Comment sécuriser, partager, sauvegarder et restaurer des fichiers dans un environnement informatique en groupe de travail

1 PRESENTATION DE CE DOCUMENT :

1.1 Où trouver ce document :

Ce document a été écrit par M. Guillaume MATHIEU. Une version électronique est disponible sur http://msreport.free.fr.
Une version au format PDF peut être téléchargée à l'adresse suivante :
http://msreport.free.fr/articles/Secure_share_audit_save_restore_data_workgroup.pdf

1.2 Objectifs de document :

Ce document explique comment sécuriser, partager, auditer, sauvegarder et restaurer des données dans un environnement en groupe de travail.
Il s'adresse tout particulièrement à des TPE (moins de 10 personnes) dont le budget n'est pas suffisant pour acheter un serveur Windows 2003 / Windows 2008 et une solution de sauvegarde.

2 SECURISATION ET PARTAGE DES DONNEES

2.1 Pré-requis :

2.1.1 Vérification version du système d'exploitation :

Afin de mettre en œuvre cette solution de sécurisation et de partage de dossier, il faut être sous Windows XP Pro SP2 et/ou Windows 2000 Pro.
Pour connaître la version de Windows, aller dans Démarrer | Exécuter puis taper « *Winver* ».

2.1.2 Tableau d'information à remplir par le chef d'entreprise :

Le chef d'entreprise doit remplir ce tableau afin de valider son besoin (quelles données doivent être partagées).

Prénom / Nom (pour chaque personne qui accède à la ressource)	Ressources / données	Niveau d'accès

2.1.3 Configuration du ou des disques où les données sont situées :

Attention, on ne peut sécuriser des dossiers / fichiers que si les partitions sont formatées en NTFS. Si ce n'est pas le cas, il est possible de convertir une partition FAT32 en NTFS avec l'outil « *convert* » **sans perdre les données sur la partition FAT32**.
Pour convertir un disque c:\ de FAT32 vers NTFS, aller dans *Démarrer* | *Exécuter* puis taper *cmd*.
Dans l'invite de commande Windows, taper la commande
convert c: /FS :NTFS
La capture d'écran ci-dessous montre la commande à taper pour convertir la partition E en FAT32 vers le format de fichiers NTFS.

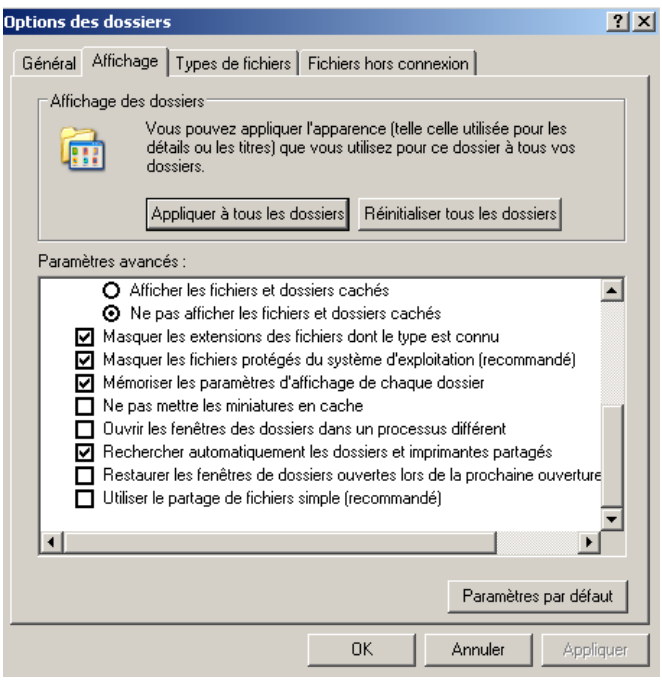
```
C:\Documents and Settings\Administrateur>convert e: /fs:NTFS
Le type du système de fichiers est FAT32.
Entrez le nom de volume en cours pour le lecteur E: Nouveau nom
Volume NOUVEAU NOM a créé 27/01/2009 15:24
Le numéro de série du volume est DCFA-6576
Windows vérifie les fichiers et les dossiers...
Vérification des fichiers et des dossiers terminée.
Windows a vérifié le système de fichiers sans trouver de problème.
    8 369 532 Ko d'espace disque au total.
    8 369 528 Ko sont disponibles.

        4 096 octets dans chaque unité d'allocation.
    2 092 383 unités d'allocation au total sur le disque.
    2 092 382 unités d'allocation disponibles sur le disque.
```

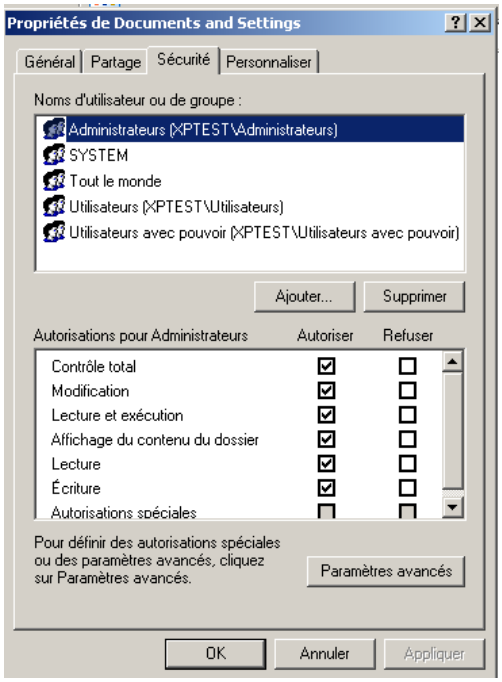
Remarque :
- La conversion du disque C ne pourra se faire qu'au redémarrage de la machine.
- Il est nécessaire de taper le nom du disque pour le convertir vers le format NTFS (vérification avant conversion).

- La commande *CONVERT* ne permet pas de passer de convertir une partition NTFS en une partition FAT32. Il est nécessaire de reformater la partition (sauvegarder les données avant formatage)

2.1.4 Désactivation du partage de fichiers simples

Au niveau de l'explorateur Windows, aller dans le menu « *Outils* » | « *Options des dossiers* » puis cliquer au niveau de l'onglet « *Affichage* ».
L'onglet « *Sécurité* » apparaît alors au niveau des propriétés d'un dossier.

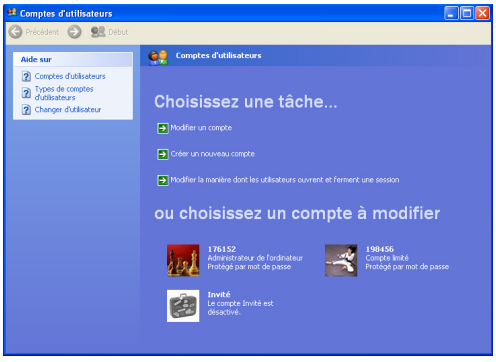


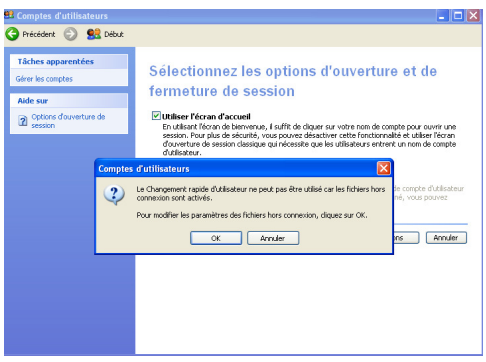


Remarque :
- Le « *Partage de fichiers simple* » ne peut pas être désactivé sous Windows XP Home.

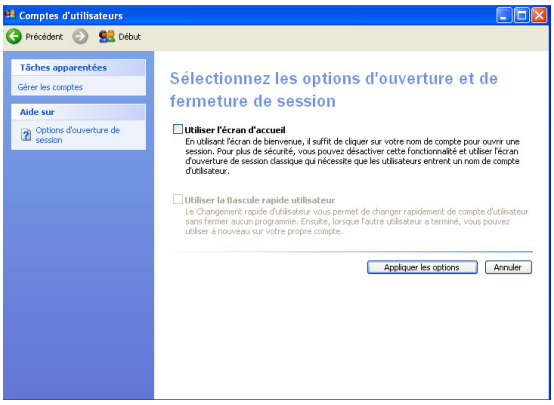
2.1.5 Désactivation de l'écran d'accueil de Windows XP :

L'écran d'accueil de Windows permet d'afficher les comptes utilisateurs de la base SAM local du Windows XP sous forme d'icône sur laquelle on clique. Cela permet de n'avoir à retenir que le mot de passe et non le nom d'ouverture de session (login).
Cependant quand on dispose d'un grand nombre de compte, il peut s'avérer désagréable de voir s'afficher le nom de tous les comptes utilisateurs.
Pour cette raison, PROSERVIA vous préconise de désactiver l'écran d'accueil sur les stations de travail Windows XP Pro qui vont servir de serveurs de fichiers.
Pour cela, dans le panneau de configuration, aller dans « *Démarrer* » | « *Panneau de Configuration* » | « *Comptes Utilisateurs* ».
Cliquer sur « *Modifier la manière dont les utilisateurs ouvrent et ferment une session* ».
Cliquer sur « Annuler » au niveau de la boîte de dialogue pour les paramètres des fichiers hors connexion.





Décocher la case « *Utiliser l'écran d'accueil* » et cliquer sur « *Appliquer les options* ».



2.1.6 Configuration du pare feu :

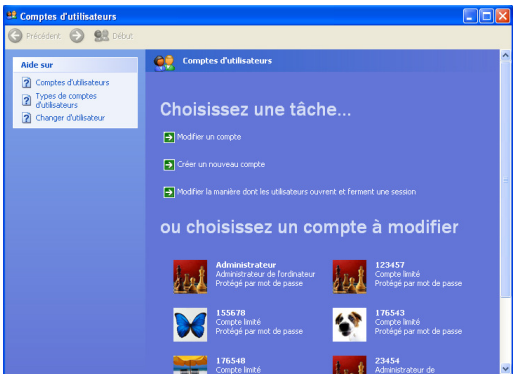
Le pare feu doit être activé mais configuré avec comme exceptions entre le service de « *Partage de fichiers et d'imprimantes* ».
Pour cela, aller dans « *Démarrer* » | « *Panneau de configuration* » puis double cliquer sur « *Pare feu Windows* ». Au niveau de l'onglet « *Général* », le pare feu doit être activé.
Au niveau de l'onglet « *Exceptions* », les programmes et services suivants doivent être cochés :

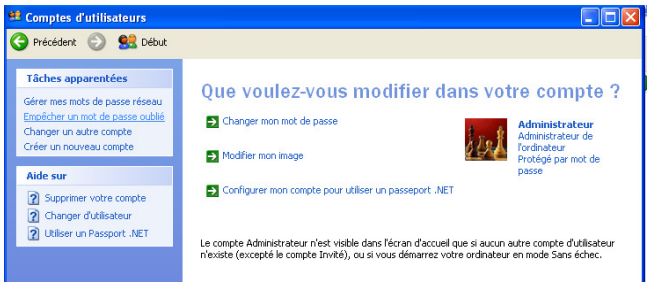
- Partage de fichiers et d'imprimantes : pour faire permettre l'accès distant aux fichiers partagés.

2.1.7 Définir un mot de passe pour le compte administrateur sur la station qui partage les données :

Ouvrir une session avec le compte « <u>administrateur</u> ».
Si celui-ci ne s'affiche pas à l'ouverture de session (en mode écran d'accueil Windows XP Pro, faire la combinaison de touches suivantes au clavier ***<u>CTRL ALT SUPPR</u>***.
Cela permet d'afficher l'écran d'accueil standard de Windows.

