Pratique système : Sécurité

Sécurisation de Windows NT 4.0

et Windows 2000

Partie 3/3

Patrick CHAMBET
patrick.chambet@edelweb.fr

Au cours des deux premières parties de cet article, nous avons commencé à sécuriser un système Windows NT 4.0 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.

Introduction

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 d'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 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.

Cette troisième partie va s'attacher aux permissions d'accès aux fichiers et répertoires, au chiffrement de fichiers, à l'activation de l'audit du système et au contrôle périodique de l'état de votre système.

Permissions d'accès aux fichiers et répertoires

Pour pouvoir affecter des permissions d'accès sur les fichiers et répertoires de votre disque, vos partitions doivent bien sûr être au format NTFS. Si vous n'utilisez pas Windows 9x/ME en même temps que Windows NT 4.0 ou Windows 2000, n'ayez pas peur de convertir toutes vos partitions en NTFS. Un argument souvent avancé pour conserver au moins une partition en FAT est que si vous avez un incident au boot de Windows NT, vous ne pouvez pas réparer vos fichiers de démarrage sur une partition NTFS. Ceci n'est plus valable avec Windows 2000 : en cas de problème, vous avez la possibilité d'installer l'utilitaire « Windows Recovery Console » à partir du CD d'installation de Windows 2000. Cet outil vous permettra, en cas d'incident de boot, de vous loguer en tant qu'Administrateur en mode console sur votre machine, et ainsi, avec un jeu d'instruction minimum, de manipuler vos fichiers et vos clés de base de registre de façon à résoudre votre problème.

Pour installer la Recovery Console, placez-vous dans le répertoire \I386 du CD d'installation de Windows 2000, et tapez :

```
Winnt32 /cmdcons
```

Les permissions d'accès aux fichiers sont trop permissives par défaut sous Windows NT 4.0. Sous Windows 2000, elles sont un peu plus sécurisées, et, de plus, vous bénéficiez du concept d'héritage des permissions. Cependant, le groupe Tout le Monde a toujours, comme sous NT 4.0, le droit Contrôle Total par défaut sur les fichiers. De même, les partages réseau sont créés avec le droit Contrôle Total pour le groupe Tout le Monde par défaut… Enfin, les partages administratifs (partages cachés C$, D$, ADMIN$, …) sont également activés par défaut. Il convient de les désactiver dans la stratégie de sécurité locale ou directement dans la base de registre, comme nous l'avons vu le mois dernier.

La technique à suivre pour affecter des permissions d'accès sur un domaine NT est la suivante :

- On commence par créer des groupes NT globaux au niveau de domaine sur le Contrôleur de Domaine.
- On affecte ensuite les utilisateurs du domaine aux groupes globaux.
- Puis on crée des groupes NT locaux sur les machines gérant directement les ressources auxquelles les utilisateurs doivent accéder (serveurs de fichiers, serveurs d'impression, etc…).
- On place alors les groupes globaux dans les groupes locaux (remarque : l'inverse est impossible).
- Enfin, on affecte les permissions d'accès aux ressources aux groupes locaux.

En procédant de la sorte, et, sous Windows 2000, en utilisant la fonction d'héritage des permissions, vous pouvez simplifier la tâche de maintenance des permissions d'accès et, surtout, vous minimisez les risques d'erreurs de configuration. De plus, vous rapprochez physiquement l'administration des ressources de leur localisation géographique.

