La gestion du système local

Un outil de support au développement

Par: Nelson Ruest et Danielle Ruest
Entreprises Résolutions

Cet article est le deuxième d'une série sur le support au développement avec les technologies Windows de Microsoft.

Dans un premier article intitulé « La machine Virtuelle » (InfoQuébec, volume 26, no. 5) nous vous avons présenté une première solution pour le support aux environnements de développement. Ce second article traite une deuxième solution, soit : La gestion des systèmes locaux.

Avec les systèmes DOS, Windows 3.x et Windows 9x les développeurs avaient la liberté nécessaire pour effectuer leur travail. Mais des conséquences énormes se présentaient avec ces systèmes, c'est-à-dire ces systèmes ne donnaient aucune sécurité et les développeurs pouvaient installer, faire fonctionner et configurer n'importe quelle application directement dans le noyau logiciel de leur ordinateur. Ceci avait souvent pour effet, la déstabilisation de leur système.

L'arrivée de Windows NT avec son système de fichier à 32-bit, NTFS, a permis de verrouiller les systèmes. NT permet le verrouillage complet du système. Ainsi les fichiers, les entrées de registre et les dossiers sont verrouillés. Pourquoi? Parce que ce verrouillage facilite le travail des groupes d'infrastructures technologiques (GIT) en diminuant les problèmes d'incompatibilité logicielle et ainsi, d'instabilité des postes de travail. Dans un système qui est complètement verrouillé, les GIT peuvent garantir la stabilité et spécifiquement le niveau de service qu'ils offrent pour l'opération des postes de travail.

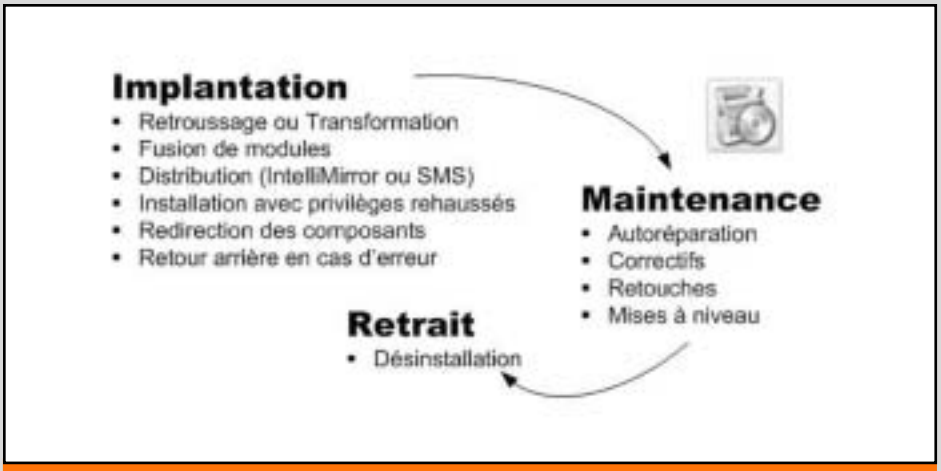
Mais pour les développeurs, cette solution de verrouillage « forcé » est difficile à vivre. Sans droits d'administration, ils ne peuvent pas modifier leurs systèmes, ils ne peuvent pas tester leur code applicatif (car ils ne peuvent pas l'installer), ils ne peuvent pas, en fait, effectuer leur travail.

Heureusement, le système Windows NT a évolué. L'arrivée de Windows 2000 et surtout, de Windows XP permet l'introduction d'un nouveau mode de verrouillage : le verrouillage « léger ». Ces nouvelles technologies apportent une sécurité NTFS plus évoluée. Dans un environnement pur Windows 2000 ou Windows XP, l'utilisateur avec pouvoir peut en faire plus et même l'administrateur a moins de possibilité d'endommager son système.

Quatre fonctions de Windows XP supportent la possibilité du verrouillage léger :

- Le système de protection de fichier Windows
- Le service Windows Installer
- Le nouveau chargeur d'applications « DLL Loader »
- La possibilité d'exécuter « en tant que... »

Ces quatre fonctions si elles sont utilisées à fond, protègent le système d'exploitation en tout temps, même si l'utilisateur a des droits d'installation.



Le service Windows Installer aide à gérer le cycle de vie des applications.

Le système de protection de fichiers Windows

La première fonction vise la protection des fichiers dits « critiques » pour la bonne opération d'un système Windows. Le système de protection de fichiers Windows (SPF), disponible depuis Windows 2000, est un service qui effectue une vigie constante des répertoires d'opération de Windows XP. À chaque fois qu'un fichier dit critique est enlevé ou remplacé par tout autre que le système d'exploitation lui-même, il est remplacé immédiatement avec la version protégée.

