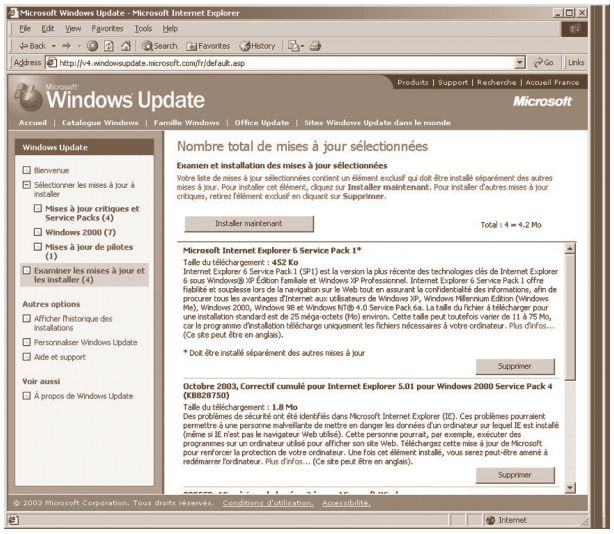
Vers, virus et autres calamités

Mise à jour automatique avec Software Update Services pour Windows 2000, XP et 2003

Laurent.Kling@epfl.ch, Faculté STI



Un ordinateur utilisant Windows Update (avant SUS)

Le problème

La découverte récurrente de *trou de sécurité* entraîne le cycle suivant:

- découverte du trou,
- mise à disposition de la rustine *(patch)*,
- (mises à jour des PC Windows),
- utilisation du trou pour infiltrer l'ordinateur non mis à jour.

La mise à jour des ordinateurs reste la solution, à condition qu'elle intervienne **avant** l'apparition du ver ou virus. En pratique, la mise à jour manuelle est fastidieuse. L'idéal serait de disposer d'une solution automatisée.

La démarche

La première solution qui vient à l'esprit est d'éduquer les usagers, pour qu'ils prennent l'habitude de vérifier régulièrement l'intégrité de leurs machines avec Windows Update. Malheureusement, son emploi n'est possible que si on possède les privilèges d'administration.

La seconde solution consiste à appliquer la rustine désirée par l'intermédiaire d'un script de démarrage et d'une stratégie de groupe (GPO, Group Policy Object). Elle possède comme principal désavantage la nécessité de mettre à disposition un partage de fichier et un travail manuel de la part de l'administrateur à réitérer pour chaque rustine.

La troisième solution, se rattachant à la création des MSI, serait de créer un MSI à partir de la rustine, puis de l'appliquer en utilisant une GPO. Malheureusement, cela risque d'entraîner des résultats hasardeux. Pour une installation standard, les DLL (Dynamic Linked Library) sont conservés dans le cache du système. Ceci pour prévenir une collision des différentes versions de DLL.

Au contraire de cette règle, une rustine de Microsoft réécrit directement la DLL. Ce comportement est sûrement dicté par le fait que Microsoft connaît les incidences de l'application de la rustine. En conséquence, la création d'un MSI n'est pas la solution. L'idéal serait de disposer d'un outil similaire à Windows Update.

La solution

Heureusement, il existe cet outil, SUS ou Software Update Services. Cet outil se décompose en trois parties :

- une source des mises à jour,
- un serveur Web intégrant le service,
- un client capable de s'alimenter sur le serveur.

Pour la source des mises à jour, elle est naturellement celle de Microsoft, dans le souci de limiter le débit réseau, on peut réutiliser un autre serveur SUS local.

Active Directory, un Machin ?

Il existe encore dans la communauté informatique, l'idée qu'Active Directory n'est que le dernier avatar d'un système d'identification ou *un machin* d'après le Général !

En réalité, Active Directory n'est pas qu'une réunion d'ordinateurs et d'usagers, mais bien plus, un méta-annuaire construit à partir de normes publiques (X500, DNS, LDAP, Kerberos). Comme l'a démontré le succès de NDS de NetWare, cette approche permet une intégration de services et dépasse largement la simple énumération des ressources.