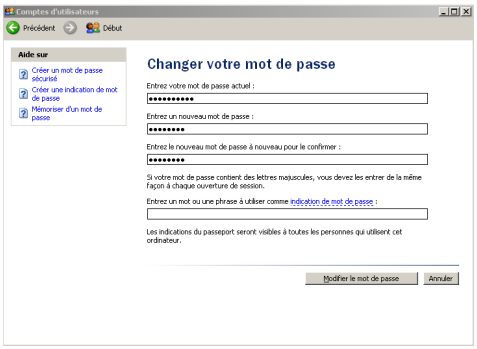
Une fois la session « *administrateur* » ouverte, aller dans « *Démarrer* » | « *Panneau de Configuration* » | « *Comptes Utilisateurs* ».





Sélectionner « *Administrateur* » puis cliquer sur « *Changer mon mot de passe* ».
Vous devez alors saisir votre ancien mot de passe puis le nouveau mot de passe.

Attention cette étape est différente d'une réinitialisation d'un mot de passe (qui fait perdre l'accès aux données chiffrées avec EFS) car on doit saisir son ancien mot de passe (pas de perte de données chiffrées avec EFS dans le cas d'un changement de mot de passe).



Remarque :

- **<u>Il est nécessaire d'appliquer cette procédure car une réinitialisation d'un mot de passe peut empêcher l'accès aux fichiers chiffrés avec EFS (la récupération des données perdues n'est pas toujours possible mais toujours couteuse).</u>**

2.2 Procédure pour sécuriser et partager des dossiers sur une station de travail Windows XP Pro :

2.2.1 Création d'un dossier :

Sur chaque station de travail jouant le rôle de serveurs de fichiers, aux deux répertoires sont à créer à la racine de C selon la convention de nommage :

- Service_lecture
- Service_modifiable

Attention, le déplacement d'un fichier dans ces répertoires conserve les anciennes permissions. Il sera nécessaire de réactiver l'héritage sur les fichiers en cas de problème d'accès.

2.2.2 Création des comptes utilisateurs des utilisateurs qui doivent accéder aux 2 dossiers sur le serveur de fichiers Windows XP :

Il faut créer les comptes utilisateurs de tous les utilisateurs qui vont accéder à ce serveur de fichiers.
Pour cela, aller dans *Démarrer* | *Panneau de configuration* | *Outils d'administration* | *Gestion de l'ordinateur*.
Au niveau de la console « *Gestion de l'ordinateur* », aller dans « *Utilisateurs et groupes locaux* » | « *Utilisateurs* » *et faire un clic droit « Nouvel utilisateur » sur « Utilisateurs ».*
Configurer le compte pour que le mot de passe n'expire pas.

2.2.3 Créer des groupes et ajouter les utilisateurs aux groupes :

Si le niveau d'accès est le même pour tous les collaborateurs du responsable, créer un seul groupe.
Si le niveau d'accès est différent, créer un groupe par type d'accès.
Si les différences sont trop importantes, il faudra créer un groupe par type d'accès (lecture ou lecture / écriture) et pour chaque ressource.
Exemple complexe : 10 personnes dans un service qui n'ont pas les mêmes niveaux d'accès :

- User1, User2, User3, User4, User5 ont le droits de lecture uniquement sur le dossier Test1
- User6, User7, User8, User9, User10 ont le droit de lecture / écriture sur le dossier Test1
- User1, User2 ont le droit ont le droits de lecture uniquement sur le dossier Test2.
- User3, User4, User5, User6, User7, User8, User9, User10 ont le droit de lecture / écriture sur le dossier Test2.

La solution : 10 personnes dans un service qui n'ont pas les mêmes niveaux d'accès :
Créer 4 dossiers, 10 utilisateurs et 4 groupes et les configurer comme suit :

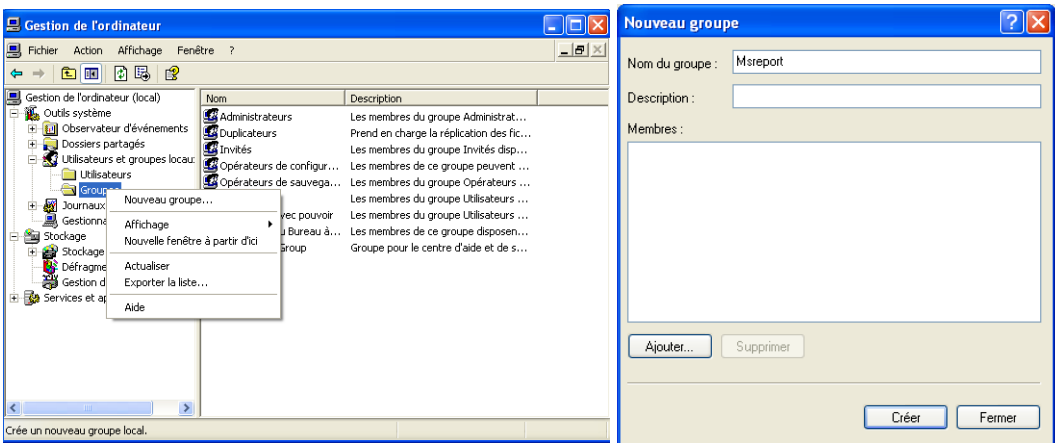
- Test1_Lecture : créer le groupe Test1_Lecture et ajouter les utilisateurs User1, User2, User3, User4, User5 dans ce groupe. Définir des permissions lecture pour le groupe Test1_Lecture sur le dossier Test1_Lecture.
- Test1_Modifiable : créer le groupe Test1_Modifiable et ajouter les utilisateurs User6, User7, User8, User9, User10 dans ce groupe. Définir des permissions Modifier (lecture / écriture) pour le groupe Test1_Modifiable sur le dossier Test1_Modifiable.
- Test2_Lecture : créer le groupe Test2_Lecture et ajouter les utilisateurs User1, User2 dans ce groupe. Définir des permissions lecture pour le groupe Test2_Lecture sur le dossier Test2_Lecture.
- Test2_Modifiable : créer le groupe Test2_Modifiable et ajouter les utilisateurs User3, User4, User5, User6, User7, User8, User9, User10 dans ce groupe. Définir des permissions Modifier (lecture / écriture) pour le groupe Test2_Modifiable sur le dossier Test2_Modifiable.

Déplacer/copier les données de TEST1 dans TEST1_Lecture ou TEST1_Modifiable
Déplacer/copier les données de TEST2 dans TEST2_Lecture ou TEST2_Modifiable

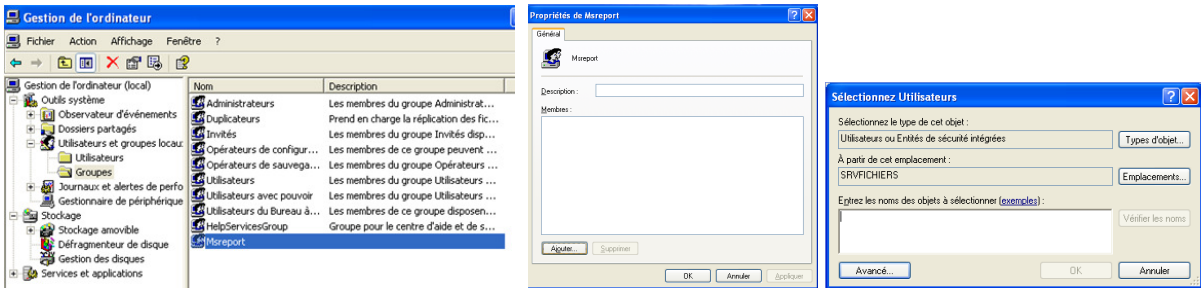
Remarque :

- **Attention, si vous fêtes un déplacement des données, les permissions du répertoire source sont conservées et peuvent être en contradiction avec le répertoire cible. Il faudra alors réinitialiser les permissions sur tous les dossiers enfants au niveau des dossiers TEST1_Lecture, TEST1_Modifiable, TEST2_Lecture ou TEST2_Modifiable. Voir paragraphe 1.2.5 de ce document.**

Procédure pour créer un groupe et ajouter les utilisateurs dans un groupe :
Créer un groupe pour identifier les utilisateurs (qui porte le nom du service).
Exemple : MSREPORT (ou compta…).



Pour ajouter les utilisateurs dans un groupe :
Aller dans « *Utilisateurs et Groupes* » | « *Groupes* » puis double cliquer sur le nom du groupe.
Cliquer sur « *Ajouter* » puis sur « *Avancé* » dans la fenêtre « *Sélectionner des utilisateurs* ».



Cliquer ensuite sur Rechercher et sélectionner les utilisateurs ajouter dans le groupe.
Cliquer sur OK deux fois pour valider la manipulation.

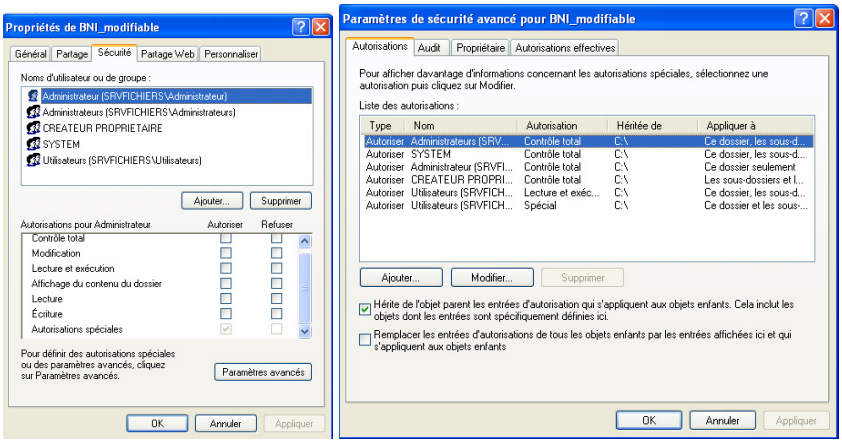
Remarque :
- Je peux sélectionner plusieurs comptes en maintenant la touche CTRL appuyée (sélection individuelle) ou la touche SHIFT (majuscule temporaire).

2.2.4 Définir des permissions :

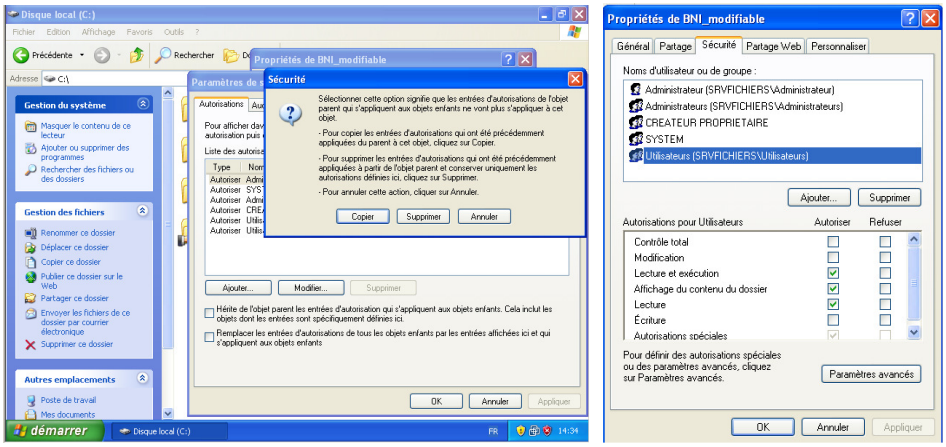
Une fois les groupes créés, il faut positionner les permissions au niveau des dossiers en utilisant les groupes que l'on vient de créer.
Pour cela, il faut commencer par supprimer l'héritage sur chaque dossier racine à partager (le premier dossier est pour l'accès en lecture, le deuxième dossier est pour l'accès en écriture).

