

Chapitre 12

Samba en tant que contrôleur de domaine

Exercice : Le chapitre suivant constitue un exercice à part entière et peut être effectué en même temps que la lecture du document, qui décrit toutes les étapes à mettre en oeuvre.

I Introduction

Jusqu'à présent, notre serveur Samba est bien seul... Il agit de manière totalement autonome et ne gère aucune authentification pour un groupe de machine. Il ne gère que les accès à ses propres partages. Nous allons voir comment nous pouvons activer cette fonctionnalité et ainsi devenir PDC (contrôleur principal de domaine) ou bien BDC (contrôleur secondaire de domaine).

Plusieurs modifications sont nécessaires : d'abord au niveau de la configuration et des partages, ensuite au niveau des comptes.

II Configuration de Samba en tant que PDC

Pour devenir contrôleur principal de domaine, il faut tout d'abord modifier quelque peu la section globale du fichier de configuration de Samba pour obtenir ceci :

```
[global]

# Identification Netbios
workgroup = mondomaine
netbios name = ubuntu

# Controle de domaine desactive
os level = 65
domain logons = yes
domain master = yes
local master = yes
preferred master = yes
wins support = yes

# Base de donnee de comptes
passdb backend = tdbsam:/var/lib/samba/mypassdb.tdb

# [...] La suite du fichier est identique à celle que nous avons
# précédemment
```

La directive "domain logons = yes" active le contrôle de domaine, c'est à dire la gestion des authentifications sur le domaine. Nous nommons au passage le domaine "mondomaine" grâce à la directive "workgroup".

Les directives "domain master" et "local master" sont un peu particulières. Lorsqu'une machine Windows désire naviguer dans le voisinage réseau, elle a besoin d'une liste de ses machines voisines. La machine qui fait office de "master browser" est là pour lui en fournir une. Il y a deux types de "master browsers", le "domain master browser" et le "local master browser". Ils sont respectivement "master browsers" pour le domaine Windows (qui peut s'étaler sur plusieurs réseaux) et pour le réseau local (qui peut faire partie d'un domaine plus vaste).

Il faut savoir qu'un système d'élections est prévu pour choisir la machine qui sera "master browser". Activer les deux options ci-dessus permet de participer à ces élections. Le résultat des élections dépend du type de système d'exploitation et du rôle de la machine (et d'autres paramètres) sur le réseau. Nous pouvons influencer ce résultat en indiquant "preferred master = yes" et en indiquant un "OS level" au maximum, c'est à dire à 65.

Attention, ne déclarez qu'un seul "preferred master" par réseau sous peine de voir vos serveur Samba se battre pour devenir "master browser" et organiser des élections en continu ! De même, ne déclarez qu'un seul "domain master" par domaine.

L'"OS level" permet également de différencier un PDC d'un BDC. Un OS level à 65 est correct pour un PDC. Pour un BDC, nous choisirons plutôt un OS level plus faible, 40 par exemple. Nous étudierons ceci un peu plus tard.

Enfin, la directive "wins support = yes" permet d'activer un serveur Wins sur la machine Samba. Ce serveur, si l'on configure correctement les clients Windows, permettra de résoudre des noms Netbios, au même titre que le ferait un serveur DNS.

III Les partages spécifiques du contrôleur de domaine

Un contrôleur de domaine digne de ce nom se doit de disposer de certains partages de base :

un partage **[homes]** contenant les répertoires homes des utilisateurs. Le répertoire home de l'utilisateur sera connecté vers un lecteur spécifié lorsque l'utilisateur s'authentifiera sur le domaine. un partage **[netlogon]** contenant les scripts de connexion (netlogon) qui seront téléchargés et exécutés par les machines clientes à la connexion des utilisateurs sur le domaine. un partage **[profiles]** contenant les profils itinérants des utilisateurs. Ces profils permettent de stocker de manière centralisée la configuration du bureau, le fond d'écran, les préférences internet (...) pour chaque utilisateur du domaine.

Chaque compte utilisateur Samba fait référence aux emplacements de ces partages particuliers, nous le verrons par la suite.

