# TP - Mise en place d'un domaine AD sous Debian

## Table des matières



## A) Introduction

Samba est le service de GNU/Linux qui permet d'émuler un contrôleur de domaine NT ou un domaine AD.

Configurer un domaine AD est beaucoup plus complexe qu'un simple domaine NT, et demande déjà de bonnes notions des services NTP, DHCP, DNS, LDAP, PAM, KERBEROS, et bien entendu SAMBA/WINBINDD.

À noter également que le passage « en force » de Windows 10, avec abandon du support de NT1, a grandement compliqué les choses.

On peut ainsi toujours créer des utilisateurs/groupes/partages depuis la console GNU/Linux, via *samba-tool*, mais bon nombre de ces objets ne sont pas « complets », comparés à ceux créés avec une vraie console RSAT, ce qui peut donc poser des problèmes par la suite.

D'autre part, là où un domaine NT se contentait de droits POSIX « basiques », il faut désormais maîtriser en sus les droits étendus via `setfacl`/`getfacl` et `setfattr`/`getfattr`, ce qui augmente la complexité.

Bref, Microsoft a fait ce qu'il fallait pour rendre sa console d'administration indispensable, et se garde bien, pour le moment, d'en produire une version pour OS libre...

L'astuce proposée ici consiste à se créer, en parallèle de la configuration SAMBA sur l'hôte GNU/Linux, une machine virtuelle que l'on configurera sous Windows 10 Pro via KVM, pour ensuite administrer le domaine via la console RSAT classique. On pourra ainsi accéder à la console d'administration depuis n'importe quel poste client.

Bien entendu, on peut aussi choisir de se faciliter la tâche, en dédiant un poste physique sous Windows. La méthode ici étudiée n'est qu'une proposition, intéressante à étudier parce que faisant intervenir la virtualisation KVM dédiée à un VM Windows « lourde ».

Dans la suite, notre contrôleur de domaine se nommera **DC1**, notre domaine sera **MONDOMAINE.LAN** (à modifier avec le nom de votre choix dans les fichiers de configuration, mais ne pas choisir une extension en **.local**, caractéristique des protocoles Zéroconf/Avahi/Bonjour), et la VM Windows contenant les outils RSAT se nommer **VM1**.

# B) Configuration du réseau

Le plus simple pour commencer est de supprimer le gestionnaire de réseau (si installé) :

```
# systemctl stop NetworkManager
# apt-get remove network-manager
```

Nous prévoyons deux réseaux (avec deux cartes réseaux physiques **eth0** et **eth1**) :

➔ WAN : réseau 192.168.0.0/24 avec passerelle en 192.168.0.1 vers l'internet

➔ LAN : réseau 192.168.10.0/24

La configuration WAN sera statique sur **eth0**.

La configuration LAN fera appel à un bridge virtuel **br0**, regroupant une interface virtuelle **tap0** (pour la VM Windows) et notre interface **eth1** de sortie vers le LAN.

```
# cat /etc/network/interfaces
# interfaces(5) file used by ifup(8) and ifdown(8)
# Include files from /etc/network/interfaces.d:
source-directory /etc/network/interfaces.d

auto lo
iface lo inet loopback
```

```
auto eth0
allow-hotplug eth0
iface eth0 inet static
        address 192.168.0.254
        netmask 255.255.255.0
        gateway 192.168.0.1

auto tap0
allow-hotplug tap0
iface tap0 inet manual
        up ip tuntap add tap0 mode tap & ip l set dev tap0 up
        down ip l set dev tap0 down & ip tuntap del tap0

# pour le DHCP et le réseau interne W10
auto eth1
allow-hotplug eth1
iface eth1 inet manual

auto br0
iface br0 inet static
        address 192.168.10.1
        netmask 255.255.255.0
        bridge_ports eth1 tap0
        bridge_waitport 0
        bridge_fd 0
```

Ne pas oublier de relancer le service **networking** et bien entendu, de vérifier la configuration via `ip a` et `ip r`.

# C) Configuration du DHCP

On prévoit tout de suite la configuration pour les clients W10.

Installez le serveur DHCP :

```
# apt install isc-dhcp-server
```

et configurez le fichier */etc/dhcp/dhcpd.conf* avec :

```
default-lease-time 600;
max-lease-time 7200;
ddns-update-style none;
subnet 192.168.10.0 netmask 255.255.255.0 {
  range 192.168.10.100 192.168.10.150;
  option domain-name-servers 192.168.10.1;
  option domain-name "mondomaine.lan";
  option subnet-mask 255.255.255.0;
  option routers 192.168.10.1;
  default-lease-time 600;
  max-lease-time 7200;
}
```

Bien entendu, le **mondomaine.lan** doit être remplacé par le nom que vous aurez choisi.