Complément d'information sur l'héritage :
- L'héritage des permissions, c'est le fait qu'un dossier enfant hérite par défaut des permissions du dossier parent (dossier dans lequel il se trouve). Les permissions héritées apparaissent sous forme de cases grises que l'on ne peut pas modifiées au niveau de l'onglet « *Sécurité* ».

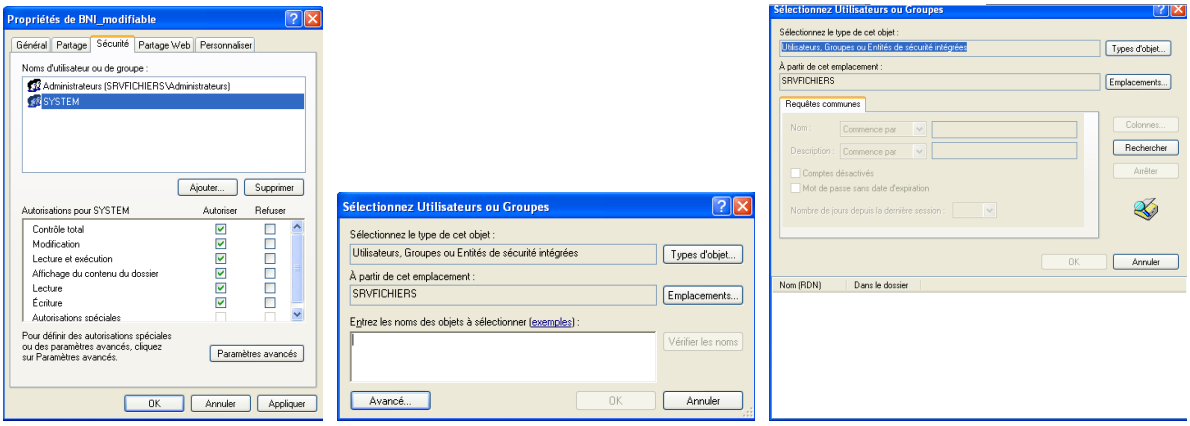
Pour supprimer l'héritage :
- Aller dans les propriétés de chaque dossier, onglet « *Sécurité* » :
- Cliquer sur « *Paramètres avancées* ».
- Décocher la case « *Hérite de l'objet parent les entrées d'autorisation qui s'appliquent aux objets enfants* ».

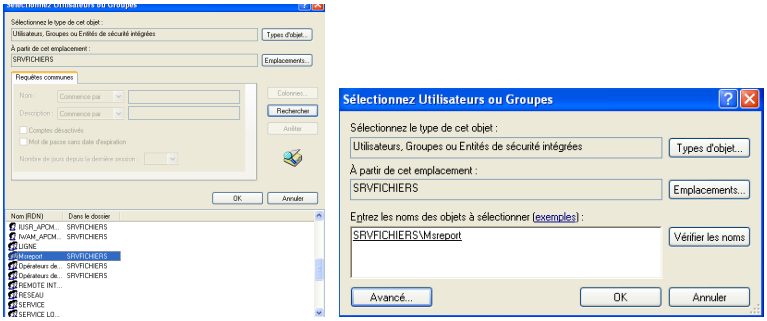


Cliquer ensuite sur « *Copier* » au niveau de la boîte de dialogue « *Sécurité* ».

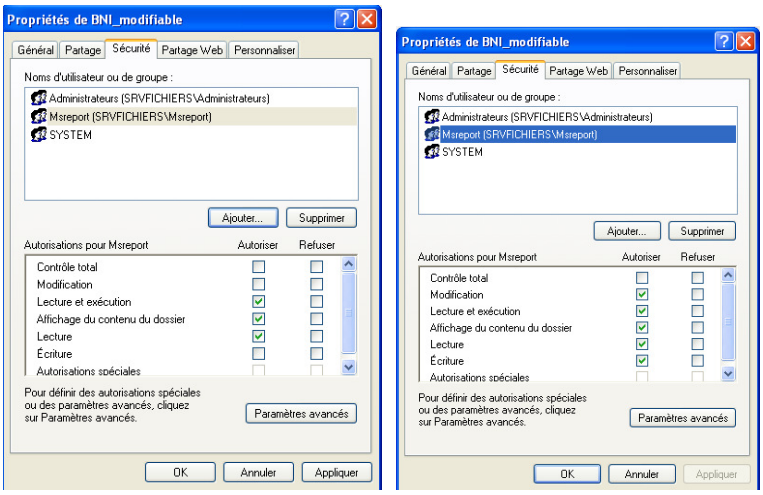


Il faut maintenant donner les bons droits (supprimer les groupes / utilisateurs qui n'ont pas à avoir accès à la ressource).
Par exemple, le groupe « *Utilisateurs* » n'a pas à avoir accès en lecture à ce dossier.
Il faut ensuite cliquer sur « *Ajouter* » au niveau de l'onglet Sécurité de la fenêtre « *Propriétés du dossier à partager / sécuriser* » et sélectionner **les groupes** à ajouter.





Le groupe apparaît alors dans l'onglet sécurité.
Attention par défaut le groupe (Msreport dans notre cas) récupère par défaut le droit en lecture sur le dossier.
Il faut le passer en modifier pour l'accès en lecture / écriture.



2.2.5 Réinitialiser des permissions sur les fichiers dans les dossiers:

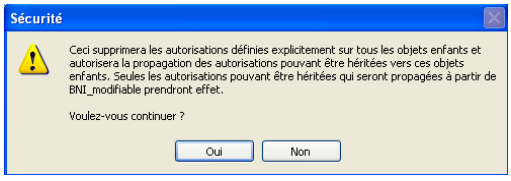
Attention, le déplacement (pas une copie) d'un fichier d'un répertoire source vers un répertoire cible (les deux répertoires étant sur la même partition) conserve les anciennes permissions. Il sera nécessaire de réactiver l'héritage sur les fichiers en cas de problème d'accès.

Soit deux dossiers :
- C:\Dossier1
- C:\Dossier1\deploy

Si je déplace le dossier « *deploy* » qui était sur le bureau de l'utilisateur dans le dossier C:\Dossier1, ce dossier « *deploy* » conserve ces droits et n'hérite pas des droits accordés sur le dossier C:\Dossier1.
Il faut donc aller sur le dossier C:\Dossier1 et forcer la réinitialisation des droits sur les dossiers.

Pour effectuer cela :
- Au niveau de l'onglet « *Sécurité* » du dossier Dossier1, cliquer sur « *Paramètres avancées* ».
- Cocher la case « *Remplacer les entrées d'autorisations de tous les objets enfants par les entrées affichées ici et qui s'appliquent aux objets enfants* ».

Cliquer ensuite sur « *Oui* » au niveau du message d'avertissement pour continuer.

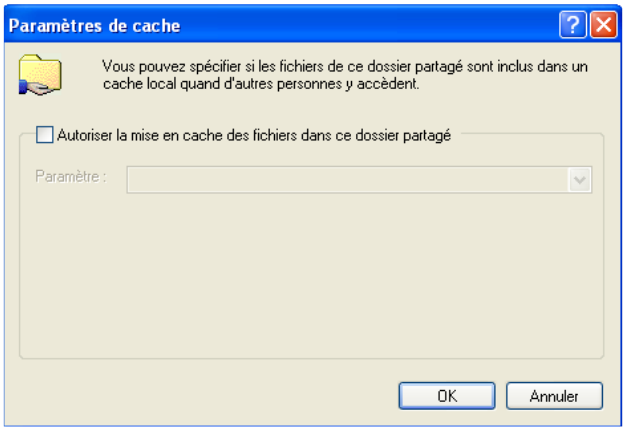


Le résultat est le suivant :
Les cases sont grisées au niveau du répertoire C:\Dossier1\deploy, ce qui montre que j'hérite du répertoire parent C:\Dossier1.

2.2.6 Partager le dossier :

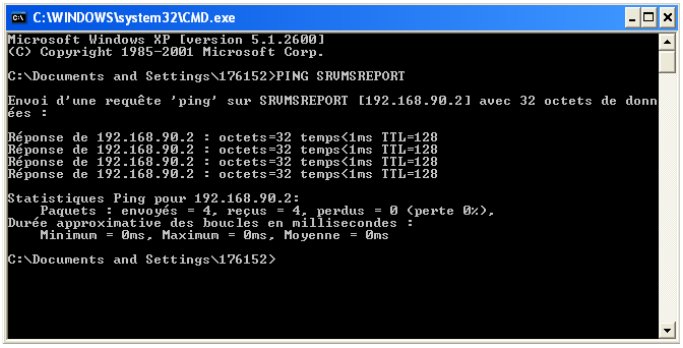
Il faut maintenant partager le dossier.
Pour cela :

- Aller dans les propriétés du dossier puis dans l'onglet « *Partage* ».
- Sélectionner « *Partager le dossier* ».
- Cliquer sur le bouton « *Mise en cache* ». Désactiver alors la mise en cache hors connexion.
- Cliquer ensuite sur le bouton « *Autorisations* ». **Quand on partage un dossier, on a par défaut le droit Lecture pour tout le monde.** Mettre « *Tout le monde* » en « *Contrôle Total* ». Les permissions qui s'appliquent réellement sont le cumul le plus restrictif entre les permissions NTFS et les permissions de partage. Donc il faut désactiver les permissions de partage pour simplifier l'administration (Contrôle Total pour tout le monde **au niveau des permissions de partage**).



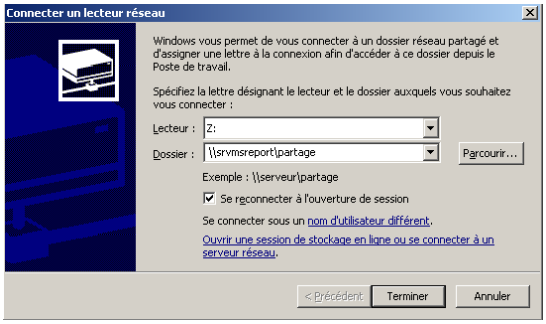
2.2.7 Accès aux données depuis une station de travail :

La première étape consiste à faire un test de connectivité réseau entre la station de travail et le serveur de fichier.
Pour cela, faire un ping du serveur de fichier.
Aller dans « *Démarrer* » | « *Exécuter* » puis taper « *cmd* » et lancer la commande « *ping nom_serveur* ». Vous devez alors obtenir « *Réponse de IP_serveur* » si tout marche bien.

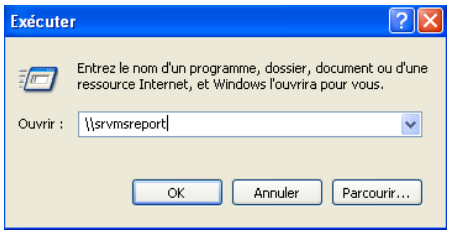


On peut accéder aux données partagées de plusieurs manières :

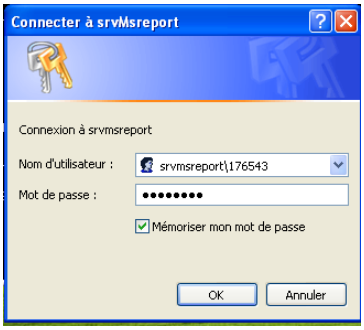
- Via le voisinage réseau. Aller dans l'icône voisinage sur le bureau (aussi accessible par « *Panneau de Configuration* » | « *Connexion Réseau* »).
- Via un lecteur réseau : cette méthode est **à bannir** en groupe de travail car vous ne pouvez pas avoir plus de **10 connexions simultanées** à une station de travail Windows XP Pro. Pour créer un lecteur réseau, lancer l'explorateur Windows puis aller dans le menu « *Outils* », « *Connecter un lecteur réseau* ». Il est possible de se connecter avant le compte d'un autre utilisateur.



