Pratique système : Sécurité

Sécurisation de Windows NT 4.0 et Windows 2000

Partie 2/3

Patrick CHAMBET
patrick.chambet@edelweb.fr

Pas sécurisé, Windows NT ? Pas si sûr. Le mois dernier, nous avons commencé à sécuriser un système Windows NT ou Windows 2000 et vu qu'il suffit d'un peu de pratique et d'une bonne dose de méthode pour obtenir un système déjà beaucoup plus solide !

Patrick CHAMBET (email : patrick.chambet@edelweb.fr) est expert en sécurité Windows NT et Windows 2000 au sein de Edelweb (http://www.edelweb.fr), l'une des premières sociétés de conseil en Sécurité des Systèmes d'Information françaises, spécialisée dans la sécurité Internet.

Windows NT 4.0 comporte de nombreuses fonctionnalités de sécurisation. Cependant, lors d'une installation par défaut du système, la configuration de ces fonctionnalités est laissée trop lâche. Avec Windows 2000, Microsoft a tenté de remédier à ce problème, et propose des configurations par défaut plus robustes, mais qui sont encore trop orientées vers la facilité d'utilisation plutôt que vers la sécurité intrinsèque du système. L'objectif de cette série de deux articles est de décrire les évolutions de Windows 2000 par rapport à Windows NT 4.0 en matière de sécurité, et de présenter des recommandations de sécurisation concernant les deux systèmes en vue d'obtenir un serveur correctement sécurisé.

Le mois dernier, nous avons traité surtout de la démarche de sécurisation, de la sécurité physique et environnementale, du paramétrage général du système, de la gestion des comptes, des stratégies de comptes et de la gestion et de la robustesse des mots de passe.

Cette deuxième partie va traiter des droits utilisateurs et du paramétrage des clés de la base de registre ainsi que du paramétrage des permissions d'accès aux clés de la base de registre. Le mois prochain, nous verrons les permissions d'accès aux fichiers et répertoires, le chiffrement de fichiers et de répertoires, l'activation de l'audit du système et le contrôle périodique de l'état de votre système.

Droits utilisateurs

Certains d'entre eux nécessitent une modification des groupes et utilisateurs par défaut :

Droit	Accorder à
Accéder à cet ordinateur à partir du réseau	Administrateurs, Utilisateurs avec pouvoir et Utilisateurs authentifiés (ou Utilisateurs)
Arrêter le système	Administrateurs
Forcer l'arrêt à partir d'un système distant	Personne. Dans le cas d'une machine membre d'un domaine, les Administrateurs du domaine

Modifier l'heure système	Administrateurs
Ouvrir une session localement	Administrateurs Utilisateurs authentifiés Opérateurs de sauvegarde
Augmenter la priorité de planification	Administrateurs
Optimiser un processus	Administrateurs
Outrepasser le contrôle de parcours	Administrateurs Opérateurs de sauvegarde (*)
Sauvegarder des fichiers et des répertoires	Administrateurs, Opérateurs de sauvegarde
Restaurer des fichiers et des répertoires	Administrateurs, Opérateurs de restauration (créer ce groupe)
Gérer le journal d'audit et de sécurité	Administrateurs
Prendre possession des fichiers ou d'autres objets	Administrateurs

