Pratique système : Sécurité

Sécurisation de Windows NT 4.0

et Windows 2000

Partie 1/3

Patrick CHAMBET
patrick.chambet@edelweb.fr

Pas sécurisé, Windows NT ? Pas si sûr. S'il est certain qu'un système « out of the box » fait penser à un certain fromage à trous, il suffit d'un peu de pratique et d'une bonne dose de méthode pour obtenir un système déjà beaucoup plus solide et adapté à nos besoins de sécurité !

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

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 du système et la protection des données. 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.

La première partie traite 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.

Le mois prochain, nous aborderons les droits utilisateurs, les permissions d'accès aux fichiers et répertoires, le chiffrement de fichiers et de répertoires, le paramétrage des clés de la base de registre, le paramétrage des permissions d'accès aux clés de la base de registre, l'activation de l'audit du système et le contrôle périodique de l'état de votre système.

La démarche de sécurisation

Dans le cas d'une entreprise, une démarche de sécurisation commence par la rédaction d'une politique de sécurité. Les étapes nécessaires pour cela sont entre autres les suivantes :

- Bilan de la stratégie de l'entreprise, de son organisation et de ses processus
- Analyse des risques (évaluation des menaces et des vulnérabilités)
- Définition d'une architecture de sécurité, rédaction d'un schéma directeur

Ensuite seulement vient l'implémentation de la sécurité, suivie au besoin par un audit de configuration puis par des tests d'intrusion.

Dans le cas d'un particulier, celui-ci devra définir ses besoins (plusieurs utilisateurs partagent l'ordinateur, …) et ses risques (accès Internet permanent, …).

Les niveaux de sécurité

Windows NT 4.0 et Windows 2000 permettent d'établir différents niveaux de sécurité, allant d'un niveau de sécurité faible à une sécurité élevée.

Pourquoi ne pas choisir systématiquement d'avoir une sécurité maximale ? Une raison est que plus un système est protégé, plus les tâches des utilisateurs deviennent complexes à accomplir. De plus, la mise en place et la gestion des protections constituent une charge supplémentaire pour les administrateurs.

D'autre part, si la sécurité est trop stricte, les utilisateurs peuvent être tentés de la contourner pour faciliter leur travail (mot de passe écrit sur un Post-It sous le clavier, pas de fermetures de sessions, etc.).

Il est donc nécessaire d'évaluer votre besoin de sécurité afin de trouver le juste équilibre entre niveau de sécurité et facilité de travail pour les utilisateurs avant de mettre en œuvre une configuration de sécurité. De plus, la mise en œuvre de paramétrages de sécurité ont un impact direct sur la configuration du système. En particulier, certaines applications exigeront peut-être des paramètres plus souples afin de fonctionner correctement. Il faut donc évaluer avec soin chacune des recommandations préconisées dans cet article en la mettant dans le contexte de votre système afin de s'assurer que celui-ci fonctionnera toujours après l'application de la recommandation.

Le résultat de cette phase d'analyse et de tests pourra être la réalisation d'un master permettant d'obtenir un système configuré pour assurer une sécurité définie comme minimale.

Les nouveautés de Windows 2000

Les nouvelles fonctionnalités concernant la sécurité, par rapport à Windows NT 4.0, sont les suivantes :

- Sécurité dans Active Directory
- Stratégies de Groupes
- Modèles de sécurité
- Autres possibilités (suppression de NetBIOS, ...)
- Authentification par Kerberos V.5
- Permissions d'accès aux fichiers plus fines
- Paramètres de la base de registre plus sécurisés
- Security Configuration Tool Set et Secedit
- Encrypting File System (EFS)
- IP Security (IPSec)
- Protection des fichiers système (WFP)
- Support des PKI intégré
- Support de Smart Cards intégré

Ces fonctionnalités seront abordées dans la suite de cet article, et les différences entre Windows NT 4.0 et Windows 2000 seront indiquées au fur et à mesure des points traités.

Sécurité physique

La pièce dans laquelle se trouve l'ordinateur, surtout lorsqu'il s'agit d'un serveur, devra être fermée à clé lorsque personne n'est là pour le surveiller afin d'éviter le vol. L'idéal serait que cette pièce se trouve dans un bâtiment dont l'accès est autorisé aux seules personnes habilitées.

Dans le cas d'un ordinateur portable, utilisez un câble antivol pour l'assurer à un point solide.

Environnement

Le déni de service le plus évident est l'interruption du courant électrique. Utilisez une protection contre les surtensions et/ou un onduleur pour protéger l'ordinateur et éviter toute perte de données ou altération des partitions au cours d'un arrêt brutal.

Faites également attention aux risques de type incendie ou dégâts des eaux en respectant les normes de locaux en vigueur.