- Via un raccourci sur le bureau. **C'est la méthode que l'on va utiliser (voir la suite de ce paragraphe).**
- En se connectant directement à la ressource : Pour cela, aller dans « *Démarrer* » | « *Exécuter* » et en tapant dans la fenêtre « *Exécuter* » \\nom_serveur_fichier\



Quelque soit la méthode, il faut s'authentifier car on est en groupe de travail, il n'y a donc pas de méthode d'authentification transparente. Bien saisir le nom de l'utilisateur sous cette forme :
Nom_serveur_fichiers\nom_d'utilisateur_sur_serveur_fichiers

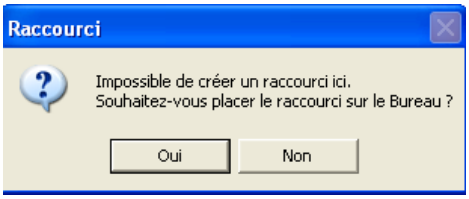


L'utilisateur doit en effet s'authentifier avec un compte qui a été créé sur le serveur de fichier (machine distante).
Cocher la case « *Mémoriser le mot de passe* ». Grâce à cette option, il ne sera plus nécessaire de s'authentifier à chaque accès au dossier partagé. Attention, en cas de changement de mots de passe, il faudra aller modifier la valeur enregistré (dans « *Gérer les mots de passe réseaux* ») (voir ci-dessous pour procédure)

Remarque :
- **Si à cette étape, vous avez un message « *Accès refusé* » au lieu de l'invite d'ouverture de session, désactiver le partage de fichier sur la station de travail Windows XP Pro (le client) et/ou changer le mot de passe du compte utilisateur sur le serveur de fichiers Windows XP Pro. Voir paragraphe 2.1.4 et 2.1.7.**
- Vous pouvez avoir un message « *Accès refusé* » après authentification mais cela indique que vous n'avez tout simplement pas assez de droits.

Une fois authentifiée, vous devez visualiser certains partages
- Double clique sur Dossier1
- Normalement, vous pouvez créer un dossier « *tests* ».

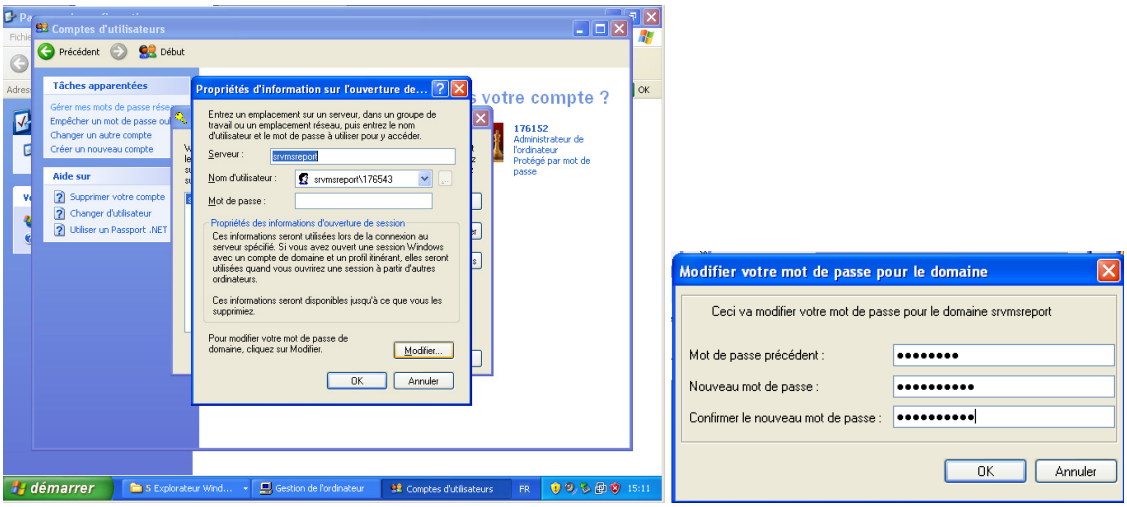
Sur le partage Dossier1, faire un clic droit et créer un raccourci.
Cliquer sur Oui



Renommer le raccourci et tester l'accès depuis ce raccourci.

Il faut maintenant demander à l'utilisateur de changer son mot de passe distant :
Aller dans « *Démarrer* » | « *Panneau de configuration* » | « *Comptes utilisateurs* ».
Cliquer sur l'utilisateur qui a sa session d'ouverte en cours.
On ne peut gérer les mots de passe réseau que pour l'utilisateur en cours de session.
Cliquer sur « *Gérer mes mots de passe réseau* ».

Dans la fenêtre « *Noms et mots de passe utilisateur enregistrés* », sélectionner le serveur de fichiers et cliquer sur « *Propriétés* », puis dans la fenêtre « *Propriétés d'information d'ouverture de session* » sur « *Modifier* ». Entrer l'ancien mot de passe et le nouveau.



Il est donc possible en groupe de travail de changer le mot de passe d'un compte utilisateur d'une autre base SAM !

2.3 Mise en place de l'audit des accès :

L'audit permet de filtrer les accès (réussite ou échec) à un dossier.
Nous allons voir comment journaliser :

- La création d'un nouveau fichier / dossier.
- La modification d'un fichier/dossier existant.
- La suppression d'un fichier / dossier existant.
- Le changement de propriétaire.
- Le changement de permissions.
- Le fait de renommer un dossier / fichier.

Les informations d'audit sont accessibles dans le journal « *Sécurité* » de Windows.
Attention, l'analyse de ce journal demeure complexe et nécessite une certaine maîtrise de Windows XP.

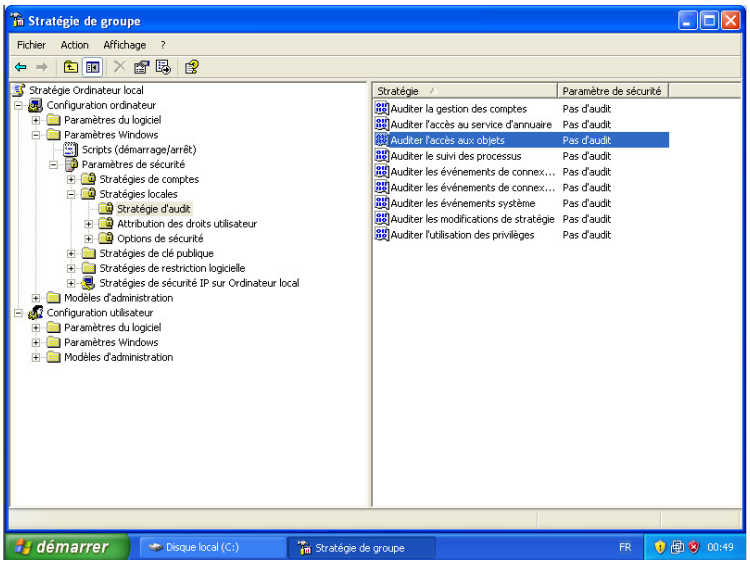
2.3.1 Procédure de mise en place :

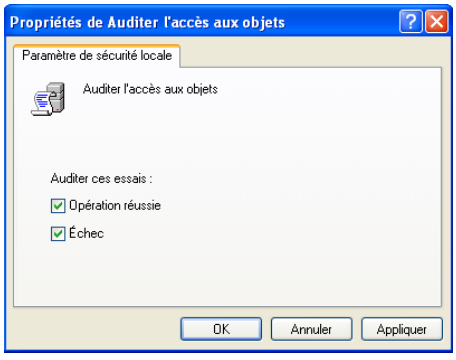
La mise en place de l'audit nécessite :

- L'activation de l'audit des objets dans les stratégies de groupe local de chaque station de travail Windows XP Pro qui joue le rôle d'un serveur de fichiers. Afin de ne pas surcharger l'audit nous n'activerons que l'audit sur les objets. Toutes les autres formes d'audit seront désactivées.
- Définir la taille du journal de sécurité. **Si celui-ci est plein, seuls les utilisateurs qui sont administrateurs pourront ouvrir une session sur la station de travail en local.**
- La définition de SACLS au niveau du dossier.

Pour activer l'audit des objets :

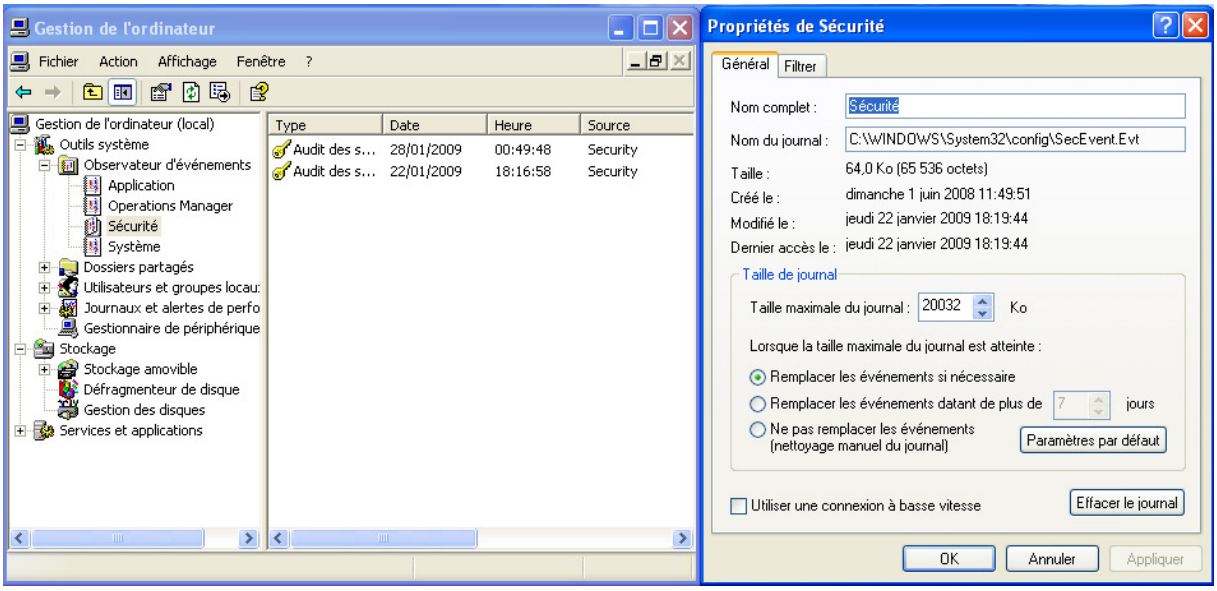
- Aller dans « *Démarrer* » | « *Exécuter* » et taper dans la commande « *gpedit.msc* ».
- Aller dans « *Configuration Ordinateur* » | « *Paramètres Windows* » | « *Paramètres de Sécurité* » | « *Stratégies locales* » | « *Stratégies d'audit* ». Double cliquer sur « *Auditer l'accès aux objets* ».