Relancez le service DHCP :

```
# systemctl restart isc-dhcp-server
```

# D) Préparation de la résolution DNS

Modifiez */etc/resolv.conf* :

```
search mondomaine.lan
nameserver 192.168.10.1
nameserver DNS_EXTERIEUR_DE_VOTRE_CHOIX
```

# E) Modification des fichiers d'hôtes

Rajoutez la machine DC1 en statique, pour éviter de dépendre de la résolution DNS.

```
# cat /etc/hosts:
127.0.0.1       localhost
... (autres DC à IP fixes par exemple)...
192.168.10.1 dc1.mondomaine.lan dc1
```

Modifiez le nom d'hôte en éditant manuellement */etc/hostname* :

```
ad1.mondomaine.lan
```

Le mieux est de relancer la machine pour fixer le changement.

# F) Modification du fichier des variables système

Décommentez la ligne

```
#net.ipv4.ip_forward=1
```

dans */etc/sysctl.conf* pour permettre la translation d'adresse LAN/WAN.

# G) Installation SAMBA de base

Si le paquet samba a déjà été installé par votre distribution, le mieux est de le purger, en vérifiant bien l'absence du fichier */etc/samba/smb.conf*.

Installez les programmes principaux :

```
apt install samba winbindd libpam-winbind libnss-winbind
```

N.B. : Si vous oubliez cette étape, vous risquez de tomber sur un message d'erreur indiquant l'absence du fichier suivant :

```
/usr/share/samba/setup/ad-schema/AD_DS_Attributes__Windows_Server_2012_R2.ldf.
```

Effacez ou sauvegardez */etc/samba/smb.conf*.

Générez le fichier de configuration principal :

```
# samba-tool domain provision --use-rfc2307 -interactive
Realm [MONDOMAINE.LAN]:
Domain [MONDOMAINE]:
Server Role (dc, member, standalone) [dc]:
```

```
DNS backend (SAMBA_INTERNAL, BIND9_FLATFILE, BIND9_DLZ, NONE) [SAMBA_INTERNAL]:
DNS forwarder IP address (write 'none' to disable forwarding) [none]:
IP_DNS_EXTERIEUR_DE_VOTRE_CHOIX
Administrator password:
Retype password:
...
```

Lancez le service :

```
# systemctl start samba-ad-dc.service
```

N.B. : Dans le cas où l'IPV6 serait désactivée au démarrage (option **ipv6.disable=1** du noyau, à placer dans */etc/default/grub*), vous obtiendrez l'erreur suivante :

```
erreur : service_setup_stream_socket(address=::,port=0) for netlogon mgmt failed
- NT_STATUS_INVALID_PARAMETER_MIX
```

Il suffit alors de rajouter les options suivantes dans *smb.conf* :

```
interfaces = 127.0.0.0/8 br0
bind interfaces only = yes
```

et de relancer le service.

# H) Complexité des mots de passe

Cette partie n'est pas obligatoire et relève d'un choix d'administration.

Commencez par regarder les options disponibles :

```
# samba-tool domain passwordsettings show
```

Testez les changements suivants :

```
# samba-tool domain passwordsettings set --complexity=off
# samba-tool domain passwordsettings set --history-length=0
# samba-tool domain passwordsettings set --min-pwd-age=0
# samba-tool domain passwordsettings set --max-pwd-age=0
# samba-tool domain passwordsettings set -min-pwd-length=4
```

et n'hésitez pas à voir les autres options de la commande :

```
# samba-tool domain passwordsettings -h
```

# I) Mise en place de KERBEROS

La gestion des tickets d'autorisation d'accès est centralisée par ce service, via un système de jetons qu'on n'étudiera pas ici.

Installez les paquets nécessaires :

```
apt install krb5-config krb5-user
```

Copiez le fichier */var/lib/samba/private/krb5.conf* dans */etc/*.

Son contenu doit se résumer à :

```
[libdefaults]
        default_realm = MONDOMAINE.LAN
        dns_lookup_realm = false
        dns_lookup_kdc = true
```

et n'oubliez pas de relancer **samba-ad-dc**.

# J) Vérification du DNS

Nous avons ici choisi de laisser la gestion du DNS à SAMBA, ce qui n'est pas toujours une bonne idée dans la pratique, BIND restant de surcroît la référence en la matière.