La forte intégration de ce méta-annuaire avec le système d'exploitation offre une interrelation élevée. Elle permet de mettre en œuvre rapidement la solution décrite dans cet article.

Utilisation de Poledit, un piège ?

Dans l'article du numéro 7/2003 du Flash informatique, Paulo de Jesus préconise l'emploi de Poledit pour sécuriser les postes clients.

Je me permets d'apporter mon expérience sur cet outil que j'ai abondamment utilisé sous Windows NT 4, il possède un défaut qui peut s'avérer rédhibitoire, il s'applique directement sur la base de registres et certains de ses paramètres pour la sécurité ne peuvent êtres rétablis. La seule solution consistant alors en la réinstallation du Système.

Il a été avantageusement remplacé par les stratégies de groupes, GPO, dans Windows 2000, XP ou 2003, qui elles sont réversibles, combinables et hiérarchiques.

Pour le serveur Web, la meilleure solution consiste à dédier une machine pour ce rôle, suivant les recommandations de la documentation, le serveur est un Pentium III 600 MHz avec 512 Mb. Contrairement à la documentation de la version 1.01 de SUS, il ne peut être un serveur de domaine. SUS s'installe simplement sur IIS.

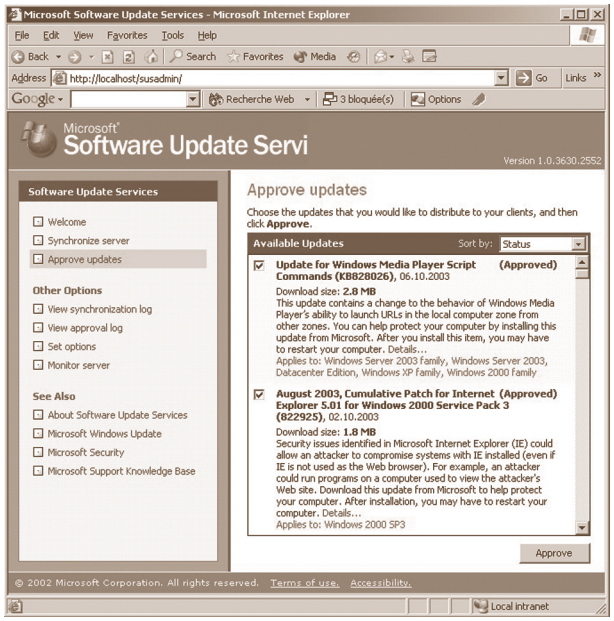
Pour le client, il existe un préalable pour son utilisation, il doit au minimum être un poste avec Windows 2000 SP3. Pour un client Windows 2003 ou Windows XP, les composants nécessaires sont déjà intégrés.

Les plates-formes antérieures (NT 4, 98, 95, 3.11) ne sont plus supportées par Microsoft, et à part les passages obligés, en particulier pour l'instrumentation, je recommande la migration vers un OS plus récent dès que possible.

En pratique

Dans un premier temps, le serveur SUS doit être à jour, c'est un pléonasme. À intervalle régulier, il télécharge les nouvelles rustines.

La seule opération humaine consiste à approuver les rustines proposées dans les différentes versions de langages. Certaines rustines peuvent entraîner un effet de bord sur les logiciels métiers entraînant une incompatibilité.



Approbation des rustines

Dans un monde parfait, on devrait disposer de différentes plates-formes en test pour vérifier cette compatibilité. En pratique, il est généralement plus simple de désinstaller la rustine problématique.

Si on estime pouvoir faire confiance à Microsoft et disposer des ressources réseau adéquates, on peut se passer de serveur SUS, mais on multipliera le trafic externe par le nombre de clients.

Ensuite le client doit pouvoir se connecter au serveur.

La configuration est conservée dans une série de clés de registre, pour éviter de manipuler celles-ci directement sur chaque machine, il est plus simple d'utiliser une stratégie de groupe (GPO). On pourra ainsi changer de stratégie sans intervention physique sur les ordinateurs.

