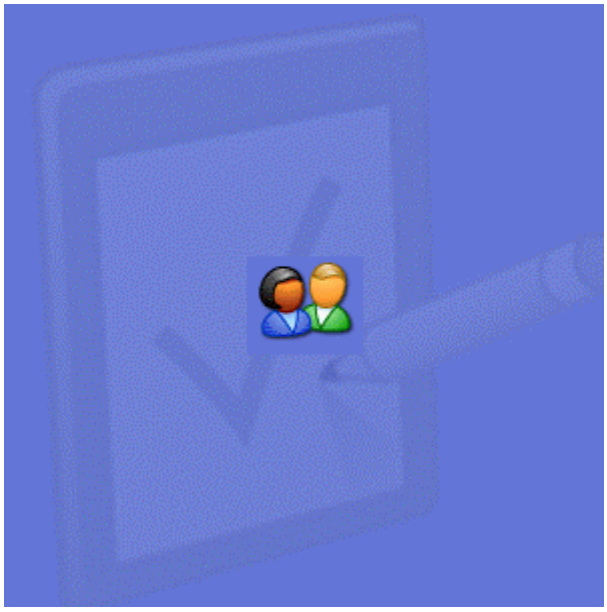
Sécurité informatique
et
Protection de la vie privée

Microsoft Windows



Travailler avec un compte « limité »

« Comment transformer un compte Administrateur en compte Limité »

© Pierre Pinard Février 2007
http://assiste.com- ASAP

Table des matières

1 Produits auxquels s'applique ce protocole....4
2 Avant propos....4
2.1 Navigation sur l'Internet, lecture des e-mails et droits « Administrateurs »....4
2.2 Administrateur auto-censuré avec DropMyRights....5
2.3 Utilisateur « limité » et « Exécuter en tant qu'administrateur »....5
2.3.1 Demandez de l' « Administrateur » tout en restant « Limité »....5
2.3.2 L'esprit du « Principe de moindre privilège » de Windows Vista....5
2.4 Notion de « compte d'utilisateur »....7
2.5 Emplacement des documents des utilisateurs....8
3 « Droits Administrateur » et « Droits limités » : Différences....10
3.1 Grandes différences entre droits « Administrateur » et « Limités »....10
3.2 Détail des droits....11
4 Passer à NTFS....13
4.1 Comment savoir quel est mon système de fichiers actuel ?....13
4.2 Comment convertir un système de fichiers FAT en système NTFS ?....13
5 Faire apparaître l'onglet « Sécurité »....14
5.1 Faire apparaître l'onglet « Sécurité » sous Windows XP Pro....14
5.1.1 Solution 1....14
5.1.2 Solution 2....14
5.2 Faire apparaître l'onglet « Sécurité » sous Windows XP Home (familiale)....14
5.2.1 Solution 1....14
5.2.1.1 Télécharger "Security Configuration Manager"....14
5.2.1.2 Décompresser "Security Configuration Manager"....15
5.2.1.3 Faire un point de restauration du système....15
5.2.1.4 Installez....15
5.2.2 Solution 2....15
6 Régler l'explorateur de Windows....16
6.1 Afficher les dossiers sous forme de listes détaillées....16
6.2 Faire apparaître le propriétaire d'un objet dans l'explorateur....17
6.3 Autres options d'affichage et généralisation des réglages....17
6.4 Propagation des réglages à tous les dossiers....17
7 Le protocole de passage d' « Administrateur » à « Limité »....18
7.1 Préambule....19
7.1.1 Chronologie du protocole :....19
7.1.2 La machine utilisée pour présenter ce protocole :....19
7.2 Créer un nouveau compte Administrateur....20
7.2.1 Appeler le panneau de configuration....20
7.2.2 Appeler le panneau de gestion des comptes d'utilisateurs....20
7.2.3 Lancer la création d'un nouveau compte....21
7.2.4 Donner un nom au nouveau compte....22
7.2.5 Attribuer des droits « Administrateur » au nouveau compte....22
7.2.6 Ouvrir la fiche du nouveau compte administrateur....23
7.2.7 Ouvrir l'option d'attribution d'un mot de passe....23
7.2.8 Attribuer un mot de passe au nouveau compte administrateur....25
7.3 S'identifier sous le nouveau compte administrateur....27
7.3.1 Re-démarrer sous le nouveau compte administrateur....27
7.4 Basculer l'ancien compte « administrateur » en compte « limité »....28
7.4.1 Appeler le panneau de configuration....28
7.4.2 Appeler le panneau de gestion des comptes d'utilisateurs....29
7.4.3 Ouvrir la fiche de l'ancien administrateur....29
7.4.4 Ouvrir la fonction de modification du type de compte....30
7.4.5 Protéger ce compte en le basculant en mode « Limité »....30
7.5 Attribuer au compte « Limité », le droit de contrôle total....31

7.5.1 Le propriétaire actuel....33
7.5.2 Accéder aux propriétés d'un objet....34
7.5.3 Accéder à la sécurité d'un objet....34
7.5.4 Ajouter le nom de l'utilisateur protégé à la liste des utilisateurs....35
7.5.5 Attribution du contrôle total de l'objet à l'utilisateur protégé....38
7.5.6 Retrait des droits sur cet objet aux autres utilisateurs....38
7.5.7 Propagation des droits à tous les objets du conteneur....40
7.6 S'identifier sous le nouveau compte « limité »....43
7.7 S'approprier les partitions, dossiers et fichiers personnels....43

8 Fin du protocole....46

9 Ressources complémentaires – Pour en savoir plus....47
9.1 Stratégies de groupe....47
9.2 La Microsoft Management Console "GPEDIT.MSC"....47
9.3 Les stratégies systèmes sous XP....47

1 Produits auxquels s'applique ce protocole

Les informations contenues dans cet article s'appliquent aux produits suivants:

- Microsoft Windows XP Édition familiale avec système de fichiers NTFS
- Microsoft Windows XP Professionnel avec système de fichiers NTFS

2 Avant propos

Nous allons apporter ici une solution, mais… une solution à quoi ? Quel est le problème ?

Lorsque votre machine est compromise par un parasite (virus[1], cheval de Troie[2], logiciel crapuleux etc. ...), elle l'est, la plupart du temps, à cause des privilèges « Administrateur » dont dispose la session en cours d'exécution.

La création de comptes d'utilisateurs, outre l'accès protégé et exclusif aux fichiers et données personnels que cela procure, sur un ordinateur partagé entre plusieurs, permet de limiter les droits de faire tout et n'importe quoi, dont des bourdes, même si vous êtes l'unique utilisateur de votre ordinateur. Cela limite considérablement, par la même occasion, le champ d'action des parasites[3] qui ne peuvent tout simplement plus s'installer.

2.1 Navigation sur l'Internet, lecture des e-mails et droits « Administrateurs ».

Internet est la source de la quasi-totalité des attaques et de l'insécurité[4]. Vous ne devez ni surfer sur le Web, ni consulter vos e-mails, ni accéder sous quelque forme que ce soit (messagerie instantanée[5] [6], P2P etc. ...) à l'Internet (ne pas vous connecter du tout) lorsque vous êtes en mode Administrateur. Cela est dangereux pour votre ordinateur et vos données. Le mode Administrateur donne des droits extrêmement étendus (prise de contrôle totale de l'ordinateur, matériels et logiciels) dont l'usage est très rarement requis.

Ces droits sont nécessaires pour des opérations d'administration de l'ordinateur (ajouter ou retirer un matériel ou un logiciel ou modifier ceux-ci), lors de l'installation de l'ordinateur. Par la suite ils ne le sont quasiment plus jamais sauf lors des mises à jour (Windows Update - Microsoft Update) et pour quelques rares opérations (installer un pare-feu ou un antivirus, par exemple).

Dans 99,9999% des cas vous n'avez pas besoin des droits « Administrateur »
Les parasites, auxquels nul n'échappe, en ont besoins, eux !
Ne les leur offrez pas !

Chaque application que vous lancez « bénéficie des droits » ou « est limitée aux droits » du compte qui lance cette application. Si vous êtes identifié (logué) en mode administrateur, les applications que vous lancez, et surtout celles qui se lancent sans votre consentement, simplement en visitant un site Internet piégé ou en ouvrant un message électronique, ont tous les droits.

Si un parasite se connecte avec vos droits « administrateur », il bénéficie, par votre faute, des droits les plus étendus pour prendre le contrôle total de votre machine et en faire un Zombie[7] ou voler vos données ou les compromettre.

Un « Administrateur » a le contrôle total de l'ordinateur
dont le pouvoir d'installer de nouveaux programmes

Un virus ou un cheval de Troie en mode « Administrateur »
prend le contrôle total de l'ordinateur et s'installe

Un virus ou un cheval de Troie en mode « limité » ne peut s'installer

1 Virus : http://assiste.com.free.fr/p/carnets_de_voyage/virus.html
2 Cheval de Troie (Trojan) : http://assiste.com.free.fr/p/carnets_de_voyage/trojans.html
3 Parasites : http://assiste.com.free.fr/p/abc/a/parasites.html
4 Attaques et insécurité sur le Net : http://assiste.com.free.fr/p/abc/abc_de_la_securite_sur_internet.html
5 Messageries instantanées et vers : http://assiste.com.free.fr/p/abc/a/messageries_instantanees_et_vers.html
6 Messageries instantanées et vie privée : http://assiste.com.free.fr/p/abc/a/messageries_instantanees_et_vie_privee.html
7 Zombie : http://assiste.com.free.fr/p/abc/a/zombies_et_botnets.html

Si vous avez ouvert une session en tant qu'administrateur d'un ordinateur local, un cheval de Troie peut

- reformater votre disque dur
- supprimer des fichiers
- créer un nouveau compte d'utilisateur bénéficiant d'un accès administratif.

Si vous avez ouvert une session en tant que membre du groupe Administrateurs de domaine, Administrateurs de l'entreprise ou Administrateurs du schéma dans Active Directory, un cheval de Troie pourrait:

- créer un nouveau compte d'utilisateur de domaine bénéficiant d'un accès administratif
- mettre les données schéma, configuration ou domaine en danger.

2.2 Administrateur auto-censuré avec DropMyRights

Que faire pour les irréductibles du contexte inutile et dangereux "Administrateur" ?

Nous vous avons proposé d'utiliser "DropMyRights" !
http://assiste.com.free.fr/p/logitheque/dropmyrights.html

Ceci n'est pas la panacée et n'en profitez pas pour restez en mode Administrateur ! Il est préférable d'utiliser les mécanismes mis en place nativement dans Windows.

2.3 Utilisateur « limité » et « Exécuter en tant qu'administrateur »

2.3.1 Demandez de l' « Administrateur » tout en restant « Limité »

Vous craignez, en tant que « simple utilisateur limité », ne pouvoir accéder rapidement à certaines fonctions d'administration. Vous pensez qu'il va falloir :

1. fermer votre session utilisateur
2. ouvrir votre session administrateur
3. exécuter la fonction souhaitée
4. fermer votre session administrateur
5. rouvrir une session utilisateur

C'est faux !

Vous vous êtes créé 2 comptes, pour vous-même : un compte administrateur et un compte limité

Sur un ordinateur local, il est recommandé d'ajouter votre compte d'utilisateur de domaine *uniquement* dans le groupe Utilisateurs (et non pas dans le groupe Administrateurs) pour effectuer des tâches de routine, y compris l'exécution de programmes et la visite de sites Internet. Lorsqu'il devient nécessaire d'effectuer des tâches administratives sur l'ordinateur local ou dans Active Directory, utilisez « Exécuter en tant que,,, » pour démarrer un programme en utilisant les informations d'identification administratives (vous exécutez un programme avec vos droits administratifs sans quitter votre session limitée).

« Exécuter en tant que,,, » vous permet d'accomplir des tâches administratives sans avoir à exposer votre ordinateur ou les données stockées dans Active Directory à des risques inutiles.

2.3.2 L'esprit du « Principe de moindre privilège » de Windows Vista

« Exécuter en tant que... » avec Windows XP représente, dans son esprit, les prémices de ce que Microsoft impose désormais avec Windows Vista : « Le principe de moindre privilège » :

Windows Vista n'est pas forcément une référence en matière de protection de la vie privée mais, en matière de sécurité, Microsoft a compris que les privilèges Administrateur sont inadmissibles.

La sécurité sous Windows Vista passe par le fonctionnement obligatoire des administrateurs en mode que nous appelons "limité" dans XP (le terme "limité" disparaît dans Vista dont la sécurité en matière d'utilisateurs s'appui sur le "principe de moindre privilège").

Puisque le déploiement de Vista semble extrêmement lent et que XP en a encore pour au moins jusqu'en 2015 (y compris Windows 2000), faites ce qu'il faut : ne travaillez pas en mode Administrateur !

Travailler constamment en mode "limité" et utiliser "Exécuter en tant que...", sous Windows XP permet de faire exactement ce qu'avance, à grand bruit, Microsoft, pour Windows Vista :

> **Windows Vista :**
>
> **Par défaut, les administrateurs exécutent la plupart des tâches avec un privilège d'utilisateur standard. Lorsqu'ils doivent effectuer une tâche administrative, ils doivent d'abord donner leur consentement dans la fenêtre qui s'affiche alors. Ils n'obtiendront des privilèges élevés que pendant la durée de vie de ce processus. Toutes les autres tâches continueront de s'exécuter en mode utilisateur standard.**

Pour plus d'informations, voir :

Utilisation de Exécuter en tant que...
http://www.microsoft.com/technet/prodtechnol/windowsserver2003/fr/library/ServerHelp/9368d1d4-d91b-4fb6-a29e-bc0be842d7a8.mspx?mfr=true

Pour plus d'informations sur l'utilisation de « Exécuter en tant que,,, », voir :

Exécuter un programme avec des informations d'identification administratives.
http://www.microsoft.com/technet/prodtechnol/windowsserver2003/fr/library/ServerHelp/9368d1d4-d91b-4fb6-a29e-bc0be842d7a8.mspx?mfr=true

Si vous devez exécuter des tâches d'administration telles que la mise à niveau du système d'exploitation ou la configuration des paramètres du système, déconnectez-vous et reconnectez-vous en tant qu'administrateur.

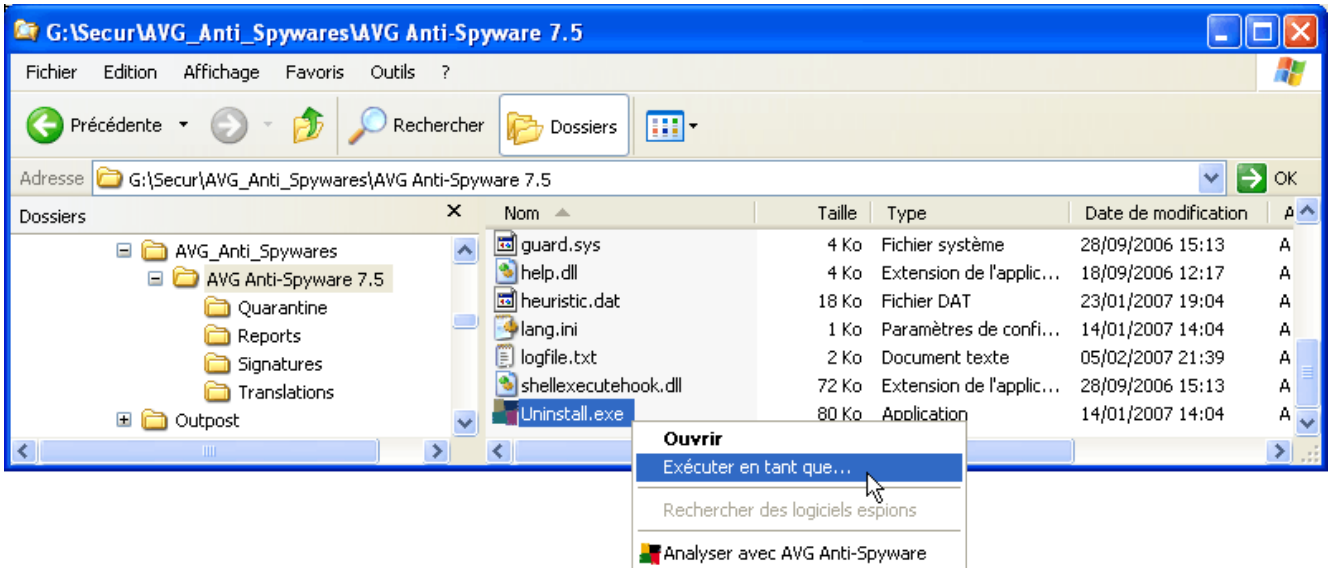


Illustration 1: Exécuter en tant que...

