

ASR3



Windows Server® 2008

Partie 1 – principes de base

Plan

1- Historique

2- Qu'est-ce que Windows Server 2008 ?

3- Les versions de Windows Server 2008

4- Le système de sécurité

- La SAD
- Les DACL
- Les droits utilisateur
- Les audits

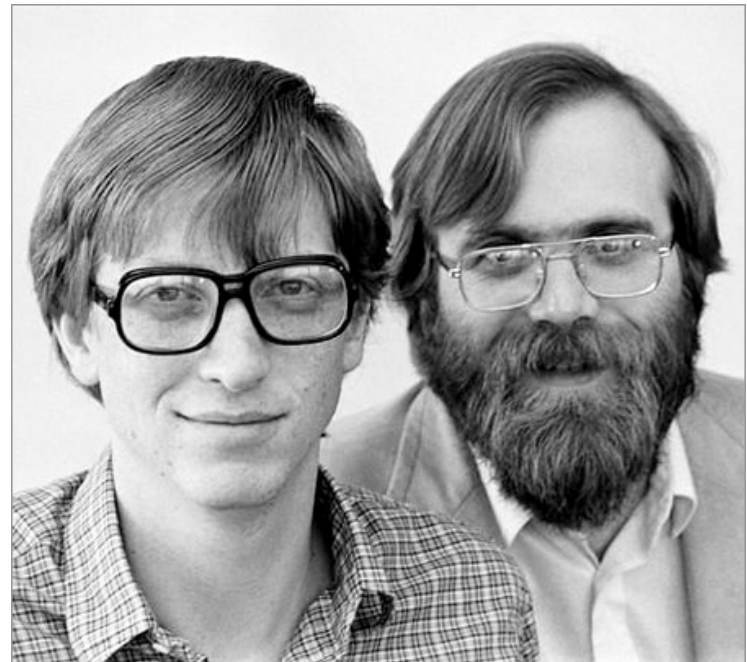
5- Notion de domaine

6- Relation d'approbation

1

Historique de MicroSoft Windows

- **1955** : naissance à Seattle de William Henry **Gates III** KBE
- **1975** : fondation de **Micro-Soft** (**micro**computer **software**)
 - avec P. Allen, un copain de lycée
- **1975** : développement d'un interpréteur **BASIC** pour l'ordinateur ALTAIR
 - Premier coup de maître : la licence **seule** est accordée à ALTAIR
 - Reversement de 35\$ pour chaque ordinateur vendu à Microsoft
 - donc BASIC se répand sur d'autres ordinateurs





Historique de MicroSoft Windows

- **1980** : IBM commande à Microsoft un SE pour son nouveau Personnal Computer
 - Achat pour 25 000 \$ du SE **QDOS**
 - Adaptation au cahier des charges d'IBM
→ naissance d'**IBM PC-DOS 1.0**
 - Vente de la licence à IBM...
 - ... et aux autres constructeurs : **MS-DOS** (Microsoft Disk Operating System) → **deuxième coup de maître**

