

Management de patches grâce à LANguard N.S.S. & Microsoft SUS

Une solution rentable et facile à utiliser pour la gestion de patches sur le réseau

Ce livre blanc fournit une vue d'ensemble de l'utilisation de GFI LANguard Network Security Scanner (N.S.S.) et de Microsoft Software Update Services (SUS) pour garder votre réseau à jour en téléchargeant automatiquement les patches de sécurité les plus récents.

Introduction

Le management de patch est une tâche d'administration essentielle. Elle consiste à parcourir les machines du réseau afin de trouver les patches manquants et à les déployer dès qu'ils sont disponibles. Ne pas effectuer cette tâche rend le réseau doublement vulnérable, car non seulement la vulnérabilité existe, mais elle a également été publiée, ce qui l'amène à être utilisée par des utilisateurs malveillants, pirates et développeurs de virus.

Cependant, régulièrement, un grand nombre d'administrateurs n'appliquent pas les bons patches, comme l'ont prouvé des vers tels que Slammer, le ver de janvier 2003 qui se déploie en exploitant des failles connues des serveurs Microsoft SQL 2000 sans patch. Jusqu'à présent, la raison principale était le fait qu'une installation de patches était une tâche lourde et décourageante. Néanmoins, avec la venue d'outils sophistiqués de management de patches, ce scénario peut être éliminé.

Ce livre blanc fournit une vue d'ensemble sur l'utilisation de GFI LANguard Network Security Scanner (N.S.S.) et Microsoft Software Update Services (SUS) pour garder votre réseau à jour.

Introduction.....	2
Comment configurer le management de patch sur votre réseau.....	3
Conclusion.....	8
A propos de GFI Software.....	9

A propos de GFI LANguard Network Security Scanner (N.S.S.)

GFI LANguard N.S.S. est le principal scanner de sécurité fonctionnant sous Windows. Il parcourt votre réseau à la recherche de points faibles de sécurité, en scannant l'intégralité de votre réseau pour détecter des patches de sécurité manquants, des services packs, des partages ouverts, des ports ouverts, des comptes d'utilisateurs inutilisés et bien plus. Ses fonctions de rapports puissantes permettent de protéger votre réseau en interdisant facilement l'accès aux pirates. GFI LANguard N.S.S. peut également déployer à distance des services packs et patches manquants dans les applications et le système d'exploitation.

A propos de Microsoft Software Update Services (SUS)

Microsoft SUS est un outil de management de patches gratuit fourni par Microsoft pour aider les administrateurs de réseau à déployer les patches de sécurité plus facilement. En d'autres mots, Microsoft SUS est une version de Windows Update qui s'exécute sur votre réseau. Il n'est plus nécessaire pour chaque poste de travail de se connecter à Internet pour mettre à jour Windows, mais ceux-ci doivent se connecter au serveur Microsoft SUS à la place et effectuer la mise à jour à partir de celui-ci. Le serveur Microsoft SUS nécessite seulement un accès public à Internet lors de sa connexion à Windows Update.

En se connectant à Windows Update, le serveur Microsoft SUS offre une notification des mises

à jour importantes et effectue également une distribution automatique de ces mises à jour vers vos postes de travail et serveurs. Le serveur SUS donne à l'administrateur le contrôle des mises à jour : l'administrateur peut tester et approuver les mises à jour du site public de Windows Update avant un déploiement sur l'intranet de l'entreprise. Ce déploiement prend place selon un emploi du temps défini par l'administrateur.

Pourquoi utiliser GFI LANguard N.S.S. et le serveur Microsoft SUS ensemble ?

Le serveur Microsoft SUS est une bonne solution pour déployer les patches des systèmes d'exploitation. Il supporte tous les patches de systèmes d'exploitation, y compris les patches pour des applications faisant partie du système d'exploitation comme IIS et IE.