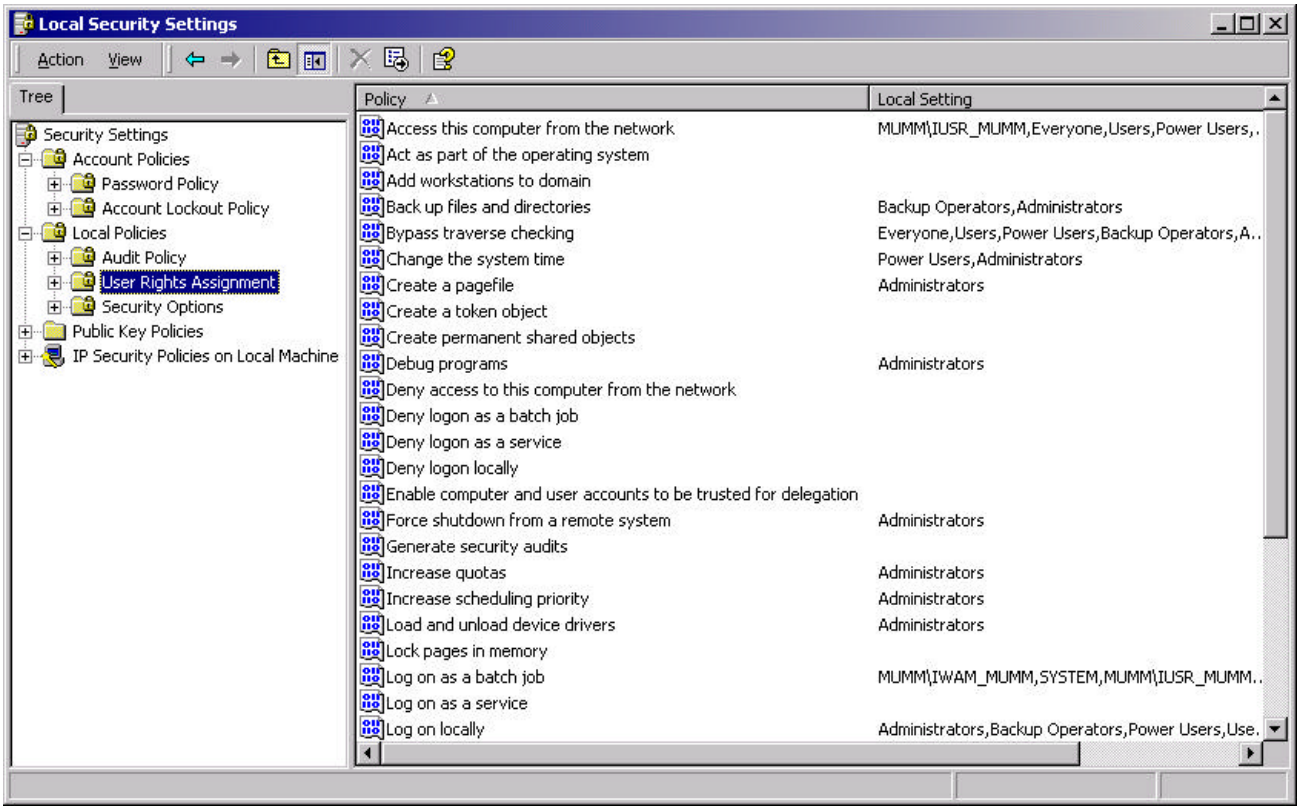

Fig. 1 : le paramétrage des droits utilisateurs.

Les autres droits ne nécessitent généralement pas de modification des paramètres par défaut. Toutefois, il est conseillé de les parcourir et d'effectuer les modifications jugées nécessaires en fonction des besoins spécifiques du système.

De plus, sous Windows 2000, vous pouvez spécifier explicitement des utilisateurs pour le droit « Interdiction d'ouvrir une session localement ».

Paramétrage des clés de la base de registre

Le paramétrage de la base de registre est quasi obligatoire avec Windows NT 4.0. Sous Windows 2000 par contre, comme nous l'avons vu, de nombreux paramètres de sécurité sont accessibles depuis la MMC, dans l'outil d'administration nommé « Stratégie de sécurité locale », et, dans le cas où on se trouve dans un domaine Windows 2000, depuis Active Directory.

