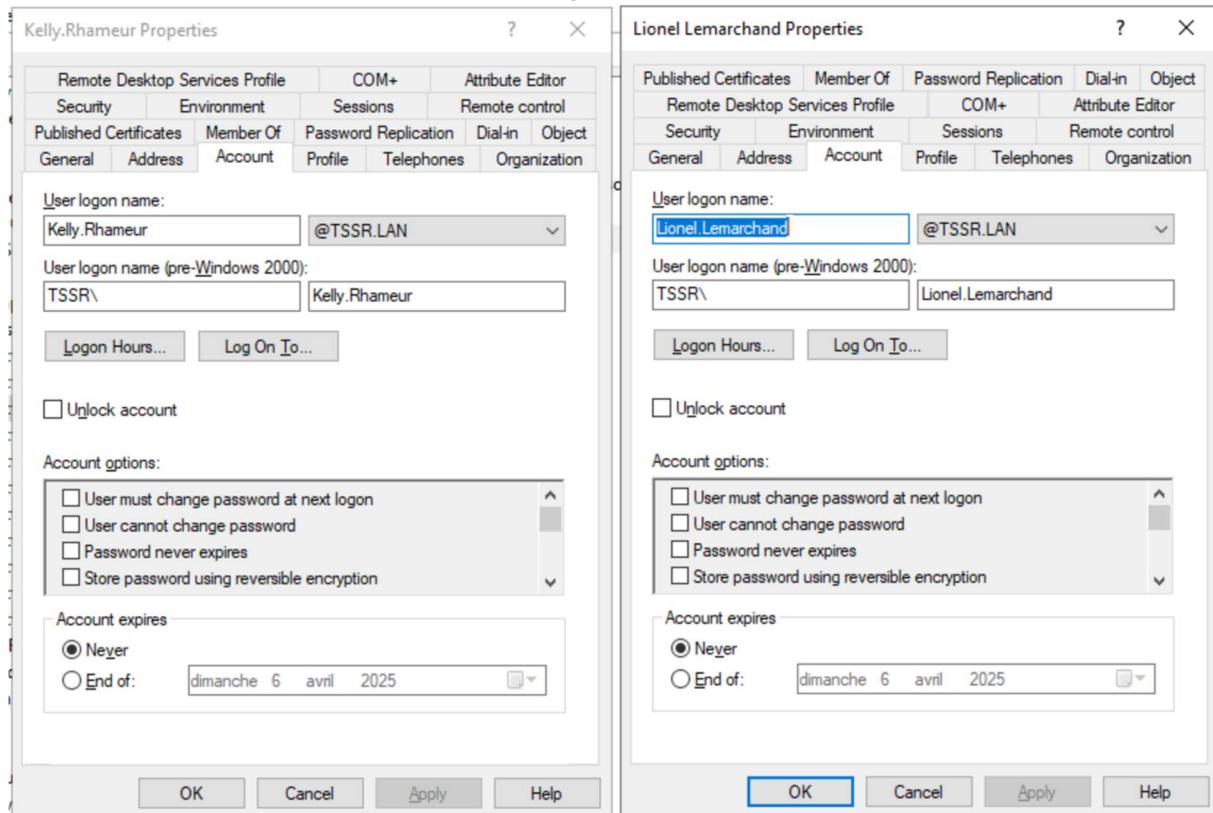


## Exercice 1 - VM Windows

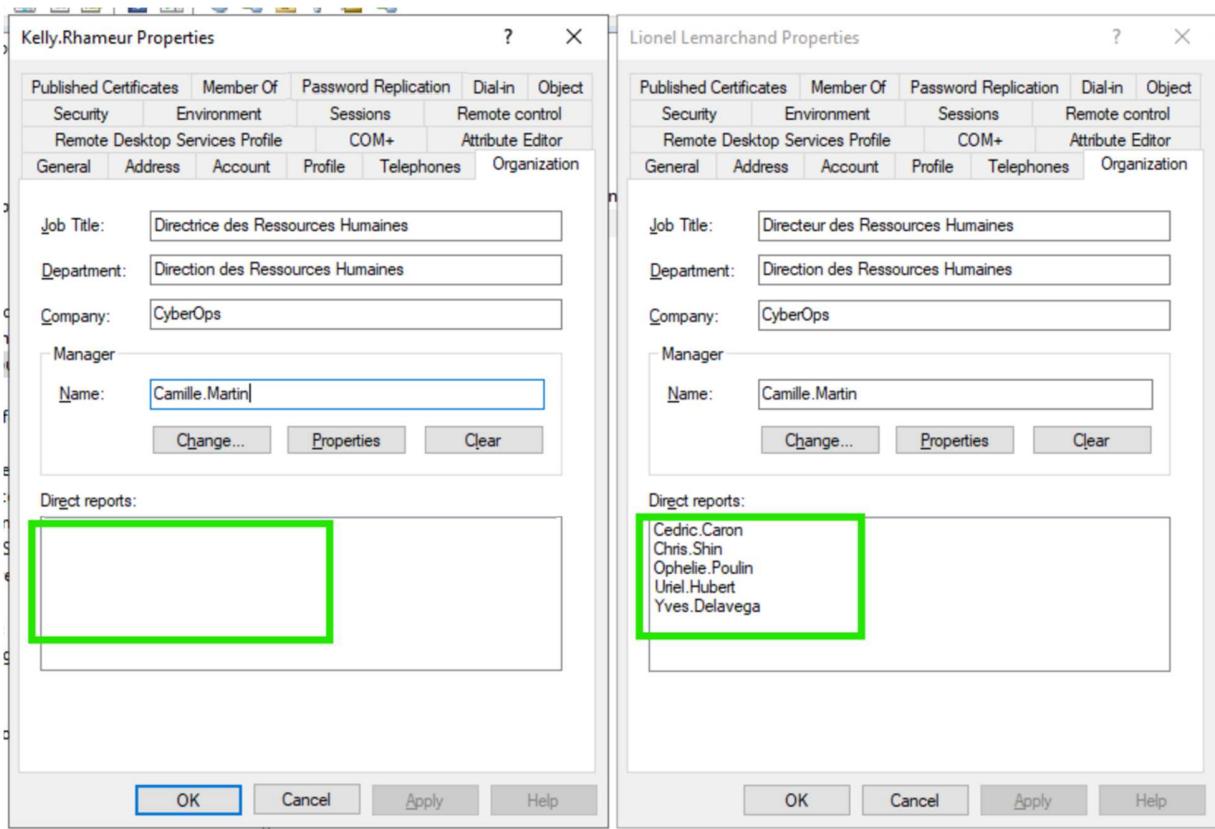
### Partie 1 - Gestion des utilisateurs

#### Q.1.1.1

Pour créer l'utilisateur **Lionel Lemarchand**, j'ai copié la fiche de Kelly Rhameur et j'ai modifié / ajouté les informations nécessaires sur chacun des onglets.



J'ai notamment modifié l'onglet Organization pour rattacher l'équipe de Kelly Rhameur à Lionel Lemarchand, en assignant à chaque collaborateur leur nouveau manager :



### Q.1.1.2

Le compte de Kelly Rhameur est à présent désactivée et déplacé dans l'OU DeactivatedUsers :

The screenshot shows the Windows Active Directory Users and Computers management console. The left navigation pane lists various organizational units (OUs) under the domain TSSR.LAN, with 'DeactivatedUsers' highlighted with a green box. The main pane displays a table of