La mise à jour peut commencer ; pour éviter une interprétation erronée, il est nécessaire de comprendre le fonctionnement de Windows Update qui se décompose en deux services :

- Le premier est le processus de recherche de mise à jour, qui se déroule sur un cycle d'une durée variable (de 17 à 22 heures):
  - le client recherche les nouvelles rustines, il interroge le serveur dont il possède l'identité et reçoit la liste des mises à jour;
  - il télécharge les fichiers depuis le serveur avec le protocole BITS (Backround Intelligent Transfer Service).
- Le second est le processus de mises à jour proprement dit, dans notre configuration c'est:
  - si cela n'a pas déjà été fait, il démarre le processus de recherche de mise à jour;
  - il installe la mise à jour (c'est notre objectif);
  - puis, il peut redémarrer pour qu'au prochain chargement du système, les versions à jour soient utilisées.

Une question se pose immédiatement, si on procède à une heure déterminée, Quid des machines éteintes à ce moment. Dans la version actuelle, ce cas est prévu, il existe la possibilité de redémarrer le processus de recherche de mises à jour un certain temps après le démarrage. Le résultat de ce processus est qu'il est parfois nécessaire d'attendre 48h pour que la machine soit effectivement à jour.

Le cas particulier du Service Pack

De l'extérieur, un Service Pack ne semble être qu'une collection de rustines. La réalité est plus complexe. En général, il n'existe pas forcément une rustine pour chaque trou de sécurité, ou certaine rustine s'adresse à une combinaison de cas particuliers et n'est pas applicable à l'ensemble d'un parc informatique. Un Service Pack est testé plus complètement et intègre des améliorations de fonctionnalités (pas toujours documentées). L'installation d'un Service Pack procède d'une manière différente de celle d'une rustine, elle propose toujours de sauvegarder l'état du système avant modification. Je vous recommande d'accepter cette option si la capacité de votre disque dur le permet, car elle permet de vous sauver de cas scabreux.

Le principal problème consiste dans l'intégrité des données. Un Service Pack est généralement volumineux (plus de 100 Mo) et il est périlleux d'utiliser un point de montage sur le réseau pour cette opération avec une connexion qui peut s'interrompre, en particulier avec une connexion sans fil.

On peut être étonné de la disproportion entre la taille d'un Service Pack pour le grand public (environ 0.5 Mo) et celle de la version réseau (plus de 100 Mo). En fait, la version grand public n'est qu'un client intégrant BITS.

BITS (Backround Intelligent Transfer Service)

Avec l'avènement de liaisons à hauts débits (câble, ADSL, WiFi), il est avantageux de tirer parti du débit mis à disposition. Il est rare qu'un ordinateur utilise l'ensemble de la bande passante sans interruption. Comme son nom l'indique BITS offre un service capable de télécharger en tâche de fond depuis un serveur Web. Un élément important de son implémentation est d'accepter une perte de connexion et de pouvoir résumer le téléchargement en cours.

Pour éviter de considérer ce service comme une gène, il n'initie jamais la connexion directement.

L'intégration de l'application d'un Service Pack avec SUS **n'est effective que depuis le 18 septembre 2003**. Cette nouveauté nous permet de disposer d'un outil pour les rustines et les Services Packs.

Pour le domaine de Faculté STI

La structure centralisée d'un domaine Active Directory possède une hiérarchie similaire à celle de la Faculté. L'utilisation d'unité d'organisation (OU) et de délégation de gestion permet une gestion décentralisée proche des usagers. L'utilisation d'une stratégie de groupes (GPO) permet d'appliquer ce nouveau service à n'importe quel endroit de cette structure.

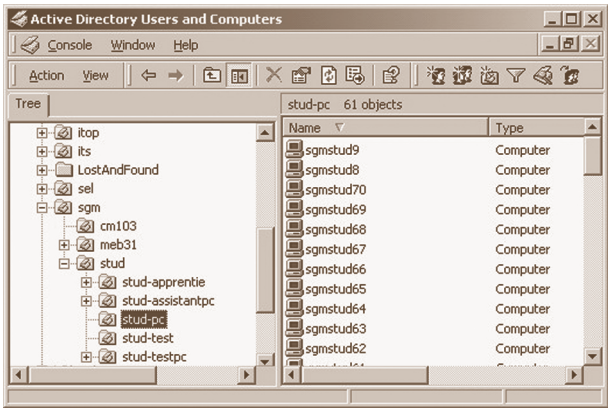
Pour l'administrateur d'une unité d'organisation (OU) du domaine STI, deux GPO préconfigurées sont disponibles:

- pour les postes de travail: **sti-update-sus-push-12h**
- pour les serveurs: **sti-update-sus-pushsrv-05h**

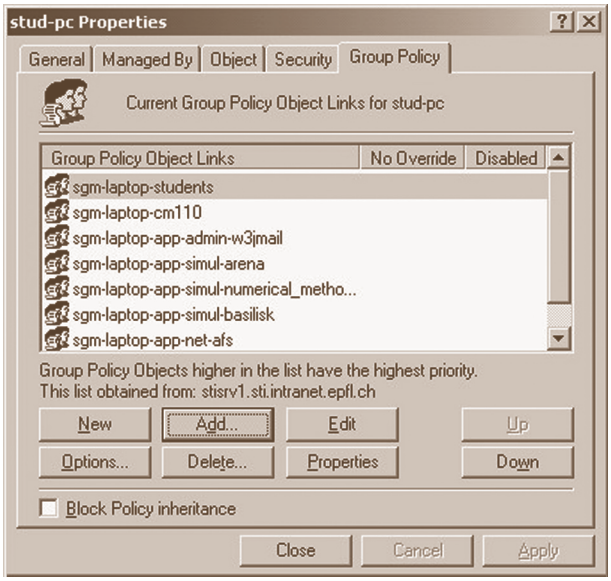
Il suffit d'appliquer la GPO adéquate sur l'OU contenant les ordinateurs à garder à jour.

Dans le détail:

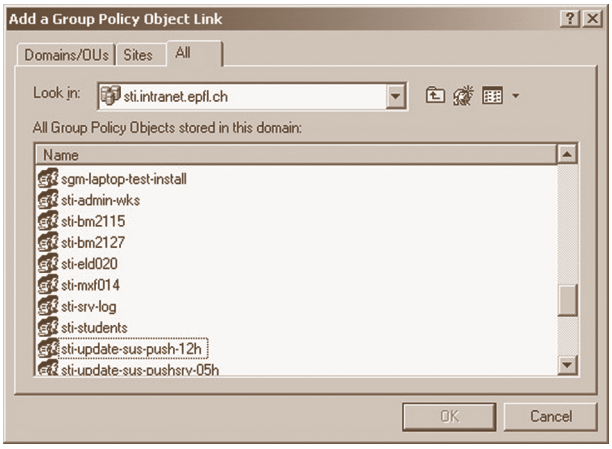
1. Sélectionner l'OU contenant les ordinateurs concernés, click droit, menu Properties



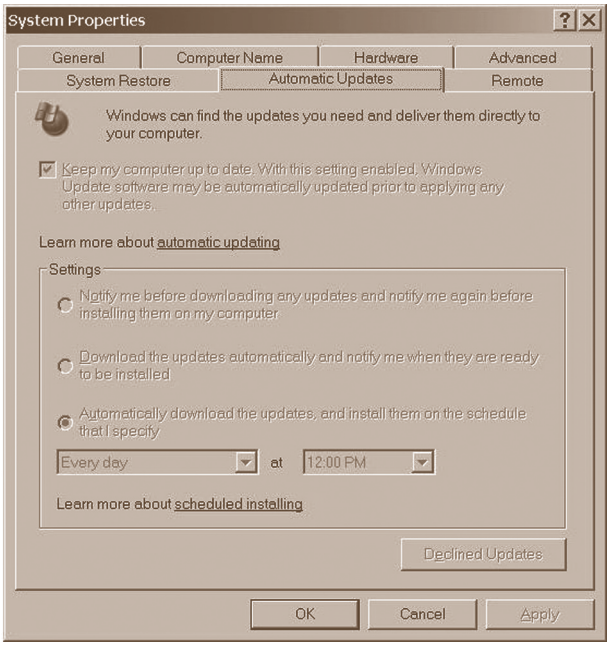
2. Dans la fenêtre des propriétés de l'OU, sélectionner l'onglet Group Policy, bouton Add