Politique de sauvegardes

Des sauvegardes régulières doivent être effectuées, afin de protéger vos données des pannes matérielles, des erreurs de manipulation, des virus et autres dommages délictueux.

Un ou plusieurs jeux de sauvegardes devront être conservés dans un lieu géographique différent. Ces sauvegardes elles-mêmes devront être sécurisées (attention au transport).

Contrôle d'accès à l'ordinateur

Il est impossible de sécuriser totalement un ordinateur si on peut y accéder physiquement. Toutefois, il est conseillé de prendre les mesures suivantes:

- Si l'ordinateur est une station de travail, configurez un mot de passe au boot dans le BIOS, et protégez également la configuration de celui-ci par un mot de passe d'administration. Dans le cas d'un serveur, si vous voulez qu'il redémarre automatiquement en cas de coupure de courant par exemple, il ne faut pas mettre de mot de passe de boot.
- Eviter les multi-boot, qui permettent de démarrer lordinateur avec un autre système d'exploitation (Linux, …).
- Désactivez l'amorçage par disquette dans la configuration du BIOS. Si possible, retirez le lecteur de disquettes, afin d'empêcher le démarrage sur un système d'exploitation permettant d'utiliser des utilitaires comme NTFSDOS pour accéder aux partitions NTFS.

- Si l'ordinateur possède une serrure physique, verrouillez-la et conserver la clé dans un endroit sûr. Toutefois, si la clé est perdue ou inaccessible, il se peut qu'un utilisateur autorisé soit dans l'incapacité de travailler sur l'ordinateur. Attention donc aux auto-dénis de service induits par des procédures mal définies.
- Toutes les partitions du disque dur doivent être au format NTFS.

Installation de Windows NT 4.0 et Windows 2000

Les étapes à suivre pour l'installation de Windows NT 4.0 ou Windows 2000 à partir des CD-ROMs originaux sont les suivantes :

- Pour un serveur ne devant pas faire partie d'un domaine, choisir une installation en serveur autonome dans un groupe de travail.
- Installez ensuite les derniers Service Packs : le SP6a pour Windows NT 4.0 et le SP1 pour Windows 2000. Vous pouvez les télécharger à: http://www.microsoft.com/windows2000/downloads
- Installez ensuite les derniers Hotfixes. Attention, ceux-ci nécessitent une installation dans un ordre chronologique précis. Vous pouvez les télécharger à: http://windowsupdate.microsoft.com
- Puis installez les services nécessaires : serveur DNS, WINS, DHCP, RAS, PPTP, etc.
- Arrêtez les services non utilisés. A titre d'information, les services indispensables pour faire fonctionner une station de travail Windows 2000 sont les suivants:
  - Event Log
  - NT LM Security Support Provider
  - Remote Procedure Call (RPC)
  - Security Accounts Manager
  - Workstation
- Notez que même le service Server est arrêté. Si vous n'avez pas de partage réseau, ce n'est pas un problème. Par contre, l'explorateur d'ordinateurs sera arrêté également, et vous ne pourrez plus lister les ordinateurs de votre domaine.
- Désinstallez les protocoles réseaux non utilisés (IPX/SPX, NetBEUI)
- Désactivez les services réseaux non utilisés sur certaines cartes réseaux (typiquement NetBIOS si on n'a pas à accéder à des partages réseaux sur un LAN).
- Installez vos applications.
- Ré-appliquez le dernier Service Pack et les Hotfixes. Ce dernier point est obligatoire sur NT 4.0. Sur Windows 2000, le mécanisme de mise à jour utilisant Windows Installer et WFP (Windows File Protection) fait qu'il n'est plus nécessaire de repasser les Service Packs.
- Testez votre serveur et vérifiez qu'il peut communiquer à travers le réseau et que les applications et services fonctionnent.
- Créez une disquette de réparation d'urgence :
  - Sous Windows NT 4.0, tapez `rdisk /s`
  - Sous Windows 2000, utilisez l'utilitaire de Backup et cliquez sur le bouton « Disquette de réparation d'urgence ».

