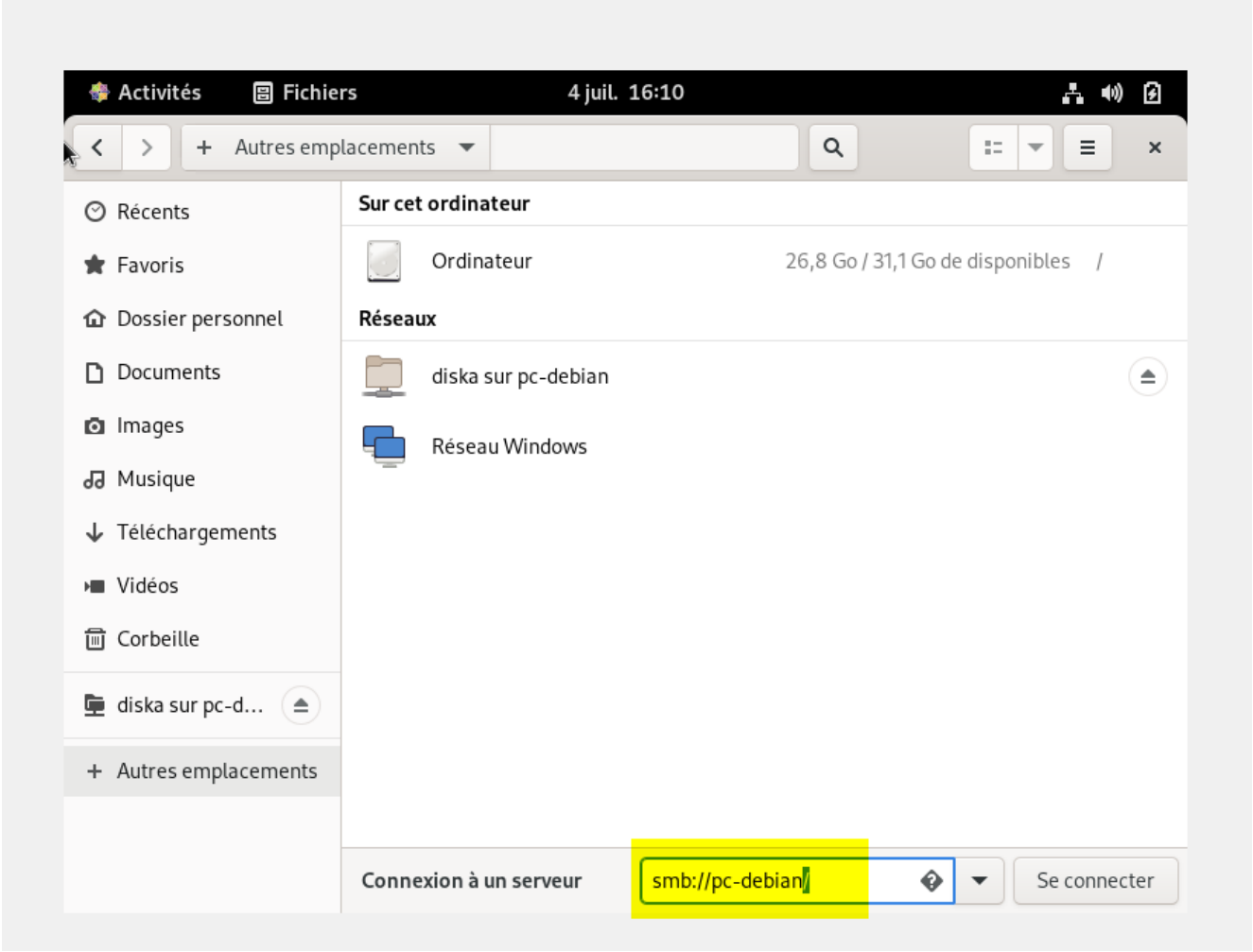
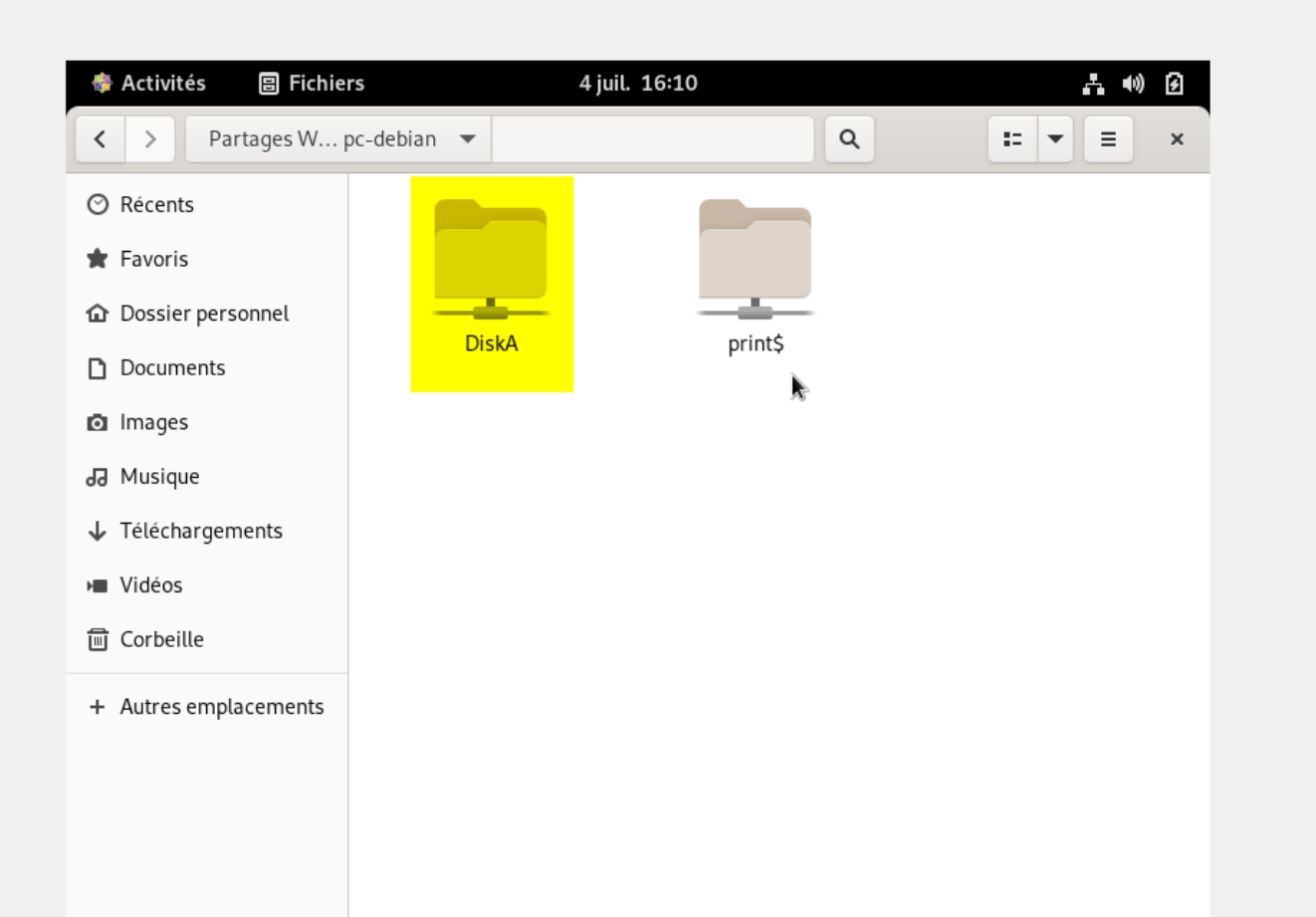
Samba Security User – Tutoriel N°1