Nous devons donc ajouter les partages suivants à notre fichier de configuration :

```
# Partages Homes
[homes]
path = /data/samba/home/%u
comment = Répertoires Homes
valid users = %S
guest ok = no
writeable = yes
create mode = 0700
directory mode = 2700
browsable = no

# Partage Netlogon - lecture seule
[netlogon]
path = /data/samba/netlogon
comment = Partage Netlogon
guest ok = no
read only = yes
browseable = no
valid users = @sambausers

# Partage Profiles
[profiles]
path = /data/samba/profiles
comment = Répertoires Profiles
guest ok = no
writeable = yes
create mode = 0700
browsable = no
valid users = @sambausers
```

Le partage [homes] est un partage virtuel : si l'utilisateur martymac se connecte, le partage [martymac] sera créé automatiquement.

Pour plus de sécurité, nous limitons l'accès au partage uniquement aux personnes ayant un login correspondant au nom du partage ("valid users = %S"), c'est à dire à la personne qui a été elle-même à l'origine de la création du partage. CQFD!

L'étape suivante est de créer les répertoires nouvellement partagés :

```
# mkdir -p /data/samba/home
# mkdir -p /data/samba/netlogon
# mkdir -p /data/samba/profiles
```

Et de leur attribuer les bons droits :

```
# chgrp sambausers /data/samba/home ; chmod 775 /data/samba/home
# chgrp sambausers /data/samba/netlogon ; chmod 555 /data/samba/netlogon
# chgrp sambausers /data/samba/profiles ; chmod 775 /data/samba/profiles
```

Pensez à créer le répertoire home de l'utilisateur martymac :

```
# mkdir -p /data/samba/home/martymac
# chown martymac:sambausers /data/samba/home/martymac
# chmod 700 /data/samba/home/martymac
```

Enfin, nous pouvons créer un script très simple pour notre utilisateur martymac qui connectera automatiquement son lecteur j : à notre partage "données" lors de son logon sur le domaine :

```
# cat > /data/samba/netlogon/martymac.cmd << EOF
@echo off
@NET USE J: \\ubuntu\donnees
@echo on
EOF
```

Attribuez-lui les bons droits :

```
# chown martymac:sambausers /data/samba/netlogon/martymac.cmd
# chmod 444 /data/samba/netlogon/martymac.cmd
```

Nous verrons comment nous pouvons modifier le compte de martymac pour qu'il tienne compte du script au logon et qu'il connecte un lecteur au répertoire home.

IV La gestion des comptes sur un contrôleur de domaine

1. La commande pdbedit

La commande pdbedit permet de lister les informations détaillées de chacun des comptes du domaine.

Nous pouvons ainsi lister les informations pour notre utilisateur martymac :

```
# pdbedit -v martymac
Unix username:          martymac
NT username:
Account Flags:          [U          ]
User SID:               S-1-5-21-1339008745-1179508330-2449281493-3000
Primary Group SID:     S-1-5-21-1339008745-1179508330-2449281493-1201
Full Name:              martymac,,,
```

```

Home Directory:          \\ubuntu\martymac
HomeDir Drive:          u:
Logon Script:            martymac.cmd
Profile Path:           \\ubuntu\profiles\martymac
Domain:                 WORKGROUP
Account desc:
Workstations:
Munged dial:
Logon time:             0
Logoff time:            Fri, 13 Dec 1901 21:45:51 GMT
Kickoff time:           Fri, 13 Dec 1901 21:45:51 GMT
Password last set:      Sun, 23 Oct 2005 14:12:49 GMT
Password can change:    Sun, 23 Oct 2005 14:12:49 GMT
Password must change:   Fri, 13 Dec 1901 21:45:51 GMT
Last bad password      : 0
Bad password count     : 0
Logon hours             : FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
  
```

Notons au passage le SID de l'utilisateur : **S-1-5-21-1339008745-1179508330-2449281493-3000** qui signifie qu'il appartient au domaine (ou workgroup ici) ayant le SID **S-1-5-21-1339008745-1179508330-2449281493** et que son compte possède la **RID 3000**. C'est le même principe pour son groupe primaire, qui possède le même SID local (de domaine).

