

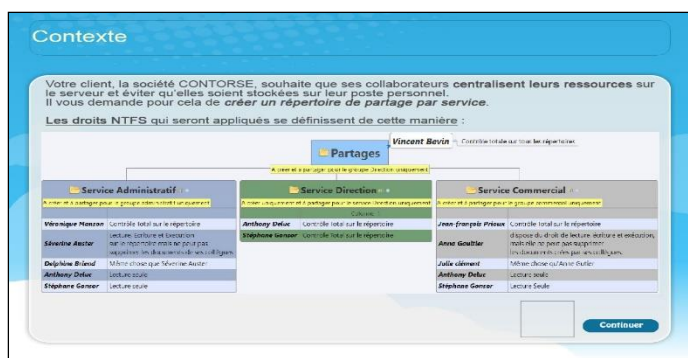
Paramétrer les partages

Objectifs

Les objectifs de cette mise en situation, sont de vous apprendre à :

- Partager des répertoires
- Paramétrer les ACL (Access Control List) NTFS
- Identifier les différences entre l'onglet partage et sécurité

Pour cela vous mettrez en place tous les partages décrits ici :



Votre client, la société CONTORSE, souhaite que ses collaborateurs centralisent leurs ressources sur le serveur pour éviter qu'elles soient stockées sur leur poste personnel. Il vous demande pour cela de créer un répertoire de partage par service.

Le tableau ci-dessous vous indique la liste des partages avec les droits NTFS à mettre en place.

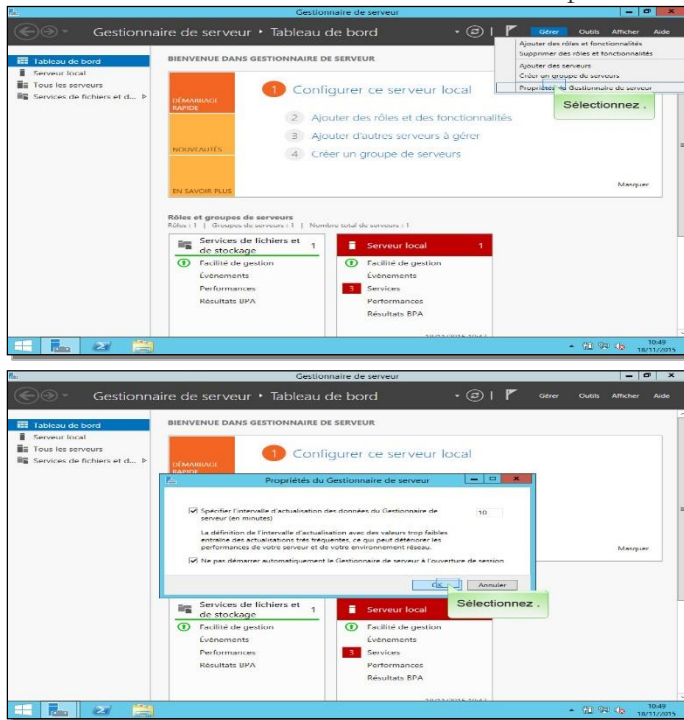
Désactiver l'ouverture du gestionnaire de serveur

Comme nous l'avons souligné précédemment, la fenêtre Gestionnaire du serveur s'ouvre automatiquement à l'ouverture de session.

Cet outil est assez lourd à se charger, notamment dû au fait que les informations sont actualisées lors de l'ouverture de session.

Toutefois, il est possible de désactiver son ouverture automatique.

Nous allons voir comment réaliser cette manipulation :



Pour ouvrir le gestionnaire de serveur, il suffira de cliquer sur son icône en bas à gauche de la barre des tâches.

Les partages administratifs

Durant l'installation de Windows Server 2012 des partages sont créés par le système.

Ces partages sont nommés Partages administratifs et Partages spéciaux.

Il existe 2 façons de visualiser ces partages

- soit en utilisant l'outil de gestion Dossiers Partagés disponible dans la Gestion de l'ordinateur
- soit en utilisant la commande Net share que nous allons voir

Dans le cours suivant, nous utiliserons l'outil Dossiers Partagés afin de contrôler nos partages.

