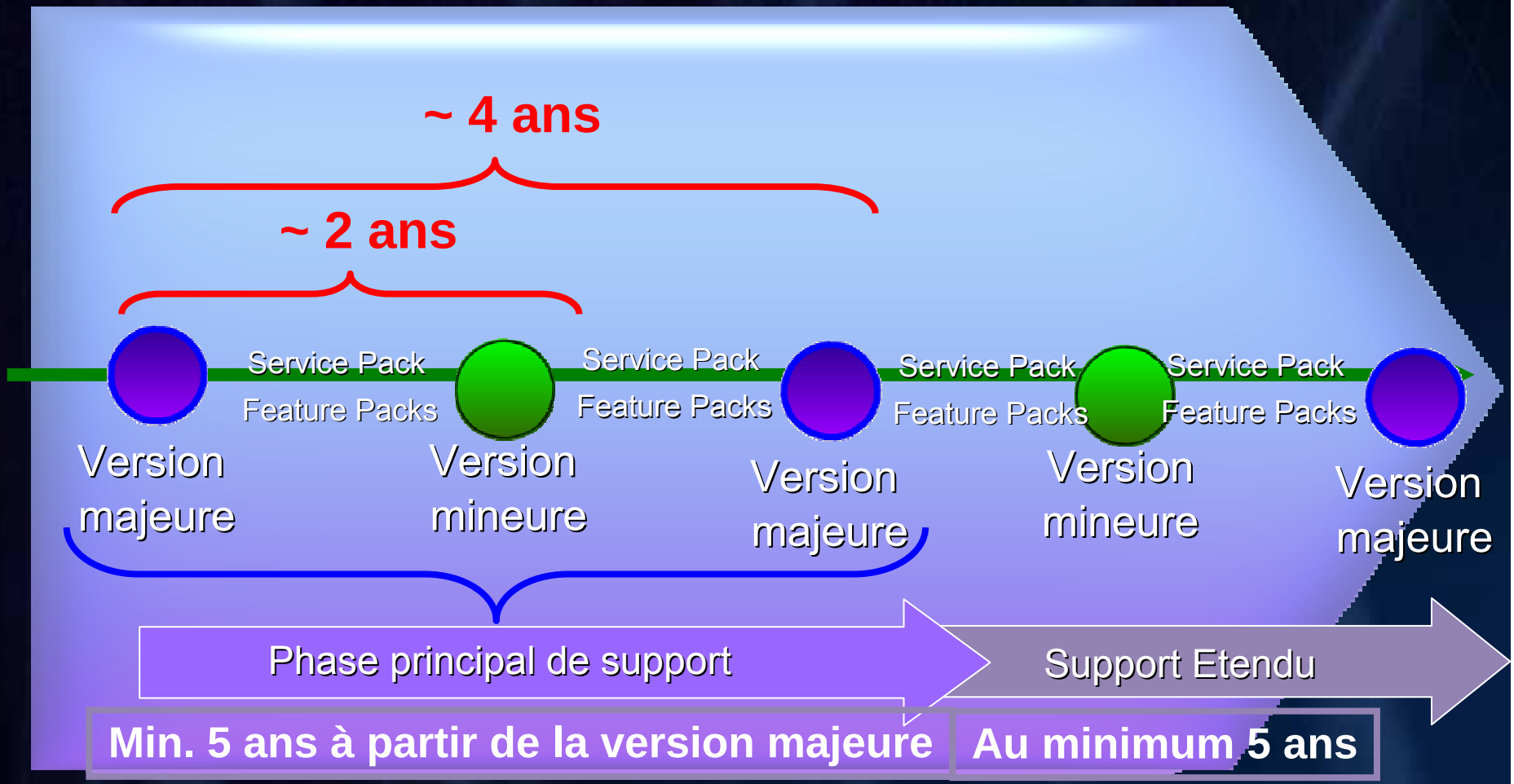
Nouveautés de Windows 2003 SP1 et Windows 2003 - R2

OSSIR – Septembre 2005

Fabrice Meillon
Architecte Infrastructure - ***Microsoft*** France
http://www.microsoft.com/france/technet

Plateforme

Cycle de disponibilité des versions Windows server



http://www.microsoft.com/windowsserver2003/evaluation/overview/roadmap.mspx

Feuille de route

Plateforme

2009

- Windows Server “Longhorn R2”

2007

- Windows Server “Longhorn”

H2 2005

- Windows Server 2003 Compute Cluster Edition
- Windows Storage Server “R2”
- Windows Small Business Server “R2”
- **Windows Server 2003 x86 et x64 “R2”**
- Windows Server “Longhorn” Beta

H1 2005

- Windows Server Update Services
- Windows Small Business Server Service Pack 1
- Windows Server 2003 x64 Editions
- **Windows Server 2003 Service Pack 1**

SP1 : Challenges clés pour nos clients

- Sécurité
  - Pouvoir sécuriser de façon simple leurs serveurs
  - Etre de mesure de lutter contre les attaques réseau dès l'installation
  - Etre en mesure de faire face aux prochaines attaques ☺
- Robustesse
  - Minimiser les interruptions réseau
- Performance
  - Améliorer les performances

