

XP & Système Fichier NTFS – sys 20 - sys 22– cours & tp-

Le Système de Fichier NTFS sous XP Michel Cabaré – Ver 1.2 – Jany 2008-

Xp & Système Fichiers NTFS Cours - TP

Michel Cabaré – Ver 1.2 – janvier 2008

www.cabare.net©

TABLE DES MATIÈRES

FAT 32 - NTFS	.4
SYSTEME DE FICHIER FAT-FAT32-NTFS :	. 4 . 4
Quana utiliser le Système NIFS :	. 5 . 5
ACCES AUX PERMISSIONS NTFS	.6
DESACTIVATION PARTAGES SIMPLIFIES :	. 6
AFFICHER PARTAGE ET SECURITE : LE CAS XP HOME :	.7 .7
SECURITE NTFS	.9
ACL ET ACE : Permissions sur Dossiers : Permissions sur fichiers :	. 9 . 9 10
PERMISSIONS STANDARD ET SPECIALES :	10
COMBINAISON FICHIER – DOSSIER EN NTFS: Exemple 1 : (fichier contre dossier). Exemple 2 : (combinaison sur dossier). Exemple 3 : (combinaison dossier).	12 12 12 12
PERMISSION NTFS ET D'AUTORISATIONS DE PARTAGE (RESEAU): <i>Exemple 1</i> : <i>Exemple 2</i> :	12 13 13 13
HERITAGE NTFS	14
NOTION D'HERITAGE CASSER UN HERITAGE RECREER UN HERITAGE RECREER PLUSIEURS HERITAGES.	14 15 15 16
PROPRIETE NTFS	17
Notion de Propriete Prendre possession des dossiers et fichiers Regles "d'affectation" des permissions NTFS:	17 17 19
COPIER-DEPLACER EN NTFS	20
CREER – COPIER DEPLACER	20 20 21 22 22 22
PERMISSIONS NTFS PAR DEFAUT	23
SUR UNE MACHINE INSTALLEE EN FAT PUIS CONVERTIE EN NTFS : Sur une machine installee en NTFS : Disque systeme XP :	23 23 24



VOIR LES AUTORISATIONS NTFS	25
AUTORISATIONS EFFECTIVES :	25 26
TP DROITS NTFS 1°	28
Objectif : Permissions de partage : Permissions de securite : Notion de Createur Proprietaire :	28 28 28 30
TP DROITS NTFS 2°	31
Objectif : Groupes et comptes : Partages : Permissions NTFS : Createur proprietaire :	31 31 32 32 34
TP APPROPRIATION DE FICHIER	35
Descriptif du probleme : Raisonnement :	35 36
TP COPIE FICHIER - PERMISSIONS	38
OBJECTIF : COMMANDE XCOPY : COPIE DE PARTAGE ? :	38 38 39





FAT 32 - NTFS

Système de Fichier Fat-Fat32-NTFS :

Comparaison des caractéristiques principales

	NTFS 4.0 - 5.0	FAT – FAT32 – FAT32X
Sécurité	Quels utilisateurs / Groupes bénéficient des différents types d'accès à un fichier ou à un répertoire.	Les fichiers ne sont pas protégés.
Journal des activités	journal des activités permettant de restaurer le disque si problèmes	pas de journal.
Services	Cryptage, Quota	Aucun service
Compression de fichier	Prend en charge la compression flexible par fichier.	La compression de fichiers n'est pas prise en charge.
Compatibilité	NT2000 gère NTFS 4.0 et 5.0	Permet l'accès aux
du système d'exploitation	NT 4.0 >= Sp4 gère NTFS 4.0 et lit NTFS 5.0 (mais ne gère pas les nouveautés)	fichiers lorsque l'ordinateur exécute un autre système d'exploitation, tel
	NT4.0 < Sp4 gère que NTFS 4.0	que MS-DOS

Comparaison des tailles de disques et de fichiers

NTFS	FAT	FAT32-FAT32X
taille minimale recommandée 10 Go	Volumes compris entre la taille d'une	Volumes compris entre 512 Mo et
taille maxi recommandée 2 Téraoctets	disquette et 2 Go	32 Go
Ne peut pas être utilisé sur des disquettes		formate jusqu'à 32 Go (peut lire plus)
La taille des fichiers est limitée	Taille maximale des	
que par la taille du volume	fichiers : 2 Go	des fichiers : 4 Go

Quant utiliser FAT32 :

Le système de fichiers FAT32, version améliorée du système de fichiers FAT, peut être utilisé sur les disques durs d'une taille comprise entre 512



mégaoctets (Mo) et 2 téraoctets (To) Mais seuls 32Giga sont adressables par Windows 2000-XP.

- Formatez la partition avec FAT32 si la partition d'installation est supérieure à 2 gigaoctets (Go) et si vous utilisez un double amorçage de Windows 2000 avec Windows 95OSR2, Windows 98.
- **N.B:** Si vous choisissez un formatage FAT lors de l'installation de Windows 2000 avec une partition supérieure à 2 Go, le formatage se fera en FAT32.

N.B: Pour une partition de plus de 32Giga, seul NTFS sera proposé

Quand utiliser le Système NTFS :

- Une sécurité d'accès pour les fichiers.
- Pour implémenter Active Directory sur un serveur
- Cryptage des fichiers : via EFS notamment.
- Quotas de disque : Analyse / contrôle d'espace utilisée par personne.
- La prise en charge de disques durs de très grande capacité très largement supérieure à celle des systèmes FAT32
- **N.B:** Si vous formatez une partition avec NTFS seul Windows NT... pourra accéder aux fichiers créés ultérieurement sur cette partition.

Versions-NTFS :

Il est possible d'avoir les versions du système NTFS par la commande

fsutil fsinfo ntfsinfo x:

C:\Users\Administrateur>fsutil	fsinfo ntfsinfo C:
Numéro de série du volume NTFS	: 0xe63cb4f03cb4bd3d
Version :	3.1

les versions stables les plus répandues sont:

- 1.2 présente avec Windows NT 4.0
- 3.0 dite aussi 5.0 apparue avec Windows 2000

Apparition de la notion de quota

3.1 dites aussi 5.1, apparue avec Windows XP, Windows Server 2003,

avec Vista, puis Seven apparition de la notion de lien symbolique vers un autre système de fichier, un dossier ou un fichier





ACCES AUX PERMISSIONS NTFS

Désactivation partages simplifiés :

Par défaut Sous un poste Xp (hors domaine) on effectue un amalgame partage réseau/ sécurité fichier

Utiliser le partage de fichiers simple (recommandé) :

Cette valeur cochée par défaut fait que lorsque l'on demande les propriétés d'un dossier on trouve un seul onglet **Partage**



Lorsque l'on désactive les partages simplifiés, dans le menu

outils / options des dossiers / affichage

ptions des dossiers	?
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	
Paramètres avancés :	
Afficher les fichiers et dossiers cachés	^
Ne pas 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 ouvertu	e
Utiliser le partage de fichiers simple (recommandé)	
	V

Alors on distingue **Partage**, et **Sécurité** – (Protection des fichiers) comme dans le chapitre suivant.



Afficher Partage et Sécurité :

A partir du moment ou l'on se trouve sur un lecteur en NTFS en cliquant sur **propriété** ...

On " D or	а	bien	accès	а	l'onglet
Par	ταξ	je –			
mai "Séc	S	aussi ité	à	JN	onglet
	Jui	110 -			

Le système NTFS sécurise l'accès au fichiers et au dossiers non seulement depuis les accès réseaux mais également depuis les accès locaux. A ce titre on sait que les permissions sont inclues dans les fichiers, dossiers, au niveau du disque lui-même

Sur un lecteur formaté NTFS on pourrait continuer à travailler avec l'onglet Partage en demandant gérer Autorisation pour les demandes d'accès depuis le réseau, mais il vaut mieux utiliser l'onglet "Sécurité" pour la sécurité. En effet ce sont les droits les plus restrictifs qui prédominent, par conséquent au niveau "Partage" on laissera le Contrôle Total à Tout le monde et on travaillera au niveau de l'onglet Sécurité

Propriétés de data ? 🗙	
Général Partage Web Partage Sécurité	
Vous pouvez partager ce dossier avec d'autres utilisateurs du réseau. Pour activer le partage de ce dossier, cliquez sur Partager ce dossier.	
O Ne pas partager ce dossier	
Partager ce dossier	
Nom du partage :	
Commentaire :	
Nombre limite d'utilisateurs : 💿 Maximum autorisé	
🖸 Autoriser 📃 🚊 utilisateurs	
Pour définir les autorisations d'accès à ce Autorisations d'accès a ce	
Pour configurer les paramètres d'accès hors connexion à ce dossier partagé, cliquez sur Mise en cache.	
Propriétés de data	1
Général Partage Web Partage Sécurité	
Nom Ajouter	
Supprimer	
Autorisations : Autoriser Refuser	
Autorisations : Autoriser Refuser	
Autorisations : Autoriser Refuser	
Autorisations : Autoriser Refuser Contrôle total Modifier Lecture et exécution	
Autorisations : Autoriser Refuser Contrôle total Modifier Lecture et exécution Afficher le contenu du dossier Lecture	
Autorisations : Autoriser Refuser Contrôle total Modifier Lecture et exécution Afficher le contenu du dossier Lecture Écriture	
Autorisations : Autoriser Refuser Contrôle total Image: Contrôle total Modifier Image: Contrôle total Lecture et exécution Image: Contrôle total Afficher le contenu du dossier Image: Contrôle total Lecture Image: Contrôle total Écriture Image: Contrôle total Autoriser Image: Contrôle total	
Autorisations : Autoriser Refuser Contrôle total Image: Contrôle total Modifier Image: Contrôle total Lecture et exécution Image: Contrôle total Afficher le contenu du dossier Image: Contrôle total Afficher le contenu du dossier Image: Contenu du dossier Lecture Image: Contenu du dossier Écriture Image: Contenu du dossier Avancé Image: Contenu du dossier Empattre aux autorisations pouvant être béritées du parent	

Le cas XP HOME :

Affichage « temporaire » des sécurité NTFS

Sur un poste XP home, l'onglet sécurité n'apparaît pas... vous pouvez accéder tout de même à l'onglet sécurité après avoir

- démarré en mode sans échec (via F8 lors du boot)
- et s'être connecté avec le compte Administrateur (celui crée lors de l'installation de XP, et pas simplement un compte ayant des droits d'administration)
- Désormais si le lecteur est en NTFS, les propriétés du dossier affichent un onglet sécurité !
- Après modifications éventuelles et re-démarrage, l'onglet disparaît...