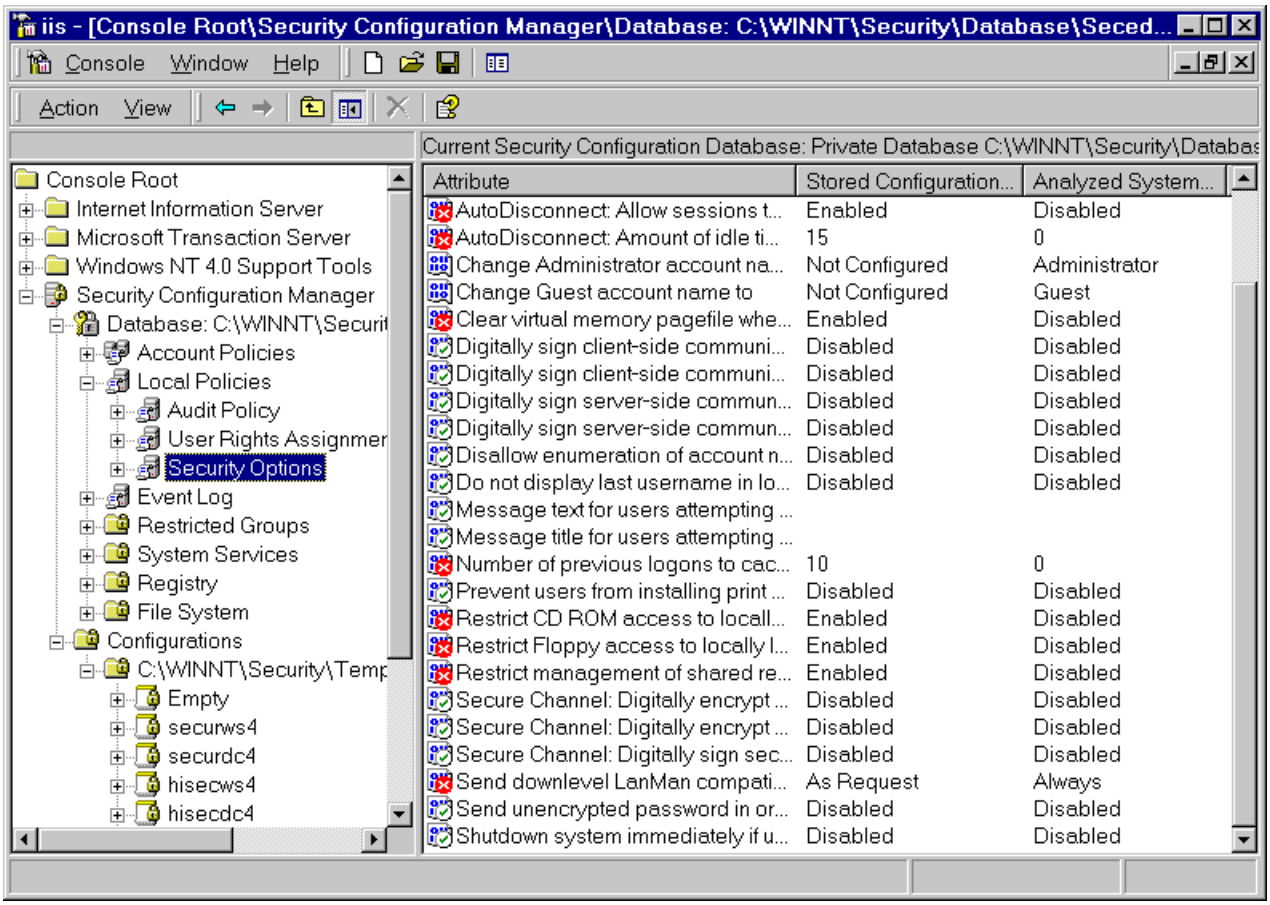
Paramétrage du système

L'application des paramètres de sécurité qui vont suivre dans cet article et le suivi des serveurs une fois configurés est laborieux car actuellement, sous Windows NT 4.0, il n'existe pas d'outil centralisé pour gérer la sécurité d'une station ou d'un serveur: l'administrateur jongle en général avec le gestionnaire des utilisateurs, l'éditeur de stratégies, l'explorateur NT, l'éditeur de registre, le journal des évènements et le panneau de configuration des services, auxquels il rajoute en général ses outils personnels.

- Windows 2000, par contre, est livré en standard avec un outil permettant de gérer depuis un seul et même endroit tous les paramètres liés à la sécurité du système local: l'outil d'administration nommé « Stratégie de Sécurité Locale » (et « Stratégie de Sécurité du domaine » dans le cas d'un Contrôleur de Domaine). Il est même possible d'ajouter dans cet outil ses propres paramètres de sécurité (les options de sécurité correspondant à des clés de la base de registre sont situées dans la clé `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ SeCEdit\Reg Values`). Windows 2000 dispose également d'un outil permettant de définir des profils de sécurité, d'analyser un système par rapport à ces profils et d'appliquer ceux-ci au système : il s'agit de l'outil « Configuration et Analyse de la Sécurité ».

