacun de ces trois résultats à une directive précise de votre `smb.conf`.

```
-rw-rw---- 1 alice formation 0 9 sept. 15:03 depuis-windows-alice.txt
```

Le fichier appartient à alice, au groupe formation, en 660.

Ce qu'on voit	Directive
propriétaire alice	security = user
groupe formation	force group = formation
droits 660	create mask = 0660

Q11. Donnez la sortie de `sudo smbstatus`. Quelles informations y trouve-t-on que `ls -l` ne donne pas ?

```
sio@srv-linux:~$ sudo smbstatus

Samba version 4.17.12-Debian
PID      Username  Group   Machine                                  Protocol  Signing
3418     alice    alice  192.168.100.1 (ipv4:192.168.100.1:54585) SMB3_11   AES-128-GMAC

Service      pid      Machine      Connected at
commun       3418     192.168.100.1 mer. sept.  9 14:57:00 2026 CEST

Locked files:
Pid  User(ID)  DenyMode  Access  R/W  Oplock  SharePath      Name
3418 1001      DENY_NONE 0x100081 RDONLY NONE    /srv/samba/commun .
```

`smbstatus` montre qui est connecté (alice), depuis quelle machine (192.168.100.1), la version du protocole (SMB3_11), la signature, l'heure de connexion et les fichiers verrouillés. `ls -l` ne donne rien de tout ça : il décrit le disque, pas les connexions en cours.

Q12. Quel message exact Windows affiche-t-il pour carla ? Quelle directive de `smb.conf` produit ce refus ? Le refus vient-il de Samba ou des droits POSIX ? Justifiez.

Le message est « Accès refusé. ». La directive est `valid users = @formation`, et carla n'est pas dans ce groupe. Le refus vient de Samba, pas de POSIX : le message n'est pas « le nom d'utilisateur ou le mot de passe est incorrect », donc carla s'est bien authentifiée. Elle a été bloquée après, à l'entrée du partage.

Q13. Expliquez à quoi sert `cmdkey /list` et pourquoi `net use * /delete /y` est indispensable avant de tester un second compte sur le même serveur.

`cmdkey /list` affiche les identifiants mémorisés par Windows. `net use * /delete /y` coupe les sessions ouvertes. C'est indispensable parce que Windows ne garde qu'une seule session par serveur : sans

ça, il réutilise le premier compte sans rien redemander, et on croit tester carla alors qu'on teste encore alice.

Q14. Connectez-vous en bob et modifiez le fichier créé par alice. Cela fonctionne-t-il ? Quelle combinaison de réglages (côté POSIX et côté Samba) rend cela possible ?

Oui, ça marche. bob a pu modifier le fichier créé par alice. Deux réglages le permettent : côté POSIX le bit SGID met le fichier au groupe formation, côté Samba create mask = 0660 donne le droit d'écriture à ce groupe.

Partie D

Q15. Donnez la sortie de `smbclient -L //192.168.100.10 -U alice`. Le partage perso y figure-t-il ? Pourquoi ?

```
sio@cli-linux:~$ smbclient -L //192.168.100.10 -U alice
Password for [WORKGROUP\alice]:

      Sharename      Type      Comment
      -----
      commun         Disk      Espace commun de l'equipe formation
      IPC$           IPC       IPC Service (Serveur de fichiers srv-linux (Samba
4.17.12-Debian))
SMB1 disabled -- no workgroup available
```

Non, il n'y a pas le partage perso. Il existe mais il est caché, on doit pouvoir le trouver avec son nom directement. C'est à cause de `browseable = no`.

Q16. Recopiez votre ligne de `/etc/fstab` et expliquez le rôle de `uid=`, `gid=` et `_netdev`. Que se passerait-il si `_netdev` était absent ?

```
//192.168.100.10/commun /mnt/commun cifs credentials=/etc/samba/credentials,uid=1000,
gid=1000,icharset=utf8,vers=3.0,_netdev 0 0
```

`uid` et `gid` c'est le propriétaire et le groupe côté client. Sans ça, tout serait en root directement et je ne pourrais pas écrire dedans. `_netdev` dit que le montage dépend du réseau. Sans ça le système passe trop tôt et on peut avoir un problème au démarrage.

