

Introduction à Samba 3.x

Le module suivant décrit l'installation du service Samba. Ce service sert généralement pour le partage de ressources (fichiers et d'imprimantes) sur le réseau avec des ordinateurs sous Windows. Fonctionnalité beaucoup moins utilisée, il permet aussi de définir votre serveur comme étant un *Contrôleur de Domaine*.

Ce service sera le noyau principal de notre domaine Linux qui permettra d'avoir une grande interopérabilité avec les systèmes clients Windows. Samba vous offre donc de nombreux avantages, et permet:

- D'offrir une administration centralisée;
- Aux utilisateurs et aux ordinateurs autorisés d'accéder aux ressources réseaux;
- De centraliser le processus d'authentification des utilisateurs;
- De définir les paramètres de notre domaine.

Concept de Samba 3

Le concept de PDC/BDC avec Samba est similaire à celui que possède Windows NT4, mais là s'arrête la ressemblance, car Samba ne dispose pas nativement d'un annuaire LDAP.

Considérer l'ajout de l'annuaire LDAP avec Samba comme la promotion d'un serveur Windows comme contrôleur de domaine. Car tout comme sous Linux, un serveur Windows ne dispose pas d'un annuaire LDAP. Aussi, il ne faut pas confondre l'annuaire LDAP et Active Directory. Active Directory est un annuaire LDAP avec une section de partage Sysvol permettant l'ajout d'option dans la gestion des objets LDAP.

C'est pour cette raison que nous allons y ajouter notre propre service d'annuaire. Pour répondre à ce besoin, nous allons utiliser OpenLDAP 2.3.x sous Samba 3.x.

Samba permettra aussi de repousser les limites de séparation entre Linux et Windows en gérant des scripts de stratégie de groupe (*Group Policy Registry*)¹ comme le ferait les GPO sous Windows 2000/2003 Serveur. CyGPR[®] vous permettra de définir un ensemble de paramètres de configuration des utilisateurs et des ordinateurs pouvant être associé à des utilisateurs et ordinateurs.

¹ Les GPR sont des stratégies de groupe découlant du Projet CyGPR[®] de Cybionet.

NOTES



Les sections Globale et de Partages

Identifié par l'entête [global], cette section contient des paramètres qui seront appliqués à l'ensemble du fichier *smb.conf*. Ces paramètres dicteront le comportement du serveur Samba, ainsi que de définir des configurations par défaut aux différents partages.

Alors que certains paramètres sont exclusifs à la section globale ou aux sections de partage, d'autres paramètres peuvent cependant être inscrits dans les deux types de sections.

Identifié par l'entête [nomdepartage], où *nomdepartage* représente le nom que vous désirez donner à votre partage, cette section permet de définir les paramètres exclusifs à votre partage. Cette section vous permettra même de contredire des paramètres définis dans la section [global].

Édition du fichier de configuration de Samba 3

Le fichier de configuration de Samba se retrouve dans le répertoire */etc/samba*. Commençons dès maintenant la configuration du service Samba en tant que PDC Linux.

```
cd /etc/samba/  
vim smb.conf
```

Pour remettre en contexte l'utilisation de Samba, ce service sera nécessaire pour l'authentification et le partage de données sur le réseau avec les clients Windows. Pour les clients Linux, le service d'annuaire OpenLDAP servira pour l'authentification (avec PAM/NSS) et Samba servira pour le partage de données sur le réseau.

Pour avoir plus d'information sur les paramètres que nous allons utiliser dans ce module, nous vous invitons à utiliser la commande **man smb.conf** qui vous indiquera tous les paramètres disponibles pour votre version de Samba 3.



NOTE: Nous allons couvrir plus en détail comment faire le partage des ressources à l'aide de Samba dans le *module 10*. Ce module ci concerne exclusivement l'installation du serveur Samba en tant que PDC.

NOTES



Configuration de la section globale

Les informations qui suivent seront inscrites dans la section *global* du fichier de configuration de Samba.