Plateforme

Windows Server 2003 SP1

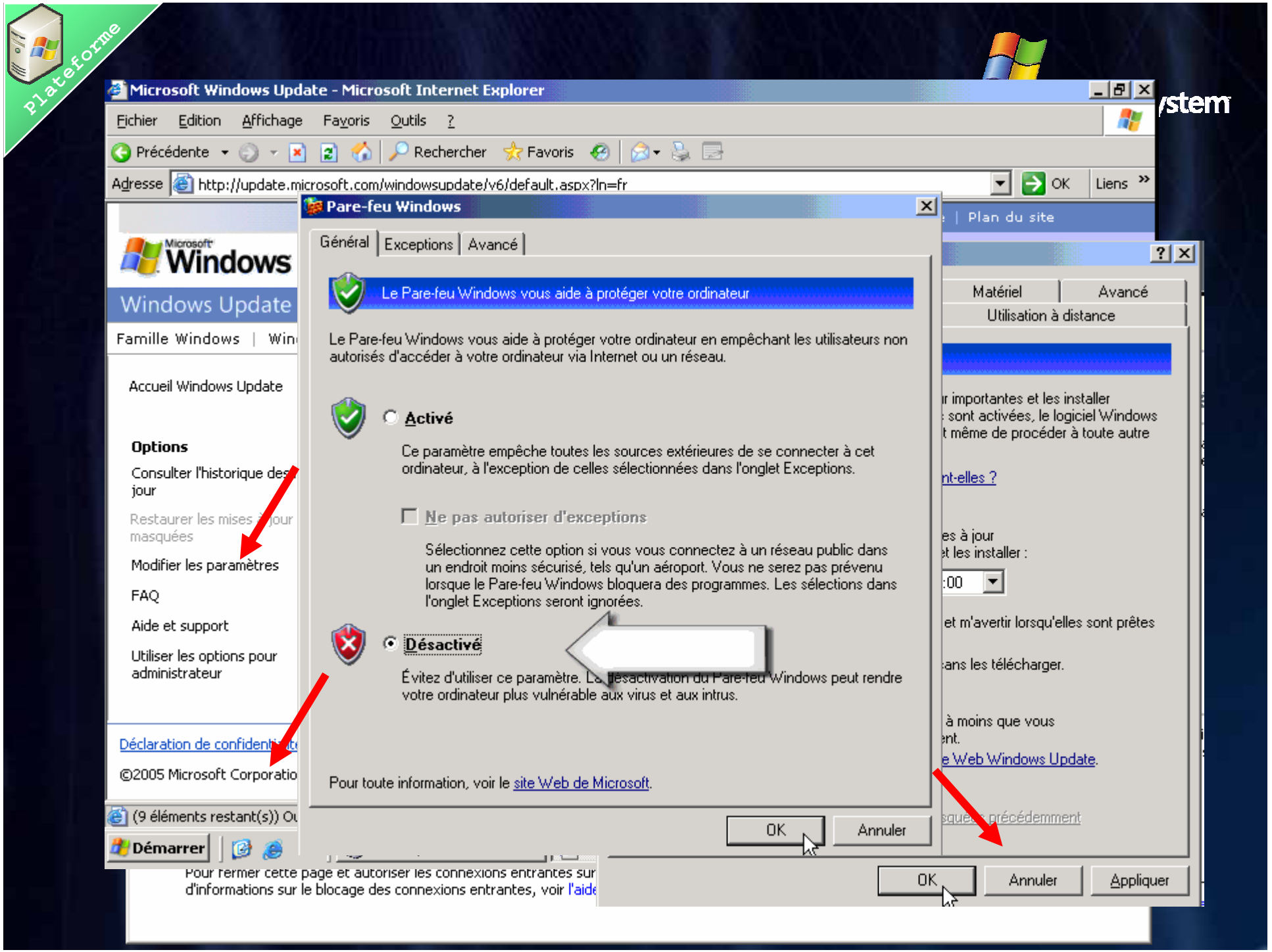
Continuer l'effort : l'Informatique de confiance

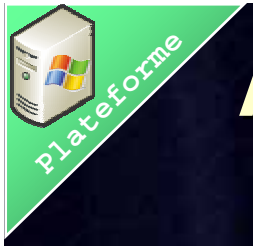
- Sécurité améliorée
  - Aider à la protection des nouveaux serveurs
  - Réduire la surface d'attaque des serveurs
  - Evolutions pertinentes du SP2 de Windows XP
  - Support de l'isolation VPN
  - Gestion et Audit de IIS 6.0
  - Terminal Server
- Active Directory
- Fiabilité et Performances améliorées
  - Amélioration 10%+ pour TPC, TPC-H, SAP, SSL, etc.

http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/BookofSP1/ed9975ba-3933-4e28-bcb4-2b80d7865b7.mspx

Mise à jour de sécurité post installation pour Windows Server (PSSU)

- Conçue pour sécuriser les serveurs après leur installation (premier démarrage) et avant l'application des derniers correctifs de sécurité
- Lancement au premier administrateur ouvrant une session si le pare feu Windows n'a pas été explicitement activé dans le script d'installation sans assistance ou les stratégies de groupe
- Bloques les connexions entrantes jusqu'au clique sur "Terminer"


Plateforme
Microsoft Windows Update - Microsoft Internet Explorer
Fichier Edition Affichage Favoris Outils ?
Précédente Rechercher Favoris
Adresse http://update.microsoft.com/windowsupdate/v6/default.aspx?ln=fr
OK Liens
Windows Update
Famille Windows
Accueil Windows Update
Options
Consulter l'historique des mises à jour
Restaurer les mises à jour masquées
Modifier les paramètres
FAQ
Aide et support
Utiliser les options pour administrateur
Déclaration de confidentialité
©2005 Microsoft Corporation
Plan du site
Pare-feu Windows
Général Exceptions Avancé
Le Pare-feu Windows vous aide à protéger votre ordinateur
Le Pare-feu Windows vous aide à protéger votre ordinateur en empêchant les utilisateurs non autorisés d'accéder à votre ordinateur via Internet ou un réseau.
Activé
Ce paramètre empêche toutes les sources extérieures de se connecter à cet ordinateur, à l'exception de celles sélectionnées dans l'onglet Exceptions.
Ne pas autoriser d'exceptions
Sélectionnez cette option si vous vous connectez à un réseau public dans un endroit moins sécurisé, tels qu'un aéroport. Vous ne serez pas prévenu lorsque le Pare-feu Windows bloquera des programmes. Les sélections dans l'onglet Exceptions seront ignorées.
Désactivé
Évitez d'utiliser ce paramètre. La désactivation du Pare-feu Windows peut rendre votre ordinateur plus vulnérable aux virus et aux intrus.
Pour toute information, voir le site Web de Microsoft.
OK Annuler
Matériel Avancé
Utilisation à distance
Annuler Appliquer
Démarrer

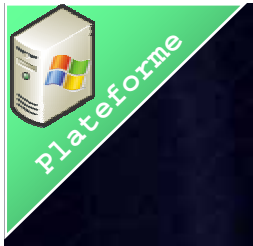


Assistant Configuration de la sécurité (SCW)

