

Survol technique de Windows Server 2003 Service Pack 1

Stéphane Asselin

Conseiller en sécurité

Microsoft Canada



Objectifs de la présentation

- Présenter les nouvelles fonctions et les nouveaux outils de Windows Server 2003 Service Pack 1.
- Examiner les nouveaux modèles de sécurité et les améliorations à ce chapitre.
- Démontrer comment gérer et tester ces changements dans votre environnement
- Méthodes éprouvées, outils et conseils
- Échanger sur SP1 et discuter de l'avenir du GSIQ

Programme

- Fonctions et outils de configuration de SP1
- Améliorations à la sécurité du système et du réseau
- Options de configuration
- Test dans un laboratoire virtuel

Service Pack1 pour Windows 2003

- Disponible depuis le 30 mars 2005, SBS 2003 Disponible!
- Anglais et allemand
- 18 autres langues d'ici 2 mois
- 32 bits, 64 bits Itanium
- Disponibilité via:
 - Téléchargeable à partir de Microsoft Download Center
 - Windows Update et SUS
 - OEM pre-installation
 - CD
 - Volume Licensing and System Builder programs

Objectifs de SP1

Amélioration de la sécurité

- Réduction de la surface vulnérable aux attaques
- Nouvelles améliorations à la sécurité

Réduction et renforcement des privilèges par défaut des services

- RPC / DCOM

Prise en charge de matériel NX (No Execute)

- Intel
- AMD

Pare-feu Windows activé par défaut

- Nouveau scénario d'installation

Assistant de configuration de sécurité qui aide les admin. TI

- Configuration et verrouillage fondés sur les rôles

Mise en quarantaine du réseau VPN

- Inspection des clients
- Correction
- Isolation

Vérification de la métabase IIS 6.0

Fiabilité accrue

Performance accrue

- Amélioration de 10 %+ dans TPC, TPC-H, SAP, SSL, etc.

Options de déploiement de SP1

- Installation manuelle
 - Update.exe /? (pour les options)
 - Update.msi
- Intégration
 - Update.exe /integrate: <path>
- Logiciel d'imagerie
 - OS deployment feature pack pour SMS 2003
- Installation par script
 - Unattend.txt

Mode d'installation

- Appareil unique
 - Installation rapide
- Plusieurs serveurs
 - Taille 330 Mo.
 - Création du point de distribution
 - `Spsp1.exe /s:c:\<dir>`
 - Intégration du SP1 aux fichiers sources
 - SUS
 - Temps d'installation +/- 30 minutes

Après l'installation de SP1

- Nouvelle installation du serveur (intégrée)
 - Appel de la protection post-installation :
 - Protection du serveur entre l'installation du SE et l'installation des dernières mises à jour
 - Le pare-feu Windows est activé s'il n'a pas été configuré explicitement durant l'installation
- Mise à niveau Server 2003 (update.exe)
 - Pare-feu désactivé par défaut
 - Entrée en vigueur de nouveaux modèles de sécurité
- Installer et exécuter l'Assistant de configuration de sécurité

Protection post-installation


L'interface PSSU (Post Setup Security Updates) permet aux administrateurs d'installer en toute sécurité des mises à jour du produit après l'installation initiale de Windows Server 2003 et de SP1

S'affiche à l'ouverture de session de l'administrateur ou en raison de l'installation d'une mise à jour du produit ou d'une autre maintenance

Le pare-feu Windows est arrêté et le service est désactivé dès que vous cliquez sur le bouton Terminer

Windows Server Post-Setup Security Updates

Windows Server 2003

 To protect your server, all inbound connections, other than those specifically opened during setup or by policy settings, are blocked until you complete the following steps.

Step 1: Install Critical Security Updates [More Information](#)

Microsoft is continually updating Windows to help protect your server from viruses and other security threats as they are discovered. While this server is protected, you should download and install all of the latest security updates from Windows Update.

Some updates require that Windows be restarted. If Windows is restarted during the update process, you should return to Windows Update to ensure that all critical updates have been installed before continuing with these steps.

[Update this server](#)

Step 2: Configure Automatic Updates [More Information](#)

The Automatic Updates feature can automatically download the latest security updates on a schedule you specify. Now that this server has been updated, you can help ensure that it stays up-to-date by configuring Automatic Updates.

