

# La Sécurité de vos applications et Services Microsoft ou comment automatiser la gestion, le support et la maintenance d'un réseau Windows

Djélani BABA

Centre d'Immunologie de Marseille Luminy (CIML) - UMR 6102

baba@ciml.univ-mrs.fr

## Résumé

*Avec Windows NT, la configuration par défaut en faisait un système dont la sécurité était insuffisante pour assurer l'exploitation d'un parc informatique. Depuis l'arrivée de Windows 2000, les efforts de Microsoft vis-à-vis de la sécurité se sont améliorés et l'on peut affirmer aujourd'hui que Windows Serveur 2003, successeur de Windows 2000, est le système d'exploitation le plus sécurisé jamais publié par Microsoft. Est-ce suffisant ? Sûrement pas. C'est pourquoi ce dernier met à disposition des outils comme WSUS (gestion des correctifs), SMS (gestion de configuration des postes et serveurs) et MOM (solution de supervision) qui ont pour but d'aider les administrateurs à améliorer la sécurité de leurs systèmes car comme chacun de nous le sait une fiabilité à 100% d'un système d'exploitation est utopique et que tout système a ses faiblesses que des comportements déviants chercheront toujours à découvrir et à exploiter.*

## Mots clefs

SP, QFE, MBSA, Correctifs, MOF, SUS, WSUS, SMS, MOM, SECURITE WINDOWS

## 1 Introduction

Chacun d'entre nous a en mémoire le bulletin de sécurité MS03-026 (Buffer Overrun in RPC Interface Could Allow Code Execution) que Microsoft avait publié avant même que le ver Blaster soit le 11 août 2003 fasse des dégâts. La propagation de ce ver a démontré que beaucoup d'administrateurs n'avaient pas fait ce qu'il fallait pour protéger leurs systèmes. Depuis l'avènement de ce ver, des éditeurs comme Microsoft proposent des outils simples d'emploi, qui permettent non seulement de contrôler et d'automatiser la distribution des correctifs, mais aussi de gérer et de superviser de manière très simple son environnement informatique. Nous allons vous présenter 3 de ces outils que nous avons déployés au Centre d'Immunologie de Marseille Luminy (CIML). L'environnement dans lequel nous avons déployé ces 3 outils est le suivant : 15 serveurs (contrôleurs de domaine Windows 2003, serveurs DNS, serveurs Web, serveur de messagerie Exchange, serveurs de bases de données SQL Server, serveurs de fichiers, serveurs d'applications etc...), 200 postes de travail sous différentes versions et

langues de Windows. Toute la gestion du parc est assurée par deux personnes.

### 1.1 Déploiement automatisé des services Packs et correctifs (WSUS ex SUS)

Pour suivre le rythme des mises à jour publiées par l'éditeur de Redmond, l'administrateur peut utiliser WSUS (Windows Server Update Services). Il est facile à implémenter et constitue une solution efficace de gestion de correctifs dans la plupart des cas. Il utilise la même technologie que Microsoft utilise depuis des années pour son site Windows Update public. Il permet de contrôler la gestion des correctifs et de maintenir à jour son environnement Microsoft grâce à une télédistribution automatique des patches.

Microsoft a sorti WSUS pour palier aux limites de SUS car ce dernier, pour ceux qui l'ont déjà déployé savent qu'il comportait plusieurs limites :

- ne prend en charge que les mises à jour critiques ou de sécurité de Windows
- pas de mise à jour des drivers
- pas de mise à jour des Services Packs
- pas de mise à jour d'applications
- n'offre pas la possibilité de faire une désinstallation.

Comme son prédécesseur, WSUS est un outil destiné à de petites structures. C'est une solution complète pour télécharger et distribuer les mises à jour des produits Microsoft critiques ou non et qui fournit un rapport centralisé. Il couvre les systèmes et les applications et à terme il prendra en charge tous les produits Microsoft.

### 1.2 Gestion de configuration des postes de travail et des serveurs Windows (SMS 2003)

Microsoft a conçu SMS (System Management Server) pour assurer :

- La gestion des Ressources Informatiques
  - Découverte
  - Inventaire matériels et logiciels
  - Reporting
- La gestion du cycle de vie des applications et des correctifs de sécurité
  - Packaging
  - Distribution des logiciels

- Installation automatique des logiciels
- Gestion de la sécurité
- Suivi d'utilisation et mise à jour
- La télé-assistance (contrôle à distance des machines)

Cet outil permet également, la gestion des ordinateurs à partir de lieux géographiques différents. Les mises à jour logicielles de SMS 2003 sont tout aussi efficaces dans les laboratoires comptant des multiples sites et de multiples serveurs dans chaque site.

### 1.3 Supervision et gestion des serveurs et applicatifs Windows (MOM 2005)

Alors que SMS est dédié à la gestion des configurations des postes et serveurs Windows, MOM (Microsoft Operations Manager) permet la surveillance de l'ensemble du parc informatique de façon préventive. Il permet de surveiller l'ensemble des serveurs Windows (état, disponibilité et performances) sans que l'on soit obligé de se connecter sur les dits serveurs.

Avec MOM, Microsoft est parti d'un constat assez simple : Quel que soit le rôle d'un serveur, 80% des paramètres d'optimisation sont identiques d'un serveur à l'autre. En plus chaque équipe de développeurs d'un produit est responsable du développement des règles liées à la supervision de son produit. MOM intègre donc ces 80% en un jeu de règles pour en faire un « **serveur idéal** » et vous notifie ou réagit dès que le serveur s'écarte de ce modèle. L'application de ce modèle aux serveurs nous permet de nous concentrer sur les 20 % de réglages spécifiques à notre situation et à nos besoins. Avant d'intégrer d'autres plates formes, MOM 2005 est essentiellement une solution serveur Windows. Les laboratoires qui disposent de beaucoup de serveurs UNIX ou LINUX jugeront peut être qu'une solution tierce est plus adaptée à leur environnement

Nous allons vous présenter comment utiliser ces 3 outils pour optimiser et gérer efficacement et en un minimum de temps votre parc Windows. Tous ces outils peuvent s'automatiser et permettre à l'administrateur de dégager du temps pour des tâches à forte valeur ajoutée, sans perdre son temps à réécrire les mêmes scripts et réinventer la roue.

Des exemples concrets illustrent la mise en place de cette architecture dans notre laboratoire

## 2 Outils Microsoft pour la gestion des correctifs

Avant de déployer les correctifs, il est nécessaire de faire la différence entre un Service Pack (SP), un Quick Fix Engineering (QFE) et un correctif de sécurité.

- Les SP permettent :

- d'apporter des mises à jour,
- de corriger les problèmes connus,
- d'étendre les fonctionnalités.