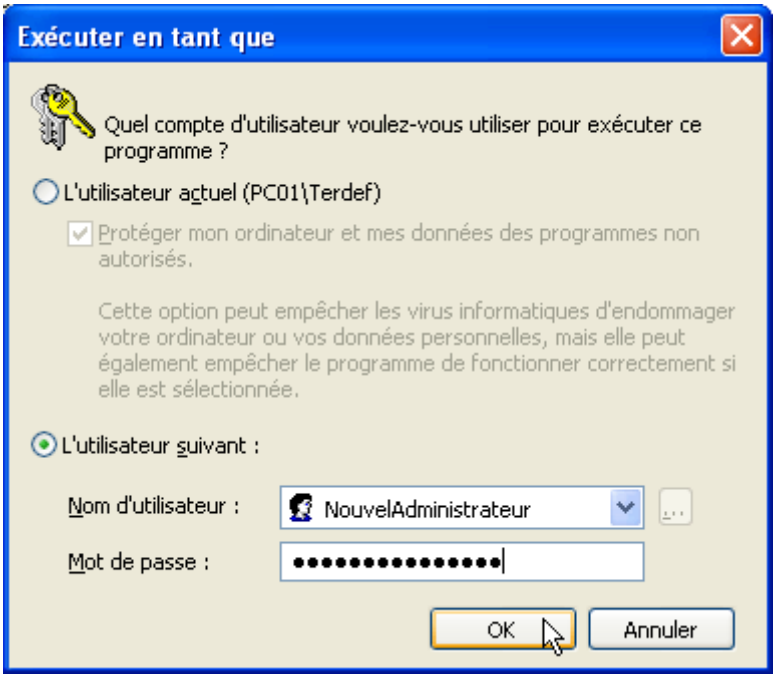


Illustration 2: Exécuter en tant que

2.4 Notion de « compte d'utilisateur »

Sous Windows, depuis Windows 95 (en 1995), la notion de « compte utilisateur » (de profil) est la solution apportée par Microsoft à l'utilisation du même ordinateur par plusieurs personnes.

- Chaque utilisateur a ses propres goûts et habitudes de travail, ce qui le conduit à faire des réglages personnels qui ne conviennent pas forcément aux autres.
- Chaque utilisateur a également des compétences en informatique plus ou moins élevées et des actions inconsidérées peuvent conduire à des états catastrophiques.

Il convient donc d'attribuer des droits plus ou moins étendus à l'un et à l'autre. Ces ensembles, goûts, habitudes, droits, sont regroupés et classés dans un profil (un compte) pour chaque utilisateur.

Ces ensembles de paramètres sont rangés dans une base de données : la **base de registre** et, plus exactement, dans la branche (« ruche ») HKCU (HKEY_CURRENT_USER) matérialisée par la présence des fichiers ntuser.dat (une « ruche » est une portion détachable de la base de registre). Lorsque qu'un utilisateur quitte (ferme) sa session et qu'un autre utilisateur ouvre une session (s'identifie – se « logue »), Windows ne fait que changer de contexte et passant d'un fichier ntuser.dat à un autre.

Vu du votre côté, un compte utilisateur sous Windows est matérialisé par un nom et un mot de passe qu'un utilisateur doit composer, pour s'identifier, avant de pouvoir travailler.

Un compte (un profil) appartient à un groupe de comptes (de profils) appelé « type ». Il y a le groupe des administrateurs (il peut y avoir plusieurs administrateurs) et le groupe des « utilisateurs limités ». Au sein de leur groupe, les utilisateurs ont des droits communs définis au niveau du groupe (et dont ils « héritent » et des paramètres plus personnels mémorisés au niveau des comptes (profils) individuels.L'attribution ou la restriction de droits, au niveau du groupe, s'applique à tous les profils (comptes individuels) de ce groupe. Elle permet de définir des paramètres s'appliquant à toute une catégorie d'utilisateurs. Les modifications apportées localement aux droits d'une personne en particulier (un compte individuel – un profil) ne s'appliquent qu'à elle.

Un compte (profil) permet, par exemple, d'isoler les fichiers de données d'un utilisateur et de les rendre inaccessibles (invisibles, non modifiables etc. …) aux autres. Un compte permet donc à un utilisateur :

- d'avoir un espace « propriétaire » sur une machine partagée avec d'autres (au bureau, à la maison…) – typiquement : le dossier « Mes Documents » avec ses fichiers, images etc. ….

- d'avoir ses propres comptes de messageries et son propre carnet d'adresse
- d'avoir ses propres « favoris »
- d'avoir ses propres mots de passe et login stockés dans son profil personnel (hors du profil général du groupe auquel il appartient) pour accéder à ses sites, forums, blogs, messageries instantanées etc. …
- d'avoir son propre bureau (apparence, thème, fond, économiseur, icônes et dossiers…)
- d'avoir ses propres paramétrages de comportement des logiciels utilisés, même si ceux-ci sont utilisés par tous (y compris ses propres listes des « derniers utilisés » (appelés MRUs – voir http://assiste.com.free.fr/p/abc/a/mru.html).

Mais, avant de modifier les profils des comptes, ce qui n'est pas à la portée du premier venu (qui connaît les « stratégies de groupes » sous Windows), contentons-nous de travailler en mode utilisateur et non pas en mode Administrateur.

Pourquoi ?

Parce qu'un parasite qui réussirait à pénétrer votre machine hériterait immédiatement des droits de l'utilisateur courrant et, si cet utilisateur courant à des droits « administrateur », c'est-à-dire les droits les plus élevés sous Windows, il pourra tout faire et défaire !

2.5 Emplacement des documents des utilisateurs

Par défaut, les documents de l'utilisateur actuellement identifié se trouvent dans « Mes documents ». Il s'agit d'un sous répertoire du répertoire de l'utilisateur dans le répertoire « Documents and Settings », sur le disque système. Si la présence de « Documents and Settings » se justifie sur le disque système (on y trouve tous les droits et les paramètres de chaque utilisateur), en revanche, les documents en eux-mêmes n'ont rien à faire sur le disque (dans la partition) système.

Prenons un exemple : sur une machine donnée il y a 3 comptes : Pierre, Paul, Jacques. En schématisant, nous allons avoir, sur la partition système (utilisez l'explorateur de Windows pour le voir) :

Lorsque Pierre est identifié (c'est lui qui démarre une session Windows)

C:\Documents and Settings
C:\Documents and Settings\All Users
C:\Documents and Settings\All Users\Documents partagés
C:\Documents and Settings\Pierre
C:\Documents and Settings\Pierre\Mes documents (Pierre est identifié (loggué))
C:\Documents and Settings\Paul
C:\Documents and Settings\Paul\Documents de Paul
C:\Documents and Settings\Jacques
C:\Documents and Settings\Paul\Documents de Jacques

Lorsque Paul est identifié (c'est lui qui démarre une session Windows)

C:\Documents and Settings
C:\Documents and Settings\All Users
C:\Documents and Settings\All Users\Documents partagés
C:\Documents and Settings\Pierre
C:\Documents and Settings\Pierre\Documents de Pierre
C:\Documents and Settings\Paul
C:\Documents and Settings\Paul\Mes documents (Paul est identifié (loggué))
C:\Documents and Settings\Jacques
C:\Documents and Settings\Paul\Documents de Jacques

Remarques :

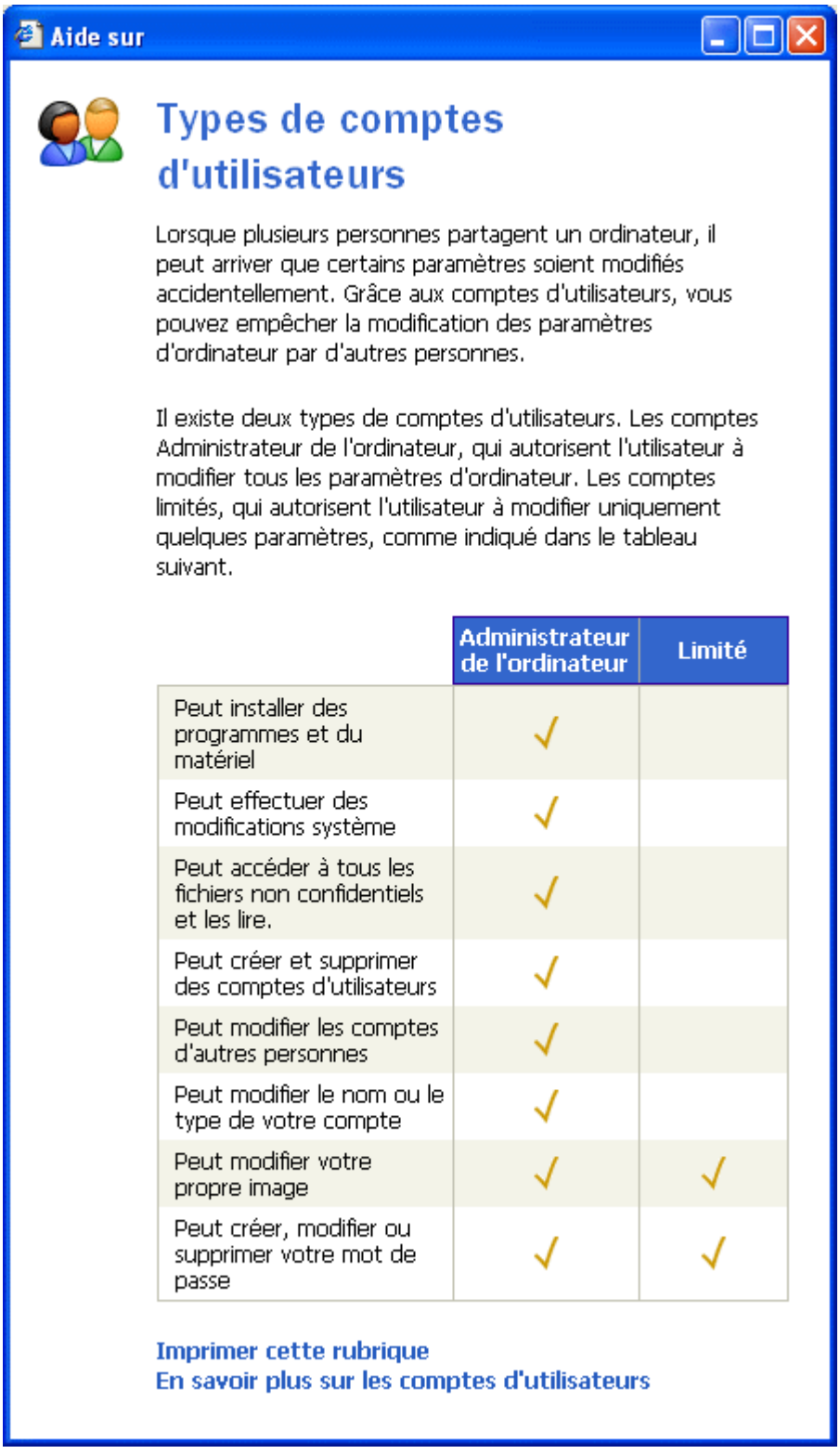
Le nom du répertoire de documents s'appelle « Mes documents » pour l'utilisateur actuellement identifié et « Documents de untel » pour les autres répertoires de documents des autres utilisateurs.

Les documents communs à tous les utilisateurs sont dans un sous-répertoire appelé « Documents » (qui apparaît sous le nom de « Documents partagés » dans l'explorateur de Windows) du répertoire commun, appelé « All Users » (tous les utilisateurs).

Il est recommandé de déplacer les répertoires « Documents » hors de la partition système ou de ne pas l'utiliser du tout et de stocker les documents dans des répertoires créés sur une ou des partitions distinctes de la partition système (voire même d'utiliser un disque dur physiquement distinct du disque système).

3 « Droits Administrateur » et « Droits limités » : Différences

3.1 Grandes différences entre droits « Administrateur » et « Limités ».



Aide sur

Types de comptes d'utilisateurs

Lorsque plusieurs personnes partagent un ordinateur, il peut arriver que certains paramètres soient modifiés accidentellement. Grâce aux comptes d'utilisateurs, vous pouvez empêcher la modification des paramètres d'ordinateur par d'autres personnes.

Il existe deux types de comptes d'utilisateurs. Les comptes Administrateur de l'ordinateur, qui autorisent l'utilisateur à modifier tous les paramètres d'ordinateur. Les comptes limités, qui autorisent l'utilisateur à modifier uniquement quelques paramètres, comme indiqué dans le tableau suivant.

	Administrateur de l'ordinateur	Limité
Peut installer des programmes et du matériel	√	
Peut effectuer des modifications système	√	
Peut accéder à tous les fichiers non confidentiels et les lire.	√	
Peut créer et supprimer des comptes d'utilisateurs	√	
Peut modifier les comptes d'autres personnes	√	
Peut modifier le nom ou le type de votre compte	√	
Peut modifier votre propre image	√	√
Peut créer, modifier ou supprimer votre mot de passe	√	√

Imprimer cette rubrique
En savoir plus sur les comptes d'utilisateurs

Sous Windows, il existe deux grands types de comptes utilisateurs :

- Les « Administrateurs » qui ont tous les droits
- Les « Limités » pour les utilisateurs normaux et pour l'usage normal de l'ordinateur.

Il existe également quelques types intermédiaires comme les :

- « Power User » (« Utilisateurs avec pouvoirs », intermédiaires entre « Administrateurs » et « Limités »)
- « Invités » (Droits plus restreints que les « Limités »)

Enfin, il est possible de créer des types de comptes et de totalement personnaliser les droits pour chaque type de comptes, voire pour chaque compte individuel, grâce aux « stratégies de groupe ».

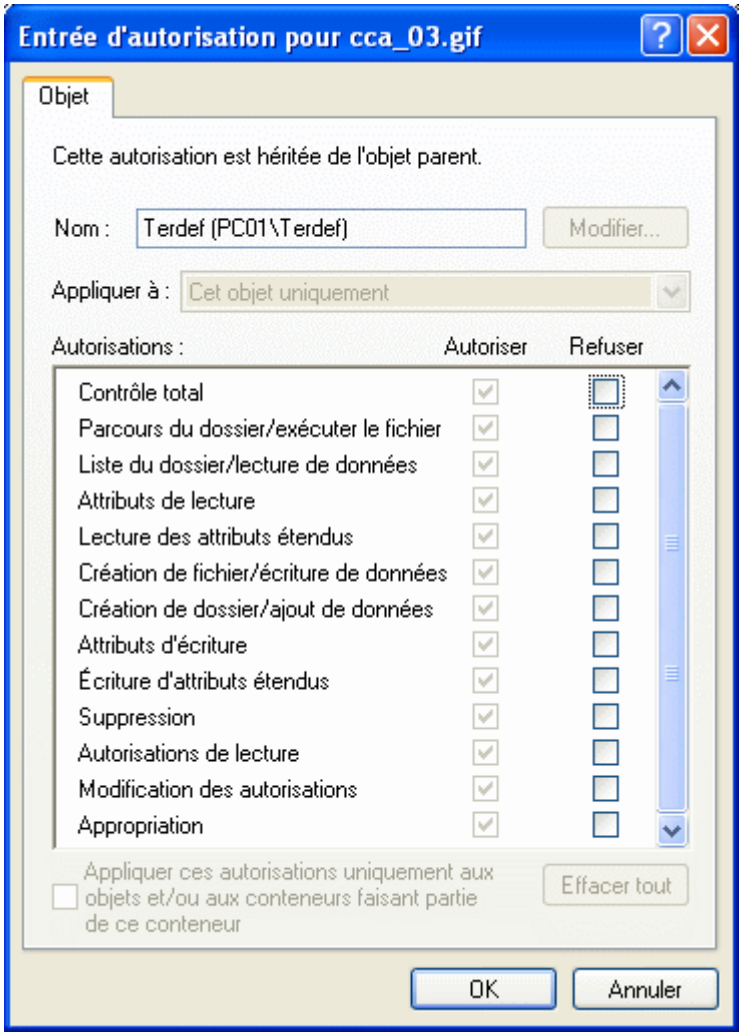
Par défaut, Windows vous fait travaillez en mode administrateur et donc n'importe qui ou n'importe quel virus a accès à tous vos fichiers et aux fichiers système.

La création de comptes à droits limités, aussi bien en environnement domestique qu'en environnement professionnel (en entreprise) permet de parfaitement distribuer les droits entre les uns et les autres (Papa, Maman, Enfant 1, Enfant 2, Visiteur, Ressources Humaines, Paye, Comptabilité, Direction, Recherches et Développements, Achat, Marketing, Force de vente, Utilisateurs nomades etc. …).

Dans tous les cas, il s'agit de mettre en place un véritable contrôle d'accès aux partitions (disques), répertoires (dossiers) et fichiers (de données ou programmes exécutables) afin de limiter leurs ouvertures et/ou modifications aux seuls ayant droit.