users. One user, 'Kelly.Rhameur', is selected and also highlighted with a green box. The table has columns for 'Name' and 'Type', showing 'Kelly.Rhameur' as a 'User'. The top menu bar includes File, Action, View, Help, and various toolbar icons.

Name	Type
Kelly.Rhameur	User

### Q.1.1.3

Pour modifier le groupe de l'OU dans laquelle était Kelly Rhameur, on clique droit sur le groupe GrpUsersDirectionDesRessourcesHumaines, et dans l'onglet Members on supprime le compte de Kelly Rhameur :

Formation  
GestionDesPerformances  
**GrpUsersDirectionDesRessourcesHumaines**  
Lionel.Lemarchand  
Recrutement  
SanteEtSecuriteAuTravail

Organizational Unit  
Organizational Unit  
Security Group - Global  
User

GrpUsersDirectionDesRessourcesHumaines Properties

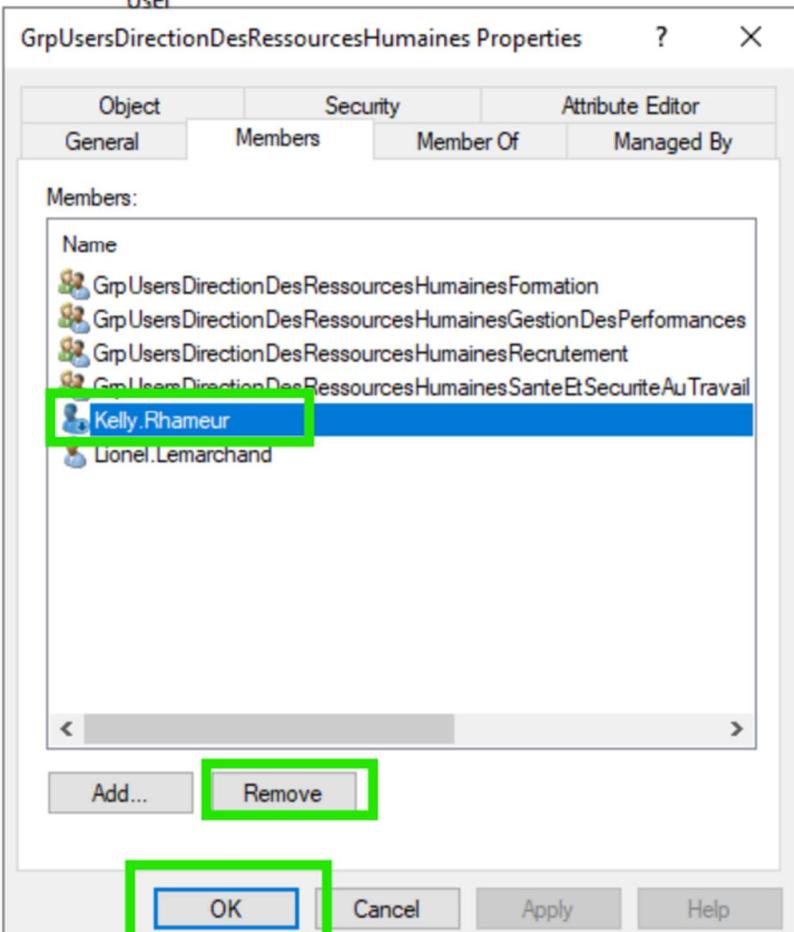
Object	Security	Attribute Editor
General	Members	Member Of
		Managed By

Members:

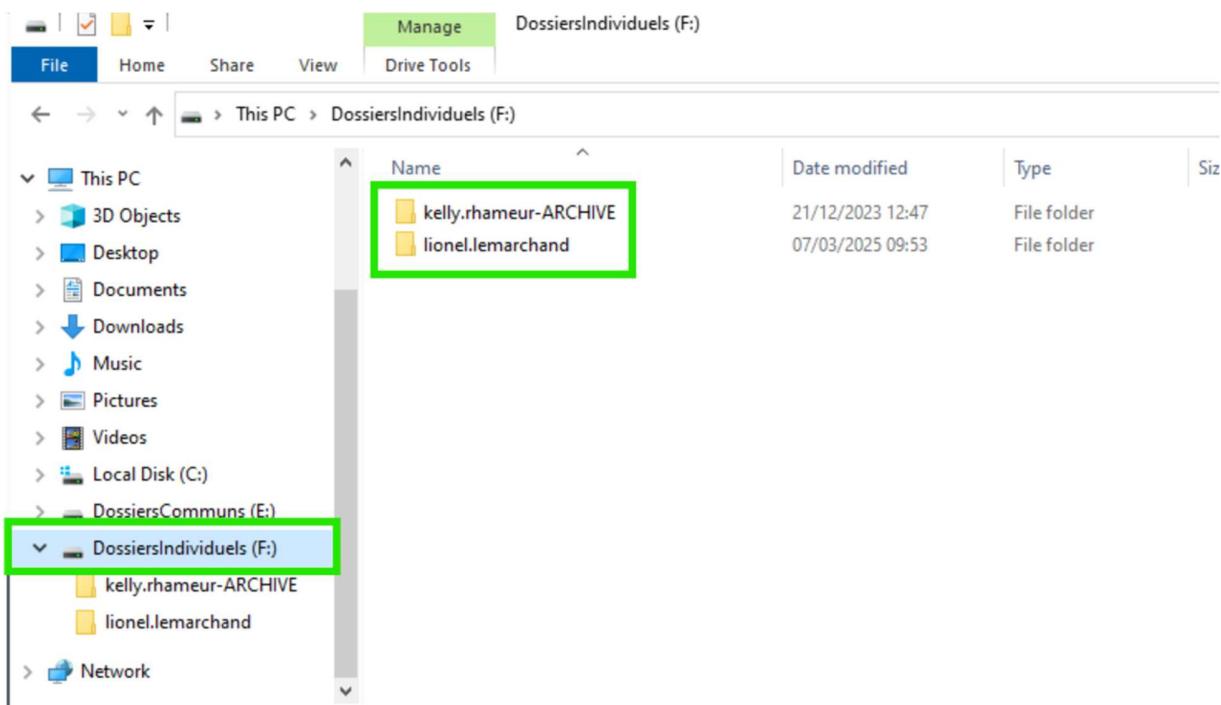
Name
GrpUsersDirectionDesRessourcesHumainesFormation
GrpUsersDirectionDesRessourcesHumainesGestionDesPerformances
GrpUsersDirectionDesRessourcesHumainesRecrutement
GrpUsersDirectionDesRessourcesHumainesSanteEtSecuriteAuTravail
<b>Kelly.Rhameur</b>
Lionel.Lemarchand