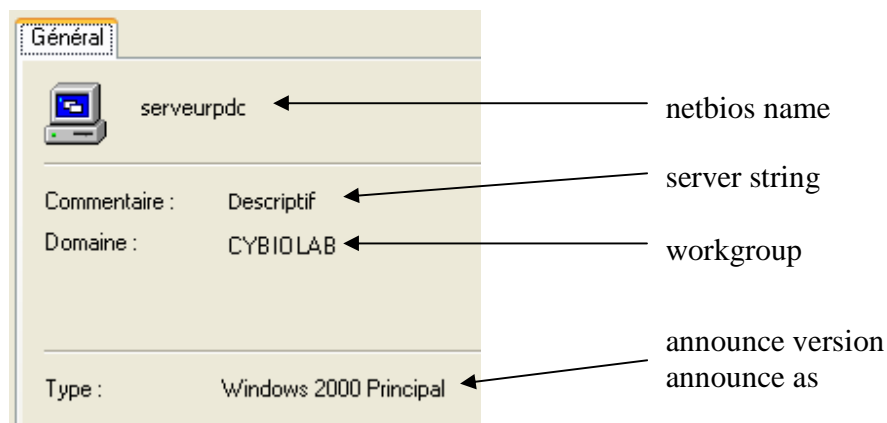
Définition du nom de serveur et de domaine

Nous allons donc débuter par définir les informations concernant notre serveur PDC que vous avez préalablement inscrit dans l'*Annexe A*. Pour ce faire vous allez avoir besoin des informations suivantes, soit:

- Le nom netbios de votre serveur PDC;
- Le nom de votre domaine;
- Le descriptif de votre serveur.

```
[global]
netbios name = serveurpdc
workgroup = cybiolab
server string = Descriptif
announce version = 5.0
announce as = NT
...
```

Nous faisons ici un point de référence entre la configuration que l'on va inscrire dans la section globale du fichier de configuration de Samba et avec la fenêtre de propriété par le Favoris réseau de Windows.



NOTES



Nous allons définir le nom netbios de votre serveur afin qu'il soit reconnu comme tel sur le domaine. Ce nom netbios sera reconnu uniquement dans les réseaux Microsoft et n'est nativement pas reconnu par les ordinateurs fonctionnant sous Linux.

netbios name = serveurpdc

Définissons maintenant le nom de notre domaine Linux. A remarquer que nous n'inscrivons pas *cybiolab.lan* comme valeur pour l'entrée workgroup pour la simple et bonne raison que le *.lan* n'est pas un nom de domaine reconnue par le DNS, mais représente un nom de domaine de premier niveau (TLD: *Top Level Domain*).

workgroup = cybiolab

Quoique pas vraiment indispensable, cette entrée va vous permettre d'identifier votre serveur PDC lors de son affichage dans une recherche d'un ordinateur ou dans la navigation dans le Favoris réseau.

server string = Descriptif

Les deux entrées suivantes permettent de définir comment votre contrôleur de domaine va s'annoncer sur le domaine. Dans notre cas nous allons faire passer notre serveur Linux pour un *Contrôleur de Domaine Windows 2000 Server*.

announce version = 5.0
announce as = NT



NOTE: Cependant une valeur de 5.0 et supérieure bloquera l'utilisation de l'outil *usrmgr.exe* de Microsoft NT4 si ce dernier n'est pas la toute dernière version disponible.

Version	Description (avec un <i>announce as = NT</i>)
5.2	Windows Principal
5.1	Windows Principal
5.0	Windows 2000 Principal
4.9 (par défaut avec Samba 3.x)	Windows NT 4.9 Principal
X.X	Windows NT X.X Principal

NOTES



Version	Description
NT	Windows Serveur
NT Server (identique que NT)	Windows Serveur
NT Workstation	Windows Workstation
WFW	Windows pour WorkGroup Principal
Win95	Windows 95

Configuration du rôle explorateur

Le service *browser* tient à jour une liste des domaines, des groupes de travail et d'ordinateurs de votre réseau Microsoft, ainsi que de tous autres équipements réseau utilisant le protocole netbios.

Au démarrage, les ordinateurs Windows s'annoncent par une diffusion LMB sur le sous-réseau. Tout ordinateur capable de collecter, maintenir et distribuer une liste *browse* est considéré comme un explorateur (*browser*) et peut jouer un ou plusieurs des cinq rôles explorateurs.