3.2 Détail des droits

Donné pour mémoire. En utilisation « domestique » il ne sera probablement pas nécessaire de descendre à un tel niveau de détail.


Entrée d'autorisation pour cca_03.gif
Objet
Cette autorisation est héritée de l'objet parent.
Nom : Terdef (PC01\Terdef)
Modifier...
Appliquer à : Cet objet uniquement
Autorisations :
Autoriser
Refuser
Contrôle total
Parcours du dossier/exécuter le fichier
Liste du dossier/lecture de données
Attributs de lecture
Lecture des attributs étendus
Création de fichier/écriture de données
Création de dossier/ajout de données
Attributs d'écriture
Écriture d'attributs étendus
Suppression
Autorisations de lecture
Modification des autorisations
Appropriation
Appliquer ces autorisations uniquement aux objets et/ou aux conteneurs faisant partie de ce conteneur
Effacer tout
OK
Annuler

4 Passer à NTFS

Si le système de fichiers n'est pas encore NTFS (« "New Technology File System »), le convertir.

NTFS est de beaucoup préférable au précédent système - FAT (FAT16 ou FAT32), que ce soit en termes de stabilité et fiabilité, qu'en termes de sécurité et de fonctionnalités. NTFS est obligatoire pour créer des comptes et donner des droits.

Les systèmes en dual boot avec Linux et Windows (XP, 2000 ou NT) ne sont pas gênés par NTFS que Linux sait manipuler nativement.

Pour plus d'informations voir : Jean-Claude Bellamy – Comparaison NTFS – FAT

http://www.bellamyjc.org/fr/theoriemultiboot2.html#FATvsNTFS

4.1 Comment savoir quel est mon système de fichiers actuel ?

Le système de fichiers est propre à chaque partition de votre système (une partition = une « lettre » comme (C:), (D:) etc. …). Les partitions peuvent avoir des systèmes de fichiers différents (par exemple (C:) en NTFS, (D:) en FAT32 etc. …)

Faire :

Démarrer > Tous les programmes > Accessoires > Explorateur de Windows > Déployer « Poste de travail » (clic sur le signe « + » devant « Poste de travail »).> Clic droit (clic avec le bouton droit de la souris) > Propriétés > Onglet « Général »

Là, vous pouvez lire quel est le système de fichiers du volume (de la partition).

4.2 Comment convertir un système de fichiers FAT en système NTFS ?

Ceci peut être fait à tout moment.

- L'intégralité des fichiers et répertoires est conservée.
- L'intégralité de la hiérarchisation des fichiers et répertoires est conservée.
- L'intégralité des données est conservée.
- L'intégrité des données est assurée – en cas de problème, la procédure comporte de nombreuses précautions et, si NTFS ne peut être installé, la procédure restaure le mode FAT.

Protocole :

- Fermez toutes vos applications car il sera impossible d'accéder aux données de la partition durant sa conversion.
  - Si des répertoires ou fichiers sont ouverts, la procédure vous prévient et vous devez accepter que le système (Windows) , « démonte » temporairement le volume (la partition)).
  - Si le volume (la partition) ne peut être démonté (cas de la « partition système » c:) la conversion sera lancée automatiquement au prochain redémarrage de l'ordinateur.
- Ouvrir une fenêtre en mode commande (dite « Fenêtre DOS » pour beaucoup).
  Démarrer > Tous les programmes > Accessoires > Invite de commande
- Saisir la commande suivante :
  Convert *volume* /FS:NTFS [/V]
  Volume étant C: ou D: etc. …

5 Faire apparaître l'onglet « Sécurité »

L'accès à l'onglet « Sécurité » sur les objets « Partitions », « Répertoires » et « Fichiers » sera indispensable. C'est à partir de là que sont gérés les droits avancés aux objets NTFS.

Cet onglet n'est pas toujours visible sous Windows XP Pro et n'existe qu'en mode « sans échec » sous Windows XP Home (Windows édition Familiale). La raison en est l'usage, par défaut, de la « stratégie de partage simple » car Microsoft n'imagine pas un ordinateur sous Windows XP tout seul : il est censé appartenir à un « WorkGroup » et y fonctionner en mode Client / Serveur, y compris au sein d'un foyer dans le cadre d'un réseau domestique.

5.1 Faire apparaître l'onglet « Sécurité » sous Windows XP Pro.

5.1.1 Solution 1

Démarrer > Tous les programmes > Accessoires > Explorateur de Windows > Outils > Options des dossiers > Onglet « Affichage » > Dans les Paramètres avancés, décocher la case "Utiliser le partage de fichiers simple" > Appliquer > Ok

5.1.2 Solution 2

Démarrer > Exécuter > Regedit > Localiser la clé
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa
Mettre la valeur de « forceguest » à 0

Cet article de Microsoft
Microsoft Security Advisory (906574) - Clarification of Simple File Sharing and ForceGuest
http://www.microsoft.com/technet/security/advisory/906574.mspx

5.2 Faire apparaître l'onglet « Sécurité » sous Windows XP Home (familiale).

Microsoft n'ayant pas prévu que les utilisateurs de NTFS sous Windows XP Home puissent bénéficier des avantages de NTFS, nous allons utiliser le « Security Configuration Manager » de Windows NT4 qui fonctionne parfaitement sous Windows NT5

Pour mémoire :

- Windows 2000Pro = Windows NT5
- Windows XP Home = Windows NT5.1
- Windows XP Professional = Windows NT5.1
- Windows Server 2003 = Windows NT5.2
- Windows Server 2003 x64 = Windows NT5.2
- Windows XP Professional x64 Edition = Windows NT5.2

Pour être tout a fait exact, l'onglet « Sécurité » apparaît tout de même sous Windows XP Home lorsque l'on démarre en mode « sans échec », ce qui n'est pas « pratique ».

5.2.1 Solution 1

En mode Administrateur

5.2.1.1 Télécharger "Security Configuration Manager"

Microsoft met le "Security Configuration Manager" (SCM) à notre disposition

En Ftp sur :
ftp://ftp.microsoft.com/bussys/winnt/winnt-public/tools/scm/scesp4i.exe

En Http sur :
http://download.microsoft.com/msdownload/sp4/x86/en/scesp4i.exe

Taille : 2,68 Mo (2 816 112 octets)
MD5 : f74c002dc04459b0a49fc52758f9dfd2
SHA1 : 867477f16eb2ec58d16f12884358f30b7c316a15

5.2.1.2 Décompresser "Security Configuration Manager"

Faire un double clic dessus pour le décompresser

5.2.1.3 Faire un point de restauration du système

Comment forcer la création d'un point de restauration - Windows XP Home

http://assiste.com.free.fr/p/comment/comment_activer_desactiver_les_points_de_restauration.html

Comment forcer la création d'un point de restauration - Windows XP Pro

http://assiste.com.free.fr/p/comment/comment_activer_desactiver_les_points_de_restauration.html

5.2.1.4 Installez

Faire un clic droit (clic avec le bouton droit de la souris) sur le fichier « setup.inf » obtenu lors de la décompression et choisir « Installer ».

Si une boîte de dialogue vous demande l'autorisation d'écraser le fichier « esent.dll », refusez en cliquant sur le bouton "Non pour tous".

Une fois l'installation terminée, redémarrez l'ordinateur. L'onglet « Sécurité » est désormais installé.

5.2.2 Solution 2

En mode administrateur

Dans un répertoire que vus créez pour l'accueillir, téléchargez l'utilitaire Zeb Protect

http://assiste.com.free.fr/p/logitheque/zeb_protect.html

Cet utilitaire ne nécessite pas de phase d'installation et est directement utilisable

Dans le même répertoire, téléchargez et décompressez le « HomePack »

ftp://zebulon.fr/HomePack.zip

Lancer Zeb Protect et demandez-lui d'installer l'onglet sécurité – Zeb Protect s'occupe de tout et vous vous occupez du reste.

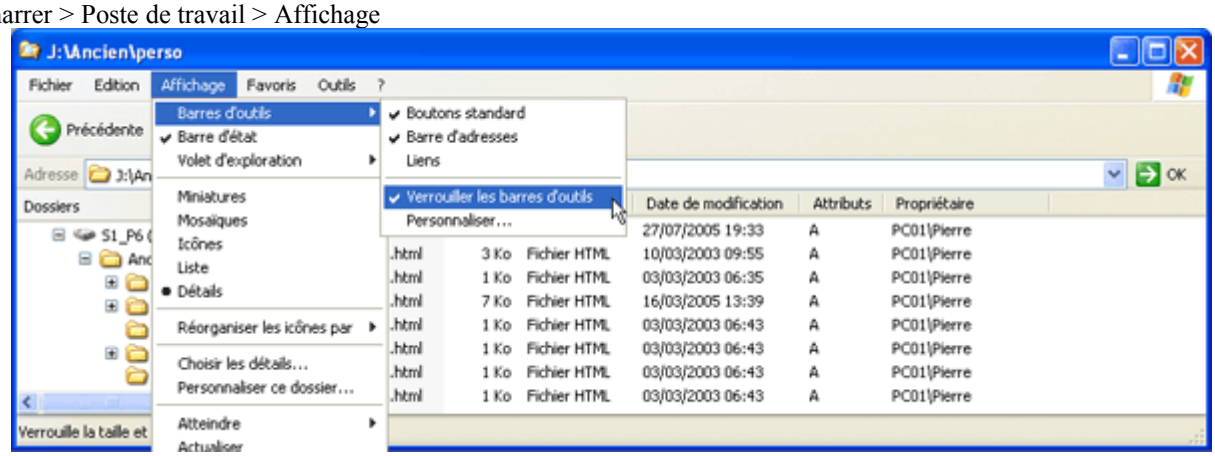
6 Régler l'explorateur de Windows

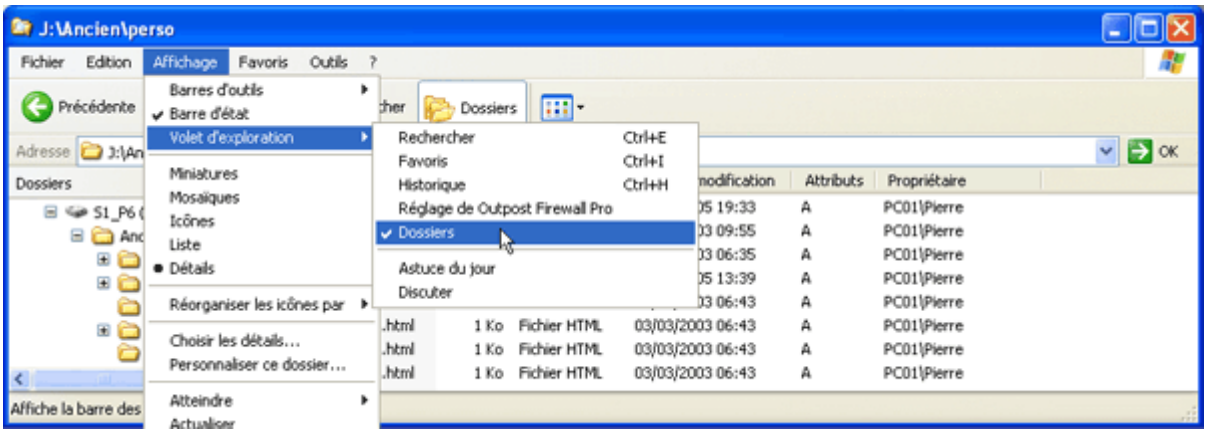
L'explorateur de Windows, pour être utile, doit être réglé comme suit : (ce réglage n'est pas spécifique au protocole de gestion des comptes d'utilisateurs et devrait être utilisé en toutes circonstances par tous).

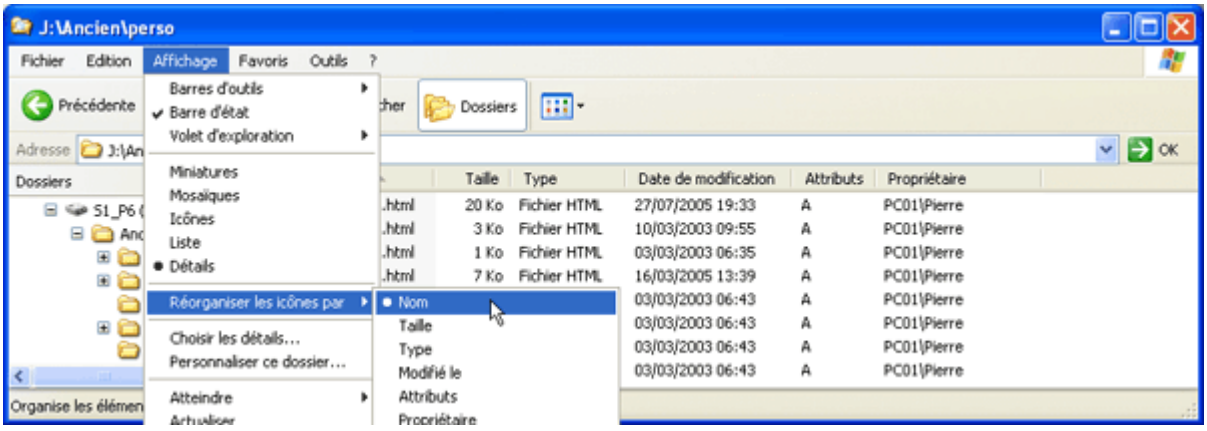
Ces réglages sont mémorisés pour le compte d'utilisateur en cours et ne s'appliquent pas aux autres utilisateurs de cet ordinateur. Chaque utilisateur identifié doit faire et mémoriser ses réglages.

6.1 Afficher les dossiers sous forme de listes détaillées

Démarrer > Poste de travail > Affichage



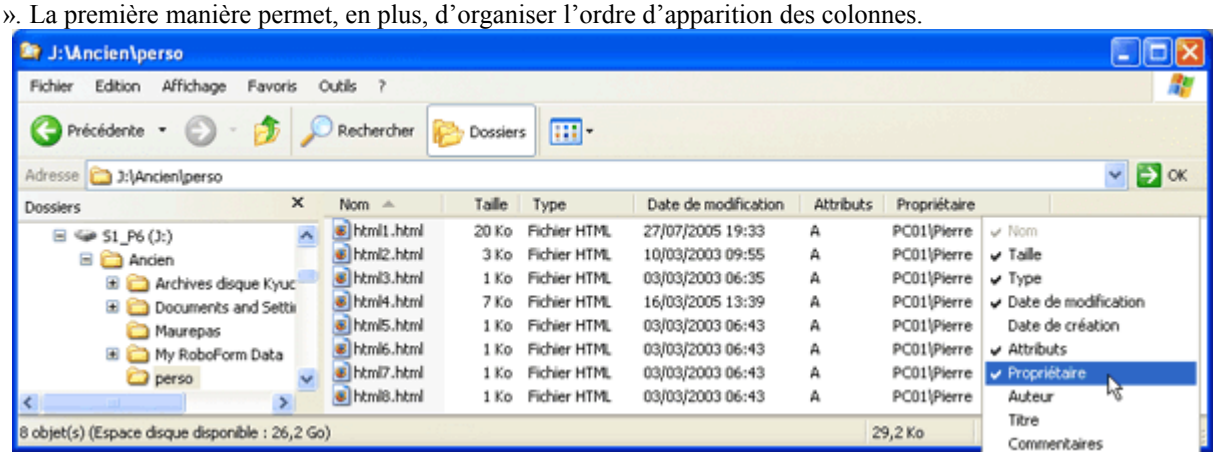




6.2 Faire apparaître le propriétaire d'un objet dans l'explorateur

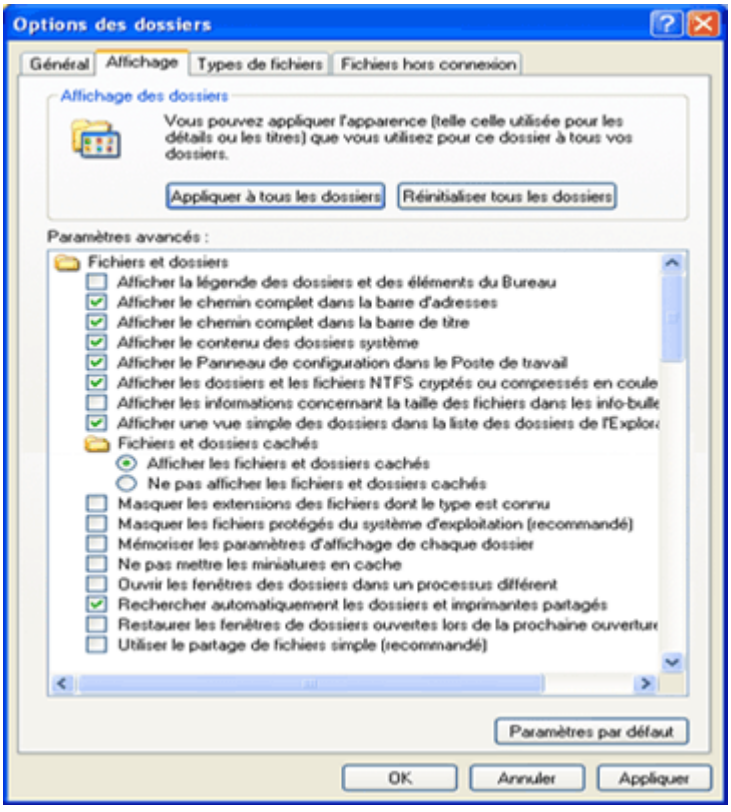
On accède à ces choix de 2 manières :

« Affichage > Choisir les détails » ou « Clic avec le bouton droit de la souris dans la zone de titres des colonnes de la liste ». La première manière permet, en plus, d'organiser l'ordre d'apparition des colonnes.