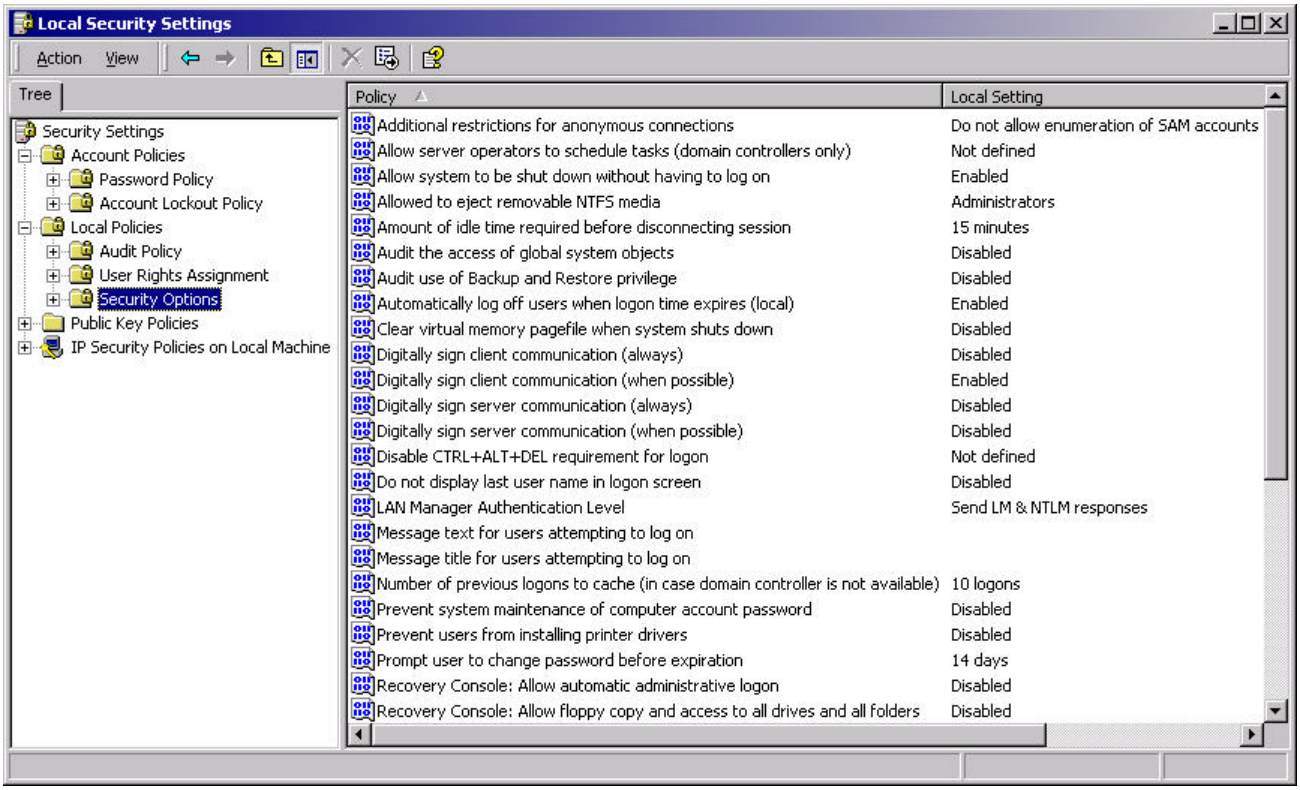

Fig.2 : les options de sécurité paramétrables directement depuis la Stratégie de Sécurité Locale.

Attention : en raison de l'importance de la base de registre pour le bon fonctionnement du système, il faut être extrêmement prudent lors de l'édition de celle-ci. Toute erreur peut rendre le système inutilisable au prochain démarrage.

Il est donc fortement recommandé d'effectuer une sauvegarde de la base de registre avant toute modification avec l'outil `regedit.exe`, et de compléter celle-ci par la mise à jour de la disquette de réparation d'urgence (ERD) avec l'utilitaire `rdisk /s` sous Windows NT 4.0 et avec l'outil `ntbackup` sous Windows 2000.