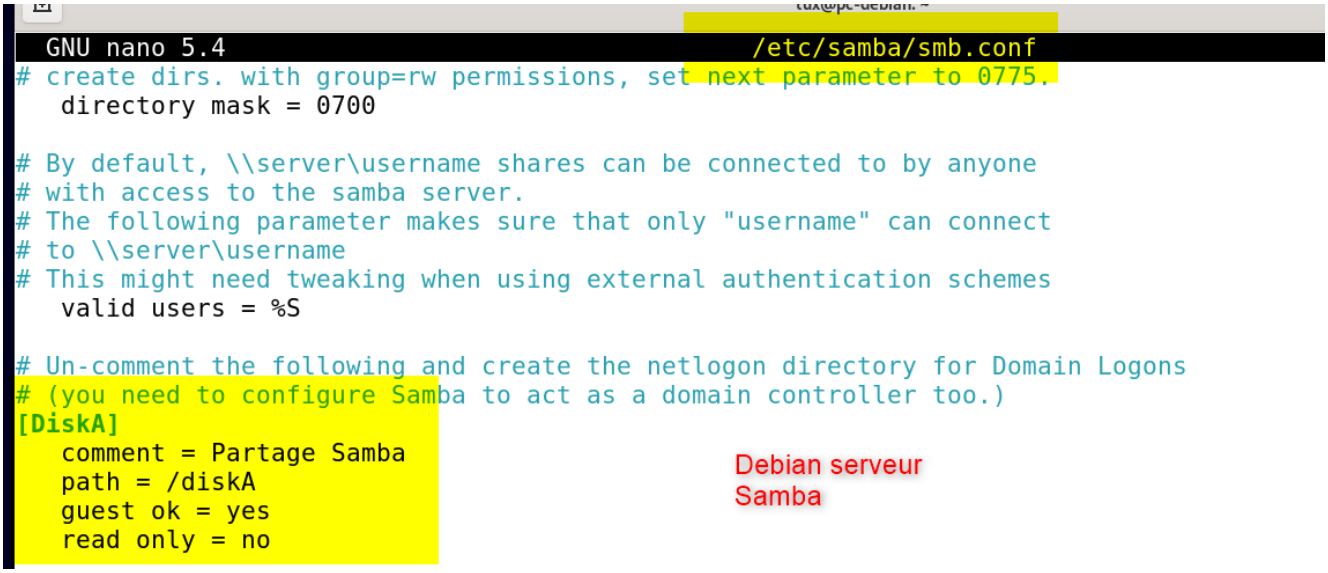
I►Nous allons voir dans cet article comment configurer le serveur Samba en mode security=user et autoriser certains partages (shares).