▪ Explorateur principal du domaine

(*Domain master browser*) (DMB)

Le contrôleur de domaine principal d'un domaine reçoit un avantage particulier lors des élections d'explorateur pour prendre le rôle d'explorateur principal de domaine. Cela permet d'assurer l'efficacité de l'exploration lorsqu'un domaine s'étend sur plusieurs sous-réseaux. Les explorateurs principaux sur chaque sous-réseau utilisent un datagramme dirigé pour s'annoncer à l'explorateur principal de domaine.

▪ Explorateur principal

(*Local master browser*) (LMD)

Le contrôleur des annonces des serveurs et des domaines, envoie les listes d'exploration aux explorateurs secondaires, répond aux clients demandant des listes d'exploration des serveurs, modifie les explorateurs potentiels en explorateurs secondaires le cas échéant et annonce le domaine pour informer les explorateurs principaux d'autres domaines du nom du domaine et de l'explorateur principal pour ce domaine.

NOTES



Configuration des caractéristiques d'authentification

Les paramètres de cette section vont nous permettre de définir les configurations d'ouverture de session pour le service Samba.

```
[global]
...
domain logons = yes
security=user
username map = /etc/samba/smbusers
...
```

Avec le paramètre *domain logons*, votre serveur Samba va activer le service netlogon pour les postes Microsoft. Avant tout, il ne faut pas perdre de vue que Samba 3 reproduit un domaine de type NT4 et par conséquent n'utilise pas encore le partage sysvol des domaines 2000 et plus.

domain logon =yes

Voici quelques combinaisons des paramètres *domain master* (défini plus haut) et *domain logons* qui affecteront le rôle de votre serveur en tant que contrôleur de domaine principal, contrôleur de domaine secondaire ou serveur membre du domaine.

```
domain master = yes
domain logons = yes
    Rôle du serveur: ROLE_DOMAIN_PDC

domain master = no
domain logons = yes
    Rôle du serveur: ROLE_DOMAIN_BDC

domain logons = no
    Rôle du serveur: ROLE_STANDALONE
```

Le paramètre *security* définit le niveau de sécurité de partage. Par exemple, si votre serveur utilise des noms d'utilisateur qui sont reconnus par ce même serveur, vous utiliserez *security=user*. Par contre si vos noms d'utilisateurs ne sont pas reconnus par le serveur vous utiliserez *security = share*.

Dans notre cas nous installons un contrôleur de domaine, par conséquent, il doit reconnaître le nom de ses utilisateurs.

security=user

NOTES



L'option *username map* vous permet de spécifier un fichier dans lequel contient une correspondance de nom d'utilisateur d'un client vers le serveur. Cette correspondance peut être intéressante pour faire correspondre certains utilisateurs de poste Windows avec les comptes du serveur sous Linux.

```
username map = /etc/samba/smbusers
```

Éditer le fichier `/etc/samba/smbusers` et ajouter les lignes.

```
root = administrator administrateur  
nobody = guest invité
```

Options de connexions

L'option *socket options* est souvent configurée par les utilisateurs de Samba de façon machinale, sans réellement savoir ce qu'elle fait. Dans les diverses documentations, elle aussi est souvent expliquée dans un contexte d'ajustement de performance (*tuning*).

```
[global]  
...  
socket options = TCP_NODELAY SO_SNDBUF=8192 SO_RCVBUF=8192  
...
```

Donc ce paramètre vous permettra de définir les options de connexion TCP avec le client. Selon la configuration, cela peut affecter grandement les performances TCP de vos connexions avec Samba. Ici nous définissons:

TCP_NODELAY: Améliore *supposément* la vitesse de 30 à 50 pourcent.

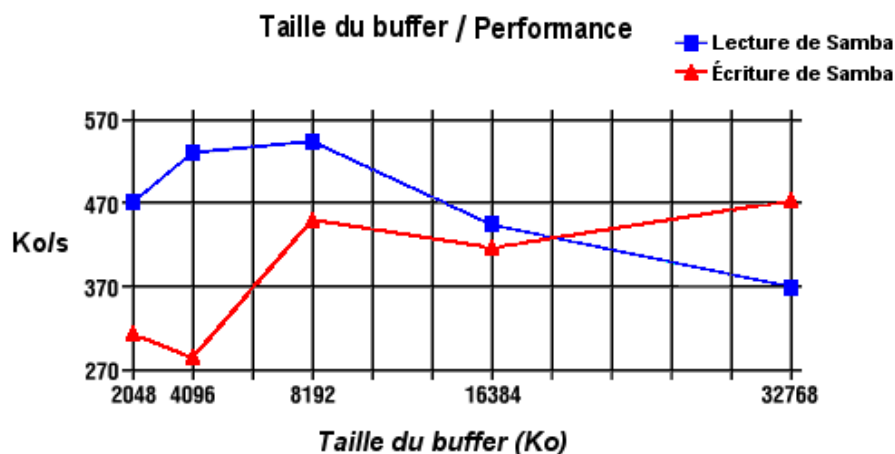
SO_SNDBUF=8192: Défini la taille du *buffer* en envoi, permettant ainsi de contredire celle du système d'exploitation.