En quelque sorte ce sont des améliorations développées après la publication du produit. Les Services Packs sont propres à un produit et à chaque produit correspond donc une série distincte de SP. Toutefois le même SP est généralement utilisé pour différentes versions d'un même produit. Par exemple le même SP sert à mettre à jour W2000 serveur et W2000 Professionnel. Les SP sont cumulatifs : tout nouveau SP contient les correctifs des précédents et les nouvelles modifications. On peut donc installer le dernier SP sans que les versions précédentes le soient.

- QFE est un groupe de Microsoft qui produit des correctifs logiciels :

Ces correctifs sont fournis uniquement pour résoudre des problèmes bloquants.

Ils ne sont pas soumis à des tests de régression intensifs et ne s'appliquent qu'à des problèmes spécifiques. Vous ne devez donc utiliser un correctif logiciel que si vous rencontrez exactement le même problème qu'il corrige et utiliser la version logicielle en cours avec son dernier SP. *Des groupes de correctifs logiciels sont souvent incorporés aux SP et dans ce cas ils subissent des tests plus rigoureux.*

- Les correctifs de sécurité ont pour but uniquement d'éliminer les vulnérabilités de sécurité :

Leurs publications concernent des problèmes rencontrés par des applications clientes (exemple des navigateurs) et elles ne sont pas pertinentes pour l'installation des serveurs.

### 2.1 Gestion des correctifs

La manière de mettre en œuvre la gestion des correctifs dépend largement de la taille et de la complexité de son environnement informatique. On ne peut donc gérer correctement la sécurité de son environnement que si l'on connaît de manière détaillée son état actuel.

Pour assurer la gestion des correctifs, il faut évaluer son environnement et savoir répondre au minimum aux questions suivantes :

- De quels systèmes est constitué son laboratoire ? (Système d'exploitation et version, niveau des correctifs, etc...)
- Quelles sont les menaces connues ?

- Quelles sont les vulnérabilités connues ?
- Quelle contre-mesures avez-vous déployé ?

Si vous pouvez répondre à ces questions, vous pourrez déterminer quelles menaces et vulnérabilités vont poser problème à votre système informatique. Le guide Microsoft de gestion des correctifs téléchargeable sur le site de Microsoft à l'adresse suivante : <http://www.microsoft.com/france/technet/securite/guidance/default.mspx> décrit les différentes tâches associées à chaque étape du processus de gestion des correctifs :

- 1<sup>ère</sup> étape : évaluer l'environnement auquel le correctif doit être appliqué
- 2<sup>ème</sup> étape : identifier les nouveaux correctifs et déterminer leurs pertinences
- 3<sup>ème</sup> étape : estimer et planifier le déploiement des correctifs. Lorsque vous prenez connaissance d'une vulnérabilité, vous devez vous demander si elle concerne votre système. Par exemple une vulnérabilité du service File Transfert Protocol (FTP) de Windows 2000 ne vous concerne pas forcément si vous n'activez jamais ce service. Si vous réagissez à des ressources et des vulnérabilités qui ne s'appliquent pas réellement à votre cas, vous consommez inutilement des ressources.
- 4<sup>ème</sup> étape : déployer les correctifs

Ces instructions relatives aux processus font partie du Microsoft Operations Framework (MOF) qui s'appuie sur les méthodes conseillées et codifiées dans l'ITIL (Information Technology Infrastructure Library) qui est la norme des méthodes conseillées des technologies de l'information.

La première étape de la gestion des correctifs passe par l'analyse de l'environnement auquel le correctif doit être appliqué. Nous avons utilisé les produits Microsoft suivants :

\* MBSA (Microsoft Baseline Security Analyzer) qui permet aux administrateurs d'évaluer des systèmes par rapport à une référence de sécurité afin d'identifier les correctifs de sécurité manquants et certains problèmes de configuration de la sécurité. Une interface utilisateur graphique (GUI) et une interface ligne de commande sont disponibles. Cet outil est disponible en téléchargement gratuit sur le site de Microsoft. La dernière version est disponible à l'adresse suivante : <http://www.microsoft.com/technet/security/tools/mbsahome.mspx>

\* vérification de la base de registre : `HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Hotfix` : (exemple Qxxxxxx où xxxxxx fait référence à l'article de la Base de Connaissance qui traite du correctif en question)

\* utilisation de la commande `Qfecheck.exe /v` qui indique le niveau de Service Pack et les correctifs installés. Il signale également les correctifs qui n'ont pas été installés correctement.

\* utilisation de la commande `Hotfix.exe -l` qui affiche les correctifs logiciels installés.

Lorsqu'un nouveau correctif est créé, il faut évaluer son importance car cela permettra de déterminer s'il est urgent de le déployer ou non. Microsoft fournit une évaluation des différentes vulnérabilités et son équipe Microsoft Security Response Center (MSRC) affecte un niveau de gravité à chaque correctif publié dans un bulletin de sécurité.

Les classes de vulnérabilité définies par Microsoft sont les suivantes :

- *Critique* : l'exploitation de cette vulnérabilité peut permettre la propagation d'un ver, tel que Code Red ou Nimda sans intervention de l'utilisateur.
- *Important* : l'exploitation de cette vulnérabilité peut toucher à la confidentialité, l'intégrité et la disponibilité des données.
- *Moyen* : les conséquences de cette vulnérabilité sont sérieuses mais souvent atténuées par exemple par la configuration par défaut ou d'autres facteurs comme la nécessité d'une intervention utilisateur.
- *Faible* : l'impact de cette vulnérabilité est minime.

Evidemment en fonction de cette évaluation, le délai d'application des correctifs varie et on peut s'inspirer de ce tableau fourni par Microsoft qui conseille un délai dans l'application d'un correctif en fonction de son niveau de criticité :

	<i>Délai conseillé d'application des correctifs</i>	<i>Délai d'application maximum recommandé</i>
critique	Dans les 24 heures	Dans les deux semaines
important	Dans le mois	Dans les 2 mois
moyen	attendez le prochain Service Pack ou la prochaine mise à jour qui comprend le correctif, sinon déployer le correctif dans les 4 mois	Déployer la mise à jour dans les 6 mois
faible	attendez le prochain Service Pack ou la prochaine mise à jour qui comprend le correctif, sinon déployer le correctif dans l'année	Déployer le correctif dans l'année ou choisissez de ne pas le déployer du tout

Grâce à cette classification, nous savons exactement quand il faut déployer un correctif et dans quel délai.