2. Le mapping de groupes et le rôle des RIDs

Nous avons vu qu'un domaine NT prédéfinissait certains comptes et groupes par défaut, en leur attribuant des RID particuliers, synonymes d'un rôle particulier sur le domaine, les "well-known RIDs". Il est nécessaire pour un contrôleur Samba de ré-utiliser ces RIDs pour les comptes du domaine.

Ces RIDs particuliers sont notamment importants au niveau des groupes des utilisateurs. Ainsi, pour que les utilisateurs du groupe sambausers soient des "utilisateurs du domaine" au sens Windows du terme (RID égal à 513), il va falloir explicitement l'indiquer à Samba. De même, nous aurons besoin, pour les comptes de machines, d'un groupe sambamachines, correspondant au groupe "machines du domaine" (RID égal à 515).

Commençons par créer notre groupe de machines (le groupe sambausers existe déjà) :

```
# groupadd -g 515 sambamachines
```

Attribuons ensuite les bons RIDs aux deux groupes :

```
# net groupmap add rid=515 unixgroup=sambamachines ntgroup="Domain Computers"
# net groupmap set "Domain Users" sambausers
```

Note : "net groupmap add" ajoute un mapping, et "net groupmap set" en modifie un. Nous utilisons "net groupmap set" pour les utilisateurs du domaine car Samba propose déjà un mapping non initialisé.

Enfin, nous pouvons vérifier les "mappings" créés listant les mappings existants :

```
# net groupmap list
System Operators (S-1-5-32-549) -> -1
```

```

Replicators (S-1-5-32-552) -> -1
Guests (S-1-5-32-546) -> -1
Domain Users (S-1-5-21-1339008745-1179508330-2449281493-513) -> sambausers
Domain Computers (S-1-5-21-1339008745-1179508330-2449281493-515) -> sambamachines
Power Users (S-1-5-32-547) -> -1
Print Operators (S-1-5-32-550) -> -1
Administrators (S-1-5-32-544) -> -1
Domain Admins (S-1-5-21-1339008745-1179508330-2449281493-512) -> -1
Domain Guests (S-1-5-21-1339008745-1179508330-2449281493-514) -> -1
Account Operators (S-1-5-32-548) -> -1
Backup Operators (S-1-5-32-551) -> -1
Users (S-1-5-32-545) -> -1
  
```

Nous avons bien "mappé" les deux groupes sambausers et sambamachines vers leur équivalent NT.

Attention : Lors de la création d'un mapping faisant intervenir le groupe primaire Unix d'un utilisateur, Samba ne modifie pas, pour cet utilisateur, la valeur de son "primary group sid" correspondant au nouveau mapping. Ceci provoque une décorrélation entre ces deux IDs (la valeur mappée et la valeur effective apparaissant au niveau du compte Samba). La solution est de créer les mappings AVANT de créer les comptes utilisateurs.

Pour corriger ce problème, je vous propose de supprimer l'utilisateur martymac et de le re-crée :

```

# smbpasswd -x
# smbpasswd -a martymac
  
```

Cette fois, si nous étudions le SID de groupe primaire de l'utilisateur martymac, nous voyons qu'il se termine bien par 513 :

```

# pdbedit -v martymac | grep -i "primary group sid"
Primary Group SID:      S-1-5-21-1339008745-1179508330-2449281493-513
  
```

3. Les paramètres avancés de chaque compte

Nous avons créé les partages homes, netlogon et profiles sur notre contrôleur de domaine. Pour qu'un utilisateur en bénéficie, il va falloir modifier ces informations au sein de son compte.

Ceci se fait par le biais de la commande pdbedit, avec laquelle nous indiquons le chemin de tous ces éléments, ainsi que la lettre de lecteur attribuée au répertoire home de l'utilisateur :

```

#pdbedit -h "\\ubuntu\martymac" -D "U:" -S "martymac.cmd" \
-p "\\ubuntu\profiles\martymac" martymac}
  
```

Notez que le script de netlogon est toujours relatif au partage "netlogon" du contrôleur de domaine.