Sur un serveur Windows NT 4.0 ou Windows 2000, parmi les fichiers et les répertoires à protéger figurent ceux du système d'exploitation lui-même. Pour visualiser ces fichiers dans l'explorateur de fichiers, cochez la case « Visualisation des fichiers système/cachés » et décochez la case « Cacher les fichiers protégés du système » dans la boîte de dialogue d'options d'affichage des répertoires :

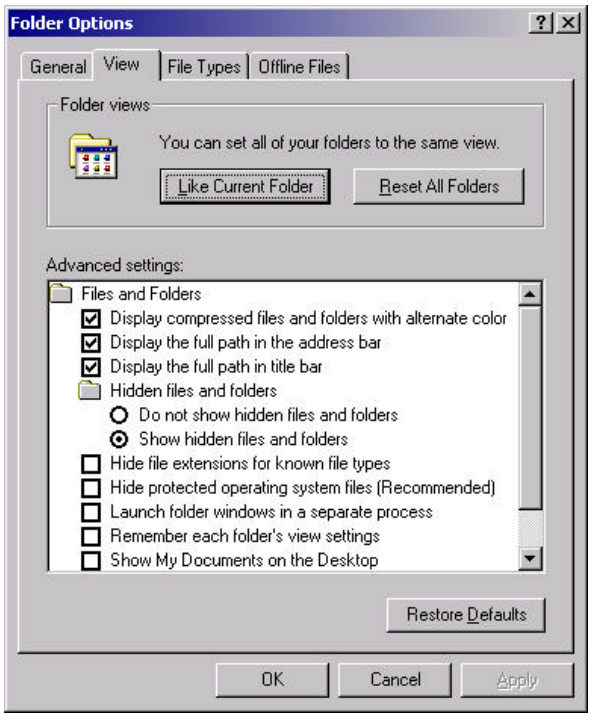
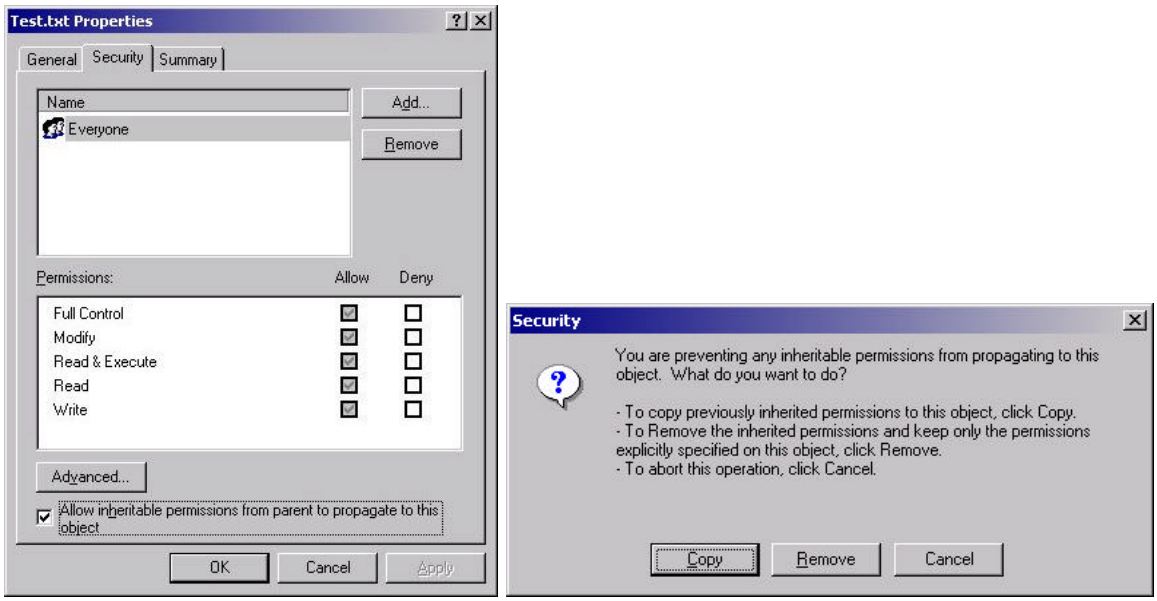


Figure 1 : Options d'affichage de l'explorateur de fichiers.