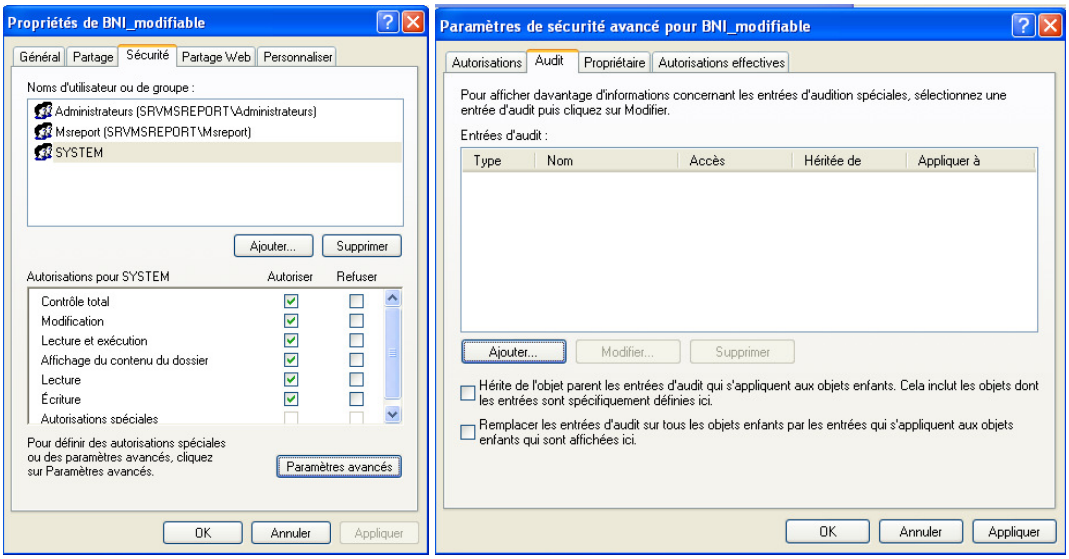
Pour définir la taille du journal de sécurité :

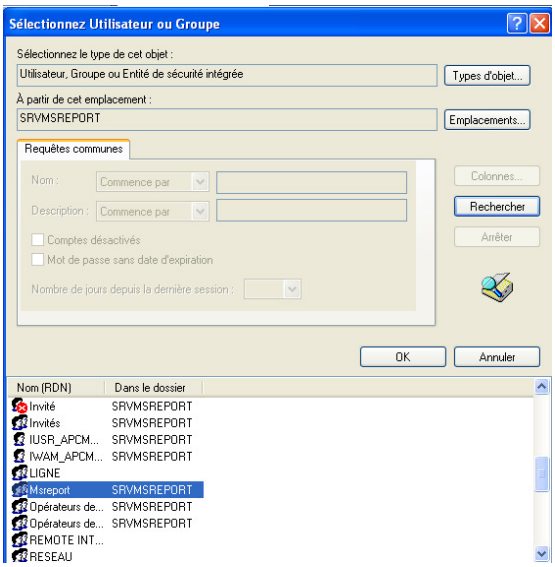
- Aller dans « *Démarrer* » | « *Panneau de Configuration* » | « *Outils d'administration* » puis cliquer sur « *Gestion de l'ordinateur* »
- Développer « *Outils Systèmes* » | « *Observateurs d'événements* » | « *Sécurité* ».
- Faire un clic droit, puis cliquer sur « *Propriétés* ».
- Dans la fenêtre, « *Propriétés de Sécurité* », modifier la valeur maximum du journal de sécurité et la définir sur 20032 Ko.
- **Définir le paramètre de remplacement sur « *Remplacer les événements si nécessaire* ». Il ne sera peut être pas possible de retrouver des actions remontant à plusieurs mois sur les dossiers mais on ne risque pas de bloquer l'ouverture de session en saturant le journal de sécurité.**

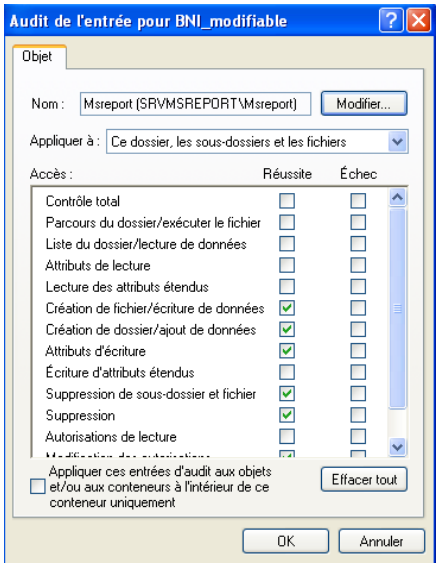


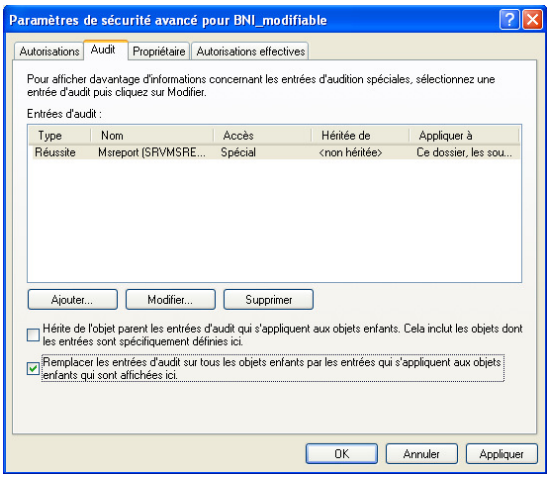
Définir les SACLS au niveau du répertoire à auditer (surveiller) :

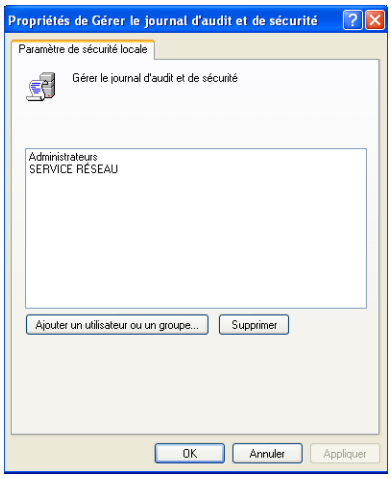
- Aller dans les propriétés du dossier, dans l'onglet « *Sécurité* ». Cliquer sur « *Paramètres avancées* ».
- Cliquer sur « *Ajouter* » et sélectionner le groupe (contenant les utilisateurs accédant à ce dossier) que l'on veut surveiller.
- Dans la fenêtre « *Audit de l'entrée pour Dossier1* », sélectionner les cases suivantes :
  - ✓ Création de fichiers / écritures de données
  - ✓ Création de dossiers / ajouts de données
  - ✓ Suppression
  - ✓ Suppression de sous dossier / fichiers
  - ✓ Modifications des permissions
  - ✓ Appropriation
- Sélectionner « *Remplacer les entrées d'audit sur tous les objets enfants par les entrées qui s'appliquent sur tous les objets enfants qui sont affichées ici* ».







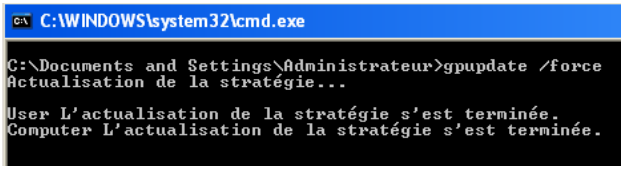




Remarque :

- Il est possible de définir qui peut gérer le journal sécurité dans les stratégies de groupe. Aller dans « *Démarrer* » | « *Exécuter* » et taper dans la commande « *gpedit.msc* ». Aller dans « *Configuration Ordinateur* » | « *Paramètres Windows* » | « *Paramètres de Sécurité* » | « *Stratégies locales* » | « *Attribution des droits utilisateur* » et configurer le paramètre « *Gérer le journal d'audit et de sécurité* ».

Actualiser les stratégies de groupe :
Aller dans « *Démarrer* » | « *Exécuter* » et taper « *cmd* ».
Dans la fenêtre invite de commande, taper la commande « *gpupdate /force* ».

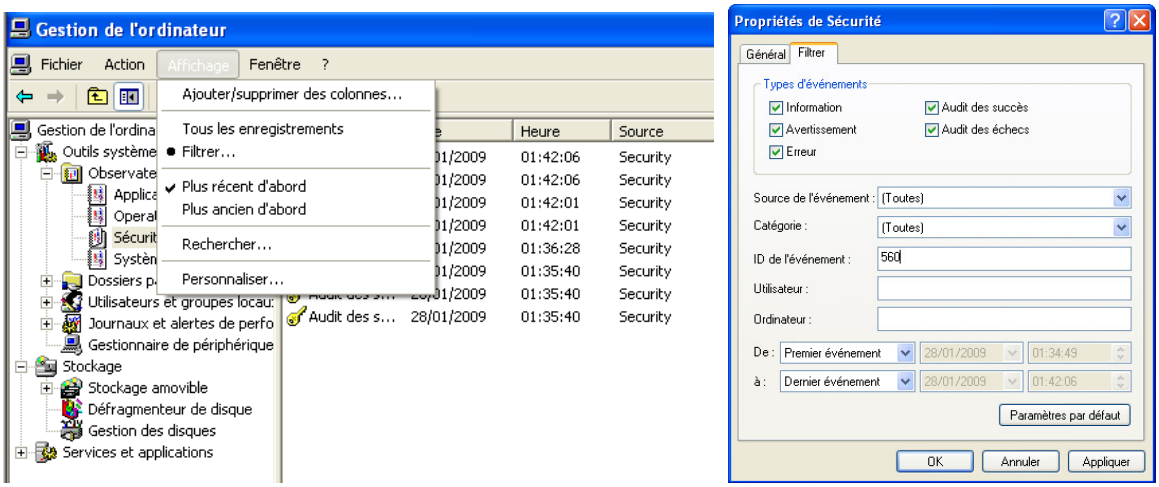


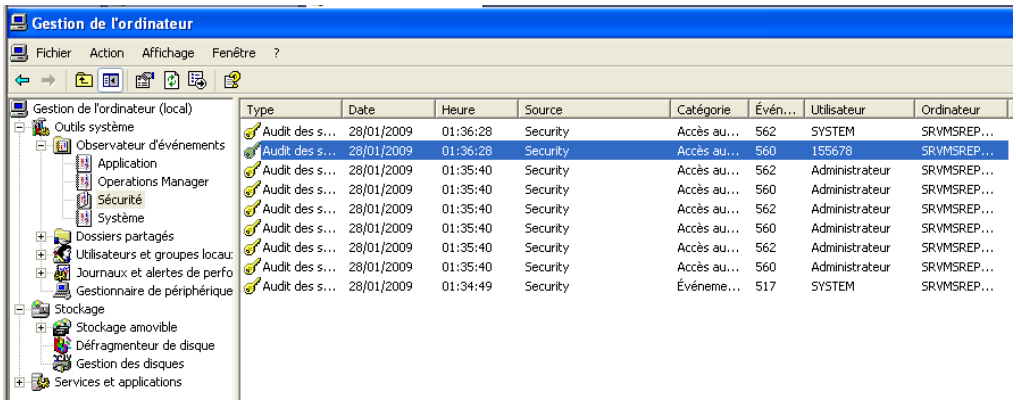
2.3.2 Exploitation de l'audit :

Si on crée un dossier dans le dossier « *Dossier1* » puis que l'on supprime ce dossier, on obtient 5 événements suivants dans le journal de sécurité.
Il faut en fait filtrer sur les événements avec un ID 560.
Pour cela :

- Aller dans « *Démarrer* » | « *Panneau de Configuration* » | « *Outils d'administration* » puis cliquer sur « *Gestion de l'ordinateur* ». Développer « *Outils Systèmes* » | « *Observateurs d'événements* ». Aller dans le menu « *Affichage* » et cliquer sur « *Filtrer* ».