L'idée générale est donc de ne pas permettre en standard l'affichage du panneau sécurité NTFS pour un poste Windows HOME



Malgré ce que l'on vient de dire précédemment, il est possible de demander de faire afficher systématiquement l'onglet de gestion de la sécurité NTFS, mais cette opération n'est pas supportée par microsoft, et ne doit en aucun cas être généralisée...

Avec un fichier scesp4i.exe (en provenance serveur FTP microsoft)

1. Télécharger le "Security Configuration Manager" de Windows NT4, disponible chez Microsoft :

ftp://ftp.microsoft.com/bussys/winnt/winnt-public/tools/scm/scesp4i.exe (Taille : 2.68 Mo)

- 2. Ne pas exécuter directement le fichier **scesp4i.exe**, mais le décompresser (avec Winzip, Winrar,..) dans un dossier quelconque (par exemple c:\scesp4i).
- 3. Effectuer un clic droit sur le fichier SETUP.INF qui se trouve dans ce dossier (attention, il existe plusieurs fichiers xxxx.INF), puis sélectionner "Installer"

En effet, si on l'exécute, une routine de détection de version du système est lancée, et, constatant qu'on n'est pas sous NT4, refuse l'installation !

- 4. Un écran vous demande alors si vous souhaitez remplacer le fichier ESENT.DLL, refusez en cliquant sur NON POUR TOUS (Ne cliquez en aucun cas sur oui, cela rendrait votre système instable!)
- 5. Redémarrer votre poste de travail

Avec un fichier **ntfs.exe** (en provenance de NT4.0)

- 1. installer l'utilitaire NTFS.EXE
- 2. Dans le répertoire de décompression, sélectionnez SETUP.INF, click droit/Installer
- 3. Un écran vous demande alors si vous souhaitez remplacer le fichier ESENT.DLL, refusez en cliquant sur NON POUR TOUS (Ne cliquez en aucun cas sur oui, cela rendrait votre système instable!)
- 4. Redémarrer votre poste de travail





SECURITE NTFS

ACL et ACE :

Le système NTFS stocke une liste de contrôle d'accès nommée ACL (Access Control List) associée à chaque fichier et dossier d'une partition NTFS.

La liste ACL contient tous les groupes d'utilisateurs; tous les utilisateurs bénéficiant de l'accès au dossier ou au fichier, avec le type d'accès qui leur est accordé.

Pour qu'un utilisateur puisse accéder à un fichier ou à un dossier, la liste ACL de ce fichier dossier doit contenir une entrée, appelée ACE (Access Control Entry) auquel l'utilisateur est associé.

Si aucune entrée **ACE** n'existe dans la liste **ACL** de la ressource, l'utilisateur ne peut accéder à cette ressource.

Permissions sur Dossiers :

Il est possible en NTFS de définir 6 sortes principales de permissions sur un dossier, via l'onglet **Sécurité**

iénéral Partage Sécurité Perso	nnaliser	
Noms d'utilisateur ou de groupe :		
🕵 Administrateur (SRV1-XP\Adm	iinistrateur)	
🕂 🖉 Administrateurs (SRV1-XP\Adr	ministrateurs)	
CREATEUR PROPRIETAIRE		
SYSTEM		
🕵 Utilisateurs (SRV1-XP\Utilisate	eurs)	
[Alau tau	. ·
	Alouter	Supprimer
L	Alouter	Supprimer
Autorisations pour Administrateur	Alouter	Supprimer Refuser
Autorisations pour Administrateur Contrôle total	Alouter	Refuser
Autorisations pour Administrateur Contrôle total Modification	Alouter	
L Autorisations pour Administrateur Contrôle total Modification Lecture et exécution	Alouter	Refuser
Autorisations pour Administrateur Contrôle total Modification Lecture et exécution Affichage du contenu du dossier		Refuser
Autorisations pour Administrateur Contrôle total Modification Lecture et exécution Affichage du contenu du dossier Lecture		Refuser
Autorisations pour Administrateur Contrôle total Modification Lecture et exécution Affichage du contenu du dossier Lecture Écriture		Refuser

Ces 6 combinaisons standard, peuvent être **héritées** (dans ce cas elles sont grisées)

Et ont deux valeurs possibles Autoriser, ou Refuser

Les autorisations Spéciales ne sont que des combinaisons particulières (détaillées dans permissions spéciales plus loin), posées entre les dossiers et les fichiers... Il n'est pas nécessaire de s'en préoccuper car elles sont gérées automatiquement souvent par le système



Permissions sur fichiers :

Il est possible en NTFS de définir 5 sortes principales de permissions Il manque afficher) sur un fichier, via l'onglet **Sécurité**

priétés de Nouveau Document texte	.txt	?
iénéral Sécurité Résumé		
Noms d'utilisateur ou de groupe :		
🕵 Administrateur (SRV1-XP\Administrateur)		
🕵 Administrateurs (SRV1-XP\Administrateurs	:)	
🕵 SYSTEM		
🕵 Utilisateurs (SRV1-XP\Utilisateurs)		
	Ajouter Supprime	r
Autorisations pour Administrateur	Autoriser Refuser	_
Contrôle total		
	×	
Modification		
Modification Lecture et exécution		
Modification Lecture et exécution Lecture		
Modification Lecture et exécution Lecture Écriture		

Ces 5 combinaisons standard, peuvent être **héritées** (dans ce cas elles sont grisées)

Et ont deux valeurs possibles **Autoriser**, ou **Refuser**

 \rightarrow

N.B: DANS UN SOUCIS DE SIMPLIFICATION, ON NE DEVRAIT JAMAIS DONNER DES PERMISSIONS AU NIVEAU DES FICHIERS, MAIS TOUJOURS PLUS GLOBALEMENT AU NIVEAU DES DOSSIERS

Permissions standard et spéciales :

En fait, les permissions standards, ne sont qu'une combinaison prédéfinie d'un certain nombre de permissions spéciales, plus fines

Autorisations spéciales	Contrôle total	Modifier	Lire & exécuter	Afficher le contenu du dossier (dossiers uniquement)	Lecture	Écriture
Parcourir le dossier / Exécuter le fichier	×	×	×	×		
Liste du dossier / Lecture de données	×	×	×	×	×	
Attributs de lecture	×	×	×	×	×	
Lire les attributs étendus	×	×	×	×	×	
Création de fichiers / Écriture de données	×	×				×
Création de dossiers / Ajout de données	×	×				×
Attributs d'écriture	×	×				×
Écriture d'attributs étendus	×	×				×
Suppression de sous- dossiers et de fichiers	×					
Supprimer	×	×				
Autorisations de lecture	×	×	×	×	×	×
Modifier les autorisations	×					
Appropriation	×					
Synchroniser	×	×	×	×	×	×

Autorisations de fichier et de dossier

N.B: ici il y a une différence importante entre Modifier et Contrôle Total, c'est la possibilité de supprimer ou non les sous-dossier ...

N.B: DANS UN SOUCIS DE SIMPLIFICATION, ON NE DEVRAIT JAMAIS DANS UN 1° TEMPS TRAVAILLER AU NIVAU DES PERMISSIONS SPECIALES MAIS TOUJOURS AU NIVEAU DES PERMISSIONS STANDARDS...