Entrez la commande « net share » dans l'invite de commandes.

La commande net share permet d'afficher les répertoires partagés sur le serveur.

Mais elle permet également de créer et de supprimer un partage.

En saisissant la commande « net share /? » il est possible de voir toutes les options disponibles pour cette commande.

Tout Nom de partage se terminant par un \$ est un partage caché car il n'apparaît pas dans les partages disponibles pour les utilisateurs du réseau.

Par exemple, si je crée un répertoire toto et que je lui donne comme nom de partage toto\$ alors ce dossier partagé sera invisible pour les utilisateurs du réseau.

Le partage ADMIN\$ est utilisé lors de l'administration à distance.

Il permet d'accéder au répertoire Windows.

Comme pour le partage ADMIN\$, le partage C\$ permet aux administrateurs de se connecter à la racine du lecteur C:.

Le partage IPC\$ est exploité par les programmes pendant l'administration à distance et l'examen des ressources partagées.

En clair, le partage IPC\$ est utilisé par un client lorsqu'il veut envoyer une commande au serveur.

Cette commande peut simplement être la demande de la liste des partages disponibles sur la machine par exemple ou de démarrer un service.

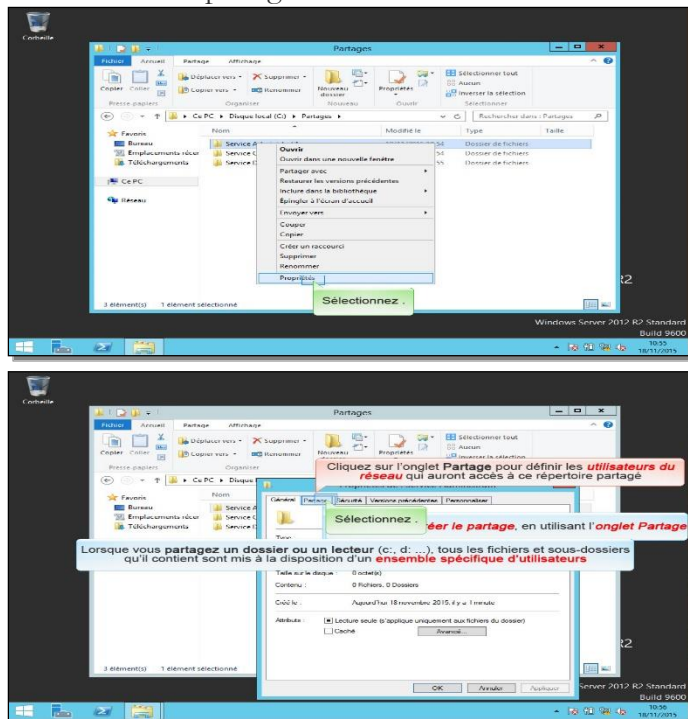
Il est important de savoir à quoi servent ces partages spéciaux afin d'éviter de les supprimer inutilement et de risquer de rendre le système instable.

Dans tous les cas, si un de ces partages est supprimé par erreur, il sera recréé au prochain redémarrage du serveur.

Nous allons maintenant créer nos répertoires et les partager conformément au cahier des charges.

Créer les partages

Pour commencer, créez tous les répertoires qui devront être partagés.
Voici comment partager un dossier :



Pour partager un répertoire et le rendre accessible aux utilisateurs du réseau, il faut d'abord créer le partage, en utilisant l'onglet Partage.

Lorsque vous partagez un dossier ou un lecteur (c:, d: ...), tous les fichiers et sous-dossiers qu'il contient sont mis à la disposition d'un ensemble spécifique d'utilisateurs.
Cliquez sur l'onglet Partage pour définir les utilisateurs du réseau qui auront accès à ce répertoire partagé.

L'onglet Partage nous propose de partager notre répertoire en utilisant un assistant qui est très simple d'accès mais limité dans les choix.

Cela évite aux personnes qui ne sont pas sensibilisées à la gestion des partages de faire des erreurs de paramétrage pouvant amener certaines personnes à accéder à des répertoires partagés auxquels elles ne doivent pas avoir accès.