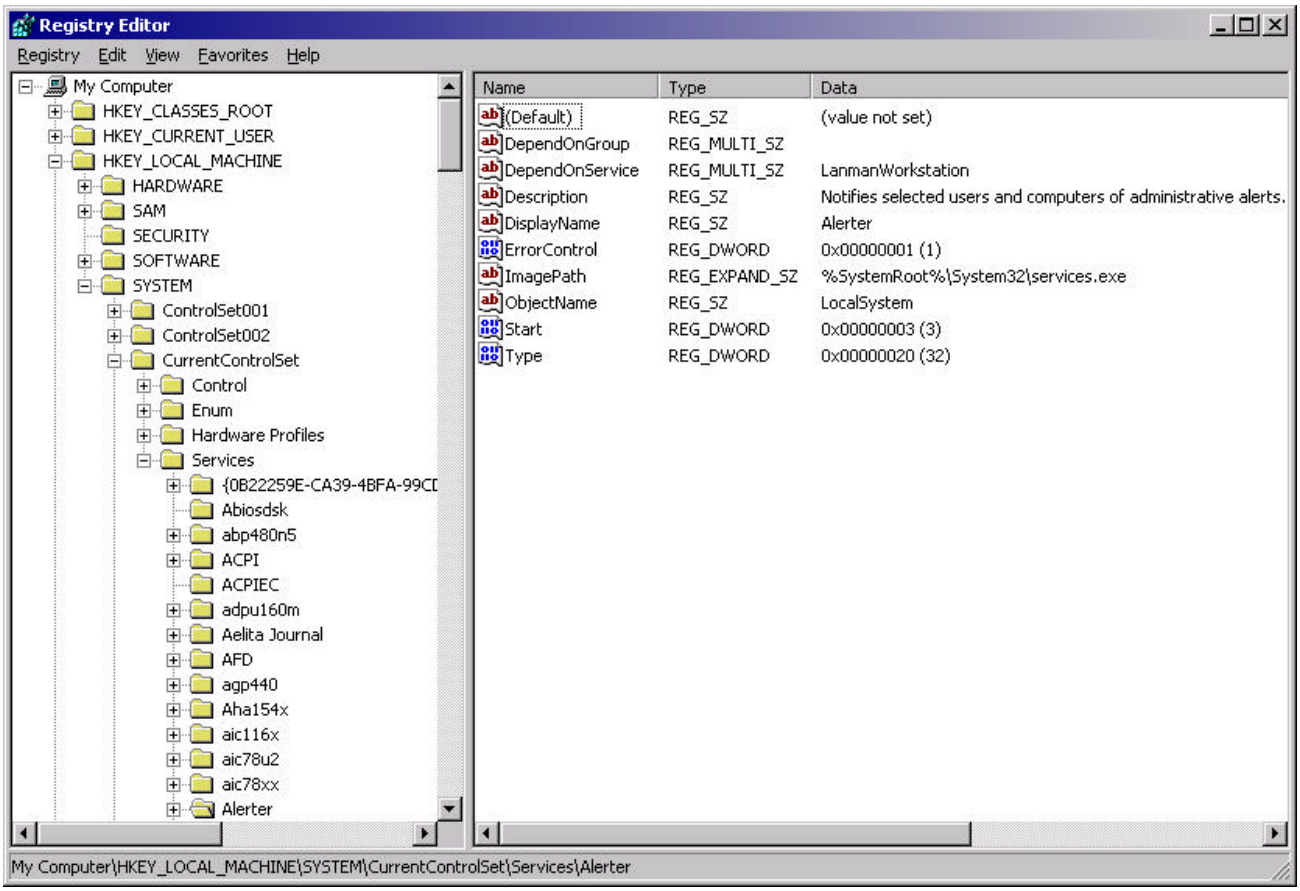

Fig. 3 : éditeur de registre.

Audit du système

Activez l'audit de tous les privilèges : la valeur `FullPrivilegeAuditing` dans la clé `[HKEY_LOCAL_MACHINE] \SYSTEM\CurrentControlSet\Control\Lsa` doit être positionnée à 1.

Activez l'audit sur les objets de base dès leur création : la valeur `AuditBaseObjects` dans la clé `[HKEY_LOCAL_MACHINE] \SYSTEM\CurrentControlSet\Control\Lsa` doit être positionnée à 1.

Vérifiez que la valeur `CrashOnAuditFail` dans la clé `[HKEY_LOCAL_MACHINE] \SYSTEM\CurrentControlSet\Control\Lsa` est positionnée à 1 afin que la machine s'arrête en cas de saturation des fichiers journaux.