En règle générale, il faut appliquer toute mise à jour proposée par Windows Update et Microsoft Office Update pour des laboratoires moyens. Pour des gros laboratoires, identifier les correctifs les plus appropriés. Un correctif de sécurité doit souvent être installé rapidement pour éviter des problèmes graves. Le cycle de vie d'une vulnérabilité est composé de 6 phases qui sont :

1. La vulnérabilité est signalée et seuls Microsoft et l'auteur du rapport en ont connaissance (en règle générale la firme de Redmond ne confirme jamais les vulnérabilités)
2. Un correctif est mis au point. Au cours du développement et du test du correctif, seuls Microsoft et l'auteur du rapport ont connaissance de la vulnérabilité. D'ailleurs à ce stade si la vulnérabilité était rendue publique, les intrus disposeraient des mêmes informations que Microsoft.
3. Un bulletin de sécurité et un correctif sont publiés. La vulnérabilité est maintenant connue de tous, mais le mécanisme utilisé pour l'exploiter ne l'est pas. Les intrus éventuels sont informés de la vulnérabilité et le correctif doit être distribué avant qu'ils ne puissent lancer d'attaques.
4. La logique du correctif est reconstituée. Une fois le correctif publié, la logique du code est rapidement reconstituée et le mécanisme d'exploitation tout aussi découvert.
5. Le code du ver ou du virus est créé. A ce stade, le mécanisme d'attaque existe mais n'a pas encore été lancé.
6. Le code du ver ou du virus est activé. Une fois le ver ou le virus lancé, les systèmes non protégés ou non équipés d'un correctif sont rapidement infectés.

En fonction de ce cycle, nous voyons bien que nos systèmes doivent être protégés à partir du moment où le bulletin de sécurité a été publié. Le laps de temps entre le signalement d'une attaque et la mise à disposition du correctif adapté est très variable. Les exemples dans le tableau suivant montrent que, dans tous les cas, une gestion préventive des correctifs de sécurité peut éviter des vulnérabilités avant qu'elles ne soient exploitées par les pirates.

<i>Virus</i>	<i>Détection publique</i>	<i>Niveau gravité MSRC</i>	<i>Date bulletin MSRC</i>	<i>jours avant attaque</i>
Trojan-Kaht	5/05/03	Critique	17/03/03	49
SQL Slammer	24/01/03	Critique	24/07/02	184
Klez-E	17/01/02	N/A	29/03/01	294
Nimda	18/09/01	N/A	17/10/00	336
CodeRed	16/07/01	N/A	18/06/01	28

Les correctifs Microsoft peuvent être déployés de façon manuelle ou quasi automatique. Nous avons utilisé les deux méthodes au Centre d'Immunologie et depuis l'arrivée de SUS et de son successeur WSUS, nous avons abandonné la procédure manuelle car celle ci est vite devenue ingérable pour notre environnement.

## 2.2 Déploiement manuel des correctifs

La procédure manuelle passe par l'installation de l'exécutable sur chaque machine ou serveur non protégé. Le nom du correctif est souvent riche d'information. Exemple : *WindowsXP-KB873376-x86-enu.exe* (*KB873376* est le numéro de l'article dans la base de connaissances, *WindowsXP* est le produit auquel le correctif est destiné, *x86* l'architecture du processeur et enfin *Enu* la langue concernée). Il arrive des fois que le correctif soit de la forme *KBxxxxx.exe*, dans ce cas il est en général propre aux applications tels que Internet Explorer (IE).

Plusieurs commutateurs peuvent être employés avec l'exécutable :

- y pour effectuer une désinstallation
- f pour forcer la fermeture des applications lors de l'arrêt
- n pour ne pas créer de répertoire de désinstallation
- z empêche le démarrage à la fin de la mise à jour
- q installation en mode silencieux
- m mode sans assistance
- l dresse une liste des correctifs installés

Les correctifs propres à une application ne prennent pas généralement en charge les commutateurs ci-dessus. En règle générale après chaque correctif on est invité à rebooter sa machine car les fichiers qui sont verrouillés ou en cours d'utilisation ne peuvent être remplacés. Si on a donc plusieurs correctifs à mettre sur une machine, on peut utiliser l'utilitaire *QChain* qui permet d'enchaîner plusieurs correctifs et de redémarrer une seule fois.

Pour cela il suffit d'exécuter le programme d'installation de chaque correctif avec le commutateur *-z* pour que la machine ne démarre pas et ensuite lancer *QChain.exe* et rebooter la machine.

Avant de déployer les correctifs, les outils d'analyse (MBSA, Outil d'inventaire Office), les services de mise à jour en ligne (Windows Update, Office Update) permettent d'analyser son environnement.

L'outil MBSA évoqué un peu plus haut permet d'évaluer les systèmes par rapport à une référence de sécurité donné pour identifier les correctifs de sécurité manquants et certains problèmes de configuration de la sécurité. Cet outil nous avait permis d'analyser un ou plusieurs ordinateurs à la fois et fonctionne sur des logiciels et systèmes Microsoft très divers (Windows NT, 2000, 2003, XP, IIS toutes versions, SQL 7 et 2000, IE,

lecteur Media Player etc...) que nous utilisons au Centre d'Immunologie.

Son fonctionnement est assez simple : au lancement de MBSA, ce dernier télécharge à partir du centre de téléchargement Microsoft un fichier CAB qui contient *MSSecure.xml* et vérifie sa signature numérique. Ce fichier qui peut être copié sur les ordinateurs locaux contient les informations suivantes :

- Nom des bulletins de sécurité
- Mise à jour spécifique des produits
- Information des versions
- Clés des registres modifiés
- Numéros d'articles de la base de connaissances Microsoft

Il analyse le système d'exploitation et ses composants ainsi que les applications des systèmes cibles. Il examine le fichier *MSSecure* pour voir si des mises à jour sont disponibles et contrôle le système pour voir si des mises à jour requises sont manquantes. Enfin il génère un rapport contenant la liste des mises à jour absentes du système. Cet outil s'utilise selon deux méthodes :

- Mode GUI : des bons résultats pour des réseaux de petite taille
- Mode ligne de commande permet d'effectuer des analyses automatisées en utilisant les paramètres de ligne de commande. Exemple *mbsacli /d MonDomaine /f rapport.txt*. Utilisé en mode *HFNetChk* il génère un rapport détaillé des correctifs manquants sur chaque ordinateur, ce qui vous permet de créer un rapport (liste délimité par des tabulations) des ordinateurs vulnérables.

Quelques exemples de ligne de commande :

```
Mbsacli /r « 10.1.1.1-10.1.1.254 » /wus  
http://NomServeurWSUS /n « SQL » /n  
« \\MonServeur\Partage\rapport.txt »
```

cette commande analyse tous les ordinateurs dont l'adresse IP est comprise dans la plage 10.1.1.1 à 10.1.1.254 par rapport à la liste de mises à jour approuvées du serveur WSUS nommé MonServeurWSUS. Cette commande n'effectue pas l'analyse SQL. Le fichier résultat qui s'appelle rapport.txt sera stocké sur un partage réseau sur le serveur nommé MonServeur.