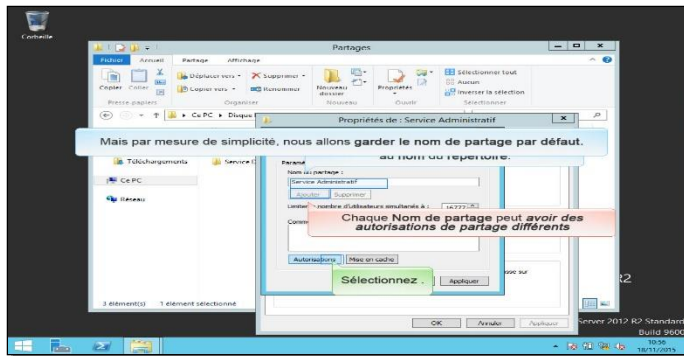
Mais pour ce cours, nous allons utiliser « Partage avancé », car il va vous permettre de comprendre comment fonctionnent les partages d'une part et d'autre part il offre beaucoup de choix dans la gestion des partages.

Enfin, remarquez le conseil de Windows qui vous dit que si un utilisateur doit accéder à un partage, il doit absolument avoir un mot de passe défini sur son compte.

En effet, pour des raisons de sécurité, un utilisateur qui n'a pas de mot de passe sur son profil ne pourra accéder à aucun partage réseau.

Nous allons maintenant mettre en place notre partage.

Paramétrer les partages



Par défaut, le nom de partage est identique au nom du répertoire.
 Toutefois, il est possible de donner plusieurs Noms de partage à un dossier.
 Chaque Nom de partage peut avoir des autorisations de partage différentes.
 Mais par mesure de simplicité, nous allons garder le nom de partage par défaut.

Quand on crée un partage, il est par défaut accessible à Tout le monde en Lecture.

Cela signifie que tous les utilisateurs du réseau peuvent consulter le contenu du répertoire partagé.

Le fait de définir des droits d'accès (ici Lecture) pour un utilisateur ou un groupe d'utilisateurs se nomme Jeu d'autorisation de partage.

Un jeu d'autorisation de partage concerne uniquement les droits de partage qui ont été définis sur l'onglet partage.

Nous allons maintenant définir qui aura le droit d'accéder à ce partage comme précisé dans le contexte.

Le cahier des charges précise que

- le groupe Service Administratif doit accéder en écriture à ce répertoire
- le groupe Service Direction doit avoir uniquement accès en Lecture
- l'administrateur doit avoir un accès en Contrôle total

C'est le travail de l'Administrateur d'assurer la maintenance de ces répertoires.

Il doit être en mesure de supprimer des répertoires, de modifier des droits d'accès lorsque l'on lui demande.

C'est la raison pour laquelle il doit avoir le droit Contrôle Total sur tous les répertoires partagés.

Pour que tous les utilisateurs n'aient pas accès en lecture à ce répertoire, il faut supprimer le groupe Tout le monde de la liste des autorisations.

Significations des droits à attribuer

Avec l'autorisation **Lecture**, les utilisateurs peuvent :

- Afficher les noms des fichiers et des sous-dossiers
- Accéder aux sous-dossiers du partage
- Lire les données et les attributs des fichiers
- Exécuter des fichiers programmes

Avec l'autorisation **Modifier**, les utilisateurs disposent des autorisations de Lecture, ainsi que du droit de :

- Créer des fichiers et des sous-dossiers
- Modifier les fichiers
- Modifier les attributs des fichiers et des sous-dossiers
- Supprimer des fichiers et des sous-dossiers

Avec l'autorisation **Contrôle total**, les utilisateurs bénéficient des autorisations précédentes ainsi que du droit de :

- Modifier les autorisations des fichiers et des sous-dossiers.
- S'approprier des fichiers et des sous-dossiers.

Comme les employés du groupe Administratif doivent pouvoir créer des documents, nous leur appliquons le droit de Modification

Onglet sécurité

Attention et nous insistons fortement sur ce point, l'onglet Partage concerne uniquement les personnes qui accèdent au partage à travers le réseau.

