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

<u>1</u>	PRESENTATION DE CE DOCUMENT :	<u> 3</u>
1.1	O U TROUVER CE DOCUMENT :	3
1.2	O BJECTIFS DE DOCUMENT :	3
2	SECURISATION ET PARTAGE DES DONNEES	4
2.1	PRE-REQUIS :	4
2.1	1 VERIFICATION VERSION DU SYSTEME D'EXPLOITATION ·	
2.1.	2 TABLEAU D'INFORMATION A REMPLIE PAR LE CHEF D'ENTREPRISE	4
2.1.	3 CONFIGURATION DU OU DES DISQUES OU LES DONNEES SONT SITUEES :	4
2.1.	4 DESACTIVATION DU PARTAGE DE FICHIERS SIMPLES	5
2.1.	5 DESACTIVATION DE L'ECRAN D'ACCUEIL DE WINDOWS XP :	5
2.1.	6 CONFIGURATION DU PARE FEU :	6
2.1.	7 DEFINIR UN MOT DE PASSE POUR LE COMPTE ADMINISTRATEUR SUR LA STATION QUI PARTA	GE
LES	DONNEES :	6
2.2	PROCEDURE POUR SECURISER ET PARTAGER DES DOSSIERS SUR UNE STATION DE TRAVAIL	Ĺ
WI	NDOWS XP PRO :	8
2.2.	1 CREATION D'UN DOSSIER :	8
2.2.	2 CREATION DES COMPTES UTILISATEURS DES UTILISATEURS QUI DOIVENT ACCEDER AUX 2	
DOS	SSIERS SUR LE SERVEUR DE FICHIERS WINDOWS XP :	8
2.2.	3 CREER DES GROUPES ET AJOUTER LES UTILISATEURS AUX GROUPES :	8
2.2.	4 DEFINIR DES PERMISSIONS :	9
2.2.	5 REINITIALISER DES PERMISSIONS SUR LES FICHIERS DANS LES DOSSIERS:	. 11
2.2.	6 PARTAGER LE DOSSIER :	. 12
2.2.	ACCES AUX DONNEES DEPUIS UNE STATION DE TRAVAIL :	. 12
2.3	MISE EN PLACE DE L'AUDIT DES ACCES :	. 15
2.3.	1 PROCEDURE DE MISE EN PLACE :	. 15
2.3.	2 EXPLOITATION DE L'AUDIT :	. 17
2.3.	3 SUPPRESSION DU CONTENU DU JOURNAL DE SECURITE :	. 19
<u>3</u>	SAUVEGARDE :	<u>.20</u>
3.1	PRE-REQUIS :	. 20
3.1.	1 TABLEAU D'INFORMATION A REMPLIR PAR LE CHEF D'ENTREPRISE :	. 20
3.1.	2 MODIFICATION DE MOT DE PASSE ADMINISTRATEUR :	. 20
3.1.	3 PRE-REQUIS AU NIVEAU WINDOWS XP :	. 20
3.1.	4 PRE-REQUIS AU NIVEAU DES DISQUES :	. 20
3.1.	5 POLITIQUE DE SAUVEGARDE :	. 21
3.1.	6 PROCEDURE DE SAUVEGARDE :	. 21
3.2	SURVEILLANCE TACHE DE SAUVEGARDE :	. 25
3.3	COMPLEMENT D'INFORMATIONS SUR NTBACKUP :	. 26
4	PROCEDURE DE RESTAURATION	.27

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 <u>http://msreport.free.fr</u>. 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 ».

À propos de Windows 🛛 🔀
Copyright © 1985-2001 Microsoft Corporation
Microsoft ® Windows Version 5.1 (numéro 2600.xpsp_sp2_rtm.040803-2158 : Service Pack 2) Copyright © 1981-2001 Microsoft Corporation
La licence de ce produit est accordée conformément aux termes du <u>Contrat de Licence Utilisateur Final</u> à :
Mémoire physique disponible : 261 616 Ko
<u> </u>

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.



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.

Options des dossiers	? X Propriétés de Documents and Settings ? X
Général Affichage Types de fichiers Fichiers hors connexion Affichage des dossiers Vous pouvez appliquer l'apparence (telle celle utilisée pour les détails ou les titres) que vous utilisez pour ce dossier à tous vos dossiers. Appliquer à tous les dossiers Réinitialiser tous les dossiers	Général Partage Sécurité Personnaliser Noms d'utilisateur ou de groupe : Administrateurs (XPTEST\Administrateurs) SYSTEM Dut le monde Utilisateurs (XPTEST\Utilisateurs) Utilisateurs avec pouvoir)
Paramètres avancés : Afficher les fichiers et dossiers cachés Afficher les fichiers et dossiers cachés Masquer les extensions des fichiers dont le type est connu Masquer les fichiers protégés du système d'exploitation (recommandé) Mémoriser les paramètres d'affichage de chaque dossier Ne pas mettre les miniatures en cache Ouvrir les fenêtres des dossiers dans un processus différent Rechercher automatiquement les dossiers et imprimantes partagés Restaurer les fenêtres de dossiers ouvertes lors de la prochaine ouvertur Utiliser le partage de fichiers simple (recommandé)	Autorisations pour Administrateurs Autoriser Refuser Contrôle total Modification Lecture et exécution Alfichage du contenu du dossier Ecriture Ecriture Ecriture Pour définir des autorisations spéciales ou des paramètres avancés, cliquez
Paramètres par défa OK Annuler Appl	iguer OK Annuler Appliquer

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.