Microsoft détaille les permissions spéciales ainsi:

Parcourir le dossier / Exécuter le fichier	 Pour les dossiers : L'autorisation Parcourir le dossier permet à l'utilisateur de se déplacer dans les dossiers pour atteindre d'autres dossiers ou fichiers, même s'il n'est pas muni des autorisations correspondant aux dossiers ainsi parcourus (cette autorisation s'applique uniquement aux dossiers). Elle n'est effective que lorsque le groupe ou l'utilisateur n'a pas reçu le droit Outrepasser le contrôle de parcours dans le composant logiciel enfichable Stratégie de groupe (par défaut, ce droit est octroyé au groupe Tout le monde). Pour les fichiers : L'autorisation Exécuter le fichier permet ou interdit l'exécution de fichiers programmes (cette autorisation s'applique uniquement à des fichiers). L'établissement de l'autorisation Exécuter le fichier sur tous les fichiers contenus dans le dossier.
Liste du dossier / Lecture de données	L'autorisation Liste du dossier permet ou interdit l'affichage des noms des fichiers et des sous-dossiers contenus dans le dossier. Cette autorisation affecte uniquement le contenu de ce dossier et n'a aucune influence sur l'affichage ou non du dossier pour lequel vous définissez l'autorisation. Cette autorisation s'applique uniquement aux dossiers. L'autorisation Lecture de données permet ou interdit l'affichage des données des fichiers (cette autorisation s'applique uniquement aux fichiers).
Attributs de lecture	Permet ou interdit l'affichage des attributs d'un fichier ou d'un dossier, tels que les attributs Lecture seule ou Masqué. Les attributs sont définis par le système de fichiers NTFS.
Lire les attributs étendus	Permet ou interdit l'affichage des attributs étendus d'un fichier ou d'un dossier. Les attributs étendus sont définis par des programmes et peuvent varier selon le programme utilisé.
Création de fichiers / Écriture de données	L'autorisation Création de fichiers permet ou interdit de créer des fichiers au sein du dossier (cette autorisation ne s'applique qu'aux dossiers). L'autorisation Écriture de données permet ou interdit de modifier le fichier et d'en remplacer le contenu actuel (cette autorisation ne s'applique qu'aux fichiers).
Création de dossiers / Ajout de données	L'autorisation Création de dossiers permet ou interdit de créer des dossiers au sein du dossier (cette autorisation ne s'applique qu'aux dossiers). L'autorisation Ajout de données permet ou interdit de modifier la fin du fichier mais pas de modifier, de supprimer ou de remplacer les données existantes (cette autorisation ne s'applique qu'aux fichiers).
Suppression de sous-dossiers et de fichiers	Permet ou interdit de supprimer des sous-dossiers et des fichiers même si l'autorisation Supprimer n'a pas été octroyée pour le sous-dossier ou le fichier concerné (cette autorisation s'applique à des dossiers).
Supprimer	Permet ou interdit de supprimer le fichier ou le dossier. Vous pouvez supprimer un fichier ou un dossier sur lequel vous ne possédez pas l'autorisation Supprimer si vous disposez de l'autorisation Suppression de sous-dossiers et de fichiers relative au dossier parent.
Autorisations de lecture	Permet ou interdit les autorisations de lecture du fichier ou du dossier, telles que Contrôle total, Lecture et Écriture.
Modifier les autorisations	Permet ou interdit de modifier les autorisations du fichier ou du dossier, telles que Contrôle total, Lecture et Écriture.
Appropriation	Permet ou interdit de prendre possession du fichier ou du dossier. Le propriétaire d'un fichier ou d'un dossier peut en modifier les autorisations à tout moment, indépendamment des autorisations existantes.

Avec encore

Attributs d'écriture	Permet ou interdit de modifier les attributs d'un fichier ou d'un dossier tels que les attributs Lecture seule ou Masqué. Les attributs sont définis par le système de fichiers NTFS.
Écriture d'attributs étendus	Permet ou interdit la modification des attributs étendus d'un fichier ou d'un dossier. Les attributs étendus sont définis par des programmes et peuvent varier selon le programme utilisé. L'autorisation Écriture d'attributs étendus n'implique pas la création ou la suppression de fichiers ou de dossiers : elle inclut uniquement l'autorisation de modifier les attributs d'un fichier ou d'un dossier. Pour
Synchroniser	Permet ou interdit que des threads différentes attendent le handle du fichier ou du dossier et se synchronisent à une autre thread qui l'a signalé. Cette autorisation s'applique uniquement aux programmes multi-thread et multitraitement.





Combinaison Fichier – Dossier en NTFS:

Plusieurs règles régissent les combinaisons de permission NTFS

- 1. Les permissions de fichier **sont prioritaires** par rapport aux permissions affectées aux dossiers qui les contiennent :
- 2. la permission effective de l'utilisateur est la permission la moins restrictive obtenue par la **combinaison des différentes permissions**
- 3. si la permission "aucun accès" est donnée, cette dernière **prime sur** les autres permissions, et la permission effective est "aucun accès"

Donc si l'utilisateur est membre de plusieurs groupes, la permissions résultant finale est :

la somme de toutes les permissions définies à travers chacun des groupes,

sauf si la permission "aucun accès" est spécifiée pour au moins un groupe !

Exemple 1 : (fichier contre dossier)

Un utilisateur ayant le droit "lire" pour un dossier, et un droit "écrire" pour un fichier de ce même dossier,

alors il pourra modifier le fichier (écrire dedans) mais pas créer un autre fichier dans ce dossier...

Exemple 2 : (combinaison sur dossier)

Un utilisateur Util1 dispose de la permission Ecrire sur un dossier Données



mais **Util1** est également membre d'un groupe "**Tout le monde**" qui dispose de la permission **Lire** sur ce même dossier

Util1 se retrouve avec la permission Lire et ecrire sur ce dossier Données

Exemple 3 : (combinaison dossier - fichier)

Un utilisateur **Util1** dispose de la permission **Lire** et **Ecrire** sur un fichier **Fichier1** du dossier **Données**



mais Util1 est également membre d'un groupe "commerciaux" qui dispose des permissions lire sur ce même dossier Données

Util1 se retrouve avec la permission Lire sur ce dossier Données mais avec Lire et Ecrire sur le fichier Fichier1 du dossier Données





Permission NTFS et d'Autorisations de partage (réseau):

Dans ce cas, la résultante est la combinaison la plus restrictive des deux

Exemple 1 :

Un utilisateur **Util1** dispose lors d'une connexion réseau de l' **autorisation** "**lire**" au niveau du partage pour un dossier partagé nommé **public** ,sur un

ordinateur1 et de la permission NTFS contrôle total sur un fichier A s'y trouvant.

1 	Do	ossie	rs	×	Nom
r			- 🗐 public		🖹 A.txt

Q: Quelle est la permission effective de **Util1** lorsqu'il accède au fichier **A** à travers **l'accès réseau** au dossier partagé **Données** ?

R: Depuis un accès réseau la permission effective de Util1 pour le fichier A est lire car celle-ci est plus restrictive que celle attribuée en NTFS localement, et s'applique



R: Depuis une session locale sur ordinateur1 la permission effective de Util1 pour le fichier A est contrôle total

Exemple 2 :

Un dossier **Données** est crée avec à l'intérieur 3 sous-dossiers nommés **Dutil1**, **Dutil2** et **Dutil3** respectivement

🗋 Dor	nnées
	Dutil1
	Dutil2
	Dutil3

Le dossier **Données** est partagé avec l'autorisation **contrôle total** pour un groupe Utilisateurs.

🗟 Do	nnées
	Dutil1
·	Dutil2
·	Dutil3

Les 3 Utilisateurs Util1, Util2 et Util3 font partie du groupe Utilisateurs mais ne disposent de la permission NTFS contrôle total que pour leur propre dossier

Q : Quelle est la permission effective de Util1 lorsqu'il accède au dossier Dutil1 à travers l'accès réseau au dossier partagé Données ?

R: Util1 dispose de la permission contrôle total sur le dossier Données et son dossier Dutil1

] Q : Quelle est la permission effective de Util2 pour le dossier Dutil1

R : Util2 ne bénéficie pas de l'accès au dossier Dutil1 car la permission NTFS contrôle total sur ce dossier à été attribuée uniquement a Utils1





HERITAGE NTFS

Notion d'héritage

Donc lorsque l'on **crée** un dossier (ou respectivement un fichier), celui-ci **hérite** des droits du dossier à l'intérieur duquel il a été crée

Visuellement cela se traduit par le fait que les propriétés sont grisées, et semblent donc non modifiables.

ropriétés de Nouveau dossier Général Partage Sécurité Personna Noms d'utilisateur ou de groupe : Administrateur (SRV1-XP\Administ	liser rateur)	?	
Administrateus (SRVTXP Vadminis CREATEUR PROPRIETAIRE SYSTEM Utilisateurs (SRVTXP\Utilisateurs) Autorisations pour Utilisateurs	jouter	Supprimer	Ici le groupe des utilisateurs est manifestement en lecture seule, non modifiable Il serait possible de rajouter
Contrôle total Modification Lecture et exécution Affichage du contenu du dossier Lecture Écriture Autorisations spéciales			des permissions Modification Mais pas de modifier les permissions existantes

Si on modifie les permissions des parents, seuls sont concernés alors ensuite dans l'arborescence ceux qui ont accepté l'héritage (sous NT 4 on demandait d'appliquer au dossier et aux fichiers ... sans discrimination !)

- **NB**: Si les autorisations de l'objet ont été **héritées** de l'objet parent. Les modifications peuvent s'effectuer de trois manières :
 - Exécutez les modifications sur l'objet parent ; l'objet héritera alors de ces autorisations.
 - Sélectionnez l'autorisation opposée (Autoriser ou Refuser) pour substituer l'autorisation héritée.
 PEU CONSEILLE !
 - Casse l'héritage en désactivant la case à cocher
 Permettre aux autorisations pouvant être héritées du parent d'être propagées à cet objet.
 On peut alors modifier les autorisations et supprimer des utilisateurs.

On peut alors modifier les autorisations et supprimer des utilisateurs ou des groupes. Mais l'objet n'héritera plus de l'objet parent...



Casser un héritage

N.B : si on veut pouvoir modifier directement les permissions, il est nécessaire d'abords de désactiver la case à cocher « Permettre aux autorisations pouvant être héritées du parent... »

	Hérite	de l'obje	t parent le	es entrées	d'autorisati	on qui s'a	appliquent	aux objets	enfants.	Cela incl	ut les
×.	objets	dont les	entrées s	ont spécifi	quement d	éfinies ici	i.				