Les limites du serveur Microsoft SUS

Microsoft SUS n'offre pas les fonctionnalités suivantes fournies par GFI LANguard N.S.S. :

- Déploiement immédiat des patches (particulièrement important dans le cas d'une infection virale à haut risque nécessitant l'installation immédiate d'un patch)
- Déploiement des patches des applications Microsoft et des services packs pour Microsoft Office, Microsoft SQL Server, Microsoft Exchange Server et Microsoft ISA Server
- Possibilité de vérifier que tous les patches ont été installés correctement grâce aux rapports.
- Déploiement des patches sur les machines fonctionnant sous Windows NT
- Déploiement de patches de logiciels de tierce partie et des logiciels.

Par conséquent, l'utilisation conjointe de GFI LANguard N.S.S. et Microsoft SUS est une combinaison parfaite pour garder les machines Windows à jour, y compris les patches et services packs des applications Microsoft et des logiciels de tierce partie ainsi que les patches de logiciels.

Comment configurer le management de patch sur votre réseau

Etape 1 : Installation du serveur Microsoft SUS

Parce que le serveur Microsoft SUS n'est pas réellement un outil de vérification basé sur le poste de travail, mais plutôt un serveur automatisé conçu pour travailler en arrière plan, il est plus difficile de le mettre en œuvre que d'autres outils de management de patch. Cependant, une fois configuré, le processus de management de patch est automatisé, et vaut donc bien cet effort supplémentaire.

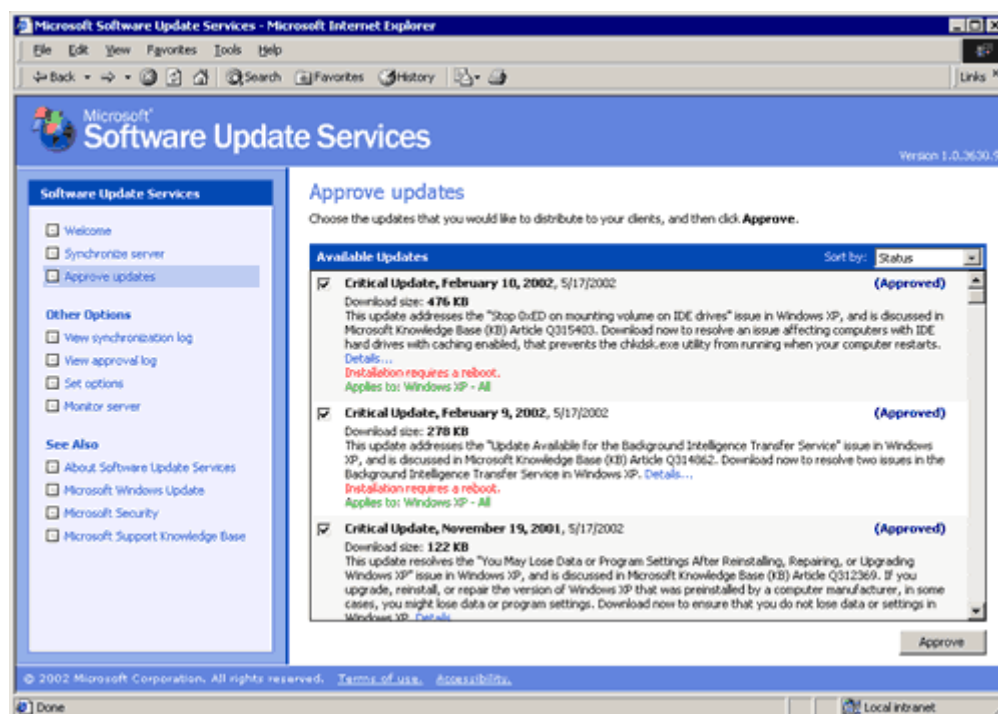
L'installation est assez simple. Vous installez le serveur Microsoft SUS (IIS est requis), et le configurez pour vérifier les mises à jour. Assurez-vous ensuite que vos postes de travail et vos serveurs fonctionnent sous Windows 2000 SP3, Windows XP SP1/SP2 ou Windows .2003, ou

que le client Microsoft SUS soit installé. Notez que Windows NT n'est pas supporté.