🥮 Comptes d'utilisateurs	🔟 🗖 🗖	😫 Comptes	d'utilisateurs	
🕒 Précédent 🕤 😫 Début		Précédent	: 📀 🕵 Début	•
Ade sur (2) Control d'ubischeurs (3) Poet de combis (3) Poet de combis (3) Poet de combis (3) Poet d'ubischeur (3) Charger d'ubischeur	Consistence and address of the second secon	Täches ap Gifer lis co Aide sur (a) Option session	parentées notes d'ouverture de Compt 2	Selectionnez les options d'ouverture et de femeter de session Meret de de session Meret de de sette de la de de de sette de la de

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 « administrateur ».

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 CTRL ALT SUPPR.

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</u> empêcher l'accès aux fichiers chiffrés avec EFS (la récupération des données perdues n'est pas toujours possible mais toujours couteuse).

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...).

島 Gestion de l'ordinateur		Nouveau group	e 🤋 🔀
Gestion de l'ordinateur Fichier Action Affichage Fenêtre ? Fichier Action Affichage Fenêtre ? Gestion de l'ordinateur (local) Gostervateur (local) Gostervateur d'événements Gostervateurs Gosterva	Description Les menhres du groupe Administrat Prend en charge la réplication des fic Les membres du groupe purviés disp Les membres du groupe Diviseturs Les membres du groupe Utiliseturs Les membres du groupe Utiliseturs Les membres de ce groupe disposen Groupe pour le centre d'aide et de s	Nom du groupe : Description : Membres : Ajouter	ve ? X Msreport
			Créer Fermer
Crée un nouveau groupe local.			

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* ».

🛢 Gestion de l'ordinateur	Propriétés de Msreport	
📕 Fichier Action Affichage Fenêtre ?	Général	
	Mireport	
	Resolution:	Sélectionnez Utilisateurs Image: Comparison of the second of

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 ».

Propriétés de BNI_modifiable	Paramètres de sécurité avancé pour BNI_modifiable				
Général Partage Sécurité Partage Web Personnaliser	Autorisations Audit Propriétaire Autorisations effectives	_			
Noms d'utilisateur ou de groupe : Administrateur (SRVFICHIERSVAdministrateur)	Pour afficher davantage d'informations concernant les autorisations spéciales, sélectionnez une autorisation puis cliquez sur Modifier.				
Administrateurs (SRVFICHIERS\Administrateurs) CREATEUR PROPRIETAIRE	Type Nom Autorisation Héritée de Appliquer à				
SVSTEM Ditisateurs (SRVPICHIERS/Utilisateurs) Ajouter Supprimer Autorisations pour Administrateur Autorisations pour Administrateur Autorisations Dominie toxid Dominie toxid	Autoriser Administrateurs (SRV Controlle total C: Ce doster, les sous-d Autoriser SYSTEM Controlle total C: Ce dossier, les sous-d Autoriser Administrateur (SRVFI Controlle total C: Ce dossier, les sous-d Autoriser CREATEUR PROPRIN Controlle total C: Les sour-dossier et l Autoriser Utilisateurs (SRVFICH Lecture et exéc C: Ce dossier, les sous-d Autoriser Utilisateurs (SRVFICH Spécial C: Ce dossier et les sous-d Autoriser Utilisateurs (SRVFICH Spécial C: Ce dossier et les sous-d Autoriser Modifier Suprimer Suprimer Xing				
Lecture Éciture Autorisations spéciales	Hérite de l'objet parent les entrées d'autorisation qui s'appliquent aux objets enfants. Cela inclut les objets dont les entrées sont spécifiquement définies ici. Remplacer les entrées d'autorisations de tous les objets enfants par les entrées affichées ici et qui				
Pour définir des autorisations spéciales ou des paramètres avancés, cliquez sur Paramètres avancés. Paramètres avancés	└─ s'appliquent aux objets enfants				
OK Annuler Appliquer	OK Annuler Appliq	iet			

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.

Dransiétés de DNI medifishie		Sélectionnez Utilisateurs ou Groupes	<u> 2 X</u>
Propriétés de UNI_modifiable Général Patage Sécurité Patage Web Personnaîser Nome d'ultisateur ou de groupe :		Sélectionnes le type de cet objet : Uthanteurs, Groupes ou Entrés de sécurité intégrées À partir de cet emplacement : Securitoriumes	Types d'objet
Administrateurs (SRVFICHERS Vadministrateurs) SySTEM Ajouter Supprimer		Non: Connerce par Description: Connerce par Connerce par Connerce par Image: Connerce par Connerce par Descriptes déscrivés Connerce par	Colonnes Rechercher
Autorisation: pour SYSTEM Autoriser Refuser Controle total V Modification Lecture et execution V Autorisation: pour System V Lecture et execution Lecture et execution V Lecture V Lecture V Lecture V Autorisations raciciales V	Sélectionnez Utilisateurs ou Groupes ? X Sélectionnez le type de cet objet : Utilisateurs, Groupes ou Entités de sécurité intégrées Types d'objet À patri de cet emplacement : SRVFICHIERS Emplacement : SRVFICHIERS Emplacement :	Nombre de jours depuis la dernière session .	Annuler
Pou défini des autoriaites spéciales ou des parentes avancés. Paramètres avancés. DK Annuter Appliquer	Vérifer les nons Vérifer les nons Avancé OK Annuler		