Dans ce cas, on peut choisir si on veut les supprimer complètement ou les appliquer à notre arborescence mais pouvoir les modifier...

Sécurité			_	×	
?	Sélectionner cette opti parent qui s'appliquent objet.	on signifie que aux objets enf	les entrées d'autoris ants ne vont plus s'a	ations de l'objet ppliquer à cet	
4	 Pour copier les entrée appliquées du parent à 	es d'autorisatior a cet objet, cliqu	ns qui ont été précéo Jez sur Copier.	lemment	
	 Pour supprimer les en appliquées à partir de l' autorisations définies ic 	trées d'autorisa 'objet parent et si, cliquez sur S	ations qui ont été pré conserver uniquem upprimer.	cédemment ent les	
	- Pour annuler cette ac	tion, cliquer su	r Annuler.		
	Copier	Supprimer	Annuler		
Si Cop	bier			Si Su	pprimer
- Ioms d'utilis	sateur ou de groupe :				
🖸 Admini	istrateur (SBV1-XP\Admini	istrateur)		Général Partage S	écurité Personnaliser
🚮 Admini	istrateurs (SRV1-XP\Admi	nistrateurs)		Nesse d'utilisations au	
🕵 CREA	TEUR PROPRIETAIRE				lue groupe :
🕵 SYSTE	EM				
🖋 Utilisat	teurs (SRV1-XP\Utilisateur	rs)			
		Ajouter	Supprimer		
utorisation	s pour Utilisateurs	Autoriser	Refuser		
Contrôle	total		~		Ajouter
Modificat	tion			Autorisations	Autorise
Lecture e	et exécution	\checkmark		Autorisations	Autorise
Affichage	e du contenu du dossier	\checkmark		Contrôle total	
Lecture		\checkmark		Modification	
Écriture				Lecture et execut	
Autorisati	ions spéciales	V		Amenage du cont	
				Écriture	
				Londie	

Recréer un héritage

Soit un dossier **test-ntfs**, sur lequel , après avoir cassé l'héritage en supprimant toutes les permissions, on a posé la sécurité suivante :

Supprimer

Refuser

Compte Administrateur Contrôle Total

Groupe Tout le Monde Lecture Seule

On crée un sous dossier sous-test. Vérifier de quoi ce sous dossier hérite...

	<u>test-ntfs</u>	
±	🛅 sous-tes	t

En se replaçant sur le dossier **test-ntfs** on reconstruit l'héritage d'origine en cochant **Hérite de l'objet parent...**

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.

Vérifier les nouvelles permissions ...



Recréer plusieurs héritages

Soit un dossier **test-ntfs**, sur lequel , après avoir cassé l'héritage en supprimant toutes les permissions, on a posé la sécurité suivante :

Compte Administrateur Contrôle Total

Groupe Tout le Monde Lecture Seule

On construit trois sous-dossiers, respectivement **sstest1**, **sstest2**, **sstest3**, qui héritent donc de la sécurité du dossier parent.



pour sstest1 on, casse l'héritage en copiant les permissions

pour sstest2 on, casse l'héritage en supprimant les permissions

pour **sstest3** on, casse l'héritage en copiant les permissions et ajout du groupe des utilisateur- en Modifier

On souhaite ensuite "retrouver" notre structure de départ :

Il faut depuis le dossier test-ntfs, demander la case à cocher

Remplacer les entres d'autorisation de tous les objets enfants...

Remplacer les entrées d'autorisations de tous les objets enfants par les entrées affichées ici et qui s'appliquent aux objets enfants

Туре	Nom	Autorisation	Héritée de	Appliquer à
Autoriser A	Administrateur (TRAV	Contrôle total	<non héritée=""></non>	Ce dossier, les sous-d
Autoriser 1	Tout le monde	Lecture et exéc	<non héritée=""></non>	Ce dossier, les sous-d
Ajouter.	Modifier			
Hérite de objets do	l'objet parent les entrées nt les entrées sont spéci	s d'autorisation qui s'a fiquement définies ici	appliquent aux objel	ts enfants. Cela inclut les
Remplac s'applique	er les entrées d'autorisati ent aux objets enfants	ions de tous les objet	s enfants par les er	trées affichées ici et qui
_				





PROPRIETE NTFS

Notion de Propriété

Par défaut l'utilisateur qui crée un dossier ou un fichier en est le propriétaire.

C'est la raison du groupe prédéfini **Créateur Propriétaire**, qui est géré automatiquement par Windows (on ne peut spécifier qui fait partie de ce groupe, ni savoir qui en fait partie... cela dépends de l'objet que l'on pointe !)

N.B : En tant que propriétaire on peut <u>toujours redéfinir des permissions</u> de dossier ou son fichier.

Un utilisateur peut attribuer la permission "**Prendre possession**" aux autres utilisateurs ou groupe

Pour connaître qui est propriétaire d'un objet, on demande pour un dossier-

fichier

onglet Propriétaire



Prendre possession des dossiers et fichiers

Paramètres avancés

On peut s'approprier un objet :

- si on en a les droits
- si l'on est administrateur

Mais on ne peut pas « rendre » la propriété... Un administrateur ne peut pas "donner" une ressource, le futur propriétaire doit toujours se l'approprier...

Ce qui fait que cela ne peut pas se faire à l'insu du propriétaire légitime...





par défaut les membres du groupe Administrateurs ont toujours la possibilité de prendre possession d'un fichier :

- en ouvrant une session en tant qu'Administrateur
- a partir de l'onglet sécurité on peut demander avancé pour déterminer le propriétaire ou sur Appropriation pour "devenir" le propriétaire

imaginons que cela soit toto qui ait crée le dossier sous-test

🛅 test	-ntfs
	<u>sous-test</u>

En tant qu'administrateur, si on va regarder qui est propriétaire de ce dossier on trouve normalement toto...

itorisations Audit	Propriétaire	Autorisations effectives	
/ous pouvez vous a	pproprier un o	bjet si vous disposez des autorisations nécessaires.	
Propriétaire actuel d	e cet élément :		
toto (SRV1-XP\toto)		
Sélectionner un nou	veau propriéta	aire :	
Nom			
🕵 Administrateur	(SRV1-XP\Adi	ministrateur)	
🕵 Administrateurs	(SRV1-XPVA	dministrateurs)	



Et éventuellement tout le contenu de l'arborescence...

N.B: cela ne change en aucune manière pour l'instant les permissions existante, sauf que maintenant l'administrateur <u>aussi</u> a le droit de travailler et modifier la sécurité dans ce dossier...

N.B: mais pas à l'insu de l'utilisateur toto, qui, s'il demande qui est le propriétaire de son dossier va voir désormais

Propriétaire actuel de cet élément :
Administrateur (SRV1-XP\Administrateur)
Sélectionner un nouveau propriétaire :
Nom
🕜 A desinistratour (CD) (1 VD) A desinistratour)
Administrateur (Shivit Ar Vadministrateur)

EXEMPLE :

Si un utilisateur quitte la société (compte supprimé), l'administrateur prends possession du fichier, et modifie les permissions afin de ré-autoriser l'accès à cette donnée à un autre utilisateur, qui pourra alors s'approprier cette donnée...



Règles "d'affectation" des permissions NTFS:

Deux règles essentielles existent

Pour les dossiers contenant des programmes

- 1. Enlever la permissions par défaut "Contrôle total" attribuée à tout le monde, et la donner uniquement au Groupe des administrateurs
- 2. Pour les responsables des mises à jour, donner une permissions contrôle total
- 3. Pour les utilisateurs, s'ils doivent avoir accès au dossier, donner une permissions lecture seule

Pour les dossiers contenant des données

- 1. Enlever la permissions par défaut "Contrôle total" attribuée à tout le monde, et la donner uniquement au Groupe des administrateurs
- 2. Pour les utilisateur donner la permission lire et modifier, et au groupe Créateur Propriétaire la permission Contrôle Total. Cela permet aux utilisateurs locaux de ne détruire ou de modifier que les dossiers et les fichiers qu'ils copient ou créent sur l'ordinateur local





COPIER-DEPLACER EN NTFS

Créer – Copier- - Déplacer

Lorsque l'on **crée** un dossier, celui-ci hérite des droits du dossier à l'intérieur duquel il a été crée

Lorsque l'on **copie** un dossier ou des fichiers, les permissions **héritées** sont celles du dossier de destination. De plus, l'utilisateur qui réalise la copie **devient le propriétaire** du dossier ou du fichier.

Pour une **copie**, les permissions nécessaires sont les suivantes :

permission **lire** sur le **dossier d'origine**

permission ajouter sur le dossier de destination

Lorsque l'on **déplace** un dossier ou un fichier à l'intérieur de la même unité de disque, ses permissions d'origine ainsi que son appartenance sont maintenues. Mais si on effectue le déplacement entre différentes unités de disque; on se retrouve comme pour une copie !

Pour un **déplacement**, les permissions nécessaires sont les suivantes :

permission ajouter sur le dossier de destination

permission Modifier ou Contrôle total sur le dossier d'origine

N.B: bien sur toute copie/déplacement sur des unités FAT entraîne alors une perte de toutes les permissions !

Sensibilisation aux finesses de l'interface

Penser à sensibiliser vos utilisateurs à l'interface graphique ne faisant pas la même chose selon ce que :

- On glisse dans le même lecteur... (déplacer)
- On glisse d'un lecteur à l'autre... (copier)
- On glisse avec CTRL appuyé... (copier)

Et aux... copier/couper/coller...