[Configure automatic updating for this server](#)

To close this page and allow inbound connections to this server, click Finish. For more information about blocking incoming connections, see the [Security Configuration Wizard Help](#).

Finish

PSSU

- S'exécute dans le cas:
 - D'une mise à jour de Windows NT 4.0 vers Windows 2003 SP1
 - D'une nouvelle installation de Windows 2003 SP1
- Ne s'exécute pas dans le cas:
 - D'une mise à jour de Windows 2000 vers Windows 2003 SP1
 - Mise à jour de Windows 2003 à SP1

Configuration

- Avec la commande Netsh
- Stratégie de groupe (GPO)
- Interface graphique

Assistant de configuration de sécurité

- Repère les ports ouverts
 - L'Assistant doit être exécuté de concert avec les applications et services nécessaires
- Sélectionne les rôles du serveur à partir d'une base de données de configuration
- Configure les services nécessaires
- Configure les ports pour le pare-feu Windows
- Configure la sécurité pour LDAP et SMB
- Configure une politique de vérification
- Configure les paramètres propres aux rôles joués par le serveur

Assistant de configuration de sécurité

- Configuration enregistrée dans un fichier XML
- Appliquée par l'assistant
 - Application d'une politique de sécurité existante
- Appliquée à partir de la ligne de commande
 - `scwcmd.exe configure /p:webserverpolicy.xml`
 - Utilisée dans les scripts
 - Scripts d'installation automatique

Comment convertir des politiques de sécurité en GPO?

- La commande à utiliser
 - `scwcmd transform [/p:policyfile.xml] [/g:GPODisplayName]`
- Copier le résultat dans sysvol
- L'administrateur doit lier la GPO au OU(s) désiré(s)

Programme

- Fonctions et outils de configuration de SP1
- Améliorations à la sécurité du système et du réseau
- Options de configuration
- Test dans un laboratoire virtuel

Améliorations à la sécurité du système

Prévention de l'exécution des données (DEP)

- Imposée par le matériel et le logiciel
- DEP par le matériel
 - Exige le soutien du processeur
 - Le processeur marque certaines zones de mémoire comme non exécutables à moins qu'elles contiennent spécifiquement du code exécutable
 - Peut causer des problèmes de compatibilité
- DEP par le logiciel
 - Fonctionne sur n'importe quel processeur qui prend en charge Windows Server 2003
 - Protège les programmes en binaire contre les progr. d'exploitation de la vulnérabilité relatifs au traitement des exceptions
 - Ne devrait pas causer de problèmes de compatibilité

Améliorations à la sécurité du système

Prévention de l'exécution des données

- Configuration de boot.ini
 - */noexecute=PolicyLevel*
 - OptIn – Activation de la DEP par le logiciel; activation de la DEP par le matériel uniquement pour les applications configurées à cette fin
 - OptOut – Activation de la DEP par le logiciel et le matériel; désactivation uniquement pour les applications de la liste d'exceptions
 - AlwaysOn – Activation permanente de la DEP par le logiciel et le matériel, sans tenir compte des exceptions configurées
 - AlwaysOff – Désactivation de la DEP par le logiciel et le matériel

Améliorations à la sécurité du réseau

Sécurité DCOM

- Autorisations DCOM
 - Lancement
 - Activation
 - Accès
- Sécurité à l'échelle du système
 - Configurée par l'administrateur
 - Touche tous les serveurs DCOM
 - Services de composants
 - Stratégie de groupe

Améliorations à la sécurité du réseau

Sécurité RPC

- RPC est un protocole de communication réseau
- Améliorations de SP1
 - Exige des connexions authentifiées
 - Incompatible avec les tubes nommés (named pipes)
- Paramètres de sécurité ADP
 - RestrictRemoteClients
 - EnableAuthEpResolution

Programme

- Fonctions et outils de configuration de SP1
- Améliorations à la sécurité du système et du réseau
- Options de configuration
- Test dans un laboratoire virtuel