Cela étant, il s'agit de vérifier que la résolution DNS fonctionne, pour éviter tout problème ultérieur :

```
root@dc1 ~ # dig dc1.mondomaine.lan
...
;; QUESTION SECTION:
;dc1.mondomaine.lan.                IN      A
;; ANSWER SECTION:
dc1.mondomaine.lan.         900     IN      A       192.168.10.1
;; AUTHORITY SECTION:
mondomaine.lan.                 3600      IN         SOA       dc1.mondomaine.lan.
hostmaster.mondomaine.lan. 1 900 600 86400 3600
...
;; Query time: 0 msec
;; SERVER: 192.168.10.1#53(192.168.10.1)
;; WHEN: mar. mars 16 17:34:57 CET 2021
;; MSG SIZE  rcvd: 96

root@dc1 ~ #  dig -t SRV _kerberos._tcp.mondomaine.lan
...
;; QUESTION SECTION:
;_kerberos._tcp.mondomaine.lan.    IN      SRV
;; ANSWER SECTION:
_kerberos._tcp.mondomaine.lan. 900 IN      SRV     0 100 88 dc1.mondomaine.lan.
;; AUTHORITY SECTION:
mondomaine.lan.                 3600      IN         SOA       dc1.mondomaine.lan.
hostmaster.mondomaine.lan. 1 900 600 86400 3600
;; Query time: 0 msec
;; SERVER: 192.168.10.1#53(192.168.10.1)
;; WHEN: mar. mars 16 17:35:03 CET 2021
;; MSG SIZE  rcvd: 115
root@dc1 ~ # dig -t SRV _ldap._tcp.mondomaine.lan
...
;; QUESTION SECTION:
;_ldap._tcp.mondomaine.lan.                IN      SRV
;; ANSWER SECTION:
_ldap._tcp.mondomaine.lan. 900     IN      SRV     0 100 389 dc1.mondomaine.lan.
;; AUTHORITY SECTION:
mondomaine.lan.                 3600      IN         SOA       dc1.mondomaine.lan.
hostmaster.mondomaine.lan. 1 900 600 86400 3600
...
;; Query time: 4 msec
;; SERVER: 192.168.10.1#53(192.168.10.1)
;; WHEN: mar. mars 16 17:35:08 CET 2021
;; MSG SIZE  rcvd: 111
```

```
root@dc1 ~ #  dig www.google.fr
...
;; QUESTION SECTION:
;www.google.fr.                 IN      A
;; ANSWER SECTION:
www.google.fr.          23      IN      A       172.217.19.227
...
;; Query time: 28 msec
;; SERVER: 192.168.10.1#53(192.168.10.1)
;; WHEN: mar. mars 16 17:35:12 CET 2021
;; MSG SIZE  rcvd: 47
```

# K) Configuration de WINBIND

Dans */etc/samba/smb.conf*, rajoutez, dans la section principale, les lignes :

```
template shell = /bin/bash
winbind use default domain = true
winbind offline logon = false
winbind nss info = rfc2307
winbind enum users = yes
winbind enum groups = yes
```

et relancez **samba-ad-dc**.

# L) Configuration de PAM

Attention : les modifications ici sont hyper-sensibles et peuvent planter votre système !

Lancez la commande :

```
# pam-auth-update
```

et activez la création du **$HOME** au login utilisateur.

Dans */etc/nsswitch.conf*, rajoutez l'option **winbind** aux lignes **passwd** et **group** :

```
passwd:         files systemd winbind
group:          files systemd winbind
shadow:         files
gshadow:        files
```

Dans */etc/pam.d/common-password*, virez l'option **try_authtok** (astuce de tecmint) pour que les usagers ne puissent pas changer leur mot de passe depuis la console GNU/Linux (ils doivent passer obligatoirement par AD).

Ainsi la ligne :

```
password          [success=1  default=ignore]         pam_winbind.so  try_authtok
try_first_pass
```

devient :

```
password        [success=1 default=ignore]      pam_winbind.so try_first_pass
```

Contrôlez les groupes :

```
# wbinfo -g
MONDOMAINE\cert publishers
MONDOMAINE\ras and ias servers
MONDOMAINE\allowed rodc password replication group
MONDOMAINE\denied rodc password replication group
MONDOMAINE\dnsadmins
MONDOMAINE\enterprise read-only domain controllers
MONDOMAINE\domain admins
MONDOMAINE\domain users
MONDOMAINE\domain guests
MONDOMAINE\domain computers
MONDOMAINE\domain controllers
MONDOMAINE\schema admins
MONDOMAINE\enterprise admins
MONDOMAINE\group policy creator owners
MONDOMAINE\read-only domain controllers
MONDOMAINE\dnsupdateproxy
```

Contrôlez les usagers :

```
# wbinfo -u
MONDOMAINE\administrator
MONDOMAINE\guest
MONDOMAINE\krbtgt
MONDOMAINE\bob
```

Contrôlez l'usager **bob** (nom théorique, puisqu'il s'agit de votre utilisateur à l'installation)

```
# wbinfo -i bob
MONDOMAINE\bob:*:3000015:100::/home/MONDOMAINE/bob:/bin/bash
```

Normalement, les commandes classiques `getent passwd` et `getent group` doivent vous renvoyer les mêmes éléments. Si ce n'est pas le cas, vous avez sûrement oublié d'installer **libnss-winbind** ou de relancer SAMBA.