Add... Remove

OK Cancel Apply Help

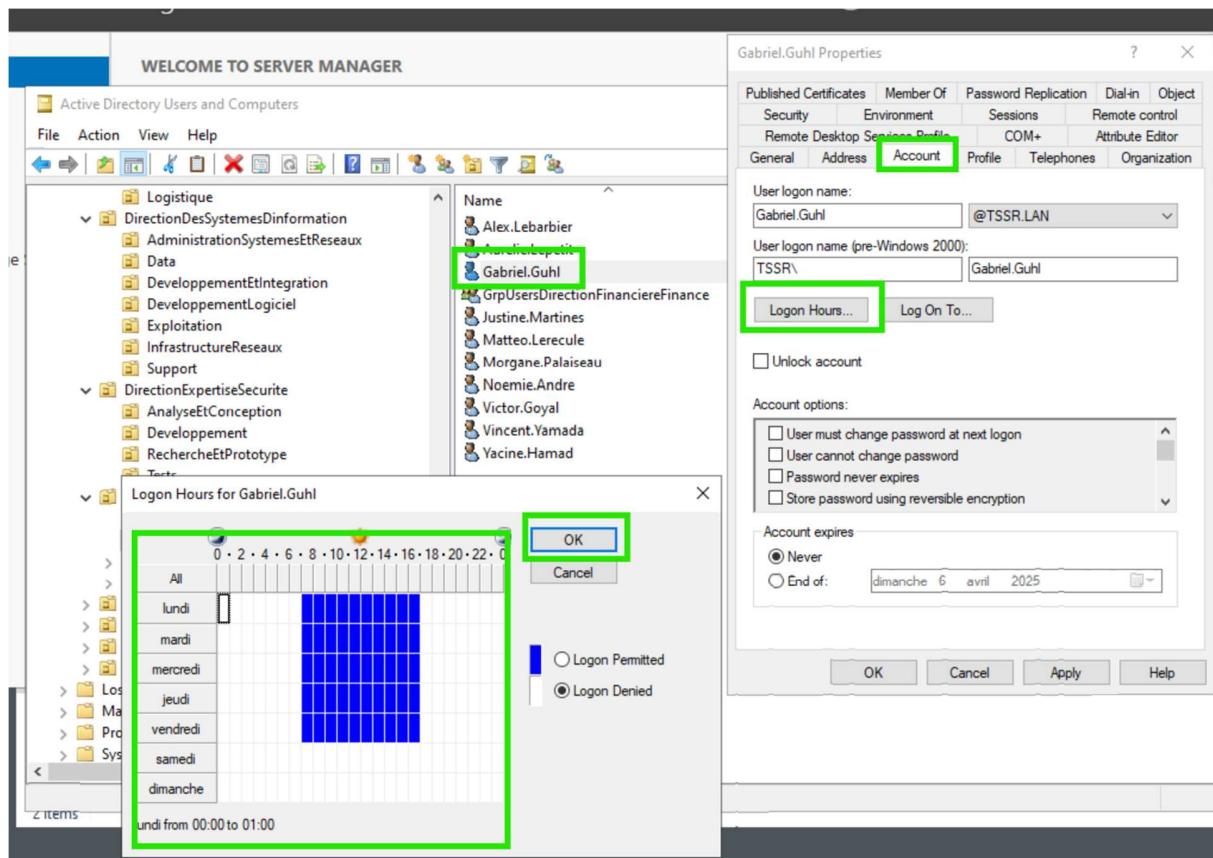


#### Q.1.1.4

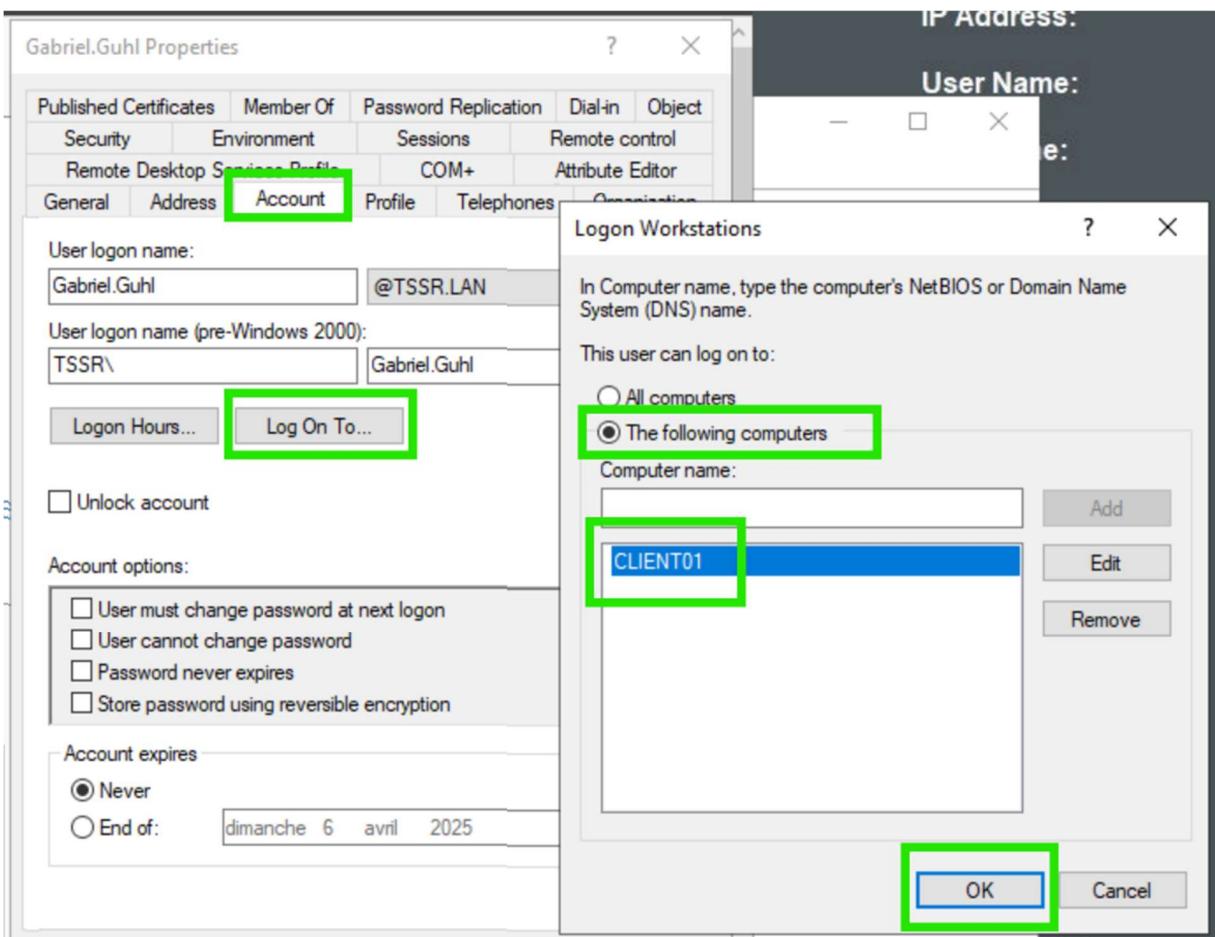


#### Partie 2 - Restriction utilisateurs

##### Q.1.2.1



### Q.1.2.2



### Q.1.2.3

Mise en place d'une stratégie de mot de passe pour LabUsers

Nous allons utiliser une Stratégie de Groupe (GPO). Voici les différentes étapes :

- Ouvrir le Gestionnaire de stratégies de groupe
- Aller dans Forest > Domains > TSSR.lan
- Cliquer droit sur Group Policy Objects > New
  - o Nom de la GPO : durcissement\_mdp\_labusers > OK
  - o Cliquer droit sur durcissement\_mdp\_labusers > Edit
- Aller dans Computer Configuration > Policies > Windows Settings > Security Settings > Account Policies > Password Policy
- Définir par exemple :
  - o Longueur minimale : 12 caractères
  - o Complexité requise : Activé
  - o Historique des mots de passe : 5 anciens mots
  - o Expiration : 30 jours
  - o Blocage après échecs : 5 tentatives

Policy	Setting
Enforce password history	5 passwords remembered
Maximum password age	30 days
Minimum password age	29 days
Minimum password length	12 characters
Minimum password length audit	Not Defined
Password must meet complexity requirements	Enabled
Relax minimum password length limits	Not Defined
Store passwords using reversible encryption	Not Defined

Pour appliquer la GPO à LabUsers :

- Cliquer droit sur sur l'OU LabUsers > Link an Existing GPO > Sélectionner durissement\_mdp\_labusers
- Terminer en ouvrant l'invite de commande et en tapant gpupdate /force, ce qui permet de mettre à jour les stratégies de l'AD