Assurez-vous d'appliquer des autorisations aux répertoires parents avant d'en appliquer à leurs sous-répertoires. Attention également à l'héritage des permissions : vous serez amené à supprimer cet héritage lorsque vous voudrez affecter des permissions différentes de celles du répertoire parent. Dans la fenêtre des propriétés d'un fichier ou d'un répertoire, la case « Permettre aux autorisations pouvant être héritées du parent d'être propagées à cet objet » est cochée par défaut. Si vous décochez cette case, une fenêtre de dialogue vous demande alors si vous voulez configurer vos nouvelles permissions d'accès à partir d'une copie de celles du parent, ou bien si vous voulez partir à zéro (sans aucune permission) :



Figures 2 et 3 : Permissions d'accès et héritage.

Les permissions d'accès conseillées sont les suivantes :

Répertoires ou fichiers	Droits
Fichiers sous la racine : Boot.ini Ntdetect.com Ntldr	Groupe Administrateurs : Contrôle total System : Contrôle total
Fichiers sous la racine : Autoexec.bat Config.sys	Groupe Administrateurs : Contrôle total System : Contrôle total Interactif : Lecture
Autres fichiers sous la racine (en dehors de pagefile.sys)	Groupe Administrateurs : Contrôle total System : Contrôle total
\TEMP	Groupe Administrateurs : Contrôle total System : Contrôle total Interactif : Accès spécial au répertoire : RWX
\Winnt\Repair	Groupe Administrateurs : Contrôle total
Pour chaque profil utilisateur : \Winnt\Profiles\%user% (sous Windows NT 4.0) \Documents and Settings\%user% (sous Windows 2000)	Groupe Administrateurs : Contrôle total System : Contrôle total %user% : Changer
Autres répertoires et fichiers sous \Winnt	Groupe Administrateurs : Contrôle total System : Contrôle total Interactif : Lecture
Autres sous-répertoires de la racine (et leur contenu)	Groupe Administrateurs : Contrôle total System : Contrôle total Interactif : Lecture

Ces permissions constituent une base, à laquelle il faut ajouter toutes les permissions d'accès sur les données personnelles et/ou confidentielles présentes sur le serveur.

Chiffrement des fichiers et répertoires

Windows 2000, grâce à EFS (Encrypting File System), supporte le chiffrement de fichiers et de répertoires. Mais ce mécanisme est mono utilisateur : seul l'utilisateur qui a chiffré un fichier pourra le déchiffrer, en dehors de l'agent de récupération de clés. Vous ne pouvez donc pas partager de fichiers chiffrés sur un serveur de fichiers, par exemple.

Pour chiffrer un fichier ou un répertoire, celui-ci doit se trouver sur une partition NTFS 5 (Windows 2000). Faites un clic droit dessus, choisissez Propriétés, cliquez sur le bouton Avancé et cochez la case correspondante :

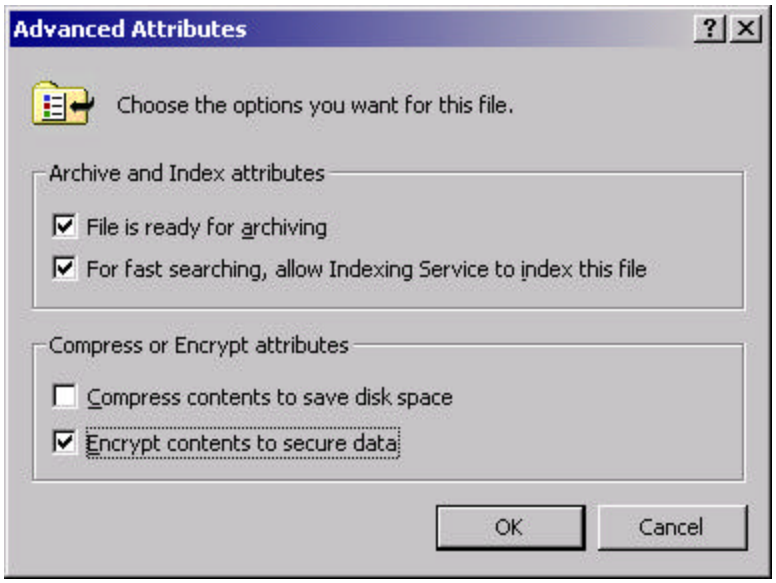


Figure 4 : Chiffrement d'un fichier ou d'un répertoire.