- Les utilisateurs de NT 4.0 peuvent installer et utiliser un outil de ce type : le « Security Configuration Tool Set », livré sur le CD-ROM du SP4 pour NT 4.0, dans le répertoire `\MSSCE\i386` (bien qu'il ne soit pas installé par défaut en même temps que le SP4), ou téléchargeable depuis le site de Microsoft : ftp://ftp.microsoft.com/bussys/winnt/winnt-public/tools/scm

Le Security Configuration Tool Set est un « composant enfichable » qui s'installe dans la MMC (Microsoft Management Console), l'interface graphique de gestion centralisée du système, introduite sur NT 4.0 avec l'Option Pack et qui est le coeur de la gestion de Windows 2000.



Cet outil permet de:

- **Définir** ses modèles de sécurité, en plus des 10 modèles fournis en standard
- **Analyser et contrôler** la configuration courante du système et la comparer à un modèle de sécurité
- **Appliquer** au système les paramètres de sécurité définis dans un modèle

Attention : dans le cas d'un poste connecté en réseau, les options de sécurité du domaine ont priorité sur les options de sécurité locales en cas de conflit.

En effet, dans Active Directory, il est possible (et conseillé) de définir des Stratégies de Groupe, qui peuvent s'appliquer à tout conteneur Active Directory : sites, domaines et unités organisationnelles (OU).

Les Stratégies de Groupe (Windows 2000 uniquement)

Les stratégies de groupe affectent tous les utilisateurs et tous les ordinateurs du conteneur auxquelles elles s'appliquent, et peuvent être contrôlées ensuite par les groupes auxquels appartiennent l'utilisateur et l'ordinateur.

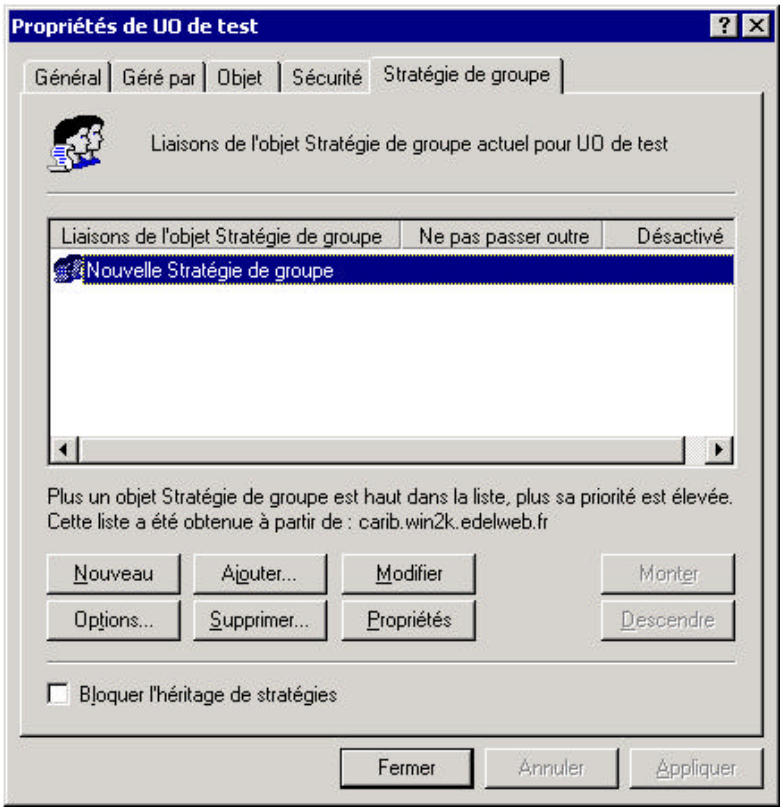
L'ordre d'application des stratégies de groupe est le suivant:

- Stratégies style NT 4.0 (NTConfig.pol)
- Stratégie de Groupe locale

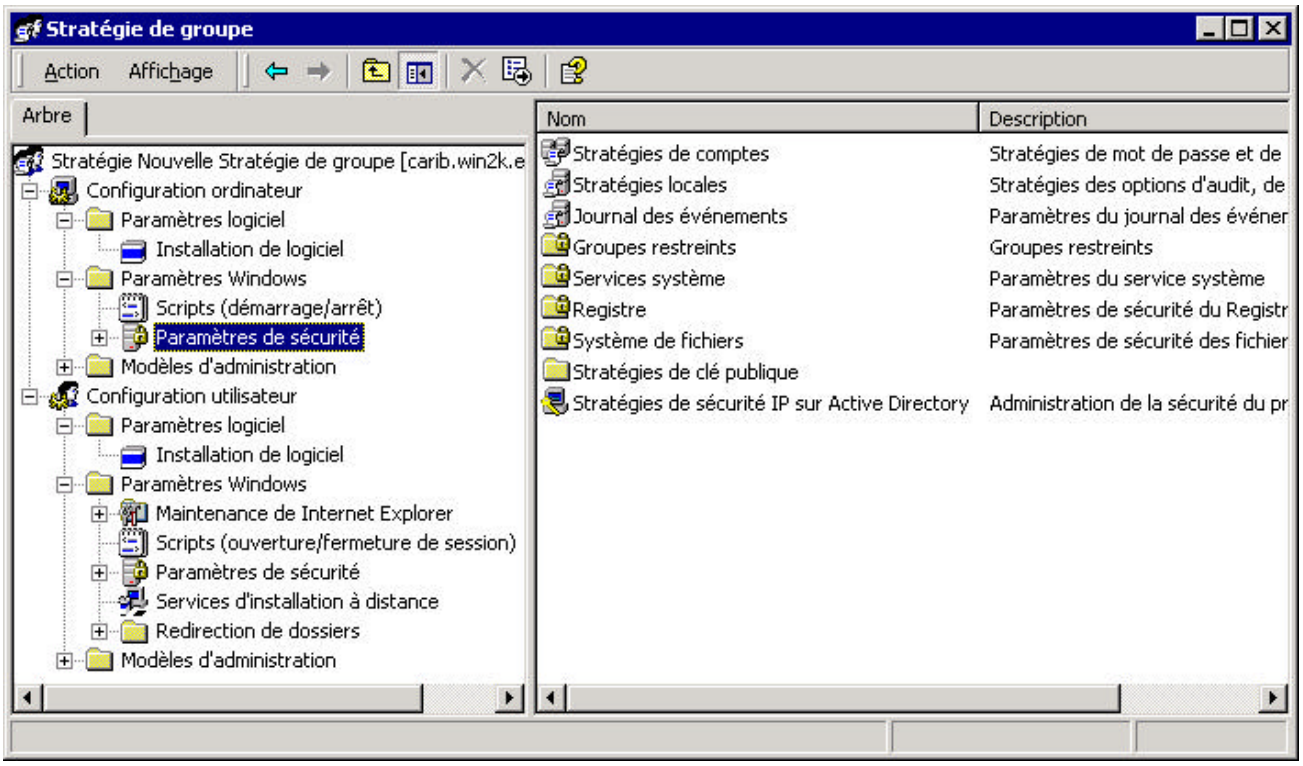
- Stratégies de site, dans l'ordre administratif
- Stratégies de domaine, dans l'ordre administratif
- Stratégies d'OU, du haut vers le bas et dans l'ordre administratif

Par défaut, les dernières stratégies « écrasent » les premières. Il est donc extrêmement important de bien définir ses stratégies de groupe afin que les paramètres de sécurités soient appliqués dans le bon ordre.

Pour créer une stratégie de groupe, ouvrez l'outil d'administration « Utilisateurs et Groupes Active Directory », faites un clic droit sur le conteneur de votre choix et choisissez Propriétés. Cliquez sur l'onglet Stratégie de Groupe :



Vous pouvez alors créer les stratégies de votre choix sur chacun des conteneurs de votre forêt Active Directory :



Gestion des comptes utilisateurs

Sous Windows 2000, la gestion des comptes utilisateurs se fait par l'outil d'administration « Gestion de l'Ordinateur » (nœud Utilisateurs et Groupes Locaux) pour les comptes définis dans la base SAM locale, ou par l'outil d'administration « Utilisateurs et Ordinateurs Active Directory » pour les comptes définis dans Active Directory sur un Contrôleur de Domaine.

Quelques recommandations :

?? Utilisez des comptes distincts pour l'administration et l'activité de tous les jours des utilisateurs. Pour éviter toute modification accidentelle de ressources sensibles, il est conseillé d'utiliser le compte ayant le moins de privilèges pour effectuer la tâche souhaitée. Les virus notamment peuvent causer beaucoup plus de dommages s'ils sont activés par l'intermédiaire d'un compte ayant des privilèges élevés.

   Sous Windows 2000, utilisez la commande `RunAs` pour lancer des outils d'administration avec des privilèges plus élevés par exemple.

?? Renommez le compte Administrateur en un compte moins évident. Ce compte très puissant est le seul qui ne peut être verrouillé à la suite de plusieurs échecs de tentatives d'ouverture de session. Les attaquants essaieront donc en priorité de pénétrer dans le système en tentant de deviner à plusieurs reprises le mot de passe de ce compte. En le renommant, vous faites perdre du temps

supplémentaire aux attaquants. Vous pouvez de plus ajouter un compte leurre aux privilèges réduits nommé Administrateur si vous le désirez. Dans tous les cas, choisissez un mot de passe extrêmement fort pour le compte Administrateur réel.