# M) La VM Windows (optionnelle)

## 1) Installation

Créez le dossier */kvm* qui contiendra la VM Windows, et le sous-dossier */kvm/iso* qui contiendra les images de base (qu'on aura récupéré sur le web).

```
# mkdir -p /kvm/iso
```

Nous ne passerons pas ici via **virt-manager** : nous allons créer notre VM « à la main », depuis la console, avec le script */kvm/install.w10.sh* suivant :

```
#!/bin/bash

DISK=/kvm/w10.img
WINIMG=/kvm/iso/Win10_XXYY_vZ_French_x64.iso
VIRTIMG=/kvm/iso/virtio-win.iso

kvm \
```

```
-drive file=${DISK},if=virtio,cache=off \
-smp cores=4 \
-m 2048 \
-net nic,model=virtio \
-net user \
-cdrom ${WINIMG} \
-drive file=${VIRTIMG},index=3,media=cdrom \
-rtc base=localtime,clock=host \
-usb \
-device usb-tablet
```

Le fichier *w10.img* est à créer en format **RAW** avec :

```
# qemu-img create -f raw w10.img 100g
```

NE PAS UTILISER LE FORMAT DYNAMIQUE **QCOW2** ! (évite les ralentissements)

Il faut donc ici choisir une taille définitive, en sachant que W10 occupe déjà 40 à 50Go avec ses seules mises à jour, là où une distribution GNU/Linux complète (maj + autres logiciels libres) occupe généralement dans les 12Go maxi.

L'image *Win10_XXYY_vZ_French_x64.iso* est à récupérer chez Microsoft.

L'installation de la VM se fera avec les pilotes de paravirtualisation de RedHat/Fedora (virtio-*win.iso*), qui évitent l'émulation via KVM, et accélèrent donc grandement la réactivité de la VM. URL de téléchargement :

```
https://fedorapeople.org/groups/virt/virtio-win/direct-downloads/stable-virtio/
virtio-win.iso
```

Bien entendu, c'est au début de l'installation de Windows en VM qu'il faudra indiquer l'ISO à intégrer, via le CD-ROM virtuel.

Remarquez que nous n'appliquons pas encore ici la configuration réseau, non nécessaire pour l'installation de base.

On considérera dans la suite que cette opération (longue et assez pénible) est terminée, et que votre VM est fonctionnelle et surtout : réactive !

N'hésitez pas à en faire des copies si vous voulez l'utilisez dans d'autres usagers, en gardant à l'esprit que la version est activée pour 90 jours sans licence.

## 2) Lancement de la VM Windows

Créez le script */kvm/start.w10.sh* :

```
#!/bin/bash

DISK=/kvm/w10.img
MAC=52:54:00:12:34:56
TAP=tap0
INTER1="-net nic,macaddr=${MAC},model=e1000 -net tap,ifname=${TAP},script=no"
VNC=192.168.10.1:1
```

```
kvm \
-drive driver=raw,file=${DISK},if=virtio,cache=off \
-smp cores=4 \
-m 2048 \
${INTER1} \
-k fr \
-rtc base=localtime,clock=host \
-usb \
-vnc ${VNC} \
-device usb-tablet \
-net user
```

On aura remarqué l'ajout de **VNC**, qui permet d'accéder à la VM à la fois depuis le poste, mais aussi depuis le réseau LAN. Bien entendu, on peut choisir l'inverse, et attaquer la VM depuis le réseau WAN.

Ce script sera appelé par l'unité systemd *rc-local* qu'il faut activer ou créer.

```
systemctl enable rc-local
```

Contenu de */etc/rc.local* :

```
#!/bin/bash

sleep 3
/kvm/start.w10.sh &

exit 0
```

Ne pas oublier de relancer le service :

```
# systemctl start rc-local
# systemctl status rc-local
```

## 3) Installation des outils RSAT

Depuis la version 1809, il n'y a plus de KB à aller chercher, il faut passer par :

➔ clic droit sur menu logo

➔ Applications et fonctionnalités

➔ Fonctionnalités facultatives

➔ + Ajouter une fonctionnalité

➔ et choisir enfin les fonctionnalités **RSAT** nécessaires

Les deux outils indispensables sont la console **Domaines et approbations Active Directory** et la **console de Gestion des stratégies de groupe**. Le plus simple, une fois les outils **RSAT** installés, est de se créer un raccourci pour ces deux outils sur le bureau.

# N) Mise en place de la configuration générale

Dans la suite, nous choisirons de mettre nos profils et nos partages dans le dossier */home/samba* que l'on laissera en mode **0755** sous **root:root**.

À noter également que notre configuration va automatiquement créer les dossiers utilisateurs POSIX dans le dossier */home/MONDOMAINE/*, lequel sera configuré avec les mêmes droits que précédemment.

Ce qui permet, par exemple, de stocker la messagerie d'un usager dans son *~/Maildir*, via la commande

```
maildirmake /home/MONDOMAINE/NOMUTILISATEUR/Maildir
```

puis d'utiliser un outil comme **getmail** pour récupérer les messages entrant et les stocker dans un ou plusieurs dossiers cibles. On pourra ensuite ajouter un serveur *Postfix* et *IMAPD* local pour se passer complètement d'un serveur *Exchange*, tout en ayant la trace des messages envoyés et reçus.

Cela étant, ces configurations supplémentaires ne seront pas abordées ici. L'idée est juste de se dire qu'on pourra retrouver toutes les possibilités de configuration habituelles pour l'usager sous GNU/Linux.