## 2.3 Déploiement automatique des correctifs avec Windows Server Update Services (WSUS)

Comme beaucoup d'entre vous, notre laboratoire a d'abord commencé à utiliser Microsoft Update. Si ce dernier convient parfaitement aux petites structures, il s'avère inadapté dès que le nombre de postes devient conséquent. Dès sa sortie, nous avons utilisé SUS depuis 2 ans ce qui nous a permis de contrôler le flux des patches

appliqués aux systèmes. Malheureusement ce système a présenté pas mal de limites dans notre environnement (ne prend pas en compte la désinstallation des patches, ne supporte pas certains produits Microsoft que nous utilisons). L'arrivée de WSUS avec ses principales améliorations nous a permis d'alléger considérablement le fardeau du déploiement des patches sur tous les produits Microsoft de notre laboratoire.

Proposé en téléchargement gratuit sur le site de l'éditeur, il offre une palette de fonctionnalité beaucoup plus impressionnante que SUS. Non seulement il déploie des correctifs qui vont au-delà du simple logiciel basé sur Windows, il est fondé aussi sur la nouvelle infrastructure Microsoft Update qui fournit des correctifs pour tous les produits Microsoft tels SQL, Exchange, Office, IIS présents au CIML.

### Nouveautés dans WSUS

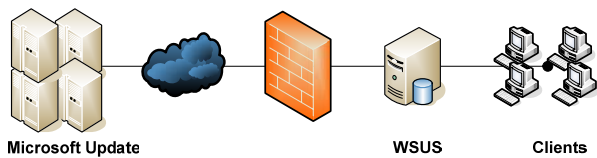
- Supporte plusieurs produits Microsoft (Office, SQL, Exchange...). A terme il couvrira tous les produits Microsoft.
- Possibilité de télécharger les mises à jour par produit ou par type
- Plusieurs langues supportées
- Utilise le service de transfert intelligent en arrière plan BITS (Background Intelligent Transfer Service) dans sa version 2. C'est une technologie Microsoft qui permet à des programmes de télécharger des fichiers en employant la largeur de bande disponible.
- Possibilité de cibler des mises à jour à des ordinateurs spécifiques ou à des groupes d'ordinateur prédéfini.
- Possibilité de vérifier si les mises à jour conviennent avant installation. (Cela se fait automatiquement pour les mises à jour critiques et de sécurité)
- Déploiements flexibles
- Plusieurs possibilités de rapports
- Extension possible par API (application programming interface)

### Scénarios de déploiement d'un serveur WSUS

Plusieurs scénarios existent pour le déploiement d'un serveur WSUS. D'un déploiement simple avec un seul serveur à un déploiement multiple avec plusieurs serveurs, en passant par une importation manuelle des mises à jour.

#### *Déploiement simple avec un seul serveur*

Le déploiement de WSUS le plus simple consiste à installer un serveur derrière le Firewall pour servir les ordinateurs sur un Intranet privé, comme illustré ci dessous.

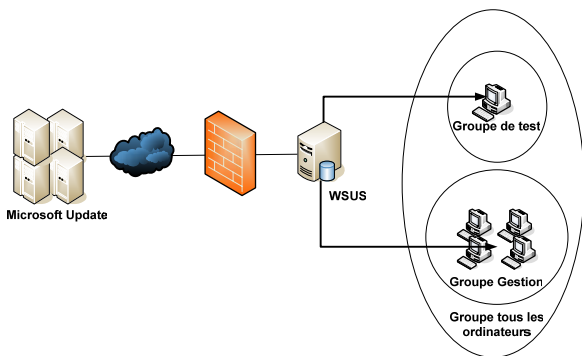


Cette configuration suffit souvent largement pour la plupart de nos laboratoires. D'ailleurs c'est ce que nous avons déployé lors du passage de SUS à WSUS. Le serveur WSUS obtient les mises à jour sur le site de Microsoft par synchronisation. Il détermine si des mises à jour sont disponibles depuis la dernière fois où il y a eu synchronisation. Lors de la première synchronisation toutes les mises à jour sont rendues disponibles pour approbation. Pour obtenir des mises à jour à partir du site Web de Microsoft, le serveur WSUS utilise les ports HTTP et HTTPS. Ces valeurs ne sont pas modifiables. Bien que cette synchronisation impose l'ouverture des ports 80 et 443, rien ne vous empêche de configurer plusieurs serveurs WSUS pour qu'ils se synchronisent via des ports personnalisés.

#### Déploiement ciblé par groupe d'ordinateurs

La notion de groupe d'ordinateurs est une donnée importante dans le déploiement de WSUS. Cette notion permet de cibler les ordinateurs sur lesquels vous souhaitez appliquer telle ou telle mise à jour.

Par défaut il y a deux groupes d'ordinateur : *Tous les ordinateurs* et *Ordinateurs non affectés*. Quand un ordinateur entre en contact avec le serveur WSUS, ce dernier l'ajoute à ces deux groupes. On peut donc déplacer tout ordinateur du *Groupe non affecté* à un groupe que l'on crée mais il est impossible d'enlever un ordinateur du groupe *Tous les ordinateurs* car ce dernier permet de viser rapidement des mises à jour à chaque ordinateur du réseau indépendamment de l'adhésion à un groupe. Par contre le groupe *Ordinateurs non affectés* permet de viser seulement les ordinateurs qui n'ont pas été assignés à un groupe. Le fait de créer des groupes d'ordinateur permet de mieux maîtriser les mises à jour comme l'illustre le schéma suivant :



Dans cet exemple deux groupes ont été créés. Groupe Test et Groupe Gestion. Cela permet d'abord d'approuver les mises à jour pour le groupe test. Si les

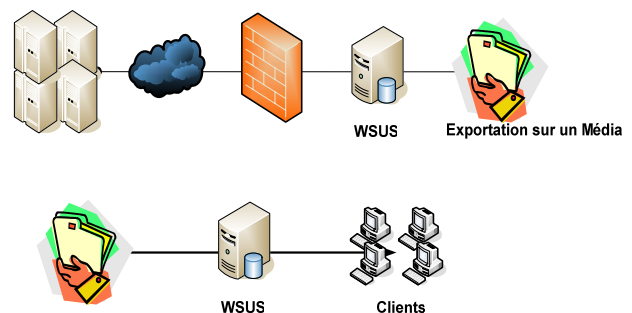
mises à jour sont concluantes, on pourra les déployer au groupe gestion. Au centre d'Immunologie nous avons créé 5 groupes d'ordinateurs différents auxquels nous appliquons des mises à jour ciblées : Groupe d'ordinateurs d'acquisition (ce sont les ordinateurs qui pilotent des appareils). Dans ce groupe seules les mises à jour de sécurité sont déployées. Groupe de portables où les mises à jour sont effectuées normalement ou par VPN. Groupe de Serveurs où les mises à jour sont installées manuellement alors que le téléchargement est automatique. Groupe Stations (sans données critiques) où les mises à jour sont automatiques et enfin Groupe Gestion où les mises à jour sont déployées uniquement s'il n'y a pas de contre indication avec les applications nationales tel XLAB. Pour les tests, nous avons installé une machine qui contient toutes les applications critiques et qui héberge aussi tous les systèmes d'exploitation que nous utilisons (à savoir Windows 2000 Professionnel, Windows 2003 Serveur et Windows XP).