Q17. Pourquoi le fichier d'identifiants doit-il être en 600 et appartenir à root ? Quelle serait l'alternative si l'on ne voulait aucun mot de passe stocké sur le client ?

Le fichier contient directement le mot de passe en clair. En 600 il n'y a que root qui peut lire le fichier. Si on ne veut pas de mot de passe en clair, on utilise Kerberos.

Partie E

Q18. Recopiez votre ligne de `/etc/exports` puis la sortie de `sudo exportfs -v`. Citez deux options que vous n'avez pas écrites et qui apparaissent pourtant : d'où viennent-elles ?

```
/srv/nfs/partage 192.168.100.0/24(rw,sync,no_subtree_check,root_squash)

sio@srv-linux:~$ sudo exportfs -v
/srv/nfs/partage
192.168.100.0/24(sync,wdelay,hide,no_subtree_check,sec=sys,rw,secure,
root_squash,no_all_squash)
```

Je n'ai pas écrit `wdelay` ni `sec=sys`. Ce sont des valeurs par défaut.

Q19. Que se passe-t-il si l'on modifie `/etc/exports` sans exécuter `exportfs -ra` ? Quel message obtient le client ?

Si on le modifie, le serveur garde l'ancienne table et le client obtient access denied by server while mounting.

Q20. À qui appartient fichier-de-david.txt vu depuis cli-linux, en nom (ls -l) puis en numéro (ls -ln) ? Expliquez le résultat et proposez deux corrections durables.

```
sio@cli-linux:/mnt/nfs$ ls -l /mnt/nfs/
-rw-r--r-- 1 1601 david 0 10 sept. 09:26 fichier-de-david.txt
sio@cli-linux:/mnt/nfs$ ls -ln /mnt/nfs/
-rw-r--r-- 1 1601 1601 0 10 sept. 09:26 fichier-de-david.txt
```

fichier-de-david appartient à 1601, en nom comme en numéro. C'est parce que NFS transporte des numéros et pas des noms. Sur le serveur 1601 c'est david, mais sur le client david est en 1701, donc 1601 ne correspond à personne. On pourrait imposer le même UID sur les deux machines, ou centraliser en LDAP pour que ce soit les mêmes partout.

Q21. À qui appartient fichier-cree-par-root.txt sur le serveur ? Quelle option l'explique ? Que se passerait-il, en termes de sécurité, avec no_root_squash ?

Il appartient à nobody, en numéro 65534, grâce à root_squash. En no_root_squash il resterait root, et il pourrait déposer un binaire SUID root sur le partage pour prendre les droits root sur le serveur.

Q22. Placez-vous dans /mnt/nfs puis tentez sudo umount /mnt/nfs. Quel message obtenez-vous ? Quelle commande identifie le processus fautif, et comment démontez-vous proprement ?

```
sio@cli-linux:/mnt/nfs$ sudo umount /mnt/nfs
umount.nfs4: /mnt/nfs: device is busy
```

Le message est umount.nfs4: /mnt/nfs: device is busy. La commande qui trouve le processus fautif est fuser -vm /mnt/nfs, mais elle n'est pas installée sur ma machine. Le coupable c'était mon propre shell, qui était dans le répertoire. Je suis sorti avec cd / et le démontage est passé.

Partie F

Q23. Combien de démarrages journalctl --list-boots liste-t-il avant puis après votre modification ? Expliquez la différence.

Avant modification j'en avais 8 et après 9. La différence c'est le reboot de plus. Le journal était déjà persistant, on le voit depuis le 7 septembre donc le TP1, donc la modification n'a rien changé en fait.

Q24. Recopiez les directives ajoutées à /etc/systemd/journald.conf. Pourquoi faut-il impérativement associer un plafond de taille à Storage=persistent ?

```
[Journal]
Storage=persistent
SystemMaxUse=500M
```

J'ai décommenté Storage et SystemMaxUse et j'y ai rajouté persistent et 500M. Il faut un plafond parce que le journal persistant ne s'efface plus au démarrage, et sans limite il grossirait jusqu'à remplir la partition.