mechonnez ornisateurs ou Groupes	L 🖸 🚺
Sélectionnez le type de cet objet :	
Utilisateurs, Groupes ou Entités de sécurité intégrées	Types d'obiet
À parti de cet employement :	
SEVECHERS	Endecements
	Citylaconanta
Requêtes communes	
Non: Commence par 👻	Colonnes
	Bechevcher
Description: Commence par 👻	mechaicher
Comptes désactivés	Aniter
Mot de passe sans date d'expiration	
	26
	~
05	Amite
dk.	Annae
Nom (RDN) Dans le dossier	<u>~</u>
2 IUSR_APCM SRVFICHIERS	
TIWAM_APLM SRVHLHEHS	
SRVRCHERS	
Dpérateurs de SRVFICHIERS	
Dpérateurs de SRVFICHERS	
PREMOTE INT	
EX NEDLAD	
SERVICE LD.	~

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.

ropriétés de BNI_modifiable		? 🗙				
Général Partage Sécurité Partage	Web Personnalis	er	Propriétés de	BNI_modifiable		? 🛛
Noms d'utilisateur ou de groupe :			Général Parta	ge Sécurité Partage	Web Personnalis	er
Administrateurs (SRVFICHIERSV	Administrateurs)		Noms d'utilisal	eur ou de groupe :		
Msreport (SRVFICHIERS\Msrep	ort)		Administrateurs (SRVFICHIERS\Administrateurs)			
🕵 SYSTEM			Msreport	(SRVFICHIERS\Msrep	ort)	
			🕵 SYSTEN	1		
	Ajouter	Supprimer			Ajouter	Supprimer
Autorisations pour Msreport	Autoriser	Refuser	Autorisations r	our Msrenort	Autoriser	Befuser
Contrôle total			Contrêle tel	al		
Modification			Modification	u 1		
Lecture et exécution			Lecture et	exécution		H I
Affichage du contenu du dossier			Affichage o	u contenu du dossier		
Lecture			Lecture			
Ecriture			Écriture		~	
Autorisations spéciales			Autorisation	s spéciales		
Pour définir des autorisations spéciales ou des paramètres avancés, cliquez sur Paramètres avancés.	Paramè	tres avancés	Pour définir de ou des param sur Paramètre	es autorisations spéciales ètres avancés, cliquez s avancés.	Parami	ètres avancés
ОК	Annuler	Appliquer		ОК	Annuler	Appliquer

2.2.5 Réinitialiser des permissions sur les fichiers dans les dossiers:

Attention, le <u>déplacement</u> (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.

Sécurité						
1	Ceci supprimera les autorisations définies explicitement sur tous les objets enfants et autorisers la propagation des autorisations pouvant être héritées vers ces objets enfants. Seules les autorisations pouvant être héritées qui seront propagées à partir de BNI_modifiable prendront effet. Voulez-vous continuer ?					
	Oui Non					

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).

Paramètr	es de o	cache				?
	Vous cach	pouvez spécil e local quand	fier si les fichi d'autres persi	ers de ce do onnes y acc	ossier partagé so èdent.	ont inclus dans un
Auto	oriser la n	nise en cache	des fichiers c	lans ce dos	sier partagé —	
Paramè	tre :					~
					OK	Annuler

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.

C:\WINDOWS\system32\CMD.exe	- 🗆 X							
Microsoft Windows XP Eversion 5.1.2600] (C) Copyright 1985-2001 Microsoft Corp.								
C:\Documents and Settings\176152>PING SRUMSREPORT								
Envoi d'une requête 'ping' sur SRUMSREPORT [192.168.90.2] avec 32 octets de ées :	donn							
Réponse de 192.168.90.2 : octets=32 temps<1ms TTL=128 Réponse de 192.168.90.2 : octets=32 temps<1ms TTL=128 Réponse de 192.168.90.2 : octets=32 temps<1ms TTL=128 Réponse de 192.168.90.2 : octets=32 temps<1ms TTL=128								
Statistiques Ping pour 192.168.90.2: Paquets : envoyés = 4, recus = 4, perdus = 0 (perte 0x), Durée approximative des boucles en millisecondes : Minimun = Oms, Maximun = Oms, Moyenne = Oms								
C:\Documents and Settings\176152>								
	-							

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 <u>simultanées</u> 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 » <u>\\nom serveur fichier\</u>

Exécute	· ? 🛛
	Entrez le nom d'un programme, dossier, document ou d'une ressource Internet, et Windows l'ouvrira pour vous.
Ouvrir :	\\srvmsreport
	OK Annuler Parcourir

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

Connecter à srvMs	report 🛛 🛛 🔀
	GE
Connexion à srvmsrep	port
Nom d'utilisateur :	😴 srvmsreport\176543
Mot de passe :	•••••
	Mémoriser mon mot de passe
	OK Annuler

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 cidessous 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* ».