#### Chaîne de serveurs WSUS

Contrairement aux déploiements simples de WSUS on peut créer des déploiements complexes avec de multiples serveurs. Quand on met plusieurs serveurs WSUS ensemble, le premier serveur ascendant se synchronise avec le serveur de Microsoft et il partage avec les serveurs descendants les mises à jour et le Metadata. Microsoft recommande un maximum de trois niveaux pour ce genre de configuration. Cela se comprend aisément car chaque niveau rajoute un temps de latence additionnel de propagation des mises à jour. Théoriquement il n'y a aucune limite quand au nombre de serveurs WSUS dans un laboratoire. Au CIML, nous n'avons qu'un seul serveur WSUS.

#### Clients déconnectés du réseau

Une autre possibilité offerte par WSUS (que nous n'avons pas déployée) et qui est très intéressante est la mise à jour des clients déconnectés du réseau. Quand vous avez des machines qui ne sont pas reliées à Internet, rien ne vous empêche de déployer WSUS dans cette configuration. Comme l'illustre l'exemple ci-dessous, il suffit d'avoir un serveur WSUS relié à l'internet mais isolé dans l'intranet. Après avoir téléchargé les mises à jour sur ce serveur, il suffira de débrancher le serveur de l'internet et de le mettre dans l'intranet en exportant et en important les mises à jour.



## Base de données pour WSUS

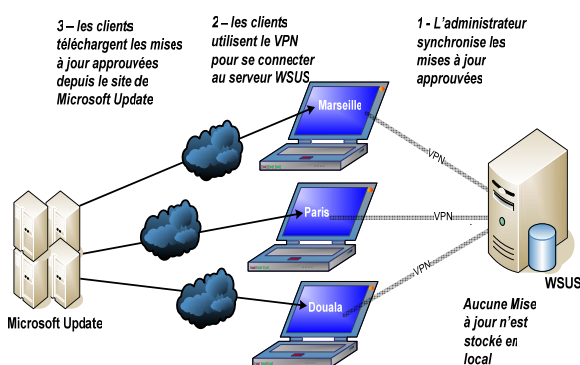
La base de données de WSUS stocke les informations suivantes :

- Information de configuration de serveur WSUS
- Metadata qui décrit ce que fait chaque mise à jour
- Informations sur les clients, les mises à jour et l'interaction entre les clients et les mises à jour.

Pour gérer ces données nous avons utilisé SQL Serveur, mais rien n'empêche d'utiliser la version gratuite de SQL qui est Microsoft Windows SQL Server Desktop Engine (WMSDE).

Dans un environnement Windows Serveur 2003, il n'y a pas de limitations quant à la taille de la base de données. Par contre dans un environnement Windows 2000 Serveur, la taille de la base de données de WMSDE est limitée à 2 Go. Pour un stockage en local, Microsoft recommande un minimum de 6 Go, mais l'idéal serait de disposer d'un espace de stockage de 30 Go.

*Remarque :* On a la possibilité de ne pas choisir un stockage local. Dans ce cas les mises à jour sont stockées sur les serveurs de Microsoft. L'administrateur configure le serveur WSUS pour approuver les mises à jour qu'il souhaite (ici la synchronisation du serveur WSUS avec le site Microsoft ne télécharge que le Metadata de mises à jour car les fichiers de mises à jour sont stockés sur le serveur de Microsoft) Cette pratique est particulièrement intéressante car vous avez la possibilité de configurer les portables pour que, dès qu'ils sont connectés par VPN sur votre serveur WSUS, ils ne téléchargent à partir du site de Microsoft que les mises à jour que vous avez approuvées et seules ces mises à jour sont installées. La figure suivante illustre ce procédé.



## Matériels recommandés :

→ Pour moins de 500 clients

Condition	Minimum	Recommandé
CPU	750 mégahertz	1 GHz ou plus
RAM	512 MB	1 GB
Base de données	WMSDE/MSDE	WMSDE/MSDE

→ De 500 à 15.000 clients

Condition	Minimum	Recommandé
CPU	1 GHz ou plus	3 GHz Biprocasseur ou plus (utiliser un biprocasseur pour 10 000 clients et plus)
RAM	1 GB	1 GB
Base de données	SQL 2000 SP3a	SQL 2000 SP3a

## 2.4 Installation et configuration du Serveur WSUS

Avant d'installer le serveur WSUS il est nécessaire d'installer, de vérifier ou de configurer les étapes suivantes :

### Configuration du Firewall

Puisque WSUS va chercher les fichiers de mises à jour à l'extérieur du laboratoire, il doit « traverser » les équipements de sécurité utilisés pour protéger le laboratoire contre les attaques extérieures. Par conséquent si un pare-feu se trouve entre le serveur WSUS et Internet, il sera peut être nécessaire de le paramétrer afin de garantir que WSUS puisse bien obtenir les mises à jour. Comme nous l'avons vu plus haut le serveur WSUS utilise les ports 80 et 443. Or ces valeurs ne sont pas modifiables. Par conséquent si votre laboratoire n'ouvre pas l'accès à ces ports ou à ses protocoles à toutes les adresses, vous pouvez restreindre l'accès seulement aux domaines suivants de sorte que le serveur WSUS puisse communiquer avec Microsoft Update :

- <http://windowsupdate.microsoft.com>
- [http://\\*.windowsupdate.microsoft.com](http://*.windowsupdate.microsoft.com)
- [https://\\*.windowsupdate.microsoft.com](https://*.windowsupdate.microsoft.com)
- [http://\\*.update.microsoft.com](http://*.update.microsoft.com)
- [https://\\*.update.microsoft.com](https://*.update.microsoft.com)
- [http://\\*.windowsupdate.com](http://*.windowsupdate.com)
- <http://download.windowsupdate.com>
- <http://download.microsoft.com>
- [http://\\*.download.windowsupdate.com](http://*.download.windowsupdate.com)
- <http://wustat.windows.com>
- <http://ntservicepack.microsoft.com>

De même si un serveur Proxy réside sur le réseau, il sera peut être nécessaire de configurer WSUS pour qu'il utilise ce serveur.

### *Installation et configuration de IIS*

Pour utiliser WSUS, il faut installer et configurer IIS. Si vous utilisez Windows 2000, il faut télécharger et installer la dernière version de IIS Lockdown pour sécuriser IIS. Avec Windows 2003, vous n'avez pas besoin de cet outil car cette fonctionnalité est incluse dans le système d'exploitation.