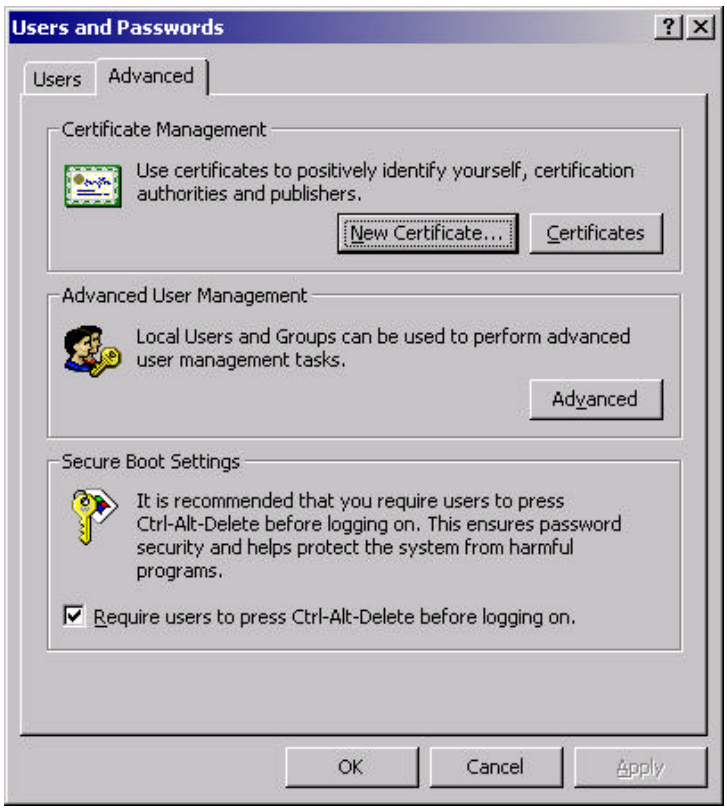
?? Assignez un mot de passe au compte Invité et désactivez-le.

Remarque : le compte Invité est déjà désactivé sur les versions Serveur de Windows NT 4.0 et Windows 2000.

Ouverture de session

Appuyer TOUJOURS sur CTRL+ALT+SUPPR avant d'ouvrir une session. En effet, des programmes conçus dans le but de recueillir des mots de passe peuvent apparaître comme un écran d'ouverture de session. En appuyant sur CTRL+ALT+SUPPR, vous désactivez ces programmes avant d'obtenir l'écran d'ouverture de session sécurisée de Windows NT.

Sous Windows 2000 Professional, la nécessité d'appuyer sur CTRL+ALT+SUPPR n'est pas obligatoire par défaut. Il faut l'activer par l'intermédiaire de l'onglet « Avancé » du panneau de contrôle « Utilisateurs et mots de passe » :



Enfin, l'ouverture de session sous Windows 2000 supporte en standard l'utilisation de Smart Cards (cartes à puce). Vous pouvez connecter un lecteur de carte supporté à

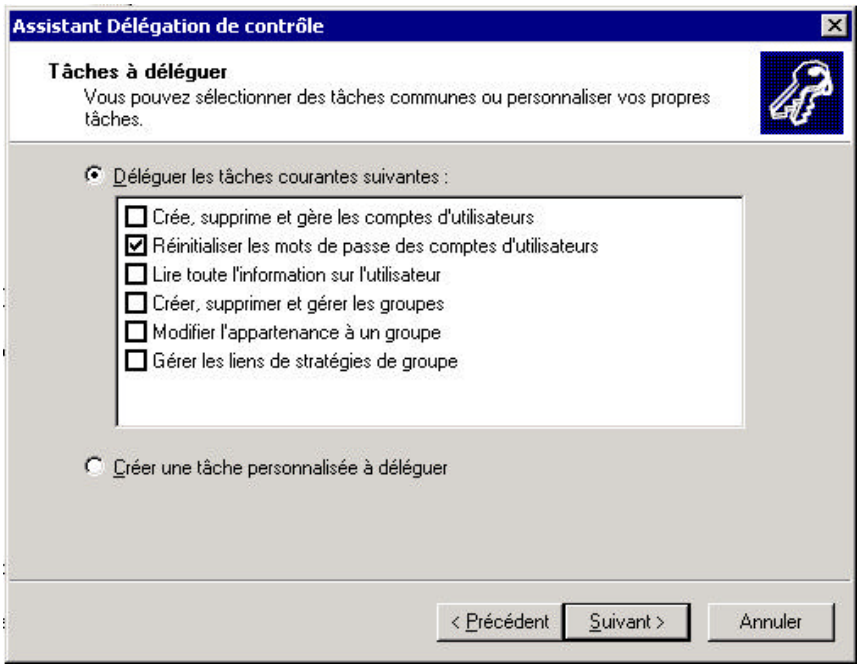
l'ordinateur et utiliser votre carte pour vous authentifier, sans avoir à saisir de mot de passe.