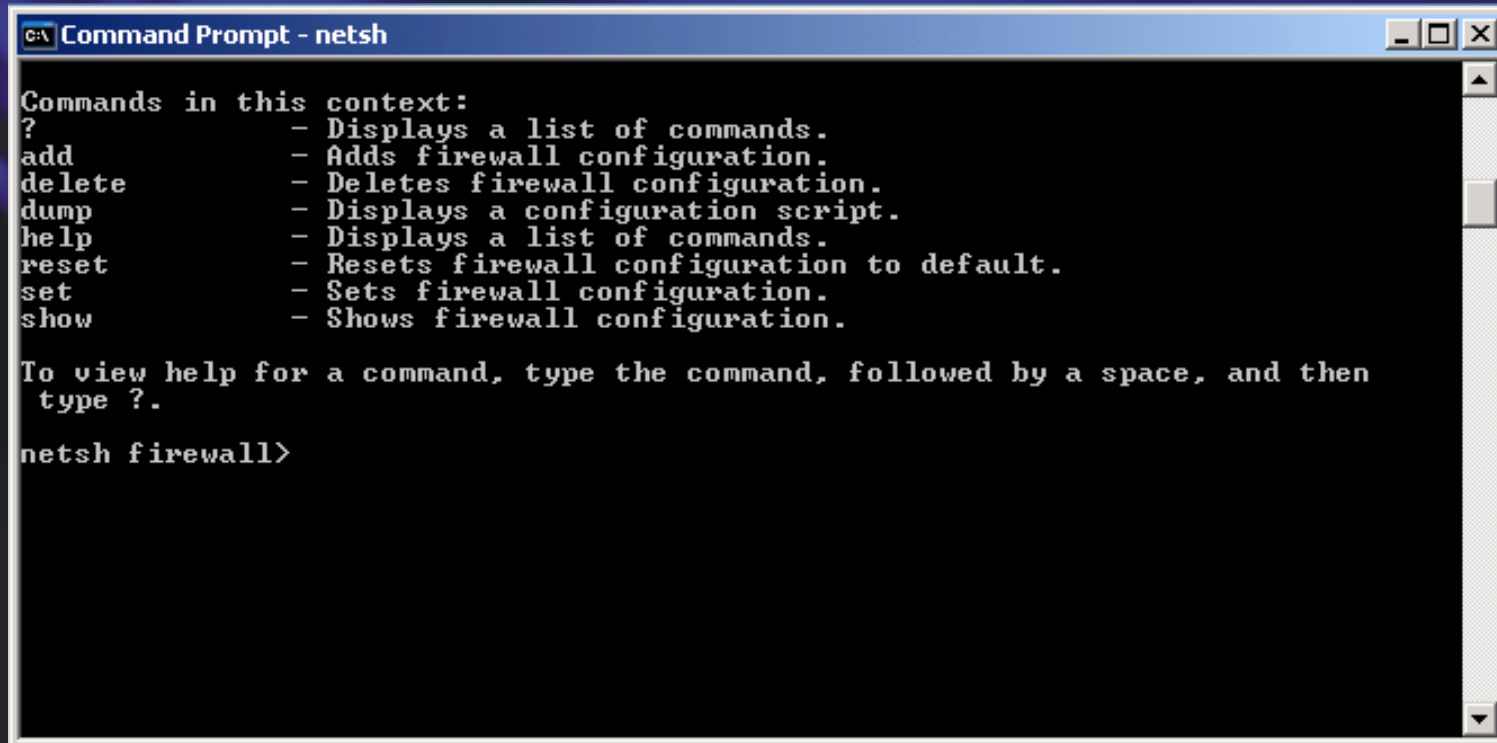
Gestion des fonctions

Pare-feu Windows (paramètres par défaut)

- ✓ Activé par défaut (installation intégrée seulement)
- ✓ Paramètres par défaut globaux de configuration et de restauration
- ✓ Profils multiples
- ✓ Activé sans exceptions
- ✓ Liste d'exceptions du pare-feu Windows
- ✓ Restrictions au sous-réseau local
- ✓ Prise en charge de la ligne de commande
- ✓ Sécurité à l'amorçage
- ✓ Prise en charge de l'installation automatique
- ✓ Prise en charge de RPC pour les services système

