Windows NT 4.0 SP4

Le Service Pack 4 et la sécurité

Patrick CHAMBET
pchambet@fr.ibm.com
e-business Services

Planning

- Introduction
- Généralités
- Nouveautés
- Impact sur les autres composants
- Manques
- A vous de jouer !

Introduction

- **Rappel et définitions**
  - Service Pack = évolution majeure
  - HotFix = réparation d'urgence
- **Principes**
  - Imbrication des correctifs
  - D'où ordre chronologique strict

Généralités

- **Download:**
  ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/*usa*/nt40/ussp4/

- **600 *modifications* (Q150734)**
  - **Inclue les HotFixes post-SP3**
  - **Autres bugs corrigés**
  - **Nouvelles fonctionnalités**

Nouveautés

- An 2000 et euro:
  - Compatibilité an 2000
  - Symbole “€”
  - MDAC 2.0 (MS Data Access Components)

Nouveautés

- Management
  - Quotas utilisateurs
  - Nouveaux évènements dans l'Event Log:
    - Clean shutdown event (ID 6006)
    - Dirty shutdown event (ID 6008)
    - System version event (ID 6009)

Nouveautés

- Sécurité
  - Security Configuration Manager (SCM)
  - NTLM v.2
  - Secure Channel amélioré
  - Privilège de sécurité pour consulter l'Event Log (SE_SECURITY_NAME)
  - Certificate Wizard

Nouveautés

- Networking
  - TAPI 2.1
  - RRAS (with HotFix 3)
  - PPTP
  - DCOM/HTTP Tunneling (port 80)
  - IGMP v.2 (utilisateurs mobiles)
  - Remote Winsock (DNS/Port 53)

Nouveautés

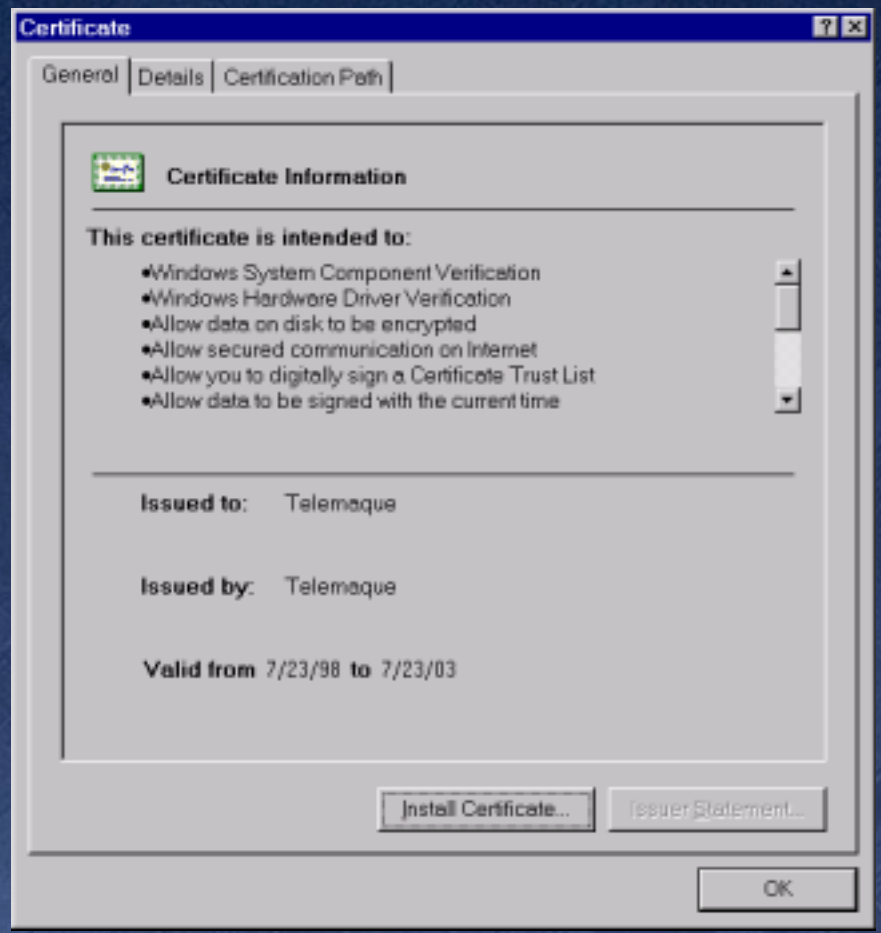
- Analyse des outils:
  - Certificate Wizard
  - Security Configuration Editor (SCE ou SCM)

