

TP de révision : intranet de la comptabilité

1. Environnement

- srv-linux : Debian 12.15, noyau 6.1.0-53, Apache 2.4.68, Samba 4.17.12
 - ens34 (VMnet2) : 192.168.100.10/24, ens33 : NAT en DHCP
 - Poste Windows : 192.168.100.1, SSH depuis PowerShell
 - VM refaite de zéro, instantané « Avant révision » après install des paquets
- ```
sudo apt install -y apache2 samba smbclient curl
systemctl is-active apache2 smbd cron -> active active active
```

### 2. Partie A : comptes et arborescence

```
sudo groupadd compta
sudo useradd -m -s /bin/bash -G compta mlefevre
sudo useradd -m -s /bin/bash -G compta pdurand
sudo useradd -m -s /bin/bash jmartin
printf '%s\n' 'mlefevre:****' 'pdurand:****' 'jmartin:****' | sudo chpasswd
sudo mkdir -p /srv/compta/web /srv/compta/documents /srv/compta/archives /var/log/compta
/opt/compta
sudo chown root:root /srv/compta && sudo chmod 755 /srv/compta
sudo chown root:www-data /srv/compta/web && sudo chmod 750 /srv/compta/web
sudo chown root:compta /srv/compta/documents && sudo chmod 2770 /srv/compta/documents
sudo chown root:root /srv/compta/archives && sudo chmod 700 /srv/compta/archives
sudo chown root:adm /var/log/compta && sudo chmod 750 /var/log/compta
sudo chown root:root /opt/compta && sudo chmod 750 /opt/compta

sio@srv-linux:~$ ls -ld /srv/compta /srv/compta/* /var/log/compta /opt/compta
drwxr-x--- 2 root root 4096 30 sept. 09:37 /opt/compta
drwxr-xr-x 5 root root 4096 30 sept. 09:37 /srv/compta
drwx----- 2 root root 4096 30 sept. 09:37 /srv/compta/archives
drwxrws--- 2 root compta 4096 30 sept. 09:37 /srv/compta/documents
drwxr-x--- 2 root www-data 4096 30 sept. 09:37 /srv/compta/web
drwxr-x--- 2 root adm 4096 30 sept. 09:37 /var/log/compta
sio@srv-linux:~$ sudo -u mlefevre touch /srv/compta/documents/essai-mlefevre.txt
sio@srv-linux:~$ sudo ls -l /srv/compta/documents/
-rw-r--r-- 1 mlefevre compta 0 30 sept. 09:37 essai-mlefevre.txt
sio@srv-linux:~$ sudo -u jmartin touch /srv/compta/documents/essai-jmartin.txt
touch: impossible de faire un touch './essai-jmartin.txt': Permission non accordée
```

Fichier de mlefevre au groupe compta = SGID ok. jmartin refusé = normal.

- 2770 documents : le 2 = SGID, les fichiers créés prennent le groupe compta, tout le service peut les lire
- 750 root:www-data web : Apache lit et traverse par le groupe, pas besoin d'écrire, les autres rien
- 700 archives : les sauvegardes ont tous les documents, root seul

### 3. Partie B : site intranet

```
echo '<h1>Intranet Comptabilite</h1><p>Site du service compta sur srv-linux.</p>' | sudo tee
/srv/compta/web/index.html
sudo chown root:www-data /srv/compta/web/index.html && sudo chmod 640 /srv/compta/web/index.html
sudo sed -i '/^Listen 80$/a Listen 8080' /etc/apache2/ports.conf
grep -n Listen /etc/apache2/ports.conf -> 5:Listen 80 6:Listen 8080
```

Ligne d'écoute dans /etc/apache2/ports.conf, pas dans le vhost.