SO_RCVBUF=8192: Défini la taille du *buffer* en réception, permettant toujours de contredire celle du système d'exploitation.

NOTES



Le tableau représente un test de performance effectué sur des accès en lecture et écriture sur Samba 2.0x. L'idée de ce tableau est plus de montrer l'impact de la configuration de cette option que de donner une valeur précise (*Tableau: 2001, O'Reiley & Associates Inc*).



Remarquez aussi dans le tableau qu'une valeur trop basse (en dessous de la valeur par défaut des systèmes d'exploitation) ou une valeur trop élevée, dégrade les performances de lecture et d'écriture de Samba.



NOTE: Selon l'équipe de Samba, l'option `SO_RCVBUF=8192` pourrait fortement diminuer les performances d'accès à Samba 3 par l'interface *loopback*.

Définition des mots de passe

Nous allons définir le minimum de paramètre concernant les mots de passes et son application dans le fichier *smb.conf*. La définition de trop de paramètres ne ferait que vous nuire plus tard et ne vous apporterait aucune sécurité supplémentaire.

```
[global]
...
encrypt passwords = yes
; password level = 8
; username level = 8
; unix password sync = yes
; pam password change = yes
...
```

NOTES



Afin que notre mot de passe ne soit pas communiqué en texte clair nous allons exiger une encryption. Par défaut, cette option est prédéfinie à la valeur `yes`.

```
encrypt passwords = yes
```

Nous vous présentons maintenant deux autres paramètres, qui à première vue semble intéressant, mais *peuvent compromettre la sécurité de votre contrôleur de domaine* et ralentir considérablement l'authentification.

```
; password level = 8
```

```
; username level = 8
```

Ce paramètre indique au système d'ouverture de session de Samba de faire une inversion de case en le nombre de chiffre défini, l'un sur le mot de passe et l'autre sur le nom de l'utilisateur, si ceux-ci ne correspondent pas. Dans le cas-ci, l'inversion se fera sur 8 caractères.

L'option *pam password change* autorise le changement de mot de passe avec le mécanisme d'authentification PAM. Alors que l'option *unix password sync* permet de synchroniser les mots de passe Samba et mots de passe systèmes Unix.

```
; pam password change = yes
```

```
; unix password sync = yes
```

Dans les deux cas nous ne les activerons pas inutilement, car nous allons justement modifier ce mécanisme d'authentification pour le centraliser sur l'annuaire LDAP.

Définition des services WINS, NTP

Nous allons maintenant configurer des paramètres qui indiqueront les rôles que le service `nmbd` ce verra assignés, soit le rôle de serveur WINS ainsi que de serveur NTP.

```
[global]
...
time server = yes

wins support = yes
; wins server = 192.168.0.2
...
```

NOTES



Le paramètre *time server* indique au service *nmbd* de s'annoncer comme un serveur de temps aux clients Windows. Naturellement Samba n'est pas un serveur de temps et un service NTP devra être installé sur le PDC. Pour ce faire, utiliser *openntpd* ou *ntpd* par exemple.

```
time server = yes
```

Nous allons maintenant installer un serveur WINS sur notre domaine (yurk!). Cela est quasi essentiel, car nous fonctionnons avec un domaine de type NT4, et Samba génère des erreurs (mineurs) si nous n'avons pas de serveur WINS valide d'installé.

