

Administration du partage des dossiers

Le partage de dossier est un élément extrêmement important au sein d'une entreprise. Les raisons d'exister d'un système informatique sont les données qu'il contient et son échange entre les différents intervenants.

Cette unité vous donnera des concepts de base à retenir afin de bien élaborer vos partages. Il vous montrera aussi les paramètres les plus utilisés dans des partages de ressources dans un environnement d'entreprise.

Préparation de l'environnement de partage

Premièrement, nous vous recommandons d'utiliser un serveur de fichier exclusif pour le partage des fichiers et qui ne se trouvera surtout pas sur votre contrôleur de domaine principal. Consulter le module d'intégration de BDC et de serveurs membres Linux (Module 15) pour monter un serveur Linux joint au domaine.

Idéalement, pour l'entreposage de vos données, utiliser des disques en RAID physique. Utiliser du RAID 1 (miroir) ou du RAID 5 (agrégat avec parité) selon vos besoins et budgets. Aussi, il existe de très bonnes cartes RAID SATA qui feront le bonheur de vos portefeuilles (et du comptable par la même occasion). Par contre, si la performance est votre préoccupation principale, les cartes RAID SCSI sont toujours des incontournables.

Aussi, il pourrait être intéressant d'utiliser les volumes logiques (LVM2) qui vous permettra de facilement augmenter ou diminuer la taille de vos disques durs. C'est l'équivalent des disques dynamiques sous Microsoft, mais avec Linux.



NOTE: Si vous désirez des informations supplémentaires sur le LVM2 (*Logical Volume Manager*), visitez le site officiel au sourceware.org/lvm2/

NOTES



Nous allons procéder à la création de notre environnement de partage de fichiers en créant un répertoire du nom de **smbroot** à la racine de votre système. Ce répertoire sera la racine de votre service de fichier qui va contenir les différents répertoires de partages.

```
/smbroot
|
|_____Workspace
|
|_____Depot
```

```
cd /
mkdir smbroot
chown root:root smbroot
chmod 2770 smbroot
```

Attention, si vous prévoyez faire du partage de fichiers à des utilisateurs non authentifiés, définissez les permissions à 2775 au lieu de ceux indiqués précédemment.

Cependant, si vous avez prévu d'ajouter un disque dur supplémentaire pour vos partages, exécuter les commandes suivantes, sinon passer directement à la création d'un partage.

```
fdisk /dev/hdb
mke2fs -j /dev/hdb1
mount /dev/hdb1 /smbroot
```

Ajuster le fichier `fstab` pour son nouveau point de montage.

```
vim /etc/fstab
```

Et ajouter la ligne,

```
/dev/hdb1 /smbroot ext3 noatime,acl 0 0
```

Puis, nous allons faire en sorte que le système prenne en compte immédiatement le nouveau disque dur.

```
mount -t ext3 -o remount,rw,acl /dev/hdb1 /smbroot/
```

Faites la vérification que la partition est bien montée.

```
mount
```

NOTES



Création d'un partage

Configuration d'un partage

Plusieurs paramètres existent pour créer un partage de fichiers sur le réseau. Nous vous présenterons les paramètres les plus utilisés suivis de scénarios les plus communs rencontrés en entreprise. Pour avoir la totalité des paramètres disponibles, saisissez la commande **man smb.conf** en console sur le serveur Linux. Utiliser uniquement les paramètres qui sont précédés des caractères (S).

A la toute fin du fichier de configuration smb.conf, ajouter vos lignes de configuration de votre partage.

```
[<nom_du_partage>]
comment = <Description du partage>
path = /smbroot/<nom_du_repertoire>

browseable = <yes | no>
read only = <yes | no>
```

[<nom_du_partage>]

Le nom entre crochet représente le nom du partage sur le serveur de fichier Linux. Ce nom doit respecter les consignes suivantes:

- Le nom ne devrait pas avoir plus de 12 caractères, surtout si vous utilisez d'ancien client Windows ou Linux. Ce manuel ne tiens pas compte de ce type de client. Lors d'une vérification de votre configuration Samba, vous pourriez obtenir l'avertissement suivant:

```
WARNING: You have some share names that are longer than 12
characters.
```

- N'insérer pas d'espace dans les noms de partage. Quoi que supporté par les différents clients, un espace dans un nom de partage est très désagréable d'utilisation sous les clients Linux.
- Aussi porter une attention aux noms que vous donner à vos partages, car les clients Linux sont sensibles à la case. Utiliser

NOTES



donc toujours la même convention de nommage pour vos noms de partage.

- Éviter les caractères spéciaux ou les accents dans vos noms de partage.

comment = <Description du partage>

Ce paramètre donne une description du partage. Cette description est visible uniquement si votre paramètre *browseable* a la valeur *yes* ou *true*.

path = /smbroot/<nom_du_repertoire>

L'emplacement qui contient les répertoires partagés, dans ce manuel, ce chemin est situé dans le répertoire /smbroot. Il sera à vous de créer les répertoires de partage localement sur le serveur.