Vous pouvez remplacer le client SUS qui utilise la Stratégie de Groupe avec la fonction 'deploy custom software' (déployer le logiciel personnalisé) de GFI N.S.S. Après quoi, vous devez utiliser la Stratégie de Groupe pour configurer les stations de travail clients afin d'obtenir des mises à jour automatiques à partir de votre serveur SUS. Tout ce qui précède est clairement décrit dans les documents qui accompagnent Microsoft SUS.

La gestion du serveur Microsoft SUS

La gestion du serveur Microsoft SUS est entièrement basée sur le Web, vous permettant ainsi de le gérer à distance. Le serveur Microsoft SUS télécharge automatiquement toutes les mises à jour disponibles et vous avertit des nouvelles mises à jour par email. Les nouvelles mises à jour peuvent être approuvées avant leur déploiement ou rejetées, vous assurant un contrôle total de ce qui est installé sur votre réseau. L'interface permettant d'approuver les mises à jours est très semblable à la mise à jour d'une machine unique avec Windows Update.

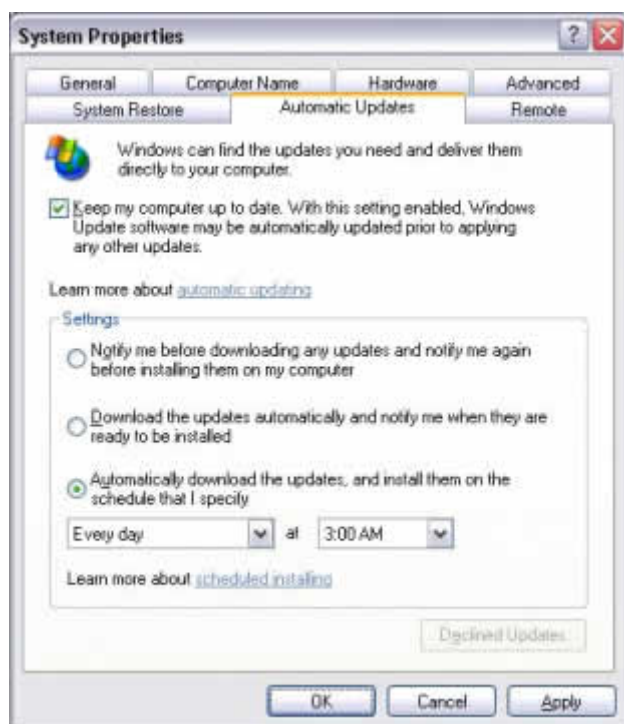


Autorisation des mises à jour en utilisant l'interface d'administration du serveur Microsoft SUS

Le client Microsoft SUS

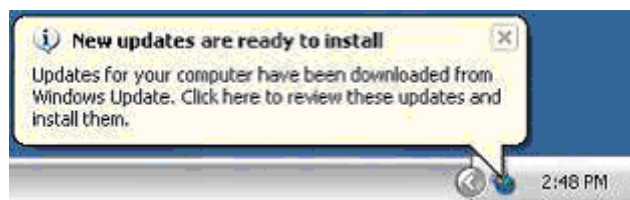
Une fois que le serveur Microsoft SUS et le client Microsoft SUS sont installés, toutes les mises à jours sont déployées automatiquement. En tant qu'administrateur, vous pouvez configurer le déroulement du processus. Vous pouvez configurer l'heure à laquelle la mise à jour doit

s'effectuer, et autoriser les utilisateurs, si vous le désirez, à avoir un certain contrôle pendant le processus. La capture d'écran ci-dessous vous montre les options disponibles. Ces options peuvent bien sûr être bloquées en utilisant la Stratégie de Groupe.