Location	Enforced	Link Enabled
LabUsers	No	Yes

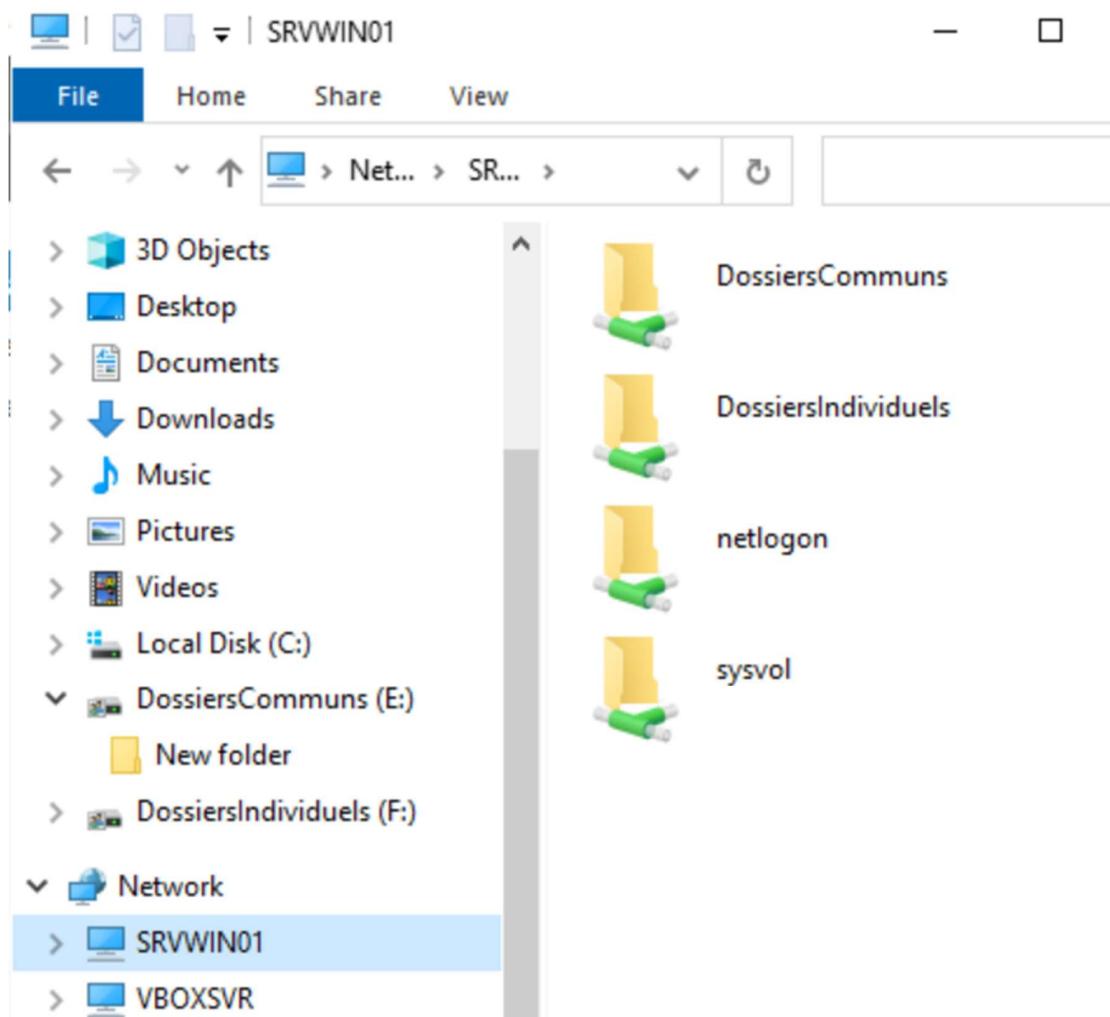
## Partie 3 - Lecteurs réseaux

Création d'une GPO "Drive-Mount" pour monter les lecteurs E: et F sur les clients

Voici les étapes :

### 1) Partager les lecteurs E: et F: sur le réseau

- Cliquer droit sur le lecteur E: > Properties
- Onglet Sharing > Advanced Sharing
- Cocher Share this folder et donner les permissions d'accès en cliquant sur Permissions
- Nommer le partage DossiersCommuns
- Valider > OK
- Faire pareil sur F: (nommer le partage DossiersIndividuels)

