Éléments d'administration de Windows XP PRO

- Introduction
- Tour du propriétaire
- La base de registre
- Comptes d'utilisateurs, profils, sessions
- Sécurité, contrôle d'accès, privilèges
- Applications, processus, services
- Réseau, partages
- Annexes

Patrice Tréton
patrice.treton@ac-rouen.fr
Septembre 2005

Introduction

Ce document est le support d'un stage de formation d'une journée aux bases de l'administration sous Windows XP PRO qui a eu lieu à Bernay, le 27 septembre 2005. Il insiste sur les spécificités de ce système par rapport aux précédents : Windows 95-98-ME. La sécurité et les outils d'administration des postes y sont les principaux points développés.

Ces quelques pages n'ont pas la prétention de constituer une référence exhaustive sur le sujet, tout au plus un aide mémoire pour retrouver rapidement le nom d'une commande ou d'un utilitaire ainsi que quelques exemples d'utilisation. On y trouvera également un minimum de points théoriques indispensables : le fonctionnement des ACL, le cheminement des jetons, le calcul des droits d'accès et le mécanisme d'authentification défi/réponse utilisé en poste à poste.

Dans la suite de ce document, Windows XP désignera la version professionnelle. Windows 9x désignera Windows 98 ou Windows Millennium Edition. Par ailleurs, il ne sera pas fait mention de Windows XP édition familiale, même si certains points abordés s'appliquent également à ce système.

Cette version a été corrigée et complétée. Parmi les ajouts, on trouvera une description de la planification des tâches ainsi que de l'assistance à distance présentée par Sandrine Dangreville, lors de la deuxième journée de formation.

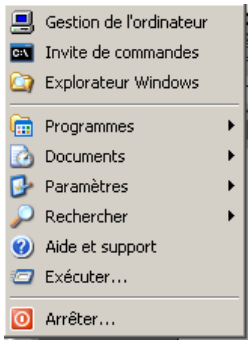
Les corrections et ajouts de cette version résultent essentiellement des remarques et questions des participants que je remercie ici.

Tour du propriétaire

Ce chapitre consiste en un parcours de l'interface utilisateur et en un repérage de l'emplacement des principaux utilitaires pertinents pour l'administrateur.

Bureau et menu Démarrer

Windows XP propose deux styles de menu Démarrer : le menu Démarrer XP et classique. La boîte de dialogue « Propriétés de la barre des tâches » permet de passer de l'un à l'autre, et offre diverses possibilités de paramétrages. On la fait apparaître en utilisant le menu contextuel de la barre des tâches, puis en choisissant l'item « Propriétés ».



Pour personnaliser le contenu du menu Démarrer, utiliser le menu contextuel du bouton « Menu démarrer », puis les items « Explorer » et « Explorer Tous les utilisateurs » suivant le profil sur lequel on souhaite intervenir.

Barre des tâches

Windows XP propose une nouvelle fonctionnalité : le groupement des boutons similaires. Il est possible de la paramétrer ;

La sélection de plusieurs boutons de la barre des tâches (à l'aide de CTRL + clic gauche), puis l'utilisation du menu contextuel sur l'un des boutons permet de réaliser une réorganisation des fenêtres en cascade ou en mosaïque ainsi que de fermer plusieurs fenêtres simultanément ;

La zone de notification des tâches (TNA) possède une fonction de masquage automatique des icônes, qu'il est possible de désactiver.

Explorateur de fichiers

L'explorateur de fichiers possède quelques paramètres utilisables en ligne de commande et exploitables dans le champ « Cible » des raccourcis.

Pour ouvrir une fenêtre de l'explorateur sur le dossier C:\rep et ouvrir ce dossier :

```
explorer.exe  /e,C:\rep
```

Pour ouvrir une fenêtre de l'explorateur sur le dossier C:\rep, ouvrir ce dossier et y placer la racine de l'arborescence :

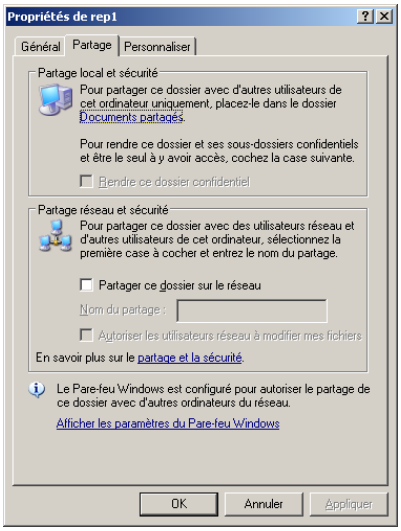
```
explorer.exe  /e,/root,C:\rep\fic.txt
```

Pour ouvrir une fenêtre de l'explorateur sur le dossier C:\rep et sélectionner le fichier fic.txt :

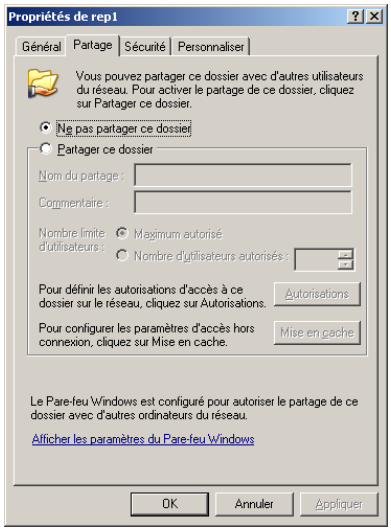
```
explorer.exe  /e,/select,C:\rep\fic.txt
```

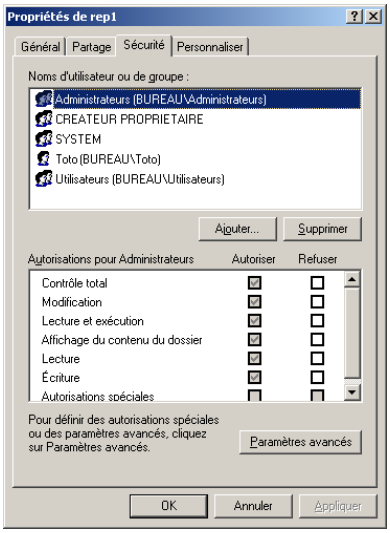
Si le paramètre /e est omis, l'arborescence des dossiers n'est pas affichée dans la partie gauche de la fenêtre.

L'onglet affichage du menu « Options des dossiers » propose quelques options qu'il est utile de connaître : « Fichiers et dossiers cachés », « Masquer les fichiers protégés du système d'exploitation » et « Utiliser le partage de fichiers simple » qui a aussi des répercussions au niveau de la sécurité. Pour la suite, il est indispensable de désactiver l'option « Partage de fichiers simple » :



Dialogue en mode simplifié
(un seul onglet)





Dialogue en mode normal
(deux onglets)

Menus « Outils système » et « Outils d'administration »

Le menu « Outils d'administration » n'est pas directement visible. Pour le faire apparaître, utiliser le menu contextuel de la barre des tâches, onglet « Menu démarrer », bouton « Personnaliser… », dans les options avancées, cocher « Afficher les outils d'administration ». Il est également possible de lancer le dialogue « Outils d'administration » à partir du panneau de configuration.

Panneau de configuration

Le panneau de configuration possède deux modes d'affichage : le mode classique en vrac et le mode par catégories.

Certaines applettes sont accessibles sans passer par le panneau de configuration, de façon plus rapide :

Applette Système : clic droit sur « Poste de travail », puis « Propriétés ». Cette boîte de dialogue comporte de nombreux paramètres importants du système ;

Applette Connexions réseau : clic droit sur « Favoris réseau », puis « Propriétés » ;

Applette Barre des tâches et Menu Démarrer : clic droit sur la barre des tâches, puis « Propriétés » ;

Applette Affichage : clic droit sur « Bureau », puis « Propriétés » ;

Applette Options des dossiers : dans l'explorateur de fichiers, menu « outils », puis « Options des dossiers » ;

Applette Options Internet : dans Internet Explorer, menu « outils », puis « Options Internet » ;

Parmi les autres applettes, on notera les suivantes apparues avec le SP2 : « Centre de sécurité », « Mises à jour automatiques » et « Pare-feu Windows ».

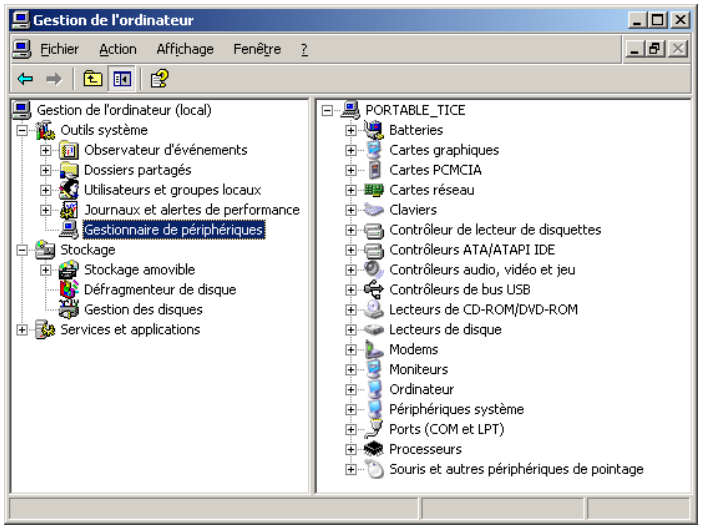
Console de gestion

Les consoles de gestion sont des boîtes de dialogue personnalisables dédiées à la gestion des postes. Chaque console est un fichier d'extension .msc de faible poids (inférieur à 100ko).

Ces consoles sont constituées de composants enfichables qui sont implémentés sous la forme de bibliothèques (dll).

Un certain nombre de consoles prédéfinies sont localisées dans le dossier C:\WINDOWS\system32.

En voici quelques unes parmi les plus utiles :



compmgmt.msc : Gestion de l'ordinateur. Cette console peut également être lancée par un clic droit sur « Poste de travail », puis sur « Gérer » ;

devmgmt.msc : Gestionnaire de périphériques (inclus dans la « Gestion de l'ordinateur ») ;

diskmgmt : Gestion de disques (inclus dans la « Gestion de l'ordinateur ») ;

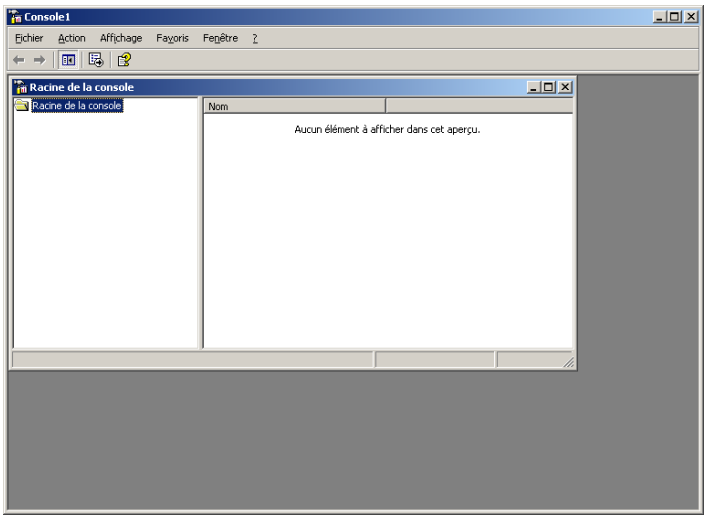
lusrmgr.msc : Utilisateurs et groupes locaux (inclus dans la « Gestion de l'ordinateur ») ;

services.msc : Services (inclus dans la « Gestion de l'ordinateur ») ;

secpol.msc : Paramètres de sécurité locale ;

gpedit.msc : Stratégie de groupe ;

Pour créer ou modifier des consoles, on a recours au « Microsoft Management Console ». Il suffit de lancer le fichier mmc.exe.



Au démarrage, l'application présente une console vide. Pour la peupler, sélectionner le menu Fichier, puis « Ajouter/Supprimer un composant logiciel enfichable ». Dans le dialogue qui s'affiche, cliquer sur le bouton « Ajouter… ». Sélectionner les composants un par un.

Organiser ensuite la fenêtre comme souhaité. On pourra utiliser le menu « Affichage », « Personnalisé » pour cela.

Il est possible de brider l'interface de la console en procédant comme suit : menu « Fichier », puis « Options ». Comme « mode de console », sélectionner : « Mode utilisateur - Accès limité, fenêtre unique ».

Une fois l'opération terminée, sauvegarder le fichier. Fermer mmc et ouvrir le fichier .msc créé en double-cliquant dessus.

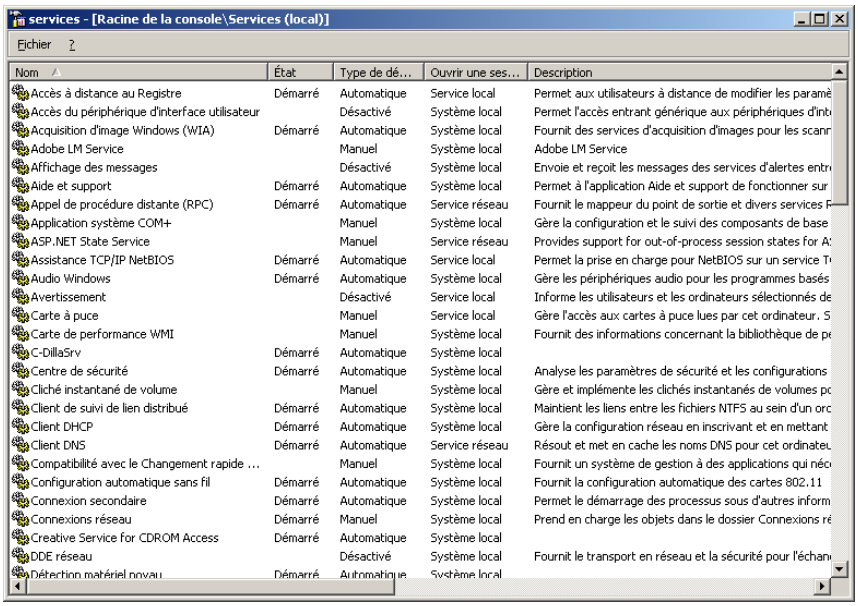
Remarque :

Pour modifier une console sauvegardée en mode utilisateur, il faut l'ouvrir comme suit :

```
mmc  chemin\fic.msc  /a
```

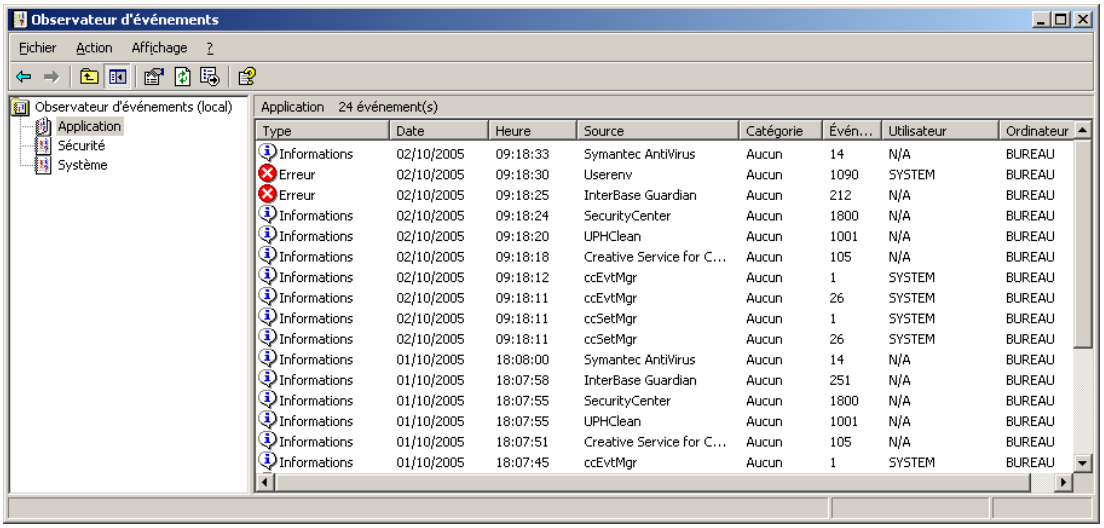
Le paramètre /a force l'ouverture en mode auteur.