 Configurer non compte pour utiliser un passeport. NET 	😫 Comptes d'utilisateurs		🔦 Noms et mots de passe utilisateur enregistrés 👘 🕐 🔀
	Précédent Précédent	Ourse voorse	Windows peut stocker vos informations d'ouverture de session concernant les emplacements réseau et les sites Web. Pour ajouter une entrée, cliquez sur Ajouter. Pour modifier une entrée existante, sélectionnez-la puis cliquez sur Propriétés. stromsreport Ajouter Supprimer Supprimer Propriétés Propriétés

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.

Pice S Completa d'utilisateurs Pice Précédent © 100 pice Idres Tâches apparentés Idres Calera nes moto de passe rése Encérter un note de passe d'utilisateur Calera nu norveau comple Idres Précédent © 100 pice Idres Précédent voit compte Idres Précédent voit compte Idres un nouveau comple Précédent voit compte Idres un nouveau comple Précédent voit compte Idres un Passport. NAT Utilier un Passport. NAT	Propriétés d'information sur l'ouverture de… ? Propriétés d'information sur l'ouverture de… ? Protection emplocement résul, pui entre le non de d'utilisateur et le moi de passe à utilise pour y accéder. Serveur : Mon d'utilisateur :	npte?	Modifier votre mot de passe pour le domaine Image: Ceci va modifier votre mot de passe pour le domaine srvmsreport Mot de passe précédent : •••••••• Nouveau mot de passe : •••••••• Confirmer le nouveau mot de passe : ••••••••
🛃 démarrer 📄 🖻 5 Explore	teur Wind 🔹 🚍 Gestion de l'ordinateur 🛛 👯 Comptes d'utilisateurs 🛛 FR 🚺	9 9 🗞 🔿 🦁 15:11	OK Annuler

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.

县 Gestion de l'ordinateur				Propriétés de Sécurité
具 Fichier Action Affichage Fené	itre ?		_8×	Général Filtrer
⇔ → 🗈 💽 💣 🖓 🔩 😫)			
Gestion de l'ordinateur (loca) Gutils système Goservateur d'événements Operations Manager Gosers partagés Gosers partagés Gosers partagés Gosers partagés Gosens partagés Gostionnaire de périphérique Gestionnaire de périphérique Gestion des disques Gestion des disques Services et applications	Type Date <i>A</i> udit des s <i>Q</i> Audit des s <i>Q</i> Audit des s <i>Q</i> Audit des s <i>Q</i> 2/01/2009	Heure 00:49:48 18:16:58	Source Security Security	Nom complet : Sécurité Nom du journal : C:\WINDOWS\System32\config\SecEvent.Evt Taille : 64.0 Ko (65 536 octets) Créé le : dimanche 1 juin 2008 11:49:51 Modifié le : jeudi 22 janvier 2009 18:19:44 Dernier accès le : jeudi 22 janvier 2009 18:19:44 Taille de journal Taille de journal Taille maximale du journal : 20032 📚 Ko Lorsque la taille maximale du journal est atteinte : Image: Remplacer les événements si nécessaire Remplacer les événements datant de plus de 7 💿 jours Ne pas remplacer les événements (nettoyage manuel du journal)
				Utiliser une connexion à basse vitesse
<	<)		>	OK Annuler Appliquer

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 ».

Propriétés de BNI_modifiable 🛛 🛛 🔀	Paramètres de sécurité avancé pour BNI_modifiable
Général Partage Sécurité Partage Web Personnaliser Noms d'utilisateur ou de groupe : Ø Administrateurs (SRVMSREPORT\Administrateurs) Ø Mareport (SRVMSREPORT\Msreport) Ø SYSTEM	Autorisations Audit Propriétaire Autorisations effectives Pour afficher davantage d'informations concernant les entrées d'audition spéciales, sélectionnez une entrée d'audit puis cliquez sur Modifier. Entrées d'audit : Type Nom Accès Héritée de Appliquer à
Ajouter Supprimer Autorisations pour SYSTEM Autoriser Refuser Contrôle total Image: Contrôle total Image: Contrôle total Image: Contrôle total Modification Image: Contrôle total Image: Contrôle total Image: Contrôle total Image: Contrôle total Lecture et exécution Image: Contrôle total Image: Contrôle total Image: Contrôle total Image: Contrôle total Autorisation activation Image: Contrôle total Image: Contrôle total Image: Contrôle total Image: Contrôle total Autorisations sociales Image: Contrôle total Image: Contrôle total Image: Contrôle total Image: Contrôle total Pour définit des autorisations spéciales Image: Contrôle total Image: Contrôle total Image: Contrôle total Pour définit des autorisations spéciales Image: Contrôle total Image: Contrôle total Image: Contrôle total Sur Paramètres avancés Image: Contrôle total Image: Contrôle total Image: Contrôle total Image: Contrôle total Paramètres avancés Image: Contrôle total Image: Contrôle total Image: Contrôle total Image: Contrôle total Sur Paramètres avancés Image: Contrôle total Image: Contrôle	Ajouter Supprimer Hérite de l'objet parent les entrées d'audit qui s'appliquent aux objets enfants. Cela inclut les objets dont les entrées ont spécifiquement définies ici. Remplacer les entrées d'audit sur tous les objets enfants par les entrées qui s'appliquent aux objets enfants qui sont affichées ici.
OK Annuler Appliquer	OK Annuler Appliquer

