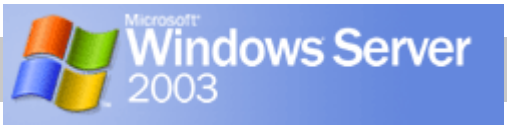
Révision 1.0



Benoît HAMET

Les nouveautés sécurité de Windows Server 2003

Date de publication : 27 juin 2003

Introduction

Avec Windows Server 2003, Microsoft nous livre un système d'exploitation serveur des plus abouti et des plus mature ; il relève sans grande difficulté tous les défis et se révèle très novateur, surtout en matière de sécurité – sujet hautement sensible.

Il s'agit du premier produit disponible sur le marché s'inscrivant dans la nouvelle vision « **Trustworthy Computing** », initiée par Bill GATES en Janvier 2002. Cette inscription dans cette initiative visant à rendre l'informatique plus sécurisée marque une révolution culturelle dans le monde Microsoft, en effet dorénavant lorsqu'il y a à choisir entre une nouvelle fonctionnalité et la sécurité, c'est la sécurité qui prévaudra. Ces nouvelles orientations se traduisent dans la réalité par un nouveau framework dénommé **SD^3 + C** :

- Secure by Default (sécurité par défaut)
- Secure by Design (sécurité par la conception)
- Secure by Deployment (sécurité dans le déploiement)
- Communications

Nous allons donc nous pencher sur ces nouvelles orientations en matière de sécurité qui apparaissent dans Windows Server 2003.

Quoi de neuf ?

Tout d'abord, le bilan, après trois ans de mise à l'épreuve de Windows 2000, est globalement positif ; la plateforme Windows 2000 s'est avérée stable, relativement sécurisée et performante. Cependant, ce bilan aussi bon soit-il n'est pas encore totalement satisfaisant en matière de sécurité.

Ainsi, Windows Server 2003 tente d'offrir une meilleure sécurité par rapport à son prédécesseur. Pour ce faire Microsoft a totalement repensé la conception et le mode de fonctionnement par défaut de Windows.

Ainsi de nombreuses fonctionnalités, telles que Internet Information Service, le service d'affichage ou Telnet sont désactivées. Et lorsque ces fonctionnalités sont activées, elles fonctionnent à l'aide d'identité ayant des privilèges plus restreints. Par exemple, lorsque vous installez le serveur web, seules les fonctionnalités statiques (ASP et ASP.Net doivent être activée par la suite) sont activées tandis que les applications d'administration ne sont plus démarrées automatiquement.

Parallèlement à ces limitations de services, Microsoft propose un assistant de configuration du serveur. Cet assistant propose différents rôles (serveur de fichier, d'impression, web…) et mettra en œuvre la configuration la plus appropriée suivant le rôle défini. Bien entendu, un serveur peut assumer plusieurs rôles simultanément.