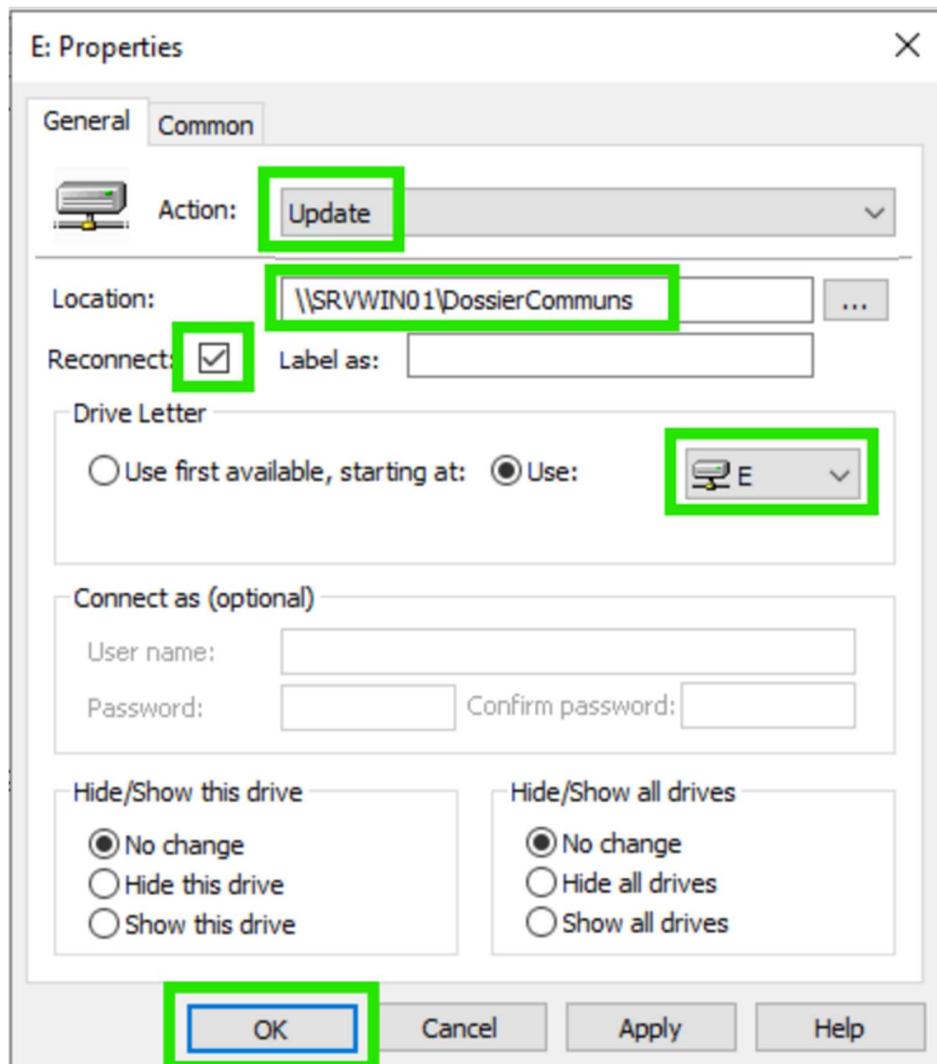


### 2) Créer la GPO

- Ouvrir le Gestionnaire de stratégies de groupe
- Aller dans Forest > Domains > TSSR.lan
- Cliquer droit sur Groupe Policy Object > "New"
  - o Nom de la GPO : Drive-Mount > OK
  - o Cliquer droit sur "Drive-Mount" > Edit

3) Ajouter des lecteurs réseau

- Aller vers : User Configuration > Preferences > Windows Settings > Drive Maps
- Cliquer droit sur la partie droite : New > Mapped Drive
  - o Action : Créer
  - o Emplacement : \\SRVWIN01\DossiersCommuns
  - o Reconnect : Oui
  - o Lettre du lecteur : E
  - o Valider avec OK



Répéter pour le lecteur F :

- a. Action : Créer
- b. Emplacement : \\SRVWIN01\DossiersIndividuels
- c. Reconnect : Oui
- d. Lettre du lecteur : F
- e. Valider avec OK

Drive Maps					
Name	Order	Action	Path	Reconnect	
E:	1	Create	\SRVWIN01\Communs	Yes	
F:	2	Create	\SRVWIN01\Individuels	Yes	

Fermer l'éditeur de GPO

#### 4) Lier la GPO aux PC client

- Retourner dans Group Policy Management
- Pour appliquer la GPO aux PC du domaine, cliquer droit sur l'OU LabComputers > Link an Existing GPO > Sélectionner Drive-Mount > OK
- Terminer en ouvrant l'invite de commande et en tapant gpupdate /force, ce qui permet de mettre à jour les stratégies de l'AD

#### Q.1.3.1

Exercice 2 - VM Linux

Partie 1 - Gestion des utilisateurs

#### Q.2.1.1

```
root@SRVLX01:~# useradd -m -s /bin/bash philippe
root@SRVLX01:~# passwd philippe
Nouveau mot de passe :
Retapez le nouveau mot de passe :
passwd: password updated successfully
```

#### Q.2.1.2

Comme préconisations, je propose :

- d'appliquer le principe de moindre privilège avec un droit d'accès minimum étant donné que ce compte est utilisé pour un usage personnel
- d'utiliser un mot de passe fort et le changer régulièrement
- d'utiliser des clés SSH plutôt que des mots de passe

Partie 2 - Configuration de SSH

#### Q.2.2.1

```
GNU nano 5.4          /etc/ssh/sshd_config *
#PermitRootLogin prohibit-password

# Désactiver l'accès root
PermitRootLogin no
```

# Redémarrer SSH pour appliquer les changements

```
root@SRVLX01:~# systemctl restart ssh
```

#### Q.2.2.2

```
GNU nano 5.4          /etc/ssh/sshd_config *
#      PermitTTY no
#      ForceCommand cvs server

AllowUsers philippe
```

# Redémarrer SSH pour appliquer les changements

```
root@SRVLX01:~# systemctl restart ssh
```

### Q.2.2.3

**A NOTER :** j'ai fait les manip sur le serveur Debian alors qu'il est seul sur le réseau, normalement il faut un client pour établir une connexion SSH.

**# Se connecter en tant que philippe**

**# Générer une paire de clés SSH**

```
philippe@SRVLX01:~$ ssh-keygen -t rsa -b 4096
Generating public/private rsa key pair.
Enter file in which to save the key (/home/philippe/.ssh/id_rsa):
Created directory '/home/philippe/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/philippe/.ssh/id_rsa
Your public key has been saved in /home/philippe/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:IbeQdCBSS4LTNDBkKrvfaGNya1Auok+hFxS1leqRKMc philippe@SRVLX01
The key's randomart image is:
+---[RSA 4096]---+
| =XBo+ o..
| B.o* + o
| ++o . + o
| ==E + o
| +++ S
| ++.o
| =oo
| o+*o
| B=o.
+---[SHA256]---+
```

**# Copier la clé publique dans le fichier authorized\_keys**

```
philippe@SRVLX01:~$ cat ~/.ssh/id_rsa.pub >> ~/.ssh/authorized_keys
```

**# Clé ssh**

```
philippe@SRVLX01:~/ssh$ cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQCVP01W2gkr0PtJYht0Xl4MPmccH8Q0fELnxdk10EM/PYxLrzcJb1KvdSL77mTz277KVKIQmA
CePHd07CgKqRv0TlQAzeoQezFctKTpmVPJSkp2uRnZcCuCsndr7yUVBhZj833Jpc4FEYfGt/BpEHr0QJ2e5ULGt6Lakf93sK38dUVZjS7yV5AQU
tZuWgdPVSLaHevs9Szo5MVsivTEHPz1C26GCtkGXrNPg0IKbENv2xB59Ri100N1/HS/SakrnzJMxBj43NReP01Lb9Y0Lkb4uVMBBP1e3TWgaK5Q
SoS1euSghBil0XLtXb/wy016ZX8xI4fOGFWtc4oNwNEQpWLrkAmwS3U/aEowb3jYm2ehU8RJiXcYNPgxhGAXRSGeXSs97Gu7Nn3N/nWDB0xmD
v+W2KbHDY6tTepnY9u3xZq7PZZf6hbH00CWSil/uPB6YLcuLGd3rfthnWwITl2Z6xF15d/NcS091z0ordodZc9Ng+wXSfEop56bRIwgcc5LILS
OYTSBCK0rb6yazh5EpwNyRXXiwv+JgVJcc9r924WMKMsHAEvAGvS6MYDPfkbyWW5gTe1DyvN3V9pBFbDSIQ0H0sHFYjv1J3UZoPhZnuyYNBx012
w1U0PEGt1Ktty2KTh57rK7AWRolkdaZz4VnDsKEEW8cJEqFqDQgN3r8Q== philippe@SRVLX01
```