Sélectionnez Utilisateur ou Groupe	Audit de l'entrée pour BNI_modifiable	?×
Sélectionnez le type de cet objet :	Objet	
Utilisateur, Groupe ou Entité de sécurité intégrée Types d'objet		
À pattir de cet emplacement :	Nom : Msteport (SBVMSBEP0BT\Msteport) Modifie	
SRVMSREPORT Emplacements		
Requêtes communes	Appliquer à : Ce dossier, les sous-dossiers et les fichiers	~
Colonnes	Accès : Réussite Échec	
Nom : Commence par V	Contrôlo total	
Description: Commence par 💌	Parcours du dossier/exécuter le fichier	
Comptes désactivés Arrêter	Liste du dossier/lecture de données	
Mot de passe sans date d'expiration	Attributs de lecture	
Nombre de jours depuis la demière session :	Lecture des attributs étendus	
	Création de fichier/écriture de données 🔽 📃	=
	Création de dossier/ajout de données 🔽 📃	
OK Annuler	Attributs d'écriture	
	Écriture d'attributs étendus	
	Suppression de sous-dossier et fichier	
Invités SRVMSREPORT	Suppression	
2 IUSR_APCM SRVMSREPORT	Autorisations de lecture	~
	Appliquer ces entrées d'audit aux objets	
Msreport SRVMSREPORT	et/ou aux conteneurs à l'intérieur de ce	out
32 Opérateurs de SRVMSREPORT 32 Opérateurs de SRVMSREPORT	Conteneur uniquement	
BREMOTE INT	OK An	nuler
M RESEAU 🕙		
Paramètres de sécurité avancé pour BNI_modifiable	Propriétés de Gérer le journal d'audit et de sécurité	
Autorisations Audit Propriétaire Autorisations effectives	Paramètre de sécurité locale	
Pour afficher davantage d'informations concernant les entrées d'audition spéciales, sélectionnez une	Gérer le journal d'audit et de sécurité	
entree d'audit puis cliquez sur Modifier.		
Envices a duar .		
Réussite Msreport (SRVMSRE Spécial <non héritée=""> Ce dossier, les sou</non>	Ádministrateurs	
	SERVICE RÉSEAU	
Ajouter Modifier Supprimer		
Hérite de l'objet parent les entrées d'audit qui s'appliquent aux objets enfants. Cela inclut les objets dont les entrées sont snécifiquement définies ici	Ajouter un utilisateur ou un groupe Supprimer	
Remplacer les entrées d'audit sur tous les objets enfants par les entrées qui s'appliquent aux objets		
enfants qui sont affichées ici.		
OK Annuler Appliquer	OK Annuler Appliquer	

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 ».

Gestion de l'ord	inateur			
🛃 Fichier 🛛 Action 🗍	Affichage Fenêtre ?			
← → 🗈 💽	Ajouter/supprimer des colonnes	5		
J Gestion de l'ordina	Tous les enregistrements	3	Heure	Source
🗄 🌇 Outils système	 Filtrer 	01/2009	01:42:06	Security
🖻 🔝 Observate	 Plus récept d'abord 	01/2009	01:42:06	Security
Applica	Plus appien d'abord	01/2009	01:42:01	Security
Operal Operal		01/2009	01:42:01	Security
Securit	Rechercher	01/2009	01:36:28	Security
Bossiers p	Personnaliser	01/2009	01:35:40	Security
E Custers p		<u></u>	01:35:40	Security
E 🖓 Journaux et	alertes de perfo	28/01/2009	01:35:40	Security
🔄 🔜 Gestionnaire	e de périphérique			
Stockage				
🛨 🔐 Stockage an	novible			
Defragment	eur de disque			
🔤 Gestion des				
- 👷 Services et appl	Ications			

<mark>opri</mark> Génér	étés de Sécurit al Filtrer	é				?
INT S S S S S	Des d'événements] Information] Avertissement] Erreur		✔ Audit des ✔ Audit des	succè échec	5 8	
Sour	ce de l'événement :	(Toute	s)			*
Caté	gorie :	(Toute	s)			*
ID de Utilis	e l'événement : ateur :	560				
Ordin	nateur :					
De:	Premier événemer	nt 💌	28/01/2009	V	01:34:49	*
à:	Dernier événemer	nt 💌	28/01/2009	~	01:42:06	A V
				Pa	ramètres par c	léfaut
			ОК	Ann	ller Ar	opliquer