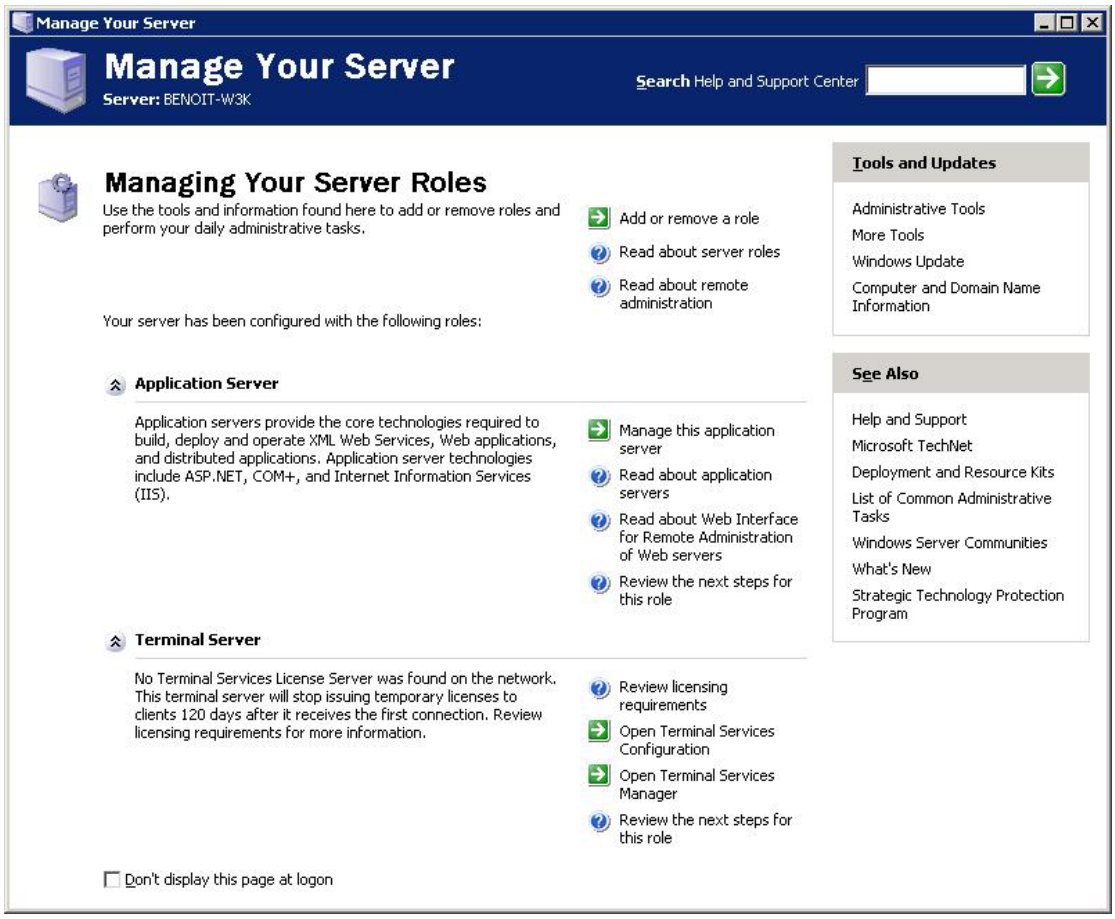


Figure 1 - Assistant de configuration de rôle

Par ailleurs, l'impersonnalisation (possibilité d'exécuter une application en utilisant une identité différente) est désormais un privilège pouvant être attribué (ou non) à un profil (compte utilisateur). De même, les audits de login enregistrent les adresses IP source et le port associé, facilitant ainsi la lisibilité des attaques.

En parlant d'attaque, Windows 2003 intègre la fonctionnalité apparue avec Windows XP qu'est le firewall. Ce firewall logiciel est en fait constitué de 2 parties :

- La première partie (ICF – Internet Connection Firewall) s'applique sur les connexions réseau – notamment lors du partage de connexion internet (ICS) ; cette partie est la plus proche du firewall de Windows XP