Gestion des fonctions

Config. ligne de commande avec Netsh



```
C:\> Command Prompt - netsh

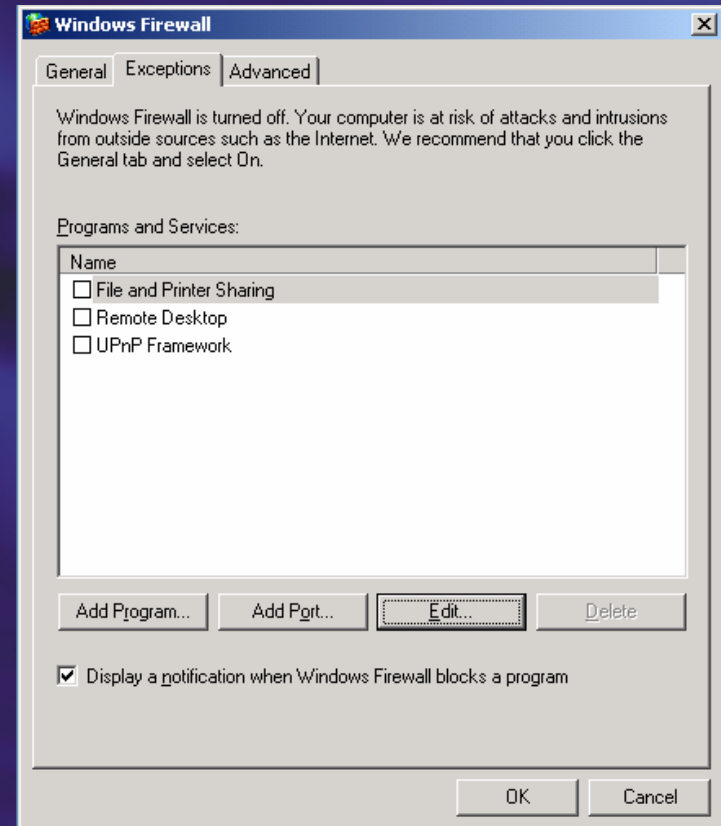
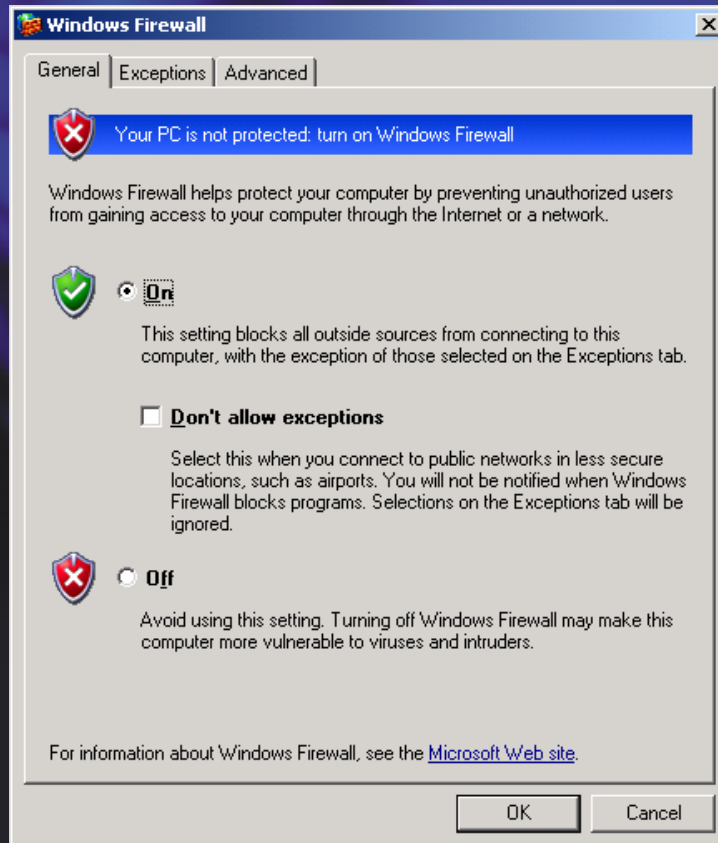
Commands in this context:
?           - Displays a list of commands.
add         - Adds firewall configuration.
delete      - Deletes firewall configuration.
dump        - Displays a configuration script.
help        - Displays a list of commands.
reset       - Resets firewall configuration to default.
set         - Sets firewall configuration.
show        - Shows firewall configuration.

To view help for a command, type the command, followed by a space, and then
type ?.

netsh firewall>
```