#### /etc/apache2/sites-available/compta.bts-sio.lan.conf

```
<VirtualHost *:8080>
 ServerName compta.bts-sio.lan
 DocumentRoot /srv/compta/web

 ErrorLog /var/log/compta/error.log
 CustomLog /var/log/compta/access.log combined

 <Directory /srv/compta/web>
 Options -Indexes
 AllowOverride None
 AuthType Basic
 AuthName "Intranet Comptabilite"
 AuthUserFile /etc/apache2/.htpasswd-compta
 <RequireAll>
 Require ip 192.168.100.0/24
 Require valid-user
 </RequireAll>
 </Directory>
</VirtualHost>
```

```

</Directory>
</VirtualHost>

sudo htpasswd -c /etc/apache2/.htpasswd-compta mlefevre (-c que pour le 1er, sinon écrasé)
sudo htpasswd /etc/apache2/.htpasswd-compta pdurang
echo '192.168.100.10 compta.bts-sio.lan' | sudo tee -a /etc/hosts
Windows (PowerShell admin) : Add-Content C:\Windows\System32\drivers\etc\hosts
"192.168.100.10\tcompta.bts-sio.lan"
sudo a2ensite compta.bts-sio.lan.conf
sudo apache2ctl configtest -> Syntax OK
sudo systemctl reload apache2
sudo apache2ctl -S -> *:8080 compta.bts-sio.lan (.../compta.bts-
sio.lan.conf:1)
sudo ss -tulnp | grep apache -> *:8080 et *:80 en LISTEN

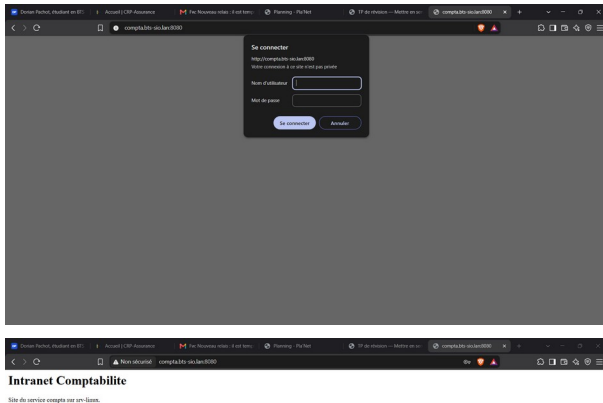
curl -I http://compta.bts-sio.lan:8080/ -> HTTP/1.1 401 Unauthorized
curl -I -u mlefevre http://compta.bts-sio.lan:8080/ -> HTTP/1.1 200 OK
curl -I -u jmartin http://compta.bts-sio.lan:8080/ -> HTTP/1.1 401 Unauthorized

```

- 401 : pas d'identifiant

- 200 : bon réseau + bon compte (les 2 conditions du RequireAll)

- 401 jmartin : existe sous Linux mais pas dans .htpasswd-compta



## 4. Partie C : partage Samba

### /etc/samba/smb.conf (ajouts)

```

[global]
interfaces = lo ens34
bind interfaces only = yes
hosts allow = 127.0.0.1 192.168.100.0/24
server min protocol = SMB2
...
[compta]
comment = Documents du service comptabilite
path = /srv/compta/documents
browseable = yes
read only = no
valid users = @compta
write list = @compta
create mask = 0660
directory mask = 2770

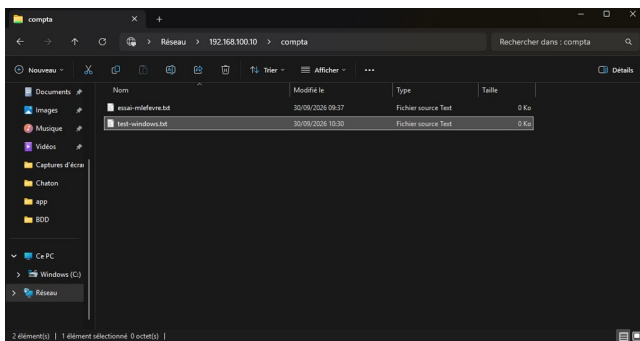
```