Notez que les options de compression et de chiffrement sont exclusives : un fichier peut être soit compressé, soit chiffré.

Attention, le chiffrement ne remplace pas les permissions d'accès à vos fichiers : en effet, si un fichier sensible est chiffré, il ne pourra pas être lu par un utilisateur malveillant, mais il pourra être effacé s'il n'a pas de permissions d'accès suffisamment restrictives ! Donc, dans l'ordre, affectez des permissions à vos fichiers, puis chiffrez-les.

Activation de l'audit du système

L'audit de sécurité de Windows NT est un mécanisme de journalisation des évènements de sécurité ayant lieu sur le système. Il peut vous informer des actions présentant un risque pour la sécurité du système, et identifier les comptes à partir desquels les actions ont été effectuées.

Il est conseillé de paramétrer votre stratégie d'audit dans les outils d'administration « Stratégie de sécurité locale » et « Stratégie de sécurité du domaine », en choisissant d'auditer **au moins** les évènements suivants :

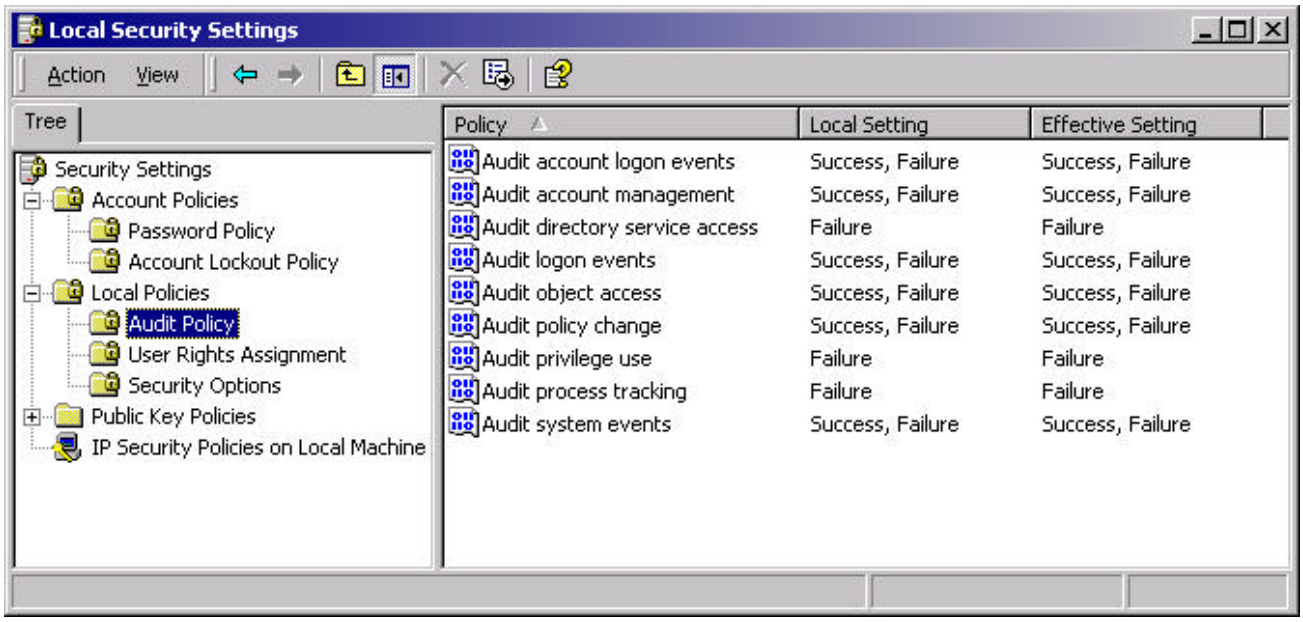


Figure 5 : Stratégie d'audit.