On pourra éviter cette tâche fastidieuse de modification de comptes en ajoutant les directives suivantes à la section globale de notre fichier de configuration :

```
[global]
# [...]
# Paramètres Samba par défaut pour un utilisateur
logon drive = U:
logon home = \\ubuntu%\%U
logon path = \\ubuntu\profiles%\%U
logon script = %U.cmd
# [...]
```

Ainsi, chaque utilisateur Samba ajouté (par smbpasswd par exemple) prendra ces valeurs par défaut.

4. Création du compte POSIX de manière autonome

Un contrôleur de domaine Samba peut être manipulé à distance, soit graphiquement par un outil de gestion de domaine, tel celui proposé par NT4, soit en ligne de commande avec la commande net Samba. Cependant, à l'heure actuelle, notre contrôleur de domaine n'est pas capable d'ajouter un compte de manière autonome. En effet, Samba peut ajouter la partie lui concernant mais n'est pas configuré pour ajouter, auparavant, la partie POSIX du compte.

Voici quelques directives qui permettent de palier ce problème :

```
[global]
# [...]
# Gestion des comptes POSIX
add machine script = /usr/sbin/useradd -g sambamachines \
                    -c Machine -d /dev/null -s /bin/false '%u'
add user script = /usr/sbin/useradd -g sambausers \
                  -c Utilisateur -d /dev/null -s /bin/false '%u'
add group script = /usr/sbin/groupadd '%g'
add user to group script = /usr/bin/gpasswd -a '%u' '%g'
delete user script = /usr/sbin/userdel -r '%u'
delete group script = /usr/sbin/groupdel '%g'
delete user from group script = /usr/bin/gpasswd -d '%u' '%g'
set primary group script = /usr/sbin/usermod -g '%g' '%u'
# [...]
```

Chacune de ces commandes va être appelée par Samba pour ajouter la partie POSIX d'un compte avant la partie Samba :

- **add machine script** : ajout d'une machine (jonction d'une machine au domaine)
- **add user script** : ajout d'un utilisateur
- **add group script** : ajout d'un groupe
- **add user to group script** : ajout d'un groupe pour un utilisateur
- **delete user script** : suppression d'un utilisateur
- **delete group script** : suppression d'un groupe
- **delete user from group script** : suppression d'un groupe pour un utilisateur
- **set primary group script** : positionnement d'un groupe en groupe primaire pour un utilisateur

Les comptes POSIX étant stockés sur la machine elle-même, nous faisons appel aux commandes standard de manipulation de comptes sous GNU/Linux. Pour des comptes situés sur un annuaire LDAP, il faudrait

faire appel à des scripts particuliers, tels les ldapscripts.

5. Le superutilisateur Samba

Le superutilisateur Samba est nécessaire pour effectuer diverses opérations d'administrations, notamment pour la jonction d'une machine au domaine. Ce superutilisateur doit avoir un uid Posix égal à 0. L'utilisateur root est traditionnellement utilisé, ajoutons-le à nos utilisateurs Samba :

```
# smbpasswd -a root
```

Nous pouvons tester cet utilisateur en ajoutant un compte via une commande RPC :

```
# net rpc user add test -U root -S ubuntu
```

L'utilisateur root est celui avec lequel nous allons joindre notre machine cliente au domaine...

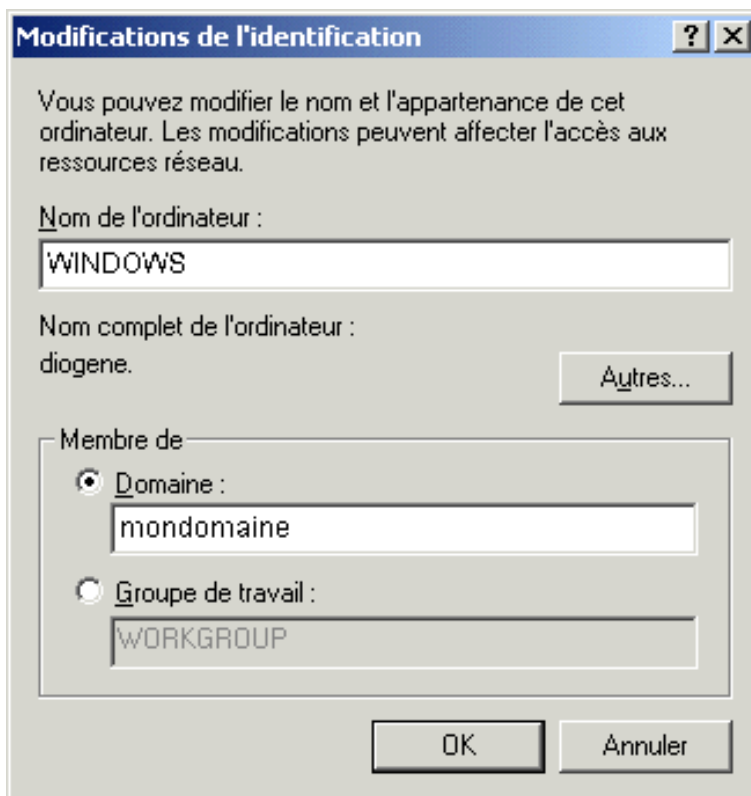
6. Jonction au domaine et test de notre contrôleur