Expérimentation : créer une console « Services » plus lisible comme dans l'exemple suivant :

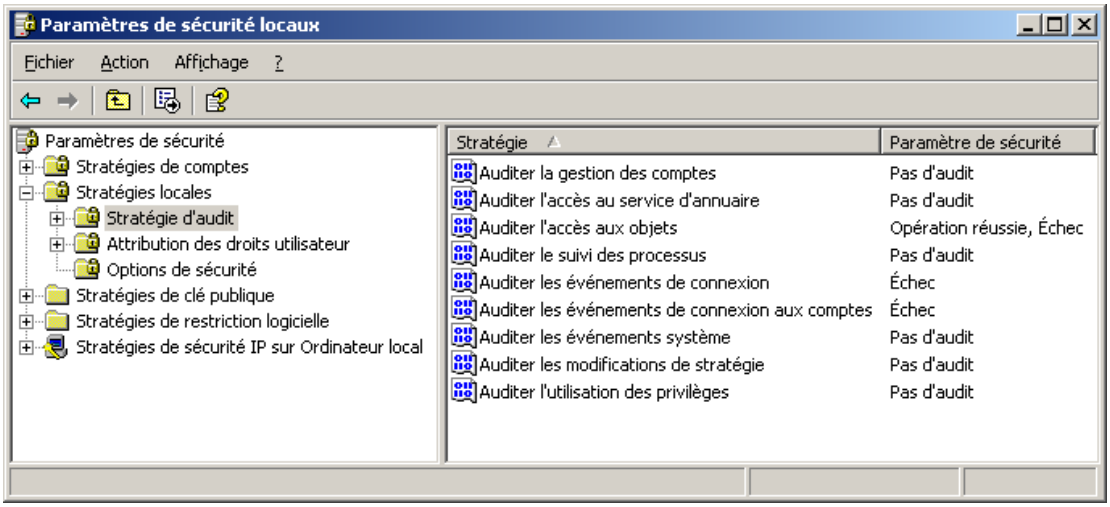


Journalisation des évènements

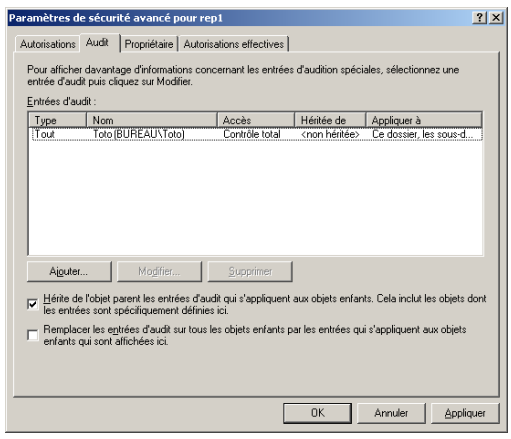
Pour afficher l'Observateur d'évènements, lancer eventvwr.msc.
(l'observateur d'évènements est également inclus dans la console « Gestion de l'ordinateur »).



Pour configurer les paramètres de journalisation, lancer la console de gestion « Paramètres de sécurité locaux » par : secpol.msc. Sélectionner ensuite « Stratégies locales », puis « Stratégie d'audit ». Sélectionner ce qui doit être audité et dans quels cas – réussite ou échec – l'audit doit avoir lieu.



Expérimentation : Pour auditer les opérations sur les fichiers, on sélectionnera « Opération réussie » et « Echec » au niveau de la ligne « Auditer l'accès aux objets ».

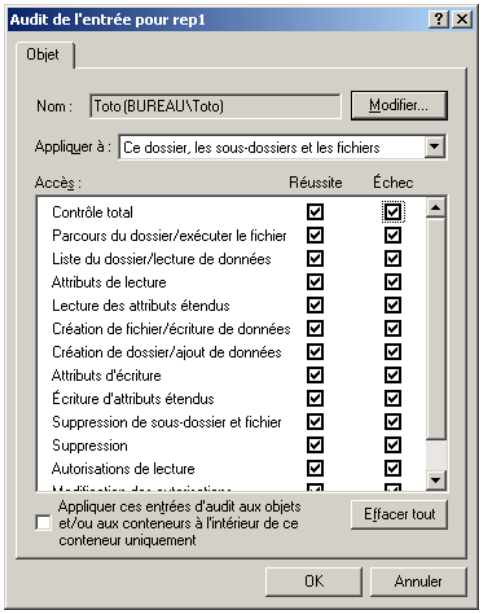


Remarque : pour ce qui suit, il est nécessaire d'avoir désactivé le partage de fichiers simple pour accéder à l'onglet Sécurité. Voir la méthode au chapitre intitulé « Tour du propriétaire ».

Pour le test, créer un dossier c:\rep1. Dans le menu contextuel du dossier, sélectionner « Partage et sécurité… », puis l'onglet « Sécurité ». Cliquer

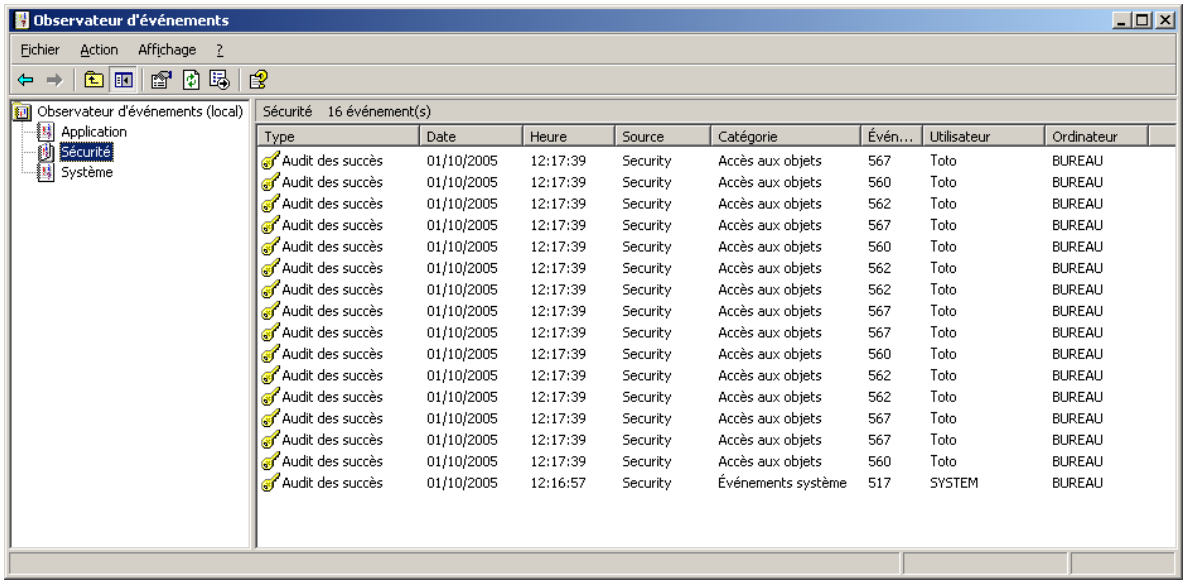
ensuite sur le bouton « Paramètres avancés », puis sur l'onglet « Audit ». Cliquer enfin sur le bouton « Ajouter ».

A ce niveau, saisir le nom de l'utilisateur dont on souhaite auditer les opérations sur le dossier (Ne pas se laisser abuser par l'intitulé « Entrez le nom de l'objet à sélectionner », c'est bien un nom d'utilisateur ou un nom de groupe qu'il faut saisir ici.). On peut également cliquer sur « Avancé », puis sur « Rechercher » pour obtenir une liste d'utilisateurs ou de groupes. Pour cet exercice, le plus simple consiste à saisir le compte que l'on utilise actuellement. Lorsque c'est fait valider par OK.



Dans le dialogue qui apparaît, sélectionner les opérations que l'on souhaite auditer : soit en réussite, soit en échec, soit les deux. Dans l'exemple, on a choisi d'auditer toutes les opérations réalisées sur le dossier (ainsi que sur chaque sous-dossier et fichier qu'il contient.)

Pour constater la mise en œuvre de l'audit, ouvrir le dossier c:\rep1 dans l'explorateur, dans une session ouverte par l'utilisateur choisi plus haut. Cette simple opération crée une quinzaine d'évènements visibles grâce à l'Observateur d'évènements, en sélectionnant le journal de sécurité.



Dans la pratique, il conviendra de sélectionner uniquement les opérations pertinentes (souvent les Echecs) afin de ne pas être submergé par les évènements. Ne pas oublier également de supprimer les entrées d'audit au niveau du dossier quand elles ne servent plus.

La base de registre

La base de registre est une base de données utilisée par le système pour stocker ses paramètres divers et variés. Elle a été conçue pour remplacer l'utilisation des fichiers .ini. Le registre possède une structure arborescente permettant une meilleure organisation des données. Elle est physiquement constituée de plusieurs fichiers appelés **ruches** qui sont situés, pour l'essentiel, dans le dossier C:\WINDOWS\system32\config ainsi que, pour la clé HKEY_CURRENT_USER, dans le dossier du profil des utilisateurs.

Les clé racines sont les suivantes :

HKEY_CLASSES_ROOT (HKCR) est un alias de HKEY_LOCAL_MACHINE\SOFTWARE\Classes. Cette clé comporte, entre autre, les informations sur les associations entre les extensions de fichiers et les applications à lancer pour les ouvrir ;

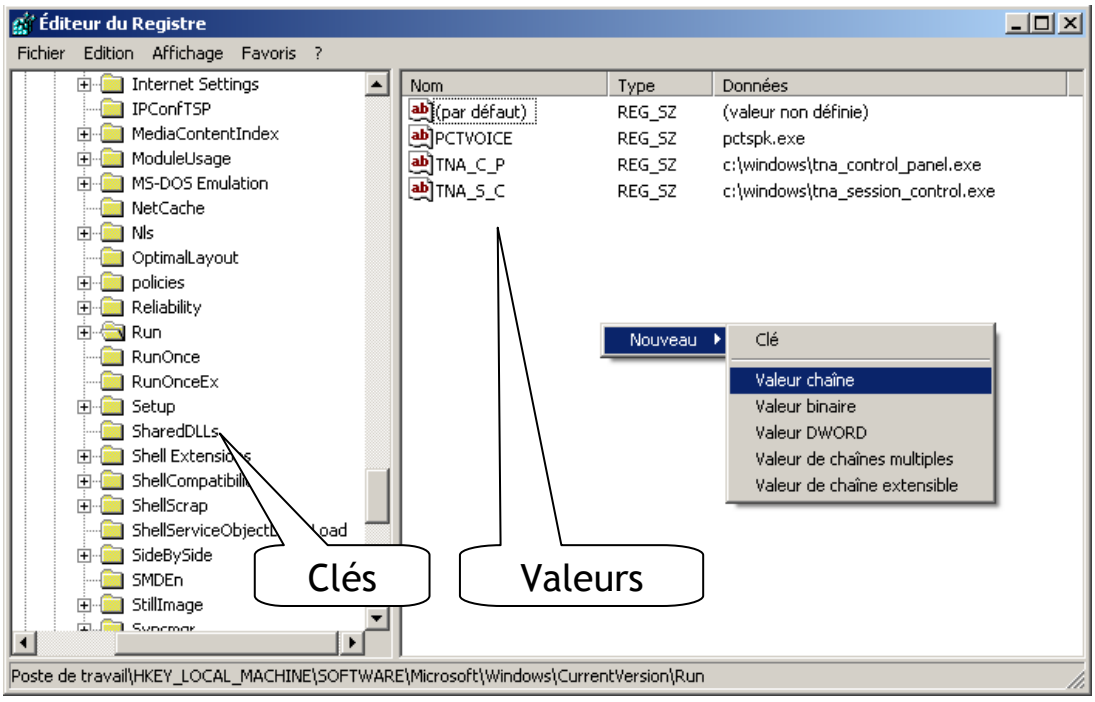
HKEY_CURRENT_USER (HKCU) correspond au fichier ntuser.dat de l'utilisateur actuellement connecté « physiquement » au poste. Il s'agit d'un alias sur l'une des sous-clés de la clé HKEY_USERS ;

HKEY_LOCAL_MACHINE (HKLM) contient des paramètres systèmes propres à la machine ainsi que des paramètres logiciels communs à tous les utilisateurs ;

HKEY_USERS (HKU) contient une sous-clé pour chaque utilisateur ayant actuellement une session ouverte, ainsi qu'une clé pour le compte .DEFAULT.

HKEY_CURRENT_CONFIG (HKCC) est un alias partiel de sous clés de HKEY_LOCAL_MACHINE.

Le principal outil permettant de consulter et de modifier le registre est l'Éditeur du registre. A la différence d'autres outils tels que la console « Paramètres de sécurité locaux » (c'est-à-dire secpol.msc), il permet l'accès à la totalité du registre. L'Éditeur du registre correspond au fichier exécutable C:\WINDOWS \regedit.exe.



L'Éditeur du registre présente à gauche l'arborescence des **clés** et à droite la liste des **valeurs** de la clé actuellement sélectionnée et dont le chemin complet est affiché dans la barre d'état. Les clés sont aux valeurs ce que les dossiers sont aux fichiers : un moyen d'organiser l'information de façon hiérarchique.

Une clé nouvellement créée ne comporte qu'une seule valeur appelée « (par défaut) ». Les autres valeurs sont créées par la suite.

La structure du registre est imposée par le système et les applications. Il est important de la respecter.

Le registre propose les types de valeurs suivants :

dword :	nombre codé sur 4 octets ;
binaire :	suite d'octets de longueur quelconque ;
chaîne :	chaîne de caractères ;
chaîne extensible :	chaîne contenant des variables pouvant être interprétées ;
chaîne multiple :	liste de chaînes de caractères.

Attention !

La base du registre contient des données sensibles. Il convient donc d'être particulièrement attentif lors de la modification de ces données. Des changements hasardeux de certaines valeurs peuvent rendre le système inutilisable.

Le chargement et le déchargement des ruches sont réalisés par le système, mais il est possible d'y procéder manuellement (pour corriger une ruche endommagée, par exemple). Utiliser pour cela le menu « Fichier », « Charger la ruche » ou « Décharger la ruche ». Une ruche ne peut être chargée que sous l'une des clés HKEY_LOCAL_MACHINE ou HKEY_USERS.

Il est possible d'exporter une clé et tout son contenu (valeurs et sous-clés) sous forme d'un fichier, puis d'importer ce fichier dans le registre sur un autre poste, par exemple. L'opération d'import d'un fichier .reg au registre s'appelle aussi « **fusion** ».