Ce système s'alimente à partir d'un répertoire spécial nommé « DLLCache ». Ce répertoire sert de tampon pour l'entreposage d'une copie de tous les fichiers critiques. Il est facile de voir le SPF en action. Il s'agit de naviguer vers le répertoire « \Windows\System321 », de localiser le fichier d'exécution de la calculatrice Windows, « CALC.EXE », et de le détruire complètement. Pour être sûr, videz la corbeille. Ensuite surveillez le répertoire System32. Le fichier CALC.EXE devrait réapparaître dans quelques instants.

Ainsi, SPF remplace en tout temps tout fichier protégé du système d'exploitation. Cette fonction est en opération par défaut sur tous les systèmes Windows 2000 et Windows XP.

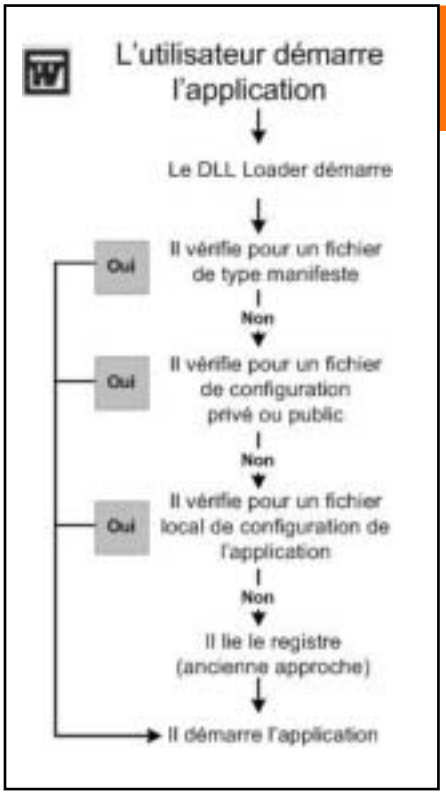
Le service Windows Installer

Le deuxième point d'appui du verrouillage léger est le service Windows Installer. Celui-ci a déjà été discuté dans InfoQuébec (volume 25, no. 4). Ce service permet la gestion du cycle de vie des applications ou logiciels sur des systèmes Windows. Un des avantages de l'intégration des applications à ce service est l'autoréparation. Toute application qui est installée par l'entremise du service Windows Installer devient immédiatement autoréparable. Windows Installer prend une copie de tous les détails d'une installation et l'insère dans une base de données de cohérence localisée sur le système Windows. Lors du démarrage d'une application, Windows Installer vérifie la cohérence de l'application contre cette base de données et corrige tout élément défectueux avant le démarrage.

Ainsi, si toutes les applications supportées par les groupes d'infrastructures technologiques sont intégrées à ce service, elles fonctionneront toujours quoiqu'il arrive. Alors, le développeur peut avoir le droit d'installer des applications car les GIT savent que les applications qui sont sous leur responsabilité vont s'autoréparer même si d'autres applications non conformes ont été ajoutées au système.

Seules les applications qui affichent le sigle « conçu pour Windows 2000 » ou « conçu pour Windows XP » font utilisation de ce service par défaut. Il est évident que ceci ne couvre pas toutes les applications sur le marché. Les GIT peuvent par contre utiliser un outil de retroussage pour intégrer l'installation d'une application patrimoniale à Windows Installer. Plusieurs produits sont disponibles sur le marché, notamment, Wise for Windows Installer et Package Studio de la société Wise, Prism Pack de Lanovation (voir InfoQuébec volume 26, no. 3), WinInstall LE et 2000 de Veritas, et beaucoup d'autres.

D'ailleurs plusieurs autres raisons existent pour une telle intégration de toutes les applications d'un parc informatique. Les GIT feraient bien de procéder à cette opération s'ils effectuent une migration vers Windows 2000/XP.