# O) Mise en place des profils itinérants

Dans /etc/samba/smb.conf, configurez la section suivante :

```
[profiles]
        comment = Profils utilisateurs
        path = /home/samba/profiles
        browseable = no
        read only = no
        force create mode = 0600
        force directory mode = 0700
        csc policy = disable
        store dos attributes = yes
        vfs objects = acl_xattr
        map acl inherit = yes
```

On remarquera que les droits côté stockage sont restreints au seul propriétaire, en **0600** pour les fichiers et **0700** pour les dossiers.

Dans */home/samba*, créez le dossier partagé */home/samba/profiles* en mode **1770** :

```
drwxrwx--T  6 root users 4096 avril 12 14:41 profiles/
```

# P) GPO windows

Le plus simple ici est d'utiliser le menu :

➔ Logo (clic gauche) > Outils d'administration Windows > Gestion des stratégies de groupe (ou *gpmc.msc* pour le domaine, pas *gpedit.msc* en local)

➔ Gestion de stratégies de groupe > Forêt : $REALM > Domaines > $REALM > Clic droit

➔ Créer un objet GPO dans ce domaine, et le lier ici...

➔ Lui donner le nom Profils utilisateurs par exemple

➔ Sur la stratégie de groupe créée : Clic droit > Modifier

➔ Configuration ordinateur > Stratégie > Modèles d'administration > Système > Profils utilisateur > Définir un chemin d'accès de profil itinérant pour tous les utilisateurs ouvrant une session sur cet ordinateur

➔ Activer puis indiquer le chemin :

```
\\DC1\Profiles\%USERNAME%
```

Testez le résultat sous **VM1**, dans une console **administrateur**, via `gpudate /force`.

## 1) Dossier sysvol pour les stratégies de groupe

Dans */etc/samba/smb.conf*, configurez la section suivante :

```
[sysvol]
        path = /home/samba/sysvol
        read only = No
```

Créez le dossier partagé */home/samba/sysvol* :

```
# mkdir /home/samba/sysvol
```

Les droits seront attribués via les deux commandes suivantes :

```
# samba-tool ntacl sysvolreset
# samba-tool ntacl sysvolcheck
```

Si tout s'est bien passé, normalement, vous devez voir les droits suivants :

```
drwxrwx---+ 3 root BUILTIN\administrators 4096 mars  31 22:36 sysvol/
```

Le **+** nous indique qu'il ne faut plus considérer les droits POSIX, mais les droits étendus.

```
# getfacl /home/samba/sysvol/
getfacl : suppression du premier « / » des noms de chemins absolus
# file: home/samba/sysvol/
# owner: root
# group: BUILTIN\\administrators
user::rwx
user:root:rwx
user:BUILTIN\\administrators:rwx
user:NT\040AUTHORITY\\authenticated\040users:r-x
user:BUILTIN\\server\040operators:r-x
user:NT\040AUTHORITY\\system:rwx
group::rwx
group:BUILTIN\\administrators:rwx
group:NT\040AUTHORITY\\authenticated\040users:r-x
```

```
group:BUILTIN\\server\040operators:r-x
group:NT\040AUTHORITY\\system:rwx
mask::rwx
other::---
default:user::rwx
default:user:root:rwx
default:user:BUILTIN\\administrators:rwx
default:user:NT\040AUTHORITY\\authenticated\040users:r-x
default:user:BUILTIN\\server\040operators:r-x
default:user:NT\040AUTHORITY\\system:rwx
default:group::---
default:group:BUILTIN\\administrators:rwx
default:group:NT\040AUTHORITY\\authenticated\040users:r-x
default:group:BUILTIN\\server\040operators:r-x
default:group:NT\040AUTHORITY\\system:rwx
default:mask::rwx
default:other::---
```

Tout ce qui commence par default seront les droits propagés aux dossiers enfants.

Remarquez qu'ici, il n'y a pas d'attributs spéciaux sur le dossier :

```
# getfattr /home/samba/sysvol/
#
```

# Q) Dossier netlogon pour les scripts batch

Ce dossier contient les fichiers **batch** (*.bat*) ou **powershell** (*.ps*) à créer et mettre impérativement au format dos, via la commande `unix2dos` du paquet *dos2unix* (à installer donc).

Exemple de contenu d'un fichier .bat classique pour fixer des noms de lecteurs à des partages réseau :

```
echo on
net use r: /delete
net use r: \\192.168.10.1\compta
net use s: /delete
net use s: \\192.168.10.1\administration
net use u: /delete
net use u: \\192.168.10.1\scanner
"o:\GroupPolicies\infosdujour.bat"
...
```

Changement majeur avec W10 : dans */etc/samba/smb.conf*, on mettait avant l'option :

```
        logon script = %U.bat
```

qui permettait d'indiquer à seven/xp que l'utilisateur **%U** avait un script *.bat* personnel. Malheureusement avec AD et W10, le script utilisateur fait maintenant partie des attributs LDAP du compte respectif, et l'option précédente n'est donc plus prise en compte.