L'export d'une clé avec ses valeurs et ses sous-clés à partir de l'Editeur du registre crée un fichier .reg analogue au suivant :

```
Windows Registry Editor Version 5.00

[HKEY_CURRENT_USER\Temp]
"chaine"="valeur de la chaine"
"dword"=dword:12345678
"binaire"=hex:12,34,56,78,90
"chaine extensible"=hex(2):25,00,56,00,41,00,52,00,\
                           49,00,41,00,42,00,4c,00,45,\
                           00,5f,00,44,00,5f,00,45,00,\
                           4e,00,56,00,49,00,52,00,4f,\
                           00,4e,00,4e,00,45,00,4d,00,\
                           45,00,4e,00,54,00,25,00,5c,\
                           00,6d,00,6f,00,6e,00,66,00,\
                           69,00,63,00,68,00,69,00,65,\
                           00,72,00,2e,00,74,00,78,00,\
                           74,00,00,00
"chaine multiple"=hex(7):63,00,68,00,61,00,69,00,\
                         6e,00,65,00,20,00,31,00,00,\
                         00,63,00,68,00,61,00,69,00,\
                         6e,00,65,00,20,00,32,00,00,\
```

```
                        00,63,00,68,00,61,00,69,00,\
                        6e,00,65,00,20,00,33,00,00,\
                           00,00,00
; un commentaire
```

Ce fichier est encodé en unicode. (Toutefois, les fichiers créés manuellement et encodés en ANSI sont également reconnus lors de l'import.)

Windows 9x utilisait un format moins complet et toujours encodé en ANSI. Windows XP reconnaît également et est capable d'importer des fichiers .reg de ce type. En voici un exemple :

```
REGEDIT4

[HKEY_CURRENT_USER\Temp]
"chaine"="valeur de la chaine"
"dword"=dword:12345678
"binaire"=hex:12,34,56,78,90
```

L'ancien format ne prenait pas en charge les types chaînes extensibles ni les chaînes multiples. Toutefois, la majorité des données du registre étant de l'un des trois types acceptés par le format des fichiers .reg de Windows 9x, ce dernier pourra sans véritable restriction être utilisé comme format commun aux deux plateformes.

Remarque :

L'Editeur du registre de Windows 9x possède un bogue qui l'empêche de prendre en compte la dernière ligne des fichiers .reg. Pour le contourner, il suffit de terminer le fichier par une ligne vide.

La fusion d'un fichier .reg peut être réalisée soit à l'aide de l'Editeur du registre, soit en double-cliquant sur le fichier .reg voulu.

Il est possible de supprimer une clé ou une valeur à partir d'un fichier .reg. Il suffit d'utiliser un signe moins, comme dans les exemples suivants :

```
Windows Registry Editor Version 5.00

; Suppression d'une valeur
[HKEY_CURRENT_USER\Temp1]
"nom_de_valeur"=-

; Suppression d'une clé (et de toutes ses sous-clés)
[-HKEY_CURRENT_USER\Temp2]
```

On prendra garde au fait que la suppression d'une clé entraîne celle de toutes ses sous-clés.

Cette technique fonctionne également avec le format des fichiers .reg de Windows 9x.

Pour fusionner un fichier .reg au registre à partir d'un script .bat sans dialogue de confirmation, procéder comme suit :

```
regedit  /s  chemin\fic.reg
```

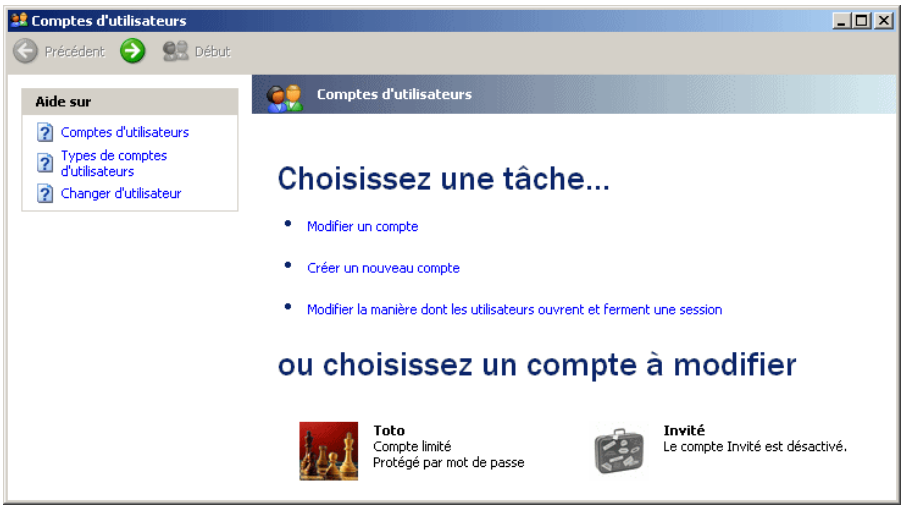
Le paramètre /s force le mode silencieux.

Expérimentation :
- Édition manuelle directe. Exemple avec le bogue du bloc-notes ;
- Export de deux fichiers .reg, regroupement et adaptation en un seul, puis fusion du résultat au registre d'un autre poste.

Comptes d'utilisateurs, profils, sessions

Les utilisateurs et leur gestion

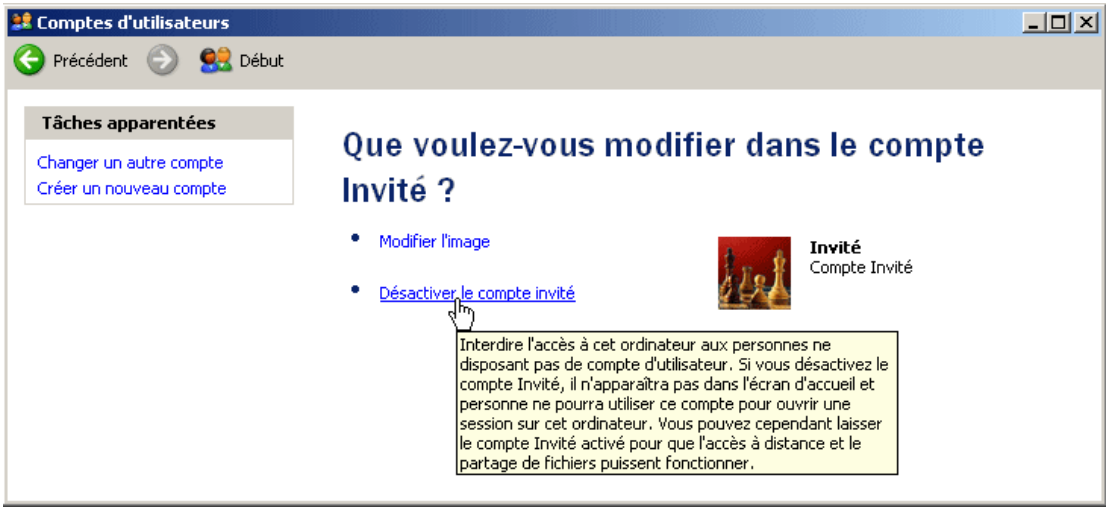
L'applette « Comptes d'utilisateurs » permet une gestion simpliste des comptes.



Attention !

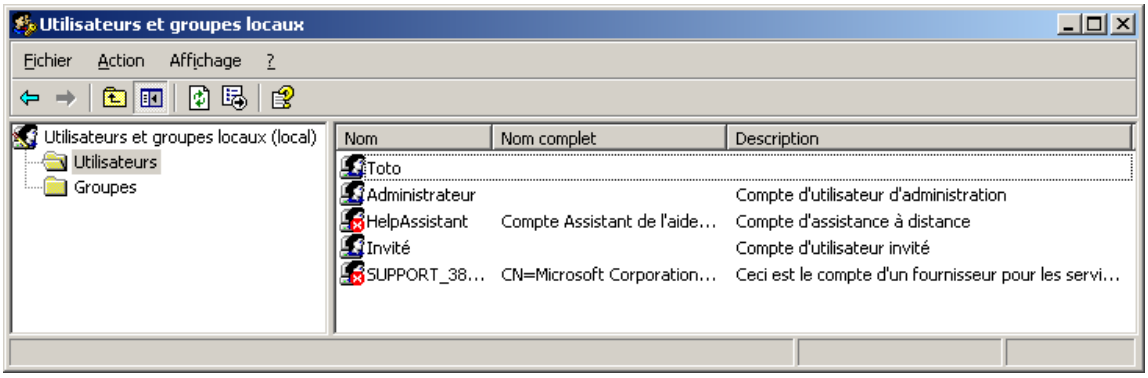
L'option « Désactiver le compte invité » – voir figure – ne désactive pas réellement le compte. Seule l'ouverture d'une session locale en tant qu'invité est interdite ; le compte invité reste disponible pour l'accès aux partages, par exemple.

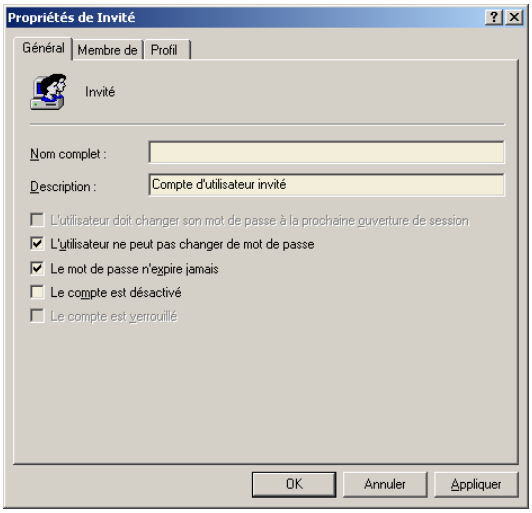
La version américaine emploie « turn off » dans ce dialogue alors qu'elle utilise « disable » pour la désactivation. La version française n'opère aucune distinction terminologique ce qui contribue à la confusion comme on peut le constater ci-dessous..



Le texte de l'info-bulle n'est pas très clair. La dernière phrase doit en fait être comprise comme « Ce faisant, vous laissez le compte Invité disponible pour que l'accès à distance et le partage de fichiers puissent fonctionner. »

On préfèrera à cette applette la console « Utilisateurs et groupes locaux » qui est incluse dans la console « Gestion de l'ordinateur » ou qui peut être lancée directement par : lusrmgr.msc.





Un double-clic sur l'un des items permettra d'accéder aux principaux paramètres du compte d'utilisateur correspondant..

Compte « administrateur »

Ce compte est créé lors de l'installation du système. Il fait partie du groupe « Administrateurs » – noter le « s » – et dispose donc de suffisamment de droits pour gérer le poste.

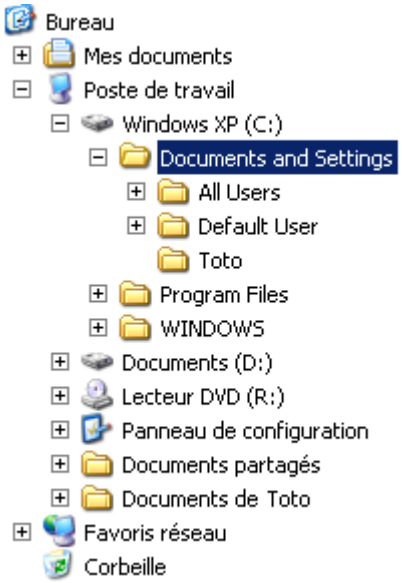
Ce compte est identifié par le système grâce à son SID (voir plus loin), il peut donc être renommé sans problème.

Compte « invité »

Ce compte a une fonction essentielle dans l'accès aux partages réseau.

Malgré la suggestion faite dans l'applette « Comptes d'utilisateurs » de l'utiliser pour ouvrir des sessions locales, il est préférable de l'éviter. On pourra créer un autre compte à cette fin : « invite » (sans accent), « anonyme »…

Les profils



Les paramètres propres à un utilisateur donné sont stockés dans un **profil**. Il s'agit d'un dossier contenant un fichier ruche (ntuser.dat) ainsi qu'un ensemble de dossiers.

Le fichier **ntuser.dat** correspond à la clé hkey_current_user une fois chargé dans le registre.

Les dossiers qui constituent un profil sont les suivants :

Application Data : ce dossier est présent pour permettre aux applications qui le souhaitent de stocker des informations propres à l'utilisateur. Une application qui préférerait créer un fichier .ini au lieu de stocker les paramètres dans le registre devrait placer ce fichier ici. C'est le cas du navigateur Firefox, par exemple.

Ce dossier contient en particulier le dossier « Microsoft\Internet Explorer\Quick Launch » qui regroupe les raccourcis correspondant à la barre d'outils de lancement rapide.

Bureau : ce dossier contient les icônes visibles sur le bureau de l'utilisateur. Certaines icônes telles que le « Poste de travail », les « Favoris réseau », le dossier « Mes documents » ou la corbeille sont des icônes ajoutées par le système. Il est d'ailleurs possible de les masquer.

Cookies, Favoris : contiennent les cookies et les favoris d'Internet Explorer.

Local Settings : à la différence des autres dossiers, celui-ci n'est jamais transféré sur le serveur dans le cas d'un profil itinérant. Il contient un dossier **Application Data**, ayant la même fonction que celui décrit plus haut, un dossier **Historique**, pour Internet Explorer, un dossier **Temp**, celui vers lequel pointent les variables d'environnement TEMP et TMP, ainsi que le dossier **Temporary Internet File**, qui est le cache d'Internet Explorer.

Menu démarrer : ce dossier contient les raccourcis qui apparaissent dans le menu Démarrer de l'utilisateur. Il contient en particulier le dossier **Programmes** qui comporte lui-même le dossier **Démarrage**.

Mes documents : ce dossier est le conteneur par défaut des documents créés par l'utilisateur. Les applications devraient initialement ouvrir leurs boîtes de dialogue « Ouvrir » et « Enregistrer sous » dans ce dossier.

Modèles : ce dossier contient des fichiers utilisés à la création de nouveaux documents d'un certain type.

Recent : ce dossier contient des raccourcis vers les derniers fichiers ouverts (dont les plus récents apparaissent dans le sous-menu Document du menu Démarrer).

SendTo : ce dossier contient des raccourcis qui apparaissent dans le sous-menu « Envoyer vers » du menu contextuel de la partie droite de l'Explorateur de fichiers.

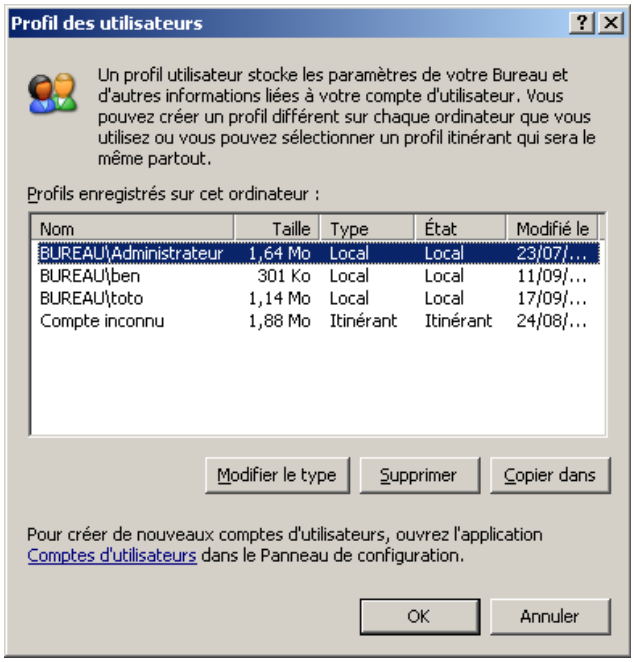
UserData : ce dossier est utilisé par la plateforme .NET pour stocker les données de certaines applications.

Voisinage d'impression, **Voisinage réseau** : ces dossiers contiennent des raccourcis vers les ressources réseau auxquelles l'utilisateur a déjà accédé.

Lorsqu'un utilisateur ouvre une session locale pour la première fois sur un poste, le système crée un profil à la volée, en dupliquant le profil « Default User » puis en adaptant cette copie.

Tous les comptes n'ont pas forcément de profil.

Pour copier un profil d'un utilisateur vers un autre, il faut utiliser la boîte de dialogue « Profil des utilisateurs » accessible à partir de la boîte de l'applette « Propriétés système ». Sélectionner le profil source puis cliquer sur « Copier dans ». Spécifier ensuite où le profil doit être copié et quel utilisateur doit pouvoir l'utiliser. Le système modifie alors non seulement les ACL des dossiers et fichiers du profil, mais également les ACL des clés de ntuser.dat (qui est une ruche du registre).



