

Créer vos propres définitions correspondances de lecteur réseau.

- N'utiliser pas les lettres D, E, F et G pour les lecteurs réseaux, car ils pourraient entrer en conflit avec les lecteurs locaux (IDE, SCSI ou USB) des postes de travail.
- Ne créer pas de mappage de lecteur réseau directement sur le poste de travail. Assigner les plutôt par un script dans le partage netlogon, cela facilitera leur gestion.

Il est important que vous fassiez la planification de votre structure de répertoire qui recevra les partages. Vous devez vous poser certaines questions, tel que:

- Quels sont les permissions nécessaires sur les partages.
- Y a-t-il un croisement dans la structure de répertoire utilisé par les partages.

Application des permissions

Manipulation des fichiers et répertoires du serveur de fichiers

La population de document sur un partage réseau sous Samba doit toujours se faire par l'intermédiaire d'un client Samba. Si le répertoire est partagé après que les documents soient dans le partage, il est fort probable que les permissions soient incorrectes.

Il va de même pour les modifications des fichiers partagés qui doivent toujours passer par l'intermédiaire d'un client Samba. Une copie ou une modification autre que par un client Samba, par exemple par un client SSH, entraînera une mauvaise assignation des permissions et des erreurs d'accès surviendront pour les clients.

Il est important de comprendre qu'un partage Samba est en fait un point d'entrée vers des ressources partagées. N'assigner donc pas d'autorisation directement sur le partage, mais faites le plus au niveau des ACL.

NOTES



Ordre d'application des permissions

L'ordre d'application des permissions pour un client accédant à un partage Samba sur une ressource sur un serveur Linux, se fera dans l'ordre suivant.

- Samba
- Posix
- ACL (EA)

L'application de base des permissions se font de la même façon que sur un partage sous Windows. Nous pouvons résumer grossièrement de cette façon: Les permissions plus permissives du côté du partage sont retenues, ensuite les permissions plus permissives du côté des permissions du système de fichier sont retenues, puis la plus restrictive des permissions de ces deux résultats sont appliqués pour l'utilisateur sur la ressource.

Plus restrictive 		
S A M B A ↓	P O S I X ↓	A C L ↓
Les permissions sont cumulatives sur le partage.	Les première permissions POSIX à correspondent sont appliquées, les autres sont immédiatement écartées.	Les ACL(EA) sont cumulatives.
Lecture/ Ecriture	Lecture/ Écriture/ Exécution	Lecture/ Écriture/ Exécution

C'est pour cette raison qu'il est important de ne pas assigner d'autorisation directement sur le partage, mais faites le plus au niveau des ACL. Cela vous donnera une plus grande latitude dans l'attribution des différentes permissions réelles sur la ressource.

NOTES