Le poste Client CentOS !





Le serveur Samba DEBIAN !



Cet article présente avant tout Samba et le potentiel de ses possibilités. Il existe plusieurs modes de sécurité sous samba (l'authentification …) :

1. Security = user *# étudié dans cet article*
   L'accès aux ressources nécessite une authentification

avec des comptes Samba (souvent interconnectés aux comptes Unix)

2. Security = Share
   # L'accès aux ressources peut se faire avec et sans mot de passe, il n' y a pas besoin d comptes Samba. le contrôle se fait par rapport aux partages (Shares Samba)
3. Security = Domain(NT4) ou ADS(Active Directory)
   # Dans ce mode Samba s'intégre dans un domaine NT ou AD est grâce à WinBind est capable d'aller rechercher les comptes utilisateurs existant déjà dans l'annuaire du serveur Microsoft.
4. Security = Server
   # ce mode permet de configurer Samba en tant que Contrôleur de Domaine (PDC) et ne nécessite pas de serveur d'annuaire installés dans un réseau Windows.

Outils :
Commandes utiles :
La commande **smbpasswd** -a tux permet d'ajouter l'utilisateur tux à samba.
La commande **smbstatus** liste tous les utilsateurs connectés à samba.

Lorsqu'on teste l'accès depuis un poste Windows vers le Serveur Samba, on s'authentifie donc et quelquefois ça ne marche pas ! □ ! tout bon Geek le vivra tôt ou tard …
Alors on voudrait parfois réinitialiser la connexion persistante pour cela, on utilisera : **net use * /delete**

On passe dans le vif du sujet ….

Voici le fichier de conf de Samba : /etc/samba/smb;conf Ce fichier est composé de sections :

- [global] : indique les paramètres généraux et les paramètres des différents partages,