@compta = groupe. smbpasswd -a pour mlefevre et pdurang, pas jmartin.

```

testparm -s -> Loaded services file OK.
sudo ss -tlnp | grep smbd -> 192.168.100.10:445/139 et 127.0.0.1, rien sur ens33
sio@srv-linux:~$ smbclient -L //192.168.100.10 -U mlefevre
print$ Disk Printer Drivers
compta Disk Documents du service comptabilite
IPC$ IPC IPC Service (Samba 4.17.12-Debian)
mlefevre Disk Home Directories
SMB1 disabled -- no workgroup available

```



```
sio@srv-linux:~$ sudo ls -l /srv/compta/documents/
-rw-rw---- 1 mlefevre compta 0 30 sept. 10:30 test-windows.txt
sio@srv-linux:~$ sudo smbstatus
1371 mlefevre mlefevre 192.168.100.1 SMB3_11 - partial(AES-128-GMAC)
compta 1371 192.168.100.1 mer. sept. 30 10:30:41 2026 CEST
sio@srv-linux:~$ smbclient //192.168.100.10/compta -U jmartin
tree connect failed: NT_STATUS_ACCESS_DENIED
PS> net use \\192.168.100.10\compta /user:jmartin
Le mot de passe ou nom d'utilisateur n'est pas valide ... L'erreur système 3227320323 s'est produite.
```

Fichier Windows en compta et 660 = SGID + create mask ok. jmartin refusé des deux côtés.

## 5. Partie D : journaux et rotation

```
for i in $(seq 1 12); do curl -s -u 'mlefevre:****' http://compta.bts-sio.lan:8080/ > /dev/null; done
for i in $(seq 1 7); do curl -s -u 'mlefevre:****' http://compta.bts-sio.lan:8080/page-absente > /dev/null; done
for i in $(seq 1 4); do curl -s http://compta.bts-sio.lan:8080/ > /dev/null; done
+ 5 requêtes depuis Windows (curl.exe) pour avoir une 2e IP
```

-u ajouté sur page-absente, sinon 401 et pas 404.

```
sio@srv-linux:~$ sudo cat /var/log/compta/access.log | wc -l
34
sio@srv-linux:~$ sudo awk '{print $9}' /var/log/compta/access.log | sort | uniq -c | sort -rn
19 200
8 404
7 401
sio@srv-linux:~$ sudo awk '{print $1}' /var/log/compta/access.log | sort | uniq -c | sort -rn | head -1
26 192.168.100.10
sio@srv-linux:~$ sudo awk '{print $7}' /var/log/compta/access.log | sort | uniq -c | sort -rn | head -3
26 /
7 /page-absente
1 /favicon.ico
sio@srv-linux:~$ sudo awk '{s+= $10} END {print s " octets"}' /var/log/compta/access.log
14200 octets
```

### /etc/logrotate.d/compta (644 root:root)

```
/var/log/compta/*.log {
 daily
 rotate 7
 compress
 delaycompress
 missingok
 notifempty
 create 640 root adm
 sharedscripts
 postrotate
 systemctl reload apache2 > /dev/null 2>&1 || true
 endscript
}
```

```
sudo logrotate -d /etc/logrotate.d/compta -> log does not need rotating (1re fois, pas d'état)
sudo logrotate -f /etc/logrotate.d/compta
sio@srv-linux:~$ sudo ls -l /var/log/compta/
-rw-r----- 1 root adm 0 30 sept. 10:40 access.log
-rw-r--r-- 1 root root 3709 30 sept. 10:39 access.log.1
-rw-r----- 1 root adm 0 30 sept. 10:40 error.log
-rw-r--r-- 1 root root 138 30 sept. 09:40 error.log.1
```

.1 pas compressés = delaycompress. Nouvelle requête après : access.log passe à 98 octets, Apache écrit bien dans le nouveau.

## 6. Partie E : sauvegarde et supervision

Scripts dans /opt/compta, 750 root:root.