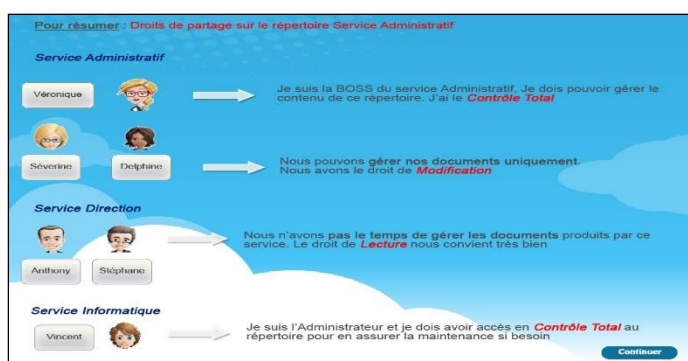
Si un utilisateur (autre que ceux définis dans l'onglet partage) se connecte physiquement sur le serveur, il aura quand même accès au répertoire.

Pourquoi me direz-vous ?

C'est très simple, tous les accès à des répertoires locaux sont gérés par l'onglet Sécurité. C'est donc l'onglet sécurité qui va se charger de vérifier si un utilisateur local a le droit d'accéder à ce répertoire.

Il faut retenir et c'est très important, que l'onglet partage sert uniquement à définir quels sont les utilisateurs du réseau qui auront accès à ce répertoire partagé.

Alors que l'onglet sécurité va se charger de répondre à cette question : « Qui est-ce qui a le droit d'écrire sur mon système de fichiers ? ».



Nous venons de préciser dans l'onglet partage quels sont les utilisateurs qui peuvent accéder à ce répertoire partagé.

Nous avons pu voir que les droits proposés sont un peu limités.

En effet, les droits de partage se limitent à Lecture, Modification et Contrôle Total.

Hors dans le contexte, il est précisé qu'il est interdit que les utilisatrices Séverine Auster et Delphine Briend puissent supprimer les documents qui ne leur appartiennent pas.

C'est l'onglet Sécurité qui va nous permettre de réaliser cela.

Notons que l'onglet Sécurité est disponible uniquement sur un système de fichiers NTFS.

Très régulièrement, on emploie le terme ACL NTFS quand on parle de l'onglet sécurité.

ACL signifie Access Control List.

En clair une ACL est tout simplement une liste d'autorisation d'accès qui définit les entités (personnes, groupes) qui ont des droits sur le répertoire et quels sont ces droits.

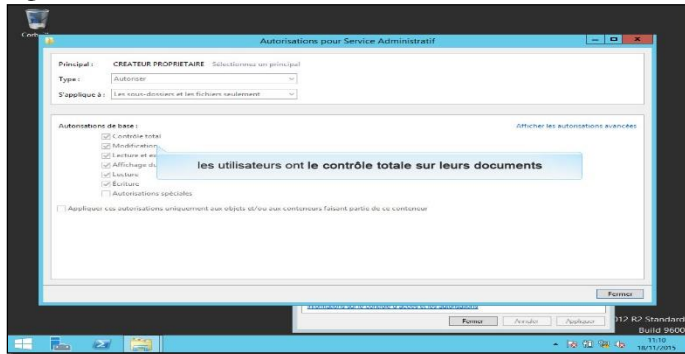
Par défaut, un certain nombre de groupes sont déjà présents et chacun dispose d'autorisations qui lui sont propres.

Comme son nom l'indique, le groupe CREATEUR PROPRIETAIRE permet de définir des droits de paternité.

Cela signifie que si une secrétaire crée un document, alors le groupe CREATEUR PROPRIETAIRE la désigne comme Propriétaire du document.

A moins d'avoir le droit de « Contrôle Totale », il n'est pas possible de supprimer un document dont vous n'êtes pas le propriétaire.

Pour chaque groupe, il est possible de voir quels sont les droits qui lui sont attribués sur ce répertoire.



Le groupe CREATEUR PROPRIETAIRE a les droits de « Contrôle Total ».

Ce qui signifie que grâce à ce groupe les utilisateurs ont le contrôle total sur leurs documents.