Gestion des fonctions

Interface graphique du pare-feu Windows



Gestion des fonctions

Stratégie de groupe

The screenshot shows the Group Policy console window titled "Console1 - [Console Root\Local Computer Policy\Computer Configuration\Administrative Templates\Network\Network Connec...". The left pane displays a tree view of the Group Policy hierarchy, with "Windows Firewall" selected under "Network Connections". The right pane shows a list of 14 settings, all of which are currently "Not configured".

Setting	State
Windows Firewall: Protect all network connections	Not configured
Windows Firewall: Do not allow exceptions	Not configured
Windows Firewall: Define program exceptions	Not configured
Windows Firewall: Allow local program exceptions	Not configured
Windows Firewall: Allow remote administration exception	Not configured
Windows Firewall: Allow file and printer sharing exception	Not configured
Windows Firewall: Allow ICMP exceptions	Not configured
Windows Firewall: Allow Remote Desktop exception	Not configured
Windows Firewall: Allow UPnP framework exception	Not configured
Windows Firewall: Prohibit notifications	Not configured
Windows Firewall: Allow logging	Not configured
Windows Firewall: Prohibit unicast response to multicast or broad...	Not configured
Windows Firewall: Define port exceptions	Not configured
Windows Firewall: Allow local port exceptions	Not configured

démonstration

Pare-feu Windows

- ◆ **Modification de l'état du pare-feu Windows et du service de partage de connexions Internet (ICS) pour activer la configuration du pare-feu**
- ◆ **Configuration du pare-feu Windows à l'aide de l'interface graphique, de la ligne de commande et de la stratégie de groupe**

Programme

- Fonctions et outils de configuration de SP1
- Améliorations à la sécurité du système et du réseau
- Options de configuration
- Test dans un laboratoire virtuel

Test dans un laboratoire virtuel

Pourquoi tester?

- Connaître les effets de la mise à jour
- Planifier le déploiement
- Régler les problèmes éventuels dans l'environnement de test
- Aplanir le processus de mise à niveau

Comment tester l'installation de SP1 dans votre environnement

1

Créer un environnement de test représentatif des ordinateurs, des logiciels et des services de votre entreprise

2

Installer le SP1 sur chaque ordinateur et appliquer les paramètres et modèles de sécurité