- La sécurité doit être appliquée mais construire son propre modèle n'est pas si simple pour beaucoup
- Objectif de l'assistant : Aider les administrateurs dans la réduction de la surface d'attaque des serveurs Windows en tenant compte des rôles du serveur
- Composant optionnel de Windows Server 2003
- Simple et fonctionnel
  - Simple d'utilisation, basé sur des questions/réponses
  - Automatique en regard des guides papiers
  - Entièrement testé et supporté par Microsoft

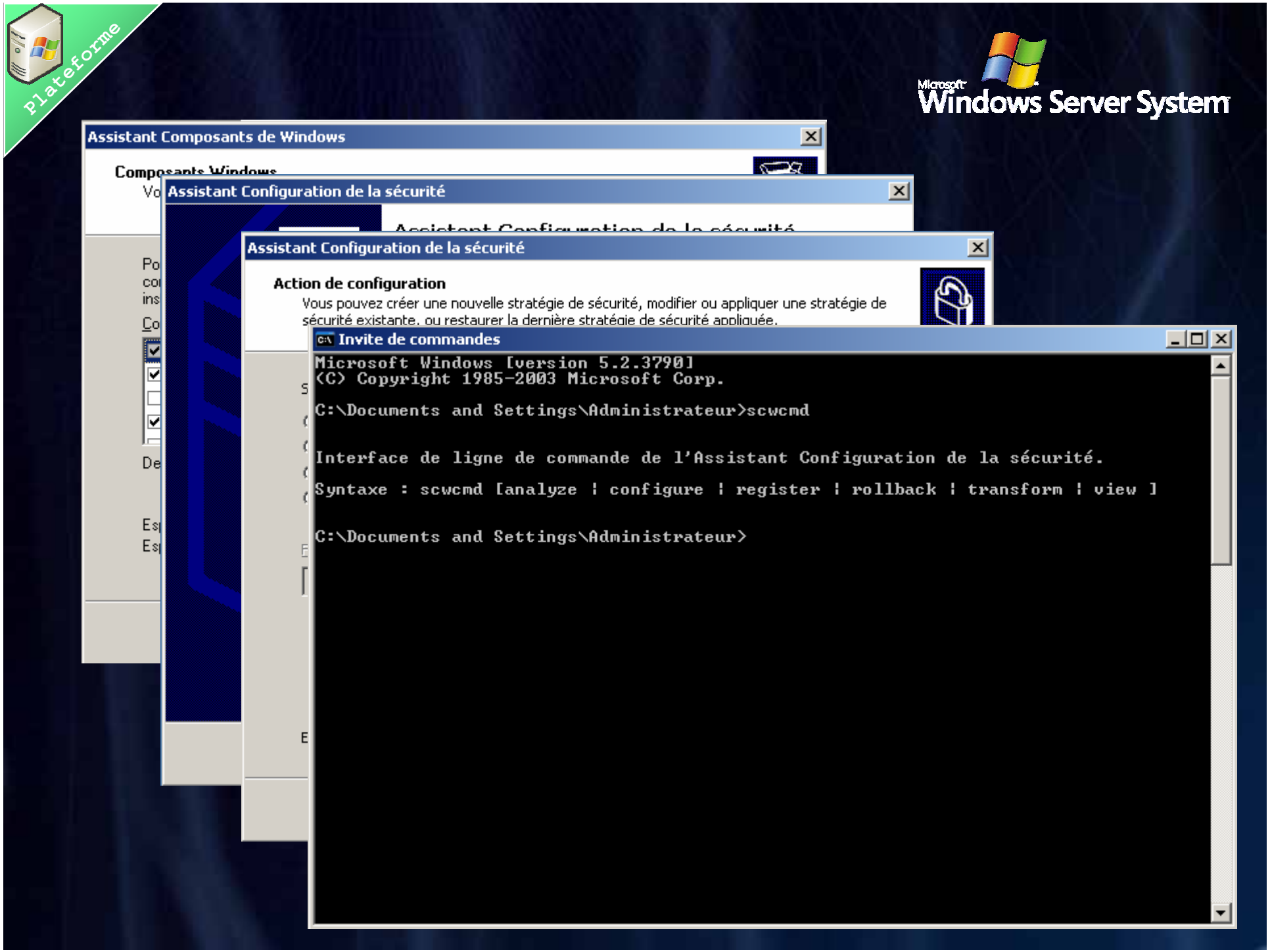
Assistant Configuration de la Sécurité

- Réduction de la surface d'attaque pour les serveurs Windows
  - Basé sur des modèles ←→ des rôles
  - Désactive les services non nécessaires
  - Désactive les Extensions Web IIS non nécessaires
  - Bloque les ports non utilisés, y compris sur les systèmes à plusieurs cartes réseau
  - Aide la sécurisation des ports laissés ouverts par IPsec
  - Réduit l'exposition des protocoles (signature LDAP & SMB, Compatibilité Lan Man et LMHash...)
  - Configure l'audit (SACLs)
  - Possibilité d'importer des modèles SCE
- Fichiers xml