Хсору

Il est possible de copier les fichiers en gardant leur permissions, mais en utilisant une commande en ligne



parmi la multitude d'option, les plus intéressantes dans notre cas sont

/o /s

voire une combinaison du genre /s /e/c /o ou du genre /c /h /o /s /e ...

∕A	Copie uniquement les fichiers ayant l'attribut archive, ne modifie pas l'attribut.
∠ M	Copie uniquement les fichiers ayant l'attribut archive,
(D: :	Contra la fistione madifié à mantin de la date enérgifiée
∕⊅•⊪−J−a	Copie les fichiers moutries à partir de la date specifiée.
	Si aucune date n'est donnee, copie uniquement les fichiers dont
VENCT HIDE . C .	I neure source est plus recente que i neure de destination.
/ENCLODE I IC	nitt finzitt finzit.
	apecifie une fiste de fichiers contenant des chaines, quand une
	de ces chaines se retrouve dans le chemin d'acces absolu au
	fichier a copier, ce fichier est exclu de la copie. Far exemple,
	specifier une chaine telle que (obj) ou cobj exclura tous les
	fichters au repertoire ong ou tous les fichters aont l'extension
2D	est .ong, respectivement.
/r /0	Conta las vérente avait la creation de chaque fichier de destination.
/0	wide
/E	Contra las vénentaines et seus-réportaines - « sempris vides
/E	Identicue à Ce /E Deut âtre utilies pertoires, y compris viues.
11	lientique a 73 /E. Feut etre utilise pour mourier /I.
20	leve demande d'annuer our une touche auant la conie
10	Continue a appuyer sur une couche avant la copie.
1	Continuer la copie meme si ues erreurs se produisent.
/1	an la destination n'existe pas et que plus u un richier est
/ 0	Nofich assume que la destination est un repertoire.
	A arriche pas les nome se richters tors de la copie.
	Afficha las fichians qui sensient conjés
	Conja ágalament las fichians cachás et las fichians sustàme
	Dampic equipment its itentity caula soula
	Code la stuicture de vénertaires mais ne conje nas les fichiers
/ 1	N'inclut nas les vénertoires ou sous-rénertoires uides /T/F
	inclut les vénertaires et sous-vénertaires uides.
211	Conje seulement les fichiers qui existent délà en destination
∠ K	Conie les attributs. Xconu normal rétablira les attributs de
, 11	lecture seule.
∠N	Conie en utilisant les noms courts générés.
20	Conie les informations d'annartenance et d'ACL des fichiers.
ZX	Copie les paramètres d'audit de fichiers (implique /0).
2Y	Supprime la demande de confirmation de remplacement de
	fichiers de destination existants.
/-Y	Provogue la demande de confirmation de remplacement d'un fichier
	de destination existant.
/Z	Copie les fichiers du réseau en mode redémarrable.

Sur une commande du genre, histoire de garder une trace des messages d'erreur, il semblerait bon de rediriger la sortie par défaut dans un fichier texte

Genre xcopy c:*.* d:*.* /s/e/c/o > info.txt

ici > info.txt permet de rediriger le flux de la sortie video par défaut dans un fichier nommé info.txt



Cacls

En standard, depuis 2000 PRO, Permet d'avoir un information sur les permissions NTFS, voire de les modifier.

E:\data>cacls Affiche ou modifie les listes de contrôle d'accès (ACL) des fichiers CACLS nom_de_fichier [/T] [/E] [/C] [/G util:perm] [/R util [...]] nom_de_fichier [/T] [/E] [/C] [/G util:perm] [/R util [...]] nom_de_fichier Affiche les ACL. /T Modifie les ACL des fichiers spécifiés dans le répertoire en cours et tous les sous-répertoires. /E Édite l'ACL au lieu de la remplacer. /C Continue la modification des ACL en ignorant les erreurs. /G util:perm Donne à l'utilisateur spécifié les droits d'accès. Perm peut être : R Lecture W Écriture C Modification (en écriture) F Contrôle total /R util Retire les droits d'accès de l'utilisateur (avec /E). /P util:perm Remplace les droits d'accès de l'utilisateur spécifié. Perm peut être : N Aucun R Lecture W Écriture C Modification (en écriture) F Contrôle total /D util Refuse l'accès à l'utilisateur spécifié. Des caractères génériques peuvent être utilisés pour préciser plusieurs fichiers dans une commande. Vous pouvez spécifier plus d'un utilisateur dans une commande.

.exe

Xcacls

Utilitaire fourni avec le kit de ressource technique 2000 Pro,

Qı	uick Details	
	File Name:	xcacls_setup
	Version:	1.00.0.1
	Date Published:	5/15/2002
	Language:	English
	Download Size:	582 KB

SubInACL

Utilitaire fourni avec le kit de ressource technique 2000 Pro,

Quick	Details	
File	Name	

Version: 5.2.3790.11	80
Date Published: 6/14/2004	
Language: English	
Download Size: 371 KB	



PERMISSIONS NTFS PAR DEFAUT

Sur une machine installée en FAT puis convertie en NTFS :

De manière générale les permissions données sur le disque sont partout de type **Everyone – Full Control**

Sur une machine installée en NTFS :

Les dossiers Program Files et Documents & settings

	C:\Documents and Settings\Administrator and <subfolders> Administrator - Full Control Administrators - Full Control System - Full Control</subfolders>
C:\Program Files and <subfolders> Administrators - Full Control Creator/Owner - Full Control Users - Read System - Full Control Power Users - Change Terminal Server User - Change</subfolders>	C:\Documents and Settings\All Users and <subfolders> Administrators - Full Control Power Users - Change Users - Read Everyone - Read System - Full Control</subfolders>
C:\Documents and Settings Administrators - Full Control Power Users - Read Everyone - Read Users - Read System - Full Control	C:\Documents and Settings\Default User and <subfolders> Administrators - Full Control Power Users - Read Users - Read Everyone - Read System - Full Control</subfolders>

Les dossiers %SystemRoot%

	C:\%SystemRoot%\System	
	Administrators- Full Control	C:\%SystemRoot%\System32\Config
	Creator/Owner - Full Control	Administrators- Full Control
	Power Users - Change	Creator/Owner - Full Control
	Users - Read	Power Users - Read
	System - Full Control	Users - Read
		System - Full Control
C:\%SystemRoot%	C:\%SystemRoot%\System32	
Administrators- Full Control	Administrators- Full Control	C:\%SystemRoot%\System32\Dhcp
Creator/Owner - Full Control	Creator/Owner - Full Control	Administrators- Full Control
Everyone - Read	Power Users - Change	Creator/Owner - Full Control
Power Users - Change	Users - Read	Power Users - Read
Users - Read	Everyone - Read	Users - Read
System - Full Control	System - Full Control	System - Full Control

et de manière générale

```
Any other folders
Administrators- Full Control
Creator/Owner - Full Control
Power Users - Change
Users - Read
System - Full Control
```



Windows XP & Système NTFS http://www.cabare.net Page 23 - SYS 20 - SYS 22 - Cours TP - ver 1.2 - Michel Cabaré -

Disque système XP :

Administrateurs (SRV1-XP\Administrateurs)

Autorisations pour Administrateurs	Autoriser
Contrôle total	>
Modification	×
Lecture et exécution	×
Affichage du contenu du dossier	×
Lecture	\$
Écriture	>

Dieu a tout pouvoir...

CREAT	EUR PROPRIETAIRE			
	Autorisations spéciales	4]	Ļ
	Autoriser CREATEUR PROPRI	Contrôle total	<non héritée=""></non>	Les sous-dossiers et l
	Si j'ai pu créer , j'ai tout p	pouvoir dans l	es sous-dossier	et fichiers
SYSTE	м			
	Autorisations pour SYSTEM	Autoris	ser	

Α	utorisations pour SYSTEM	Autoriser
ſ	Contrôle total	×
L	Modification	\checkmark
L	Lecture et exécution	\checkmark
L	Affichage du contenu du dossier	\checkmark
L	Lecture	\checkmark
	Écriture	\checkmark

Windows a tout pouvoir...

💅 Tout le	monde		
	Autorisations spéciales	V	\downarrow
	Autoriser Tout le monde	Lecture et exéc <non héritée=""></non>	Ce dossier seulement

Tout le monde (authentifié) peut lire la racine du disque ...

🕵 Utilisateurs (SRV1-XP\Utilisateurs) Autorisations pour Utilisateurs Autoriser Modification \checkmark Lecture et exécution Affichage du contenu du dossier \checkmark \checkmark Lecture Écriture Autorisations spéciales Autoriser Utilisateurs (SRV1-XP... Lecture et exéc... <non héritée> Ce dossier, les sous-d... Autoriser Utilisateurs (SRV1-XP... Création de dos... <non héritée> Ce dossier et les sous-... Autoriser Utilisateurs (SRV1-XP... Création de fichi... <non héritée> Les sous-dossiers seul...

Les utilisateur (de ce poste) peuvent tout lire, créer un dossier et des sous dossier, et des fichier dans les dossiers et sous dossier, mais pas à la racine du disque.