Q25. Recopiez /etc/rsyslog.d/30-sio.conf. Que fait la ligne & stop ? Comment avez-vous vérifié qu'elle produisait bien l'effet attendu ?

```
local1.* /var/log/sio/application.log
& stop
```

& stop arrête le traitement du message et donc il ne finit pas dans /var/log/syslog. Je l'ai vérifié avec sudo grep -c sauvegarde /var/log/syslog, qui renvoie 0.

Q26. Recopiez les deux fichiers de la centralisation. Quelle est la différence entre @ et @@ dans une destination rsyslog ? Lequel avez-vous choisi et pourquoi ?

Sur srv-linux, /etc/rsyslog.d/10-collecteur.conf :

```
module(load="imudp")
input(type="imudp" port="514")
module(load="imtcp")
input(type="imtcp" port="514")

template(name="DistantFile" type="string"
          string="/var/log/distant/%HOSTNAME%/%PROGRAMNAME%.log")

if $fromhost-ip != '127.0.0.1' then {
    action(type="omfile" dynaFile="DistantFile")
    stop
}
```

Sur cli-linux, /etc/rsyslog.d/90-vers-srv-linux.conf :

```
*.* @@192.168.100.10:514
```

Un @ c'est de l'UDP et @@ c'est du TCP. J'ai pris TCP pour que la livraison soit vérifiée et ne rien perdre en route.

Q27. Donnez le chemin exact du fichier créé sur le collecteur par votre message de test, et expliquez comment ce chemin a été construit.

Le chemin est /var/log/distant/cli-linux/test-centralisation.log. Il vient de mon template DistantFile, qui vaut /var/log/distant/%HOSTNAME%/%PROGRAMNAME%.log. %HOSTNAME% a été remplacé par cli-linux, la machine qui a émis, et %PROGRAMNAME% par test-centralisation, le nom que j'ai donné avec l'option -t de logger.

Partie G

Q28. Recopiez votre fichier de configuration. Listez les fichiers présents dans /var/log/sio/ après la première puis après la seconde rotation, et expliquez l'effet de delaycompress à partir de ce que vous observez.

```
/var/log/sio/*.log {
    daily
    rotate 7
    compress
    delaycompress
    missingok
    notifempty
    create 0640 root adm
    postrotate
        /usr/lib/rsyslog/rsyslog-rotate
    endscript
}
```

Après la première rotation :

```
-rw-r----- 1 root adm  0 10 sept. 14:27 application.log
-rw-r----- 1 root adm 78 10 sept. 14:27 application.log.1
-rw-r----- 1 root adm 126 10 sept. 14:11 application.log.2.gz
```

Après la seconde :

```
-rw-r----- 1 root adm  0 10 sept. 14:28 application.log
-rw-r----- 1 root adm 78 10 sept. 14:28 application.log.1
-rw-r----- 1 root adm 96 10 sept. 14:27 application.log.2.gz
-rw-r----- 1 root adm 126 10 sept. 14:11 application.log.3.gz
```

delaycompress fait que la dernière archive, .1, n'est pas compressée tout de suite. Elle ne devient un .gz qu'à la rotation suivante, quand elle passe en .2. Ça laisse le temps à un programme qui aurait encore le fichier ouvert de finir d'écrire dedans.

Q29. *Le message émis après la première rotation est-il bien arrivé dans le nouveau application.log ? Quelle directive le garantit, et que se passerait-il sans elle ? Par quoi logrotate est-il déclenché sur Debian 12 ?*

Oui, le message est bien arrivé dans le nouveau application.log :

```
2026-09-10T14:27:03.176931+02:00 srv-linux sauvegarde: Message apres rotation
```

C'est le postrotate qui le garantit : il appelle rsyslog-rotate, qui dit à rsyslog de rouvrir ses fichiers. Sans lui, rsyslog continuerait d'écrire dans l'ancien fichier renommé, et le nouveau resterait vide. Sur Debian 12, logrotate n'est pas lancé par cron mais par un timer systemd, logrotate.timer, qui tourne tous les jours à minuit.