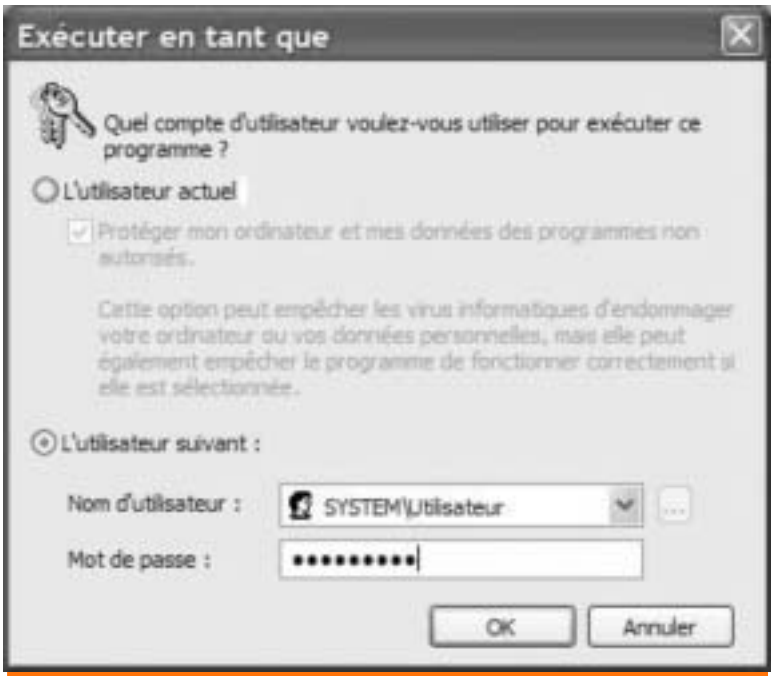


Le nouveau chargeur d'applications de Windows XP peut démarrer des applications sans lire le registre.

Le chargeur d'applications

Une troisième fonction, celle-ci particulière à Windows XP, libère les développeurs d'avoir besoin de s'intégrer au registre de Windows lors de l'utilisation ou de l'installation d'une application. En effet, le chargeur d'applications Windows, le « DLL Loader », peut maintenant utiliser des fichiers externes au registre pour mettre en place les paramètres requis pour exécuter une application.

Dans les versions précédentes de Windows, toute application digne de ce nom devait s'inscrire au registre afin de pouvoir fonctionner. C'est ce qui fait que lorsqu'une application est installée, elle est automatiquement associée au type de fichiers qu'elle génère. Ainsi, tous les fichiers de type DOC sont reliés à Microsoft Word et ainsi de suite...



Exécuter « en tant que... » permet de tester une application en utilisant un compte utilisateur.

Mais avec Windows XP, Microsoft introduit le concept de « manifeste », un fichier externe qui inclut les paramètres de l'application. Ce fichier peut se comparer aux fichiers de type « INI » qui existaient dans les anciennes versions de Windows. Les doyens de l'informatique se souviendront sûrement de WIN.INI, le fichier de paramétrisation et d'initialisation de Windows 1, 2, et 3. Le manifeste est comme le fichier INI sauf qu'il doit normalement être signé numériquement. Cette signature en valide l'authenticité. Faute de manifeste, le développeur peut utiliser un fichier de configuration privé ou public (signé numériquement) ou même tout simplement un fichier local de configuration de l'application.

Au démarrage de l'application, le chargeur d'applications vérifie d'abord pour un fichier manifeste, ensuite pour les autres types de fichiers et s'ils n'existent pas, il lie le registre afin de préparer l'environnement requis.

L'avantage pour les développeurs est qu'avec cette méthode, ils n'ont plus besoin d'avoir accès en écriture au registre de Windows pour tester leurs composants applicatifs car l'installation d'une application se limite à une copie de fichiers. Le registre peut donc être verrouillé sans impact pour le développeur.

Exécuter « en tant que… »

Finalement, Windows fournit son propre contexte « virtuel » de sécurité pour l'exécution des applications qu'il nomme « exécuter en tant que... ». Cet outil permet aux développeurs d'effectuer des essais de leur code applicatif sans avoir à se déconnecter ou fermer leur session. Avec cette fonction, les développeurs peuvent faire fonctionner l'application à l'intérieur d'un autre contexte de sécurité soit sous un compte utilisateur sans avoir à changer de contexte global. Cette fonction peut aussi être utilisée par des administrateurs pour rehausser leurs droits d'accès lors de besoins particuliers.

Le verrouillage léger

Toutes ces améliorations permettent aux organisations de livrer des systèmes qui sont protégés de façon permanente. Elles permettent aussi de livrer des systèmes qui offrent plus de convivialité au niveau du développement et de leurs besoins particuliers. Le tout, en s'assurant de la stabilité de ces solutions et de la conformité des composants qui sont gérés centralement par les gestionnaires des infrastructures technologiques.

Il va de soi que la mise en place de ces solutions n'est ni simple, ni sans coûts. Mais si l'organisation doit s'appuyer sur du développement interne pour poursuivre sa mission, elle doit s'engager à mettre en place des infrastructures qui rencontrent les besoins de leurs utilisateurs, et ce, à tous les niveaux. Après tout, la gestion des infrastructures technologiques est un service qui dessert une clientèle. Seuls des services de haute qualité qui rencontrent les besoins exprimés ont des clientèles satisfaites.

Le prochain article portera sur comment mettre fin à « l'enfer des DLLs », une fois pour toute.

1 *Sur Windows 2000, ce répertoire est le « \WINNT\System32 ».*