3

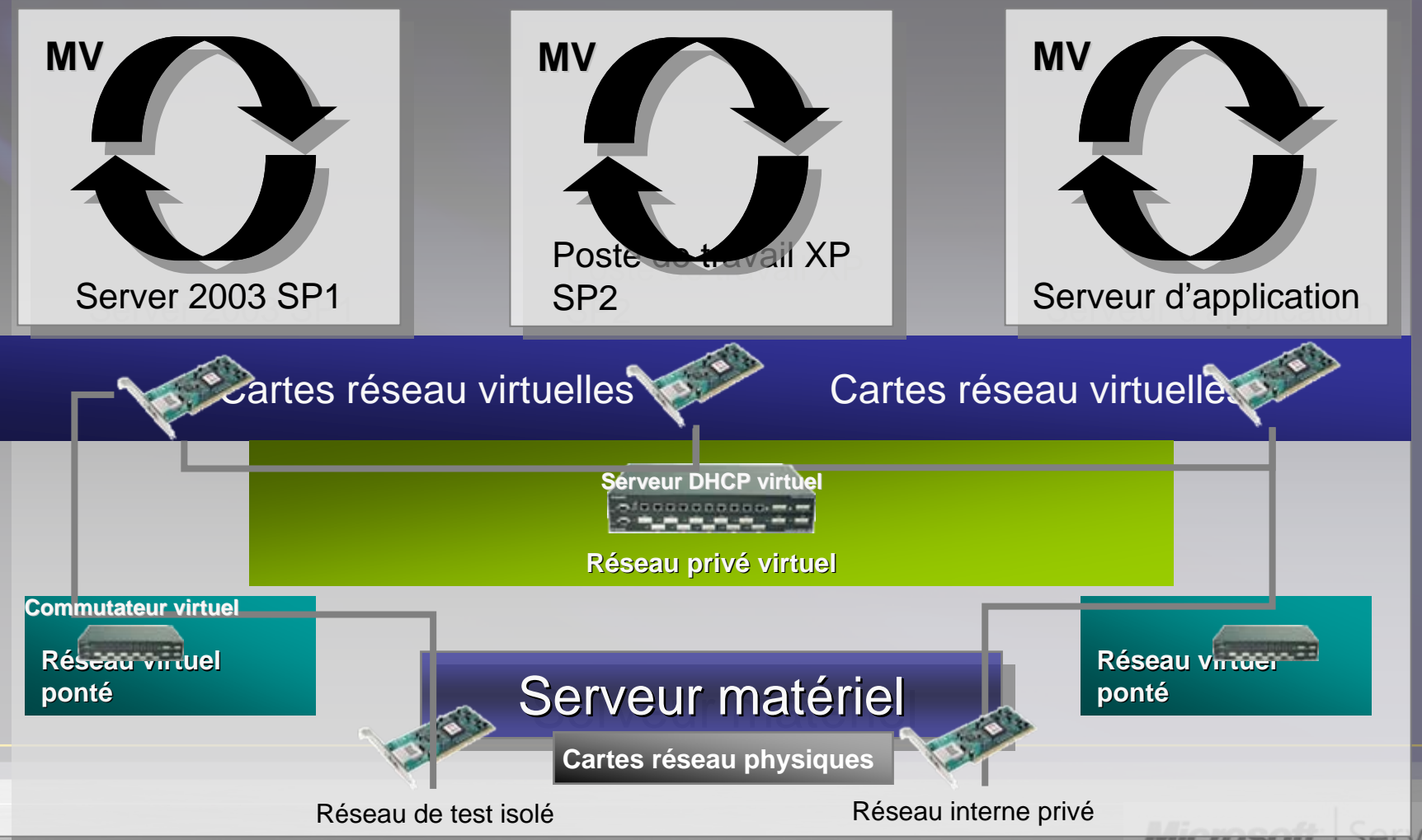
Vérifier que les logiciels et les services continuent de bien fonctionner