Partie H

Q30. *Recopiez /etc/fail2ban/jail.local. Expliquez la différence entre findtime et bantime, et pourquoi backend = systemd est le bon choix sur Debian 12.*

```
[DEFAULT]
backend = systemd
ignoreip = 127.0.0.1/8 ::1

[sshd]
enabled = true
maxretry = 3
bantime = 10m
findtime = 10m
```

findtime c'est la fenêtre pendant laquelle on compte les échecs. Il faut atteindre maxretry échecs dans ces 10 minutes pour être banni. bantime c'est la durée du bannissement une fois qu'il est décidé, 10 minutes aussi. Les deux valent 10m chez moi mais ils ne servent pas à la même chose : l'un compte avant, l'autre punit après.

backend = systemd est le bon choix sur Debian 12 parce que les messages de sshd vont dans le journal systemd. Avec un autre backend, fail2ban irait chercher un fichier de log qui n'existe pas forcément, et il ne compterait aucun échec.

Q31. *Donnez la sortie de fail2ban-client status sshd après les échecs. Combien de tentatives ont été comptées ? Quelle adresse est bannie ? Donnez ensuite la règle correspondante relevée dans le pare-feu.*

```
sio@srv-linux:~$ sudo fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| |- Currently failed: 1
| |- Total failed: 4
| `-- Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM=sshd
`- Actions
  |- Currently banned: 1
  |- Total banned: 1
  `-- Banned IP list: 192.168.100.50
```

4 tentatives ont été comptées (Total failed: 4) et l'adresse bannie est 192.168.100.50, celle de cli-linux. La règle dans le pare-feu :

```
chain f2b-sshd {
    ip saddr 192.168.100.50 counter packets 0 bytes 0 reject
    counter packets 5 bytes 532 return
}
```

```
}
```

Q32. Depuis cli-linux, retentez une connexion SSH pendant le bannissement : quel comportement observez-vous, et en quoi diffère-t-il d'un simple mot de passe refusé ? Reliez ce dispositif au durcissement SSH du jour 2 : que fait fail2ban que le durcissement ne fait pas, et l'inverse ?

```
sio@cli-linux:/$ ssh inexistant@192.168.100.10
ssh: connect to host 192.168.100.10 port 22: Connection refused
```

Le message n'est plus le même. Avant, j'avais Permission denied (publickey) : le serveur répondait et c'est l'authentification qui échouait. Là, c'est la connexion qui est refusée, je n'atteins même plus le service SSH. Le blocage est passé de l'authentification au pare-feu.

Le durcissement du TP1 empêche de rentrer avec un mot de passe, mais il laisse quelqu'un essayer autant de fois qu'il veut. fail2ban ne change rien à la façon dont on s'authentifie, mais il coupe l'accès à celui qui insiste. Les deux se complètent : l'un ferme la porte, l'autre met dehors celui qui frappe trop.

5. Fichiers de configuration

srv-linux : /etc/samba/smb.conf

```
[global]
workgroup = BTSSIO
server string = Serveur de fichiers %h (Samba %v)
netbios name = SRV-LINUX
security = user
map to guest = Never
log file = /var/log/samba/log.%m
max log size = 1000
logging = file
interfaces = lo ens33
bind interfaces only = yes
hosts allow = 127.0.0.1 192.168.100.0/24
hosts deny = 0.0.0.0/0
server min protocol = SMB2
server role = standalone server
passdb backend = tdbsam
unix charset = UTF-8
```

```
[commun]
comment = Espace commun de l'equipe formation
path = /srv/samba/commun
browseable = yes
read only = no
guest ok = no
valid users = @formation
write list = @formation
create mask = 0660
directory mask = 2770
force group = formation
```

```
[perso]
comment = Répertoire personnel de %U
path = /home/%U
browseable = no
read only = no
guest ok = no
valid users = %U
create mask = 0600
directory mask = 0700
```

srv-linux : /etc/exports

```
/srv/nfs/partage 192.168.100.0/24(rw, sync, no_subtree_check, root_squash)
```