Aussi, assurez-vous bien que le répertoire ait les permissions 2770 et que l'utilisateur propriétaire soit root et que le groupe propriétaire soit root. Nous verrons plus tard les scénarios de partage de fichiers les plus communs.

browseable = <yes | no>

Le paramètre suivant va indiquer si ce répertoire est navigable ou non par les clients. Si la valeur est à *yes* le partage est navigable, alors qu'une valeur *no* indiquera que ce répertoire n'est pas navigable. Cela ne l'empêchera cependant pas d'accéder à tous les fichiers contenus dans ce répertoire s'il connaît le chemin complet.

read only = <yes | no>

Pour rendre le contenu du partage en lecture seule ou autoriser l'écriture, utiliser le paramètre *read only*. Une valeur à *yes* indique que le partage est en lecture seule, alors que la valeur *no* indique que l'utilisateur a le droit d'écriture sur le partage.

Le paramètre *writeable* est l'antonyme du paramètre *read only*. Utiliser uniquement le paramètre *read only*, ce qui est amplement suffisant.

NOTES



Utilisateurs autorisés

Vous pouvez définir des restrictions dans le partage des utilisateurs ou groupes d'utilisateurs qui pourront accéder aux ressources réseaux. Nous vous conseillons cependant d'appliquer les recommandations suivantes:

- N'autoriser pas les utilisateurs non authentifiés à accéder à vos ressources partagés, sauf si c'est ce que vous désirez absolument faire. Par exemple un répertoire public accessible par les employés, consultants externes et visiteurs.
- Ne mettez pas de restriction directement sur vos partages, mais appliquer uniquement les permissions du système de fichier. En faisant cela, vous évitez de faire des erreurs et de complexifier la gestion des autorisations.

```
guest ok = <yes | no>
valid users = %U, nom, %group
guest account = nobody
write list = %U, nom, %group
read list = %U, nom, %group
```

guest ok = <yes | no>

Vous désirez que le partage soit ouvert à tous, ce même si cet utilisateur n'est pas membre de votre domaine, utiliser ce paramètre.

Il va de soit que pour le partage d'information en entreprise, ce paramètre n'est pas l'idéal, mais peut être fort utile en certaine circonstance.

NOTE: Le fait d'avoir choisi le paramètre *security = user* dans la configuration de Samba ne vous permettra pas aux utilisateurs non authentifiés d'accéder au partage, ce même avec le paramètre *guest ok* à yes.

C'est pour cette raison qu'il n'est pas idéal d'utiliser un contrôleur de domaine pour partager des ressources réseaux.

NOTES



valid users = <valeur1, valeur2, ...>

Ce paramètre permet de définir quel groupe d'utilisateur ou utilisateur peut accéder au partage. Nous vous recommandons de ne pas utiliser ce paramètre mais appliquer uniquement les permissions du système de fichier.

L'utilisation de ce paramètre décentralise la gestion et complexifie la gestion des autorisations. Si vous prévoyez tout de même utiliser ce paramètre, appliquer le uniquement qu'aux groupes et non aux utilisateurs. Ceci toujours dans le but de simplifier et faciliter la gestion de vos ressources réseaux.

%U	Variable définissant l'utilisateur actuellement actif.
<utilisateur>	Nom d'un utilisateur valide.
%<groupe>	Nom d'un groupe valide.

guest account = <valeur>

Ce paramètre n'a pas à être défini, car il est parfaitement adapté par défaut. Nous vous la montrons uniquement pour que vous sachiez qu'il existe en cas de besoin. Par défaut, ce paramètre a la valeur *nobody*.

write list = <valeur1, valeur2, ...>

Ce paramètre détermine une liste de groupes ou d'utilisateurs qui ont les permissions d'écrire sur le partage. Encore ici, nous vous recommandons de ne pas utiliser ce paramètre mais appliquer uniquement les permissions du système de fichier.

Cependant, si vous prévoyez tout de même utiliser ce paramètre, appliquer le uniquement qu'aux groupes et non aux utilisateurs.

Exemple:

```
write list = root, @DomainAdmins, @DomainsUsers
```

NOTE: Ce paramètre ne fonctionne pas si le paramètre global *security* est défini à *share* sous Samba 3.

NOTES



read list = <valeur1, valeur2, ...>

Ce paramètre détermine une liste de groupes ou d'utilisateurs qui ont les permissions de lire sur le partage. Encore ici, nous vous recommandons de ne pas utiliser ce paramètre mais appliquer vos droits d'accès directement à partir des permissions du système de fichier.

Si vous prévoyez tout de même utiliser ce paramètre, appliquer le uniquement qu'aux groupes et non aux utilisateurs.

Exemple:

```
read list = root, @DomainAdmins, @DomainsUsers
```



NOTE: Tout comme le paramètre *write list*, le *read list* ne fonctionne pas si le paramètre global *security* est défini à *share* sous Samba 3.

Masques d'un partage

La grande difficulté de compréhension dans l'attribution des permissions sur les partages Samba se retrouve ici: *les masques de partage*.