La méthode la plus simple pour personnaliser le profil d'un utilisateur consiste à ouvrir une session en tant que cet utilisateur.

Il peut arriver qu'une ruche ntuser.dat ne puisse être déchargée en fin de session. Cela se produit dès qu'une application oublie de libérer une clé qu'elle a ouverte sous la clé HKEY_CURRENT_USER. Divers problèmes peuvent en résulter. En particulier, les stratégies de groupes peuvent ne pas être appliquées correctement. Ce problème est de plus assez aléatoire. Microsoft propose une parade sous la forme d'un correctif : le service **UPHclean**. Une fois installé, le service « User Profile Hive Clean » se charge de forcer la libération des clés en fin de session pour permettre le déchargement du fichier ntuser.dat.

Le système crée trois profils particuliers pour des usages spécifiques :

Default User

Ce pseudo profil – l'utilisateur « Default User » n'existe pas – sert de modèle à Windows lorsqu'il doit créer les profils des utilisateurs.

Pour personnaliser le fichier ntuser.dat de ce profil, on pourra créer une copie du fichier ntuser.dat d'un autre profil, comme décrit plus haut. Pour des modifications ponctuelles, on pourra utiliser la technique du chargement/déchargement d'une ruche dans le registre, à l'aide de l'Éditeur du registre.

.DEFAULT

Ce profil est chargé dans le registre en permanence. A la différence des autres profils, celui-ci est stocké – à l'abri, en quelque sorte – dans le dossier :

C:\WINDOWS\system32\config\systemprofile

Ce profil est utilisé par les comptes système, donc en particulier par les services. Il est également utilisé par l'application **winlogon** chargée par le système de gérer les ouvertures des sessions. Ceci explique que les paramètres d'affichage du bureau de l'ouverture de

session y soient stockés. Par exemple, le thème, les couleurs et l'arrière plan de la boîte de dialogue d'ouverture de session sont définis ici.

Pour un usage normal, il n'est pas utile de personnaliser les dossiers de ce profil.

All Users

Ce pseudo profil est utile dans la mesure où il permet de définir des paramètres communs à tous les utilisateurs. On pourra ainsi définir le contenu de base du menu Démarrer de tous les utilisateurs en plaçant les raccourcis uniquement dans le dossier « Menu Démarrer » du profil All Users. On pourra ensuite laisser vides les dossiers « Menu Démarrer » des utilisateurs, ou les compléter au besoin.

Sessions

A tout instant, le système se trouve dans l'un des trois états suivants :

1. En attente d'ouverture de session. La boîte de dialogue d'identification est affichée. On notera que les paramètres de ce bureau sont stockés dans le profil .DEFAULT.

2. Session en cours. Un utilisateur a ouvert une session, soit localement soit à distance.

3. Economiseur d'écran. Le système utilise un troisième état pour afficher l'économiseur d'écran.

Pour ouvrir une session, l'utilisateur doit s'authentifier en saisissant un identifiant et un mot de passe. Le système propose deux types de dialogue pour ce faire : l'écran d'accueil de Xp et la boîte de dialogue classique.

L'écran d'accueil XP

Dialogue classique

Pour accéder au dialogue classique à partir de l'écran d'accueil, saisir deux fois de suite la séquence de sécurité **CAD** (les touches CTRL-ALT-SUPPR simultanément).

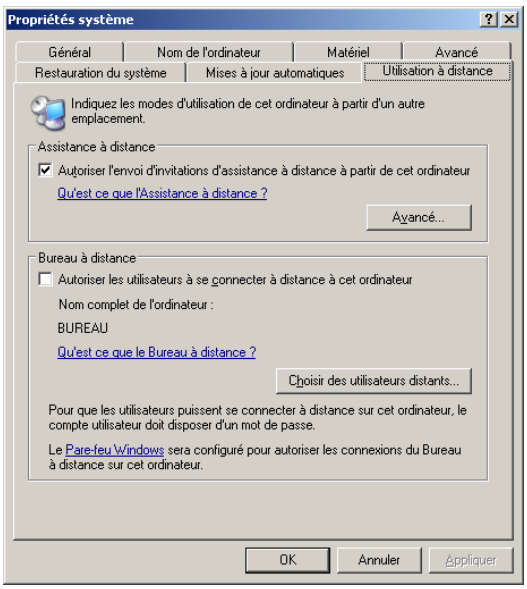
Pour que le dialogue classique soit affiché directement, lancer l'applette « Comptes d'utilisateurs », puis cliquer sur « Modifier la manière dont les utilisateurs ouvrent et ferment une session ». Décocher la case « Utiliser l'écran d'accueil ». Noter que lorsque le poste a joint un domaine, l'écran d'accueil est automatiquement désactivé au profit du dialogue classique.

Pour éviter les leurres – faux dialogues d'ouverture de session destinés à récupérer les identifiants et mots de passe des utilisateurs – les véritables boîtes de dialogue invitent les utilisateurs à saisir la séquence de touches **CAD**. En effet, seule la boîte de dialogue

authentique intercepte cette séquence ; saisie sur un faux dialogue, la boîte de dialogue « Sécurité de Windows » apparaîtrait, révélant ainsi la supercherie.

En cours de session, la séquence de sécurité **CAD** a une autre fonction décrite au chapitre « Applications, processus et services ».

Assistance à distance

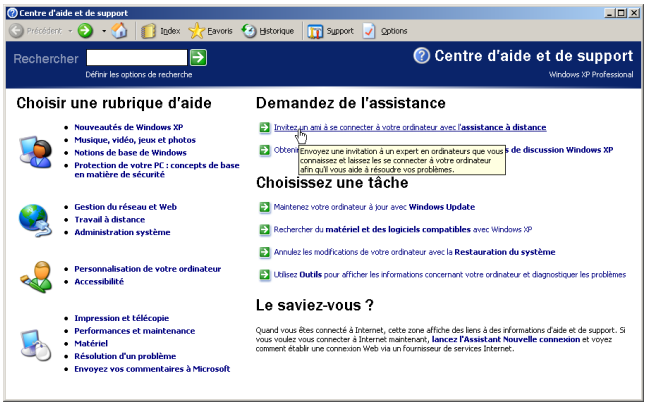


L'assistance à distance permet à un utilisateur distant – désigné sous le terme de conseiller – d'interagir avec la session actuellement ouverte (ou qui sera ouverte lors du contact) par l'assisté. Pour cela, vérifier au niveau de la boîte de dialogue des « Propriétés système » du poste assisté que l'assistance à distance est activée.

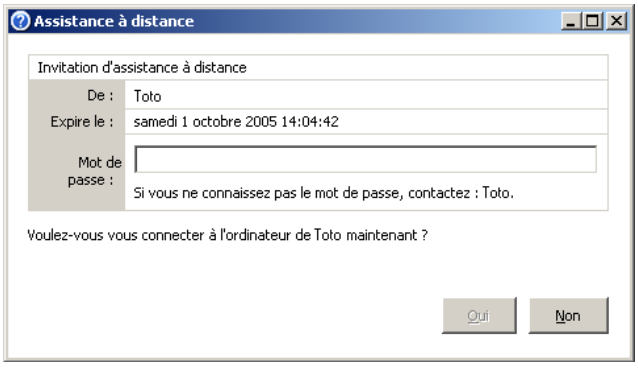
Il y a deux types d'assistance. L'assistance sollicitée : l'assisté envoie une invitation à laquelle le conseiller répond. L'assistance proposée : le conseiller prend directement contact avec l'assisté. Dans les deux cas, le conseiller démarre l'assistance que l'assisté doit toutefois valider.

Détail des étapes :

Méthode 1 : **Assistance sollicitée**

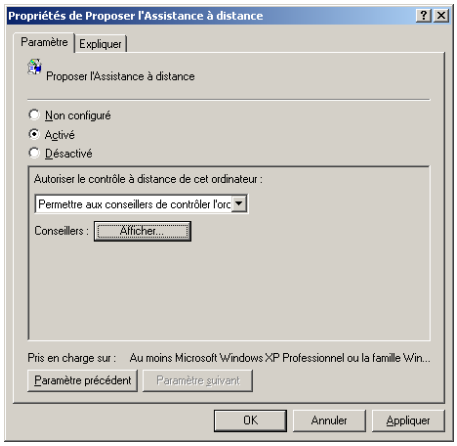


A partir du poste de l'assisté, dans le menu Démarrer, « Aide et support », cliquer sur « Invitez un ami à se connecter à votre ordinateur avec l'assistance à distance ». Cliquer ensuite sur « Inviter quelqu'un à vous aider ». Plusieurs méthodes sont proposées. On pourra par exemple cliquer sur « Enregistrer l'invitation dans un fichier ». Dans le panneau suivant on précisera la date d'expiration de l'invitation. On définira éventuellement un mot de passe, puis l'on sauvegardera l'invitation sous la forme d'un fichier d'extension .msrcincident. Ce fichier pourra être envoyé par courriel en pièce jointe au conseiller.



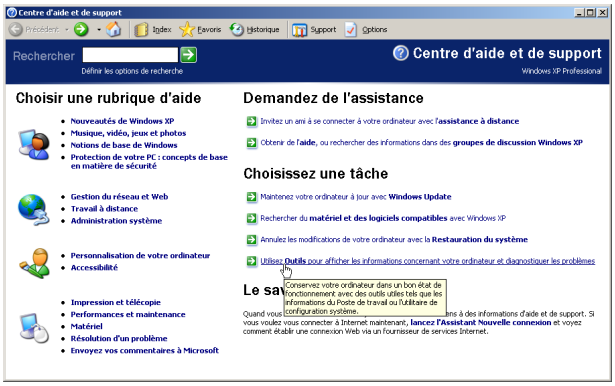
Lorsque le conseiller double-clique sur l'invitation, il est invité à s'identifier pour établir la connexion.

Méthode 2 : **Assistance proposée**

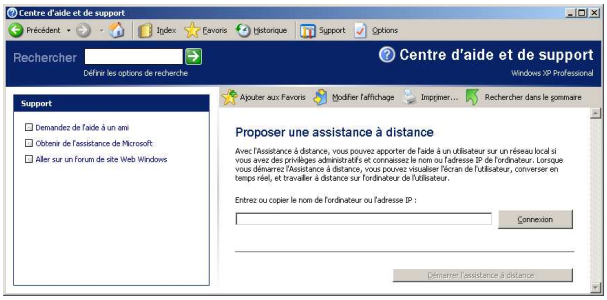


Pour commencer, sur le poste de l'assisté, lancer la console de « Stratégies de groupe locale » par gpedit.msc. Aller dans Configuration ordinateur, Modèles d'administration, Système, Assistance à distance. Activer le paramètre « Proposer l'assistance à distance ». Préciser également l'identifiant du conseiller.

Ensuite, à partir du poste du conseiller, dans le menu Démarrer, « Aide et support », cliquer sur « Utilisez Outils pour afficher les informations concernant votre ordinateur et diagnostiquer les problèmes ». Dans la liste d'outils affichée à gauche, sélectionner « Offrir une assistance à distance ».

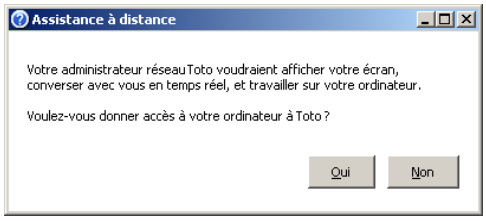


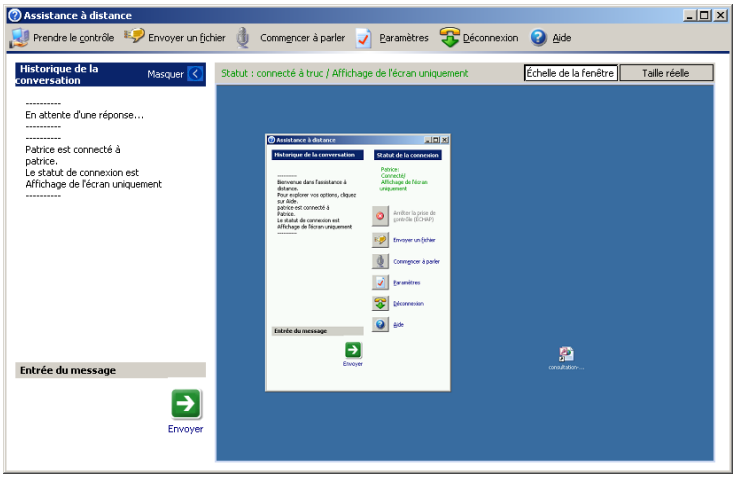
Le dialogue prend alors l'aspect ci-dessous. Le nom ou l'adresse IP du poste peuvent être saisis. Valider, puis sélectionner la session avec laquelle le conseiller doit interagir. Après validation, le bouton « Démarrer l'assistance à distance » devient actif.



La suite est identique dans les deux cas de figure :

L'assisté voit apparaître sur son bureau la fenêtre ci-contre qui lui demande s'il accepte ou non l'assistance du conseiller. En cliquant sur « Oui », l'assistance démarre.

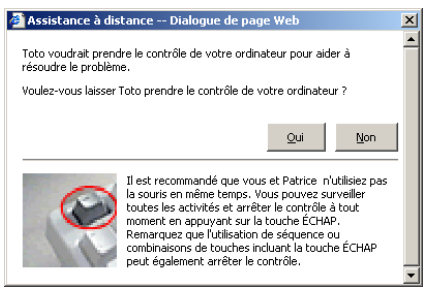




Le conseiller dispose d'une vue globale du bureau de l'assisté.

Pour prendre le contrôle du poste de l'assisté, il lui suffit de cliquer sur le bouton correspondant.

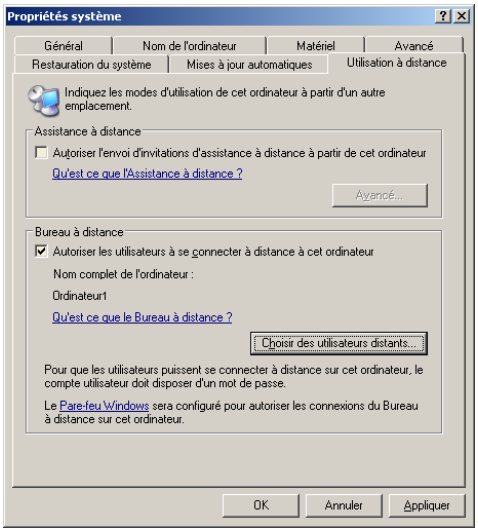
A cet instant, l'assisté doit accepter la demande :



Remarque : le conseiller doit utiliser sur son poste un compte identique (avec le même mot de passe) à l'un

des comptes du poste de l'assisté. En effet, le système ne propose à aucun moment au conseiller d'utiliser un autre compte.

Bureau à distance



Le bureau à distance (Terminal Service) permet d'ouvrir une session à distance sur un poste XP à partir d'un autre poste XP (ou à partir d'un poste sous Windows 9x, moyennant l'installation d'un logiciel client fourni sur le CD d'installation de Windows XP). Windows XP n'autorise l'ouverture que d'une seule session à un moment donné (alors que Windows 2003 Server en autorise plusieurs).

A la différence de l'assistance à distance, le bureau à distance ouvre une nouvelle session sans interaction.

Pour l'utiliser, commencer par autoriser sur le poste serveur (celui qui va être pris en main) la connexion à distance. Pour cela, cocher la case idoine de l'onglet « Utilisation à distance » du dialogue « Propriétés système ».