### /opt/compta/sauvegarde.sh

```
#!/bin/bash
=====
Objet : sauvegarde des documents et du site de la compta
Auteur : Dorian Pachot
Date : 30/09/2026
Usage : sudo /opt/compta/sauvegarde.sh (sans argument)
Codes : 0 succès, 1 échec d'archivage, 2 mauvais usage,
3 espace insuffisant
=====
set -euo pipefail

JOURNAL=/var/log/compta/sauvegarde.log
DEST=/srv/compta/archives
SOURCES=(/srv/compta/documents /srv/compta/web)
ARCHIVE="$DEST/compta-$(hostname)-$(date +%Y%m%d-%H%M).tar.gz"
MIN_MO=100
RETENTION=7

journal() {
 echo "$(date '+%Y-%m-%d %H:%M:%S') [$1] $2" >> "$JOURNAL"
}

if ["$#" -ne 0]; then
 echo "Usage : sudo $0 (sans argument)" >&2
 exit 2
fi

if ["$(id -u)" -ne 0]; then
 echo "Erreur : ce script doit etre lance en root (sudo)." >&2
 exit 2
fi

journal INFO "Debut de la sauvegarde"

libre_mo=$(df -m --output=avail "$DEST" | tail -1 | tr -d ' ')
if ["$libre_mo" -lt "$MIN_MO"]; then
 journal ERREUR "Espace insuffisant : ${libre_mo} Mo libres, ${MIN_MO} Mo demandes"
 echo "Erreur : espace insuffisant sur $DEST (${libre_mo} Mo libres)" >&2
 exit 3
fi

if ! tar -czf "$ARCHIVE" "${SOURCES[@]}" 2>> "$JOURNAL"; then
 journal ERREUR "Echec de la creation de $ARCHIVE"
 echo "Erreur : echec de l'archivage" >&2
 exit 1
fi

if ! tar -tzf "$ARCHIVE" > /dev/null 2>&1; then
 journal ERREUR "Archive illisible : $ARCHIVE"
 echo "Erreur : archive illisible" >&2
 exit 1
fi

nb_fichiers=$(tar -tzf "$ARCHIVE" | grep -vc '/$' || true)
taille=$(du -h "$ARCHIVE" | cut -f1)
journal INFO "Archive creee et verifiee : $ARCHIVE ($taille, $nb_fichiers fichiers)"

find "$DEST" -name 'compta-*.tar.gz' -mtime +"$RETENTION" -delete
nb_archives=$(find "$DEST" -name 'compta-*.tar.gz' | wc -l)
journal INFO "Purge faite : $nb_archives archive(s) conservee(s)"

printf '%-22s %s\n' "Archive :" "$ARCHIVE"
printf '%-22s %s\n' "Taille :" "$taille"
printf '%-22s %s\n' "Fichiers :" "$nb_fichiers"
printf '%-22s %s\n' "Archives conservees :" "$nb_archives"

journal INFO "Fin de la sauvegarde (code 0)"
exit 0
```