6.3 Autres options d'affichage et généralisation des réglages

Explorateur de Windows > Outils > Options des dossiers > Onglet « Affichage » > Régler comme l'exemple ci-dessous (en particulier, décocher la case « Utiliser le partage de fichiers simple (recommandé) ». Une fois les réglages faits, clic sur le bouton « Appliquer » en bas à droite



6.4 Propagation des réglages à tous les dossiers

En dernier lieu, clic sur le bouton « Appliquer à tous les dossiers » afin de généraliser ces réglages (de les propager à tous les dossiers) > Oui > Ok

7 Le protocole de passage d' « Administrateur » à « Limité »

Nous supposons que vous travaillez depuis des mois ou des années avec votre unique compte administrateur. Vos documents et vos paramètres (réglages, mots de passe, comptes e-mails etc. …) se trouvent dans le répertoire « Documents and Settings » où ailleurs selon votre méthode de travail.

Dans ce qui suit, nous allons vous guider pour que vous puissiez vous ouvrir un compte « utilisateur limité » conservant tout l'aquis des années antérieures de travail et un compte administrateur à utiliser avec parcimonie (voire jamais).

Notez bien ceci :

La procédure habituellement proposée, qui semble logique, consiste à conserver le compte administrateur actuel et à créer un compte « utilisateur limité » puis à tenter, durant des heures et des heures, de tout transférer sous ce nouveau compte, avec force sueurs froides et pertes de données.

Notre procédure est strictement inverse – nous allons créer un nouveau compte administrateur et simplement protéger le compte actuel, sans rien toucher ni déplacer, en le basculant d' « administrateur » à « limité ». C'est tout !

Si vous avez déjà tenté de créer un compte, vous vous êtes aperçu que ce n'est pas aussi évident que cela : votre compte utilisateur est plutôt aisé à créer mais dès que vous vous identifiez sous ce compte (login et mot de passe) le bureau est vide (pas de raccourcis d'accès aux applications) et vos données (vos fichiers que vous manipulez depuis des années) sont la propriété de l'administrateur : vous ne pouvez pas les modifier, les supprimer etc. … Alors vous avez peut-être fait un clic droit (clic avec le bouton droit de la souris) sur un fichier et vous avez tenté d'accéder aux propriétés du fichier. Vous avez vu son appartenance à quelqu'un d'autre (l'administrateur)… Vous avez même fouillé un peu et êtes peut-être tombé sur les « stratégies de groupes »… Alors là !… Vous n'avez rien compris (c'est normal !). Vous avez fermé la session « Utilisateur » et êtes retournez travailler en mode « Administrateur »…

Allons-y !...

7.1 Préambule

7.1.1 Chronologie du protocole :

- Créer un nouveau compte administrateur
- S'identifier sous le nouveau compte administrateur
- Basculer l'ancien compte « administrateur » en compte « limité » (bureau conservé etc. …)
- Attribuer au compte « Limité », le droit de contrôle total des partitions, répertoires et fichiers qui lui sont personnels (non système ni personnels à d'autres utilisateurs)
- S'identifier sous le nouveau compte « limité »
- S'approprier les partitions, dossiers et fichiers personnels

7.1.2 La machine utilisée pour présenter ce protocole :

- 1 utilisateur identifié sous « Terdef » fonctionne en droits « administrateur » depuis des années avec ses profils, ses comptes e-mails, ses mots de passe, ses documents un peu partout sur plusieurs disques (partitions), toute la sécurité installée etc. …
- « Terdef » va créer un nouveau compte administrateur : Appelons-le « NouvelAdministrateur »
- Ce nouvel administrateur va protéger « Terdef » en le mettant en « droits limités ». Terdef conserve donc son bureau, ses réglages, ses paramètres de connexion, ses mots de passe, ses boîtes e-mail, ses correspondances etc. ...
- Ce nouvel administrateur va donner à « Terdef » le contrôle total des fichiers, répertoires et partitions de Terdef (à l'exclusion de tout autre)
- « Terdef » va s'approprier ses fichiers, répertoires et partitions et va travailler immédiatement dans son environnement habituel (bureau inchangé etc. …)

7.2 Créer un nouveau compte Administrateur

Nous allons créer un second compte administrateur (il y en a toujours un existant, même si Windows démarre sans rien vous demander).

Nota : Si vous avez perdu le mot de passe de votre compte administrateur, rendez-vous sur
http://www.bellamyjc.org/fr/pwdnt.html

7.2.1 Appeler le panneau de configuration

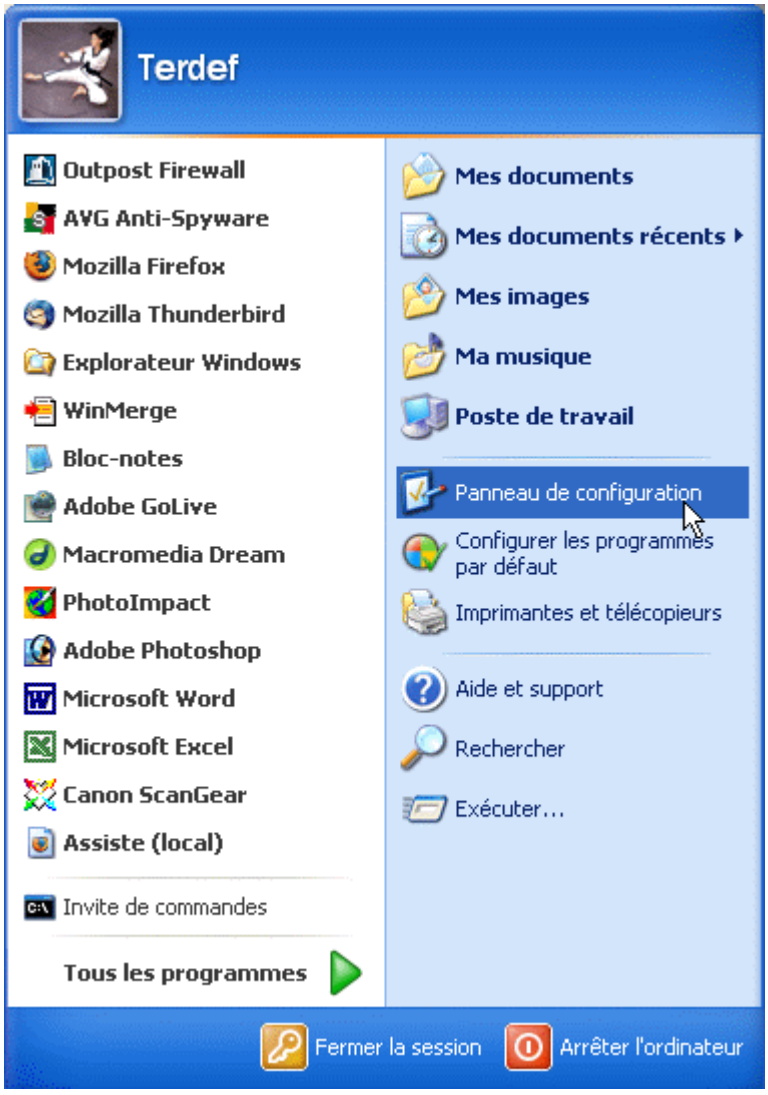


Figure 1 - Démarrer > Panneau de configuration

7.2.2 Appeler le panneau de gestion des comptes d'utilisateurs

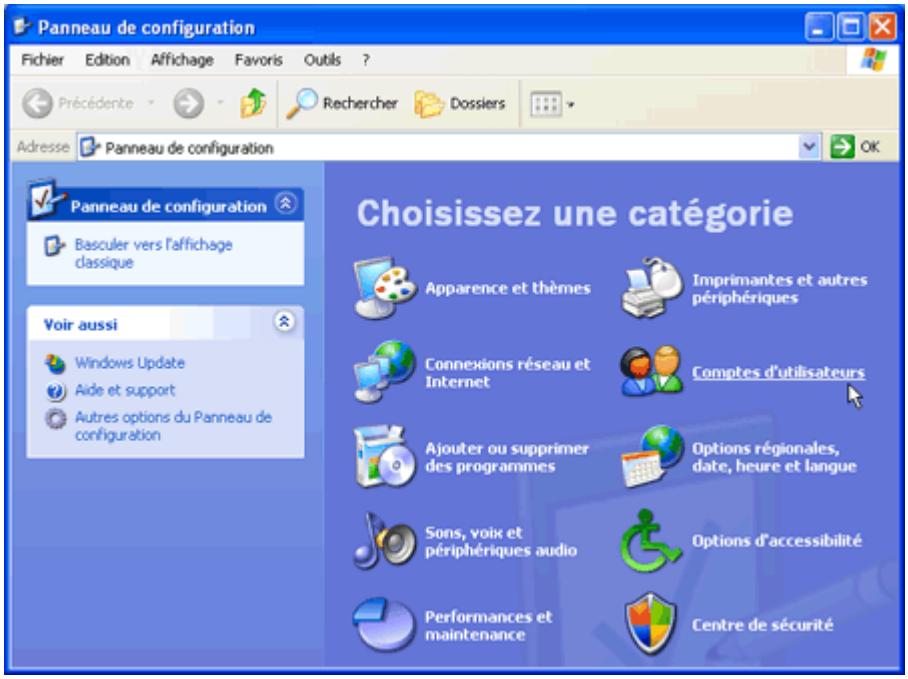


Figure 2 - Comptes d'utilisateurs

7.2.3 Lancer la création d'un nouveau compte

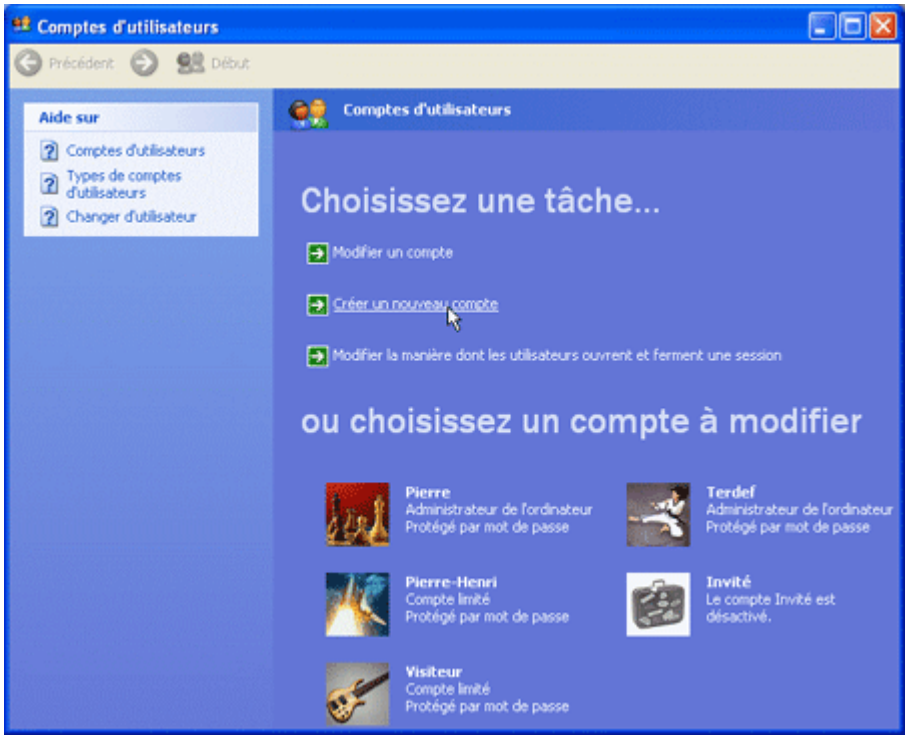


Figure 3 - Créer un nouveau compte

7.2.4 Donner un nom au nouveau compte

Figure 4 - Nommer le nouveau compte

7.2.5 Attribuer des droits « Administrateur » au nouveau compte.

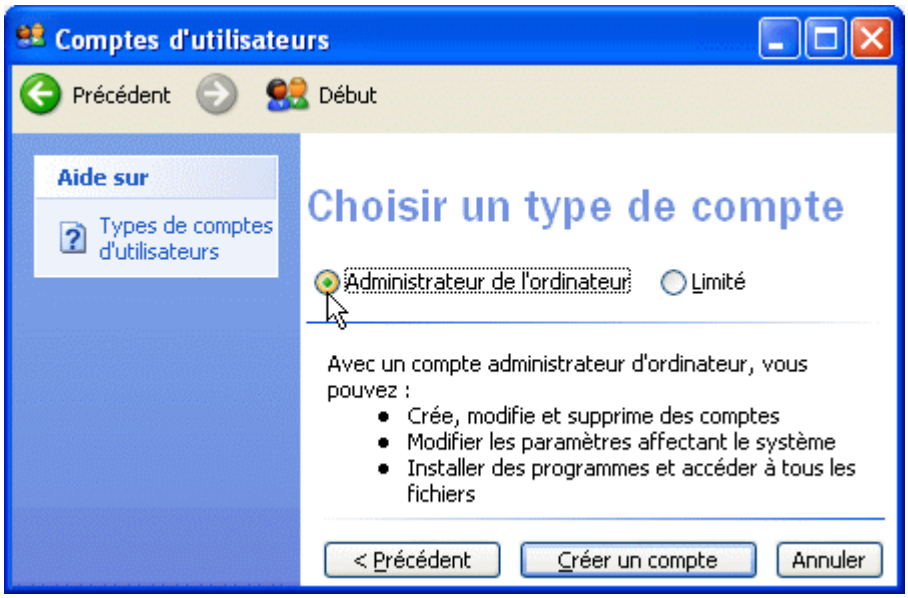


Figure 5 - Choisir le type "Administrateur" et « clic » sur « Créer un compte »

7.2.6 Ouvrir la fiche du nouveau compte administrateur

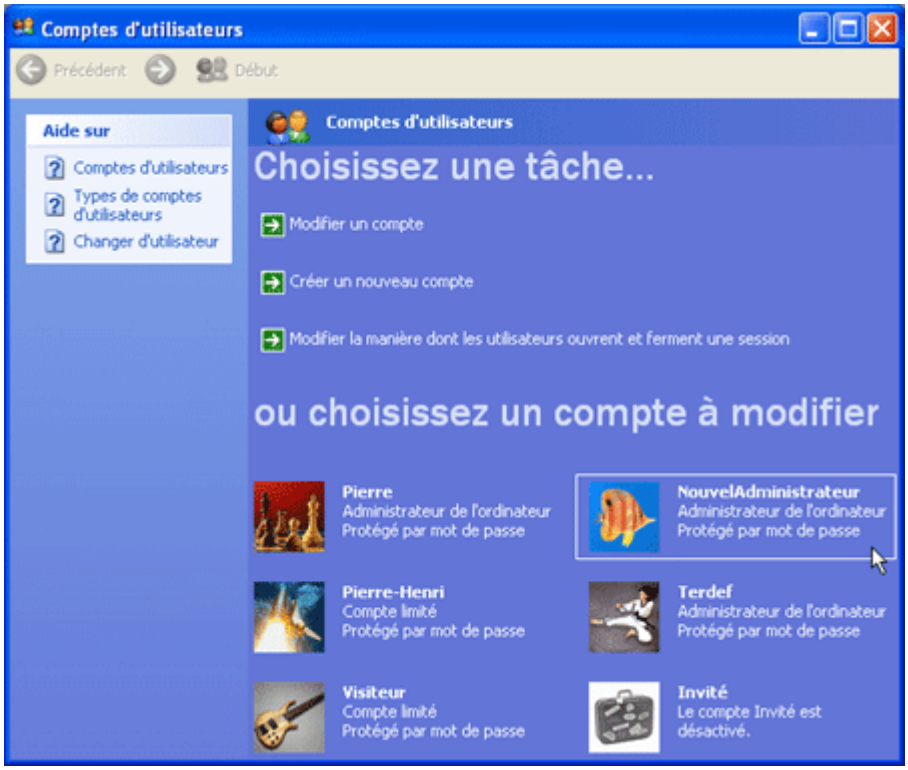


Figure 6 - Le nouveau compte administrateur est créé. Clic dessus…

7.2.7 Ouvrir l'option d'attribution d'un mot de passe

Figure 7 - Modifier le compte nouvellement créé pour lui attribuer un mot de passe