Accès distant aux fichiers journaux

Paramétrez la valeur RestrictGuestAccess dans les clés [HKEY_LOCAL_MACHINE] \SYSTEM \CurrentControlSet\Services\EventLog\Application, \SYSTEM\CurrentControlSet\Services\EventLog\Security et \SYSTEM\CurrentControlSet\Services\EventLog \System à 1 afin d'interdire l'accès distant aux fichiers journaux.

Dans le cas d'une machine membre d'un domaine, cette valeur peut ne pas être positionnée pour permettre aux administrateurs d'exploiter les journaux de la machine à distance.

Simplification du système

Désactivez les sous-systèmes OS/2 et Posix sont inhibés : les valeurs suivantes doivent être absente de la base de registre :

Os2LibPath dans la clé :

```
[HKEY_LOCAL_MACHINE]
   \SYSTEM\CurrentControlSet\Control\Session
  Manager\Environment
```

Os2 et Posix dans la clé :

```
   \SYSTEM\CurrentControlSet\Control\Session
  Manager\SubSystems
```

Mire de connexion

Désactivez l'affichage du nom de login du dernier utilisateur : la valeur DontDisplayLastUserName dans la clé [HKEY_LOCAL_MACHINE] \SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon doit être à 1.

Définissez un message de présentation : paramétrez les valeurs LegalNoticeCaption et LegalNoticeText dans la clé [HKEY_LOCAL_MACHINE] \SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon.

Définissez un message d'accueil : paramétrez les valeurs LogonPrompt et Welcome dans la clé [HKEY_LOCAL_MACHINE] \SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon.

Connexions locales

Vérifiez que la connexion automatique d'un utilisateur n'est pas activée. La clé [HKEY_LOCAL_MACHINE] \SOFTWARE\Microsoft\Windows NT\CurrentVersion\WinLogon ne doit pas contenir les valeurs :

AutoAdminLogon

```
DefaultDomainName
DefaultPassword
DefaultUserName
```

Connexions distantes

Interdisez l'utilisation du mécanisme d'authentification LanManager : la valeur `LMCompatibilityLevel` dans la clé `[HKEY_LOCAL_MACHINE] \SYSTEM\CurrentControlSet\Control\Lsa` doit être positionnée à 2.

Attention, ce paramètre n'est valable que pour un environnement entièrement Windows NT 4.0 et/ou Windows 2000. Cette valeur peut-être supérieure ou égale à 3 si le Service Pack 4 est installé sur les machines Windows NT 4.0.

Forcez les canaux sécurisés à être scellés et chiffrés : les valeurs `SealSecureChannel`, `SignSecureChannel` et `RequireSignOrSeal` dans la clé `[HKEY_LOCAL_MACHINE] \SYSTEM\CurrentControlSet\Services\NetLogon\Parameters` doivent être positionnées à `True`.

Inhibez l'historique des informations de connexion : la valeur `CachedLogonsCount` dans la clé `[HKEY_LOCAL_MACHINE] \SOFTWARE\Microsoft\Windows NT\CurrentVersion\ Winlogon` doit être positionnée à 0.

Accès anonymes

Interdisez les connexions réseaux anonymes : la valeur `RestrictAnonymous` dans la clé `[HKEY_LOCAL_MACHINE] \SYSTEM\CurrentControlSet\Control\Lsa` doit être à 1.

La valeur `RestrictNullSessAccess` dans la clé `[HKEY_LOCAL_MACHINE] \SYSTEM \CurrentControlSet\Services\LanManServer\Parameters` doit être positionnée à True.

Les valeurs `NullSessionPipes` et `NullSessionShares` dans la clé `[HKEY_LOCAL_MACHINE] \SYSTEM\CurrentControlSet\Services\LanManServer\Parameters` doivent être vides.

Accès media amovibles

Vérifiez que les medias amovibles ne sont pas accessibles depuis le réseau lorsqu'un utilisateur est connecté sur le poste : les valeurs `AllocateCDRoms` et `AllocateFloppies` dans la clé `[HKEY_LOCAL_MACHINE] \SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon` doivent être positionnée à 1.