Sur le poste client, aller dans le menu Programmes, Accessoires, Communications et cliquer sur « Connexion bureau à distance ». Saisir les paramètres d'ouverture de session, puis cliquer sur « Connexion ». Voir la fin du chapitre intitulé « Réseau, partages » pour les subtilités de l'authentification.

Noter que si un utilisateur était déjà connecté sur le serveur, la connexion ne serait possible que dans deux cas : le client est un administrateur ou le client est précisément l'utilisateur actuellement connecté sur le serveur. Dans ce cas, la session sur le serveur serait verrouillée pour permettre à la session distante de s'ouvrir. Toutefois, si l'utilisateur du serveur décidait de le déverrouiller, la session distante du client serait close aussitôt.

Remarque : le « changement rapide d'utilisateurs » – disponible uniquement si le poste n'a pas joint un domaine – est en fait une ouverture de session au dessus d'une autre. Il s'agit de la même technologie que celle mise en œuvre dans le bureau à distance.

Sécurité, contrôle d'accès, privilèges

Le système a recours à divers types d'objets pour fonctionner. En voici une liste non exhaustive : les fenêtres, les fichiers, les imprimantes, les clés du registre, les emplacements mémoire, les processus, les fils d'exécution (thread), les sémaphores, les évènements, les minuteurs...

Windows XP étant un système intégrant la sécurité, les accès à certaines catégories d'objets sont limités. On parle dans ce cas d'objets sécurisés. Les fichiers, les clés du registre et les processus sont des exemples d'objets sécurisés. Les fenêtres, par contre, n'en sont pas (Sans doute pour des raisons de performance, Windows utilise un type d'objet appelé « Window Station » pour sécuriser un ensemble de fenêtres).

Les entités susceptibles de recevoir des autorisations ou des interdictions d'accéder à certains objets sont appelées **principaux de sécurité**. Ces principaux peuvent être des utilisateurs, des services (en fait des comptes d'utilisateurs adaptés à ces services), des groupes ou enfin des postes de travail.

SID

Chaque principal de sécurité est identifié par un **SID** (Security IDentifier) qui est et demeure unique aussi longtemps que le système d'exploitation existe. Si un principal est détruit, son SID ne sera pas réutilisé par un autre. Par ailleurs, deux postes distincts utilisent des SID différents. Chaque SID peut donc être considéré comme un identifiant unique au monde (voir toutefois plus loin la remarque concernant le clonage).

Quelques exemples de SID et les comptes associés :

```
S-1-1-0                       Tout le monde
S-1-3-0                       Créateur propriétaire
S-1-5                         Pseudo domaine NT (AUTORITE NT)
S-1-5-2                       AUTORITE NT\RESEAU
S-1-5-6                       AUTORITE NT\SERVICE
S-1-5-7                       AUTORITE NT\ANONYMOUS LOGON
S-1-5-11                      AUTORITE NT\Utilisateurs authentifiés
S-1-5-18                      AUTORITE NT\SYSTEM
S-1-5-19                      AUTORITE NT\SERVICE LOCAL
S-1-5-20                      AUTORITE NT\SERVICE RÉSEAU
S-1-5-21-xxxx-xxxx-xxxx       CE_POSTE
S-1-5-21-xxxx-xxxx-xxxx-500   CE_POSTE\Administrateur
S-1-5-21-xxxx-xxxx-xxxx-501   CE_POSTE\Invité
S-1-5-21-xxxx-xxxx-xxxx-1000  CE_POSTE\utilisateur1
S-1-5-32                      BUILTIN\BUILTIN
S-1-5-32-544                  BUILTIN\Administrateurs
S-1-5-32-545                  BUILTIN\Utilisateurs
S-1-5-32-546                  BUILTIN\Invités
S-1-5-32-547                  BUILTIN\Utilisateurs avec pouvoir
```

Dans ces exemples, « CE_POSTE » doit être remplacé par le nom NETBIOS effectif du poste.

Expérimentation avec l'utilitaire SID ;

Groupes de sécurité

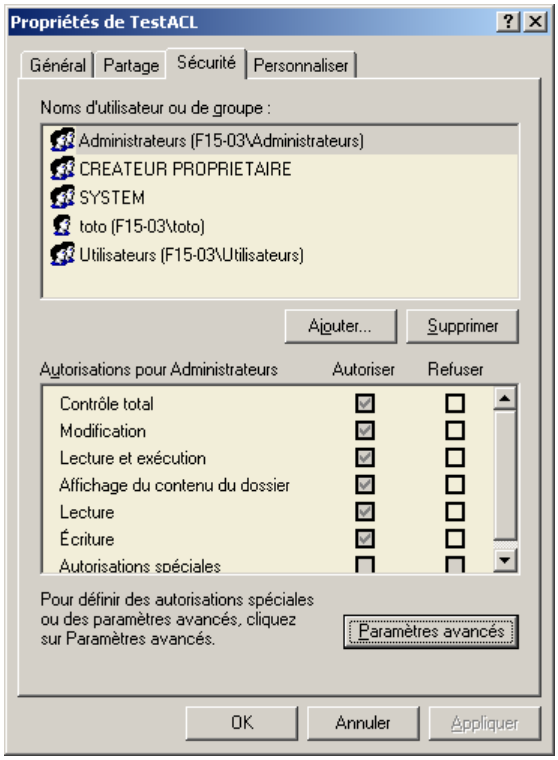
Les groupes de sécurité permettent à l'administrateur de gérer plus facilement les autorisations. Ils sont accessibles grâce à la console « Utilisateurs et groupes locaux » également utilisée pour la gestion des utilisateurs. Le système propose un ensemble de groupes prédéfinis qui devrait suffire dans la majorité des cas.

Il convient de distinguer le groupe « Tout le monde » dont tous les utilisateurs, sans exception, sont membres, du groupe « Utilisateurs authentifiés », qui correspond à tous les utilisateurs à l'exception de comptes « Invités » et « ANONYMOUS LOGON ». Le compte « Invité » est utilisé lors de la mise en œuvre des partages réseau. Le compte « ANONYMOUS LOGON » est utilisé par les service pour ouvrir des sessions nulles (lorsque les clients ne fournissent pas d'accréditations).

Listes de contrôles d'accès (ACL)

Les objets sont sécurisés grâce à des listes de contrôle d'accès (ACL). Pour certains types d'objets, une interface utilisateur est prévue pour en permettre le paramétrage. Pour d'autres, la configuration n'est possible que par programmation. Les objets admettant des ACL configurables par les administrateurs sont : les fichiers sur NTFS (pas sur FAT32), les clés du registre, les imprimantes et les partages.

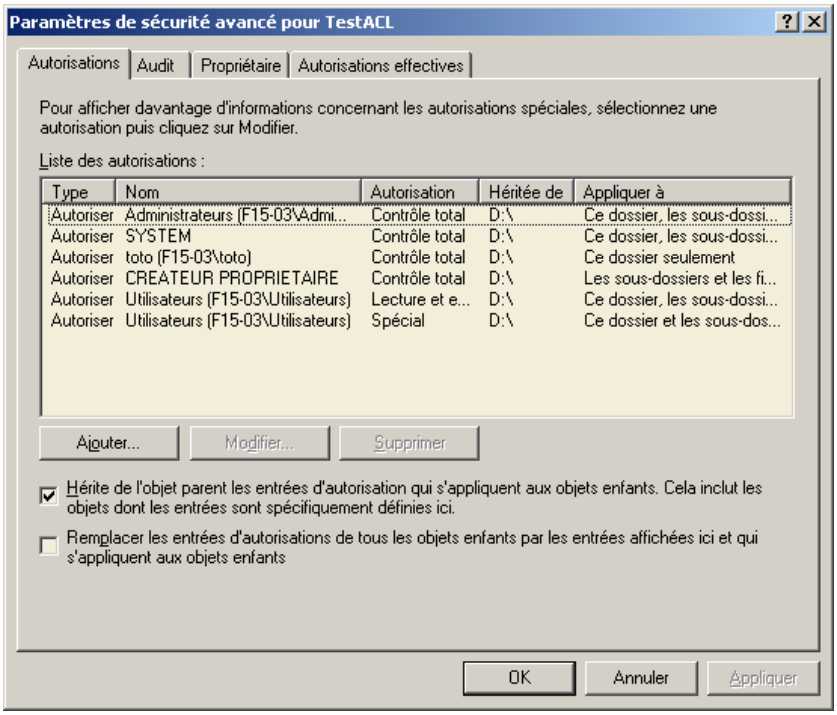
Dans le cas des fichiers, il faut commencer par désactiver le mode de partage simplifié (Options des dossiers, onglet Affichage, décocher la dernière case intitulée « Utiliser le partage de fichiers simple »).



L'onglet « Sécurité » de la boîte de dialogue « Propriétés » est représenté ci-contre.

On notera que les utilisateurs et les groupes n'y apparaissent qu'une fois et dans l'ordre alphabétique. Cette présentation censée simplifier la lecture de ces informations les rend en fait plus confuses.

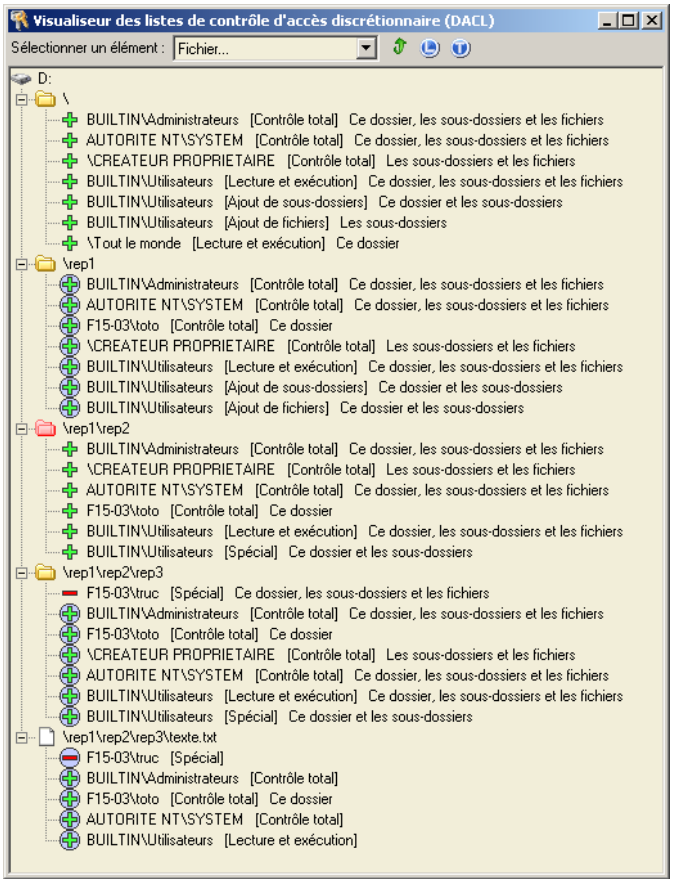
On lui préfèrera la boîte du dialogue avancé, plus complète et mieux adaptées à la compréhension des ACL et en particulier à ses mécanismes d'héritage.



Expérimentation : A la racine d'un disque, créer une arborescence de dossiers : D:\rep1\rep2\rep3 et créer dans rep3 un fichier texte vide. Modifier les ACL de rep2 en interrompant l'héritage à l'aide du dialogue « Paramètre de sécurité avancé ».

Au niveau de Rep3, ajouter une ACE négative (un refus) pour un autre utilisateur que l'utilisateur courant (truc, dans l'exemple).

Lancer ensuite l'utilitaire de visualisation des ACL (ListACL.EXE), sélectionner le fichier texte et analyser la structure obtenue. Dans le menu contextuel, décocher « Masquer les ACL héritées ». Constater que l'héritage est appliqué. Noter aussi l'apparition d'une ACE pour un utilisateur toto (F15-03 est le nom du poste) ; toto est en fait le propriétaire des répertoires ou des fichiers. L'ACE correspondante a été créée automatiquement lors de la création de l'objet en vertu de la présence de l'ACE « \CREATEUR PROPRIETAIRE ».



Les fichiers et les dossiers ne sont pas les seuls à bénéficier d'une protection par des ACL. Les clés du registre, les partages et les imprimantes en disposent également. L'utilitaire de visualisation des ACL permet de localiser rapidement les objets qui disposent d' ACE propres, c'est-à-dire, non héritées.

Mécanisme de détermination des droits

Pour déterminer si la réalisation d'une opération sur un objet par un processus est autorisée ou non, le système utilise les informations contenues dans le jeton du processus. Le jeton est le plus souvent créé à l'ouverture de la session d'un utilisateur. Il contient entre autre le SID de l'utilisateur, le SID de chacun des groupes dont il est membre et les privilèges (voir plus loin) dont il dispose.

Par exemple, lorsqu'un utilisateur essaie d'ouvrir un fichier texte à l'aide du bloc-notes, le système confronte le jeton présenté par le processus du bloc-notes et les opérations souhaitées (ici, ouvrir le fichier) aux ACL du fichier à ouvrir.

Dans l'ACL d'un objet, les ACE sont toujours placées dans l'ordre suivant : les ACE négatives (refus) non héritées puis les ACE positives (autorisations) non héritées. Viennent ensuite les ACE héritées de l'objet parent immédiat (dossier, par exemple), les négatives en premier, les positives ensuite. On poursuit avec les ACE héritées des objets parents en remontant jusqu'à la racine (sauf si le mécanisme d'héritage est interrompu au niveau de l'un des parents, auquel cas, on s'arrête à son niveau).

Pour déterminer si les autorisations sont accordées ou non, le système passe en revue les ACE de l'ACL de l'objet comme suit :

Il commence par analyser les ACE négatives propres à l'objet lui-même. Si l'une de ces ACE refuse au processus l'une des opérations demandées (accès en lecture, en écriture…), ce dernier est éconduit. Sinon, le système passe en revue les ACE positives propres. Si au terme de ces ACE toutes les opérations demandées par le processus sont autorisées, le système lui donne son feu vert.

Sinon, le système poursuit en parcourant les ACE négatives, puis positives héritées de l'objet parent immédiat, puis celles héritées du parent de cet objet et ainsi de suite jusqu'à la dernière ACE de l'ACL de l'objet. Si au terme de cette énumération la totalité des opérations demandées n'est pas accordée, le processus est éconduit.

Remarque : l'héritage est une technologie destinée à faciliter le travail des administrateurs. Il n'est, en aucun cas, un moyen d'économiser l'espace disque occupé par les ACE : chaque objet possède en effet une copie de chacune des ACE héritées des objets parents !

cacls et xcacls

Les utilitaires cacls ainsi que xcacls (ce dernier doit être installé à la main) qui permettent de modifier les ACL en ligne de commande posent problème lorsqu'ils sont utilisés avec des dossiers. En effet, ils sont basés sur des appels d'API système qui ne prennent pas en charge l'héritage (cf le livre de K.Brown sur la sécurité, cité en annexe).

Ainsi la commande suivante crée-t-elle une ACE supplémentaire uniquement au niveau du dossier C:\rep1 :

```
cacls C:\rep1 /E /G "utilisateurs avec pouvoirs:R"
```

Cette commande ajoute précisément à l'ACL du dossier C:\rep1, les droits en lecture pour le groupe « Utilisateurs avec pouvoir ». Elle correspond à l'option « Appliquer à ce dossier seulement » de la boîte de dialogue de sécurité. Les sous-dossiers et fichiers de C:\rep1 ne seront pas concernés.