srv-linux : /etc/systemd/journald.conf, lignes modifiées

```
[Journal]
Storage=persistent
SystemMaxUse=500M
```

srv-linux : /etc/rsyslog.d/30-sio.conf

```
local1.* /var/log/sio/application.log
& stop
```

srv-linux : /etc/rsyslog.d/10-collecteur.conf

```
module(load="imudp")
input(type="imudp" port="514")
module(load="imtcp")
input(type="imtcp" port="514")

template(name="DistantFile" type="string"
          string="/var/log/distant/%HOSTNAME%/%PROGRAMNAME%.log")

if $fromhost-ip != '127.0.0.1' then {
    action(type="omfile" dynaFile="DistantFile")
    stop
}
```

cli-linux : /etc/rsyslog.d/90-vers-srv-linux.conf

```
*.* @@192.168.100.10:514
```

cli-linux : les deux lignes ajoutées à /etc/fstab

```
//192.168.100.10/commun /mnt/commun cifs credentials=/etc/samba/credentials,uid=1000,
gid=1000,ioccharset=utf8,vers=3.0,_netdev 0 0

192.168.100.10:/srv/nfs/partage /mnt/nfs nfs defaults,_netdev,hard,nofail 0 0
```

cli-linux : /etc/samba/credentials

```
username=alice
password=<non recopié>
domain=BTSSIO
```

Le mot de passe n'est pas recopié ici. Le fichier est en 0600 et appartient à root.

srv-linux : /etc/logrotate.d/sio-application

```
/var/log/sio/*.log {
    daily
    rotate 7
    compress
    delaycompress
    missingok
    notifempty
    create 0640 root adm
    postrotate
        /usr/lib/rsyslog/rsyslog-rotate
```

```
} endsript
```

srv-linux : /etc/fail2ban/jail.local

```
[DEFAULT]
backend = systemd
ignoreip = 127.0.0.1/8 ::1

[sshd]
enabled = true
maxretry = 3
bantime = 10m
findtime = 10m
```

6. Difficultés rencontrées

1. Le partage Samba refusé depuis Windows (0x80070043)

Symptôme : « Windows ne peut pas accéder à \\192.168.100.10\commun », nom de réseau introuvable. Pourtant testparm ne signalait rien.

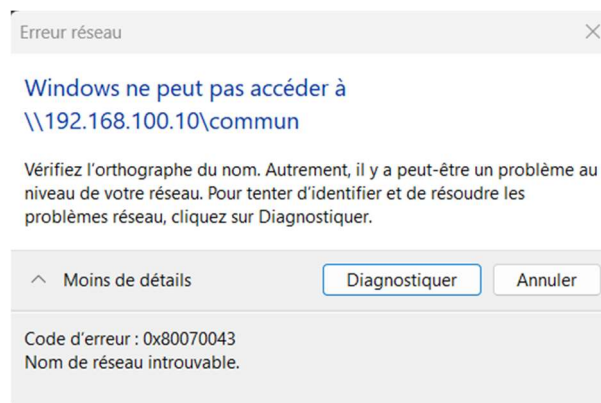


Figure 5 : l'erreur au premier essai

Ce que j'ai vérifié, dans l'ordre :

```
smbclient -L //192.168.100.10 -U alice -> commun est bien la, smb.conf OK
sudo ls -l /var/log/samba/ -> pas de log.192.168.100.1, smbd n'a rien reçu
Test-NetConnection ... -Port 445 -> PingSucceeded True, TcpTestSucceeded False
```

Le ping passe, le port non. C'est donc un pare-feu, et j'en ai posé un au jour 3.

```
chain ufw-user-input {
    # mes regles du TP2
    tcp dport 22 / 80 / 443 / 8080 / 53 / udp 53 / udp 67 accept
}

chain ufw-after-input {
    tcp dport 445 counter packets 15 bytes 780 jump ufw-skip-to-policy-input
}

chain ufw-skip-to-policy-input { counter packets 161 drop }
```

15 paquets comptés sur le 445, puis drop. Mes paquets étaient jetés avant smbd. Normal : au jour 3, Samba n'était pas encore installé. Le ping passait parce que l'ICMP est accepté plus tôt dans la chaîne.