Il faut donc bien penser, lors de la création des utilisateurs via la console **RSAT**, à passer dans l'onglet **Profil**, et à fixer le *Script d'ouverture de session* en **loginutilisateur.bat** (le nom du fichier suffit, pas besoin du chemin réseau).

Ne pas oublier non plus de fixer tout de suite l'email de l'utilisateur dans l'onglet **Général**.

Dans */etc/samba/smb.conf*, configurez la section suivante :

```
[netlogon]
        path = /home/samba/netlogon
        read only = No
```

Dans */home/samba/netlogon*, créez le script *create.sh* :

```
#!/bin/bash

echo touch $1.bat
echo chmod 700 $1.bat
echo chown root:users $1.bat
echo setfacl -m u:MONDOMAINE\\$1:rx $1.bat
```

et rendez-le exécutable avec `chmod +x create.sh`.

Il suffira à l'administrateur d'aller dans ce dossier, et de taper `./create.sh bob` pour avoir les commandes qui lui permettront de créer le fichier BATCH de bob, en fixant les droits nécessaires.

Après la première édition, ne pas oublier de faire un `unix2dos` du fichier *batch*, sinon vous allez au-devant de problèmes...

Si tout s'est bien passé, vous devriez obtenir des droits étendus similaires à ce modèle :

```
# getfacl bob.bat
# file: bob.bat
# owner: root
# group: users
user::rwx
user:MONDOMAINE\\bob:r-x
group::---
mask::r-x
other::---
```

# R) Mis en place des partages réseaux

L'idée ici est d'offrir trois partages :

➔ **un partage personnel** ouvert uniquement à l'utilisateur (et aux administrateurs évidemment)

➔ **un ou plusieurs partages de groupes**

➔ **un partage commun** ouvert à tous, facilitant les échanges du groupe de travail

Ces partages seront propagés de deux façons distinctes :

➔ **en utilisant une GPO** pour le partage utilisateur **P :** et le partage commun **O :**

➔ **en utilisant les scripts .bat** déjà vus dans la partie **netlogon** pour les partages de groupes.

En effet, dans les configurations complexes, il est généralement plus simple et plus rapide de gérer les noms des lecteurs réseau manuellement, en modifiant quelques fichiers texte, que de se farcir des exceptions qui peuvent très vite devenir nombreuses et complexes, via la console RSAT...

Dans */home/samba*, créez le dossier

```
drwxr-xr-x  7 root root 4096 avril 13 16:04 shares/
```

Créez les sous-dossiers suivants

```
# ls -l /home/samba/shares/
total 24
drwxr-xr-x   6 root root  4096 avril  1 14:35 ./
drwxr-xr-x   6 root root  4096 mars  26 16:14 ../
drwxrwx---   7 root users 4096 avril 12 13:30 commun/
drwxr-x---  13 root users 4096 avril 12 11:17 groups/
drwxr-x---  26 root users 4096 avril 12 11:13 users/
```

# S) Mise en place du partage utilisateur (users)

Attention : il ne faut pas utiliser ici le nom `[homes]`, raison pour laquelle nous choisirons donc `[users]` dans la suite...

Dans */etc/samba/smb.conf*, créez la section `[users]` :

```
[users]
        comment = Dossiers personnels
        path = /home/samba/shares/users
        read only = no
        create mask = 0600
        directory mask = 0700
        force create mode = 0600
        force directory mode = 0700
```

Dans le dossier */home/samba/shares/users*, créez le script *create.sh* :

```
#!/bin/bash

echo mkdir $1
echo chmod 700 $1
echo chown MONDOMAINE\\\\$1 $1
echo chgrp users $1
```

et rendez-le exécutable avec `chmod +x create.sh`.

Il suffira donc à l'administrateur d'aller dans ce dossier, et de taper `./create.sh bob` pour avoir les commandes qui lui permettront de créer le dossier personnel de bob, en fixant les droits nécessaires.

Bien entendu, la méthode ici retenue est une simple proposition : chacun trouvera sa manière de faire.

### 1) Liaison avec une GPO windows

On va donc attribuer le partage personnel P : à nos utilisateurs via GPO comme suit :

➔ Logo (clic gauche) > Outils d'administration > Gestion des stratégies de groupe (ou gpmc.msc pour le domaine, pas gpedit.msc en local)

➔ Gestion des stratégies de groupe > Forêt : $REALM > Domaines > $REALM > Clic droit

➔ Créer un objet GPO dans ce domaine, et le lier ici...