VOIR LES AUTORISATIONS NTFS

Autorisations effectives :

On peut connaître les autorisations qu'un utilisateur ou un groupe possède sur un objet à l'aide des autorisations effectives. On demande pour un

dossier Paramètres avancés

Et dans l'onglet Autorisations effectives on peut alors donner un nom

ramètres de Autorisations A	sécurité avano Idit Propriétaire	cé pour Nouveau Autorisations effec	u dossier tives		?
La liste suivante en se basant su	affiche les autoris r les autorisations (- ations qui vont être a appropriées.	accordées au j	groupe ou à l'utili:	sateur sélectionné,
Nom de groupe	ou d'utilisateur :				
					Sélectionner
Autorisations eff	ectives : tal				
Parcours d	u dossier/exécute	r le fichier			
🔲 🗖 Liste du da	ssier/lecture de da	onnées			
🛛 🗖 Attributs de	lecture				
🛛 🗖 Lecture de	s attributs étendus				
🛛 🗖 Création dr	e fichier/écriture de	e données			

Pour obtenir par exemple

Pour le groupe utilisateur

Autorisations Audit	Propriétaire /	Autorisations effectives		
La liste suivante affi en se basant sur les Nom de groupe ou u	che les autorisatio autorisations app t'utilisateur :	ons qui vont être accord propriées.	ées au groupe ou à l'utili	sateur sélectionné
Utilisateurs	dansaccur .			Sélectionner.
Contrôle total Contrôle total Arrow Parcours du do Liste du dossie	ossier/exécuter le r/lecture de donn	fichier		
Attributs de lec	ture ributs étendus			
Création de fic Création de do	nier/ecriture de di ssier/ajout de dor ure	onnees nnées		
 Écriture d'attrib Suppression de 	uts étendus e sous-dossier et l	iichier		
Suppression Autorisations d Modification de	e lecture es autorisations			

Qui avait ces droits de donnés :





Autorisations pour Utilisateurs	Autoriser
Contrôle total	
Modification	\checkmark
Lecture et exécution	\checkmark
Affichage du contenu du dossier	\checkmark
Lecture	\checkmark
Écriture	\checkmark
Autorisations spéciales	V

Le calcul ne tient pas compte des identificateurs de sécurité suivants :

- Ouverture de session anonyme
- Utilisateurs authentifiés
- Créateur propriétaire.

Dans Windows XP Professionnel, le groupe Tout le monde ne contient plus le groupe Ouverture de session anonyme.

Utilitaire Accesschk

Microsoft Tech	let Rechercher sur Microsoft France :
Accueil TechNet	TechCenters Téléchargements Programme TechNet Abonnement TechNet Mon TechNet Bulletins de sécurité
Exchange Server ISA Server	AccessChk v3.0
Operations Manager (MOM)	Paru le 27 février 2007
Small Business Server (SBS)	Introduction
SQL Server Systems Management Server (SMS)	Pour s'assurer qu'ils ont créé un environnement sécurisé, les administrateurs Windows ont souvent besoin de connaître le genre d'accès aux ressources (notamment aux fichiers, répertoires, clés de registre et services Windows) dont disposent des utilisateurs ou groupes spécifiques. AccessChk répond rapidement à ces questions avec une interface et une présentation des résultats intuitives.
Windows Server 2003 Windows XP Professionnel	↑ <u>Haut de page</u>
Windows Vista Autres Produits	Installation AccessChk est un programme de console. Copiez AccessChk sur votre chemin exécutable. La saisie de « accesschk » affiche sa syntaxe d'utilisation.
Déploiement des postes de travail	AccessChk fonctionne sous Windows Vista, Win2K, Windows XP et Server 2003 y compris les versions x64 de Windows.

L'utilitaire téléchargé est petit

🛚 🗀 test					
;	×	Nom 🔺	Taille	Туре	Date de modification
🗁 test	~	tst-ntfs.exe	218 Ko	Application	01/09/2007 08:16

On peut renommer le fichier, et intégrer sont chemin dans le système

dans les propriétés système/onglet avancées

variable	Valeur	
TEMP	C:\Documents and Settings\Administrat	
TMP	C:\Documents and Settings\Administrat	
ariables système	Nouveau Modifier Supprimer	
Variable	Valeur 🔼	
NUMBER_OF_P	1	
OS	Windows_NT	
Path	C:\WINDOWS\system32;C:\WINDOWS;	Modimer la variable système
	.COM:.EXE:.BAT:.CMD:.VBS:.VBE:.JS:	
PATHEXT		
PROCESSOR_A	×86	Nom de la variable : Path





Windows XP & Système NTFShttp://www.cabare.net- SYS 20 - SYS 22 - Cours TP - ver 1.2 -- Michel Cabaré -

Page 26

Si la syntaxe complète est lourde, la base est simple

Ici dans l'exemple l'utilitaire à été renommer en tst-ntfs.exe, et donc ici en

tst-ntfs xxxnomutilisateurxxx xxxchemin-dossier-fichierxxxx

C:\test>tst-ntfs toto c:*.*
AccessChk v4.02 - Check access of files, keys, objects, processes or services Copyright (C> 2006-2007 Mark Russinovich Sysinternals - www.sysinternals.com
RW c:\\$oem\$ R c:\AUTOEXEC.BAT c:\boot.ini R c:\Bootfont.bin R c:\CoNFIG.SYS RW c:\data RW c:\deuxieme site R c:\Documents and Settings RW c:\driuens2k
RW c:\Uriversxp R c:\I0.SYS R c:\MSDOS.SYS c:\MSOCache RW c:\Nouveau dossier c:\NTDETECT.COM

Les options intéressantes (et cumulables) :

- n

pas d'accès

- r

accès en lecture

-w

accès en ecriture

-d

uniquement les dossiers



TP DROITS NTFS 1°

Objectif:

🔄 dat	a
	andre bertran

, Faire que chaque utilisateur , andre, bertrand...puisse "tout and faire chez lui", sauf détruire son répertorie de base(ici homonyme)!

Le disque sur lequel on travaille à des permissions NTFS par défaut,

Permissions de partage :

On pourrait commencer par **partager** le dossier **data** (en contrôle total pour tout le monde)

andre	
Propriétés de data 🛛 ? 🗙	
Général Partage Sécurité Personnaliser	
Vous pouvez partager ce dossier avec d'autres utilisateurs du réseau. Pour activer le partage de ce dossier, cliquez sur Partager ce dossier.	Autorisations pour data Autorisations du partage
◯ Ne pas partager ce dossier	Noms d'utilisateur ou de groupe :
O Partager ce dossier	🕫 Tout le monde
Nom du partage : data 💌	
Commentaire :	*
Nombre limite 💿 Maximum autorisé	
d'utilisateurs : 🕜 Nombre d'utilisateurs autorisés : 🛛 🌲	Ajouter Supprimer
Pour définir les autorisations d'accès à ce dossier sur le réseau, cliquez sur Autorisations.	Autorisations pour Tout le monde Autoriser Refuser
	Contrôle total
	Modifier

Ainsi les accès depuis le réseau sont possible. (cela n'est pas obligatoire !)

Permissions de sécurité :

On va donc retirer l'héritage, (en demandant **de supprimer les permissions**) Ensuite on pose

- le groupe tout le monde en Lecture et éxecution Afficher le contenu Lecture (c'est le mode par défaut lorsque l'on ajoute une permission)
- le compte Administrateur en Contôle total





on a donc

🚮 Administrateurs (TEST\Administrat	eurs)	
Autorisations :	Autoriser	Refuser
Contrôle total Modifier Lecture et exécution Afficher le contenu du dossier Lecture Écriture	<u> </u>	

et

	🖋 Tout le monde			
4	Autorisations :	Autoriser	Refuser	
I	Contrôle total			
I	Modifier			
I	Lecture et exécution	\checkmark		
I	Afficher le contenu du dossier	\checkmark		
I	Lecture	\checkmark		
I	Écriture			

sur le dossier de andre, et bertrand donc, par défaut les permissions de sécurités sont celles heritées du dossier data et on aura donc

Administrateurs (TEST\Adminis	trateurs)	🚮 Tout le monde		
Autorisations :	Autoriser	Autorisations :	Autoriser Refu	user
Contrôle total	\checkmark	Contrôle total]
Modifier	\checkmark	Modifier		3
Lecture et exécution	\checkmark	Lecture et exécution	V]
Afficher le contenu du dossier	V	Afficher le contenu du dossi	er 🗹 🗌]
Lecture	V	Lecture	\checkmark]
Écriture	×	Écriture		

à l'heure actuelle les dossiers andre et bertrand sont en lecture seule pour tout le monde... Il faut maintenant autoriser andré a pouvoir aller que chez lui, et exclure tout le monde (et idem pour bertrand...)

donc pour le dossier **andre**, après avoir refusé l'héritage il faut avoir au final

l'utilisateur **andré** en (Lecture et exécution - Afficher le contenu - Lecture) plus Ecriture

L'administrateur en contrôle total

N.B: bien faire attention aux permissions effectives, qui peuvent varier selon ce que sous 2000 NT4 ou XP on copie ou supprime les permissions lors de la rupture de l'heritage !