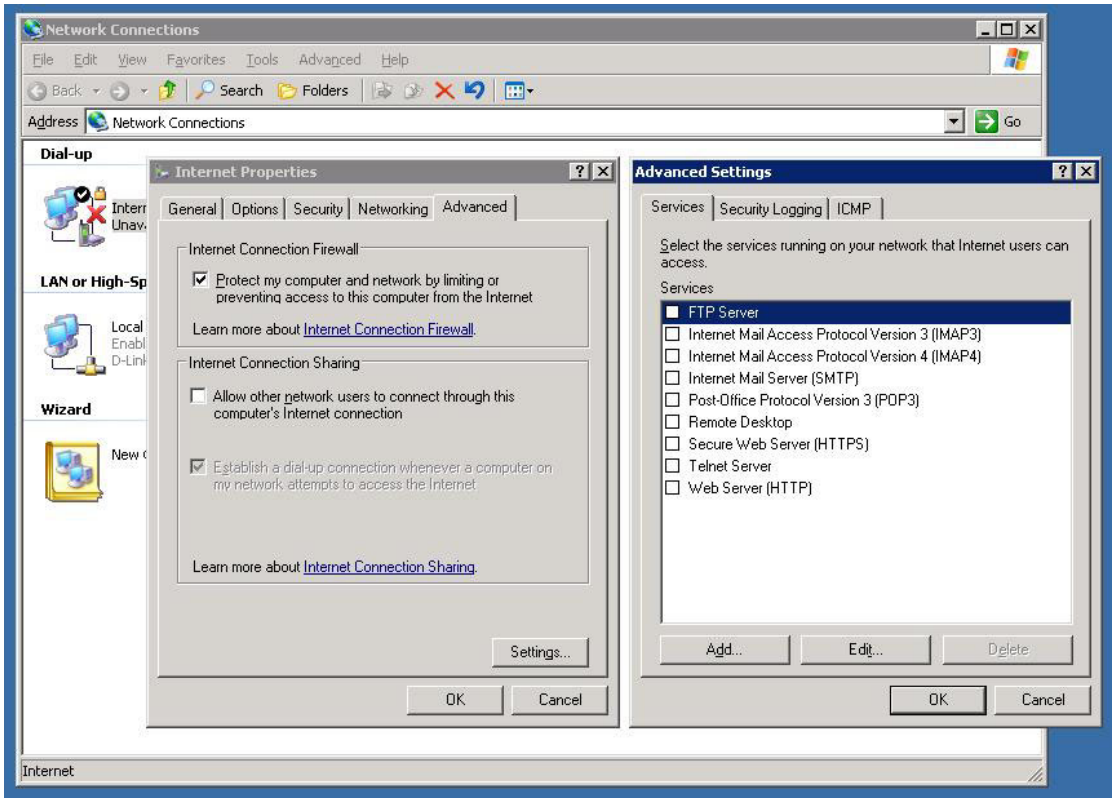


Figure 2 - Fonctionnalités de pare-feu internet

- La seconde partie est intégrée au NAT (Network Adress Translation) ; cependant, lors de la configuration des fonctionnalités de routage (et d'activation de ce pare-feu), vous devrez désactiver l'ICF.

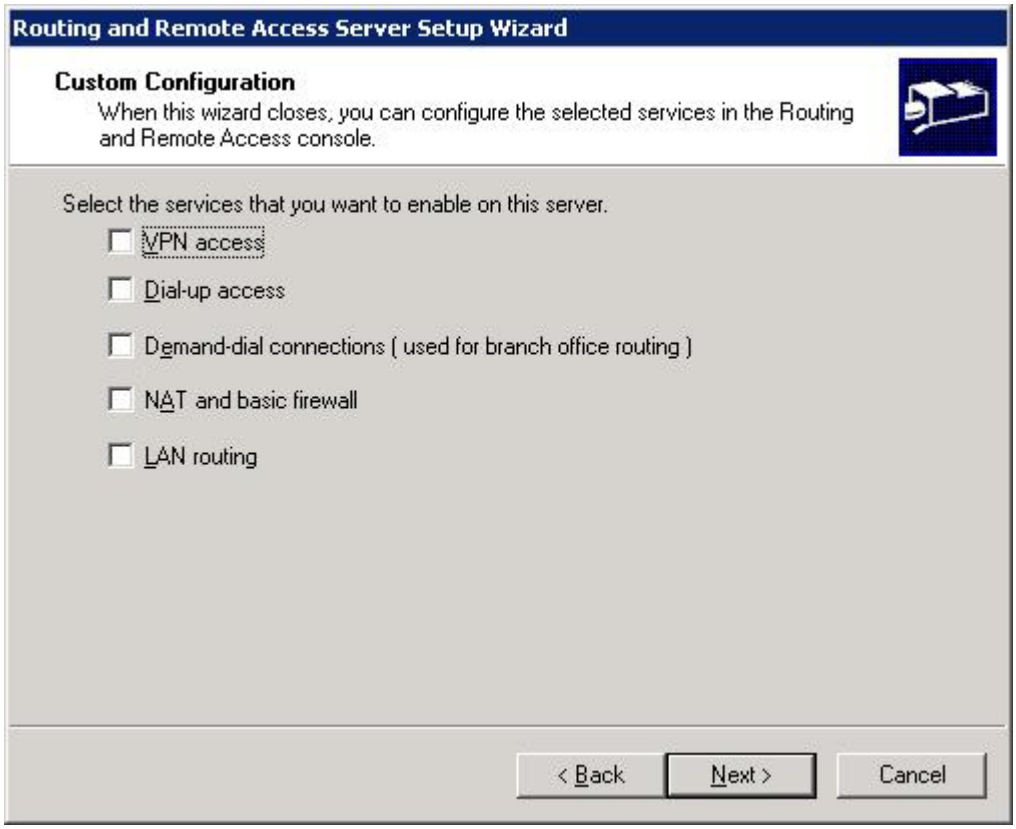


Figure 3 - Fonctionnalité de pare-feu ET de routage

Conclusion

Avec Windows Server 2003, Microsoft nous livre une première mouture de l'application de la nouvelle stratégie sécurité de la firme de Seattle. De quoi être confiant concernant la réalité de la prise de conscience concernant les problématiques de sécurité en informatique.