➔ Lui donner le nom Partage personnel par exemple

➔ Sur la stratégie de groupe créée : Clic droit > Modifier

➔ Configuration utilisateur > Préférences > Paramètres windows > Mappages de lecteurs

➔ Clic droit > Nouveau > Lecteur mappé

➔ Onglet Général > Action Créer > Emplacement **\\192.168.10.1\users\%LogonUser%**

➔ Cocher Reconnecter > Libeller en tant que : **Personnel**

➔ Sélectionner la lettre pour le lecteur : **P:**

➔ Onglet Commun

➔ Cocher Exécuter dans le contexte de sécurité de l'utilisateur connecté (option de stratégie utilisateur)

➔ Cliquer Ok

## T) Mise en place du partage commun (commun)

Dans */etc/samba/smb.conf*, créez la section [commun] :

```
[commun]
        comment = commun
        path = /home/samba/shares/commun
        read only = no
        browseable = yes
        writable = yes
        guest ok = no
        printable = no
        valid users = @"BUILTIN\Administrators",@"MONDOMAINE\domain users"
        preserve case = yes
        force user = %U
        force group = "MONDOMAINE\domain users"
        create mask = 0660
        directory mask = 0770
```

```
        force create mode = 0660
        force directory mode = 0770
        write list = @"BUILTIN\Administrators",@"MONDOMAINE\domain users"
```

### 1) Liaison avec une GPO windows

L'attribution du partage commun **O :** à nos utilisateurs se fait comme précédemment, avec une GPO que l'on nommera **Partage commun**, qui pointera sur **\\192.168.10.1\commun**.

## U) Mise en place des partages des groupes (groups)

Pour les partages de groupes, on pourrait procéder comme précédemment. Dans ce cas, dans la console **RSAT**, on passerait dans le second onglet, et on choisirait l'option Cibler le groupe affecté par le partage.

Mais comme dit plus haut, le danger dans un groupe de travail, ce sont les exceptions.

Toutes les machines n'auront peut-être pas les mêmes lecteurs libres, et traduire ces exceptions en script *powershell* n'est pas plus simple que de se farcir de simples fichiers *.bat* en console GNU/Linux. Bref, c'est un choix d'administration qui se défend suivant vos usages et vos habitudes.

Il est cependant heureux que les partages de groupe bougent très rarement, pour ne pas dire quasiment jamais, contrairement aux usagers !

Dans notre cas, nous allons juste prendre l'exemple d'un partage **ACCUEIL** destiné à des secrétaires d'accueil :

Dans la console **RSAT**, créer un groupe `grpaccueil`, et ajouter les usagers correspondants. Le fait de commencer par `grp` n'est pas obligatoire, mais vous permettra de distinguer plus facilement vos groupes de vos utilisateurs à l'usage, ce qui devient vite indispensable dans la pratique, quand le nombre d'usagers augmente...

Dans */etc/samba/smb.conf*, créez la section `[accueil]` :

```
[accueil]
        comment = Groupe accueil
        path = /home/samba/shares/groups/accueil
        read only = no
        browseable = no
        writable = yes
        guest ok = no
        printable = no
        valid users = @"BUILTIN\Administrators",@"MONDOMAINE\grpaccueil"
        preserve case = yes
        force user = %U
        force group = "MONDOMAINE\grpaccueil"
        create mask = 0660
        directory mask = 0770
        force create mode = 0660
        force directory mode = 0770
```

```
        write list = @"BUILTIN\Administrators",@"MONDOMAINE\grpaccueil"
```

Dans */home/samba/shares/groups/*, créez le dossier de partage :

```
drwxrwx---+  4 root MONDOMAINE\grpaccueil 4096 avril 12 14:01 accueil/
```

avec les droits étendus suivants :

```
# getfacl /home/samba/shares/groups/accueil/
getfacl : suppression du premier « / » des noms de chemins absolus
# file: home/samba/shares/groups/accueil/
# owner: root
# group: MONDOMAINE\\grpaccueil
user::rwx
group::rwx
other::---
default:user::rwx
default:user:BUILTIN\\administrators:rwx
default:group::rwx
default:group:MONDOMAINE\\grpaccueil:rwx
default:mask::rwx
default:other::---
```

# V) Fichier /etc/samba/smb.conf final

```
# Global parameters
[global]
        dns forwarder = 1.1.1.1
        netbios name = DC1
        realm = MONDOMAINE.LAN
        server role = active directory domain controller
        workgroup = MONDOMAINE
        idmap_ldb:use rfc2307 = yes
        interfaces = 127.0.0.8 br0
        bind interfaces only = yes

        template shell = /bin/bash
        ; template homedir = /home/%D/%U - default
        winbind use default domain = true
        winbind offline logon = false
        winbind nss info = rfc2307
        winbind enum users = yes
        winbind enum groups = yes

        logon script = %U.bat

[sysvol]
        path = /home/samba/sysvol
        read only = No

[netlogon]
        path = /home/samba/netlogon
        read only = No

[profiles]
        comment = Profils utilisateurs
        path = /home/samba/profiles
        browseable = no
        read only = no
        force create mode = 0600
```

```
        force directory mode = 0700
        csc policy = disable
        store dos attributes = yes
        vfs objects = acl_xattr
        map acl inherit = yes

[users]
        comment = Dossiers personnels
        path = /home/samba/shares/users
        read only = no
        create mask = 0600
        directory mask = 0700
        force create mode = 0600
        force directory mode = 0700

[commun]
        comment = commun
        path = /home/samba/shares/commun
        read only = no
        browseable = yes
        writable = yes
        guest ok = no
        printable = no
        valid users = @"BUILTIN\Administrators",@"MONDOMAINE\domain users"
        preserve case = yes
        force user = %U
        force group = "MONDOMAINE\domain users"
        create mask = 0660
        directory mask = 0770
        force create mode = 0660
        force directory mode = 0770
        #writable = no
        write list = @"BUILTIN\Administrators",@"MONDOMAINE\domain users"

[accueil]
        comment = Groupe accueil
        path = /home/samba/shares/groups/accueil
        read only = no
        browseable = no
        writable = yes
        guest ok = no
        printable = no
        valid users = @"BUILTIN\Administrators",@"MONDOMAINE\grpaccueil"
        preserve case = yes
        force user = %U
        force group = "MONDOMAINE\grpaccueil"
        create mask = 0660
        directory mask = 0770
        force create mode = 0660
        force directory mode = 0770
        write list = @"BUILTIN\Administrators",@"MONDOMAINE\grpaccueil"
```