**# Désactiver l'authentification par mot de passe**

```
GNU nano 5.4          /etc/ssh/sshd_config *
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication no
#PermitEmptyPasswords no

# Change to yes to enable challenge-response passwords (beware
# some PAM modules don't support it)
ChallengeResponseAuthentication no

# Kerberos options

PubkeyAuthentication yes
```

# Redémarrer SSH pour appliquer les changements

```
root@SRVLX01:~# systemctl restart ssh
```

# Tester la connexion avec la clé SSH

**A NOTER :** je l'ai fait sur le même PC alors que le test se fait normalement depuis une machine distante

```
philippe@SRVLX01:~$ ssh philippe@localhost
The authenticity of host 'localhost (::1)' can't be established.
ECDSA key fingerprint is SHA256:yx0tpERG4YXFu05CbfuIjib/LlJVJlzzNy1vnsm+Fs.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'localhost' (ECDSA) to the list of known hosts.
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 Mar  7 12:27:41 2025 from 192.168.1.27
philippe@SRVLX01:~$
```

## Partie 3 - Analyse du stockage

### Q.2.3.1

```
root@SRVLX01:~# df -h
Sys. de fichiers Taille Utilisé Dispo Uti% Monté sur
udev 470M 0 470M 0% /dev
tmpfs 98M 608K 98M 1% /run
/dev/mapper/cp3--vg-root 2,7G 1,5G 1,1G 60% /
tmpfs 489M 16K 489M 1% /dev/shm
tmpfs 5,0M 0 5,0M 0% /run/lock
/dev/md0p1 471M 49M 398M 11% /boot
tmpfs 98M 0 98M 0% /run/user/1001
```

### Q.2.3.2

```
philippe@SRVLX01:~$ lsblk -f
NAME FSTYPE FSVER LABEL UUID                                     FSAVAIL FSUSE% MOUNTPOINT
sda
└─sda1
  └─md0
    ├─md0p1 ext2   1.0      9bba6d48-3e4b-42a6-bccc-12836de215ec  397,3M  10% /boot
    ├─md0p2
    └─md0p5
      ├─cp3--vg-root ext4   1.0      t1CGJ2-LG5u-kWGc-8ku0-wAiU-icBu-07BEcN
      └─cp3--vg-swap_1 swap   1        bbc31a37-8e49-47fe-8fad-a3fe18919fdd          1G     56% /
sfd0

```

### Q.2.3.3

```
root@SRVLX01:~# lsblk
NAME          MAJ:MIN RM  SIZE RTYPE MOUNTPOINT
sda            8:0    0   8G  disk
└─sda1         8:1    0   8G  part
  └─md0         9:0    0   8G  raid1
    ├─md0p1     259:0  0 488,3M  part  /boot
    ├─md0p2     259:1  0    1K  part
    └─md0p5     259:2  0   7,5G  part
      ├─cp3--vg-root 253:0  0   2,8G  lvm   /
      └─cp3--vg-swap_1 253:1  0  976M  lvm   [SWAP]
sdb            8:16   0   8G  disk
└─sdb1         8:17   0   8G  part
```

```
root@SRVLX01:~# mdadm --manage /dev/md0 --add /dev/sdb1
mdadm: added /dev/sdb1
```

```
root@SRVLX01:~# cat /proc/mdstat
Personalities : [raid1] [linear] [multipath] [raid0] [raid6] [raid5] [raid4] [raid10]
md0 : active raid1 sdb1[2] sda1[0]
      8381440 blocks super 1.2 [2/2] [UU]
```

#### Q.2.3.4

```
root@SRVLX01:~# vgs
  VG #PV #LV #SN Attr   VSize VFree
  cp3-vg  1   2   0 wz--n- 7.51g <3.79g
root@SRVLX01:~# lvcreate -L 2G -n backup_lv cp3-vg
  Logical volume "backup_lv" created.
root@SRVLX01:~# lvs
  LV   VG Attr       LSize  Pool Origin Data%  Meta%  Move Log Cpy%Sync Convert
  backup_lv cp3-vg -wi-a---- 2.00g
  root      cp3-vg -wl-ao--- <2.77g
  swap_1    cp3-vg -wi-ao--- 976.00m
root@SRVLX01:~# mkfs.ext4 /dev/cp3-vg/backup_lv
mke2fs 1.46.2 (28-Feb-2021)
Creating filesystem with 524288 4k blocks and 131072 inodes
Filesystem UUID: fa11033b-d3c5-4883-8791-e2bc0c3f23c3
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

root@SRVLX01:~# blkid /dev/cp3-vg/backup_lv
/dev/cp3-vg/backup_lv: UUID="fa11033b-d3c5-4883-8791-e2bc0c3f23c3" BLOCK_SIZE="4096" TYPE="ext4"
root@SRVLX01:~# mkdir -p /var/lib/bareos/storage
root@SRVLX01:~# mount /dev/cp3-vg/backup_lv /var/lib/bareos/storage
root@SRVLX01:~# df -h
Sys. de fichiers Taille Utilisé Dispo Utile% Monté sur
udev                  470M     0  470M   0% /dev
tmpfs                 98M   620K  98M   1% /run
/dev/mapper/cp3--vg-root 2,7G  1,6G 999M  62% /
tmpfs                 489M   16K 489M   1% /dev/shm
tmpfs                 5,0M     0  5,0M   0% /run/lock
/dev/md0p1              471M   49M 398M  11% /boot
tmpfs                 98M     0  98M   0% /run/user/1001
/dev/mapper/cp3--vg-backup_lv 2,0G   24K  1,8G  1% /var/lib/bareos/storage
root@SRVLX01:~# nano /etc/fstab
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

# Montage permanent du volume logique dans /var/lib/bareos/storage
UUID=fa11033b-d3c5-4883-8791-e2bc0c3f23c3 /var/lib/bareos/storage ext4 defaults 0 2
```

```
root@SRVLX01:~# mount -a
root@SRVLX01:~#
```