÷.											
	🖶 Gestion de l'ordinateur										
E Fichier Action Affichage Fenêtre ?											
	🖳 Gestion de l'ordinateur (local)	Туре	Date	Heure	Source	Catégorie	Évén	Utilisateur	Ordinateur		
	🖻 🌇 Outils système	dudit des s	28/01/2009	01:36:28	Security	Accès au	562	SYSTEM	SRVMSREP		
	Observateur d'événements	of Audit des s	28/01/2009	01:36:28	Security	Accès au	560	155678	SRVMSREP		
	Application	audit des s	28/01/2009	01:35:40	Security	Accès au	562	Administrateur	SRVMSREP		
	Operations Manager	of Audit des s	28/01/2009	01:35:40	Security	Accès au	560	Administrateur	SRVMSREP		
	Suctions	💰 Audit des s	28/01/2009	01:35:40	Security	Accès au	562	Administrateur	SRVMSREP		
	H Dossiers partagés	dudit des s	28/01/2009	01:35:40	Security	Accès au	560	Administrateur	SRVMSREP		
	+ Cutilisateurs et groupes locau	of Audit des s	28/01/2009	01:35:40	Security	Accès au	562	Administrateur	SRVMSREP		
	+ Journaux et alertes de perfo	audit des s	28/01/2009	01:35:40	Security	Accès au	560	Administrateur	SRVMSREP		
	Gestionnaire de périphérique	audit des s	28/01/2009	01:34:49	Security	Événeme	517	SYSTEM	SRVMSREP		
	🖃 🚵 Stockage										
	🕀 🤮 Stockage amovible										
	🛛 👺 Défragmenteur de disque										
	🔄 🚟 Gestion des disques										
	🗄 🐝 Services et applications										
- 18	4	4									

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 Événements système Catégorie de l'événement : 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.

opriétés de NOUVE	AU NOM (E:)	? 🗵
iénéral Outils Matér	iel Partage	
NOU NOU	VEAU NOM	
Type: D	isque local	
Système de fichiers : Fa	AT 32	
Espace utilisé :	4 096 octets	4,00 Ko
Espace libre :	8 570 396 672 octets	7,98 Go
Capacité :	8 570 400 768 octets	7,98 Go
Lei	cteur E	Nettoyage de disque

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.

🖶 Gestion de l'ordinateur		Modifier la lettre de lecteur et les chemins d'accè ? 🗙
■ Fichier Action Affichage Fenê ← → € 10 20 20 X 20	itre ? 1 🗃 🔯 📓	Autoriser l'accès à ce volume en utilisant la lettre de lecteur suivante et les chemins d'accès de lecteurs :
Gestion de l'ordinateur (local) Guttis système Outis système Outis système Outis système Oussiers partagés Juliasateurs et groupes locau: Juliasateurs et groupes locau: Juliasateurs et alertes de perfo Juliasateurs et alertes de perfo Juliasateurs et alertes de perfo Juliasateurs et alertes de groupes Stockage Gestion ade sagues Services et applications	Volume Disposition Type Système de fichiers • (C) Partition De base NTES • (OUVreit Mandate) Partition De base NTES • Ouvrir Explorer Marquer la partition comme active Mordifer la lettre de lecteur et les chemins d'accès Formater Suprimer la partition • Propriétés 19,995 connecté Suprimer sources Jair	Ajouter Modifier Supprimer

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 ».

Exécute	r 🔹 🤶 🔀
	Entrez le nom d'un programme, dossier, document ou d'une ressource Internet, et Windows l'ouvrira pour vous.
Ouvrir :	ntbackup 👻
	OK Annuler Parcourir

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 ».

nvenue I Sauveg	arder Restaurer et j	gérer le média Planifie	ar les travaux			
Aujourd'hui			février 2	009		
dim.	lun.	mar.	mer.	jeu.	ven.	sam.
25	26	27	28	29	30	31
	2	3	4	5	6	7
3	9	10	11	12	13	14
5	16	17	18	19	20	21
22	23	24	25	26	27	28
	2	3	4	5	6	Évén, système

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 ».

Assistant Sauvegarde	Utilitaire de sauvegarde - [sans nom] Tiche Editor Affebras Outle 2	_ 7 🗙
Type, nom et destination de la sauvegarde Type Type </th <th>Anistant Survegarde X Image: Compare the survegarde of the sur</th> <th>le Moc</th>	Anistant Survegarde X Image: Compare the survegarde of the sur	le Moc
Sélectionnez le type de seuvegarde : Fichier Choisissez un emplacement pour enregistrer votre sauvegarde : S:\sauvegarde\ Entrez un nom pour cette sauvegarde : [undi_semaine1	Chained In type de surveyande : Named V Contemported to the surveyande : Contemported to the surveyande :	22/01/2009 22/01/2009 22/01/2009 0 22/01/2009
< Précédent Suivant > Annuler	Effecture la savegade vers : Forture Entre la savegade vers : Forture Entre la savegade vers : Savegade versale Jornal encla Savegade versale Jornal encla Savegade versale Jornal encla Savegade versale Jornal encla	Démaner

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.

Opération de sauvegarde	
Planification Paramètres	
à 12:30 le lun. toutes les 2 semaines, début : 02/02/2009	
Tâche planiliée : Heure de début :	
Toutes les semaine 🖌 12:30 🗘 Avancé	
Planification hebdomadaire	
Toutes les 2 📚 semaine(s) le : 🕑 lundi 🗌 samedi mardi dimanche mercredi	Définition des informations de compte
☐ jeudi ☐ vendredi	Exécuter en tant que : SRVMSREPORT\Administrateur
	Mot de passe :
Afficher les différents haraires.	Confirmer le mot de passe :
OK Annuler	OK Annuler

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).