Noms d'utilisateur o 2 Administrateur 2 andre (TRAVA	u de groupe : (TRAVAIL\Ad IL\andre)	ministrateur)		
2 Administrateur 2 andre (TRAVA	(TRAVAILVAd IL\andre)	ministrateur)		
🙎 andre (TRAVA	IL\andre)			
		Ajouter	Su	upprimer
Autorisations pour a	ndre	Ajouter Autoriser	Su Su	upprimer efuser
Autorisations pour a Contrôle total	ndre	Ajouter Autoriser	Su Su Bar Re	upprimer efuser
Autorisations pour a Contrôle total Modification	ndre	Ajouter Autoriser	Su er Re	upprimer efuser
Autorisations pour a Contrôle total Modification Lecture et exécu	ndre	Ajouter Autoriser	Su er Re	upprimer efuser
Autorisations pour a Contrôle total Modification Lecture et exécu Affichage du cor	ndre tion tenu du dossie	Ajouter Autoriser	Su er Re	efuser
Autorisations pour a Contrôle total	ndre	Ajouter Autoriser	Su Su Re	upprimer efuser
Autorisations pour a Contrôle total Modification Lecture et exécu Affichage du cor	ndre tion tenu du dossie	Ajouter Autoriser	Su er Re	efuser



Windows XP & Système NTFS http://www.cabare.net - SYS 20 - SYS 22 - Cours TP - ver 1.2 - - Michel Cabaré -

Donc désormais ici andré peut travailler chez lui, et pas chez bertrand. Ça c'est bien

Mais si andré peut créer un dossier (ou un fichier chez lui), il ne peut pas supprimer ce dossier (fichiers), ni même le renommer un fichier de son propre dossier, voire modifier son contenu. Il ne peut que créer... cela c'est embêtant...

Pour l'instant c'est normal car il n'a pas les droits de suppression – modification

Notion de Créateur Propriétaire :

Si on donne le droit à andré de modifier chez lui, il pourra aussi supprimer son propre dossier.... Et cela aussi c'est embêtant...

— la notion de **Créateur propriétaire** devrait résoudre le ce problème

en effet lorsque andré crée un dossier ou un fichier, il en est le propriétaire, et si on donne au **groupe créateur** le droit de **modifier** leurs documents, alors le tour est joué (chacun à droit de vie ou de mort uniquement sur ce qu'il a personnellement crée !)

Prop	oriétés de an	dre	_		?
Gé	néral Partage	Sécurité	Person	naliser	
N	oms d'utilisateur	ou de grou	pe:		
	😰 Administrate	ur (TRAVAI	LVAdmir	nistrateur)	
	😰 andre (TRAV	/AIL\andre)		
	📝 GROUPE CI	REATEUR			
			Γ	Aiouter	Supprimer
A	utorisations pour	GROUPE		Aloator	Cooppinio
C	REATEUR			Autoriser	Refuser
\Box	Contrôle total				<u>^</u>
•	Contrôle total Modification				
▶	Contrôle total Modification Lecture et exéd	cution			
•	Contrôle total Modification Lecture et exéd Affichage du ce	cution ontenu du c	dossier		
-	Contrôle total Modification Lecture et exéc Affichage du co Lecture	cution ontenu du c	dossier		
•	Contrôle total Modification Lecture et exéc Affichage du ce Lecture Écriture	cution ontenu du c	dossier		
•	Contrôle total Modification Lecture et exér Affichage du co Lecture Écriture Autorisations st	cution ontenu du o péciales	dossier		

- N.B: Maintenant, si andré essaye de supprimer son propre dossier de base, ils ne peut pas car ils n'en est pas propriétaire (c'est l'administrateur qui l'a crée). il peut éventuellement le vider de tout le contenu dont il est le propriétaire...
- **N.B:** Maintenant, si l'administrateur pose un fichier dans le dossier de André ou Bertrand, celui-ci pourra le lire, mais pas le modifier ou le supprimer (mais il pourra faire un enregistrer sous...)



TP DROITS NTFS 2°

Objectif:

Soit un groupe d'utilisateurs répartis en 2 catégories, des **commerciaux**, et des **secrétaires**...

Chaque **commercial** peut avoir globalement accès a :

- son dossier, (de manière complète)
- aux dossiers des collègues (en lecture seule)
- au dossier commun des commerciaux (de manière complète)
- mais n'a pas accès aux dossier des secrétaires....

De manière analogue, les secrétaires peuvent avoir accès a :

- leur dossier, (de manière complète)
- aux dossiers des collègues (en lecture seule)
- au dossier commun des secrétaires (de manière complète)
- mais n'a pas accès aux dossier des commerciaux....

Groupes et comptes :

il faut créer un groupe global des secrétaires et y rentrer les utilisateurs appropriés (s1,s2...)., et un groupe global des commerciaux, et y rentrer les utilisateurs appropriés (c1, c2...).

	Image: Secretaire Image: Secretaire <t< th=""><th>Groupe de sécurité - Global Groupe de sécurité - Global Utilisateur Utilisateur Utilisateur Utilisateur Utilisateur</th><th></th></t<>	Groupe de sécurité - Global Groupe de sécurité - Global Utilisateur Utilisateur Utilisateur Utilisateur Utilisateur	
Propriétés de sec	retaires	Propriétés de commerciaux	<u>?</u> ×
Membres : Nom	Membre de Gere par Dossier Active Directory test.edu/Users test.edu/Users	Membres Membres Membres: Nom Dossier Active Directory C1 test.edu/Users C2 test.edu/Users C3 test.edu/Users	





Windows XP & Système NTFShttp://www.cabare.net- SYS 20 - SYS 22 - Cours TP - ver 1.2 -- Michel Cabaré -

Partages:

Puis il faut partager (accès réseau) le dossier commerciaux en contrôle total - tout le monde et partager (accès réseau) le dossier secrétaire en contrôle total - tout le monde,



N.B: on pourrait décider de ne faire qu'un seul partage

Permissions NTFS:

sur le dossier général des secrétaires secretaires ; il faut bloquer l'héritage, (en supprimant les permissions)	Propriétés de secretaires Général Partage Web Partage Sécurité Nom Administrateurs (TEST\Administrateurs) Secretaires (TEST\secretaires)	? ×
puis donner au Administrateur une permission contrôle total, et au groupe des secretaires une permission Lecture exécution - affichage - Lecture	Autorisations : Contrôle total Modifier Lecture et exécution Afficher le contenu du dossier Lecture Écriture Ávancé Permettre aux autorisations pouvant être héri d'être propagées à cet objet	Autoriser Refuser

(et respectivement le groupe des commerciaux dans le dossier commerciaux...)

maintenant, les commerciaux peuvent aller chez eux, les secrétaires chez elles, mais uniquement en lecture seule...

N.B: si on veut que les secrétaires puissent ajouter des choses chez elles à ce niveau de la structure, il faut ajouter la permissions écriture..., a ce stade, ce n'est pas forcement souhaitable

Pour l'instant tous les "droits pratiques", pour lire un document dans n'importe quel dossier..., mais pas pour le créer, et encore moins le modifier / supprimer !



Pur chaque dossier individuel, **S1 S2** etc il faut autoriser l'utilisateur **S1** à **créer** chez lui, (mais pas **modifier**, sinon il pourrait supprimer son propre dossier) et les **administrateurs** en **contrôle total**

Donc on supprime l'héritage , (en supprimant les droits)	Propriétés de Général Pa	e s1 artage Web Partage Sécurité		<u>?</u> ×	
puis on ajoute le groupe des Administrateurs en Contrôle total, le groupe secretaires en Lecture-Afficher-Lecture seulement et enfin l'utilisateur \$1 en	Nom Admin S s1 (s1 Secret Autorisation Contrôle Modifier Lecture Afficher Lecture	istrateurs (TEST\Administrateurs) @test.edu) aires (TEST\secretaires) • • • • • • • • • • • • • • • • • • •	Autorised U	Ajouter Supprimer	
lecture plus écriture	Avancé Avancé Permeti d'être p	é tre aux autorisations pouvant être hér ropagées à cet objet	L) itées du pare	nt	
Autorisations : Auto	riser Refuser				
Contrôle total Image: Contrôle total Modifier Image: Content of the content					
autoriser chaque secrétaire à p y écrire, ainsi que l'administrateu	ouvoir p r	POUR le dossier ropriétés de sglobal Général Partage Web Partage	sgloba Sécurité	I il faut	<u>?</u> ×
on supprime l'héritage		Nom Madministrateurs (TEST\Adm Secretaires (TEST\secretaires)	ninistrateurs) res)		Ajouter Supprimer
on ajoute le groupe Administrate Contrôle Total	eur en				
		Autorisations :		Autoriser	Refuser
et le groupe secretaires en lecture-Afficher-Lecture et écriture	aussi	Contrôle total Modifier Lecture et exécution Afficher le contenu du dossier Lecture Écriture			
		Permettre aux autorisations p d'être propagées à cet objet	iouvant être	héritées du parer	ıt



Windows XP & Système NTFShttp://www.cabare.net- SYS 20 - SYS 22 - Cours TP - ver 1.2 -- Michel Cabaré -

Créateur propriétaire :

Maintenant, les secrétaires peuvent aller chez elles, **\$1** peut créer chez elle, et dans **sglobal**, et ne peut que lire chez **\$2**. de même **\$2** peut créer chez elle et dans **sgloba**l, mais ne peut que lire chez **\$1**

mais ni **S1** ni **S2** ne peuvent renommer ou supprimer quelque chose qu'elle aurait crée !

ce qui s'arrange avec la notion de créateur propriétaire...

que l'on ajoute en	Propriétés de s1	? ×
modifier pour les dossier	Général Partage Web Partage Sécurité	
31, 32 et sgiobal	Nom Administrateurs (TEST\Administrateurs) CREATEUR PROPRIETAIRE St (s1@test.edu) Secretaires (TEST\secretaires)	Ajouter Supprimer
	Autorisations :	Autoriser Refuser
	Contrôle total Modifier Lecture et exécution Afficher le contenu du dossier Lecture Écriture	
	Avancé D'autres autorisations existent ma pas s'afficher ici. Cliquez sur Avar Permettre aux autorisations pouvant être héritées d'être propagées à cet objet	is ne peuvent ncé pour les voir. : du parent
	OK Anr	nuler Appliquer

N.B: dans un tel schéma, si l'administrateur pose un fichier dans le dossier d'une secrétaire, celle-ci pourra le lire, mais pas le modifier ou le supprimer (mais elle pourra faire un enregistrer sous...)