Opérations liées à SCW

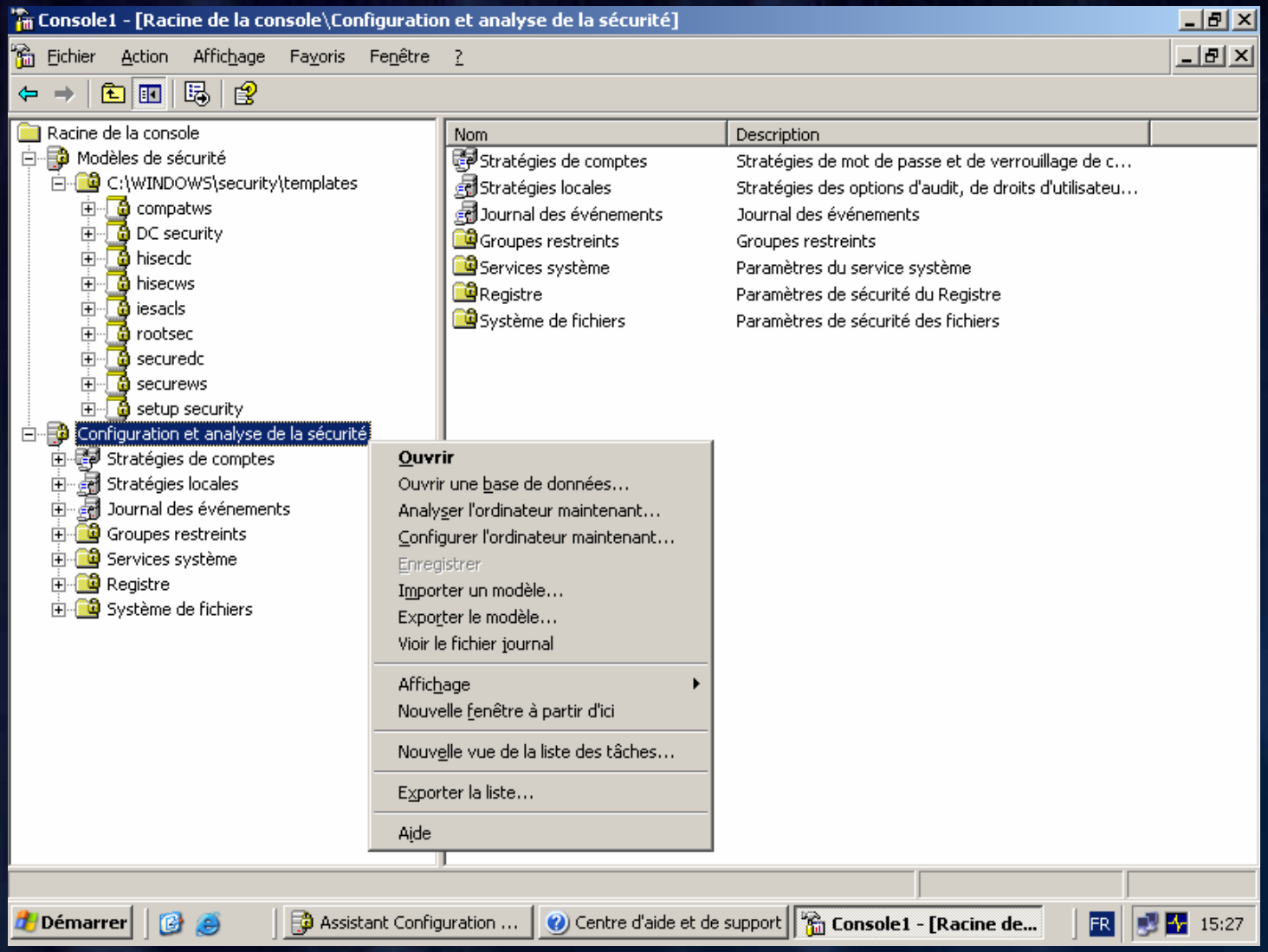
- Retour en arrière
- Analyse, pour vérifier la conformité des machines par rapport aux stratégies
- Configuration et analyse à distance
  - Interface graphique
  - Ligne de commande pour configuration et analyse à distance et en masse (scwcmd.exe)
- Intégration à Active Directory pour un déploiement par stratégies de groupe
- Possibilité d'éditer les stratégies créées, lorsque les machines sont réaffectées
- Vues XSL de la Base de Connaissances, des stratégies et des résultats d'analyse

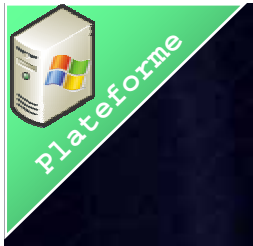

Plateforme
Microsoft Windows Server System
Assistant Composants de Windows
Assistant Configuration de la sécurité
Assistant Configuration de la sécurité
Action de configuration
Vous pouvez créer une nouvelle stratégie de sécurité, modifier ou appliquer une stratégie de sécurité existante, ou restaurer la dernière stratégie de sécurité appliquée.
Invite de commandes
Microsoft Windows [version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.
C:\Documents and Settings\Administrateur>scwcmd
Interface de ligne de commande de l'Assistant Configuration de la sécurité.
Syntaxe : scwcmd [analyze | configure | register | rollback | transform | view]
C:\Documents and Settings\Administrateur>

Néanmoins limité ex: SCW et IPsec

- Sécurité au niveau port
  - Créer des restrictions de sécurité sur le trafic réseau TCP ou UDP entrant pour chaque port, en fonction de l'adresse IP d'où provient le trafic.
    - IPSec nécessite une configuration par machine
    - SCW permet une configuration avec la règle par défaut pour les clients (Accepter le trafic entrant non signé et non crypté)
- SCW ne crée pas de stratégies IPSec “évoluées”
  - Communications DC-vers-DC
  - Segmentation Réseau
  - Quarantaine

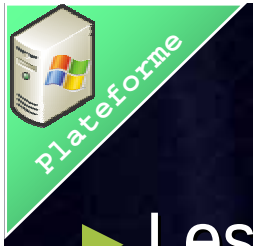
Configuration et Analyse de la Sécurité (SCE)





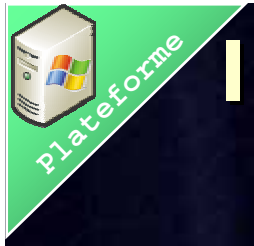
SCE vs SCW

- Choisir le bon outil
  - Appliquer une configuration générique
    - Utiliser les guides et l'outil Configuration et Analyse de la Sécurité (SCE)
  - Créer une configuration
    - Utiliser l'un ou l'autre
    - SCW est plus flexible et couvre plus d'options
  - Comprendre les paramètres
    - Utiliser les guides et la documentation de SCW
- Possibilité d'inclure des modèles SCE dans une stratégie SCW
  - Paramètres d'audit personnalisés
  - Personnalisation des permissions DACLs and SACLs
  - Paramètres non couverts par SCW



SCE vs SCW

- Les + de SCW
  - Couvre plus de domaine
  - Moins de risque “de détruire” le système
  - Les stratégies seront mieux optimiser
  - Directement utilisable à distance
  - Moins de connaissance requise
  - Possibilité d’extension
  - Meilleur support du retour arrière
- Les + de SCE
  - Plus flexible
  - Plus facile de personnaliser les paramètres individuels
  - Directement utilisable par les stratégies de groupe