3. Et finalement, dans l'onglet All, sélectionner la GPO adaptée à notre besoin, puis bouton OK



4. Le résultat sur le panneau de configuration des mises à jour automatiques



Après l'application de la stratégie de groupe (GPO), les paramètres sont grisés

Les paramètres de ces configurations sont:

sti-update-sus-push-12h

```
Computer Configuration
  Administrative Templates
    Windows Components/Windows Update
    Configure Automatic Updates Enabled
      Configure automatic updating: 4 - Auto
              download and schedule the install
        The following settings are only requi-
          red and applicable if 4 is selected.
      Scheduled install day:  0 - Every day
      Scheduled install time: 12:00
    Reschedule Automatic Updates scheduled
                          installations Enabled
      Wait after system startup(minutes):  5
    Specify intranet Microsoft update service
                                 location Enabled
      Set the intranet update service for de-
        tecting updates: http://128.178.18.101
      Set the intranet statistics server:
                          http://128.178.18.101
        (example: http://IntranetUpd01)
```

sti-update-sus-pushsrv-05h

```
Computer Configuration
  Administrative Templates
    Windows Components/Windows Update
    Configure Automatic Updates Enabled
      Configure automatic updating: 4 - Auto
            download and schedule the install
        The following settings are only requi-
          red and applicable if 4 is selected.
      Scheduled install day:  0 - Every day
      Scheduled install time: 05:00
    No auto-restart for scheduled Automatic
                Updates installations Enabled
    Reschedule Automatic Updates scheduled
                        installations Enabled
      Wait after system startup(minutes):  5
    Specify intranet Microsoft update service
                              location Enabled
      Set the intranet update service for de-
        tecting updates: http://128.178.18.101
      Set the intranet statistics server:
                        http://128.178.18.101
        (example: http://IntranetUpd01)
```

Les paramètres sont explicites, j'aimerais attirer l'attention sur les éléments suivants:

`Configure automatic updating: 4 - Auto download and schedule the install`

Cette option est obligatoire, car c'est la seule qui permet la mise à jour de la machine sans que l'usager possède un accès administrateur ou soit connecté. Elle entraîne la définition de deux paramètres supplémentaires: le jour de la semaine et l'heure où a lieu l'installation.

`Reschedule Automatic Updates scheduled installations Enabled`

Permet le lancement du processus dans le cas ou la machine est éteinte au moment prévu.

`No auto-restart for scheduled Automatic Updates installations Enabled`

C'est le seul paramètre (avec l'heure de mise à jour) qui diffère entre la version pour serveur et celle des postes de travail. Si on active ce paramètre, la machine ne redémarre pas automatiquement (utile pour un serveur). Dans le cas contraire, l'ordinateur redémarre en avertissant l'usager avec un délai de 5 minutes après la mise à jour.

`Specify intranet Microsoft update service location Enabled`

Ceci est un point crucial de Windows Update, il définit le serveur à utiliser. La documentation de SUS, propose, l'utilisation du nom NetBios de l'ordinateur comme nom du serveur. Après l'essai de celui-ci, puis du nom DNS statique, puis du nom DNS dynamique, il apparaît que l'utilisation de l'adresse IP est la seule méthode qui garantisse la connexion entre les clients et le serveur. Cette précaution peut vous éviter de chercher pourquoi SUS ne fonctionne pas correctement ! Après une recherche approfondie sur le Net, il apparaît que le problème est issu de la version 1.0 de BITS qui nécessite un transfert avec le protocole NetBios. Cette dépendance n'existera plus avec la nouvelle version 1.5 de BITS
NB: ne pas faire suivre l'adresse du serveur par un /

Comme la GPO est du type machine, elle sera effective après application sur l'OU désirée, dès le temps de réplication des contrôleurs de domaine (délai maximum de 30 minutes) et redémarrage de l'ordinateur concerné. La dernière étape du processus est de vérifier si le travail a été effectué sur l'ordinateur concerné. Il suffit de lire le contenu du fichier **%systemroot%\Windows Update.log**:

L'utilisation de Windows Update avec la technologie Akamai pour limiter le flux vers Microsoft (et prévenir un déni de service)

```
2003-08-16 05:51:11  Success   IUCTL          Starting
2003-08-16 05:51:11  Success   IUCTL          Downloaded iuident.cab from http://windowsupdate.micr
osoft.com/v4/ to C:\Program Files\WindowsUpdate\V4
2003-08-16 05:51:11  Success   IUCTL          Checking to see if new version of Windows Update
software available
2003-08-16 05:51:11  Success   IUENGINE       Starting
2003-08-16 05:51:11  Success   IUENGINE       Determining machine configuration
2003-08-16 05:51:12  Success   IUENGINE       Querying software update catalog from https://
a248.e.akamai.net/v4.windowsupdate.microsoft.com/autoupdate/getmanifest.asp
2003-08-16 05:51:12  Success   IUENGINE       Determining machine configuration
2003-08-16 05:51:12  Success   IUENGINE       Querying software update catalog from https://
a248.e.akamai.net/v4.windowsupdate.microsoft.com/autoupdate/getmanifest.asp
2003-08-16 05:51:12  Success   IUENGINE       Determining machine configuration
2003-08-16 05:51:13  Success   IUENGINE       Querying software update catalog from https://
a248.e.akamai.net/v4.windowsupdate.microsoft.com/autoupdate/getmanifest.asp
2003-08-16 05:51:13  Success   IUENGINE       Determining machine configuration
2003-08-16 05:51:14  Success   IUENGINE       Querying software update catalog from https://
a248.e.akamai.net/v4.windowsupdate.microsoft.com/autoupdatedrivers/getmanifest.asp
2003-08-16 05:51:14  Success   IUENGINE       Shutting down
2003-08-16 05:51:14  Success   IUCTL          Shutting down
```

L'utilisation de SUS

Récupération du catalogue de mise à jour, 18h00..

```
2003-10-07 18:00:56  Success   IUCTL          Starting
2003-10-07 18:01:03  Success   IUCTL          Downloaded iuident.cab from http://128.178.18.101 to
C:\Program Files\WindowsUpdate\V4
```

Détermination des mises à jour, 18h01...

```
2003-10-07 18:01:03  Success   IUENGINE       Starting
2003-10-07 18:01:03  Success   IUENGINE       Determining machine configuration
2003-10-07 18:01:12  Success   IUENGINE       Querying software update catalog from http://
128.178.18.101/autoupdate/getmanifest.asp
2003-10-07 18:01:12  Success   IUENGINE       Determining machine configuration
2003-10-07 18:01:12  Success   IUENGINE       Querying software update catalog from http://
128.178.18.101/autoupdate/getmanifest.asp
2003-10-07 18:01:12  Success   IUENGINE       Determining machine configuration
2003-10-07 18:01:12  Success   IUENGINE       Querying software update catalog from http://
128.178.18.101/autoupdate/getmanifest.asp
2003-10-07 18:01:13  Success   IUENGINE       Determining machine configuration
2003-10-07 18:01:13  Success   IUENGINE       Querying software update catalog from http://
128.178.18.101/autoupdate/getmanifest.asp
2003-10-07 18:01:13  Success   IUENGINE       Shutting down
2003-10-07 18:01:13  Success   IUCTL          Shutting down
```

Récupération des rustines avec BITS, le lendemain, 10h11

```
2003-10-08 10:11:29  Success   IUCTL          Starting
2003-10-08 10:11:30  Success   IUENGINE       Starting
2003-10-08 10:11:32  Success   IUENGINE       Shutting down
2003-10-08 10:11:32  Success   IUCTL          Shutting down
```

La suite, 10h54

```
2003-10-08 10:54:20  Success   IUCTL          Starting
2003-10-08 10:54:20  Success   IUENGINE       Starting
2003-10-08 10:54:20  Success   IUENGINE       Shutting down
2003-10-08 10:54:20  Success   IUCTL          Shutting down
```