Même raisonnement lorsque une secrétaire crée ou dépose un document dans l'espace commun, ses copines peuvent s'en servir mais pas le modifier ou le supprimer...(mais elle pourront faire un enregistrer sous...)

N.B: Maintenant, si s1 essaye de supprimer son propre dossier, elle ne peut pas car elle n'en est pas propriétaire (c'est l'administrateur qui l'a crée) mais elle le videra de tout le contenu dont elle est le propriétaire...





TP APPROPRIATION DE FICHIER

Descriptif du problème :



Imaginons un ensemble de secrétaires ayant chacune un espace propre réservé nommé s1, s2 etc et disposant d'un espace commun à toutes nommé sglobal (pour secrétaire global)

les permissions du dossier sglobal sont les suivantes :

Administrateur en Contrôle total	Propriétés de sglobal Général Partage Web Partage Sécurité	<u>? ×</u>
Créateur propriétaire en contrôle total	Nom Administrateurs (TEST\Administrateurs) CREATEUR PROPRIETAIRE Secretaires (TEST\secretaires)	Ajouter Supprimer
Le groupe secrétaire en Lecture- Affichage-Lecture et écriture	Autorisations :	Autoriser Refuser
	Contrôle total Modifier Lecture et exécution Afficher le contenu du dossier Lecture Écriture Avancé	
	Permettre aux autorisations pouvant être hérite d'être propagées à cet objet	ées du parent
on peut donc arriver à ce que dans ce dossier, il y ait des documents de di	vers propriétaires	
Dossiers X data3 s1 s2 sglobal	Nouveau Docur	ment de s2.doc
ramètres du contrôle d'accès pour Nouveau Document de s1.rtf	Paramètres du contrôle d'accès pour Nouveau D	ocument de s2.doc
Autorisations Audit Propriétaire Propriétaire Propriétaire actuel de cet élément :	Autorisations Audit Propriétaire Propriétaire actuel de cet élément :	
\$1 (\$1@test.edu) Sélectionner un nouveau propriétaire : Nom Ø Administrateur (TEST\Administrateur) Ø Administrateurs (TEST\Administrateurs)	s2 (s2@test.edu) Sélectionner un nouveau propriétaire : Nom @ Administrateur (TEST\Administrateur) @ Administrateurs (TEST\Administrateurs)	



Param Auto

Windows XP & Système NTFS http://www.cabare.net - SYS 20 - SYS 22 - Cours TP - ver 1.2 - - Michel Cabaré -

s2 peut lire un document fait par s1, mais si s2 essaye de modifier le nom du document ou de le supprimer, alors il y a refus ce qui est normal car seul le "créateur propriétaire" à ces droits...

si **s2** insiste sur vouloir modifier un document appartenant à **s1**, en tentant de se l'approprier, il essuie un refus (seul l'administrateur peut toujours s'approprier un document), et il ne peut bien sur pas changer les permissions!

Paramètres du contrôle d'accès pour Nouveau Document de s1	? ×
Autorisations Propriétaire	
Propriétaire actuel de cet élément :	
s1 (s1@test.edu)	
Sélectionner un nouveau propriétaire :	
Nom	

Comment aider S2 à modifier le document créer par S1 ?

Raisonnement :

Pour que **s2** puisse s'approprier le document...(depuis un poste NT...) **s1** doit donner à **s2** la permission voulue, voire la permission de prendre possession de ce fichier...:

N.B: il ne peut le faire que s'il a un contrôle total sur ce fichier (la différence entre contrôle total et modifier c'est que modifier ne permet pas de changer les permissions, et donc d'ajouter ou d'enlever des droits à des utilisateurs...)

	Paramètres du contrôle d'accès pour Nouveau Document	de si ?X		
s1 modifie les	Autorisations Propriétaire			
permissions du fichiers	Liste des autorisations :			
pour leauel il souhaite		Autorisation		
laisser une prise de	Nation Administrateurs (TEST\Administrateurs)	Contrôle total		
	🕺 Autor s1 (s1@test.edu)	Contrôle total		
possession,	🛞 Autor secretaires (TEST\secretaires)	Lecture, écriture et exé		
dans permissions - securité - avancées -				
on demande Ajouter _	Ajouter Supprimer Afficher/Modifi	er		
Sélectionnez Util Regarder dans : Nom titi (titi@test.edu) & andré (andre@test.	tateur, Ordinateur ou Groupe du Dans le dossier test.edu/Users .edu) test.edu/Users	? X •		
💆 bertrand (bertrand	@test.edu) test.edu/Users			
👖 🔝 s1 (s1@test.edu)	test.edu/Users			
1 (s2@test.edu)	test.edu/Users			
	Text PUTO ISER			
Nom :]				
	OK	Annuler		



sélectionner s2 puis valider

NB: il faut ici cocher au minimum modifier et	Entrée d'autorisation pour Nouveau Document de s1 ? × Objet Nom : s2 (s2@test.edu) Modifier Appliquer à : Cet objet uniquement * Autorisations : Autoriser Refuser Autorisations : Autoriser Refuser Liste du dossier / Lecture de données • Liste du dossier / Lecture de données • Création de fichiers / Écriture de données • Création de dossiers / Ajout de données • Attributs d'écriture • Écriture d'attributs étendus • Suppression de sous-dossiers et de fichiers • Suppression de lecture • Modifier les autorisations • Appropriation •
appropriation,	Appliquer ces autorisations uniquement aux objets et/ou aux conteneurs faisant partie de ce conteneur
· ·	OK Annuler

Désormais s2 lors de sa session peut s'approprier ce document...

- 1	Paramètres du contrôle d'accès pour Nouveau Document de s1	? ×
	Autorisations Propriétaire	
	Propriétaire actuel de cet élément :	
▶	s1 (s1@test.edu)	
	Sélectionner un nouveau propriétaire :	
	Nom S2 (s2@test.edu)	

pour obtenir

	Paramètres du contrôle d'accès pour Nouveau Document de s1	<u>? ×</u>
	Autorisations Propriétaire	
	Propriétaire actuel de cet élément :	
▶	s2 (s2@test.edu)	
	Sélectionner un nouveau propriétaire :	
	Nom	
	🕵 s2 (s2@test.edu)	

en résumé :

- Si ici on donne au groupe Créateur propriétaire le droit contrôle total (ici c'est le cas), s2 pourrait modifier un document créé par s1 à condition que S1 ait au préalable modifié les permissions sur son fichier pour y inclure s2...
- Si ici on donne au groupe Créateur propriétaire le droit modifier, au lieu de contrôle total, alors <u>s2 ne pourra jamais modifier un document</u> <u>créé par s1</u>
- L'**administrateur** peut lui toujours s'approprier le fichier pour en faire ce qu'il veut...



TP COPIE FICHIER - PERMISSIONS

Objectif:

Lorsque l'on copie des fichiers, sur un volume NTFS, on sait que les permissions obtenues sur les fichiers "copiés" sont celles "héritées" des dossiers de destination...

Soit ainsi l'arborescence **data2** donnée suivante située sur le disque E: avec un certain nombre de permissions NTFS posées, et que l'on souhaiterais transférer pour des raison de maintenance sur un disque G:

Si on copie cette structure classiquement on obtiendra bien

Mais toutes les permissions NTFS ont été héritées du dossier de destination, à savoir newdata2, c'est à dire **Contrôle total** pour **tout le monde** !

Commerciaux Comm

ė- 📻 (Ē:)

🕀 😱 data

🖻 🔄 data2

commande xcopy :

Il existe une comande en ligne, nommée **xcopy.exe** permettant de copier les fichiers avec leurs permissions de sécurité. La mise en œuvre pourrait être

D: \>xcopy e:\data2 g:\newdata2 /o /a

N.B: si le nouveau disque G: doit remplacer l'ancien D:, on

- arrête le service server,
- on renomme les lecteurs,
- et on re-démarre le service server...
- Il ne reste plus que les partages à refaire !





Copie de partage ? :

La copie de partage elle aussi devient tentante, mais il faut savoir qu'elle est plus risquée, non supportée "officiellement", et remplace tous les partages d'une machine par ceux "récupérés" depuis la machine d'origine, on ne peut donc pas récupérer que les partages de telle ou telle lecteur ou branche d'arborescence !

Une fois l'arborescence copiée avec **xcopy**, on

- enregistre les partages à recopier, (sur la machine dont on veut copier les partages...) en lançant regedit32, Se placer sur la clé HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Shares Et sauvegarder sur disquette depuis le menu de l'éditeur de registre
- 2. copie ce fichier sur la machine de destination
- 3. sur la machine de destination, en lançant regedit32, Se placer sur la clé HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Shares Et restaurer depuis la disquette depuis le menu de l'éditeur de registre
- 4. répondre OK
- **NB:** tous les partages de la machine de destination sont remplacés par les partages existant sur la machine d'origine !
- NB: Dans la ces ou des autorisations de partages auraient été données, on peut essayer de les retrouver avec la clé du dessous **\Security**