Définition des informations de compte 🛛 🛛 🔀				
Exécuter en tant que :	\$RVMSREPORT\Administrateur			
Mot de passe :	•••••			
Confirmer le mot de passe :	•••••			
ОК	Annuler			

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

envenue! Sauvega	arder Restaurer et j	gérer le média Planifie	r les travaux			
Aujourd' <u>h</u> ui]		février 2	009		
dim.	lun.	mar.	mer.	jeu.	ven.	sam.
25	26	27	28	29	30	31
1	2 N	3	4	5	6	7
8	9	10	11	12	13	14
15	16 N	17	18	19	20	21
22	23	24	25	26	27	28
1	2 N	3	4	5	6	Évén. système
						Ajouter une opération

Remarque :

- Le N en bleu pour le symbole d'une sauvegarde normale planifiée.
- Le D en vert pour une sauvegarde différentielle planifiée.
- Msreport <u>http://msreport.free.fr</u> Guillaume MATHIEU La connaissance s'accroît quand on la partage.

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

ڟ Tâches planifiées				∎₽⊠
Fichier Edition Affichage Favoris O	utils Avancé ?			
🕞 Précédente 👻 🌍 👻 🏓	Rechercher 😥 Dossiers	•		
Adresse 🚰 Tâches planifiées				💌 🋃 ок
	Nom 🔺	Planification	Heure de la Heure de la	État
Autres emplacements Panneau de configuration Mes documents Documents partagés Pavoris réseau	Création d'une tâche planifée	à 12:30 le lun. tout	12:30:00 02/ Jamais	
Détails 🛛 😵				

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\<u>Sauvegarde lundi semaine1.bks</u>" /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 "<u>S:\sauvegarde\lundi semaine1.bkf</u>"*

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

Sauvegar de_lun di_semaine1	🚴 Utilitaire de sauvegarde - [sans nom]	
Tâche Planification Paramètres Sécurité	Tâche Edition Affichage Outils ?	
C:\WINDOWS\Tasks\Sauvegarde_lundi_semaine1.job Exécuter: Démarrer dans: Commentaires: Exécuter en tant que :: SRVMSREPORT\Administrat Mot de passe	Bienvenuel Sauvegarder Restaurer et gérer le média Planitier les travaux Cochez les cases des lecteurs, dossiers ou fichiers à sauvegarder. Image: Cochez les cases des lecteurs, dossiers ou fichiers à sauvegarder. Image: Cochez les cases des lecteurs, dossiers ou fichiers à sauvegarder. Image: Cochez les cases des lecteurs, dossiers ou fichiers à sauvegarder. Image: Cochez les cases des lecteurs, dossiers ou fichiers à sauvegarder. Image: Cochez les cases des lecteurs, dossiers ou fichiers à sauvegarder. Image: Cochez les cases des lecteurs, dossiers ou fichiers à sauvegarder. Image: Cochez les cases des lecteurs, dossiers ou fichiers à sauvegarder. Image: Cochez les cases des lecteurs, dossiers ou fichiers à sauvegarder. Image: Cochez les cases des lecteurs, dossiers ou fichiers à sauvegarder. Image: Cochez les cases des lecteurs, dossiers ou fichiers à sauvegarder. Image: Cochez les cases des lecteurs, dossiers ou fichiers à sauvegarder. Image: Cochez les cases des lecteurs, dossiers ou fichiers à sauvegarder. Image: Cochez les cases des lecteurs, dossiers ou fichiers à sauvegarder. Image: Cochez les cases des lecteurs, dossiers ou fichiers à sauvegarder. Image: Cochez les cases des lecteurs, dossiers ou fichiers à sauvegarder. Image: Cochez les cases des lecteurs, dossiers ou fichiers à sauvegarder. Image: Cochez les cases des lecteurs, dossiers ou fichiers à sauvegarder. Image: Cochez les cases des lecteurs, dossiers ou fichiers à sauvegarder. Image: C	mentaire
N'exécuter que si une session est ouverte Activée (la tâche planifiée s'exécute aux heures spécifiées) OK Annuler Appliquer	Effectuer la sauvegarde vers : Fichier Nom du fichier ou média de sauvegarde : A:\Backup.bkf Parcourir	Démarrer

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.