# W) Conclusion

**Pour les organisations qui n'ont pas besoin de profils itinérants**, juste de partages réseaux, **un domaine NT classique reste suffisant**, et largement plus simple à exploiter et à administrer qu'un domaine AD complet, plus orienté vers les grosses entreprises.

Cela étant, **le paquet SAMBA de GNU/Linux gère indifféremment les deux cas de figure**, et permet d'émuler sans problème particulier un contrôleur de domaine primaire.

Dans le cas AD, avec une VM W10 prête à l'emploi, on choisira de préférence une licence **retail** indépendante du matériel. Mais on évitera soigneusement d'utiliser la clé USB fournie par Microsoft, laquelle n'installe toujours que la version 1909(!), et oblige donc à se farcir la mise à jour totale de l'OS, en sus des mises à jour qui sont déjà largement chronophages !

**Concrètement, la clé USB fournie par Microsoft ne sert dont à rien !**

Côté compétences, on ne va pas se mentir : la mise en place d'un domaine AD sous GNU/Linux nécessite des connaissances préalables de tous les autres services et protocoles. Elle est donc plutôt réservée à des administrateurs GNU/Linux déjà confirmés.

Pour le reste, monter un serveur GNU/Linux en RAID1 logiciel avec du matériel grand public via `mdadm` reste moins cher et largement suffisant pour une petite PME/PMI, et il faut bien avouer, avec 20 ans de recul, que le RAID1 logiciel de GNU/Linux affiche une robustesse assez extraordinaire, voire insolente face à la concurrence.

Et si le RAID1 matériel gardera toujours l'avantage d'un échange « à chaud », plus rapide et sans interruptions, l'inconvénient majeur est qu'il dépend bien souvent d'un matériel plus onéreux, lequel ne dépasse pas les 5 ans de garantie dans la pratique, sans parler des contrôleurs qui cryptent les disques, les rendant totalement inutilisables en cas de gros pépin matériel.

Maintenant, quel que soit la solution retenue : toujours prévoir un serveur de BACKUP qui ne fera que stocker les fichiers de l'entreprise en incrémental via `rsync`, et ne sera accessible qu'aux administrateurs via des identifiants particuliers.

À l'heure des *ransomwares*, qui cryptent les disques locaux et partages réseaux, il est en effet plus rapide de rechercher les fichiers récemment modifiés via `find`, d'aller rechercher via `scp` les originaux dans la dernière sauvegarde valide, pour les réintégrer aux partages principaux avec les bons droits.

Comprenez que ceux qui mettent des semaines à retrouver leurs données (quand ils les retrouvent) sont bien souvent ceux qui ont misé sur le tout Windows, **et qui n'ont pas compris que leur serveur de sauvegarde était finalement aussi vulnérable que leur serveur principal**.

Bref, faire du PDC GNU/Linux est peut-être plus compliqué au départ, mais a aussi des avantages certains à l'arrivée.

La seule chose qui est énervante sous OS libre, **c'est de devoir désormais passer par une console RSAT pour administrer son domaine**, si on veut des objets AD complets, là où un contrôleur de type NT se gère entièrement en ligne de commande (utilisateurs, groupes et partages).

Nul doute que l'équipe Samba comblera les attributs manquants aux objets LDAP/AD au fil du temps. Mais en 2020, la situation reste compliquée, et elle l'est uniquement parce que les régulateurs laissent microsoft mettre des bâtons dans les roues de ses concurrents.

Côté GPO, comme on l'a vu dans ce TP, elles sont stockées sur le dossier *sysvol* et propagées normalement sur les postes. Il n'y a donc plus de différences avec un serveur Windows classique.

Quant aux scripts de gestion, GNU/Linux a toujours brillé dans ce domaine, en proposant moults langages et commandes intégrées, relativement faciles d'apprentissage ! On ne pourra donc qu'encourager les administrateurs sous OS libres à créer et s'échanger des scripts de gestion et autres astuces entre eux !