7.2.8 Attribuer un mot de passe au nouveau compte administrateur

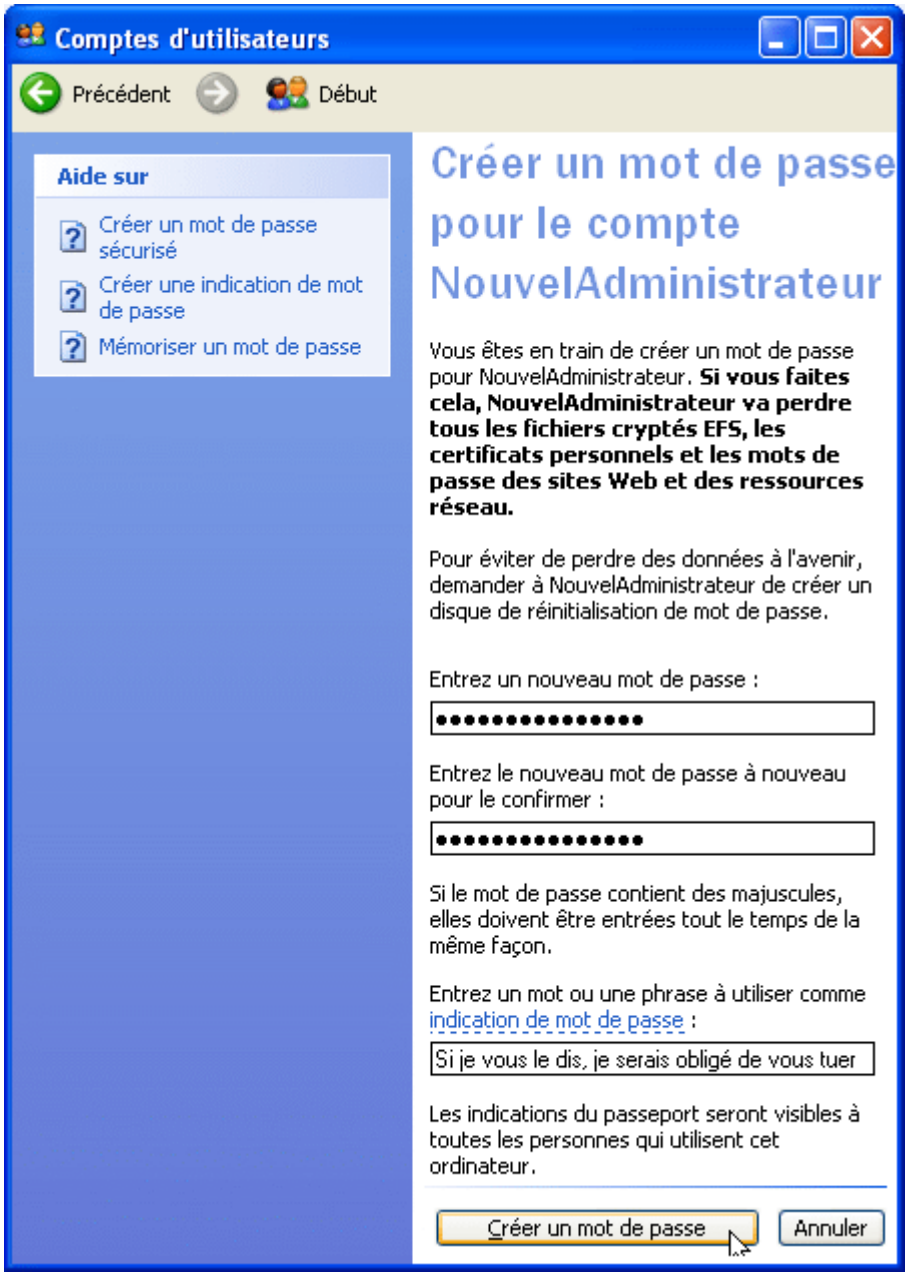


Figure 8 - Attribution d'un mot de passe

C'est fini. Vous venez de créer un compte administrateur protégé par un mot de passe. Arrêtez et redémarrez l'ordinateur puis identifiez-vous sous ce nouvel identifiant.

Nota ;
La mise en garde affichée ne retient pas notre attention car il s'agit d'un nouveau compte – il n'existe donc aucun antécédent (aucun fichier cryptés utilisant le système EFS (Encrypting File System) de Microsoft).

7.3 S'identifier sous le nouveau compte administrateur

Fermer la session ouverte précedemment et démarrer une nouvelle session en s'identifiant sous le nouveau compte administrateur.

7.3.1 Re-démarrer sous le nouveau compte administrateur

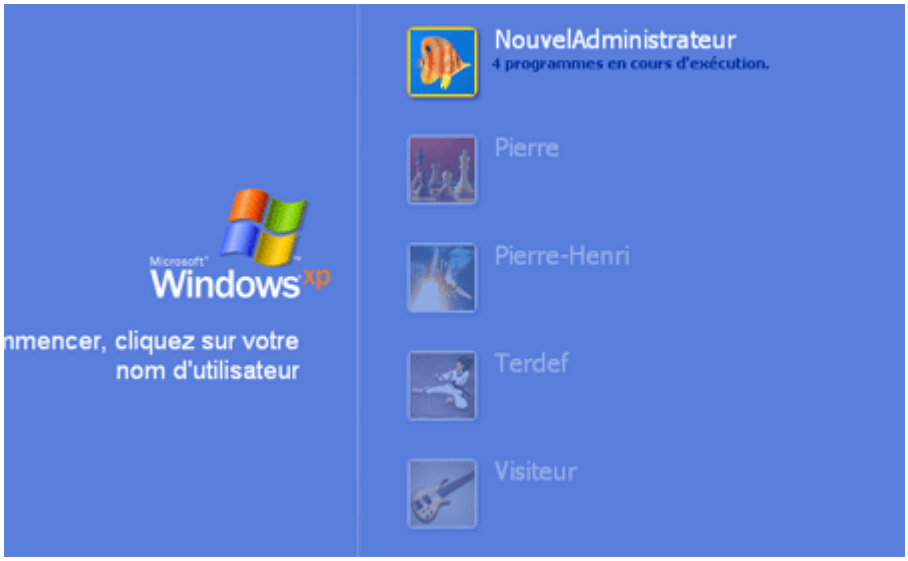


Figure 9 - Redémarrez en vous identifiant avec le nouveau compte administrateur

7.4 Basculer l'ancien compte « administrateur » en compte « limité »

7.4.1 Appeler le panneau de configuration

Le nouvel administrateur va protéger le compte (et donc le mode de travail) de l'ancien administrateur en le basculant en mode « Limité ».

Figure 10 - Démarrer > Panneau de configuration

7.4.2 Appeler le panneau de gestion des comptes d'utilisateurs

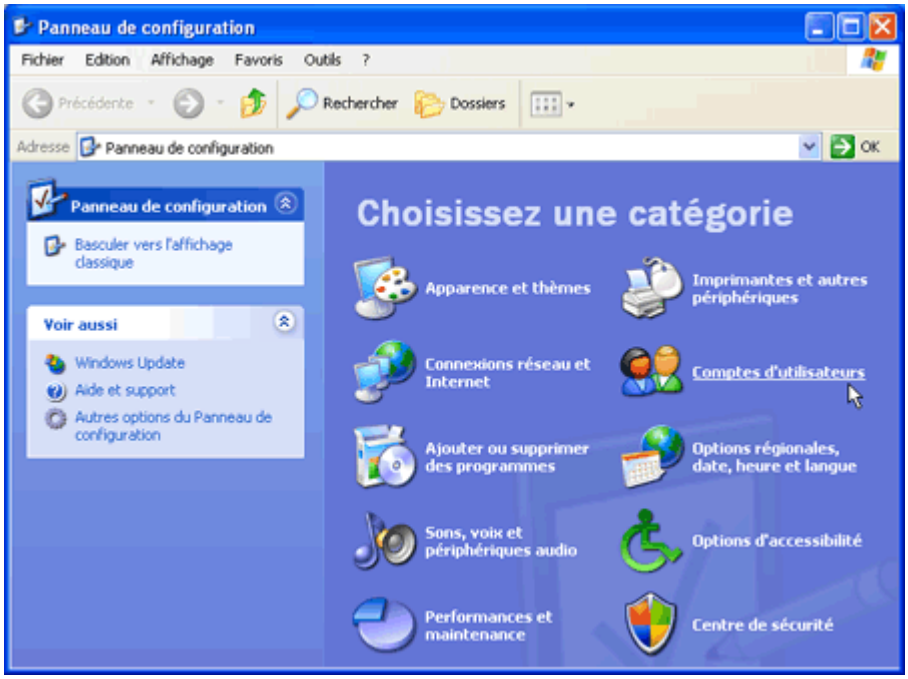


Figure 11 - Comptes d'utilisateurs

7.4.3 Ouvrir la fiche de l'ancien administrateur

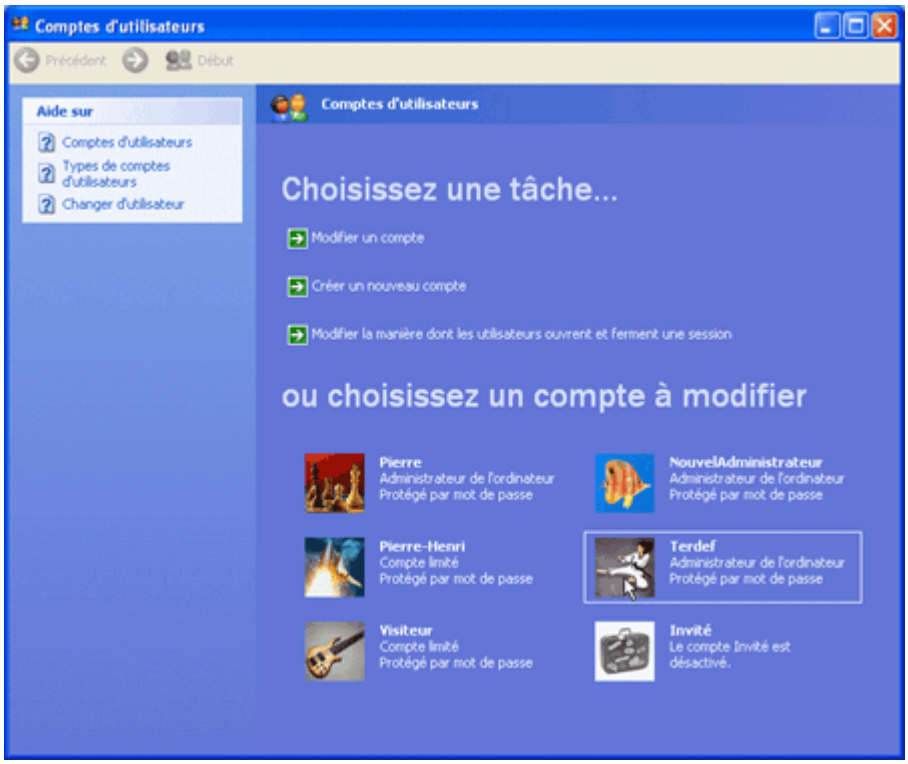
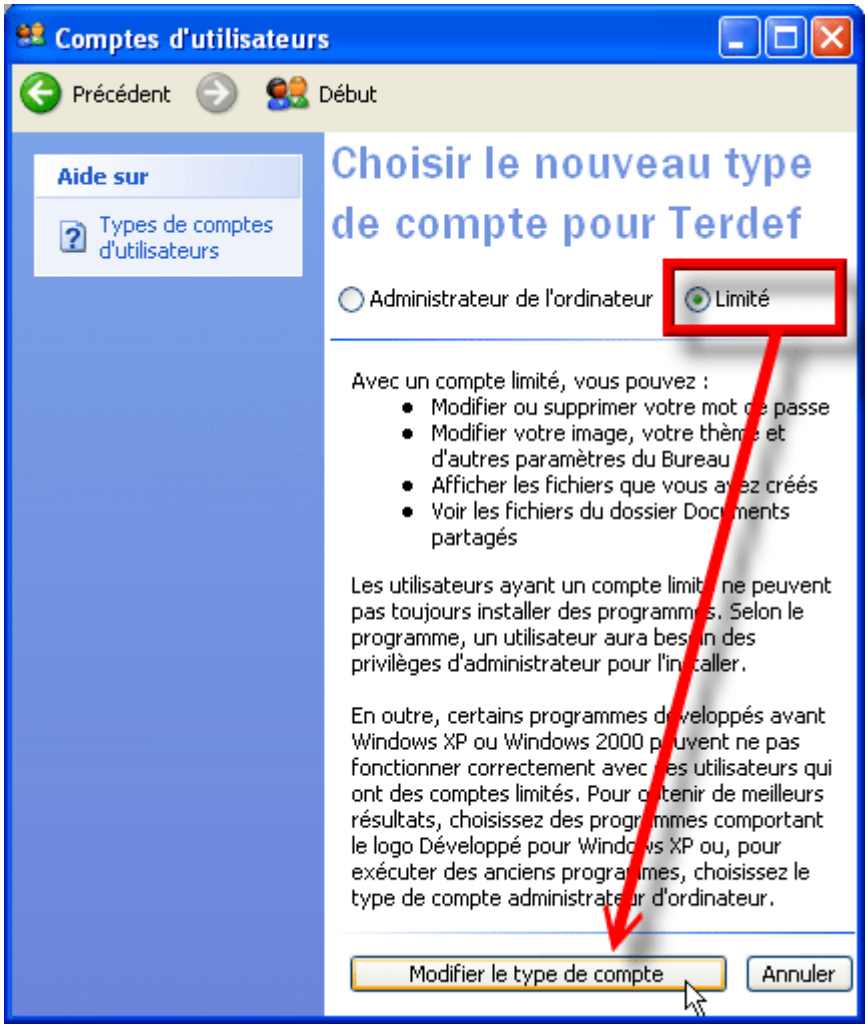


Figure 12 – Clic sur le compte de l'ancien administrateur

7.4.4 Ouvrir la fonction de modification du type de compte

Figure 13 Modifier le type de compte de l'ancien compte administrateur

7.4.5 Protéger ce compte en le basculant en mode « Limité »



7.5 Attribuer au compte « Limité », le droit de contrôle total

Le nouvel administrateur donne à l'utilisateur protégé le contrôle total des dossiers (répertoires) et fichiers auxquels il a le droit d'accéder en lecture et écriture (ceci afin de lui permettre de créer de nouveaux fichiers, d'en modifier d'anciens et d'en supprimer).

L'ordre dans lequel ceci est fait est important, d'un point de vue normatif (et paresseux), car les objets contenus dans un contenant peuvent hériter des droits du contenant (Les droits attribués à une partition peuvent ensuite être propagés automatiquement à tous les répertoires, sous-répertoires et fichiers de cette partition).

Nous commencerons donc par attribuer le contrôle total d'une partition à l'utilisateur protégé puis nous propagerons ces droits à tous les objets contenus. La manipulation est la même pour une partition ou pour un répertoire.

Objets système

Ne pas toucher aux droits de la partition système (C:\) ni à ceux des objets systèmes (« Documents and Settings », « Program Files » ; « Recycler » ; « System Volume Information » ; « Windows »).

Grouper vos documents

Il est impératif, même si ce n'est pas obligatoire, d'avoir tous les sous-conteneurs (sous-répertoires) et tous les fichiers d'un utilisateur dans un unique conteneur (une seule partition ou un seul répertoire). Si des fichiers traînent à droite et à gauche, les déplacer dans ce conteneur unique). La meilleure approche est de disposer d'une partition autre que la partition système (autre que la partition c:) et d'y créer un conteneur par utilisateur.