Certificate Wizard

- Visualisation et installation des certificats X.509 aisée
- Plus de *iisca.exe* pour installer les certificats des Certification Authorities dans la métabase d'IIS

Certificate Wizard

- **Viewer:**



Certificate Wizard

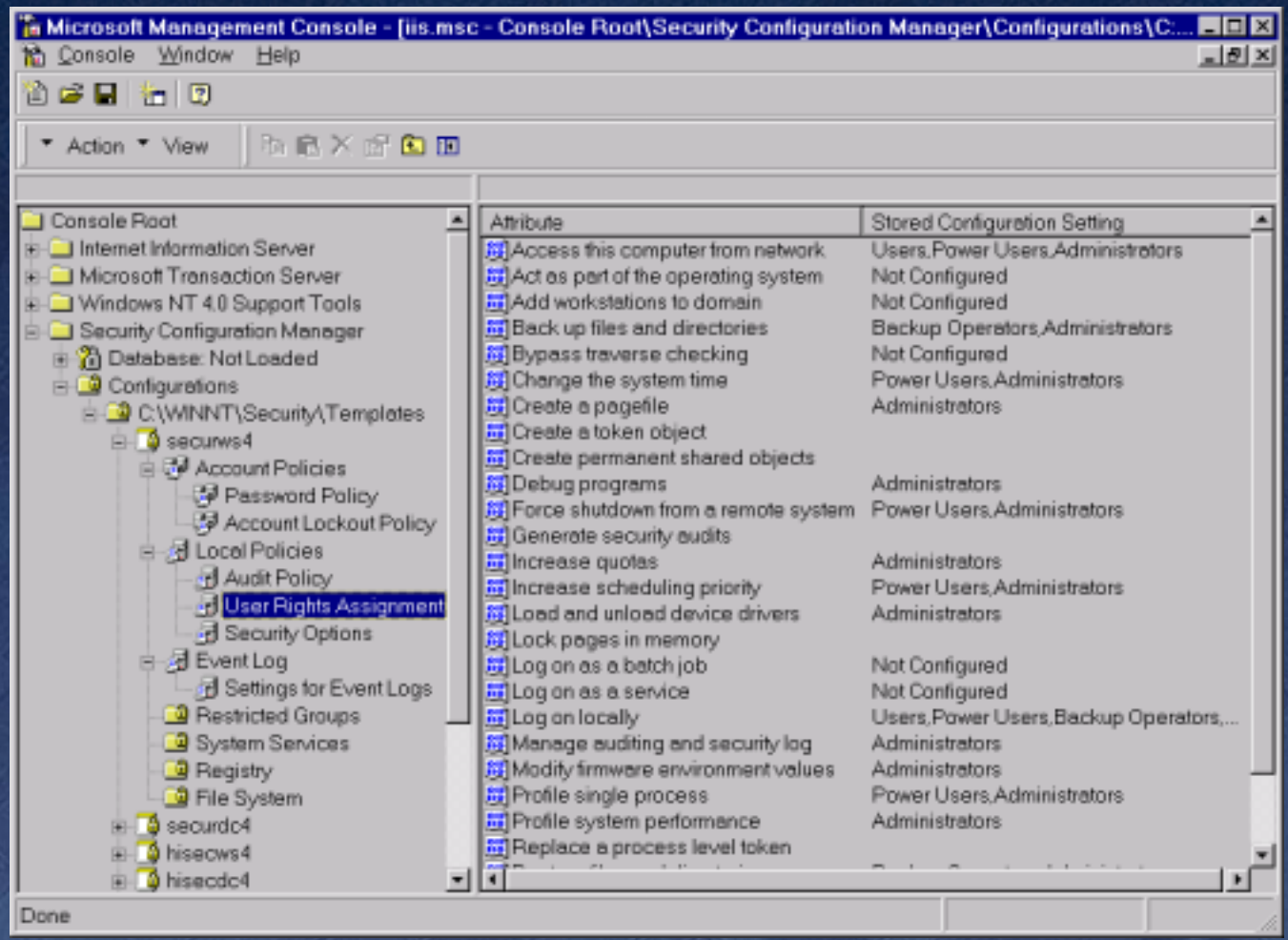
- **Installer:**

SCE

- Option du SP4 ou téléchargeable:
  ftp://ftp.microsoft.com/bussys/winnt/winnt-public/tools/scm/
- Snap-in à ajouter à la MMC
- Permet:
  - De définir des modèles de sécurité
  - De les appliquer à un système
  - D'analyser un système par rapport au modèle
- Attention, nouvel onglet "Sécurité"
  (voir Q195509 et Q195227)