### *Configuration du Serveur*

Après l'installation de WSUS, la console WSUS permet sa configuration. Un site Web d'administration est créé automatiquement à l'adresse suivante <http://NomServeurWSUS/WSUSAdmin>. Par défaut il est configuré pour utiliser Microsoft Update comme emplacement de récupération des mises à jour.

Lors de la première synchronisation avec Microsoft Update, toutes les mises à jour seront disponibles et prêtes à être approuvées. C'est à partir de ce moment que vous pouvez opérer une sélection à deux niveaux (choix des patches et logiciels à télécharger).

## 2.5 Configuration des clients

Côté client, vous pouvez définir la stratégie pour la gestion des mises à jour qui dépendra, en partie, de l'architecture logique de votre réseau. Deux méthodes sont possibles :

- Paramétrage par le biais de stratégie de groupe
- Modification du registre

### *1) Stratégie de groupe (avec ou sans Active Directory)*

Dans un environnement Active Directory (AD), on pourra s'appuyer sur l'objet stratégie de groupe (GPO – Group Policy Object). Nous avons d'ailleurs utilisé cette stratégie. Si vous êtes dans une configuration non AD, vous pourrez avoir recours à la modification de la base de registre ou à l'utilisation de l'objet stratégie de groupe locale.

Dans les deux cas vous devrez faire pointer les postes clients vers le serveur WSUS afin que ces derniers obtiennent les mises à jour automatiquement. Quelque soit la manière de configurer un client, il faut un certain temps pour que ce dernier apparaisse dans la liste Ordinateurs de la console WSUS. Si l'on utilise la stratégie de groupe AD, on peut forcer l'actualisation par la commande **gpupdate /force**. Dans un environnement Windows 2000, la commande est la suivante : **secedit/refreshpolicy machine\_policy enforce**. Pour les ordinateurs configurés

par stratégie de groupe local, il faut compter environ une vingtaine de minutes.

Avant de définir les options de stratégie de groupe, vous devez vous assurer que la dernière version du modèle d'administration a été installé sur l'ordinateur sur lequel vous configurez la stratégie de groupe.

### *2) Modification du registre*

Dans un environnement non AD vous disposez de trois méthodes :

- Stratégie de groupe locale (voir ci-dessus)
- Directement par la modification de la base de registre (regedit.exe)
- Stratégie système de Windows NT

Pour les options d'environnement vous devrez modifier la clé suivante :

**HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows\WindowsUpdate**

Pour les options de configuration des mises à jour automatiques, vous devrez modifier la clé de registre suivante :

**HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows\WindowsUpdate\AU**

*Remarque* : vous pouvez utiliser un script pour déployer cette modification sur tous vos postes ou bien les utilitaires du registre.

Après avoir configuré clients et serveur (stratégie de groupe ou modification du registre), reste à faire en sorte que les postes cibles soient mis à jour avec les bons fichiers.

Pour ce faire il est possible d'utiliser les notions de « groupe ». Il est donc tout à fait possible de créer d'autres groupes d'ordinateurs comme par exemple un groupe d'ordinateurs tests pour tester les mises à jour avant de les déployer en grande échelle.

La configuration des groupes d'ordinateurs est un processus qui comporte plusieurs étapes. La première consiste à choisir la manière d'affecter les ordinateurs aux groupes d'ordinateurs. Pour cela il existe deux options : cible côté serveur (ajout manuel de chaque ordinateur à son groupe à l'aide de la console WSUS) et cible côté client (ajout automatique des clients à l'aide des GPO ou de clés de registre). Une fois le choix opéré il faut créer les groupes sur WSUS. Enfin il faut déplacer les ordinateurs au moyen de la méthode choisie lors de la première étape. On peut donc déclarer très facilement les machines qui vont être gérées et les regrouper de manière à définir pour les différents groupes des actions différentes concernant les éléments téléchargés et approuvés.

Une fois l'ensemble de cette procédure effectué, vous êtes prêt à utiliser le service WSUS de Microsoft et ainsi bénéficier d'un service de mise à jour performant pour les environnements Windows. Sa simplicité d'utilisation est telle que même les petits laboratoires, sans véritable équipe informatique, peuvent l'installer et l'administrer.

### 3 Mise en place de Systems Management Server (SMS 2003)

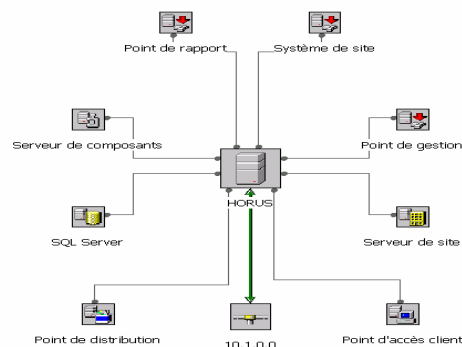
Malgré l'apport indéniable de WSUS, nous avons voulu aller au-delà d'une simple mise à jour des produits Microsoft. Avec une équipe de 2 personnes et plus de 200 postes et 15 serveurs Windows à gérer, on se devait d'avoir un outil comme SMS pour faire face aux mises à jour effrénées des produits Microsoft ainsi qu'à l'installation des nouvelles versions des produits.

La mise en place de SMS nous a permis de gérer non seulement les ressources matérielles et logicielles du laboratoire (découverte, inventaire, reporting) mais aussi la prise de contrôle à distance et le cycle de vie des applications. Il prend en compte :

- le packaging (automatisation des procédures d'installation des applications au travers de technologie telles que Windows Installer),
- la validation (vérification du bon fonctionnement avant déploiement à grande échelle),
- le déploiement (distribution et installation des applications avec prise en compte des problématiques de planification, de ciblage, de suivi et des contraintes réseau),
- la maintenance (réparation des applications et de leur configuration au travers de technologies telles Windows installer),
- la mise à jour (déploiement de correctifs applicatifs et de sécurité ainsi que des services packs),
- le suivi de l'utilisation (mesure du taux et de la durée d'utilisation des applications),
- la suppression (désinstallation des applications lorsque celles-ci ne sont plus ou ne doivent plus être utilisés).

Pour notre configuration nous avons mis en place un seul site SMS (évidemment il est possible en fonction de la complexité de l'infrastructure de mettre en place plusieurs sites SMS).

La figure suivante montre l'organisation de notre site SMS fédéré autour d'un seul serveur (HORUS).



Notre dévolu s'est porté sur SMS 2003 car très peu de solutions s'interfacent actuellement avec Active Directory.

Grâce à ce système, nous gérons de manière centralisée l'ensemble de nos postes de travail, ce qui nous a permis de réduire le coût de possession du parc machine (le fameux TCO – Total Cost of Ownership), le but étant évidemment d'intervenir le moins possible sur les machines et de réaliser toutes les tâches administratives à distance depuis sa console d'administration.