- Dans « *ID de l'événement* », taper « *560* ».



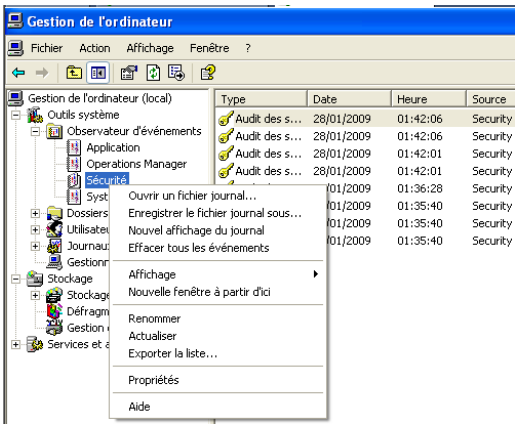


Type de l'événement : Audit des succès
Source de l'événement : Security
Catégorie de l'événement : Accès aux objets
ID de l'événement : 560
Date : 28/01/2009
Heure : 01:42:06
Utilisateur : SRVMSREPORT\155678
Ordinateur : SRVMSREPORT
Description :
Objet ouvert
Serveur de l'objet : Security
Type de l'objet : File
Nom de l'objet : C:\Dossier1\Nouveau dossier
Identificateur du handle : 1644
Identificateur de l'opération : {0,2356020}
Id. du processus : 3992
Nom du fichier image : C:\WINDOWS\explorer.exe
Utilisateur principal : 155678
Domaine principal : SRVMSREPORT
Id d'ouv. de session principale : (0x0,0x2268F5)
Utilisateur du client : -
Domaine du client : -
Id. d'ouv. de session client : -
Accès : DELETE
SYNCHRONIZE
ReadAttributes

Privilèges : -
Nombre de SID restreint : 0

2.3.3 Suppression du contenu du journal de sécurité :

Aller dans « *Démarrer* » | « *Panneau de Configuration* » | « *Outils d'administration* » puis cliquer sur « *Gestion de l'ordinateur* ». Développer « *Outils Systèmes* » | « *Observateurs d'événements* ».
Sur le journal, faire un clic droit et sélectionner « *Effacer les événements* ». Vous pouvez alors faire une sauvegarde.
Une entrée d'audit permet de savoir qui a modifié le journal.
Pour rappel, seul un administrateur peut par défaut gérer le journal d'audit.



Type de l'événement : Audit des succès
Source de l'événement : Security
Catégorie de l'événement : Événements système
ID de l'événement : 517
Date : 28/01/2009
Heure : 01:50:05
Utilisateur : AUTORITE NT\SYSTEM
Ordinateur : SRVMSREPORT
Description :
Le journal d'audit a été effacé
Utilisateur principal : SYSTEM
Domaine principal : AUTORITE NT
Id. de session principale : (0x0,0x3E7)
Utilisateur client : Administrateur
Domaine client : SRVMSREPORT
Id. de session client : (0x0,0x20934C)

3 SAUVEGARDE :

3.1 Pré-requis :

3.1.1 Tableau d'information à remplir par le chef d'entreprise :

Le chef d'entreprise doit remplir ce tableau afin de valider les dossiers / données **à sauvegarder**.

Ressources	Fréquence de sauvegarde	Emplacement de la sauvegarde	Personne en charge de la sauvegarde

3.1.2 Modification de mot de passe administrateur :

Les sauvegardes s'exécutent avec le compte administrateur. **Il ne faut donc plus modifier le mot de passe de ce compte sur les stations de travail qui sont sauvegardées ou cela nécessitera une reconfiguration de la tâche planifiée de sauvegarde.**

3.1.3 Pré-requis au niveau Windows XP :

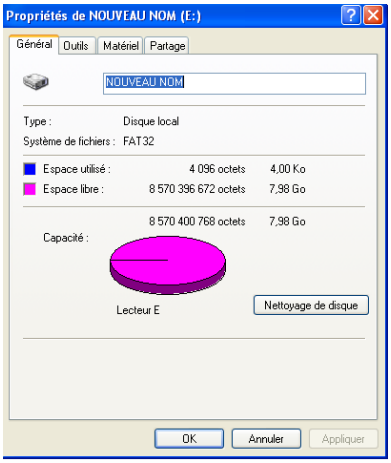
NTBACKUP est disponible uniquement sous Windows XP Pro.
Si vous voulez cependant lancer NTBACKUP depuis Windows XP Home, copier l'exécutable ntbackup.exe (dans c:\windows\system32 sur Windows XP Pro) dans c:\windows\system32 (sur le Windows XP Home).

3.1.4 Pré-requis au niveau des disques :

Il faut respecter les pré-requis suivants :

- Il faut au moins deux disques externes USB2 formatées en NTFS avec une étiquette (sauvegarde_semaine 1_nom_service ou sauvegarde_semaine 2_nom_service).
- Il doit y avoir une rotation des disques externes (un disque dans un coffre fort).
- En semaine 1, on sauvegarde sur le disque 1. Le disque 2 doit être dans un coffre fort hors de l'entreprise.
- Le disque externe semaine 1 doit avoir comme lettre de lecteur S.
- Le disque externe semaine 2 doit avoir comme lettre de lecteur T.
- Les 2 disques doivent avoir des noms différents sinon il y a des risques de problème avec les lettres de lecteur.
- Si le lecteur est en FAT32, il faut que je convertisse en NTFS pour pouvoir écrire des fichiers de plus de 4 Go.

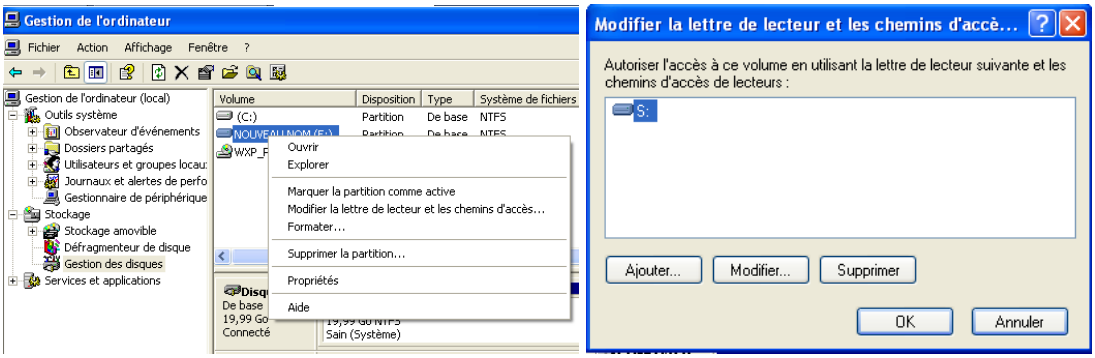
Pour convertir un disque en NTFS, voir paragraphe 1.1.2 de ce document.



Pour définir une lettre de lecteur (S ou T):

- Dans « Gestion de l'Ordinateur » | « Gestion des disques », sélectionner le disque et faire un clic droit puis aller dans « Modifier la lettre de lecteur et les chemins d'accès ».

- Cliquer sur modifier et sélectionner S ou T.



3.1.5 Politique de sauvegarde :

La sauvegarde des serveurs de fichiers se fera avec NTBACKUP sur des disques externes au format BKF.

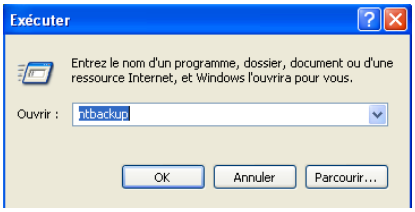
La politique de sauvegarde suivante peut être utilisée :

- Débrancher le disque dur 2 pour mise au coffre le lundi matin semaine 1
- Lundi soir semaine 1 : sauvegarde complète sur disque 1
- Mardi soir semaine 1 : sauvegarde différentielle sur disque 1
- Mercredi soir semaine 1 : sauvegarde différentielle sur disque 1
- Jeudi soir semaine 1 : sauvegarde différentielle sur disque 1
- Vendredi soir semaine 1 : sauvegarde différentielle sur disque 1
- Débrancher le disque dur 1, rebrancher le disque 2 (selon la semaine) le lundi matin
- Lundi soir semaine 2: sauvegarde complète sur disque 2
- Mardi soir semaine 2: sauvegarde différentielle sur disque 2
- Mercredi soir semaine 2: sauvegarde différentielle sur disque 2
- Jeudi soir semaine 2: sauvegarde différentielle sur disque 2
- Vendredi soir semaine 2: sauvegarde différentielle sur disque 2

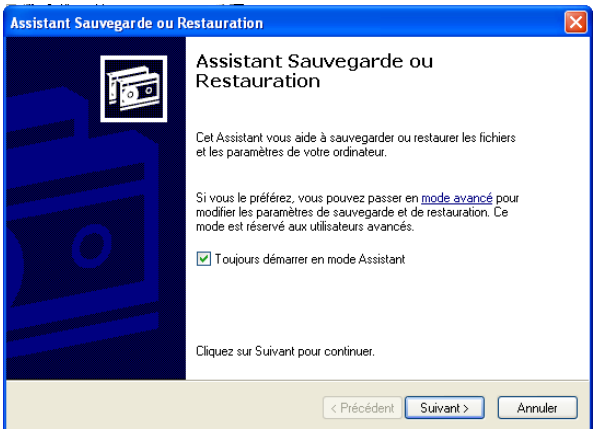
La sauvegarde mensuelle se fera sur le disque 1 (qui doit plus gros le disque 2) le premier lundi du mois à une heure différente de la sauvegarde quotidienne.
Les deux disques externes auront les lettres S et T pour éviter tout conflit avec des clés USB.

3.1.6 Procédure de sauvegarde :

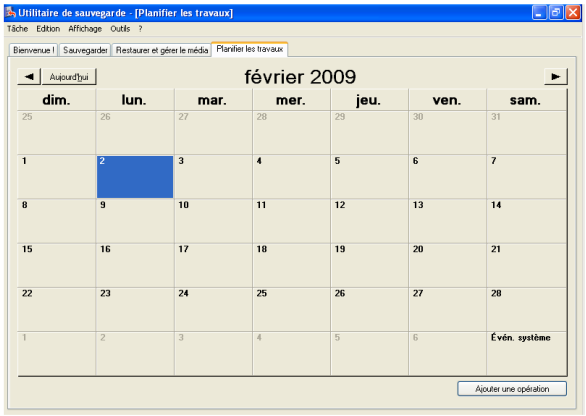
Aller dans « *Démarrer* » | « *Exécuter* » et taper « *ntbackup* ». Cliquer sur « *OK* ».



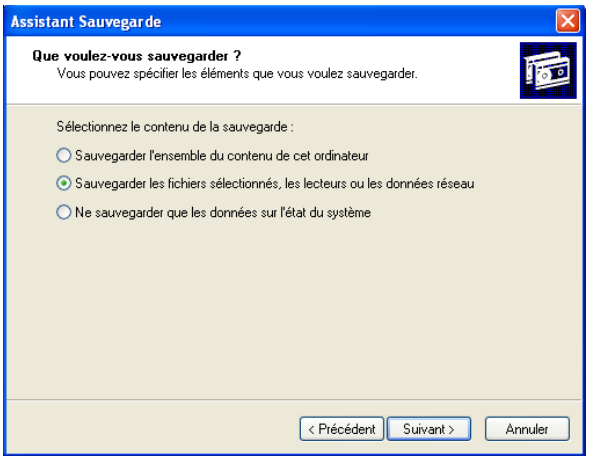
Décocher la case « *Toujours démarrer en mode Assistant* »
Cliquer sur Annuler.
Relancer ntbackup. On obtient la fenêtre ci-dessous à droite.