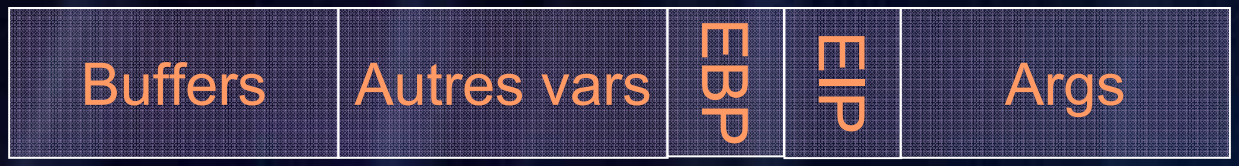
Intégration des évolutions ‘pertinentes’ apportées par Windows XP SP2

- Pare-feu Windows
  - Configuration et options
- Protection de RPC/DCOM
  - Objets RPC exécutés avec des privilèges réduits
  - Nouvelles clés de registre RPC
  - Restrictions d’accès DCOM complémentaires
- Réduire l’exposition à certains dépassement de mémoire tampon

Compilation avec /GS (Visual Studio 2003)

Une pile normale

Sens croissant des adresses



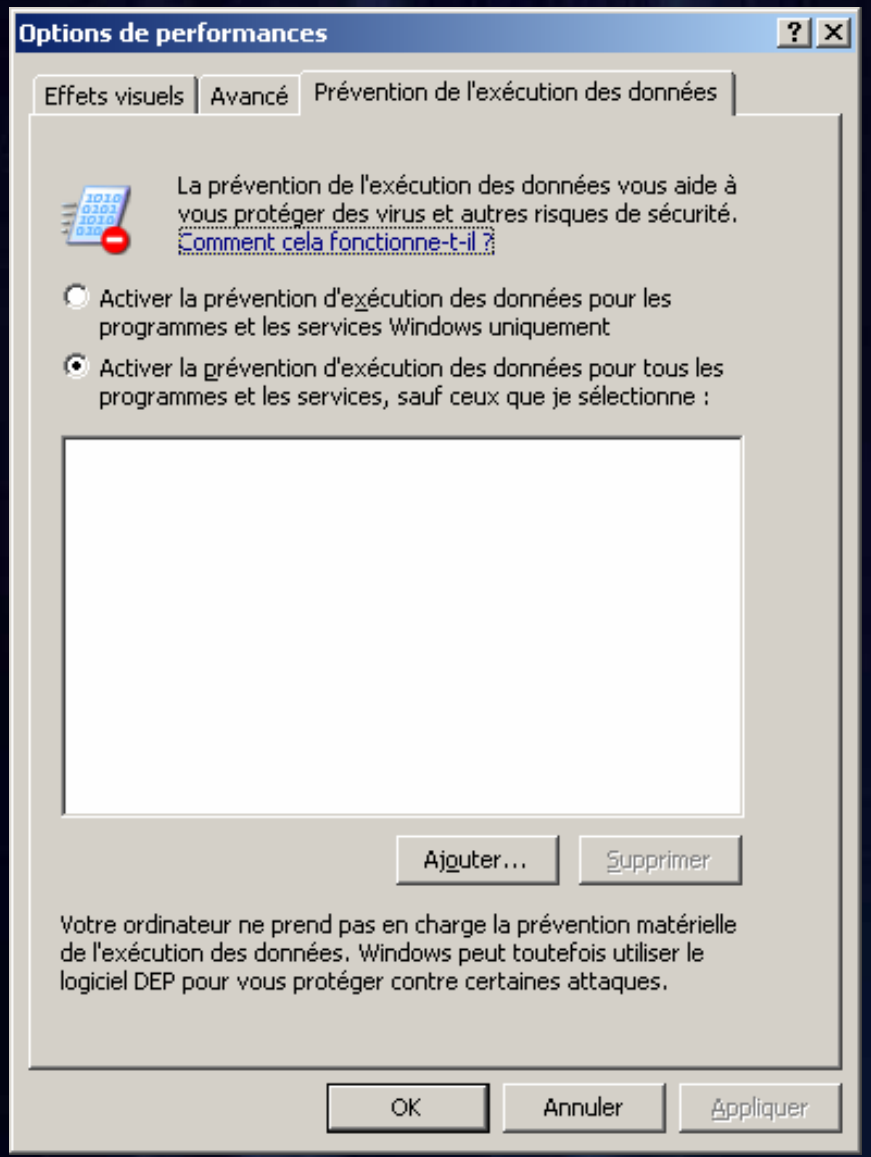
Pile VC++ 2002 (avec /GS)

Pile VC++ 2003 (avec /GS et les *safe exceptions*)

Prévention de l'exécution des données

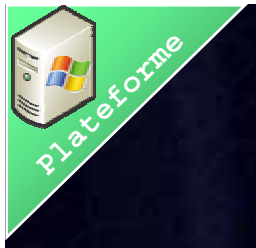
- Ne permettre l'exécution de code en mémoire que dans des régions spécifiquement marquées comme execute
- Prévention exécution de données matériel
  - Nécessite le support du processeur contre l'exécution (NX : No Execute ou XD : Execute Disable) (AMD64 / Itanium /Intel EMT)
- Prévention exécution de données logiciel
  - Applicable pour n'importe quel processus s'exécutant sur l'OS
  - Activé par défaut pour les binaires Windows.
- Configuration
  - Boot.ini switch "/noexecute=*PolicyLevel*"
    - OptIn / OptOut / AlwaysOn / AlwaysOff
  - Configuration graphique possible au travers des options de performances

Prévention de l'exécution des données



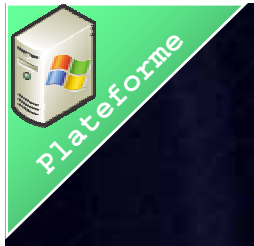
Impact sur les applications

- Pas de code dynamique
- Assurez-vous que votre application n'exécute par de code dans un segment *de données*
- Assurez-vous que vos applications et drivers supporte le mode PAE
- Utiliser les instructions valides pour que votre code fonctionne
- Tester votre code sur des processeurs 64 bit et 32 bits en mode PAE avec *protection de l'exécution*