Je vous conseille fortement de lire le Samba-HOWTO-Collection dans la section "*create mask parameter*" sur le site officiel de Samba.

Pour notre part (et toujours dans le cadre du projet), pour d'assurer que tous les fichiers et répertoires seront créés avec le groupe de la personne à qui appartient le répertoire. Nous allons utiliser les paramètres suivants:

```
force create mode = 660  
directory mode = 770
```

Ces deux paramètres vont aussi nous assurer que tout les fichiers et répertoires qui seront créer dans le partage seront en lecture/écriture par l'utilisateur propriétaire et groupe propriétaire.

N'oublier surtout pas que nous appliquons des ACL(EA) sur ces mêmes fichiers et répertoires. Ces deux paramètres sont donc indispensables.

NOTES



force create mode = <valeur_en_octale>

Ce paramètre indique une valeur en octale définissant les permissions appliquées. Samba applique le *force create mode* avec une logique OU.

Exemple:


```
force create mode = 660
```

directory mode = <valeur_en_octale>

Ce paramètre est un synonyme du paramètre "*directory mask*". Ce paramètre prend les permissions Windows pour en faire une conversion Posix. Samba applique donc le *directory mask* avec une logique ET. Il regarde les permissions Windows ET les permissions de ce paramètre et applique que ceux qui correspondent dans les deux cas.

Exemple:

```
directory mode = 770
```



NOTE: Ce paramètre ne s'applique pas aux permissions définies par un éditeur de permission d'ACL pour Windows NT/2000/XP. Si vous désirez assurer l'application du masque sur la liste de contrôle, vous devrez utiliser le paramètre '*directory security mask*'.

Fichiers cachés et spéciaux**hide dot files = <yes | no>**

Comme vous avez pu le constater, sous Linux, un fichier ou répertoire caché débute par un point. Ce paramètre vous permet de cacher complètement les fichiers cachés de Linux sous un partage Samba. Par défaut la valeur est à *no*.

Nous vous recommandons de mettre la valeur de ce paramètre à *yes*.

Exemple:

```
veto files = /cybiolab/.recycle/ /lost+found /aquota.group/ /CVS/
```

NOTES



hide files = <valeur>

Ce paramètre permet de cacher des fichiers ou des répertoires que nous ne voulons pas qu'il soit visible sur le réseau.

Exemple:

```
hide files = /cybiolab/cache/
```

Ici nous cachons le répertoire *cache* situé dans le répertoire

hide special files = <yes | no>

Ce paramètre empêche les clients de voir les fichiers spéciaux, tel que les *sockets*, *devices* et la liste des répertoires des *fifo*.

hide unreadable = <yes | no>

Ce paramètre empêche les utilisateurs de lister les fichiers qu'ils ne peuvent lire. La valeur par défaut de ce paramètre est à *no*.

hide unwriteable files = <valeur>

Ce paramètre empêche les utilisateurs de lister les fichiers qu'ils ne peuvent écrire. La valeur par défaut de ce paramètre est à *no*. Noter cependant que les répertoires dont les utilisateurs ne peuvent écrire dedans apparaîtront normalement.

veto files = <valeur>

Ce paramètre contient une liste de fichiers ou de répertoires qui ne seront ni visible ou accessible par l'utilisateur. Chacun des entrées doivent être séparées par un '/'. Les caractères wildcard '*' et '?' sont supportés. Ce paramètre est fort utile pour la corbeille réseau en autre.

Exemple:

```
veto files = /cybiolab/.recycle/ /lost+found /aquota.group/
```

NOTES



delete veto files = <yes | no>

Ce paramètre est utilisé par Samba pour tenter de supprimer les répertoires et leurs contenus, si ils sont dans la liste des veto files.

csc policy = <disable | manual | program | documents >

Ce paramètre sert pour la stratégie hors-connexion des clients, et spécifie la capacité du client à traiter les fichiers hors-connexions provenant du partage. Les valeurs disponibles pour ce paramètre sont:

manual: Cette option active la mise en cache manuelle des fichiers. Seuls les fichiers qui seront identifiés manuellement par l'utilisateur utilisant le dossier partagé seront disponibles hors connexion. Il s'agit de l'option par défaut.

programs: Cette option active la mise en cache automatique des programmes. Elle permet un accès hors connexion aux répertoires partagés contenant des fichiers lus, référencés ou exécutés sans être modifiés. Cette option a comme avantage de réduire le trafic réseau dans la mesure où les fichiers hors connexion sont ouverts directement.

documents: Cette option active la mise en cache automatique des documents. Tous les fichiers ouverts par l'utilisateur à partir du partage deviennent alors disponible hors connexion pour cet utilisateur.

disable: Cette option désactive la mise en cache automatique du côté serveur, empêchant du coup le client d'utiliser ces fichiers hors connexion.

Si vous prévoyez utiliser les fichiers hors-connexion pour effectuer des synchronisations avec des portables, définissez le paramètre *csc policy* à la valeur *manual*.

NOTES