De plus, dans l'Observateur d'événements, configurez vos journaux pour que ceux-ci aient une taille suffisante (5 Mo par exemple), et que les anciens événements ne soient pas écrasés par les nouveaux en cas de saturation des fichiers. Dans ce cas, il est préférable de sauvegarder les journaux et de les vider manuellement.

Quant aux fichiers, l'audit de leur usage se paramètre ainsi : dans l'explorateur de fichiers, faites un clic droit sur un fichier ou un répertoire, choisissez Propriétés, cliquez sur le bouton « Avancé », puis sur l'onglet « Audit ».

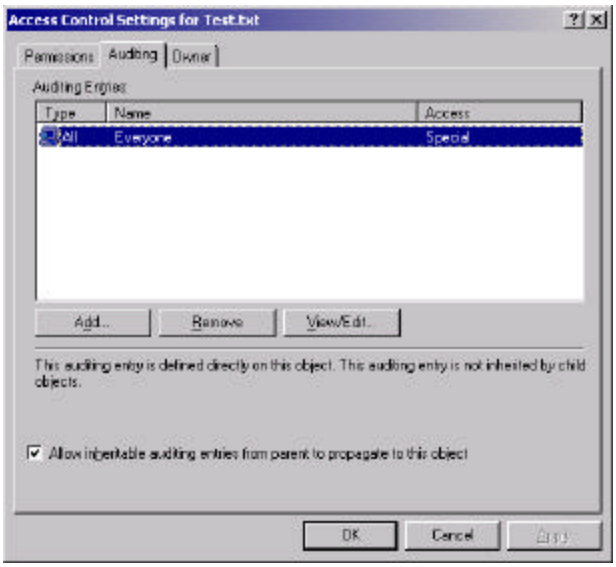


Figure 6 : Audit des fichiers.

Vous pouvez ajouter dans cette fenêtre un type d'audit en fonction des utilisateurs.

Enfin, pour paramétrer l'audit sur une clé de la base de registre, procédez comme suit : lancez `regedt32.exe`, déplacez-vous vers la clé voulue, faite un clic dessus et dans le menu Sécurité, choisissez « Permissions… », puis cliquez sur « Audit ». Vous retrouvez une interface du même type que celle qui permet de paramétrer l'audit des fichiers.

Contrôle périodique de l'état de votre système

Une fois votre système correctement paramétré, il faut vous assurer qu'il le demeure dans la durée. Pour remettre à jour la configuration de votre système périodiquement, vous pouvez utiliser l'outil d'administration « Configuration et analyse de la sécurité », fourni en standard sous Windows 2000 sous forme d'un snap-in pour la MMC :