Vérifier que le démarrage automatique des applications sur CD-ROM est interdit. La valeur `Autorun` dans la clé `[HKEY_LOCAL_MACHINE] \SYSTEM\CurrentControlSet\Services\Cdrom` doit être positionnée à 0.

Accès distant à la base de registre

L'accès distant à la base de registre suit les permissions définies sur la clé suivante :

`[HKEY_LOCAL_MACHINE] \SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg`

Si cette clé n'est pas présente, créez-la explicitement. Vérifiez que seuls les administrateurs ont accès à cette clé, et en consultation seulement.

Afin d'éviter que cette règle d'accès ne puisse être outrepassée pour certaines parties de la base de registre, la clé suivante doit être absente ou vide :

`[HKEY_LOCAL_MACHINE] \SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg\AllowedPaths.`

Communications client/serveur

Configurez le protocole SMB de façon sécurisée :

- Pour un serveur, les valeurs `EnableSecuritySignature` et `RequireSecuritySignature` dans la clé `[HKEY_LOCAL_MACHINE] \SYSTEM\CurrentControlSet\Services \LanManServer\Parameters` doivent être à 1.

- Pour une station de travail, les valeurs `EnableSecuritySignature` et `RequireSecuritySignature` dans la clé `[HKEY_LOCAL_MACHINE] \SYSTEM \CurrentControlSet\Services\LanManWorkstation\Parameters` doivent être à 1.

Arrêt du système

Vérifiez que l'arrêt du système est interdit en dehors d'une connexion interactive : la valeur `ShutdownWithoutLogon` dans la clé `[HKEY_LOCAL_MACHINE] \SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon` doit être positionnée à 0.

Purgez le fichier de pagination à l'arrêt du système : la valeur `ClearPageFileAtShutdown` dans la clé `[HKEY_LOCAL_MACHINE] \SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management` doit être positionnée à 1.

Partages administratifs

Désactivez les partages administratifs par défaut : pour un serveur, la valeur `AutoShareServer` dans la clé `[HKEY_LOCAL_MACHINE] \SYSTEM \CurrentControlSet\Services\LanmanServer\Parameters` doit être positionnée à 0.

Pour une station de travail, la valeur `AutoShareWkS` dans la clé `[HKEY_LOCAL_MACHINE] \SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters` doit être positionnée à 0.

Divers

Vous pouvez configurer votre serveur pour qu'il ne réponde pas aux explorations réseaux : la valeur `Hidden` dans la clé `[HKEY_LOCAL_MACHINE] \SYSTEM\CurrentControlSet \Services\LanmanServer\Parameters` doit être positionnée à 1.

Vérifiez que seuls les administrateurs peuvent ajouter une nouvelle imprimante : la valeur `AddPrintDrivers` dans la clé `[HKEY_LOCAL_MACHINE] \SYSTEM \CurrentControlSet\Control\Print\Providers\LanMan Print Services\Servers` doit être positionnée à 1.

Vérifier que le service de Planning n'est pas utilisable par d'autres utilisateurs que les administrateurs : la valeur `SubmitControl` dans la clé `[HKEY_LOCAL_MACHINE] \SYSTEM\CurrentControlSet \Control\Lsa` doit être positionnée à 0.

Protection de la base de registre

Protection des fichiers de la base de registre

Vérifiez que seuls les administrateurs ont accès en écriture aux fichiers contenant la base de registre. Les fichiers associés aux différentes parties de la base de registre sont les suivants :

dans le répertoire *%SystemRoot%\System32\config* :

```
[HKEY_LOCAL_MACHINE]\SAM          SAM et SAM.LOG
[HKEY_LOCAL_MACHINE]\SECURITY     SECURITY et SECURITY.LOG
[HKEY_LOCAL_MACHINE]\SOFTWARE     SOFTWARE et SOFTWARE.LOG
[HKEY_LOCAL_MACHINE]\SYSTEM SYSTEM et SYSTEM.ALT
```

dans le répertoire *%SystemRoot%\Profiles\Default User*

```
[HKEY_USERS]\DEFAULT         DEFAULT.DAT et DEFAULT.DAT.LOG
```