Aller dans l'onglet « *Planifier les travaux* ».



Cliquer sur « Non » si l'assistant vous demande si vous souhaitez conserver les paramètres définis auparavant.
Sélectionner « *Sauvegarder les fichiers sélectionnés, les lecteurs ou les données réseaux* » puis cliquer sur suivant. Sélectionner ensuite les données à sauvegarder.

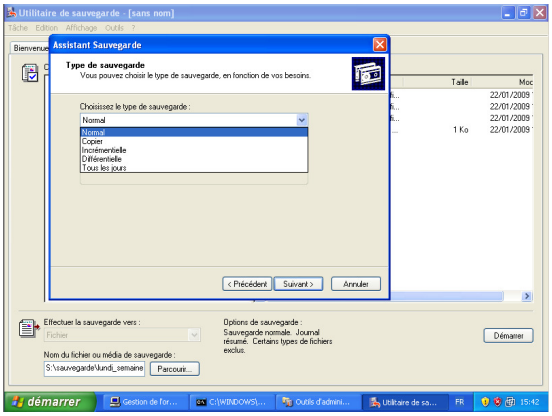


Remarque :

- Il peut être intéressant de faire une sauvegarde de l'Etat du système ou une sauvegarde complète de la machine (sauvegarde ASR).
- **Les sauvegardes ASR permettent de réinstaller complètement le système (pas les données) dans son état au moment de la sauvegarde à partir d'un média de réinstallation (touche F2). Cette méthode nécessite la présence d'un lecteur de disquette. Pour plus d'informations, voir http://www.petri.co.il/what's_asr_in_windows_xp_2003.htm**

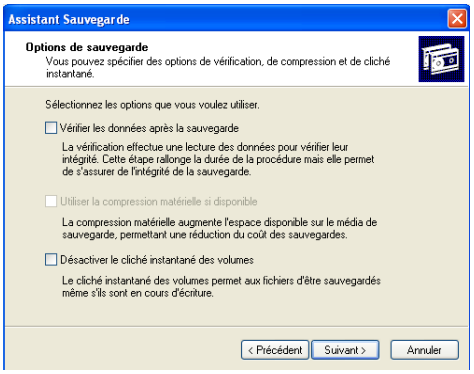
Sélectionner l'emplacement.

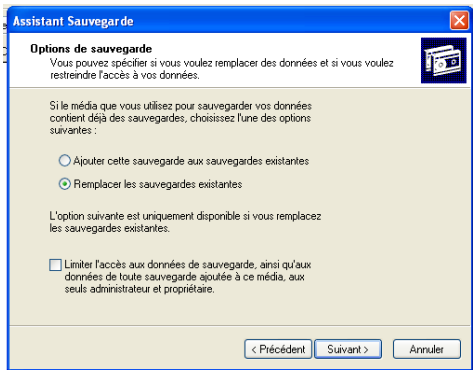
On va créer un fichier BKF par tâche de sauvegarde.
Il y a 10 tâches de sauvegarde à créer (lundi à vendredi pour la semaine 1 et la semaine 2) sans compter les sauvegardes mensuelles et annuelles.
La sauvegarde le lundi est une sauvegarde « *Normale*».
Du mardi au vendredi, c'est une sauvegarde « *Différentielle* ».



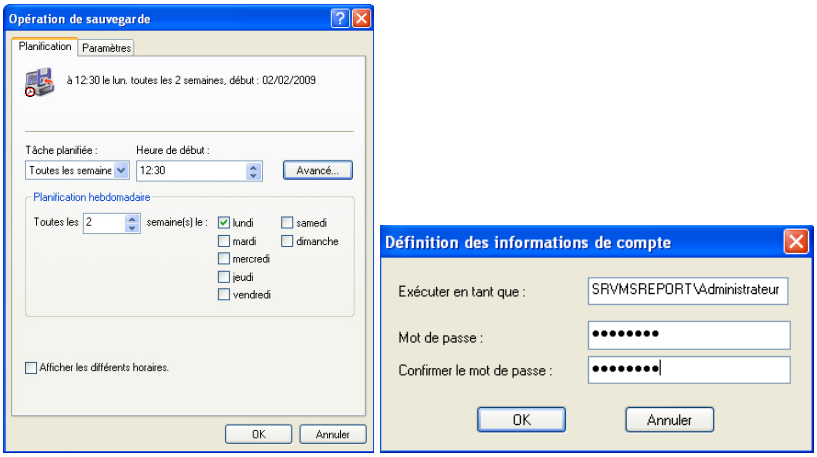
Le cliché instantané de volume permet de faire une sauvegarde à chaud des données.
Si un utilisateur a ouvert un fichier, celui est comme même sauvegardé.
Il est nécessaire de fermer toutes applications qui ne gèrent pas les sauvegarde à chaud des données (surtout les bases de données).

NTBACKUP va créer un fichier appelé lundi_semaine1.bkf (10 fichiers BKF en tout sans les sauvegardes mensuelles et annuelles). Ce fichier peut contenir une ou plusieurs sauvegardes et peut donc être très important en termes de taille.
Pour cela, nous configurons la sauvegarde des données en mode remplacement.
Chaque sauvegarde écrasera la sauvegarde faite 15 jours auparavant (le fichier BKF qui correspond à cette sauvegarde).



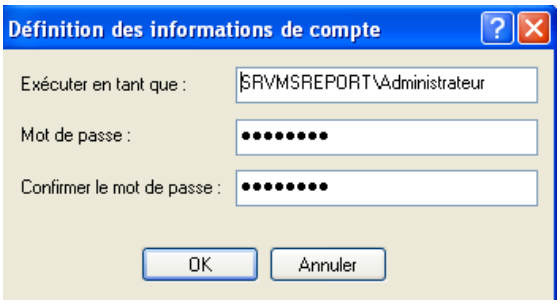


Il faut maintenant planifier les sauvegardes (à 12h ou 12h30).
Cliquer sur Planification.

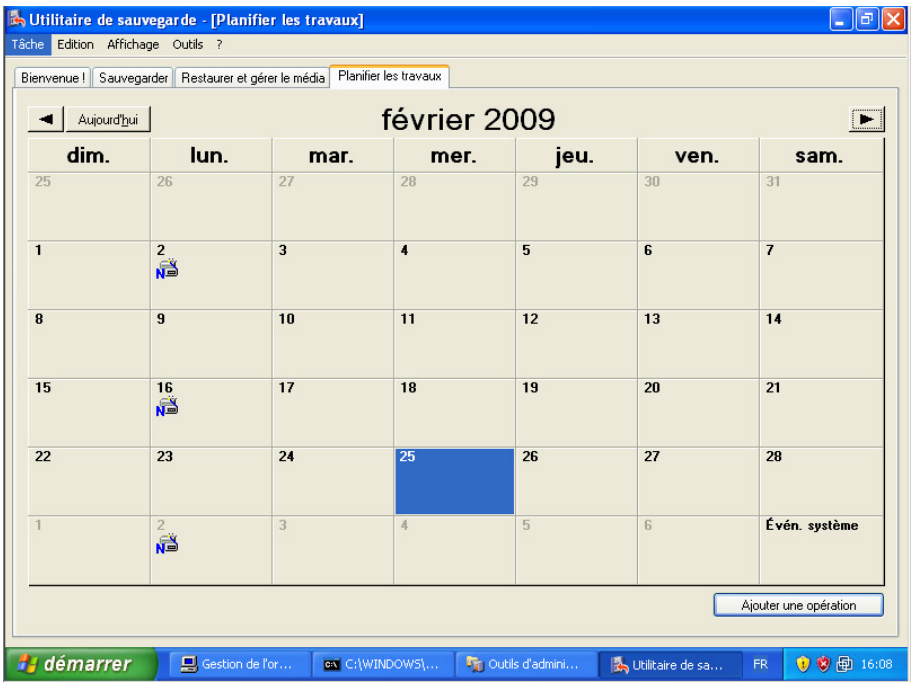


Attention pour les tâches de sauvegarde de la semaine 1 et de la semaine 2 doivent avoir une date de début décalée d'une semaine :

Il faut ensuite rentrer deux fois le mot de passe (première fois pour lancer la tâche planifiée, seconde pour que NTBACKUP s'exécute).



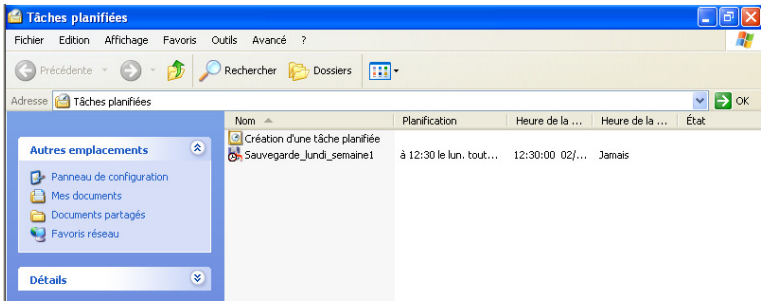
Le résumé s'affiche. Cliquer sur Terminer.
On obtient le résultat suivant.



Remarque :

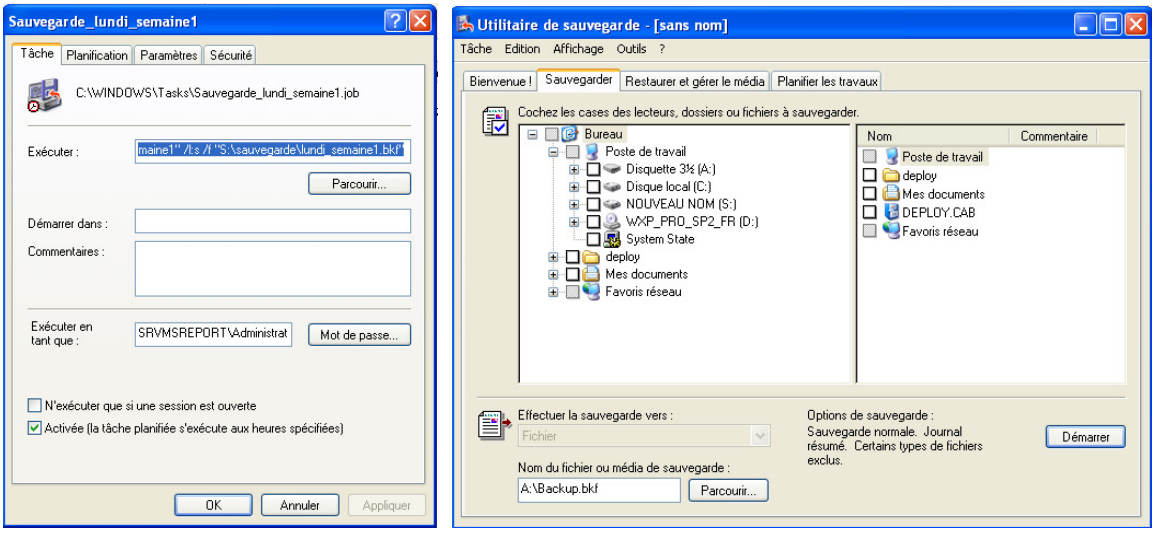
- Le N en bleu pour le symbole d'une sauvegarde normale planifiée.
- Le D en vert pour une sauvegarde différentielle planifiée.

Aller dans « *Démarrer* » | « *Programmes* » | « *Accessoires* » | « *Systèmes* » | « *Tâches planifiées* ».
On va alors la tâche planifiée.