Deux choix s'offrent à nous. Utiliser notre PDC comme serveur WINS à l'aide du paramètre *wins support* qui indique au service *nmbd* d'agir comme serveur WINS. Vous pouvez aussi installer le service WINS sur un autre serveur et indiquer au PDC l'adresse (IP ou DNS) du serveur WINS à l'aide du paramètre *wins server*.

```
wins support = yes  
; wins server = 192.168.0.2
```

Il ne faut surtout pas activer ces deux options en même temps, car il entrerait en conflit et le service *nmbd* s'arrêterait.



NOTE: Tout comme sur un domaine Microsoft, vous ne pouvez pas avoir plus d'un serveur WINS par sous-réseau d'un domaine.

Définition des configurations supplémentaires

Nous vous présentons ici, comment définir des paramètres supplémentaires pour certains ordinateurs en leurs créant un fichier de configuration personnalisé. %m représente le nom de l'ordinateur qui accédera cette configuration.

```
[global]  
...  
; include /etc/samba/smb.conf.%m  
...
```

Dans notre cas, nous n'utiliserons pas ce paramètre, mais il est toujours intéressant de connaître son existence.

NOTES



Aussi, assurez-vous bien que le répertoire aie les permissions 755 et que l'utilisateur propriétaire soit root et que le groupe propriétaire soit root.

Le paramètre suivant va indiquer que ce répertoire n'est pas navigable par le client. Cela ne l'empêchera cependant pas d'accéder à tous les fichiers contenus dans ce répertoire s'il connaît le chemin direct. Ce qui est normal car il doit pouvoir les lire et les exécuter.

```
browseable = no
```

Et enfin, pour sécuriser un minimum les fichiers se trouvant dans ce partage, nous allons nous assurer qu'ils ne peuvent être modifiés en les mettant en lecture seule.

```
read only = yes
```

Définition du partage système [profiles]

Ce partage système contient le répertoire de profil de l'utilisateur, soit le *Documents and Settings* du poste Windows Professionnel. Dans le cas où vous utilisez un profil itinérant, ce profil sera transféré sur le poste client pour être utilisé par la session active de l'utilisateur.

Nous allons donc configurer ce partage, ce même si nos utilisateurs utiliserons des profils locaux. Le choix du profil sera défini pour chacun des utilisateurs. Le type de profil sera donc défini plus tard dans l'annuaire LDAP.

```
[profiles]
comment = Partage du profil utilisateur
path = /var/lib/samba/profiles

browsable = no
read only = no

create mode = 0600
directory mode = 0700

veto files = desktop.ini
hide dot files = yes
;csc policy = disable
```

NOTES



Définition du partage système [homes]

Ce partage système contient un espace de travail réseau de l'utilisateur, généralement son répertoire personnel (*home directory*). Il n'est cependant pas obligatoire que le chemin du partage soit dans le répertoire *home* du système linux.

Aussi, nous ne vous recommandons pas que le chemin de ce partage soit identique à celui défini par le partage système [profiles].

Certaines caractéristiques concernent ce partage, tel:

- Le nom du partage sera changé de [homes] à celui du nom d'authentification de l'utilisateur.
- Si aucun chemin n'est spécifié pour le partage [homes], le chemin du répertoire personnel de l'utilisateur lui sera alors assigné.

```
[homes]
comment = Répertoire personnel
; path= /travail/%U
browseable = yes
read only = no
```

Ce paramètre donne une description du partage. Cette description sera visible par le *voisinage réseau* et de la commande net du client Windows.

```
comment = Répertoire personnel
```

Il vous serait possible de définir un chemin spécifique pour chacun des utilisateurs. Par exemple dans le répertoire /travail/<nom de l'utilisateur>.

```
; path= /travail/%U
```

Le paramètre suivant va indiquer que le répertoire partagé est navigable par le client.

```
browseable = yes
```

Ce paramètre indique que ce répertoire partagé est en lecture et écriture pour l'utilisateur propriétaire du répertoire.

```
read only = no
```

NOTES



Vérification des partages et du rôle explorateur

smbclient -L localhost

Password:

Domain=[CYBIOLAB] OS=[Unix] Server=[Samba 3.0.37]

Sharename	Type	Comment
IPC\$	IPC	IPC Service (Descriptif)
homes	Disk	Repertoire personnel

Anonymous login successful

Domain=[CYBIOLAB] OS=[Unix] Server=[Samba 3.0.37]

Server	Comment
SERVEURPDC	Cybiolab
Workgroup	Master
CYBIOLAB	serveurpdc

NOTES