La suite, 12h05

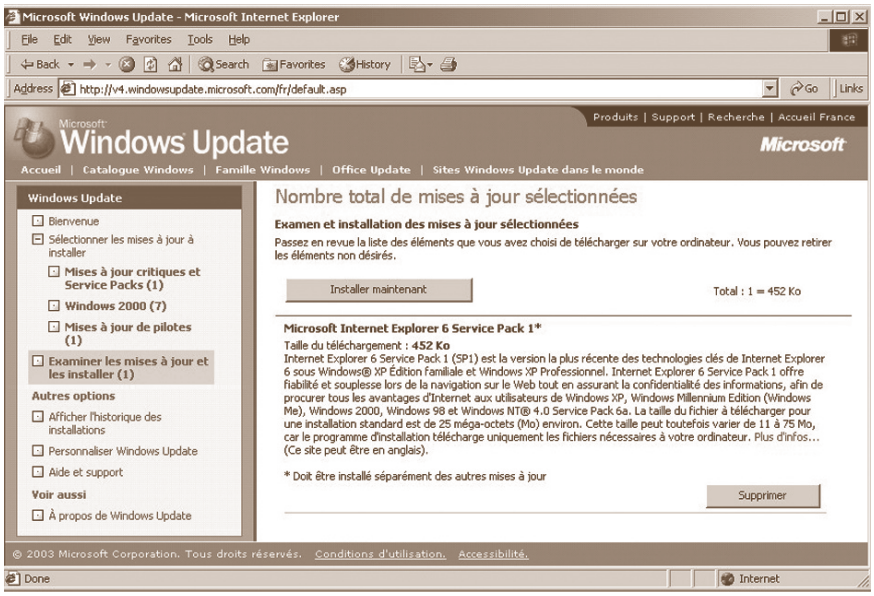
```
2003-10-08 12:05:00  Success   IUCTL          Starting
2003-10-08 12:05:00  Success   IUENGINE       Starting
2003-10-08 12:05:00  Success   IUCTL          Starting
2003-10-08 12:05:00  Success   IUENGINE       Starting
2003-10-08 12:05:00  Success   IUENGINE       Shutting down
2003-10-08 12:05:00  Success   IUCTL          Shutting down
```

Installations des rustines, 12h05

```
2003-10-08 12:05:01  Success   IUENGINE       Install started
2003-10-08 12:05:01  Success   IUENGINE       Installing SOFTWARE item from publisher com_microsoft
2003-10-08 12:05:01  Success   IUENGINE       Installer Command Type: EXE
2003-10-08 12:05:16  Success   IUENGINE       Installing SOFTWARE item from publisher com_microsoft
2003-10-08 12:05:16  Success   IUENGINE       Installer Command Type: EXE
2003-10-08 12:05:31  Success   IUENGINE       Installing SOFTWARE item from publisher com_microsoft
2003-10-08 12:05:31  Success   IUENGINE       Installer Command Type: EXE
2003-10-08 12:05:39  Success   IUENGINE       Installing SOFTWARE item from publisher com_microsoft
2003-10-08 12:05:39  Success   IUENGINE       Installer Command Type: EXE
2003-10-08 12:05:43  Success   IUENGINE       See iuhist.xml for details: Install finished
2003-10-08 12:05:43  Success   IUENGINE       Shutting down
2003-10-08 12:05:43  Success   IUCTL          Shutting down
```

Les deux processus de Windows Update sont bien séparés:

- mise à jour du catalogue et comparaison avec le système existant, puis récupération des rustines avec BITS;
- installation à l'heure prédéfinie (12h00) des rustines.



Windows Update, après l'application de la GPO, et sa mise à jour automatique.