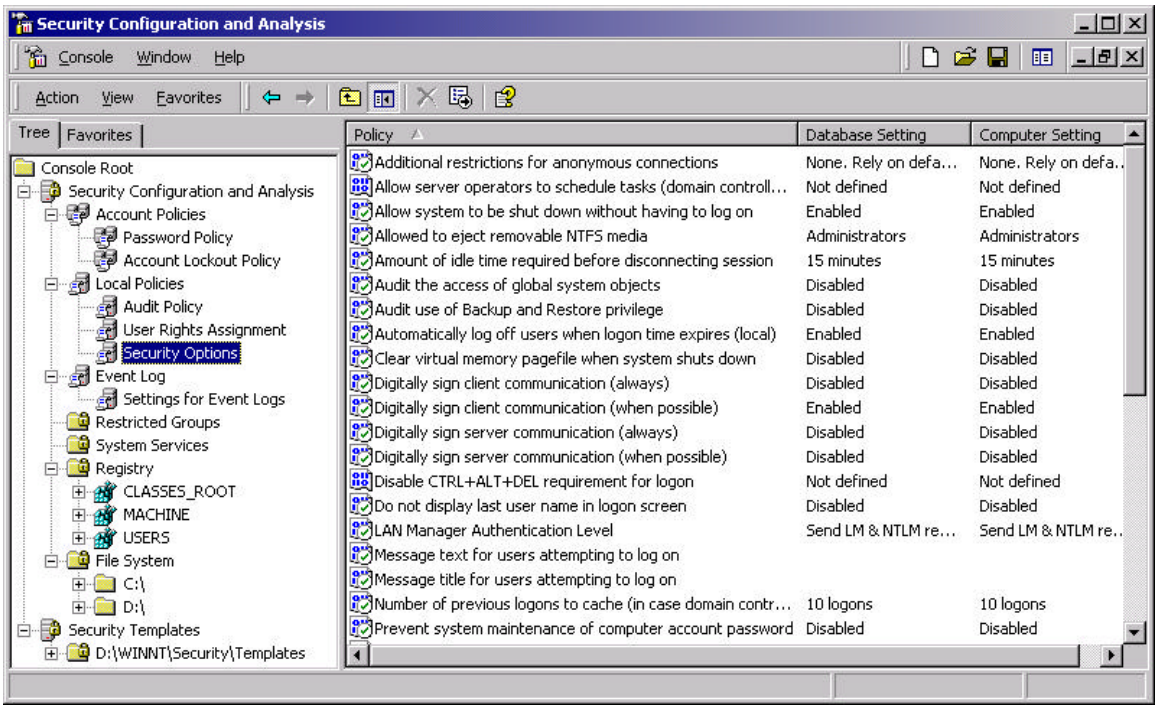


Figure 7 : L'outil « Configuration et analyse de la sécurité ».

Cet outil existe aussi sous Windows NT 4.0: il s'agit du Security Configuration Tool Set (SCTS), qui est livré sur le CD du Service Pack 4 et qu'on peut télécharger sur le site de Microsoft.

Cet outil est très puissant. Il permet de:

1. Définir ses modèles de sécurité personnalisés
2. Analyser et contrôler la configuration courante du système et la comparer au modèle de sécurité

3. Appliquer au système les paramètres de sécurité définis dans le modèle, en écrasant la configuration courante.

Pour plus de renseignements, voir l'URL suivante :
http://www.microsoft.com/france/technet/produits/Win2000s/info/info.asp?mar=/france/technet/produits/Win2000s/info/securcon.html

Cet outil peut également être démarré en mode ligne de commande (`secedit.exe` : voir l'aide pour la syntaxe), et en créant une tâche planifiée pour le lancer à intervalle régulier, par exemple.

Faites faire un audit périodique de votre système

Pour vous assurer que vous n'avez oublié aucune vulnérabilité, effectuez périodiquement un audit de votre serveur, soit en utilisant un outil de scan de vulnérabilités automatique du type Internet Security Scanner (ISS), soit en faisant appel à un consultant en sécurité informatique, qui effectuera une prestation plus « sur mesure » et adaptée à vos besoins. Ce type de prestation s'appelle un test de visibilité, et peut aller jusqu'au test d'intrusion.

Pour en savoir plus :

Voici les check-lists de référence en ce qui concerne la sécurisation très renforcée de Windows NT 4.0 :

- Trusted Systems-NSA Windows NT Security Guidelines V.2 : http://www.trustedsystems.com/nsa_dpg.htm
- US Navy Secure Windows NT Guide V.1.4: http://infosec.nosc.mil/COMPUSEC/ntsecure.html

Pour terminer, voici un résumé des recommandations de sécurisation de Windows 2000: http://www.edelweb.fr/ossir.html