Panneau de configuration des mises à jour automatiques avec options

Après avoir configuré le client Microsoft SUS, les patches sont déployés automatiquement. L'utilisateur est averti grâce à un message sur la barre des tâches (voir image).



L'utilisateur reçoit un avertissement indiquant que les mises à jours sont sur le point d'être installées

Etape 2 : Management de patches avec GFI LANguard N.S.S.

Une fois que le serveur Microsoft SUS est opérationnel sur votre réseau, il vous faut installer GFI LANguard N.S.S afin d'exécuter les tâches de management de patch suivantes :

- Déploiement des patches des applications Microsoft et des services packs pour Microsoft Office, Microsoft SQL Server, Microsoft Exchange Server et Microsoft ISA Server
- Vérifier que les patches manquants et les services pack sont installés et publier un rapport

HTML à ce sujet

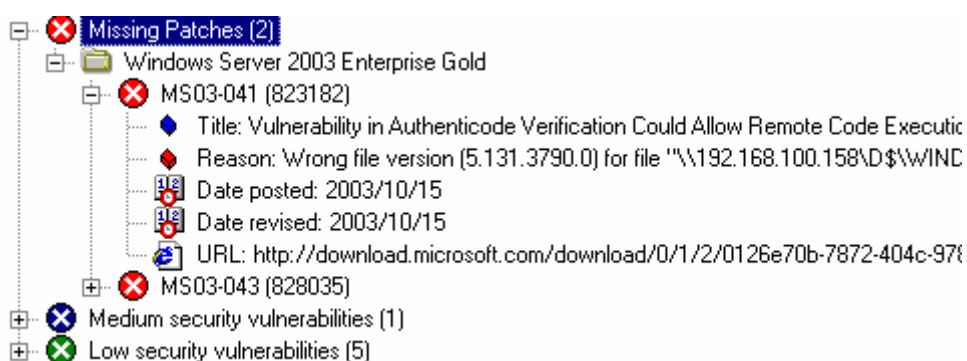
- Déploiement des patches sur les machines fonctionnant sous Windows NT
- Déploiement de patches de logiciels de tierce partie (peut aussi être utilisé pour déployer les mises à jour des signatures virales)
- Déploiement immédiat d'un patch précis dans l'évènement d'urgence ; attendre que SUS le mette à jour ne sera pas possible.

Recherche de patches manquants avec GFI LANguard N.S.S.

Une fois que vous avez votre management de patch en place, il est important de scanner régulièrement votre réseau afin de déterminer que tous les patches et services packs ont été déployés par Microsoft SUS. GFI LANguard N.S.S. scanne rapidement votre réseau et liste tous les patches manquants et les services packs sous le nœud "Alerts".

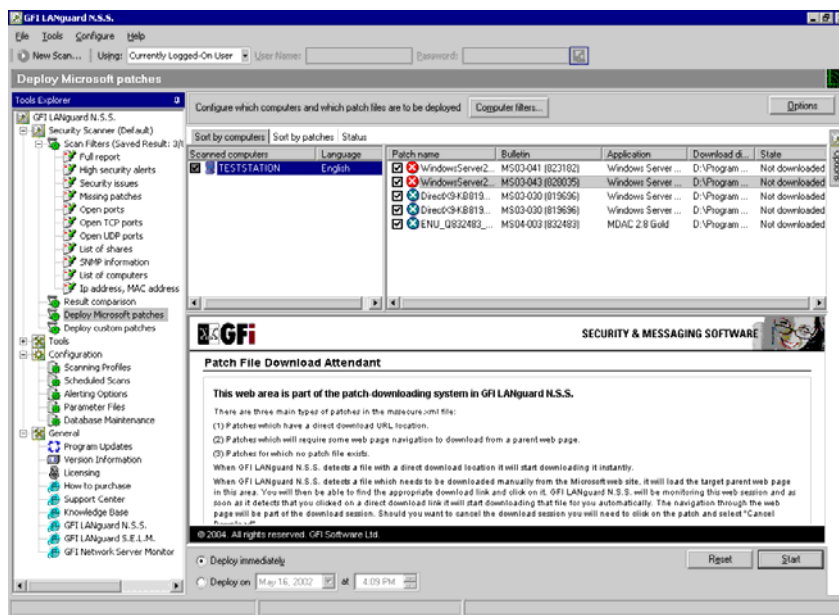
Afin de scanner votre réseau, entrez directement la fourchette d'adresses IP en haut de l'interface du scanner, ou utilisez l'Assistant de Scan (accessible à partir du menu File) pour spécifier quels ordinateurs scanner. Il est possible de scanner des domaines, des ordinateurs spécifiques et une fourchette entière d'adresses IP. Cliquez sur Finish pour démarrer le processus de balayage. Vous verrez chaque machine trouvée par GFI LANguard N.S.S. apparaître dans la fenêtre de gauche. La fenêtre de droite fournit des informations détaillées sur la progression du balayage.