Verrouillage de la station de travail

Paramétrez les écrans de veille pour qu'il verrouillent automatiquement la session en cas de non-utilisation pendant une durée déterminée. Pour cela, utilisez l'option « Protégé par mot de passe » de votre écran de veille.

Délégation d'administration

Windows 2000 permet de déléguer l'administration des éléments d'Active Directory :



Il est conseillé d'utiliser cette possibilité afin de simplifier la tâche des administrateurs et d'assurer une administration plus proche des ressources.

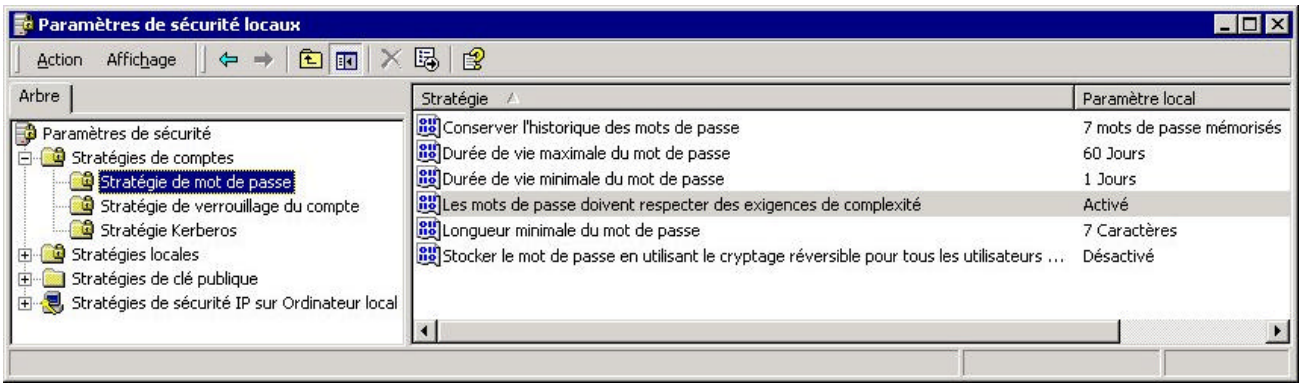
Stratégies de comptes

Les stratégies de comptes définies par défaut dans Windows NT 4.0 et Windows 2000 ne sont pas suffisantes. Paramétrez vos stratégies comme suit :

Stratégie de mots de passe :

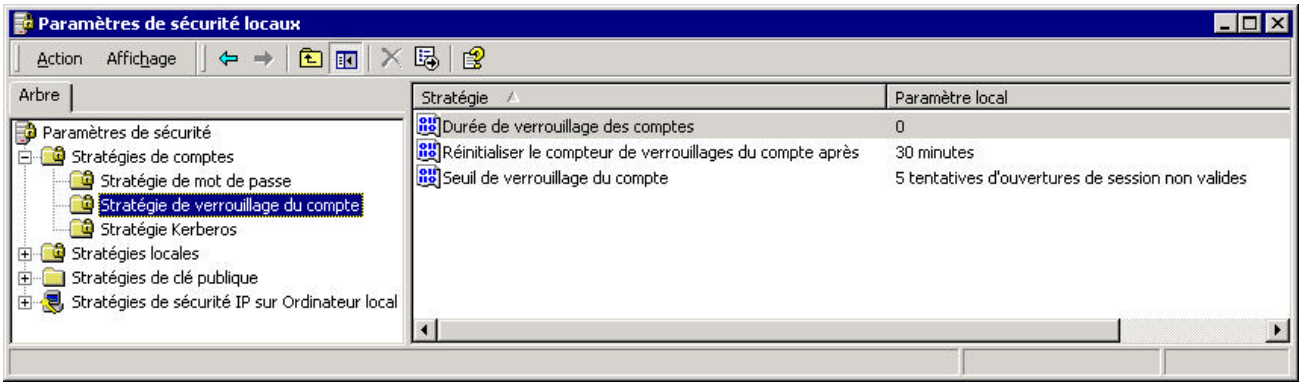
Durée de vie maximale du mot de passe	60 à 90 jours
Durée de vie minimale du mot de passe	Bien que ce paramètre semble peu important, s'il n'est pas défini, des utilisateurs pourront contourner la condition de non-réutilisation de leurs anciens mots de

	passe en changeant immédiatement leur mot de passe plusieurs fois de suite de façon à retomber sur leur mot de passe initial. Paramétrer à un jour minimum.
Longueur minimale du mot de passe	7 (ni 6, ni 8)
Conserver l'historique des mots de passe	6 ou 7
Les mots de passe doivent respecter des exigences de complexité (Windows 2000 seulement)	Activé
Stocker le mot de passe en utilisant le cryptage réversible pour tous les utilisateurs du domaine (Windows 2000 seulement)	Désactivé