Vérifiez que seuls les administrateurs, et l'utilisateur correspondant, ont accès en écriture aux fichiers représentants la base de registre utilisateur :

dans le répertoire *%SystemRoot%\Profiles\%user%* :

%SystemRoot%\Profiles\%user%
`[HKEY_CURRENT_USER]` `NTUSER.DAT et NTUSER.DAT.LOG`

Permissions d'accès sur les clés

Les permissions d'accès par défaut sur les clés de la base de registre sont plus sécurisées sous Windows 2000 que sous Windows NT 4.0. Vous devez utiliser l'utilitaire `regedt32.exe` pour gérer la sécurité des clés.

Vérifiez tout de même que seuls SYSTEM et Administrateurs possèdent le droit Contrôle Total sur l'ensemble de la base de registre (sauf [HKEY_USERS]).

Vérifiez que le groupe Interactif (et Utilisateurs Authentifiés si des connexions distantes sont nécessaires) ne possède que le droit Lecture sur l'ensemble de la base de registre (sauf [HKEY_USERS]).

Les permissions en écriture doivent être affectées en fonction des différents besoins des diverses applications installées.

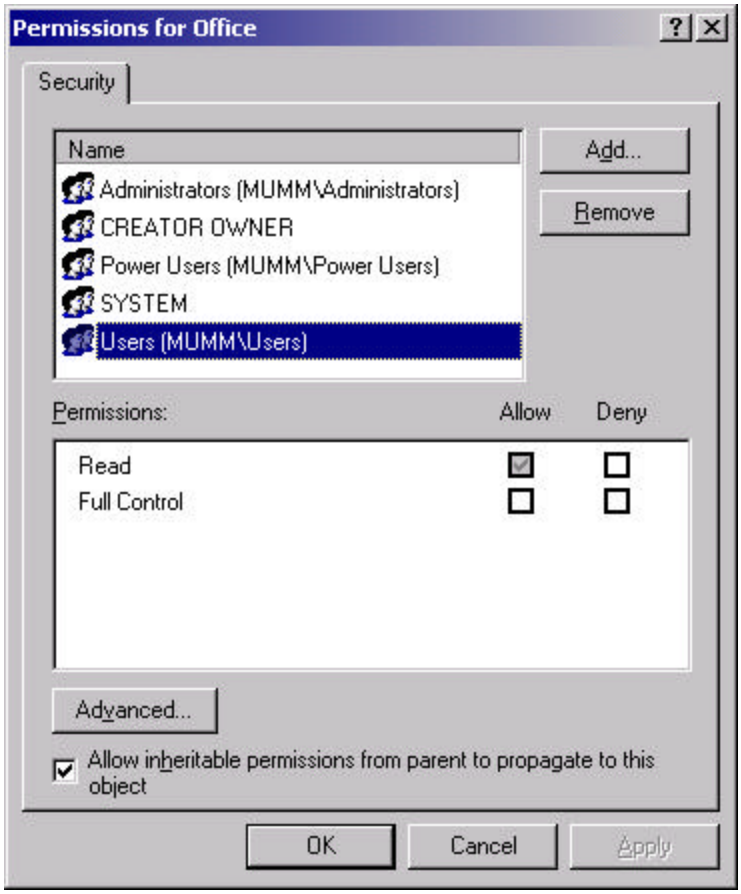

Fig. 4 : permissions sur la clé [HKEY_LOCAL_MACHINE]\Software\Microsoft\Office

Vérifiez que le groupe Interactif ne possède que le droit Lecture sur la clé [HKEY_USERS]\.Default.

Encore une fois, faites très attention au cours de l'affectation des restrictions pour les applications, car certaines lisent et écrivent sans cesse dans la base de registre…

Le mois prochain, nous aborderons les permissions d'accès aux fichiers et répertoires, le chiffrement de fichiers et de répertoires, l'activation de l'audit du système et le contrôle périodique de l'état de votre système.