#### Q.2.3.5

```
root@SRVLX01:~# vgdisplay cp3-vg
--- Volume group ---
VG Name          cp3-vg
System ID
Format           lvm2
Metadata Areas   1
Metadata Sequence No 4
VG Access        read/write
VG Status         resizable
MAX LV            0
Cur LV            3
Open LV           3
Max PV            0
Cur PV            1
Act PV            1
VG Size          7,51 GiB
PE Size           4,00 MiB
Total PE          1923
Alloc PE / Size  1465 / 5,72 GiB
Free PE / Size   458 / <1,79 GiB
VG UUID          BMardR-vL06-CToa-ad0f-XVh0-0DeS-cX70bt
```

### Partie 4 - Sauvegardes

#### Q.2.4.1

##### 1. Bareos Director (bareos-dir)

Composant principal qui gère les sauvegardes, les restaurations et la planification des tâches.

- Gère la configuration des tâches de sauvegarde, les clients à sauvegarder, etc.
- Communique avec Storage Daemon et File Daemon pour coordonner les sauvegardes et restaurations.
- Stocke les métadonnées des sauvegardes dans une base de données

##### 2. Bareos Storage Daemon (bareos-sd)

Responsable de l'écriture des données de sauvegarde sur le stockage physique

- Reçoit les données du File Daemon et les écrit sur le support de stockage
- Gère les volumes de stockage définis dans la configuration du Director.
- Peut être installé sur un serveur distant

##### 3. Bareos File Daemon (bareos-fd)

Installé sur chaque machine à sauvegarder et agit comme un agent de sauvegarde.

- Fournit les fichiers demandés par le Director lors d'une sauvegarde.
- Reçoit les fichiers du Storage Daemon lors d'une restauration.
- Peut être installé sur des serveurs Linux, Windows ou macOS.

## Partie 5 - Filtrage et analyse réseau

### Q.2.5.1

```
root@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
    }
}
```

### Q.2.5.2

Ce qui est autorisé :

- **ct state established,related accept** : Les paquets faisant partie d'une connexion en cours sont acceptés
- **iifname "lo" accept** : toutes les communications sur l'interface de loopback
- **tcp dport 22 accept** : connexion sur le port 22 (SSH)
- **ip protocol icmp accept** : Ping IPv4
- **ip6 nexthdr ipv6-icmp accept** : Ping IPv6

### Q.2.5.3

Ce qui est interdit :

**ct state invalid drop** : les connexions corrompues

Et tout ce qui n'est pas listé dans les règles autorisées

#### Q.2.5.4

```
GNU nano 5.4          /etc/nftables.conf *
#!/usr/sbin/nft -f

flush ruleset

table inet filter {
    chain input {
        type filter hook input priority 0;

        # Autoriser Bareos sur le réseau local (ports 9101-9103)
        ip saddr 192.168.1.0/24 tcp dport {9101-9103} accept
    }
    chain forward {
        type filter hook forward priority 0;
    }
    chain output {
        type filter hook output priority 0;
    }
}
```

```
root@SRVLX01:~/nftables# nft -f /etc/nftables.conf
root@SRVLX01:~/nftables# nft list ruleset
table inet filter {
    chain input {
        type filter hook input priority filter; policy accept;
        ip saddr 192.168.1.0/24 tcp dport { 9101-9103 } accept
    }

    chain forward {
        type filter hook forward priority filter; policy accept
    ;
    }

    chain output {
        type filter hook output priority filter; policy accept;
    }
}
```

## Partie 6 - Analyse de logs

### Q.2.6.1

# J'ai filtré les logs « Failed password » suite à des connexions échouées sur MobaXterm, avec la commande suivante :

```
grep "Failed password" /var/log/auth.log | tail -n 10
```

```
root@SRVLX01:~# grep "Failed password" /var/log/auth.log | tail -n 10
Mar  7 12:01:24 SRVLX01 sshd[1890]: Failed password for root from 192.168.1.27 port 52989 ssh2
Mar  7 12:26:02 SRVLX01 sshd[2098]: Failed password for invalid user root from 192.168.1.27 port 53294 ssh2
Mar  7 12:26:43 SRVLX01 sshd[2104]: Failed password for invalid user root from 192.168.1.27 port 53304 ssh2
Mar  7 12:27:15 SRVLX01 sshd[2107]: Failed password for invalid user root from 192.168.1.27 port 53305 ssh2
Mar  7 16:16:21 SRVLX01 sshd[1666]: Failed password for philippe from 192.168.1.27 port 65383 ssh2
Mar  7 16:16:26 SRVLX01 sshd[1666]: Failed password for philippe from 192.168.1.27 port 65383 ssh2
Mar  7 16:18:05 SRVLX01 sudo: philippe : user NOT in sudoers ; TTY=tty1 ; PWD=/home/philippe ; USER=root ; C
d password /var/log/auth.log
Mar  7 16:20:07 SRVLX01 sshd[1742]: Failed password for philippe from 192.168.1.27 port 49310 ssh2
Mar  7 16:20:08 SRVLX01 sshd[1742]: Failed password for philippe from 192.168.1.27 port 49310 ssh2
Mar  7 16:20:12 SRVLX01 sshd[1742]: Failed password for philippe from 192.168.1.27 port 49310 ssh2
```