Evolutions au niveau d'Active Directory

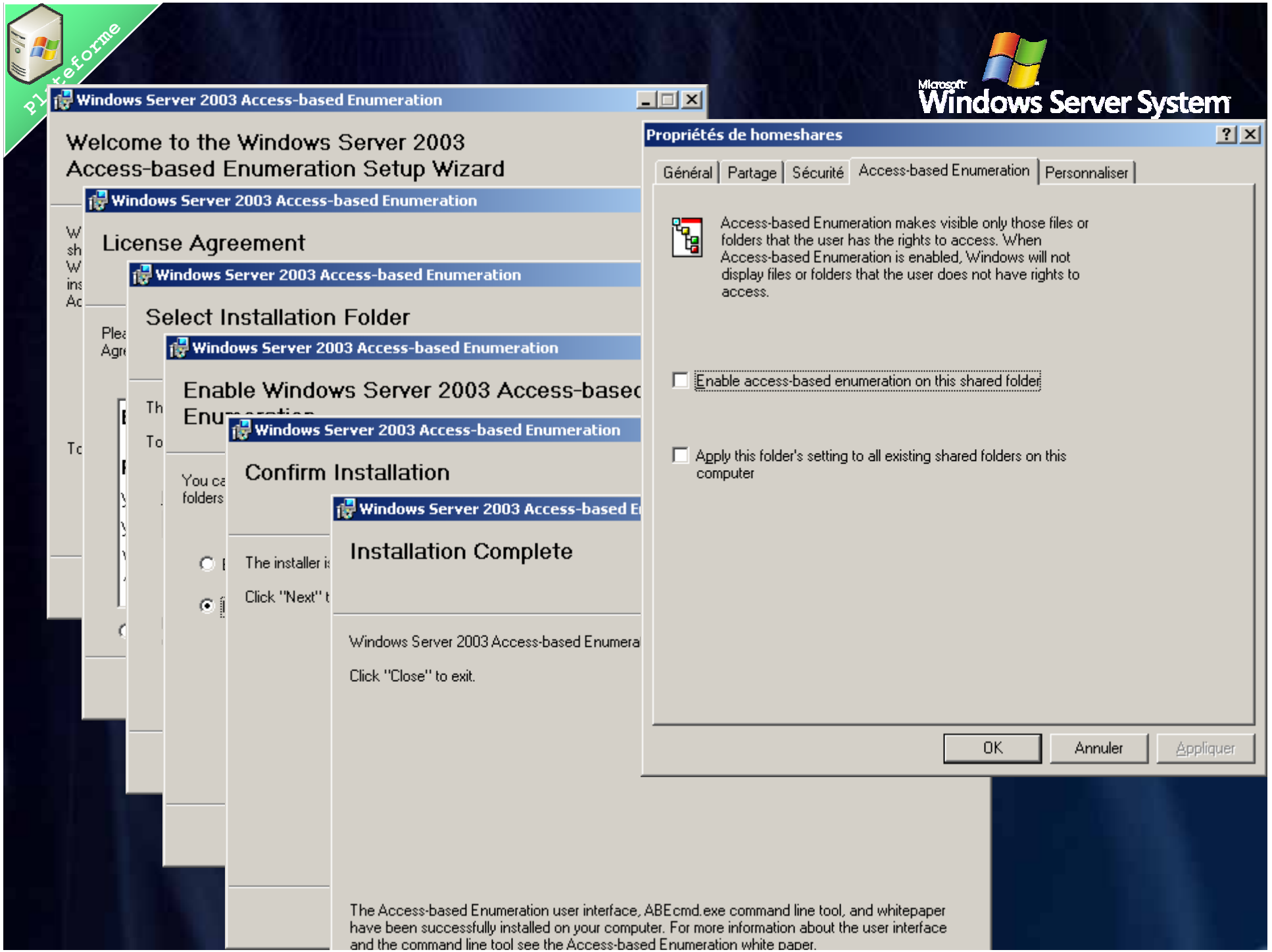
- Mise à jour d'ADPREP (Sysvol)
- Installation depuis un media (DNS)
- Evolution DCdiag (tests DNS)
- Ntdsutil (suppression des DCs)
- FSMO : status et ID Events
- Restreindre l'accès sur certains attributs
- Rappel pour les sauvegardes des partitions d'AD
- Support pour la virtualisation des DCs
- Drag and Drop dans la mmc Utilisateurs et ordinateurs Active Directory



Windows Server 2003 SP1

Quelques autres nouveautés

- *Access-based Enumeration* – ne montrer aux utilisateurs que les fichiers et répertoires auxquels ils ont accès. Outil de configuration : http://go.microsoft.com/?linkid=2726554
- RRAS : support des outils de quarantaine (rqc/rqs)
- Terminal Services : utilisation de SSL/TLS 1.0 pour l'authentification du serveur et le chiffrement (client RDP 5.2 sur Windows 2000, XP, 2003)
  What's New in TS : http://go.microsoft.com/?linkid=2700421


Windows Server 2003 Access-based Enumeration
Welcome to the Windows Server 2003 Access-based Enumeration Setup Wizard
Windows Server 2003 Access-based Enumeration
License Agreement
Windows Server 2003 Access-based Enumeration
Select Installation Folder
Windows Server 2003 Access-based Enumeration
Enable Windows Server 2003 Access-based Enumeration
Windows Server 2003 Access-based Enumeration
Confirm Installation
Windows Server 2003 Access-based E
Installation Complete
Windows Server 2003 Access-based Enumera
Click "Close" to exit.
The Access-based Enumeration user interface, ABEcmd.exe command line tool, and whitepaper have been successfully installed on your computer. For more information about the user interface and the command line tool see the Access-based Enumeration white paper.
Propriétés de homeshares
Général
Partage
Sécurité
Access-based Enumeration
Personnaliser
Access-based Enumeration makes visible only those files or folders that the user has the rights to access. When Access-based Enumeration is enabled, Windows will not display files or folders that the user does not have rights to access.
Enable access-based enumeration on this shared folder
Apply this folder's setting to all existing shared folders on this computer
OK
Annuler
Appliquer
Microsoft
Windows Server System

Plateforme

Windows Server 2003 “R2”

Qu’est-ce que c’est ?