Une fois que le balayage du réseau est complété, les services packs et patches manquants sont détaillés sous le nœud des Vulnérabilités. Si Microsoft SUS met à jour les clients correctement, vous ne devriez voir que les patches d'application manquants à cet endroit.



GFI LANguard NSS affiche les patches manquants

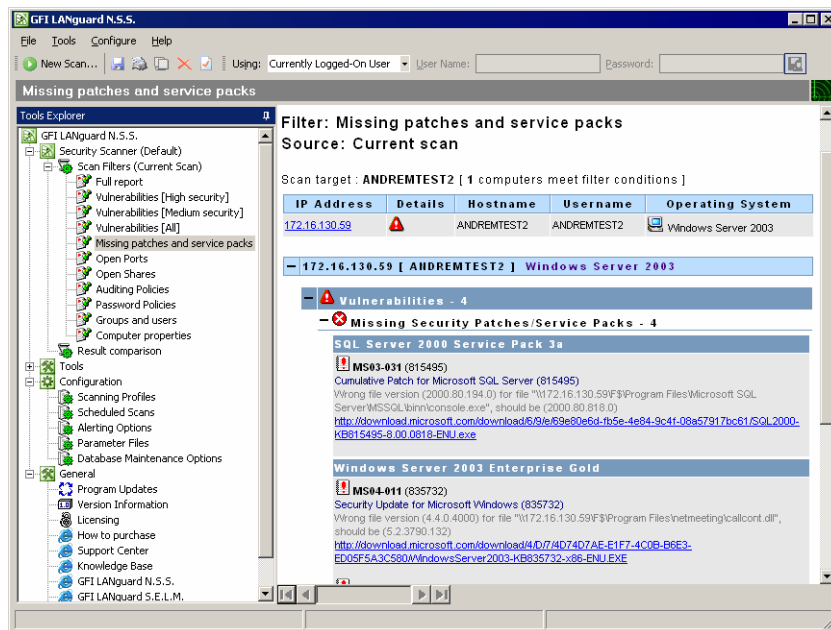
Un clic droit sur un patch ou un service pack vous permet de déployer le patch ou le service pack manquant sur cet ordinateur ou sur tous les ordinateurs. Le nœud "Deploy Patches", que vous pouvez voir dans la capture d'écran ci-dessous, vous permet de spécifier facilement quel patch déployer sur quel ordinateur.



Déploiement des patches

Etape 3 : Rapports

Une fois que vous avez scanné votre réseau, vous pouvez aussi créer un rapport concis qui fait la liste de tous les patches et services packs manquants. Pour générer un rapport des patches manquants, allez dans le menu "File > Filters" et sélectionnez "Missing patches".



Le rapport des services packs/patches manquants de GFI LANguard N.S.S.