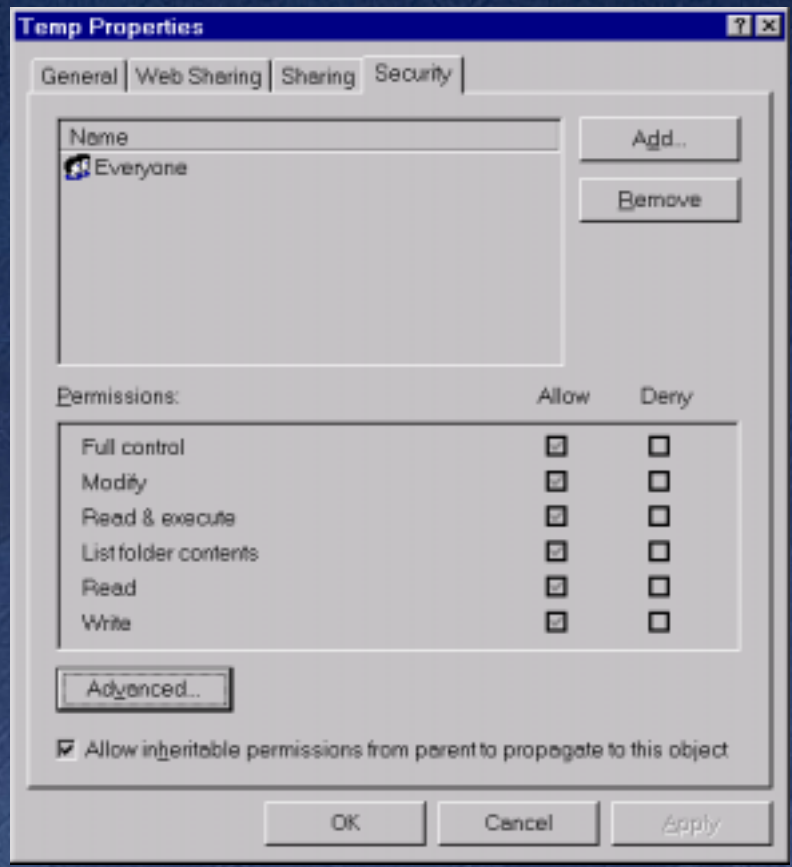
SCE

- **MMC:**



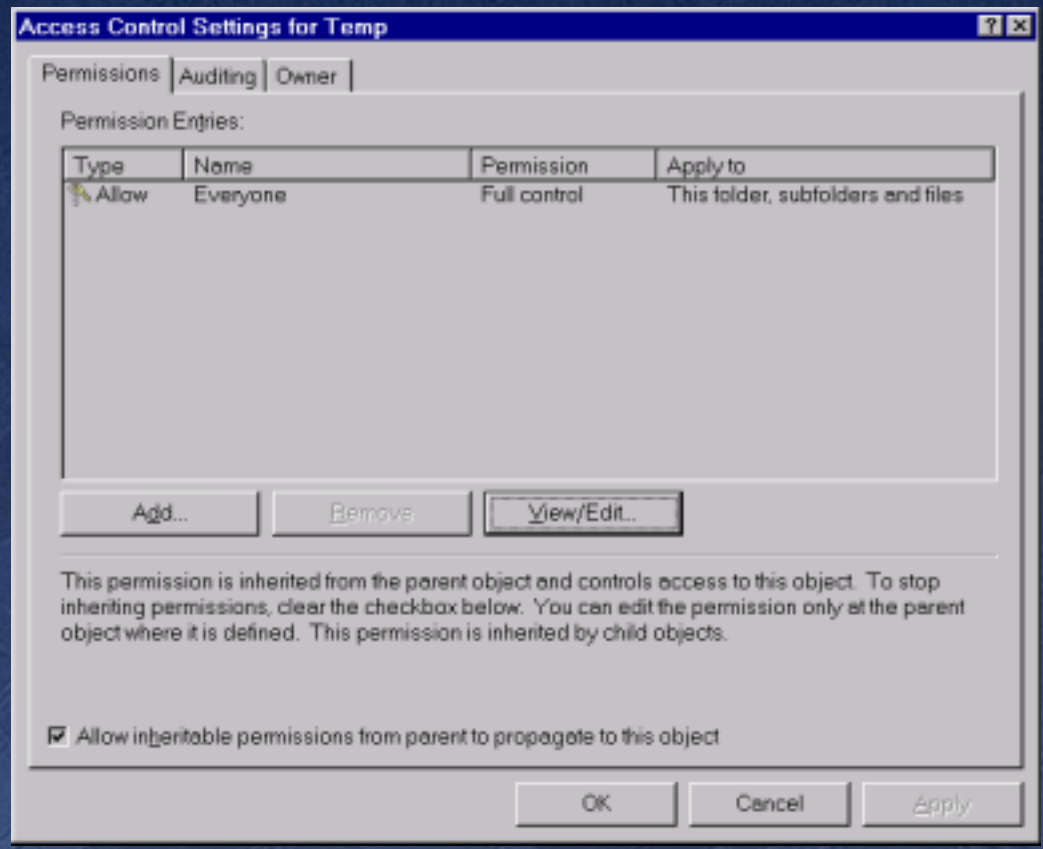
SCE

- Onglet “Sécurité”:



SCE

- **Onglet “Sécurité”:**



Impact sur les autres composants

- Option Pack
  - IIS (fix noms longs, performances, ...)
  - Certificate Server (29 Février, ...)
  - MTS (classes Java de sécurité)
  - MSMQ
  - ADO 2.0

Impact sur les autres composants

- IE 4.01
  - Installe le SP1 d'IE 4.01 automatiquement
- MS Proxy Server
  - fix Web Administration Tool

Manques...

- Le SP4 semble ne PAS corriger systématiquement:
  - Teardrop2 (LSASS.EXE)
  - RedButton (Null Sessions et connection à la Registry distante)

  … à vérifier au cas par cas.

SP4 SP1 ?

- **Fix du SP4 (Update.exe et .inf)**
  - **MTS (Q196021)**
  - **IIS directories (non documenté à ce jour)**
- **Désinstallation manuelle des HotFixes post-SP3 (Q194334)**
  - **Directories: \WINNT\$NtUninstallQxxxxxx$**
  - **Registry Keys: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Hotfix**

Tout de suite, la suite...

- Déjà des HotFixes post-SP4
  - Nprpc-fix : RPC DoS
  - Sms-fix : fuite mémoire agent SNMP
  - Clik-fix : accès Iomega Clik 40!
  - Tcpip-fix : intermediate network driver

- Downloadez-les ici:

  ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP4/

A vous de jouer !

- Réappliquer le SP4 après toute installation importante
- Surveiller les HotFixes post-SP4
- Utiliser le SCE (avec planification)