#### 3.1 Télédistribution logicielle sur les clients

Une autre opération courante concerne la télédistribution logicielle, c'est-à-dire le déploiement et l'installation de logiciels et correctifs sur les postes. Si WSUS que nous avons vu plus haut convient parfaitement à la plupart de nos laboratoires, nous avons fait le choix, compte tenu de notre infrastructure d'utiliser SMS. Outre l'extraction et le déploiement des mises à jour à partir de son site, SMS 2003 collecte les statistiques de conformité de standards. C'est une solution plus élaborée que WSUS.

Pour superviser les clients SMS pour qu'ils respectent les mises à jour logicielles de configuration de sécurité, il faut utiliser les Outils d'inventaire de mises à jour (Software Update Scanning Tools) pour étendre SMS 2003. Ces outils sont téléchargeables sur le site de Microsoft

(<http://www.microsoft.com/smserver/downloads/2003/default.mspix>). Le package contient deux outils de scanning :

- les Outils d'inventaire de mise à jour de sécurité (Security Update Inventory Tool)
- les Outils d'inventaire de mise à jour Microsoft Office (Office Inventory Tool for Updates)

Le premier outil est semblable à MBSA et comme ce dernier il recherche les Mises à jour de sécurité manquantes, crée des rapports et détecte les options de configuration qui présentent des risques potentiels de sécurité. En plus il distribue les mises à jour et configure les ordinateurs. Il supporte plusieurs plates formes et produits serveurs.

Le deuxième outil utilise Office Update Database pour déterminer si les installations Office sont à jour.

Les Outils d'inventaire de mise à jour utilisent la fonction de distribution logicielle de SMS. Il faut comprendre que la distribution logicielle comporte 3 composants : les fichiers sources (packages), les programmes et le point de distribution associé qui est un serveur qui héberge les fichiers source (dans notre cas il s'agit du serveur HORUS). Une fois le package configuré, le serveur aura besoin d'une cible (nommé collection en SMS). Une collection peut contenir des objets utilisateur, groupe et ordinateur. Pour exécuter un programme sur les membres d'une collection, il faut créer une publicité qui décrit le package, le programme ainsi que les collections qui recevront la distribution.

Pour installer « Outils d'inventaire de mise à jour », il suffit de suivre les indications apparaissant à l'écran. On sera invité à transférer le fichier *MSSecure.xml* en format compressé. L'outil d'inventaire utilise ce fichier pour vérifier les mises à jour logicielles manquantes. L'assistant affiche par défaut le nom du serveur SMS (que vous pouvez modifier si besoin). Ensuite il faut renseigner le nom du package. En cliquant sur Suivant l'installation suit son cours.

Une fois l'installation terminée, dans la console SMS l'outil crée deux collections : une collection de pré-production qui contient le nom du système de test indiqué lors de l'installation et une autre collection dans laquelle vous pouvez ajouter d'autres clients SMS et que vous utiliserez pour distribuer les outils d'inventaire. Voir l'illustré de la figure suivante :



L'installation de ces deux outils est semblable. Dès que les outils d'inventaire sont installés et peuvent être déployés, vous pouvez créer des publicités pour collecter les données. Ensuite vous pouvez packager et distribuer les mises à jour grâce aux outils d'inventaire SMS 2003. En utilisant par exemple l'assistant Distribution de mises à jour logiciels, le système vous demande quel type de mise vous voulez inclure dans un package.

A la prochaine étape vous serez invité à sélectionner un package existant ou en créer un nouveau (le package peut être personnalisée et accompagné si on le souhaite de fichier RTF décrivant par exemple ce à quoi est destinée la mise à jour en question). Une fois les mises à jour transférées à destination du serveur SMS, l'assistant affiche la liste des mises à jour et indique si elles sont prêtes pour la distribution.

Quand toutes les mises à jour sont marquées comme prêtes, on pourra cliquer sur OK et sélectionner les points de distribution.

### 3.2 Contrôle à distance

SMS nous permet de prendre la main à distance sur une machine. Ce dernier point se place dans un contexte de support et on évite ainsi, lorsque cela est possible, l'intervention physique sur place. Tout ceci met en évidence que la gestion de la configuration du poste client et la prise en main à distance demeurent des facteurs clés pour réduire les coûts de maintenance.

### 3.3 Inventaire matériel

Le plus difficile dans un laboratoire c'est de savoir combien et de quels types de machines on dispose. Pire, savoir quels types de logiciels y sont installés est un véritable casse tête. Grâce à SMS on peut avoir précisément l'inventaire matériel et logiciel des postes. D'ailleurs cet inventaire peut être couplé à la télédistribution logicielle, ce qui nous a permis par exemple au CIML de pouvoir installer un correctif de sécurité mais uniquement sur les machines qui ont Windows XP Professionnel, Internet Explorer 6.0 SP1 et qui disposent d'au moins 256 Mo de RAM.

Toutes ces tâches de gestion de parc sont incluses dans SMS. Cet outil fait partie de la gamme de produits de management avec Microsoft Operations Manager 2005, qui lui se place sur le terrain de la supervision.

## 4 Microsoft Operations Manager (MOM 2005) : solution de supervision des serveurs

Tandis que SMS est dédié à la gestion des configurations des postes de travail et des serveurs Windows, MOM permet de surveiller l'ensemble du parc informatique et génère des rapports de façon préventive et centralisée.

Il y a quelques années, la supervision était associée à quelque chose de complexe à mettre en œuvre et à maintenir. Avec MOM 2000 et aujourd'hui la version 2005, fini les déploiements lourds et les configurations difficiles, place à la simplicité d'installation, de configuration et d'utilisation.

Au Centre d'Immunologie de Marseille Luminy, nous utilisons MOM principalement pour gérer nos 15 serveurs Windows car le bon fonctionnement des serveurs, en particulier les serveurs de messagerie, DNS et Active Directory, et la qualité de service apportée aux utilisateurs ne dépendent pas uniquement de l'architecture, de la configuration et de l'installation des composants, mais aussi et surtout de la surveillance et de la gestion qui sont

effectués au quotidien. En plus matériellement il nous est impossible de surveiller individuellement chaque serveur et d'examiner les différents journaux d'événements afin de nous prémunir de tout incident.

Cet outil nous permet de surveiller l'état, la disponibilité et les performances de nos serveurs Windows et ainsi de prendre connaissance d'éventuels problèmes sans être obligés de se connecter sur ces derniers pour résoudre les problèmes.

Son fonctionnement est basé sur l'utilisation des règles prédéfinies (15 000 règles existent par défaut) afin de collecter des données et de les traiter via des réponses automatisées.

Nous allons décrire dans cette partie le fonctionnement de MOM et comment nous avons mis cet outil pour optimiser nos serveurs, assurer la maintenance de notre serveur de messagerie Exchange et renforcer la sécurité de nos serveurs.