La suivante, qui semblerait à première vue mieux adaptée à la mise en place d'ACE héritées, est celle qui pose problème :

```
cacls C:\rep1 /T /E /G "utilisateurs avec pouvoirs:R"
```

Le paramètre /T indique que l'ACE doit être ajoutée non seulement à l'ACL du dossier C:\rep1, mais également aux ACL de ses sous-dossiers et de ses fichiers. Le problème est que les ACE ainsi créées au niveau de ces sous-dossiers et fichiers sont des ACE propres et non pas des ACE héritées. Par conséquent la structure obtenue n'est plus cohérente avec celle que maintient la boîte de dialogue de sécurité, ce qui peut conduire à des problèmes (c'est le « chaos » décrit par K.Brown).

En conclusion :

- Utiliser cacls sur des fichiers ne pose pas de problème ;
- Utiliser cacls sur des dossiers est fortement déconseillé ; préférer la boîte de dialogue de sécurité à la commande cacls. Utiliser cacls sur des dossiers système tels que C:\Windows, C:\Program Files ou C:\Documents and Settings peut avoir des conséquences catastrophiques en terme de sécurité.

Copie/déplacement de fichier

Lors du déplacement d'un fichier à l'aide de l'explorateur (en restant sur un même disque formaté NTFS), les ACE propres sont conservées. Lors de la copie d'un fichier, le fichier créé n'a pas d'ACE propres.

Donc copier un fichier puis supprimer le fichier source n'a pas le même effet que déplacer le fichier (toujours à l'aide de l'explorateur et en restant sur le même disque).

Clonage et SID

Comme indiqué plus haut, les SID des postes sont censés être uniques au monde. A la suite d'un clonage, tous les postes se retrouvent avec un même SID. Divers utilitaires existent pour y remédier : sysprep de Microsoft (qui se met en place avant le clonage et remplit d'autres fonctions), NewSID de SysInternals qui s'applique après le clonage…

L'opération de changement de SID étant délicate et consommatrice de temps, la question de sa nécessité se pose.

Le seul problème répertorié et incontestable qui peut résulter de la non unicité des SID des postes est l'utilisation d'un support amovible formaté en NTFS. Mais le risque est assez faible car d'une part ces supports amovibles sont rarement formatés en NTFS et d'autre part ils suivent souvent physiquement leurs propriétaires (clés USB, par exemple).

Ce problème de SID n'est pas lié à cet autre problème qui apparaît également lors du clonage. Lorsque l'on clone un poste joint à un domaine, les postes clonés refusent de joindre ce même domaine. Pour éviter ce problème précis, il suffit de disjoindre le poste source du domaine avant le clonage, puis d'effectuer la jonction des postes après.

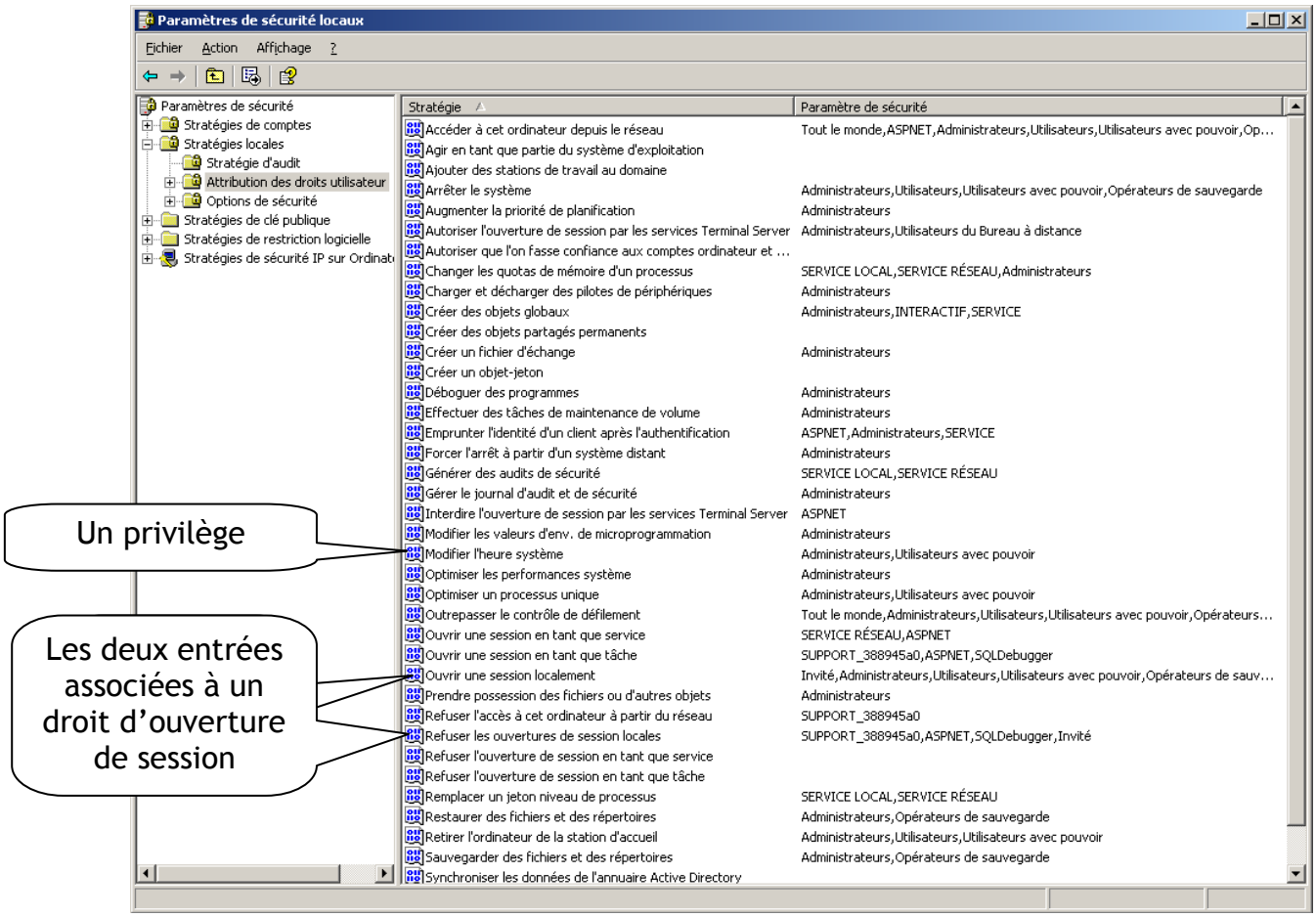
Droits et privilèges des utilisateurs

Certaines autorisations accordées ou refusées aux utilisateurs ne sont pas liées à un objet en particulier. Ces autorisations sont regroupées en droits d'ouverture de session et en privilèges.

Les **droits d'ouverture de session** vont par deux et concernent les types d'ouverture de session. Un utilisateur bénéficie d'un droit lorsqu'il est listé dans le droit « positif », comme par exemple « Ouvrir une session localement », mais pas dans le droit « négatif » correspondant, comme « Refuser les ouvertures de sessions locales ».

Les **privilèges** portent sur des opérations particulières telles que l'arrêt du système, la modification de l'heure, l'appropriation d'objets… Seuls les utilisateurs ou groupes listés bénéficient de ces autorisations.

Droits et privilèges apparaissent – mélangés – dans la console « Paramètres de sécurité locaux », sous l'intitulé « Attributions des droits utilisateur », à partir duquel ils peuvent être configurés.



Le terme **droits utilisateur** est utilisé pour désigner aussi bien les privilèges que les droits d'utilisation.

Applications, processus, services

Processus, jeton

Lorsqu'un utilisateur lance une application, le système crée un **processus**. Un processus est constitué, entre autre, des éléments suivants :

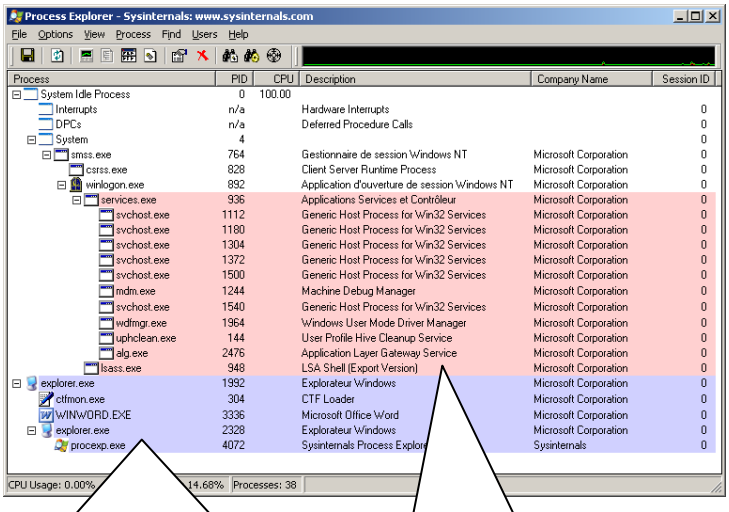
- un espace mémoire réservé pour charger le code exécutable et pour stocker les données ;
- un PID (identificateur numérique du processus) ;
- une liste d'objets ;
- un premier fil d'exécution (thread) ;
- un jeton d'accès.

Le **jeton d'accès** est utilisé pour concentrer les accréditations d'un utilisateur. Chaque jeton comporte, entre autre :

- le SID d'un principal de sécurité (qui identifie l'utilisateur) ;
- le SID de chacun des groupes dont le principal est membre.
- la liste des privilèges du principal.

Le jeton définit un **contexte de sécurité**. Lorsqu'un utilisateur ouvre une session locale, l'application système winlogon lance userinit, qui lance elle-même l'Explorateur. Cette première instance de l'explorateur apparaît sous la forme particulière du bureau. Les accréditations de l'utilisateur sont concentrées dans un jeton associé au processus de l'explorateur. Par la suite, chaque fois que l'utilisateur lance une application, en cliquant sur un raccourci du menu Démarrer, par exemple, le processus de l'Explorateur transmet une copie de son jeton au processus de l'application lancée. Ce jeton est utilisé à chaque fois qu'une autorisation est nécessaire pour réaliser une opération sur un objet sécurisé (confrontation aux ACL) ou pour réaliser certaines actions système (vérification des droits et privilèges). Toutes ces applications s'exécutent dans le même contexte de sécurité.

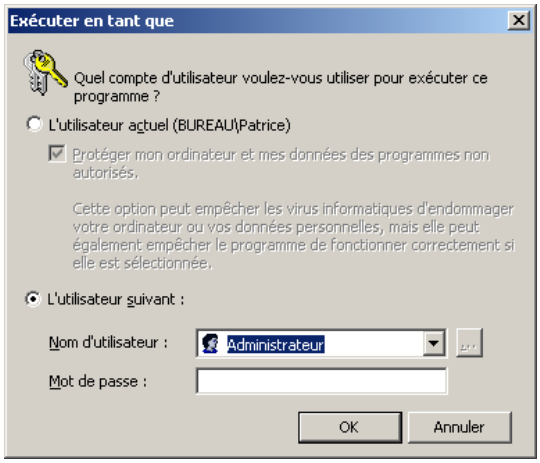
Expérimentation : visualisation des processus courants avec l'utilitaire « Process Explorer » fourni par Sysinternals. En double-cliquant sur l'entrée d'un processus, on accèdera à une boîte de dialogue dont l'onglet « Sécurité » permet de visualiser le contenu du jeton d'accès. On notera que l'Explorateur apparaît complètement à gauche. Ceci résulte du fait que son processus parent, userinit, n'existe plus (Userinit ne sert qu'à préparer et à lancer le shell, c'est-à-dire le bureau).



Par défaut, toutes les fenêtres de l'Explorateur s'exécutent dans le même processus. Pour utiliser un processus par fenêtre, cocher la case « Ouvrir les fenêtres des dossiers dans un processus différent » sous l'onglet Affichage de l'applette « Options des dossiers ». Il en résultera une ligne supplémentaire dans Process Explorer, comme dans l'exemple ci-dessus.

Exécuter en tant que…

Il est possible de lancer un processus dans un contexte de sécurité différent (donc disposant d'un jeton différent) de celui dont dispose l'Explorateur initial (le bureau). Pour cela, cliquer droit sur le raccourci d'un exécutable et sélectionner l'item « Exécuter en tant que… ». Une fenêtre analogue à la suivante apparaît :



Saisir un identifiant et un mot de passe, puis valider.

Par défaut les comptes dont le mot de passe est vide ne peuvent être utilisés ici. Voir la fin du chapitre intitulé « Réseau, partages » pour plus de détails sur ce point.

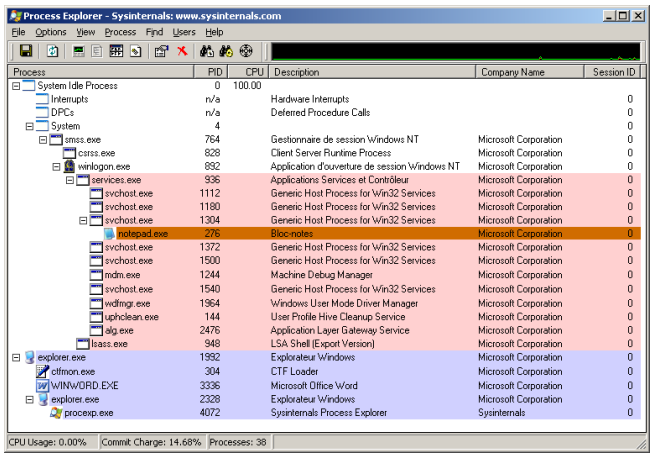
La commande **runas** joue, en ligne de commande, le même rôle que le dialogue précédent. Par exemple, pour lancer une invite de commande dans le contexte de sécurité de l'Administrateur, si la session actuellement ouverte est celle d'un utilisateur ordinaire, saisir ceci :

```
runas  /noprofile  /user:administrateur  cmd
```

Le mot de passe sera alors demandé. S'il est reconnu, la fenêtre de l'invite de commande sera affichée. Toutes les opérations réalisées dans cette console le seront avec un jeton correspondant aux accréditations de l'administrateur. La commande **whoami** permet d'afficher, en ligne de commande, le nom du compte actuellement utilisé. L'exécutable whoami n'est pas installé par défaut. Il fait partie d'un ensemble d'utilitaires téléchargeables sur le site de Microsoft.

Le paramètre /noprofile permet de ne pas charger la ruche du profil de l'utilisateur au démarrage du processus.

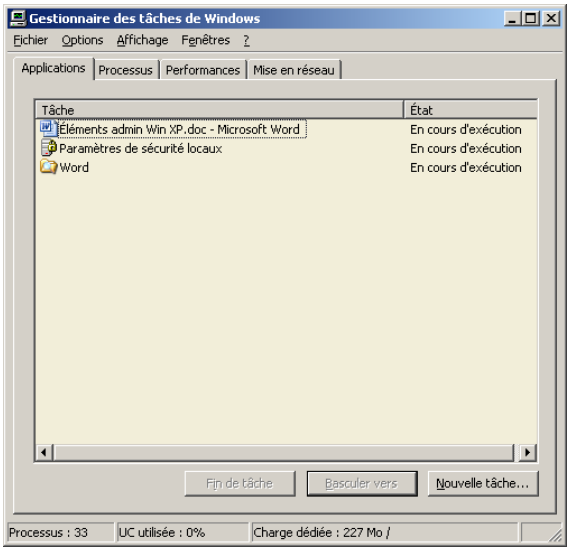
Expérimentation : lancer le Bloc-notes (notepad.exe) dans le contexte de sécurité d'un utilisateur différent de l'utilisateur courant. On conservera ici le profil. Lancer l'Editeur du registre et constater qu'un second profil est bien chargé sous la clé HKEY_USERS.