- [printers] et [print$] : indique les paramètres de partage de simprimantes
- [homes]: indique le sparamètres spécifiques de l'utilisateur connecté
- [partage] : spécifie des partages particuliers (ex : /tmp ou /data ou /telechargement)

```
[global]
workgroup = NAS_WORKGROUP
#Nom du domaine ou du WorkGroup auquel appartiendra le serveur Samba
netbios name = NAS
#le nom NetBIOS qui présente le serveur sur le réseau \\NAS
# c'est le nom du PC sur le réseau server string = %h – Nas Server – %v
# infos textuelles qui apparaîssent dans le voisinage réseau Windows ( au clic droit par ex.) #%h = hostname – %v = version de samba
dns proxy = no
log file = /var/log/samba/log.%m
max log size = 1000
syslog = 0
panic action = /usr/share/samba/panic-action %d
security = user
encrypt passwords = true
#passdb backend = tdbsam
#Les pass sont alors stockés dans le fichier /var/lib/samba/passdb.tdb (utilisé quand Samba fait office de PDC)
obey pam restrictions = yes
#L'authentification est régie par PAM
unix password sync = yes
#les comptes Samba doivent être associées à des utilisateurs UNIX
passwd program = /usr/bin/passwd %u
passwd chat = *Enter\snew\s*\spassword:* %n\n *Retype\snew\s*\spassword:* %n\n
```

```
*password\supdated\ssuccessfully* .
pam password change = yes
printing = cups
printcap name = cups
socket options = TCP_NODELAY IPTOS_LOWDELAY SO_RCVBUF=8192
SO_SNDBUF=8192
#Si les transferts de données sont très lents, on peut
optimiser les sockets
#hosts deny = all
#host allow = 192.168.0.0/24
# si l'on veut autoriser certaines IP du réseau

[homes]
comment = Repertoire Perso
browseable = no # on ne voit pas la ressource dans le
voisinage réseau … Voir plus loin (secret)
read only = no # ou writable = yes

#masque par défaut, attention ils s'appliquent en addition et
pas en soustraction comme dans les droits fondamentaux Unix
# les utilisateurs auront le droit RW (fichiers) et RWX (rép.)

create mask = 0700
directory mask = 0700
valid users = %S
# %S seul l'utilisateur connecté aura accès à son rép. perso ,
ex: tux aura accès à /home/tux
valid users = %S , bruce
# bruce par contre peut avoir accès à tous les rép. homes!! A
ne pas faire

[printers]
comment = All Printers
browseable = no
path = /var/spool/samba
printable = yes
guest ok = no
read only = yes
```

```
create mask = 0700

[print$]
comment = Printer Drivers
path = /var/lib/samba/printers
browseable = yes
read only = yes
guest ok = no

[Telechargement]
valid users = tux ,  bruce
#définit la iste des utilisateurs ou groupe qui ont le droit d'accéder à cette resource
path=/telechargement/
read only=yes

[Videos]
path=/naspool/films
comment=Films
browsable = yes
read only=yes # ou writable=no

[UpLoad]

path=/naspool/upload
comment=transfert vers serveur
browsable = yes
writable= yes
force group = films
# les fichiers créés prennet l'appprtennace du groupe 
#donne l'appartenance au groupe
#simplifie les droits

[SecretShare]
path=/naspool/secret_share
comment=Secret
browsable = no # si no ->on ne voit pas la ressource, il faut saisir \\NAS\UPLOAD
```

writable= yes

Liste des options %

%U
: session username (the username that the client wanted, not necessarily the same as the one they got).

%G
: primary group name of %U.

%h
: the Internet hostname that Samba is running on.

%m
: the NetBIOS name of the client machine (very useful).This parameter is not available when Samba listens on port 445, as clients no longer send this information. If you use this macro in an include statement on a domain that has a Samba domain controller be sure to set in the [global] section *smb ports = 139*. This will cause Samba to not listen on port 445 and will permit include functionality to function as it did with Samba 2.x.

%L
: the NetBIOS name of the server. This allows you to change your config based on what the client calls you. Your server can have a “dual personality”.

%M
: the Internet name of the client machine.

%R
: the selected protocol level after protocol negotiation. It can be one of CORE, COREPLUS, LANMAN1, LANMAN2 or NT1.

%d
: the process id of the current server process.

%a
: The architecture of the remote machine. It currently recognizes Samba (Samba), the Linux CIFS file system (CIFSFS), OS/2, (OS2), Windows for Workgroups (WfWg), Windows 9x/ME (Win95), Windows NT (WinNT), Windows 2000 (Win2K), Windows XP (WinXP), Windows XP 64-bit(WinXP64), Windows 2003 including 2003R2 (Win2K3), and Windows Vista

(Vista). Anything else will be known as UNKNOWN.

%I
: the IP address of the client machine.

%i
: the local IP address to which a client connected.

%T
: the current date and time.

%D
: name of the domain or workgroup of the current user.

%w
: the winbind separator.

%$(*envvar*)
: the value of the environment variable *envar*.

The following substitutes apply only to some configuration options (only those that are used when a connection has been established):

%S
: the name of the current service, if any.

%P
: the root directory of the current service, if any.

%u
: username of the current service, if any.

%g
: primary group name of %u.

%H
: the home directory of the user given by %u.

%N
: the name of your NIS home directory server. This is obtained from your NIS auto.map entry. If you have not compiled Samba with the *–with-automount* option, this value will be the same as %L.

%p
: the path of the service’s home directory, obtained from your NIS auto.map entry. The NIS auto.map entry is split up as %N:%p.