Vos documents dans Documents and Settings

Le répertoire « Mes documents » est le répertoire dans lequel sont rangés, par défaut, tous vos documents. Il est, par défaut, un des sous-conteneurs (sous-répertoires) de votre compte dans « Documents and Settings ». Les documents se trouvant dans le dossier « Documents and Settings », sous l'identité de chaque compte utilisateur, ont déjà les droits nécessaires. Si vous utilisiez votre ordinateur depuis des années : tout ce qui est sous votre profil dans « Documents and Settings » est conservé à sa place (incluant le « bureau », les mots de passe, les identifiants que vous pouvez avoir pour accéder à vos forums, messageries etc. … Seuls les droits de ce profil sont modifiés d'Administrateur à Utilisateur protégé (« limité ») afin d'empêcher toute attaque de bénéficier des droits administrateur (et toute fausse manipulation de votre part). Pour ces documents, vous n'avez rien d'autre à faire – la protocole s'arrête là. Toutefois, il est possible (et souhaitable – voir le point ci-dessus »Grouper vos documents ») de déplacer « Mes documents » et de le sortir de « Documents and Settings » et de la partition système c:.

Vos documents ailleurs

Vous avez probablement créé depuis longtemps des objets (partitions, répertoires, fichiers) ailleurs que dans « Documents and Settings ». Appliquez-leurs le protocole suivant. Il est hautement préférable que chaque utilisateur ait ses documents dans son espace de travail (son répertoire) et il n'est pas souhaitable d'utiliser « Mes documents », de Windows pour les y mettre car ce dernier se trouve sur le disque système, ce qui est une assez mauvaise idée.

7.5.1 Le propriétaire actuel

A cet instant du protocole, on peut voir que les partitions, répertoires ou fichiers normalement à Terdef sont considérés comme étant la propriété d'un autre utilisateur (ici, « Pierre » du groupe des administrateurs). L'utilisateur protégé « Terdef » du groupe des utilisateurs protégés (à droits limités) n'y aurait pas accès du tout.

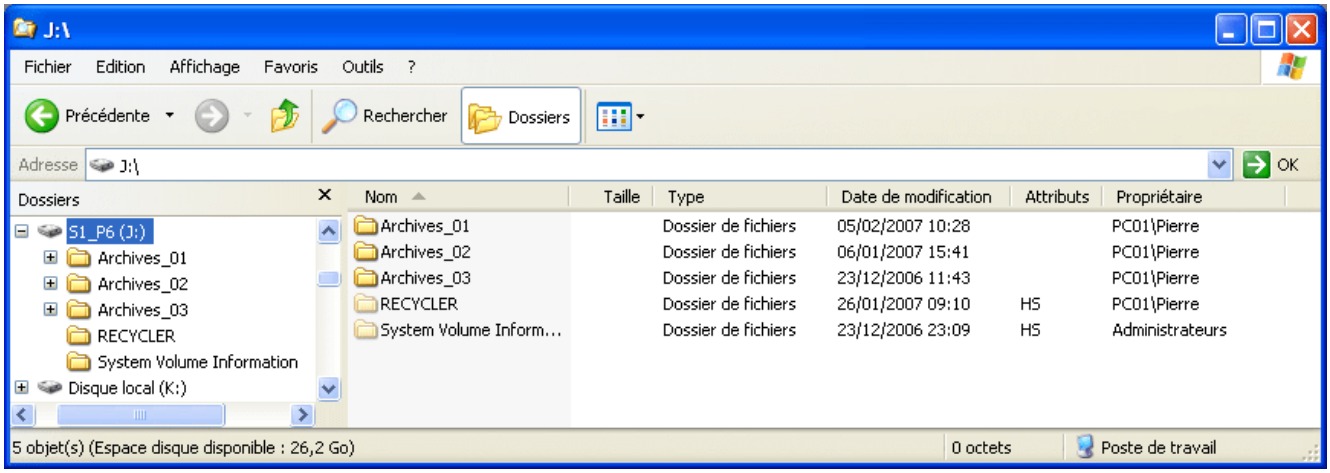


Figure 14 Explorateur de Windows pointant une partition propriété d'un autre

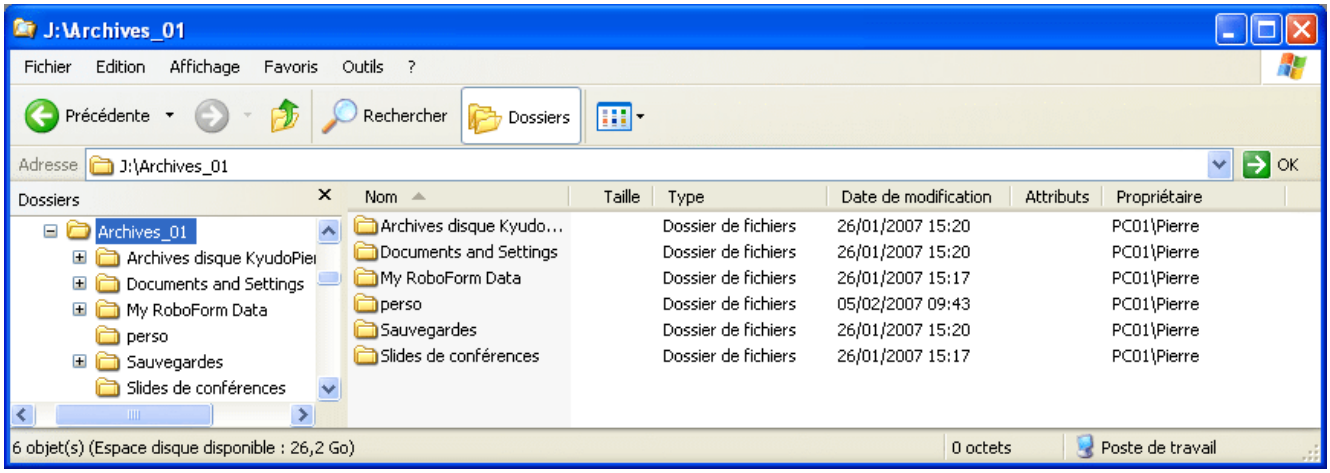


Figure 15 Explorateur de Windows pointant un conteneur (répertoire) propriété d'un autre

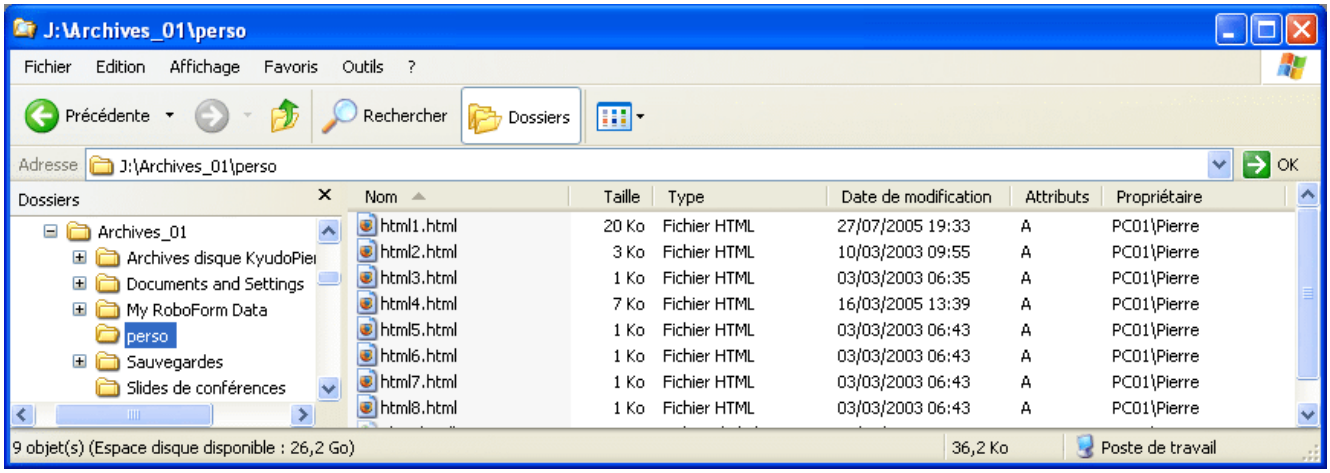


Figure 16 Explorateur de Windows pointant un sous-conteneur (sous-répertoire) propriété d'un autre. On observe que tous les fichiers sont également propriété d'un autre.

7.5.2 Accéder aux propriétés d'un objet

Dans l'explorateur de Windows, faire un clic droit (clic avec le bouton droit de la souris) sur un nom de partition ou un nom de répertoire) et sélectionner « Propriétés ».

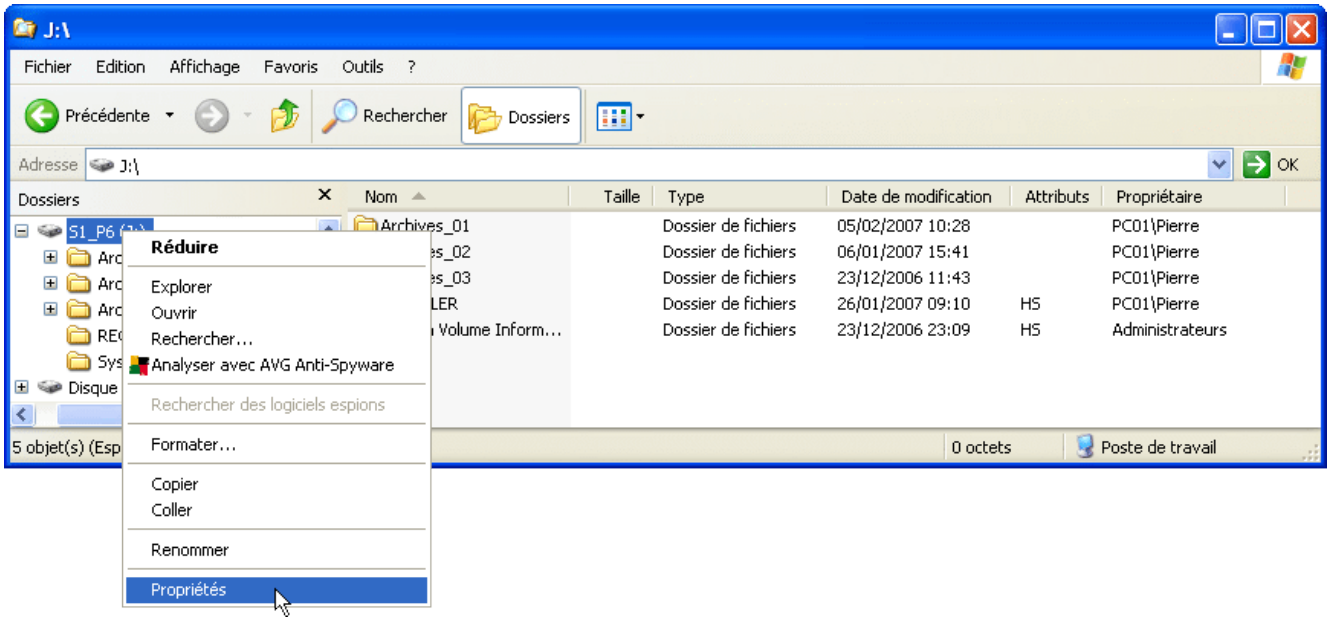


Figure 17 Accéder aux propriétés d'un objet (clic droit : menu contextuel)

7.5.3 Accéder à la sécurité d'un objet

Dans la fenêtre des propriétés de l'objet, sélectionner l'onglet « Sécurité »

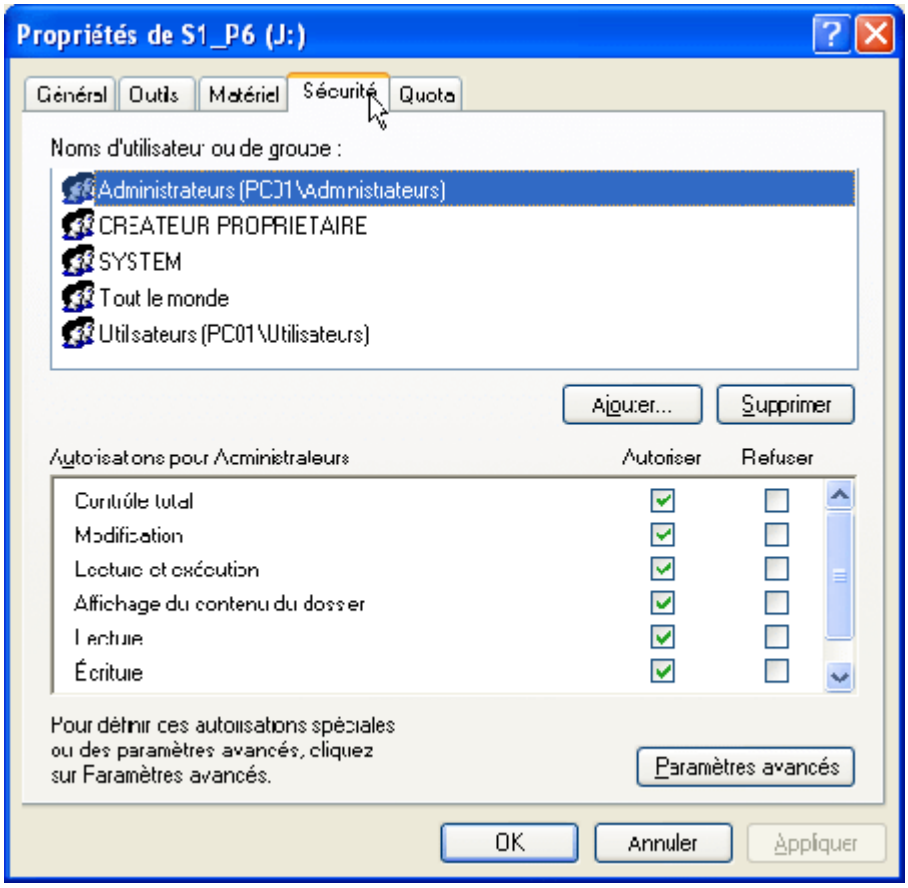


Figure 18 Onglet sécurité d'un objet avec sa liste d'utilisateurs ou de groupes ayant un ou des droits sur cet objet

7.5.4 Ajouter le nom de l'utilisateur protégé à la liste des utilisateurs

Nous allons ajouter le nom de l'utilisateur protégé à la liste des utilisateurs.

Clic sur le bouton « Ajouter »

Une nouvelle fenêtre apparaît

Saisir le nom du compte (le « login ») de l'utilisateur protégé (dans l'exemple, c'est « Terdef »)

Nous pourrions attribuer les droits à tout le groupe des utilisateurs protégés (« Limité ») auquel appartient l'utilisateur protégé « Terdef » (ce que nous ferions en entreprise pour donner des droits identiques à toutes les personnes d'un service, par exemple, qui auraient alors accès avec les mêmes droits aux partitions, répertoires et fichiers de « Terdef ». Ici, nous choisissons de réserver à l'usage exclusif de « Terdef » un ensemble d'objets.

Figure 19 Ajouter le nom de l'utilisateur protégé à la liste des utilisateurs de l'objet

Cliquer sur le bouton « Vérifier les noms »

Windows va vérifier que cet utilisateur existe et sur quel ordinateur il est identifié (dans l'exemple, l'ordinateur s'appelle PC01)

Figure 20 Vérification que ce compte (« login ») est connu (et sur quel ordinateur du réseau il est connu)

Clic sur « Ok »

Désormais, Terdef apparaît dans la liste des utilisateurs.