Lancer ensuite Process Explorer. Constater que le Bloc-notes ne s'exécute pas dans le contexte de sécurité de l'utilisateur courant. Double-cliquer sur la ligne correspondante et sélectionner l'onglet Sécurité pour cela. Le Bloc-notes est lancé par l'un des processus svchost.exe. Double-cliquer

sur sa ligne et sélectionner l'onglet Services pour afficher la liste des services que gère ce processus. Dans cette liste, on notera le service seclogon (Connexion secondaire) ; c'est celui-ci qui s'est chargé de lancer le Bloc-notes dans un contexte de sécurité différent du contexte principal (et différent également du contexte de sécurité dans lequel s'exécute svchost : « Autorité NT\SYSTEM »).

Gestion des tâches



La séquence de touches CTRL+ALT+SUPPR, fait apparaître la fenêtre « Sécurité de Windows » ou bien la fenêtre du « Gestionnaire des tâches », suivant le type d'ouverture de session actuellement sélectionné. Par contre, la séquence MAJ+CTRL+ECHAP fait toujours surgir le gestionnaire des tâches.

Le gestionnaire des tâches est essentiellement utilisé pour terminer un processus qui ne répond plus.

Le basculement des tâches s'effectue au clavier à l'aide de la combinaison ALT+TAB.

Démarrages automatiques

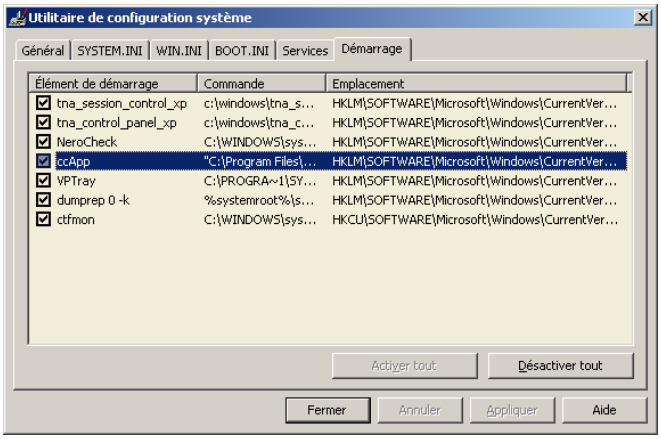
Il existe de nombreuses façons de démarrer automatiquement des applications.

A l'aide des clés du registre : HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run et HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce, à l'aide du dossier Démarrage de l'utilisateur ainsi que celui du profil ALL USERS, à l'aide des scripts de la stratégie de groupe local.

Les applications qui figurent sous la clé Run sont exécutées à chaque ouverture de session, dans le contexte de sécurité de l'utilisateur qui ouvre la session.

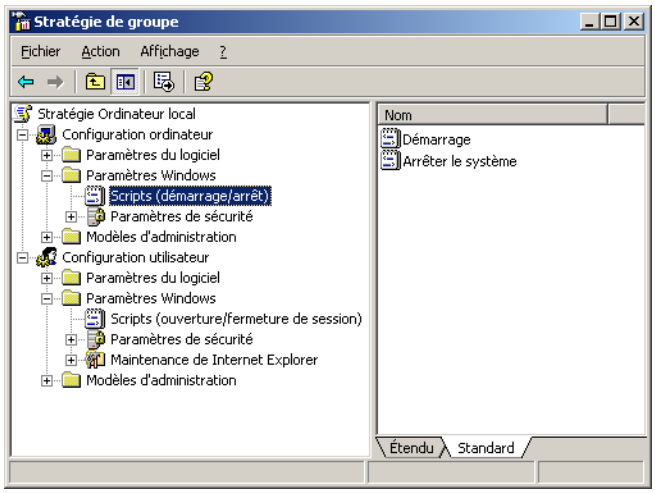
Les applications qui figurent sous la clé RunOnce ne sont exécutées qu'une seule fois et uniquement dans le contexte de sécurité d'un utilisateur membre du groupe « Administrateurs ». Si l'utilisateur n'est pas un membre de ce groupe, l'exécution des applications situées sous la clé RunOnce est différée à la prochaine session.

L'onglet « Démarrage » de l'utilitaire de configuration du système (msconfig.exe) propose un moyen simple de désactiver certaines applications de la clé Run, sans les effacer.

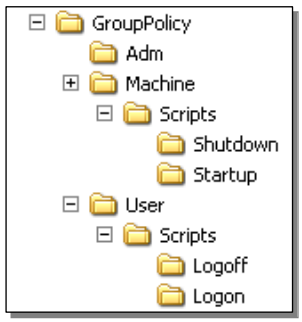


Scripts de la stratégie de groupe locale

La console « Stratégie de groupe » que l'on peut lancer par gpedit.msc, permet d'accéder à la configuration de scripts. Ces scripts peuvent être lancés, au choix, à chaque démarrage du système, à chaque arrêt du système, à chaque ouverture de session ou à chaque clôture de session. Dans les deux premiers cas, les scripts sont exécutés dans le contexte de sécurité de l'utilisateur « Autorité NT\SYSTEM ». Dans les deux autres cas, ils sont exécutés dans le contexte de sécurité de l'utilisateur qui ouvre ou ferme la session.

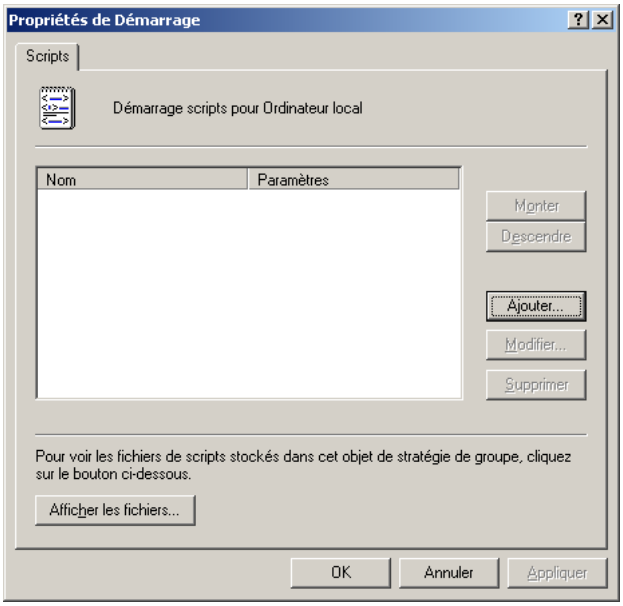


Les scripts sont situés dans des sous-dossiers du dossier suivant : C:\WINDOWS\System32\GroupPolicy qui est créé lors du premier lancement de la console « Stratégie de groupe ». Le simple fait de sélectionner « Scripts (démarrage/arrêt) » dans l'arborescence de la console crée les dossiers Scripts, Shutdown et Startup. Même chose avec « Scripts (ouverture/fermeture de session) » qui crée, lorsqu'on le sélectionne, les dossiers Scripts, Logoff et Logon. Ces quelques clics permettent d'obtenir la structure ci-contre :

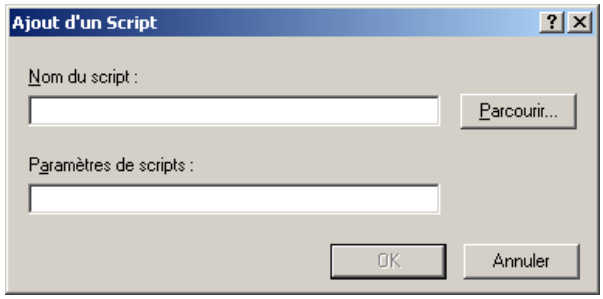


Les dossiers Startup (démarrage), Shutdown (arrêt), Logon (ouverture de session) et Logoff (déconnexion) sont prévus pour accueillir les scripts correspondants. Il n'est pas obligatoire de les placer dans ces dossiers, mais c'est conseillé.

Une fois les scripts créés et stockés dans les bons dossiers, il faut les enregistrer au près du système. Pour cela, dans la console, double-cliquer sur le type de script voulu (par exemple : Démarrage).



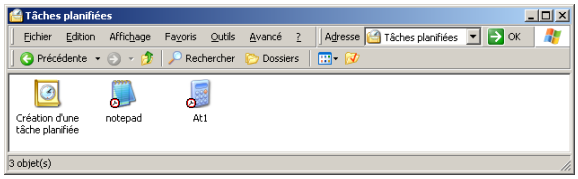
Dans la fenêtre qui apparaît, cliquer sur le bouton Ajouter. Dans le dialogue qui apparaît, saisir le chemin complet du script et indiquer les éventuels paramètres.



Remarque : Cette opération a pour effet de créer non seulement un fichier scripts.ini dans le dossier Scripts, mais également quelques clés et valeurs dans le registre. Pour cette raison, l'édition manuelle du fichier scripts.ini est à éviter.

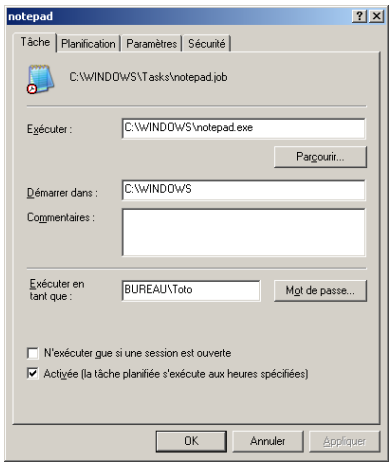
Planification des tâches

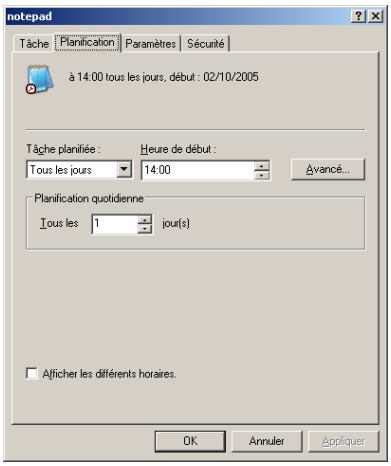
L'applette « Tâches planifiées » du panneau de configuration permet la programmation du démarrage d'une application à une date précise, sur une base régulière ou à chaque démarrage du système ou encore à chaque ouverture de session. Il est même possible de préciser le contexte de sécurité voulu, en précisant l'identifiant et le mot de passe d'un compte. La planification est intéressante pour des opérations d'administration : réalisations automatiques de sauvegardes, par exemple.



Dans l'exemple ci-contre, le Bloc-notes est démarré tous les jours à 14h, dans le contexte de sécurité de l'utilisateur Toto. Les tâches planifiées sont stockées sous la forme de fichiers .job dans le dossier C:\WINDOWS\Tasks.

Ceci explique qu'elles possèdent des ACL, comme en témoigne l'onglet Sécurité de la boîte de dialogue.





La planification des tâches en ligne de commande peut être réalisée à l'aide de la commande **at**.

La commande at saisie seule affiche la liste des tâches planifiées par at (mais pas celles planifiées par l'applette).

Les tâches planifiées à l'aide de at apparaissent dans l'applette avec un nom de la forme Atxxx, où xxx est un numéro.

Une nouvelle commande, **schtasks,** reprend et complète la commande at. Elle est le pendant en ligne de commande de l'applette « Tâches planifiées ».

```
schtasks             ; affiche la liste des tâches planifiées

schtasks /?          ; affiche l'aide de base

schtasks /create /?  ; affiche l'aide du paramètre create
```

L'exemple suivant permet de programmer l'arrêt du poste local tous les jours à 20h :

```
schtasks /create /ru SYSTEM /sc DAILY /st 20:00:00 …
         /tn "Arret du poste" /tr "shutdown -s"
```

Le paramètre /ru SYSTEM précise que le contexte de sécurité utilisé correspond au compte « Autorité NT\SYSTEM ». Pour plus de détails sur la commande shutdown, entrer : shutdown /?

Autorun étendu

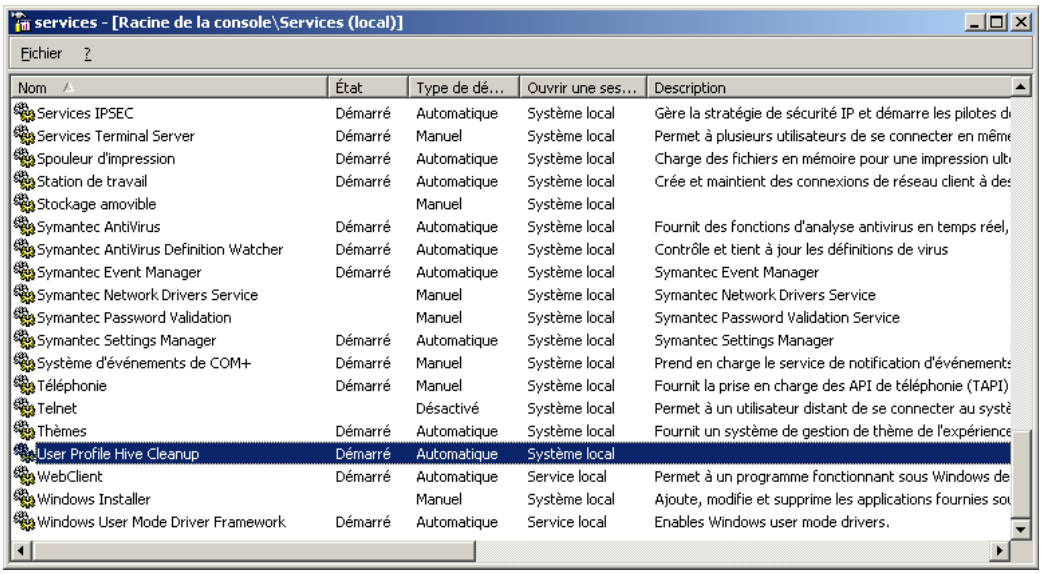
La lecture automatique à l'insertion des média (cédérom, clés USB…) peut être désactivée complètement pour tous les utilisateurs. Pour cela, définir la valeur suivante du registre :

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer]
"NoDriveTypeAutoRun"=dword:ff
```

La modification ne sera prise en compte qu'à la prochaine ouverture de session.

Services

Les services sont des applications qui s'exécutent en tâche de fond dans des contextes de sécurité spécifiques. On peut les configurer à l'aide de la console services.msc.



Plusieurs services peuvent, pour des questions d'optimisation des ressources, se partager un même processus. Par exemple, les services Accès à distance au registre, Aide et support, Connexion réseau, Téléphonie, Terminal Server (Bureau à distance) et d'autres se partagent le processus Svchost.

Il est possible de démarrer un service à l'aide de la commande net (à condition de disposer de droits suffisants).