Client IP	Date and Time	Information
128.178.113.54 **lmcpc16.epfl.ch**	29.10.2003 00:26:32	Client ID: ba896d88b251e0448b1591fd875be570 Client Function: Initialized Activity: Initialization Item: None Platform ID: Windows 2000 Status: Succeeded Error: **No Errors Recorded** Message ID: None Time Stamp: 031029002632347
128.178.113.54 **lmcpc16.epfl.ch**	29.10.2003 00:26:39	Client ID: ba896d88b251e0448b1591fd875be570 Client Function: Download Activity: Detection Item: None Platform ID: Windows 2000 Status: Succeeded Error: **No Errors Recorded** Message ID: items%3D0 Time Stamp: 031029002639425
128.178.153.207 **cmipc26.epfl.ch**	29.10.2003 00:57:27	Client ID: dcaeae3ba3fe51419913c7aae7331502 Client Function: Initialized Activity: Initialization Item: None Platform ID: Windows 2000L=fr-FR Status: Succeeded Error: **No Errors Recorded** Message ID: None Time Stamp: 031029005727867
128.178.153.207 **cmipc26.epfl.ch**	29.10.2003 00:57:33	Client ID: dcaeae3ba3fe51419913c7aae7331502 Client Function: Download Activity: Detection Item: None Platform ID: Windows 2000L=fr-FR Status: Succeeded Error: **No Errors Recorded** Message ID: items%3D0 Time Stamp: 031029005733615
128.178.153.86 **cmipc10.epfl.ch**	29.10.2003 01:03:41	Client ID: 1530fcfffedd184f80608c43aa64527f Client Function: Initialized Activity: Initialization Item: None Platform ID: Windows 2000L=fr-FR Status: Succeeded Error: **No Errors Recorded** Message ID: None Time Stamp: 031029010342096
128.178.153.86 **cmipc10.epfl.ch**	29.10.2003 01:03:45	Client ID: 1530fcfffedd184f80608c43aa64527f Client Function: Download Activity: Detection Item: None Platform ID: Windows 2000L=fr-FR Status: Succeeded Error: **No Errors Recorded** Message ID: items%3D0 Time Stamp: 031029010345643
128.178.108.80 **imxatpc1.epfl.ch**	29.10.2003 01:39:29	Client ID: 7fd536478bdc634f837f8575fd757d49 Client Function: Initialized Activity: Initialization Item: None Platform ID: Windows XP Status: Succeeded Error: **No Errors Recorded** Message ID: None Time Stamp: 031029013928846
128.178.108.80 **imxatpc1.epfl.ch**	29.10.2003 01:39:39	Client ID: 7fd536478bdc634f837f8575fd757d49 Client Function: Download Activity: Detection Item: None Platform ID: Windows XP Status: Succeeded Error: **No Errors Recorded** Message ID: items%3D0 Time Stamp: 031029013939697
128.178.47.63	29.10.2003	Client ID: 76de9aacd3ab33468acb25e342250888 Client Function: Initialized

Il est également possible d'étudier le contenu de l'activité Web du serveur SUS. Ces fichiers au format *W3C Extended Log* ne sont pas très lisibles.

Heureusement, Robert McBride, ***mcbweb@midthought.com***, a écrit un script ASP qui permet de représenter ces informations sous un format plus compréhensible. Le script est diponible a l'URL:
www.midthought.com/viewtopic.asp?forumid=28&id=386

Malgré, cette mise à jour périodique, il est tout à fait possible d'utiliser Windows Update avec un compte administrateur.

Conclusion

Ce nouveau service à l'intérieur du domaine Active Directory de la Faculté STI, offre un mécanisme simple et décentralisé pour assurer une mise à jour automatique des rustines de sécurité et des Services Pack.

Il est judicieux de mettre en place un mécanisme similaire pour la protection contre les virus ; je suggère d'utiliser ePO (article de Christian Raemy dans le FI 6/03, ***http://dit.epfl.ch/publications/FI03/fi-6-3/6-3-page1.html***).

On pourrait penser que notre travail sur le plan de la sécurité est terminé. En fait, il n'en est rien, car le principal problème reste l'utilisation de l'ordinateur, en particulier la tendance de l'usager d'essayer tout logiciel qui passe à sa portée. Parfois ils peuvent incorporer des Spyware ou pire encore un cheval de Troie. Un ver ou un virus visibles sont désagréables, les mêmes, sans incidence visible, sont nettement plus dangereux.

La solution réside en une éducation des usagers pour que l'utilisation de l'ordinateur reste ludique. ■