Le groupe SYSTEM est utilisé par le système d'exploitation ou par les services (sauvegarde, tâches planifiées, indexation...). Il ne doit pas être supprimé.

Le groupe Administrateurs a tous les droits sur le répertoire et peut donc supprimer les documents créés par d'autres personnes.

Pour rappel, l'utilisateur Vincent Bevin appartient au groupe Administrateurs.

Mais peut-être vous posez vous cette question :

Pourquoi avoir ajouté l'utilisateur Vincent BEVIN dans l'onglet partages alors que le groupe Administrateur se trouve dans l'onglet Sécurité ?

Parce que si on ajoute pas Vincent Bevin dans l'onglet Partages, il ne pourra pas avoir accès au répertoire partagé à travers le réseau.

Le groupe Utilisateurs possède certains droits par défaut.

Pour rappel, les membres du groupe Administratif sont également membre du groupe Utilisateurs.

Cela signifie que les droits qui seront appliqués aux membres du groupe du service Administratif seront ceux du groupe Utilisateurs.

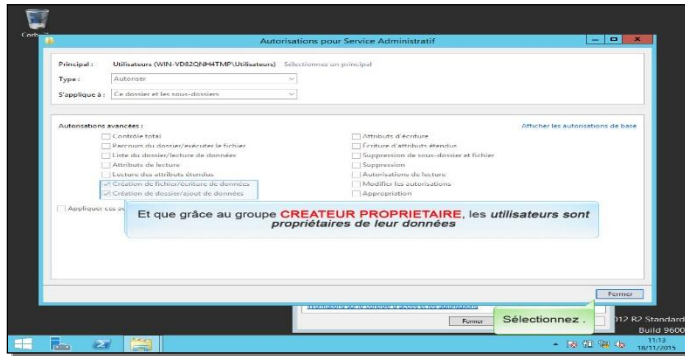
Le groupe Service Administratif étant un groupe créé par nos soins. Il ne possède pas de droits particuliers.

Seuls les groupes créés par le système d'exploitation ont des droits prédéfinis.

Donc normalement, Véronique et ses collègues ne devraient pas avoir le droit d'écrire sur le disque dur du serveur car le groupe Utilisateurs n'a pas l'autorisation d'écriture.

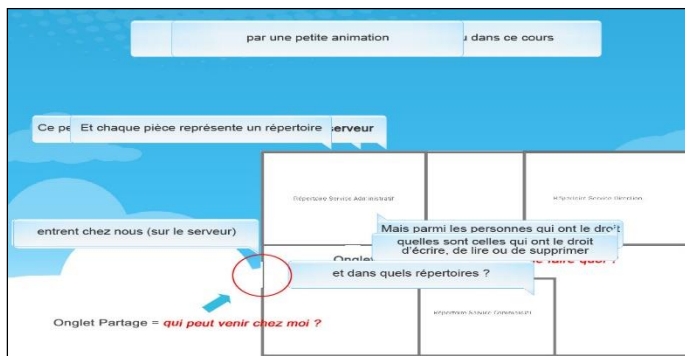
Si on descend l'ascenseur, on remarque que Autorisations spéciales est coché.

Regardons ce qu'il contient.



On peut voir que les personnes appartenant au groupe Utilisateurs peuvent créer des fichiers et des dossiers et que grâce au groupe CREATEUR PROPRIETAIRE, les utilisateurs sont propriétaires de leurs données.

Synthèse



Comme la gestion des droits de partage et de sécurité peut sembler complexe au 1er abord, nous allons illustrer ce que nous avons vu dans ce cours par une analogie.

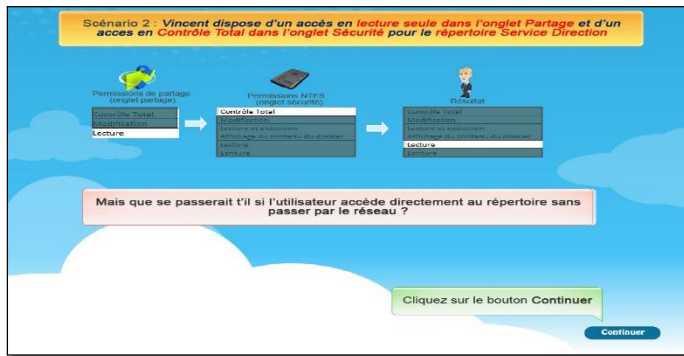
Ce petit carré représente une maison avec des pièces.
 Cette maison, c'est le disque dur du serveur.
 Et chaque pièce représente un répertoire.