Notre contrôleur de domaine est prêt. La dernière action à effectuer est de joindre notre machine cliente au domaine que nous venons de créer...

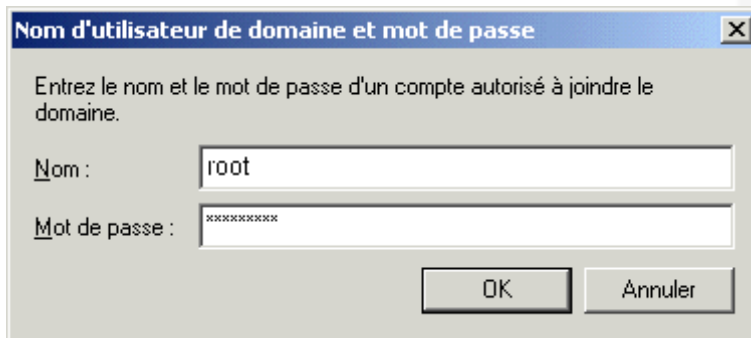
Concrètement, la jonction d'une machine au domaine correspond à la création d'un compte pour cette machine sur le PDC. Ce compte est un compte utilisateur standard, du nom netbios de la machine jointe, se terminant par un \$.

Prenons l'exemple d'une machine XP. La jonction d'une machine Windows Xp à un domaine se fait par un clic droit sur le poste de travail -> propriétés. Cliquez ensuite sur l'onglet "Nom de l'ordinateur", puis cliquez sur modifier.

Une fenêtre apparaît vous demandant le nom Netbios de votre machine et le domaine à joindre. Indiquez "mondomaine" pour le nom du domaine, et, par exemple "Windows" pour le nom netbios de votre machine.



Validez. Une fenêtre apparaît ensuite vous demandant le nom du compte habilité à joindre une station sur le contrôleur de domaine. C'est ici que nous devons utiliser le compte "root". Saisissez donc "root" et votre mot de passe et validez.



Votre machine devrait être jointe au domaine. Du côté du contrôleur de domaine Samba, un compte a bien été créé (POSIX + Samba) :

```
# getent passwd
[...]
windows$:x:1001:515:Machine:/dev/null:/bin/false
[...]

# pdbedit -L
martymac:1000:martymac,,,
root:0:root
windows$:1001:WINDOWS$
```

Nous pouvons désormais tester notre compte martymac sur la machine Windows. Connectez-vous avec ce compte au domaine "mondomaine", vous devriez avoir une lettre U : mappée vers votre répertoire home, ainsi qu'un lecteur J : mappé vers le partage données (via le script de logon). Votre profil devrait également être sauvegardé à la déconnexion.

V Samba en tant que BDC

Le rôle d'un contrôleur secondaire de domaine est double : répartir la charge liée aux authentifications avec le PDC et prendre le relais du PDC en cas de panne.

Techniquement, un BDC est une machine jointe au domaine (qui possède donc un compte sur le PDC) et qui gère les authentifications sur le domaine. Il possèdera un OS level plus faible que celui de PDC.