La version 2005 que nous avons utilisé ajoute des possibilités de supervision préventive, une meilleure évolutivité et l'interopérabilité avec des solutions tierce partie non Windows. Si cela vous intéresse vous pourrez trouver des add-on pour SPECTRUM (Aprisma), Netcool (Micromuse), AppManager (NetIQ) et iWare Integrator etc...C'est donc une solution extensible par les clients et les partenaires et qui offre la possibilité de manager d'autres applications non Microsoft et qui intègre d'autres solutions d'administration.

MOM configuré au CIML nous permet grâce aux règles pré-configurées de superviser et de corriger des problèmes, d'avoir en permanence des remontées d'alertes préventives et réactives, de bénéficier de conseil contextuel qui inclut la cause probable de l'alerte et une méthode suggérée de résolution et enfin et pas des moindres, l'accès direct aux articles appropriées de la Base de Connaissance de Microsoft (les fameux KB) et la possibilité de rajouter ses propres connaissances.

Pour déployer MOM nous sommes passés par ces 4 phases :

1. Installation des composants serveur de MOM 2005
2. Découverte des ordinateurs et déploiement des agents
3. Installation de MOM 2005 Reporting ( ce composant n'est pas obligatoire)
4. Importation des packs d'administration

Avant d'installer MOM, il faut installer et configurer SQL (pour la base de données MOM, la taille minimale prise en charge est 300 Mo. La taille maximale prise en charge s'élève à 30 Go. Une base de données de plus petite taille est préférable si vous voulez bénéficier de meilleures

performances. Il est conseillé de maintenir la taille de la base de données entre 12 et 15 Go.)

Une fois le logiciel installé et avant de déployer des agents, il faut déterminer les ordinateurs qui doivent être découverts par MOM et gérés par des agents MOM.

Quand les agents sont déployés et configurés sur chaque poste client, on peut utiliser la console Opérateur pour surveiller en temps réel les ordinateurs ou les serveurs. Cette console comporte une interface graphique de suivi d'état pour superviser de manière préventive l'état des systèmes en matière de santé, de performance et de fiabilité. Grâce à elle il est aussi possible d'avoir des données concernant des ordinateurs ou serveurs et des informations sur un événement ou sur une alerte. Il est possible d'intervenir directement sur l'ordinateur (l'isoler du réseau par exemple pour qu'il ne perturbe pas les autres composants du réseau). Cette console Opérateur permet d'avoir un grand affinage dans la résolution de problèmes et grâce au code couleur, la gravité de l'alerte ne passe pas inaperçue.

La gestion proprement dite du site MOM se fait via la console d'administration, elle permet à partir de cette interface de gérer complètement le site MOM et en particulier d'importer les packs Management auprès de Microsoft ou de fournisseurs tiers qui permettent à MOM de s'intégrer à une grande variété de logiciels serveurs. Elle permet la Configuration et l'administration de MOM, la configuration des paramètres globaux, la création de packs d'administration, l'importation et l'exportation de packs d'administration.

MOM offre une réelle opportunité pour surveiller les différents composants d'une architecture informatique. Il offre une réelle alternative à des outils comme HP OpenView surtout si votre laboratoire comporte en majorité des systèmes Windows. Une version allégée de ce produit existe sous le nom de MOM Workgroup Edition. Il est limité à dix agents et dépourvu du module reporting.

Avec MOM, nous disposons au sein du CIML :

- D'une solution pour optimiser la disponibilité de nos systèmes et applications (surveillance préventive et réactive de leur état et de leurs performances)
- D'une solution complète et pertinente (fourniture d'un pack pour les produits Microsoft intégrant la connaissance des équipes de support et de développement facilitant ainsi la mise en œuvre du produit)
- D'une solution à l'échelle de notre laboratoire souple et adaptable (architecture distribuée supportant la consolidation et le filtrage des informations, configuration centralisée, installation et configuration automatique des agents des machines supervisées)

## 5 Conclusion

La sécurité des systèmes d'informations quels qu'ils soient passe par une mise à jour régulière afin de se prémunir des failles de sécurités potentielles. La gestion de ses mises à jour est complexe surtout pour nos laboratoires qui ne disposent pas forcément des ressources nécessaires. En plus la fréquence de ces mises à jour et la multiplication de leur nombre demande de plus en plus de temps aux administrateurs, ce qui induit des coûts non négligeables.

Dès lors une automatisation de ces tâches devient quasi nécessaire, je dirais même obligatoire. En plus il n'y a pas que les systèmes d'exploitation qui doivent être mis à jour. Ainsi les services réseaux, les applications, les bases de données doivent être elles aussi mises à jour. Microsoft a compris qu'il fallait faire un effort dans ce sens et propose plusieurs solutions, toutes plus ou moins complètes. Parmi ces solutions nous vous en avons présenté trois que nous avons implanté au Centre d'Immunologie :

1. WSUS qui est un outil disponible en téléchargement gratuit, dont l'utilisation simplifiée permet d'installer les mises à jour de plusieurs produits Microsoft. Ce produit correspond à la majorité de notre environnement.
2. SMS 2003, qui permet la gestion de ressources matérielles et logicielles, la gestion des applications et la téléassistance, fonctionnalités sur lesquelles viennent se greffer plusieurs fonctions nouvelles dont la possibilité de gérer les périphériques de type Pocket PC, la gestion matérielle des machines DELL qui composent essentiellement notre parc informatique et surtout l'incontournable déploiement d'OS et de correctifs de sécurité.
3. Enfin avec MOM 2005, fini les déploiements lourds et les configurations difficiles. De par sa

simplicité d'utilisation et sa puissance, MOM 2005 est un produit qui mérite un détour pour la supervision des postes et serveurs.

D'autres solutions existent, mais malheureusement nous ne les avons pas testées. L'une d'elle d'ailleurs pourrait être une alternative intéressante. C'est l'idée d'un « patch virtuel » avec le boîtier PatchPoint de BlueLane qui, placé devant le serveur filtre le trafic. Si un flux risque de déclencher l'exploitation d'une vulnérabilité, il est modifié à la volée et il protège le serveur comme le ferait un correctif (*Revue Décision Informatique N° 646/19 septembre 2005*). L'idée est séduisante, à condition que tous les éditeurs apprécient la méthode.

## 6 Pour en savoir plus

<http://www.microsoft.com/windowsserversystem/updateservices/default.mspx>

Revue Windows IT Pro Vol. 4 – Numéro 8 – Septembre 2005 : Dossier : Special WSUS

<http://www.microsoft.com/smsserver/default.mspx>

<http://www.microsoft.com/mom/default.mspx>

<http://www.microsoft.com/technet/security/default.mspx>

<http://www.laboratoire-microsoft.org/articles/server/>