Pour exécuter la tâche immédiatement, clic droit et « *Exécuter maintenant* ».
Si on va dans les propriétés d'une tâche, on peut voir que cela lance NTBACKUP en ligne de commande avec des paramètres (fichier BKS et emplacement sauvegarde cible).
*C:\WINDOWS\system32\ntbackup.exe backup "@C:\Documents and Settings\Administrateur\Local Settings\Application Data\Microsoft\Windows NT\NTBackup\data**Sauvegarde_lundi_semaine1.bks**" /n "**lundi_semaine1.bkf** créé le 27/01/2009 à 16:07" /d "Jeu créé le 27/01/2009 à 16:07" /v:no /r:no /rs:no /hc:off /m normal /j "Sauvegarde_lundi_semaine1" /l:s /f "**S:\sauvegarde\lundi_semaine1.bkf**"*

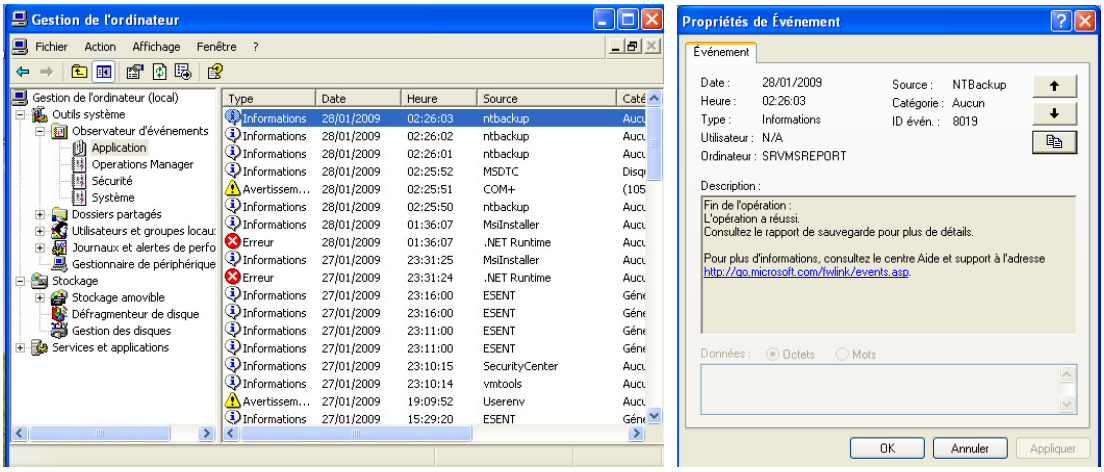
On peut ouvrir le fichier BKS, via le menu « *Edition* » quand on se trouve dans l'onglet « *Sauvegarde* ».



Le fichier BKS ne contient que la sélection des donnés à sauvegarder.
Pour modifier la destination de la sauvegarde, changer la ligne de commande.
Pour changer la planification, aller dans au niveau des propriétés de la tâches planifiées dans le gestionnaire de tâches.

3.2 Surveillance tâche de sauvegarde :

Il faut valider dans les observateurs d'événements tous les jours (au moins toutes les semaines) que les sauvegardes ont bien fonctionnées.

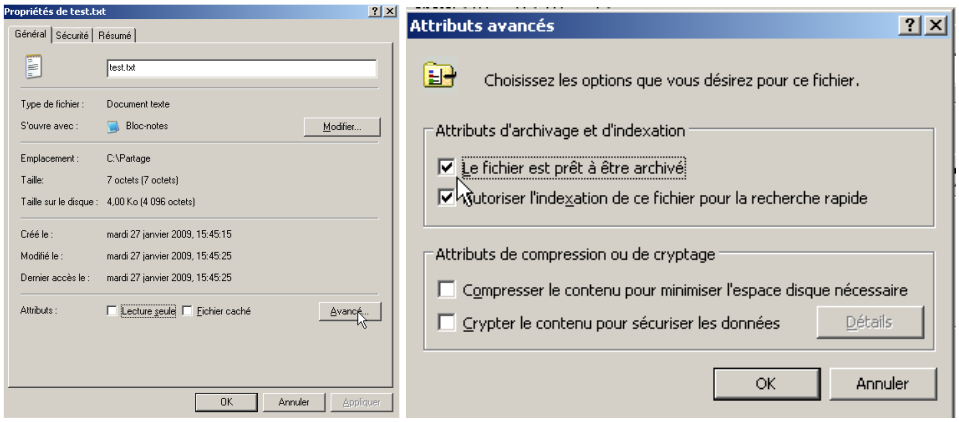


Tout message « *Erreur* » ou « *Avertissement* » avec ntbackup comme source dans le journal « *Application* » indique des problèmes de sauvegarde.

3.3 Complément d'informations sur NTBACKUP :

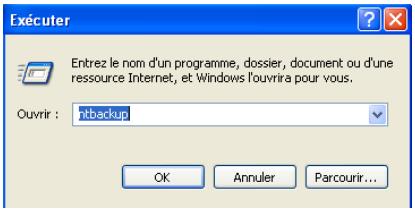
Avec NTBACKUP il existe 5 types de sauvegardes :

- Sauvegarde normale : s'appuie sur l'attribut « *le fichier est prêt à être archivé* ». Elle sauvegarde tout (que l'attribut « *Le fichier est prêt à être archivé* » et elle retire cet attribut sur les fichiers sauvegardés.
- Sauvegarde incrémentielle : s'appuie sur l'attribut « *le fichier est prêt à être archivé* ». Ne sauvegarde que les fichiers dont l'attribut « *Le fichier est prêt à être archivé* » est coché et retire cet attribut sur les fichiers sauvegardés.
- Sauvegarde différentielle : s'appuie sur l'attribut « *le fichier est prêt à être archivé* ». Ne sauvegarde que les fichiers dont l'attribut « *Le fichier est prêt à être archivé* » est coché et ne retire pas cet attribut sur les fichiers sauvegardés
- Sauvegarde « copie » : s'appuie sur l'attribut « *le dossier est prêt à être archivé* » ou « *le fichier est prêt à être archivé* ». Sauvegarde tout et ne touche pas à l'attribut « *le dossier est prêt à être archivé* ».
- Tous les jours : s'appuie sur les dates de modification des fichiers ou « le fichier est prêt à être archivé »

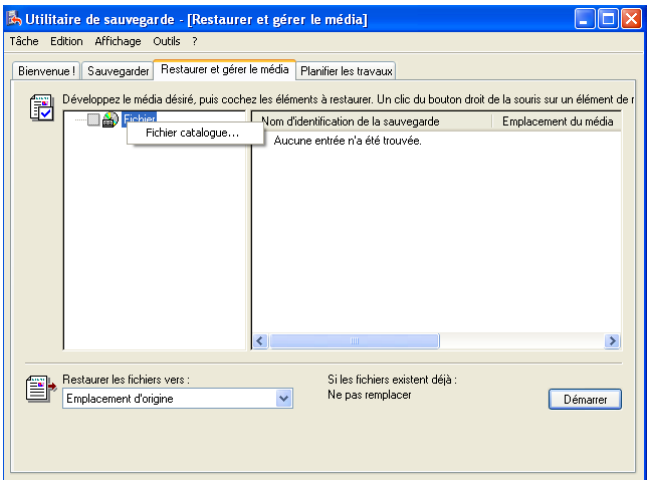


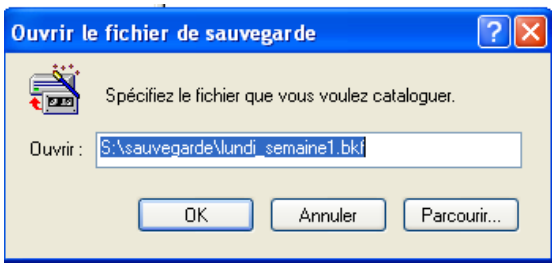
4 PROCEDURE DE RESTAURATION

Aller dans « *Démarrer* » | « *Exécuter* » et taper « *ntbackup* ». Cliquer sur « *OK* ».

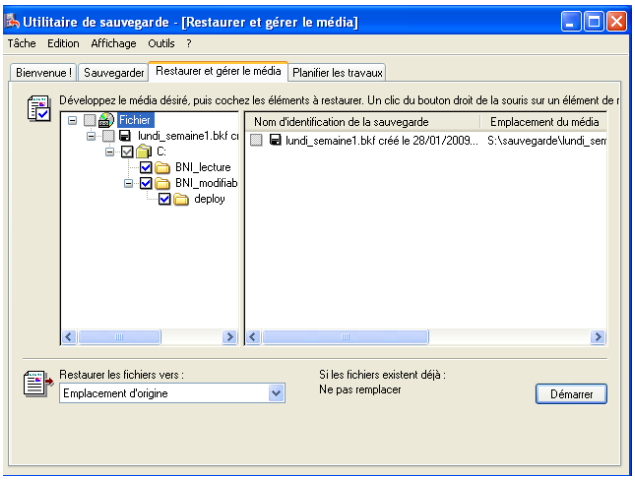


Décocher la case « *Toujours démarrer en mode Assistant* »
Cliquer sur Annuler.
Relancer ntbackup puis aller dans l'onglet « *Restaurer et gérer le média* »
Si aucune sauvegardée n'est cataloguée, faire un clic droit sur Fichier et cliquer sur « *Fichier Catalogue* ».
Cliquer sur Parcourir et aller chercher le fichier BKF contenant votre sauvegarde.

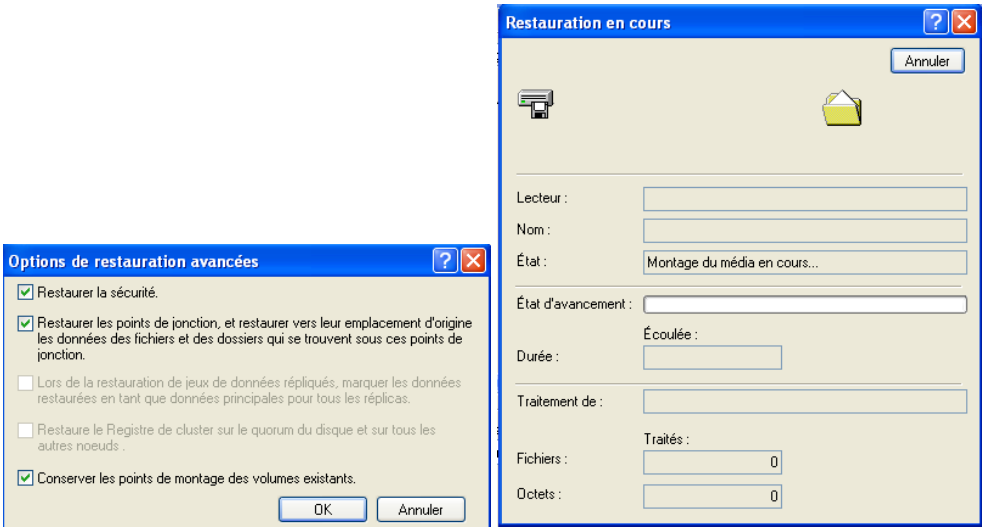




Sélectionner ensuite les données à restaurer. On peut choisir dans cette fenêtre si on restaure vers l'emplacement d'origine ou sur un autre répertoire (pratique pour faire de la fusion de données).
Cliquer ensuite sur le bouton « *Démarrer* ».



Cliquer sur le bouton « *Avancé* » dans la fenêtre « *Confirmation de restauration* ».
Il faut surtout ne pas décocher « Restaurer la sécurité » car sinon on perd les permissions NTFS.



La restauration s'effectue.
Vérifier dans le journal application que la restauration s'est bien passée (observateur d'événements).