```
net start xxx  permet de lancer le service xxx,

net stop xxx   permet de l'arrêter.

net start      permet d'afficher la liste des services en cours
```

Par exemple, en cas de bourrage de papier dans une imprimante, un administrateur peut arrêter temporairement le spooler, régler le problème, puis relancer le spooler à l'aide d'un simple fichier .bat :

```
net stop spooler
pause
net start spooler
```

En cas de cafouillage total, un administrateur peut vider la file d'attente du spooler d'impression :

```
net stop spooler
del /q %systemroot%\system32\spool\printers\*.*
del /q %systemroot%\system32\spool\printers\*.*
net start spooler
```

(Les lignes 2 et 3 sont identiques. Dans certains cas, la première seule ne suffit pas.)

Enfin, en plaçant ces quatre lignes dans un fichier clearspooler.bat, les deux commandes suivantes permettent de programmer un nettoyage du spooler à chaque démarrage et chaque ouverture de session :

```
schtasks /create /ru SYSTEM /sc ONSTART …
  /tn "Nettoyage du spouleur au demarrage" …
  /tr "c:\windows\clearspooler.bat"
schtasks /create /ru SYSTEM /sc ONLOGON …
  /tn "Nettoyage du spouleur a chaque ouverture de session" …
  /tr "c:\windows\clearspooler.bat"
```

(Il n'est pas possible de planifier une tâche en fin de session. Et c'est bien dommage !)

La planification des deux tâches précédentes peut bien sûr être réalisée directement à l'aide de l'applette « Tâches planifiées ».

Réseau, partages

La commande netsh

Cette commande permet de changer rapidement les paramètres réseau d'un poste. Elle s'avère très pratique sur un portable amené à se raccorder à divers réseaux.

Créer un fichier « local.bat » contenant la ligne suivante :

```
netsh  -f  local.txt
```

Placer dans le même dossier un fichier local.txt contenant une version adaptée de :

```
# ----------------------------------
# Configuration IP de l'interface
# ----------------------------------
pushd interface ip

set address name="Connexion au reseau local" source=static …
                              addr=10.127.1.10 mask=255.255.255.0
set address name="Connexion au reseau local" gateway=10.127.1.254 …
                              gwmetric=0
set dns name="Connexion au reseau local" source=static …
                              addr=10.127.1.254 register=PRIMARY
set wins name="Connexion au reseau local" source=static addr=none

popd
```

Créer autant de couples de fichiers que de réseaux auxquels le poste est susceptible de se raccorder.

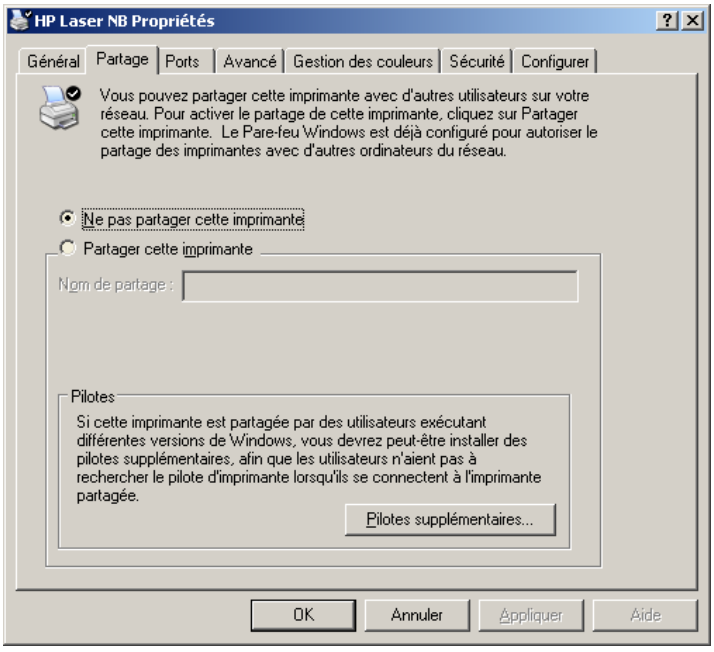
Partages

Le système propose un mode d'affichage simplifié des partages qui est activé par défaut. Pour basculer vers le mode complet, aller dans « Options des dossiers », onglet « Affichage » et décocher la dernière case intitulée « Utiliser le partage de fichiers simple ».

On trouvera en annexes un rappel des règles de construction des noms de partage.

Un caractère « $ » à la fin d'un nom de partage permet de rendre la ressources correspondante non listable ; elle n'apparaît pas dans l'explorateur. Elle reste cependant accessible par la saisie directe de son nom (le caractère « $ » inclus).

Le partage d'imprimantes possède une fonctionnalité intéressante : la possibilité de fournir plusieurs types de pilotes (pour Windows XP, pour Windows 9x…). Lorsque les clients se connectent et installent l'imprimante, ils récupèrent automatiquement le pilote auprès du poste qui réalise le partage. On notera que le système utilise le partage administratif PRINT$ pour mettre cette technique en œuvre.



Partages administratifs

Le système crée à chaque démarrage des partages dits administratifs. Il s'agit de ADMIN$, IPC$, PRINT$, C$, D$... La valeur du registre suivante permet de désactiver leur création automatique (sauf IPC$ et PRINT$) :

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters]
"AutoShareWks"=dword:0
```

Les ACL des partages administratifs ne sont pas modifiables. Elles correspondent à une seule ACE : accès complet pour le groupe « Administrateurs » (et donc, par ricochet, également pour les membres du groupe « Administrateurs du domaine »).

ACL des partages

Les partages (de dossiers) disposent d'ACL. Celles-ci sont surtout intéressantes lors du partage de dossiers situés sur une partition FAT32. Pour les partages de dossiers situés sur partition NTFS, les ACL des partages font double emploi avec celles des dossiers.

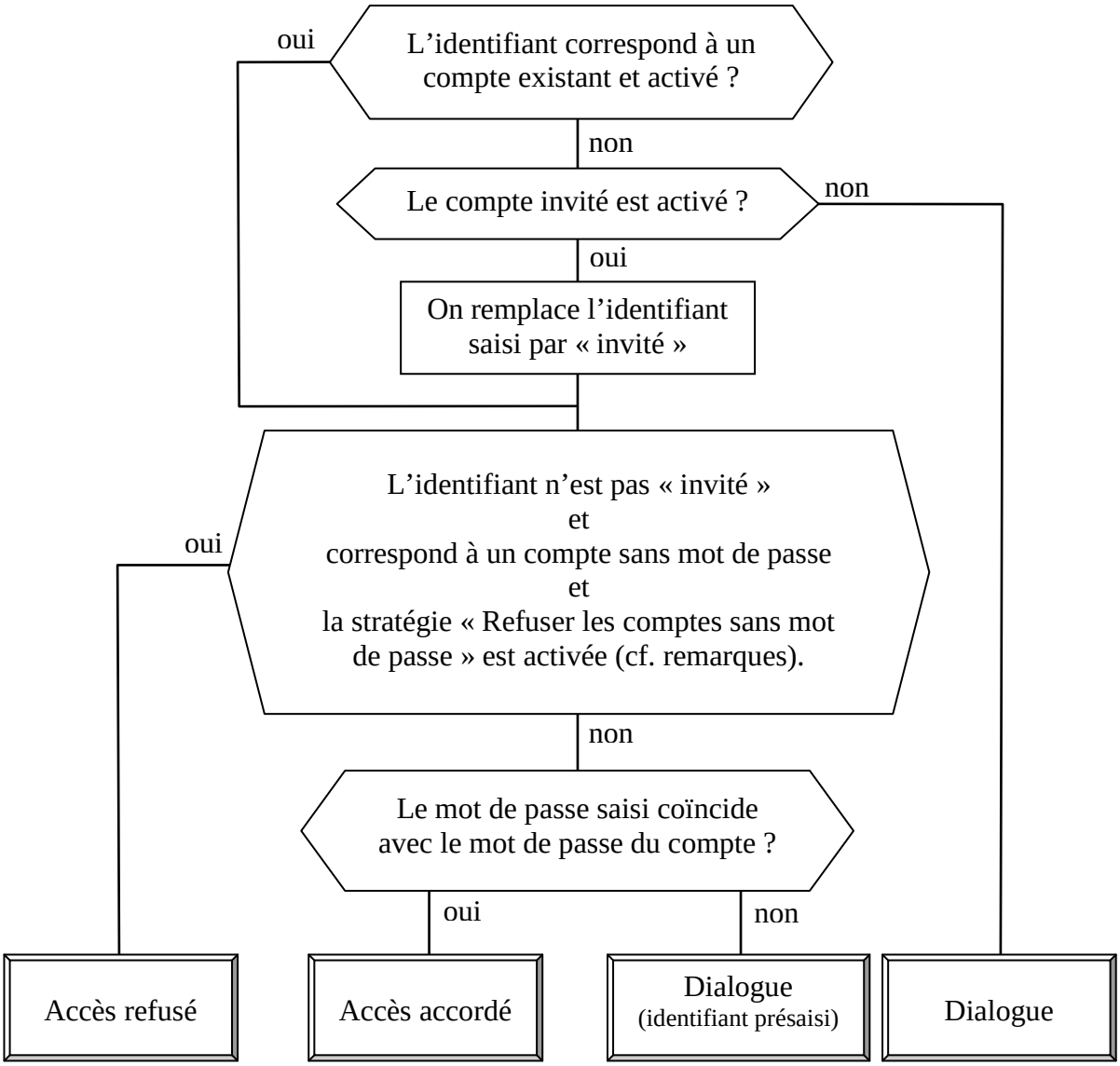
Authentification en réseau poste à poste

Lors de la connexion à une ressource partagée en réseau, si l'utilisateur n'utilise pas un compte du domaine, l'authentification est effectuée directement par le poste qui propose le partage, que nous appellerons dans la suite le serveur. Le protocole NTLM, du type défi/réponse, est mis en œuvre. Ce principe est également utilisé avec le Bureau à distance, la commande RunAs…

L'authentification se déroule comme suit :

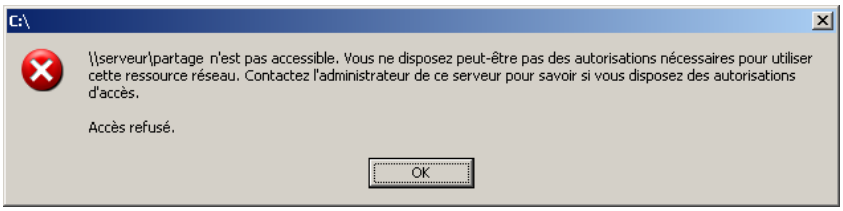
Le client commence par envoyer au serveur l'identifiant et le mot de passe (haché) de l'utilisateur actuellement connecté (ceux qu'il a saisis en ouvrant sa session, ou ceux qu'il a enregistrés lors d'un précédent accès au partage).

Ensuite, le serveur analyse le couple identifiant/mot de passe comme indiqué dans l'organigramme reconstitué suivant :



Le dialogue d'identification est représenté ci-contre. L'identifiant (Nom d'utilisateur) peut suivant le cas être présaisi ou non.

Lorsque l'accès à une ressource est refusé, le dialogue suivant est affiché :



Remarques :

- Invité n'est utilisé automatiquement que s'il n'existe pas sur le serveur de compte du même nom que celui du client qui essaye de se connecter. Si un tel compte existe avec un mot de passe différent du mot de passe local, et si l'utilisateur ne connaît pas ce mot de passe, celui-ci pourra utiliser le compte Invité en saisissant explicitement « invité » dans la boîte de dialogue.
- Si le compte Invité possède un mot de passe, il faudra saisir explicitement « invité » ainsi que le mot de passe correspondant dans la boîte de dialogue.
- Au niveau de la console « Paramètres de sécurité locaux » (secpol.msc), Stratégies locales, Options de sécurité, la stratégie intitulée « Comptes : restreindre l'utilisation de mots de passe vierge par le compte local à l'ouverture de session console » correspond au paramètre qui permet d'autoriser ou non l'utilisation des comptes sans mots de passe lors de l'authentification. Par défaut, cette stratégie est activée ; il est préférable de la laisser dans cet état pour des raisons de sécurité.
- Si des ACL existent au niveau du partage, elles sont passées en revue après l'authentification. Ce n'est qu'après cette deuxième étape que l'accès sera finalement accordé ou refusé (en lecture, en écriture…).

Annexes

Ces annexes regroupent, par commodité, des informations techniques utiles mais peu connues ou enfouies dans des documentations techniques rarement disponibles aux moments opportuns.

Règle pratique de construction des noms

La construction des noms de partages, des noms NETBIOS et des noms Internet suit des règles différentes qui sont rappelées plus bas. Pour en simplifier la mémorisation et pour éviter de mauvaises surprises par la suite, on pourra appliquer les règles plus restrictives suivantes :

Caractères autorisés	
Identifiants, noms de partage :	**a à z A à Z 0 à 9 - _**
Noms NETBIOS, nom Internet :	**a à z A à Z 0 à 9 -**
Longueur maximale	
Identifiants :	20 caractères
Noms de partage :	12 caractères
Noms NETBIOS, nom Internet :	15 caractères

Remarques :

- Les limitations indiquées ici prennent en compte les anciens systèmes Windows 9x.
- La casse n'est prise en compte dans aucun des cas ;
- Le tiret autorisé pour les noms NETBIOS et Internet correspond au signe moins. Le tiret bas « _ » n'est pas autorisé dans les noms Internet.

Règle de construction des identifiants

Les identifiants sont les chaînes saisies par les utilisateurs dans la boîte d'ouverture de session.

Ces noms sont limités à 20 caractères choisis parmi les suivants :

Caractères interdits : \ | / **[ ]** < > , : ; ? + = * " @

Caractères autorisés : a priori, tous les autres.

Règle de construction des noms des partages

Partage créé sous XP : 80 caractères au maximum

Partage créé sous 98 : 12 caractères au maximum

Accès à un partage à partir de XP : OK jusqu'à 80 caractères

Accès à un partage à partir de 98 : OK jusqu'à 21 caractères (mais visibles uniquement si ≤12)

Caractères autorisés : **a à z A à Z 0 à 9 - _** (liste exacte non connue)

Règle de construction des noms NETBIOS

Windows utilise des noms NETBIOS pour désigner les postes de travail, les groupes de travail et les domaines.

Ces noms sont limités à 15 caractères choisis parmi les suivants :

a à z A à Z 0 à 9 - _ ^ ( ) { } . ! ’ # % @ $ &

Voir toutefois la remarque au paragraphe suivant.

L’étendue NETBIOS est limitée à 240 caractères choisis comme ci-dessus.
(La règle est en fait 256 caractères en tout pour le nom et l’étendue. Le nom faisant 15+1 caractères au maximum ; le seizième caractère étant utilisé pour coder le type de ressource.)

Règle de construction des noms Internet

Windows utilise un nom Internet pour désigner les postes de travail (leurs noms d’hôte).

Ces noms sont limités à 63 caractères choisis parmi les suivants :

a à z A à Z 0 à 9 -

Remarque : Windows XP modifie automatiquement le nom NETBIOS d’un poste lorsque l’on change le nom Internet de ce poste ; le nom NETBIOS est alors constitué des 15 premiers caractères du nom Internet. Il semble donc raisonnable d’appliquer les règles plus restrictives des noms Internet dans les deux cas.

Références

Brown, K. 2004. **The .NET Developer’s Guide to Windows Security**, Addison-Wesley

Ouvrage en anglais, très complet et structuré sous forme de questions réponses pour un accès rapide à l’essentiel. Malgré son titre, il n’est pas nécessaire d’être développeur pour profiter de son contenu. Par ailleurs, l’intégralité du livre est consultable en ligne à l’adresse suivante :

http://pluralsight.com/wiki/default.aspx/Keith.GuideBook.HomePage

Russinovitch, M., Solomon, D. 2005. **Windows Internals**, Microsoft Press

Ouvrage en anglais, très dense et très complet (900 pages). Il aborde quasiment tous les aspects des systèmes Windows XP, 2000 et 2003. Bien qu’assez technique, il contient une multitude d’encadrés ainsi que des expériences à mener soi-même pour mieux assimiler certains points. Les auteurs ont d’ailleurs souvent recours à des utilitaires développés par leurs soins et disponibles à l’adresse suivante :

http://www.sysinternals.com/Utilities.html

Quelques utilitaires (tels que whoami et oh) sont disponibles sur le site de Microsoft. Tous ne fonctionnent pas sous Windows XP.

Les outils du kit de ressources de Windows 2000 :

http://www.microsoft.com/windows2000/techinfo/reskit/tools

Les outils du kit de ressources de Windows 2003 :

A l'adresse : http://www.microsoft.com/downloads , dans la zone de recherche, saisir : « 2003 resource kit tools ». Dans la page de résultats, suivre alors le lien « Windows Server 2003 Resource Kit Tools ».

La technique du **Slipstreaming** ou comment personnaliser le CD d'installation de Windows XP en y intégrant les services pack et autres mises à jour est révélée sur le site suivant, en français :

http://geeksasylum.free.fr

pour un accès direct à la première page :
http://geeksasylum.free.fr/articles/systeme/installation_automatisee_xp_sp1/part01.htm