### /opt/compta/supervision.sh

```
#!/bin/bash
=====
Objet : controle d'etat du serveur de la compta
Auteur : Dorian Pachot
```

```

Date : 30/09/2026
Usage : sudo /opt/compta/supervision.sh [seuil] (80 par default)
Code : nombre d'alertes detectees (0 = tout va bien)
=====
set -euo pipefail

SEUIL=${1:-80}
JOURNAL=/var/log/compta/supervision.log
ARCHIVES=/srv/compta/archives
alertes=0

alerte() {
 echo "$(date '+%Y-%m-%d %H:%M:%S') [ALERTE] $1" >> "$JOURNAL"
 alertes=$((alertes + 1))
}

ligne() {
 printf '%-22s %-10s %s\n' "$1" "$2" "$3"
}

if ! [["$SEUIL" =~ ^[0-9]+$]]; then
 echo "Usage : sudo $0 [seuil en %]" >&2
 exit 255
fi

echo "=== Supervision $(hostname) : $(date '+%Y-%m-%d %H:%M') (seuil ${SEUIL} %) ==="

for fs in / /srv; do
 taux=$(df --output=pcent "$fs" | tail -1 | tr -dc '0-9')
 if ["$taux" -gt "$SEUIL"]; then
 etat="ALERTE"; alerte "Disque $fs rempli a ${taux} % (seuil ${SEUIL} %)"
 else
 etat="OK"
 fi
 ligne "Disque $fs" "${taux} %" "$etat"
done

for svc in apache2 smbd; do
 if systemctl is-active --quiet "$svc"; then
 ligne "Service $svc" "actif" "OK"
 else
 ligne "Service $svc" "arrete" "ALERTE"; alerte "Service $svc arrete"
 fi
done

for port in 8080 445; do
 if [-n "$(ss -tlnH "sport = :$port")"]; then
 ligne "Port $port" "ecoute" "OK"
 else
 ligne "Port $port" "ferme" "ALERTE"; alerte "Port $port pas en ecoute"
 fi
done

nb=$(find "$ARCHIVES" -name 'compta-*.tar.gz' | wc -l)
if ["$nb" -gt 0]; then
 recente=$(find "$ARCHIVES" -name 'compta-*.tar.gz' -printf '%T@ %TY-%Tm-%Td %TH:%TM\n' | sort -n | tail -1 | cut -d' ' -f2-)
else
 recente="aucune"
fi
ligne "Archives" "$nb" "derniere : $recente"

echo "Alertes : $alertes"
exit "$alertes"

sio@srv-linux:~$ sudo /opt/compta/sauvegarde.sh ; echo "code = $"
Archive : /srv/compta/archives/compta-srv-linux-20260930-1047.tar.gz
Taille : 4,0K
Fichiers : 3
Archives conservees : 1
code = 0
sio@srv-linux:~$ sudo /opt/compta/supervision.sh ; echo "code = $"
=== Supervision srv-linux : 2026-09-30 10:47 (seuil 80 %) ===
Disque / 11 % OK
Disque /srv 11 % OK
Service apache2 actif OK
Service smbd actif OK
Port 8080 ecoute OK
Port 445 ecoute OK
Archives 1 derniere : 2026-09-30 10:47
Alertes : 0

```

```

code = 0
apache2 arrêté :
Service apache2 arrete ALERTE
Port 8080 ferme ALERTE
Alertes : 2
code = 2

hors root :
/opt/compta/sauvegarde.sh -> Permission non accordée, code 126 (dossier 750 root)
copie 755 dans /tmp -> Erreur : ce script doit etre lance en root (sudo). code 2

sio@srv-linux:~$ sudo crontab -l
30 2 * * * /opt/compta/sauvegarde.sh >> /var/log/compta/sauvegarde.log 2>&1
*/15 * * * * /opt/compta/supervision.sh >> /var/log/compta/supervision.log 2>&1

```

Sortie dans le journal (>> + 2>&1), sinon cron l'envoie par mail, pas de serveur mail, perdue (vu panne 4).

```

sauvegarde.log :
2026-09-30 10:47:45 [INFO] Debut de la sauvegarde
2026-09-30 10:47:45 [INFO] Archive creee et verifiee : .../compta-srv-linux-20260930-1047.tar.gz
(4,0K, 3 fichiers)
2026-09-30 10:47:45 [INFO] Purge faite : 1 archive(s) conservee(s)
2026-09-30 10:47:45 [INFO] Fin de la sauvegarde (code 0)
supervision.log :
2026-09-30 10:47:55 [ALERTE] Service apache2 arrete
2026-09-30 10:47:55 [ALERTE] Port 8080 pas en ecoute

```

## 7. Partie F : les cinq pannes

N°	Ma prédiction	Symptôme réel	Diagnostic	Cause	Correction
1	401, redemande l'identifiant	403 Forbidden	tail error.log	pas de x pour les autres sur /srv/compta	chmod o+x /srv/compta
2	Syntax OK, marche sur 9090	Syntax OK, connexion refusée	ss -tlnp   grep apache	pas de Listen 9090	remettre *:8080 + reload
3	redemande l'identifiant	« Windows ne peut pas accéder »	systemctl is-active smbd	smbd arrêté	start smbd (+ enable)
4	erreur dans journalctl	rien dans le journal, sortie jetée (No MTA)	journalctl -u cron	chemin relatif + pas de redirection	chemin absolu + >> 2>&1
5	groupe compta	groupe mlefevre, pdurand refusé	ls -l documents	SGID enlevé	chmod g+s + chgrp compta