📙 Gestion de l'ordinateur						Propriétés de Événement	? 🗙
🖳 Fichier Action Affichage Fenêtre ?					×	Événement	
🗢 > 🗈 📧 🗗 🕃 😫)					Date: 28/01/2009 Sauras NTDaalum	
📃 Gestion de l'ordinateur (local)	Туре	Date	Heure	Source	Caté 🔨	Heure: 02:26:03 Catégorie: Augun	
🖻 🍒 Outils système	Informations	28/01/2009	02:26:03	ntbackup	Aucu	Type : Informations ID évén : 8019	
😑 🔝 Observateur d'événements	Informations	28/01/2009	02:26:02	ntbackup	Auci	Utilisateur: N/A	ΞL
Application	Informations	28/01/2009	02:26:01	ntbackup	Auci	Ordinateur : SBVMSBEPOBT	
Operations Manager	(Informations	28/01/2009	02:25:52	MSDTC	Disq		
Securite	Avertissem	28/01/2009	02:25:51	COM+	(105	Description :	
Docciors partagós	Informations	28/01/2009	02:25:50	ntbackup	Auci	Fin de l'opération :	
Dossiers parcages	Informations	28/01/2009	01:36:07	MsiInstaller	Auci	L'opération a réussi. Comultos la consect de convegerde pour plue de détaile	
The second secon	🔇 Erreur	28/01/2009	01:36:07	.NET Runtime	Auci	consultez le rapport de sauvegarde pour plus de details.	
Gestionnaire de périphérique	Informations	27/01/2009	23:31:25	MsiInstaller	Auci	Pour plus d'informations, consultez le centre Aide et support à l'adresse	
- Stockage	🔇 Erreur	27/01/2009	23:31:24	.NET Runtime	Aucu	http://go.microsoft.com/twlink/events.asp.	
🗄 🈭 Stockage amovible	Informations	27/01/2009	23:16:00	ESENT	Géne		
🛛 🐻 Défragmenteur de disque	Informations	27/01/2009	23:16:00	ESENT	Géne		
Gestion des disques	Informations	27/01/2009	23:11:00	ESENT	Géne	J	
🗄 🎲 Services et applications	Informations	27/01/2009	23:11:00	ESENT	Géne	Données ;	
	Informations	27/01/2009	23:10:15	SecurityCenter	Auci		
	Informations	27/01/2009	23:10:14	vmtools	Auci		-
	Avertissem	27/01/2009	19:09:52	Userenv	Auci		~
	Informations	27/01/2009	15:29:20	ESENT	Géne 🞽		
	<				>	OK Annular Assis	
						OK Annuel Appliq	uer

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 »

Général Sécurité I	st 🤶 👔	Attributs avancés	? ×
	[test.bd	Choisissez les options que vous désirez pour ce fichier.	
Type de fichier :	Document texte		
S'ouvre avec :	Bloc-notes Modifier	Attributs d'archivage et d'indexation	
Emplacement :	C:\Partage	□ h = (h + k = - 2 + 2 + 2 + + k + 2)	
Taille:	7 octets (7 octets)	I le richier est pret a etre archive	
Taille sur le disque :	4,00 Ko (4 096 octets)	$\mathbf{\nabla}$ kjutoriser l'inde <u>x</u> ation de ce fichier pour la recherche rapide	
Créé le :	mardi 27 janvier 2009, 15:45:15		
Modifié le :	mardi 27 janvier 2009, 15:45:25	Attributs de compression ou de cryptage	
Dernier accès le :	mardi 27 janvier 2009, 15:45:25	Compresser le contenu pour minimiser l'espace disque nécessa	ire
Attributs :	□ Lecture seule □ Eichier caché	Crypter le contenu pour sécuriser les données	
	OK Annuler Appliquer	OK Annu	ler

4 PROCEDURE DE RESTAURATION

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

Exécute	r 🔹 💽 🔀		
-	Entrez le nom d'un programme, dossier, document ou d'une ressource Internet, et Windows l'ouvrira pour vous.		
Ouvrir :	ntbackup 🗸		
	OK Annuler Parcourir		

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.

🖧 Utilitaire de sauvegarde - [Restaurer et gérer le média]	
Tâche Edition Affichage Outils ?	
Bienvenue I Sauvegarder Restaurer et gérer le média Planifier les travaux	
Développez le média désiré, puis cochez les éléments à restaurer. Un clic du bouton droit de la souris sur un élément de r	
	Ouvrir le fichier de sauvegarde
	Spécifiez le fichier que vous voulez cataloguer.
Restaurer les fichiers vers : Si les fichiers existent déjà : Emplacement d'origine V Ne pas remplacer Démarrer	Ouvrir : S:\sauvegarde\lundi_semaine1.bkf
	OK Annuler Parcourir

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* ».

🖏 Utilitaire de sauvegarde - [Restaurer et gérer le média]	
Tâche Edition Affichage Outils ?	
Bienvenue ! Sauvegarder Restaurer et gérer le média Planifier les travaux	
Développez le média désiré, puis cochez les éléments à restaurer. Un clic du bouton droit de la souris sur un élément de r Image: Structure in the image: Str	
	Confirmation de restauration
Restaurer les fichiers vers : Si les fichiers existent déjà :	Cliquez sur Avancé pour définir les options avancées de restauration de vos données.
Emplacement d'origine Ve pas remplacer Démarrer	Cliquez sur OK pour démarrer la restauration maintenant.
	OK Annuler Avancé

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.

	Restauration en cours	
	7	
	Lecteur :	
Options de restauration avancées	Nom: État:	Montage du média en cours
Restaurer la sécurité.	État d'avancement :	
Hestaurer les points de jonction, et restaurer vers leur emplacement d'origine les données des fichiers et des dossiers qui se trouvent sous ces points de jonction.	Durée :	Écoulée :
Lors de la restauration de jeux de données répliqués, marquer les données restaurées en tant que données principales pour tous les réplicas.	Traitement de :	
Restaure le Registre de cluster sur le quorum du disque et sur tous les autres noeuds .	Fichiers :	Traités :
Conserver les points de montage des volumes existants.	Octets :	0

La restauration s'effectue.

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