- R2 est la prochaine version de Windows Server 2003
- Une nouvelle version particulière (1er version mineure) :
  - Base = WS2003 SP1,
  - Composants nouveaux installés optionnellement,
  - Même compatibilité des applications, qualité, stabilité et performance,
  - Les Services Packs à venir seront applicables sur WS2003 et R2.
- Licence et distribution :
  - R2 remplace Windows Server 2003 dans le réseau de distribution,
  - Pas de coût supplémentaire pour les serveurs sous SA/EA, disponible comme une nouvelle licence serveur sinon.
  - Pas de nouvelle CAL pour R2 – utilisation des CALs WS2003,
  - Même cycle de vie que WS2003 (fin du support en 2013).

Plateforme

Microsoft Windows Server 2003 R2

Infrastructure

Collaboration

Gestion et déploiement des serveurs d'agence

- Sauvegarde et administration centralisée des services de partage de fichiers et d'impression,
- Réplication et disponibilité des données
- Gestion hardware à distance.

Gestion de l'identité

(Active Directory Federation Services)

- Authentification unique WEB,
- Interopérabilité avec les offres SSO WEB du marché.
- Services de d'authentification et d'autorisation Unix

Gestion du stockage

- Gestion plus simple des SAN,,
- Gestion des ressources de stockage.

Intégration de packs de fonctionnalités WS2003

- Windows SharePoint Services V2, Active Directory Application Mode (ADAM), Services pour Unix, iSCSI.

Plateforme

Windows Server 2003 “R2”

Serveur d’agence, la situation

- La plupart des entreprises consolident leurs serveurs centraux :
  - Approche maîtrisée, WS2003 est adapté.
- Réflexions concernant la consolidation des serveurs d’agence :
  - Gain de TCO, mais problème plus complexe.

Serveurs centralisés ?

+ Coûts d’administration réduits.
- Impact du WAN sur les utilisateurs
  Bande passante, latence, disponibilité.

OU

Serveurs en agence ?

+ Performances (locales), disponibilité des services
- Coût de gestion plus élevé :
  Sauvegarde, restauration, administration

Plateforme

Windows Server 2003 “R2”

Serveur d’agence

- Optimisation du trafic WAN.
- Cache/Mirroring du contenu dans les agences.
- Gestion des serveurs (F&P, sauvegardes) centralisée.
- Disponibilité des services indépendante du WAN.

Windows Server 2003 “R2”

Réplication DFS

- Remplace FRS (File Replication Service) :
  - Réarchitecturé pour améliorer la disponibilité et les performances.
- Nouvelles fonctions d’administration :
  - Console MMC, config via AD, supervision via WMI, pack d’admin MOM.
- Utilise un algorithme de compression et d’échange (Remote Differential Compression) permettant d’envoyer de façon compressée les seuls octets modifiés.

Exemple : modification du titre d’un PPT de 3,5 Mo, synchro = 16Ko

Connexion	Sauvegarde des 3,5 Mo	Sauvegarde des octets modifiés
Modem 56K bps	10 minutes	3 secondes
DSL 500K bps	70 secondes	<1 seconde

Plateforme

Windows Server 2003 “R2”

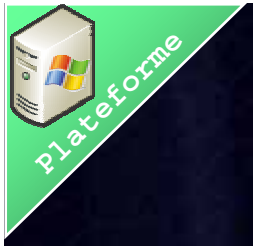
Fédération d’identités

- Logon unique pour les applications WEB,
- Support de différents jetons de sécurité (ex SAML, Kerberos, x509).
- Intéropérabilité :
  - Basée sur WS-*,
  - Fonctionne avec IIS 6.0 ou tout serveur WEB supportant WS-Federation,
  - Fonctionne avec IBM, Netegrity, Oblix, OpenNetwork, RSA et Ping Identity.

Windows Server 2003 “R2”

Gestion du stockage

- Mise en oeuvre simple de SAN :
  - Provisionning de SAN pour 3-15 serveurs, 2 switches,
  - Création, gestion, suppression de LUNs avec un outil graphique,
  - Support des SANs compatibles VDS (microsoftstoragepartners.com).
- Gestion des ressources de stockage :
  - Gestion des quotas par répertoire,
  - « File screening » limiter les types de fichiers autorisés sur un serveur,
  - Rapports automatisés pour aider à la planification de capacité.
- Support NFS :
  - Apporté par le ‘Windows Subsystem for Unix Applications’ (ex SFU).



Windows Server 2003 “R2”