On observera que ses droits sont trop limités sur ses objets : il a bien le droit de lire ses fichiers et le contenu de ses répertoires mais il n'a pas le droit de les modifier : il découle des droits actuels qu'il n'a :

- pas le droit de créer un nouveau fichier dans un répertoire
- pas le droit de créer un nouveau sous-répertoire dans un répertoire
- pas le droit de modifier le contenu de ses fichiers
- …

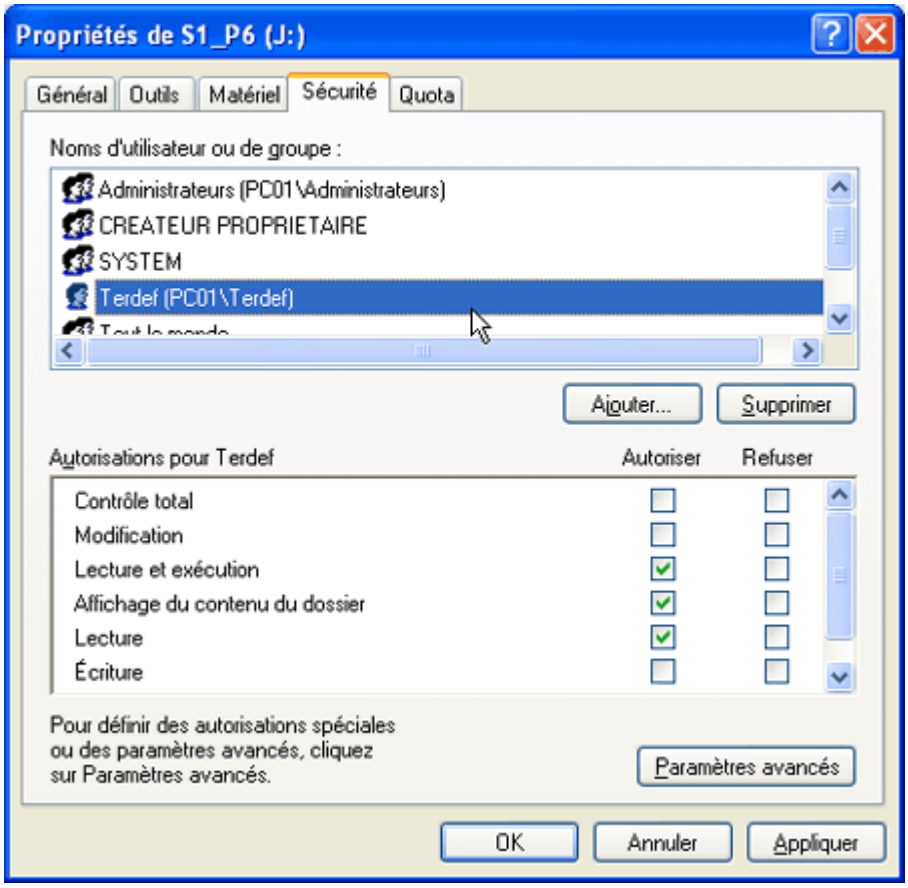


Figure 21 Observation des droits actuels de l'utilisateur protégé

7.5.5 Attribution du contrôle total de l'objet à l'utilisateur protégé

Sélectionner le compte de l'utilisateur « Terdef » et cocher la case « Contrôle total »
Cliquer sur le bouton « Appliquer »

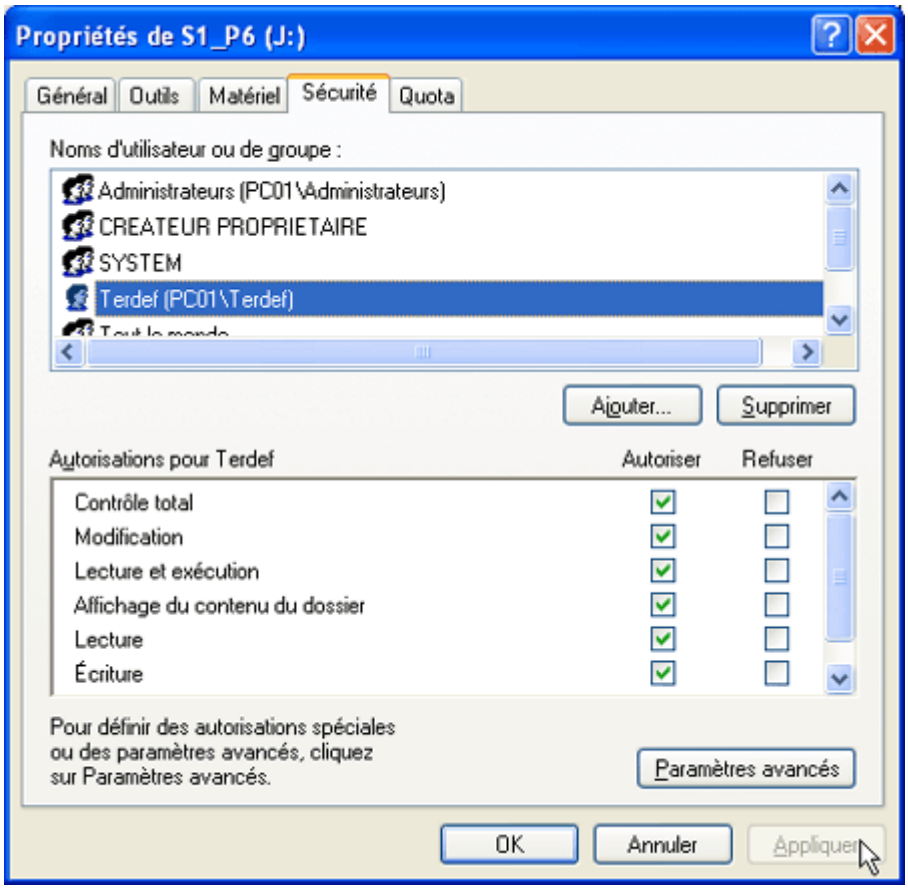


Figure 22 Attribution du contrôle total de l'objet à l'utilisateur protégé

Désormais « Terdef » à le contrôle total de la partition S1_P6 (la partition « J » sur cet ordinateur).

7.5.6 Retrait des droits sur cet objet aux autres utilisateurs

Clic sur le bouton « Paramètres avancés »

On s'aperçoit que divers groupes (et tous les comptes appartenant à ces groupes) ont accès à cet objet (la partition) et à tous les conteneurs et objets de cette partition – ils ont accès à tous les fichiers de « Terdef ».

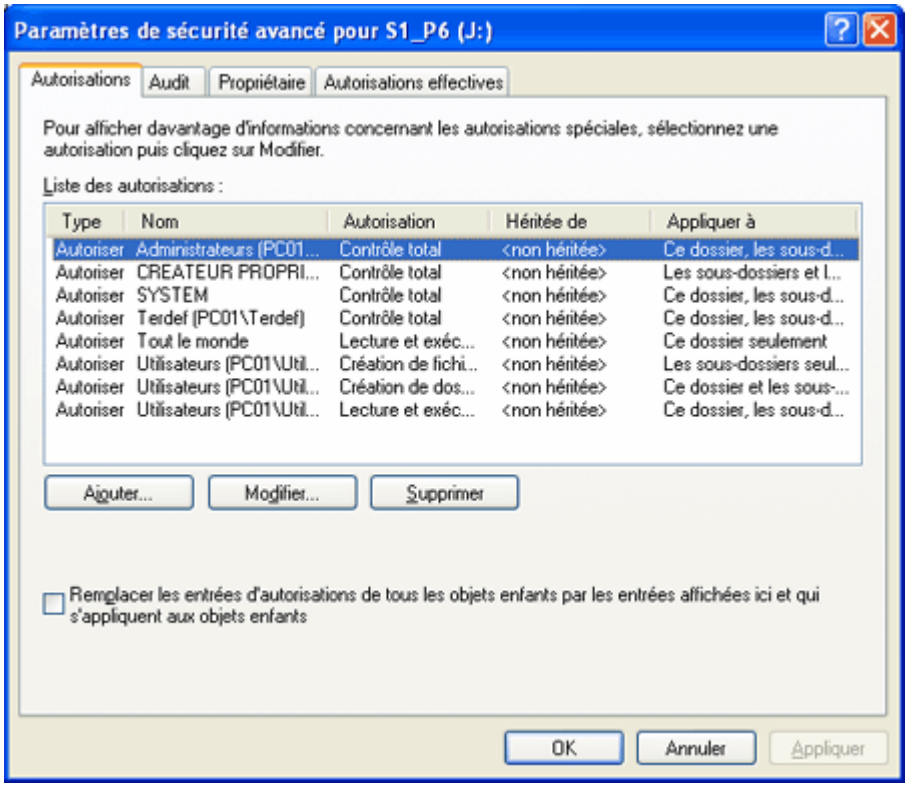


Figure 23 Liste des autorisations actuelles sur cet objet

On peut observer en détail les droits de chaque autorisation en cliquant sur le bouton « Modifier ». Par exemple :

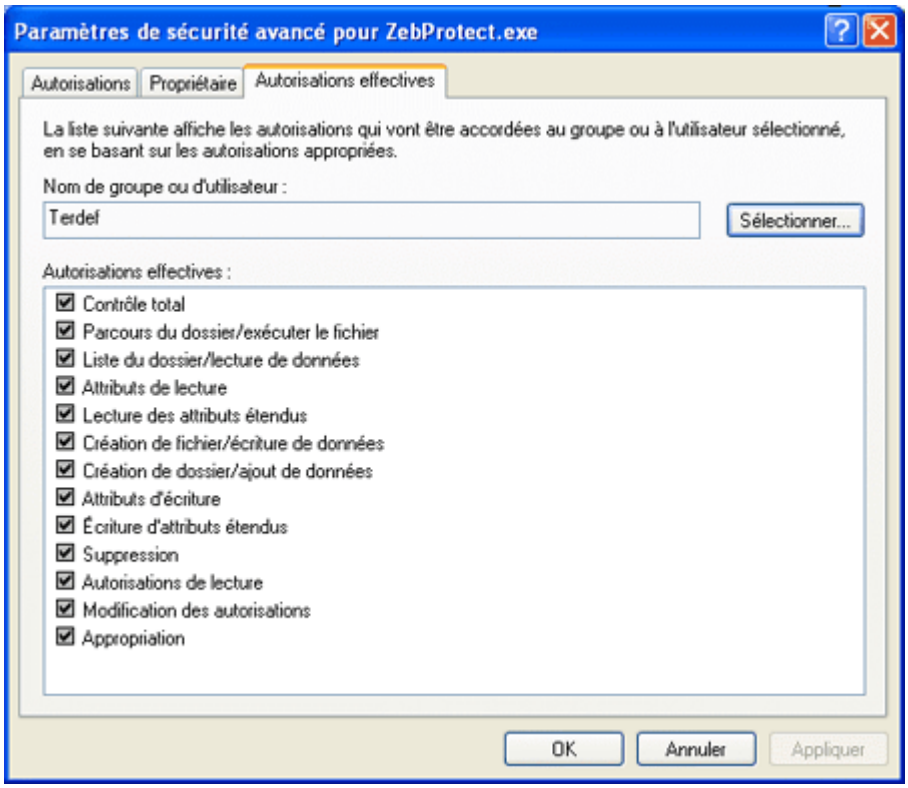


Figure 24 Droits détaillés sur un objet

Beaucoup trop de monde à donc accès aux objets de cette partition simultanément à « Terdef ».

Dans notre stratégie de sécurité, nous allons laisser le système et les administrateurs avoir accès à cette partition (et à tous les objets qui y sont contenus) ainsi que l'utilisateur protégé « Terdef ». Les autres comptes du groupe « Limité » (notés « Utilisateurs ») et le compte « Tout le monde » n'ont rien à faire ici.

Supprimons tous les autres (Sélectionner > Supprimer)

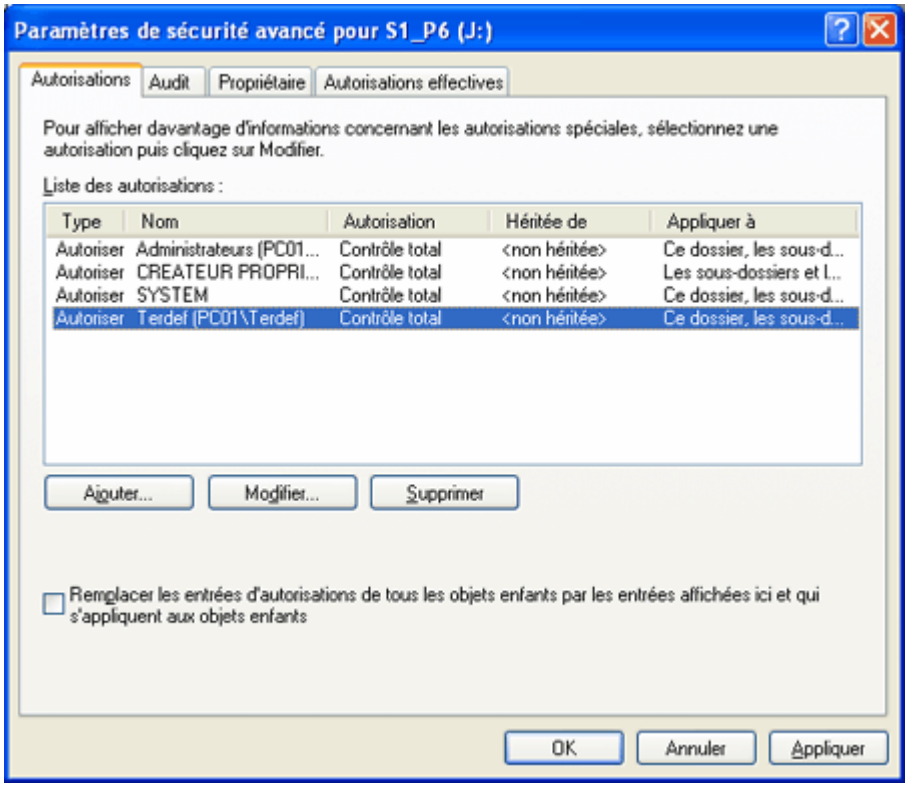


Figure 25 Suppression de droits aux autres utilisateurs

7.5.7 Propagation des droits à tous les objets du conteneur

Nous allons propager cette attribution de droits à l'ensemble des objets de cette partition.

Cocher la case « Remplacer les entrées d'autorisations de tous les objets enfants…)

Clic sur appliquer.

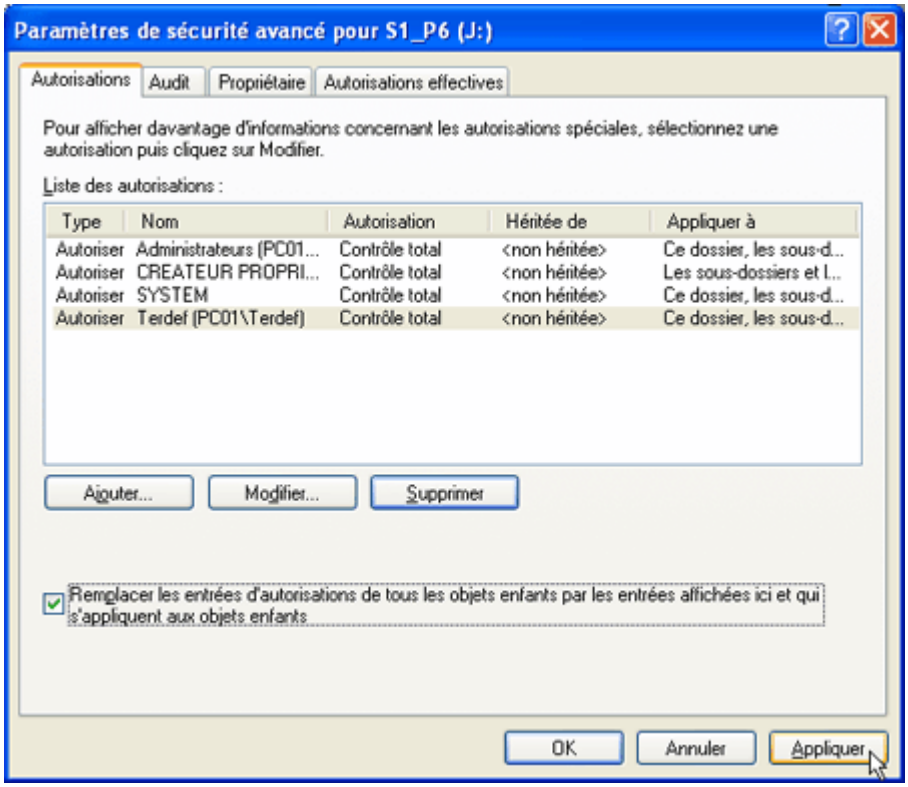


Figure 26 Propagation des droits aux objets du conteneur

Un message d'avertissement signale que, si des droits particuliers avaient été spécifiés sur tel ou tel objet « enfant », celui-ci perdra ses droits au profit des droits généraux de « Terdef ».

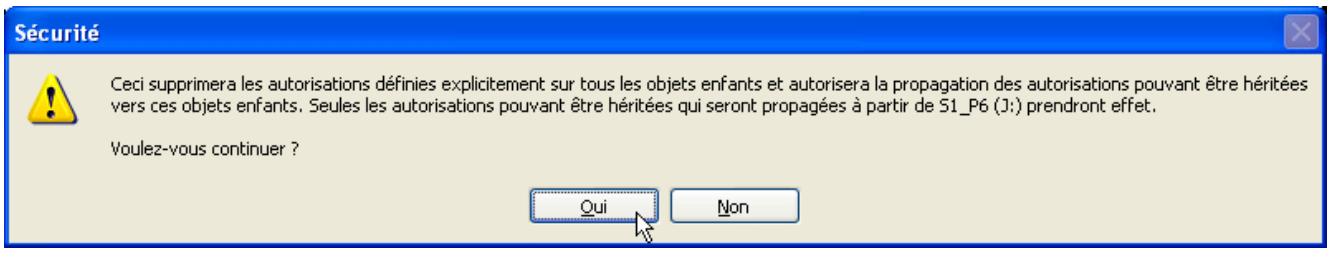


Figure 27 Message d'avertissement : la propagation des droits aux enfants est prioritaire sur les précédents droits dérogatoires des enfants

Clic sur « Oui ».