Tester avec des réseaux virtuels

Environnement de test virtuel pour le SP1

Réseau de test virtuel

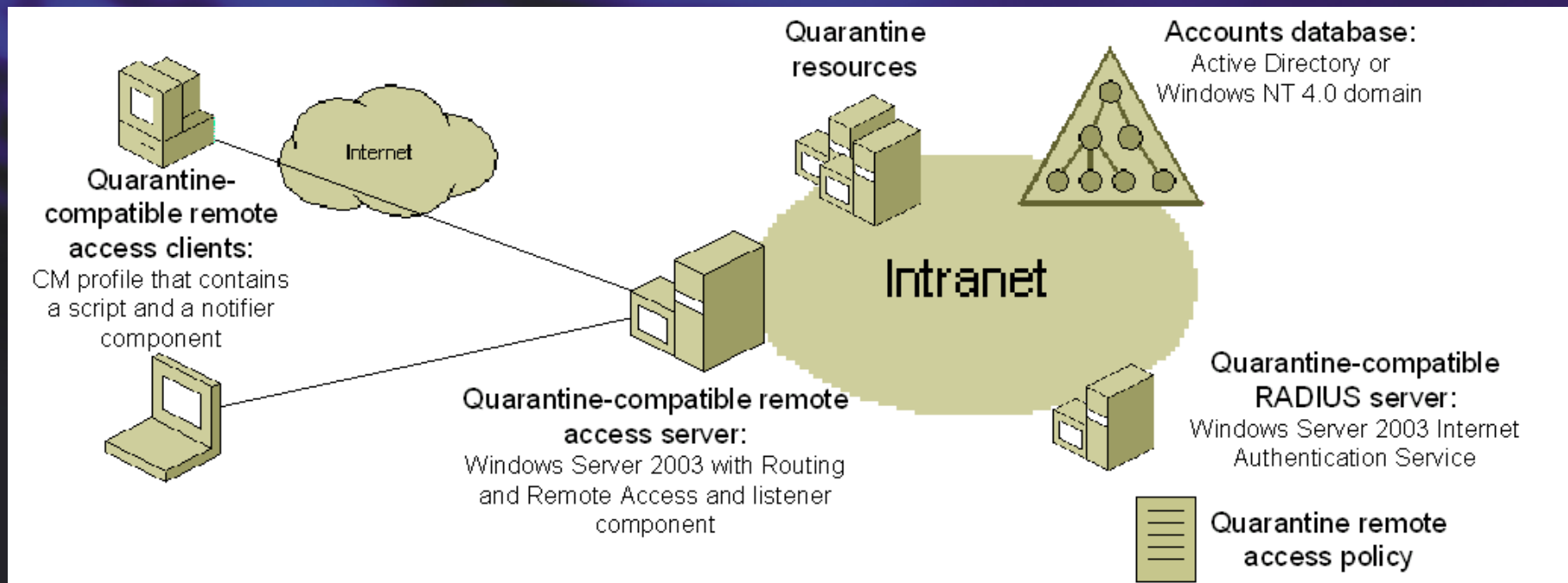


**Permet la quarantaine
automatisée**

VPN Microsoft

- Permet de valider l'intégrité d'un poste avant de lui donner accès au réseau de l'entreprise:
 - La version du Service pack et la dernière rustine de sécurité
 - La bonne version de signature de l'antivirus
 - Que le routage soit désactivé.
 - Que le garde-barrière soit installé et activé
 - Que le préservateur d'écran soit en fonction et protégé par un mot de passe

Concept



Composantes requises

- La composante “notifier” est Rqc.exe
- Le “listener” Rqs.exe
- Le profil CM créé à partir de Windows Server 2003 CMAK
- Un serveur d'accès VPN Microsoft (RRAS ou ISA 2004)

Lien de référence:

<http://download.microsoft.com/download/0/7/e/07ed1953-0ab5-41ea-b5da-41cf8bb9cdae/Quarantine.doc>

CMAK

Connection Manager Administration Kit Wizard [X]

Custom Actions

You can specify programs to start automatically before, during, or after the connection to your service.

Custom actions of the same type are run in the order in which they appear in the list. To view custom actions of a specific type, select the action type from the drop-down list.

Action type:

Custom actions:

Description	Action Type
-------------	-------------

[Up] [Down]

Qu'est-ce que ABDE?

- « Acces Base Directory Enumeration »
- Enfin on l'attendait depuis longtemps celle-là
- Requiert SP1 mais n'en fait pas partie
- S'applique au niveau du partage

Résumé

- Windows Server 2003 SP1 offre de nombreuses améliorations à la sécurité.
- Ces améliorations rehaussent la sécurité et aident à protéger contre les attaques.
- Les nouvelles fonctions de sécurité devraient être testées à fond avant leur mise en œuvre.
- SP1 contient aussi une foule de nouveaux outils pour vous aider à gérer les paramètres et les rôles du serveur.

Avenir du GSIQ

- Avant la pause, discussion sur la suite...

Pour en savoir plus

- Windows Server 2003 SP1
 - <http://www.microsoft.com/windowsserver2003/downloads/servicepacks/sp1/default.msp>
- Virtualisation d'un serveur
 - www.microsoft.com/windowsserver2003/techinfo/overview/virtualization.msp
- Quarantaine
 - <http://download.microsoft.com/download/0/7/e/07ed1953-0ab5-41ea-b5da-41cf8bb9cdae/Quarantine.doc>
- GUSMM
 - <http://www.gusmm.org/>

Problèmes de compatibilité avec Windows 2003 SP1

- <http://support.microsoft.com/?kbid=896367>

- Microsoft Exchange 2003

- <http://www.microsoft.com/exchange/evaluation/sysreqs/2003.msp>

- Microsoft Exchange 2003 en cluster

- <http://support.microsoft.com/kb/841561>

- ISA 2004

- <http://www.microsoft.com/downloads/details.aspx?familyid=69c5d85c-5c80-473c-9cb4-60dda75d568d&displaylang=en>