Voici un fichier de configuration qui pourrait convenir pour ajouter un BDC à notre domaine :

```
[global]

# Identification Netbios
workgroup = mondomaine
netbios name = ubuntuadc

# Controle de domaine active
os level = 40
domain logons = yes
domain master = no
local master = no

# Base de donnee de comptes - doit être synchronisée avec celle du PDC !
passdb backend = tdbsam:/var/lib/samba/mypassdb.tdb

# Authentification via la base de comptes locale
security = user

# Securite
encrypt passwords = yes

# Gestion des logs
log file = /var/log/samba/%m.log
log level = 2
```

Notez que nous devons synchroniser les base de comptes (POSIX et Samba) afin que notre BDC soit autonome en cas de panne du PDC ! C'est pour ceci que nous utilisons généralement un backend LDAP, afin de permettre au BDC comme au PDC de disposer de la même base de comptes (Posix et Samba)... La configuration ci-dessus n'est donc pas totalement adaptée. Nous n'étudierons pas ici le cas complet de la mise en place d'un BDC, qui reste une opération assez complexe à mettre en oeuvre.

Après avoir correctement configuré la machine et si nous disposons d'une base de comptes commune, il faut joindre le BDC au domaine. Ceci se fait de la manière suivante, depuis la machine ubuntuadc :

```
# net rpc join -S ubuntu -W mondomaine -U root
```

Un compte pour le BDC devrait être créé sur le PDC.

Chapitre 13

Administrer le serveur Samba

Nous avons déjà abordé les points essentiels liés à l'administration du serveur Samba :

- la configuration initiale
- la définition d'un partage
- l'ajout d'utilisateurs et de groupes

Il reste cependant certains points à aborder, et certaines "bonnes habitudes" à prendre, nous allons en décrire quelques-unes.

I Visualiser les connexions...

...avant de stopper un serveur pour intervention. La commande `smbstatus` permet de savoir en temps réel qui est connecté, et quels fichiers sont ouverts. Pensez à l'utiliser avant d'intervenir sur un serveur pour vous assurer que peu ou pas de personnes sont connectées.

```
# smbstatus -v
using configfile = /etc/samba/smb.conf
Processing section "[printers]"
Processing section "[tmp]"
Processing section "[donnees]"
Processing section "[homes]"
Processing section "[netlogon]"
Processing section "[profiles]"

Samba version 3.0.14a-Ubuntu
PID      Username      Group          Machine
-----
 7084    martymac     sambausers    windows      (192.168.1.1)
Opened /var/run/samba/connections.tdb

Service  pid    machine    Connected at
-----
donnees  7084   windows    Mon Oct 31 09:44:56 2005
IPC$     7084   windows    Mon Oct 31 09:44:54 2005
```

No locked files

Note : On remarque au passage que Samba gère chaque connexion par un processus différent (ici PID 7084) et que les informations relatives à la connexion sont maintenues dans un fichier tdb.

II Relire la configuration sans redémarrer Samba...

Samba peut relire sa configuration sans être redémarré. Pour ceci, il suffit d'envoyer un signal HUP aux démons qui sont en cours de fonctionnement :

```
# killall -HUP smbd nmbd winbindd
```

Attention, le comportement de Samba est parfois un peu étrange dans le sens où toute la configuration n'est pas re-parsée. Si vous avez ajouté une imprimante dans CUPS, elle ne sera pas chargée.

III En cas de problème : étude des logs !

Pensez à étudier les logs et, si besoin est, à augmenter le niveau de log au maximum, c'est à dire 10. C'est là l'un des seuls moyens de se sortir d'une situation où tout semble bloqué...

```
log file = /var/log/samba/%m.log  
log level = 10
```

```
# tail -f /var/log/samba/machine.log
```

IV Administration graphique ? Swat...

Nous avons étudié, dans ce manuel, comment administrer Samba via les lignes de commandes. L'un des principaux problèmes de Samba est qu'il ne dispose pas d'interface graphique "digne de ce nom" pour l'administration. Une interface rudimentaire est toutefois proposée en standard, il s'agit de Swat.

Swat est un outil Web, il embarque un petit serveur http et doit être démarré via (x)inetd. Plus d'informations à cette adresse :

<http://www.samba.org/samba/docs/man/Samba-HOWTO-Collection/SWAT.html>