Stratégie de verrouillage de comptes :

Seuil de verrouillage du compte	5
Réinitialiser le compteur de verrouillage du compte après	5 minutes minimum, plutôt 30 min à 1h
Durée de verrouillage des comptes	Toujours ou au minimum un jour.
L'utilisateur doit se connecter pour changer son mot de passe (NT 4.0 seulement)	Oui



Gestion et robustesse des mots de passe

?? Changez de mot de passe fréquemment et en cas de doute de compromission. Evitez de réutiliser les mêmes mots de passe, et n'assignez pas le même mot de

passe à des comptes différents.

?? Evitez d'utiliser des mots qui peuvent facilement être devinés ou des mots du dictionnaire. Choisissez par exemple une combinaison de lettres, de chiffres et d'autres caractères non alphanumériques.

?? N'écrivez votre mot de passe nulle part. Choisissez-en un que vous seul pouvez mémoriser facilement.

- Activez le verrouillage du compte administrateur sur accès distant: sous NT 4.0, par défaut, comme nous l'avons vu, le compte administrateur ne peut être verrouillé après l'échec de plusieurs tentatives d'ouverture de sessions. Toutefois, il est possible d'activer le verrouillage de ce compte après l'échec de tentatives de connexions distantes, par le réseau. Pour cela, exécutez l'outil PASSPROP du Kit de Resources Techniques de Windows NT 4.0 (syntaxe: `C:\passprop /adminlockout`). Le compte Administrateur sera alors verrouillé après le nombre d'échecs spécifié dans la stratégie de verrouillage de comptes (si elle est activée). L'Administrateur pourra toujours se loguer en local sur le serveur pour déverrouiller le compte.

- Forcez l'utilisation de mots de passe complexes: pour obliger les utilisateurs à choisir des mots de passe robustes, installez PASSFILT. PASSFILT est un filtre de mots de passe implémenté dans une DLL et fourni en standard avec NT 4.0 depuis le SP2.
  Ce filtre impose les 3 règles suivantes:
  - Le mot de passe ne doit pas contenir le nom de login ou un morceau du nom complet de l'utilisateur
  - Il doit faire au moins 6 caractères de long
  - Il doit contenir des caractères d'au moins 3 des 4 jeux suivants:
    - Alphabétiques minuscules
    - Alphabétiques majuscules
    - Chiffres
    - Caractères non alphabétiques ($,!,%,^, ...)

  Pour installer PASSFILT, vérifiez que le fichier PASSFILT.DLL se trouve bien dans \WINNT\system32 (il a du être installé par un Service Pack) ou copiez-le à la main, puis dans la clé suivante de la Registry: `HKEY_LOCAL_MACHINE\ SYSTEM\ CurrentControlSet\ Control\ Lsa`, ajoutez la chaîne "passfilt" (sans ".dll") à la valeur "Notification Packages". Si la valeur n'existe pas, créez-la.
  Attention: un administrateur pourra toujours changer un mot de passe directement dans la SAM avec le gestionnaire d'utilisateurs sans que ce mot de passe ne passe par le filtre.
  Enfin, sous Windows 2000, le durcissement des mots de passe peut se configurer en standard de manière simple: comme nous l'avons vu, dans les paramètres de sécurité locale, activez "Password must meet complexity requirements".

- Chiffrez la base de comptes: la SAM de Windows NT 4.0 contient les hashes des mots de passe LanMan et NTLM des comptes. Pour éviter que ces hashes ne soient récupérés directement par des outils de craquage de mots de passe comme L0phtCrack, utilisez l'utilitaire SYSKEY pour chiffrer la SAM locale. SYSKEY vous offre le choix de demander un mot de passe au boot de Windows NT, ou de stocker la clé de chiffrement sur une disquette qu'il faudra fournir à chaque démarrage, ou bien encore de stocker la clé de chiffrement sur le disque dur. Si vous voulez que votre serveur puisse redémarrer seul, choisissez cette dernière option.
  Sous Windows 2000, les hashes des mots de passe sont protégés dans la SAM par un mécanisme de salting, et SYSKEY n'existe plus. Mais malgré ces mécanismes de protection, il existe des outils diffusés sur Internet qui permettent tout de même de récupérer ces hashes, aussi bien sur NT 4.0 que sur Windows 2000, sous certaines conditions.

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