La porte d'entrée correspond à l'onglet partage :

- Il va effectuer un 1er filtrage.
- On ne souhaite pas que toutes les personnes venant de l'extérieur entrent chez nous (sur le serveur)

Mais parmi les personnes qui ont le droit d'accéder au serveur, l'onglet sécurité définit :

- qui a le droit de faire quoi ? et dans quels répertoires ?
- quels sont ceux qui ont le droit d'écrire, de lire ou de supprimer ?



Si l'utilisateur accède depuis le réseau, c'est le droit le plus restrictif qui s'applique.

Dans ce cas il ne peut pas écrire.

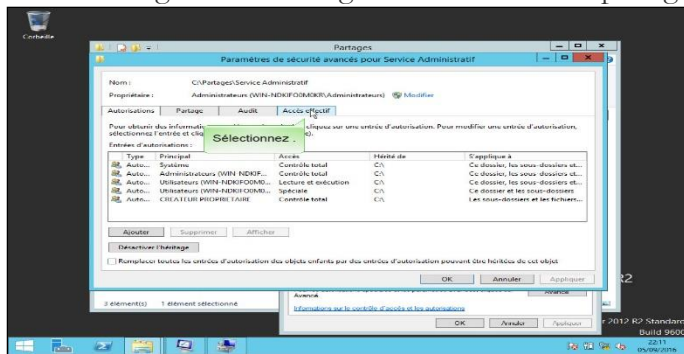
S'il accède directement au répertoire depuis une session sur le serveur il a le droit d'écrire, puisque seuls les droits NTFS s'appliquent.

Vérifier les autorisations effectives

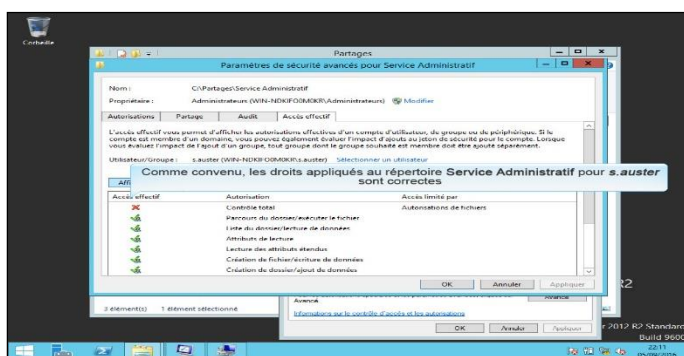
Dans Windows server 2012, une nouvelle fonctionnalité est apparue.

Elle permet de voir quels sont les droits qui seront appliqués à un utilisateur sur un répertoire.

Cela facilite grandement la gestion des droits de partage/sécurité.



Nous allons vérifier que l'utilisatrice v.manson possède bien tous les droits sur le répertoire comme indiqué dans le cahier des charges.



Conclusion

Ce cours sur les Partages et droits NTFS dans un environnement Workgroup est à présent terminé.

Nous avons pu voir que pour qu'un répertoire soit accessible à travers le réseau, il faut le partager. Mais il faut se poser la question : avec qui dois-je le partager et quelles permissions de partage je dois activer ?

Au-delà des permissions de partage, nous avons pu voir que les permissions NTFS, ou ACL NTFS ne concernent que les accès locaux sur les répertoires.

On peut alors imaginer en disant que pour accéder à un répertoire situé sur le serveur à travers le réseau, on doit passer par 2 SAS.

- 1 SAS réseau qui filtre dès le début les utilisateurs qui ont le droit d'accès au répertoire
- 1 SAS local qui vérifie parmi ces utilisateurs ceux qui peuvent écrire ou pas

Dans le cours suivant, nous allons voir comment tester l'accès à ces partages à travers une machine cliente.