Une animation signale que les droits sont en train d'être propagés (« Définition des informations de sécurité ») à tous les objets enfants.

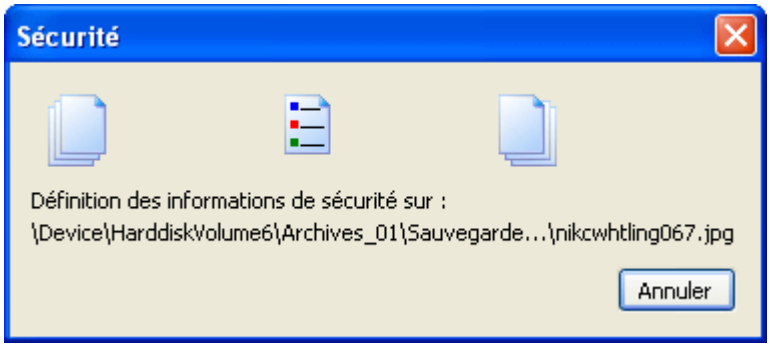


Figure 28 Animation durant la propagation des droits

A la fin, click sur « Ok ».

C'est terminé. L'utilisateur « Terdef » a le contrôle totale de tous les objets de cette partition. Refaire la même opération sur les autres partitions du l'utilisateur protégé (s'il en a plusieurs) ainsi que sur ses répertoires s'il en a ailleurs.

Une fois toutes ces manipulations terminées, fermer la session actuellement ouverte sous le compte « NouvelAdministrateur ».

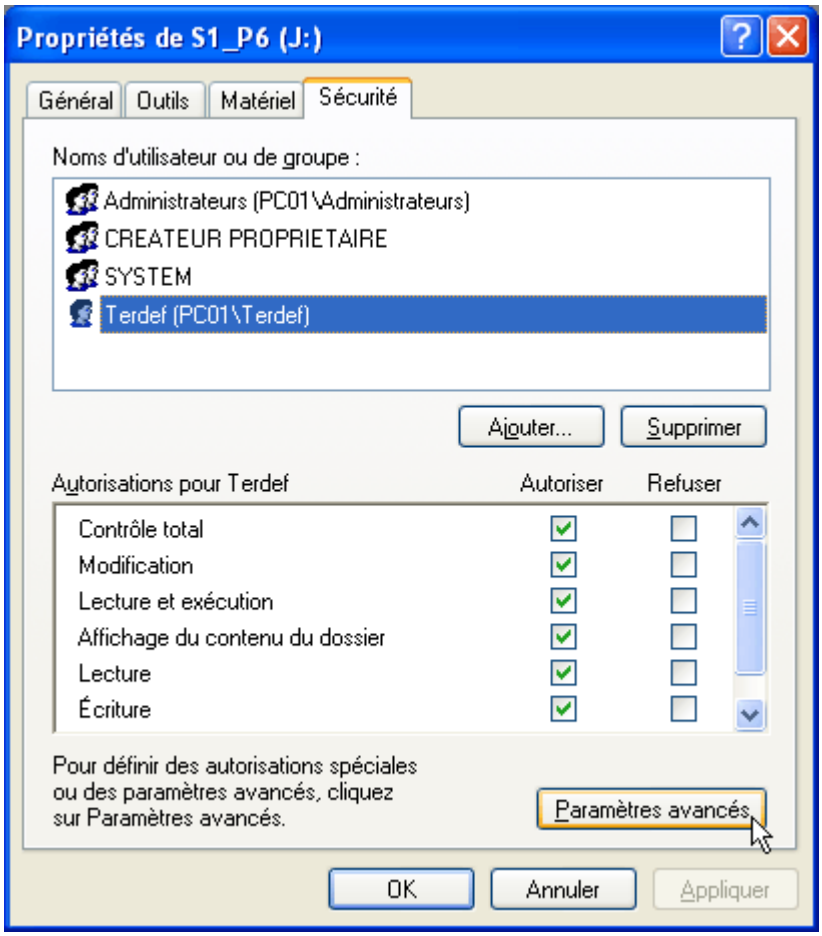
7.6 S'identifier sous le nouveau compte « limité »

Ouvrir une session sous le compte de l'utilisateur protégé.

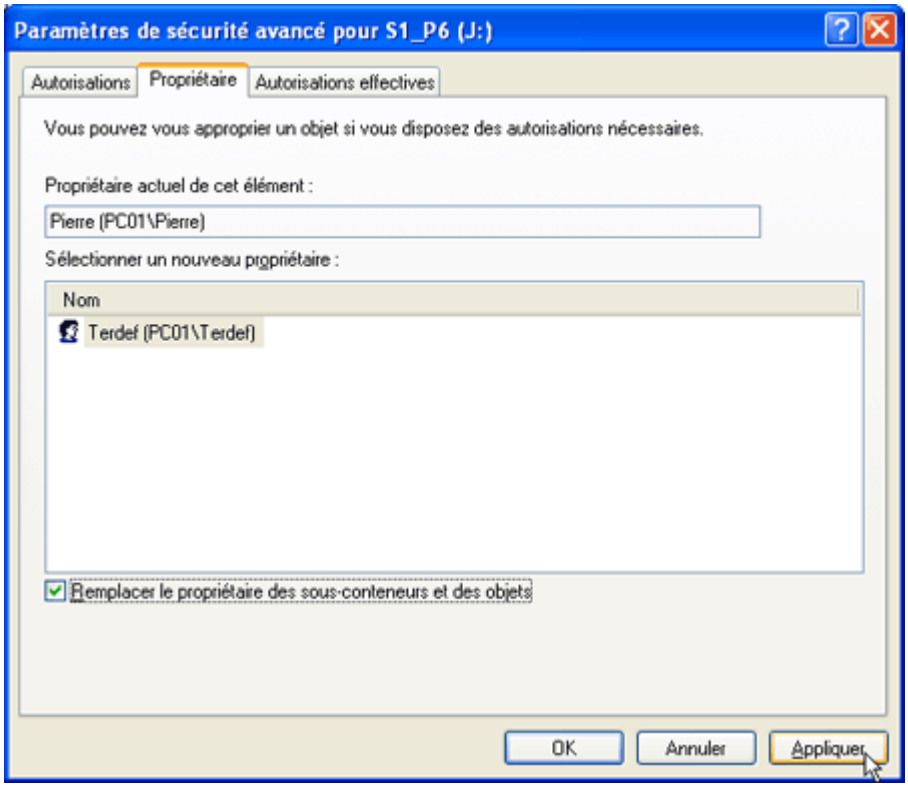
7.7 S'approprier les partitions, dossiers et fichiers personnels

Bien que « Terdef » ait le contrôle total de ses partitions, répertoires et fichiers, il n'en est pas encore propriétaire. Il doit « s'approprier » ses objets

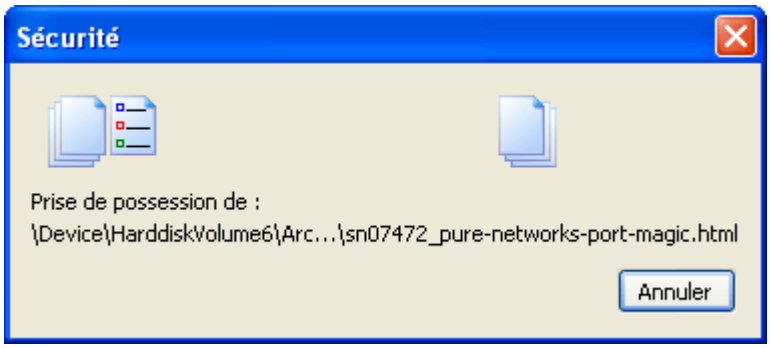
Explorateur de Windows > Clic droit sur le nom d'un objet (on commence par les objets hiérarchiquement les plus « élevés », soit les « partitions » > Onglet « Sécurité » > Sélectionner l'utilisateur protégé > Clic sur « Propriétés avancées »



Clic sur l'onglet « Propriétaire » > Sélectionner le nouveau propriétaire > Cocher la case « Remplacer le propriétaire des sous-conteneurs et des objets » > Clic sur « Appliquer »



Attendre la fin de l'animation et clic sur « Ok » > « Ok »



C'est terminé. Vérifions que tous les objets dans la partition sont bien, désormais, la propriété de « Terdef »

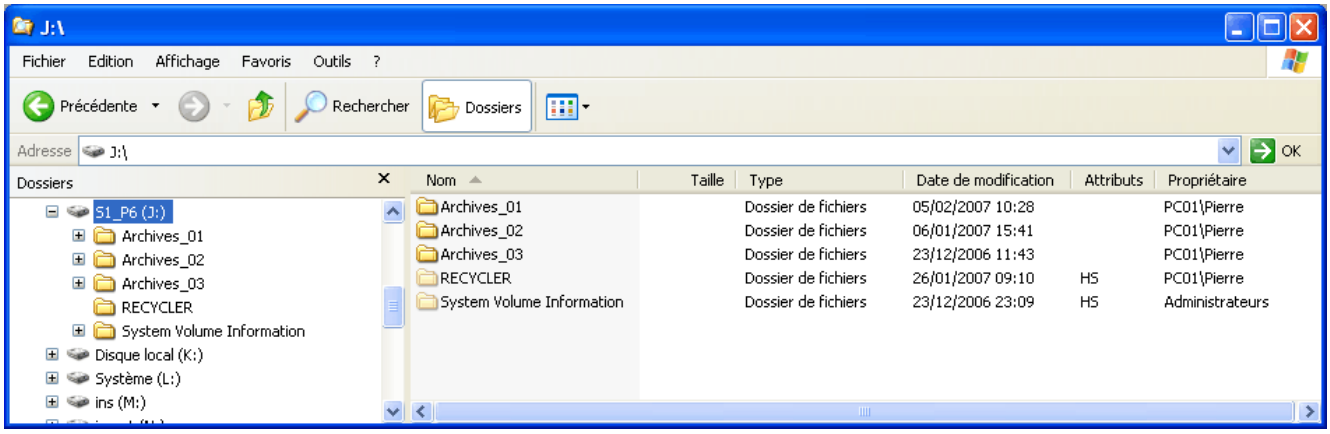


Figure 29 Propagation : Les conteneurs sont devenus propriété de l'utilisateur protégé

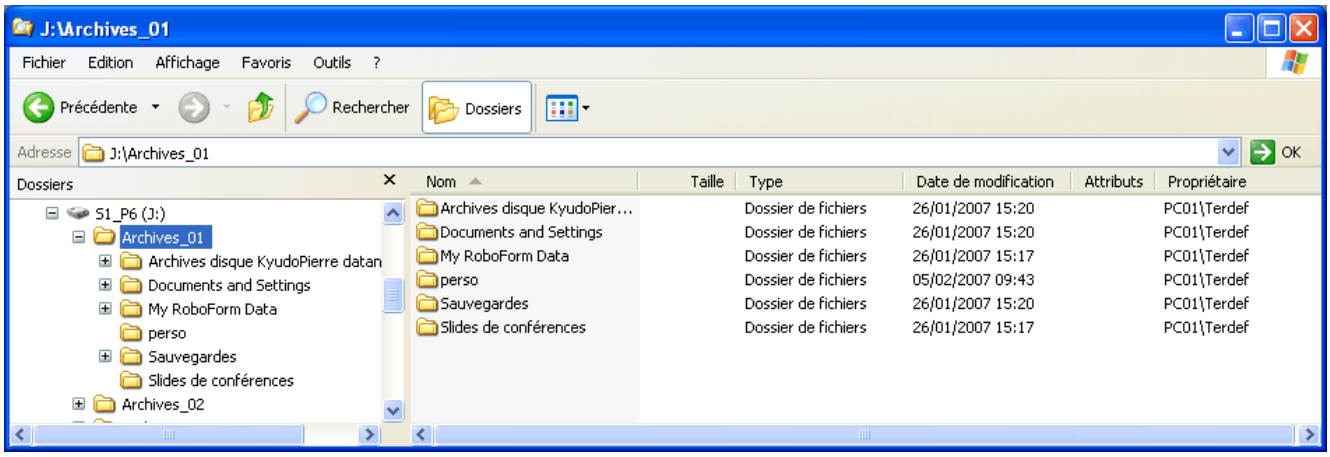


Figure 30 Propagation : Les sous-conteneurs sont devenus propriété de l'utilisateur protégé

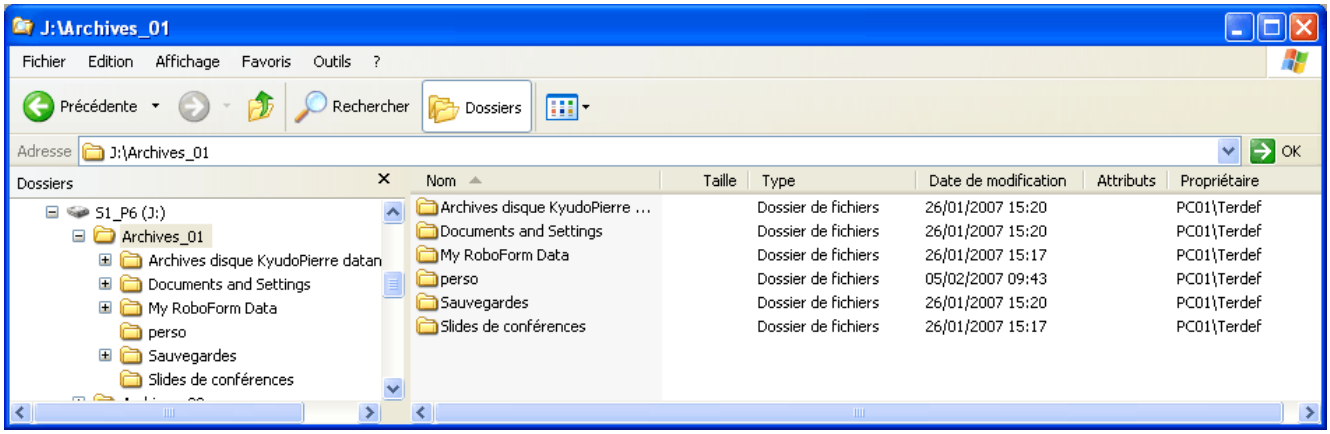


Figure 31 Propagation : Les fichiers sont devenus propriété de l'utilisateur protégé

8 Fin du protocole

L'utilisateur protégé « Terdef » peut désormais s'identifier et travailler en sécurité – dont naviguer sur l'Internet et lire ses messages – sans craindre qu'un parasite ne prenne facilement le contrôle de sa machine.

Ceci ne doit pas vous affranchir de l'usage d'un pare-feu, un antivirus et un anti-trojans ainsi que de quelques autres réglages (voir le Kit de sécurité à http://assiste.com.free.fr/p/kit_securite/kit_securite.html).

06 février 2007

Document provisoire en cours de rédaction

06.02.2007 Révision

© Pierre Pinard

http://assiste.com.free.fr – ASAP

Ce document est mis à votre disposition selon les termes de licence «Creative Commons» (http://assiste.com.free.fr/p/qui_suis_je/contrat_de_licence.html) qui s'imposent à vous. Vous avez le droit de copier et modifier la copie de cette page dans les conditions fixées par cette licence et tant que cette note est reproduite intégralement et apparaît clairement dans la copie ou la copie modifiée. Lire les conditions de la licence (http://assiste.com.free.fr/p/qui_suis_je/contrat_de_licence.html).

9 Ressources complémentaires – Pour en savoir plus

9.1 Stratégies de groupe

Définitions
http://www.bellamyjc.org/fr/strategie.html#definitions

La Microsoft Management Console "GPEDIT.MSC"
http://www.bellamyjc.org/fr/strategie.html#GPEDIT

Comment appliquer des stratégies locales sauf aux administrateurs
http://www.bellamyjc.org/fr/strategie.html#exceptadmin

Restauration des stratégies locales d'origine
http://www.bellamyjc.org/fr/strategie.html#restore

Les fichiers de résultats REGISTRY.POL
http://www.bellamyjc.org/fr/strategie.html#REGISTRYfiles

Les fichiers modèles .ADM
http://www.bellamyjc.org/fr/strategie.html#ADMfiles

Outil SHOWADM d'affichage des fichiers modèles .ADM
http://www.bellamyjc.org/fr/strategie.html#SHOWADM

Outil STRATEDIT d'édition de stratégies pour un compte donné
http://www.bellamyjc.org/fr/strategie.html#STRATEDIT

9.2 La Microsoft Management Console "GPEDIT.MSC"

http://www.bellamyjc.org/fr/strategie.html#GPEDIT
http://www.infoprat.net/astuces/windows2k_xp/astuces/perso_003.php

9.3 Les stratégies systèmes sous XP

http://www.ac-nancy-metz.fr/services/monxp/securiser_xp.htm