### Panne 1 : chmod o-x /srv/compta

Ma prédiction : 401, redemande l'identifiant

Réel : 403 Forbidden

```

sudo tail -3 /var/log/compta/error.log
AH00035: access to / denied (filesystem path '/srv/compta/web') because search permissions are
missing on a component of the path

```

Cause : www-data = « autre » sur /srv/compta, sans x il traverse plus pour aller à web. Problème du parent.

Correction : sudo chmod o+x /srv/compta -> 200

Jour : 3 et 4 (Apache, droits)

### Panne 2 : vhost sur 9090

Ma prédiction : Syntax OK, le site marche sur 9090

Réel : Syntax OK mais connexion refusée (curl (7), ERR\_CONNECTION\_REFUSED)

```

sudo ss -tlnp | grep apache -> que *:8080 et *:80
curl -I http://compta.bts-sio.lan:8080/ -> 200, 10701 octets = page par défaut sans mot de passe

```

Cause : pas de Listen 9090. configtest vérifie la syntaxe, pas la cohérence.

Correction : remettre \*:8080, reload -> 200

Jour : 3 (Apache)

### Panne 3 : systemctl stop smbd

Ma prédiction : Windows redemande l'identifiant

Réel : « Windows ne peut pas accéder à \\192.168.100.10\compta », pas d'identifiant demandé

```

systemctl is-active smbd -> inactive
sudo ss -tlnp | grep 445 -> rien

```

Cause : plus rien sur 445, Windows arrive pas à parler au serveur

Correction : `sudo systemctl start smbd`, `systemctl enable smbd` garantit le redémarrage au boot (déjà enabled)

Jour : 4 (Samba)

#### **Panne 4 : chemin relatif dans la crontab, sans redirection**

Ma prédiction : l'erreur va dans `journalctl`

Réel : rien dans `supervision.log`, `journalctl` montre juste que ça a tourné

```
sudo journalctl -u cron
CRON[2336]: (root) CMD (supervision.sh)
CRON[2335]: (CRON) info (No MTA installed, discarding output)
sudo env -i PATH=/usr/bin:/bin sh -c 'supervision.sh' -> sh: 1: supervision.sh: not found, code 127
```

Cause : `PATH` cron = `/usr/bin:/bin`, sortie envoyée par mail, pas de serveur mail, jetée

Correction : chemin absolu + `>>` `journal 2>&1`

Jour : 5 (scripts, cron)

#### **Panne 5 : `chmod g-s /srv/compta/documents`**

Ma prédiction : le fichier appartient à `compta`

Réel : groupe `mlefevre`, `pdurand` peut pas le lire

```
sudo ls -l /srv/compta/documents/
-rw-rw---- 1 mlefevre mlefevre 0 30 sept. 11:12 test-panne5.txt
sudo -u pdurand cat /srv/compta/documents/test-panne5.txt -> Permission non accordée
```

Cause : sans `SGID`, groupe perso du créateur. En prod : plein de fichiers illisibles par les collègues

Correction : `sudo chmod g+s documents` + `chgrp compta` sur le fichier (`g+s` répare que les nouveaux)

Jour : 4 (droits, `SGID`)

### **8. Difficultés**

- SSH : « REMOTE HOST IDENTIFICATION HAS CHANGED » (ancienne VM même IP) -> `ssh-keygen -R`
- `sudo chmod /opt/compta/*.sh` : le `*` est développé par `sio` qui peut pas lire le dossier -> noms en entier
- Panne 4 : réparé avant que `cron` repasse, 2 fois -> test à toutes les minutes avec un `sleep`

### **9. Conclusion**

Tout marche. Fragile : 0 prédiction juste sur 5, surtout auth vs droits fichiers et la sortie de `cron`. Retenu : « Syntax OK » ou « enabled » prouvent rien, il faut tester pour de vrai.