Correction, en limitant au réseau pédagogique :

```
sudo ufw allow from 192.168.100.0/24 to any port 445 proto tcp comment 'Samba SMB'
sudo ufw allow from 192.168.100.0/24 to any port 139 proto tcp comment 'Samba NetBIOS'
```

Même périmètre que mon hosts allow. À retenir : le message de Windows parlait du partage, la cause était dans le pare-feu du serveur. Ce sont les journaux par machine cliente de Samba qui m'ont mis sur la piste.

J'ai eu le même problème en partie E et F. J'ai ouvert 2049 pour NFS, 111 pour showmount et 514 pour rsyslog, toujours restreints à 192.168.100.0/24. J'ai aussi supprimé une vieille règle 20048 ouverte à tout le monde.

2. cli-linux n'a pas d'accès Internet

Symptôme : apt install échoue. Cause : ens32, la carte NAT, est DOWN depuis le TP1, c'était voulu. La route par défaut part vers 192.168.100.1 qui ne mène nulle part.

Manip à refaire à chaque installation :

```
sudo ip link set ens32 up
sudo ip route del default via 192.168.100.1 dev ens33
sudo dhclient ens32
sudo apt install <paquet>
# puis remettre comme avant
sudo ip link set ens32 down
sudo ip route add default via 192.168.100.1 dev ens33
```

Premier essai raté : j'avais ajouté la route NAT en metric 50, mais celle d'ens33 est en metric 0 et gagnait. Il faut supprimer celle d'ens33, pas juste en ajouter une autre.

cifs-utils, nfs-common et rsyslog n'étaient installés ni sur cli-linux ni, pour rsyslog, sur srv-linux.

3. Ligne de fstab tapée dans le terminal

J'ai collé la ligne de montage dans le shell au lieu du fichier. Résultat : rien dans fstab, mount -a ne monte rien, /mnt/commun reste un dossier local à root, et le touch est refusé. Vérification à faire à chaque fois : tail -3 /etc/fstab avant mount -a.

4. Commandes introuvables et droits de lecture

```
showmount / fuser -> dans /usr/sbin, absent du PATH utilisateur, utiliser sudo
ls /var/log/sio/ -> dossier en 0750 root:adm, utiliser sudo
journalctl -> sio n'est pas dans le groupe adm, sans sudo il ne montre rien
```

5. Erreurs Windows sur les sessions SMB

```
erreur 1219 -> une seule session SMB par serveur. L'Explorateur prenait déjà
la place en alice. Fermer la fenêtre + net use * /delete /y
erreur 1326 -> mot de passe faux. Version Windows du NT_STATUS_LOGON_FAILURE
```

7. Conclusion

Tout ce qui était demandé fonctionne. Le partage commun est accessible depuis Windows et depuis cli-linux, avec les bons droits et les bons refus. L'export NFS est monté en permanence. Les journaux sont persistants, le journal applicatif tourne, la centralisation reçoit bien les messages de cli-linux, et fail2ban bannit puis débannit.

Ce que je retiens surtout, c'est le double système de droits. Un accès qui marche en local peut être refusé par Samba, et l'inverse aussi. Quand ça ne passe pas, la bonne réaction c'est de tester avec sudo -u depuis le serveur pour savoir de quel côté ça bloque, pas de faire un chmod 777.

Le blocage du pare-feu en partie C m'a pris du temps mais c'est celui qui m'a le plus appris. Le message d'erreur de Windows parlait du nom du partage alors que le problème était trois couches plus bas. Les journaux par machine cliente de Samba m'ont permis de le voir tout de suite : pas de fichier pour mon poste, donc smbd n'avait rien reçu.

Ce qui reste en suspens : le problème d'UID en NFS. Il est constaté mais pas corrigé, je n'ai fait qu'observer ce qui se passe quand les deux machines ne sont pas d'accord. La vraie correction serait un annuaire centralisé, ce qu'on ne fait pas ici.

Les deux VM sont laissées en état pour le jour 5, avec le partage Samba et l'export NFS en place.