Conclusion

Le Serveur Microsoft SUS est parfait comme management de patch des systèmes d'exploitation. Même si vous pouvez utiliser un autre produit de management de patch à la place, utiliser le serveur Microsoft SUS vous fera gagner du temps à long terme : une fois configuré, il est facile de garder votre réseau à jour. Etant donné que le serveur Microsoft SUS est gratuit, la décision est simple à prendre. Cependant, le serveur Microsoft SUS ne peut pas effectuer tous les managements de tous les patches : il ne déploie pas les patches de logiciels d'applications comme Office, Exchange ou SQL Server. De plus, il n'a aucune fonctionnalité de balayage : vous devez passer les journaux en revue pour vérifier si un patch a été déployé avec succès ou non. Il vous faut donc utiliser un outil de management en plus du serveur Microsoft SUS.

GFI LANguard N.S.S., ajouté à Microsoft SUS, offre pour un coût minime toutes les fonctionnalités trouvées dans d'autres solutions de management de patch très onéreuses. La plupart des solutions de management de patch vont de \$1,500 pour une licence 100 machines à \$8,000 et plus pour une licence 500 machines. L'association de GFI LANguard N.S.S. et Microsoft SUS vous permet de mettre à jour les systèmes d'exploitation en utilisant Microsoft SUS (Windows 2000, XP, .NET, IIS, IE, Windows Media) et les services packs, les patches des applications Microsoft, les patches de Windows NT ainsi que les patches de logiciels de tierce partie en utilisant GFI LANguard N.S.S.

Les solutions combinées de GFI LANguard N.S.S. et Microsoft SUS ne sont pas seulement plus puissantes et plus flexibles, mais aussi moins onéreuses : Microsoft SUS est gratuit et le prix des licences GFI LANguard N.S.S. commence à € 325 pour 25 adresses IP. Pour de plus amples informations sur GFI LANguard N.S.S. et pour télécharger votre copie, veuillez visiter <http://www.gfsfrance.com/fr/lannetscan/>.

A propos de GFI Software

GFI est l'un des leaders dans le domaine de la réalisation de logiciels qui fournit une seule source intégrée permettant aux administrateurs de résoudre les problèmes de sécurisation de réseaux, de contenu et de messageries. Grâce à sa technologie innovatrice, une stratégie agressive de commercialisation et sa concentration sur le marché de petites et moyennes entreprises, GFI répond aux besoins de continuité d'affaires et de productivité des entreprises et d'autres organisations sur une grande échelle. Fondée en 1992, GFI est une entreprise internationale qui possède des bureaux à Malte, à Londres, Raleigh, Hong Kong, Adelaïde et à Hambourg avec plus de 200.000 installations de ses logiciels à travers le monde. GFI est une entreprise spécialisée et possède un réseau de plus de 10.000 partenaires à travers le monde. Partenaire stratégique de Microsoft, GFI est membre certifié du partenariat Microsoft Gold Certified Partner. Pour plus d'informations à propos de GFI, visitez le site <http://www.gfsfrance.com>.

© 2007 GFI Software. Tous droits réservés. L'information contenue dans ce document représente le point de vue actuel de GFI sur les questions abordées à la date de sa publication. Etant donné que GFI doit répondre aux conditions dynamiques du marché, il ne devrait pas être interprété comme un engagement de la part de GFI, et GFI ne peut pas garantir l'exactitude d'aucune information présentée après la date de la publication. Ce livre blanc est seulement à titre informationnel. GFI NE FAIT AUCUNE GARANTIE, EXPRESSE OU IMPLICITE, DANS CE DOCUMENT. GFI, GFI EndPointSecurity, GFI EventsManager, GFI FAXmaker, GFI MailEssentials, GFI MailSecurity, GFI MailArchiver, GFI LANguard, GFI Network Server Monitor, GFI WebMonitor et leurs logos de produit sont des marques déposées ou des brevets commerciaux de GFI Software aux Etats-Unis et/ou dans d'autres pays. Tous les noms de produit ou d'entreprises mentionnés ci-dessus peuvent être les marques déposées de leurs propriétaires respectifs.