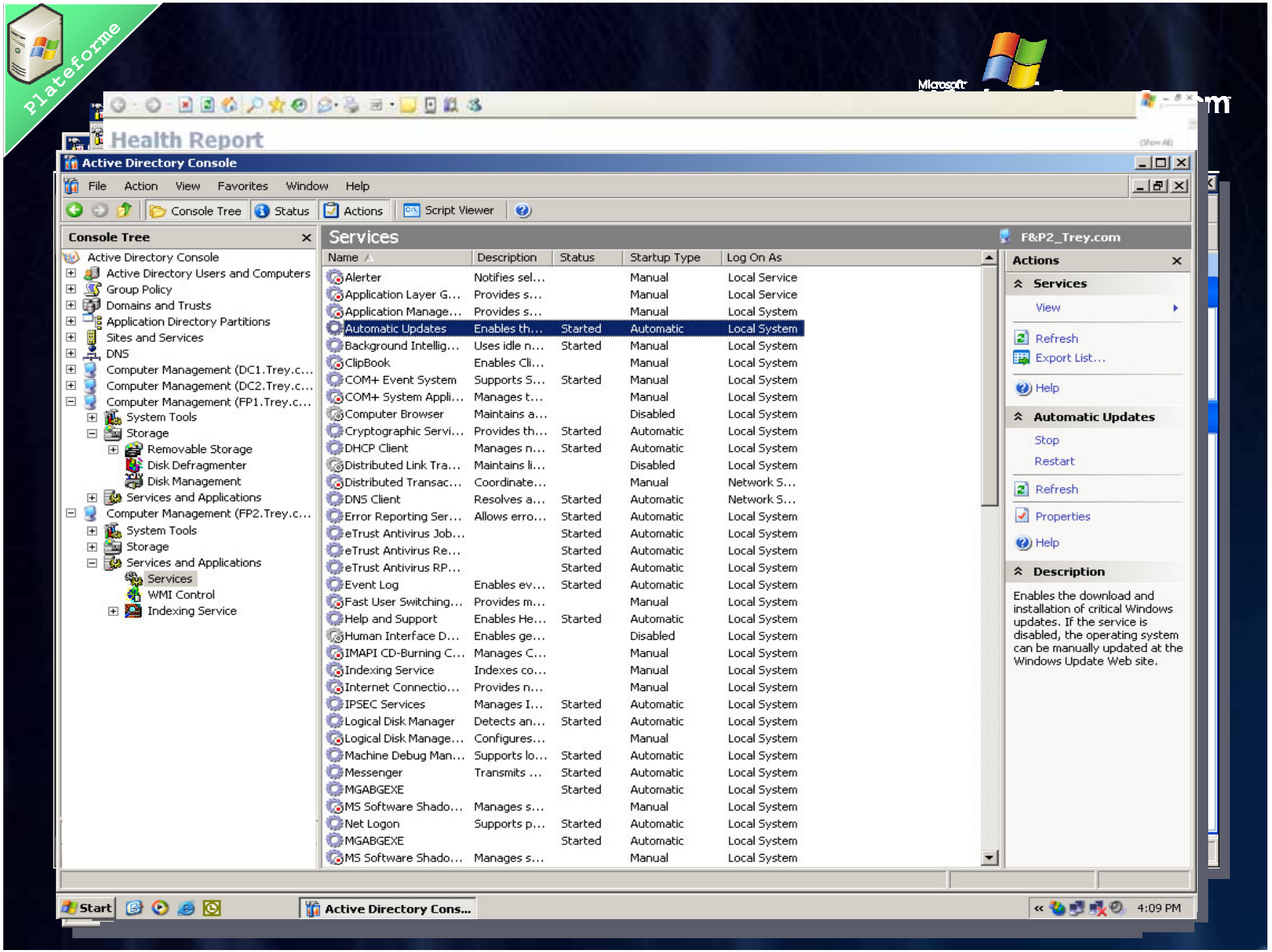
Gestion Hardware et administration

- Support IPMI
- Support du protocole Web Services for Management (WS-Management)
- Console d’administration pour le rôle de serveur de fichiers et d’impression.
- Console d’administration pour la réplication
- Console d’administration pour le stockage
- Console de Management Microsoft (MMC 3.0)

Windows Server 2003 “R2”

Ce qui a changé depuis les spécifications d’origine

- L’infrastructure NAP (Network Access Protection), pour la mise en quarantaine réseau, sera intégrée avec Longhorn Server :
  - Alliance Microsoft et Cisco,
  - Permettra une interopérabilité avec NAC (Network Admission Control) de Cisco,
  - NAP apportera le support d’IPSEC.
- Les technologies d’encapsulation http/https des protocoles SMB ou RDP (« Anywhere Access ») seront aussi fournies avec Longhorn Server.


Plateforme
Health Report
Active Directory Console
File Action View Favorites Window Help
Console Tree Status Actions Script Viewer
Console Tree
Active Directory Console
Active Directory Users and Computers
Group Policy
Domains and Trusts
Application Directory Partitions
Sites and Services
DNS
Computer Management (DC1.Trey.c...
Computer Management (DC2.Trey.c...
Computer Management (FP1.Trey.c...
System Tools
Storage
Removable Storage
Disk Defragmenter
Disk Management
Services and Applications
Computer Management (FP2.Trey.c...
System Tools
Storage
Services and Applications
Services
WMI Control
Indexing Service
Services
F&P2_Trey.com
Name Description Status Startup Type Log On As
Alerter Notifies sel... Manual Local Service
Application Layer G... Provides s... Manual Local Service
Application Manage... Provides s... Manual Local System
Automatic Updates Enables th... Started Automatic Local System
Background Intellig... Uses idle n... Started Manual Local System
ClipBook Enables Cli... Manual Local System
COM+ Event System Supports S... Started Manual Local System
COM+ System Appli... Manages t... Manual Local System
Computer Browser Maintains a... Disabled Local System
Cryptographic Servi... Provides th... Started Automatic Local System
DHCP Client Manages n... Started Automatic Local System
Distributed Link Tra... Maintains li... Disabled Local System
Distributed Transac... Coordinate... Manual Network S...
DNS Client Resolves a... Started Automatic Network S...
Error Reporting Ser... Allows erro... Started Automatic Local System
eTrust Antivirus Job... Started Automatic Local System
eTrust Antivirus Re... Started Automatic Local System
eTrust Antivirus RP... Started Automatic Local System
Event Log Enables ev... Started Automatic Local System
Fast User Switching... Provides m... Manual Local System
Help and Support Enables He... Started Automatic Local System
Human Interface D... Enables ge... Disabled Local System
IMAPI CD-Burning C... Manages C... Manual Local System
Indexing Service Indexes co... Manual Local System
Internet Connectio... Provides n... Manual Local System
IPSEC Services Manages I... Started Automatic Local System
Logical Disk Manager Detects an... Started Automatic Local System
Logical Disk Manage... Configures... Manual Local System
Machine Debug Man... Supports lo... Started Automatic Local System
Messenger Transmits ... Started Automatic Local System
MGABGEXE Started Automatic Local System
MS Software Shado... Manages s... Manual Local System
Net Logon Supports p... Started Automatic Local System
MGABGEXE Started Automatic Local System
MS Software Shado... Manages s... Manual Local System
Actions
Services
View
Refresh
Export List...
Help
Automatic Updates
Stop
Restart
Refresh
Properties
Help
Description
Enables the download and installation of critical Windows updates. If the service is disabled, the operating system can be manually updated at the Windows Update Web site.
Start
Active Directory Cons...
4:09 PM

Quelques ressources utiles

- SP1 de Windows 2003
  http://www.microsoft.com/technet/prodtechnol/windowsserver2003/servicepack/default.mspx
- Windows 2003 R2
  http://www.microsoft.com/windowsserver2003/R2/overview/default.mspx
- Site Sécurité
  http://www.microsoft.com/france/securite
- Séminaire Technet, Webcasts et Chats
  http://www.microsoft.com/france/technet/seminaires
- Newsgroup : sécurité
  microsoft.public.fr.securite

Plateforme

Questions / Réponses


Plateforme
Microsoft
Votre potentiel, notre passion.™