IBM PC



MS DOS

```
C:\>copy command.com command.save
Écraser command.save (O/N/T) ?o
      1 fichier(s) copié(s)

C:\>cd mesdoc~1

C:\MESDOC~1>subst m: .

C:\MESDOC~1>vol

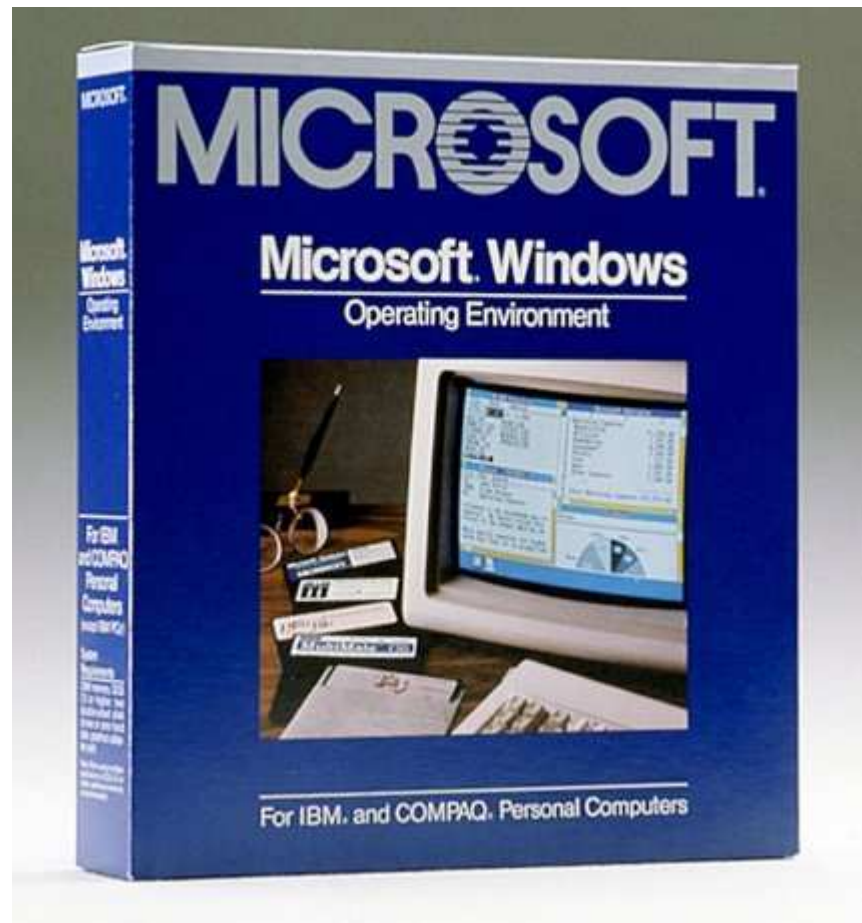
  Le volume dans le lecteur C n'a pas de nom
  Le numéro de série du volume est 257C-1810

C:\MESDOC~1>cd ..

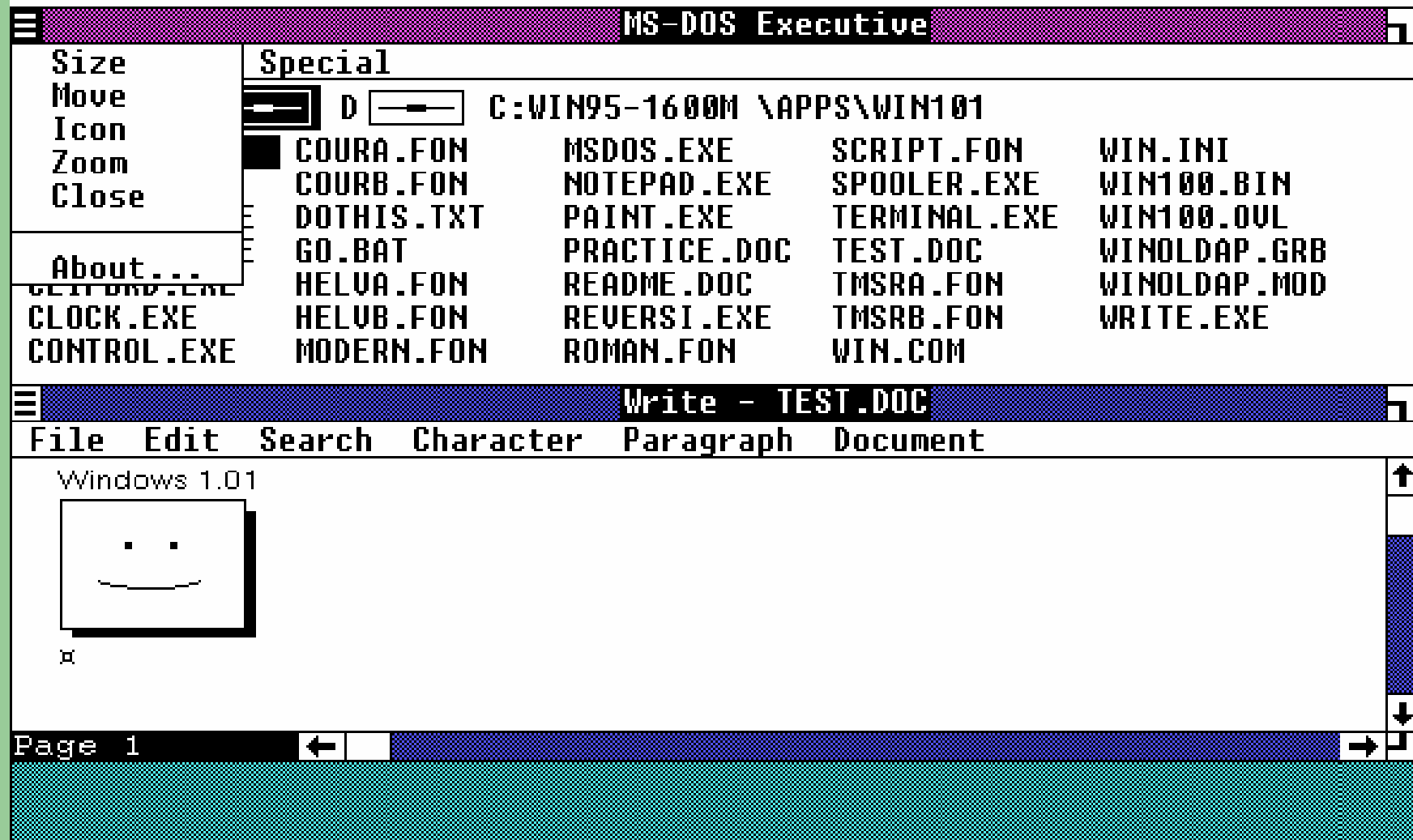
C:\>cls_
```

Historique de MicroSoft Windows

- 1985 : lancement de **Windows 1.0**, sans succès...



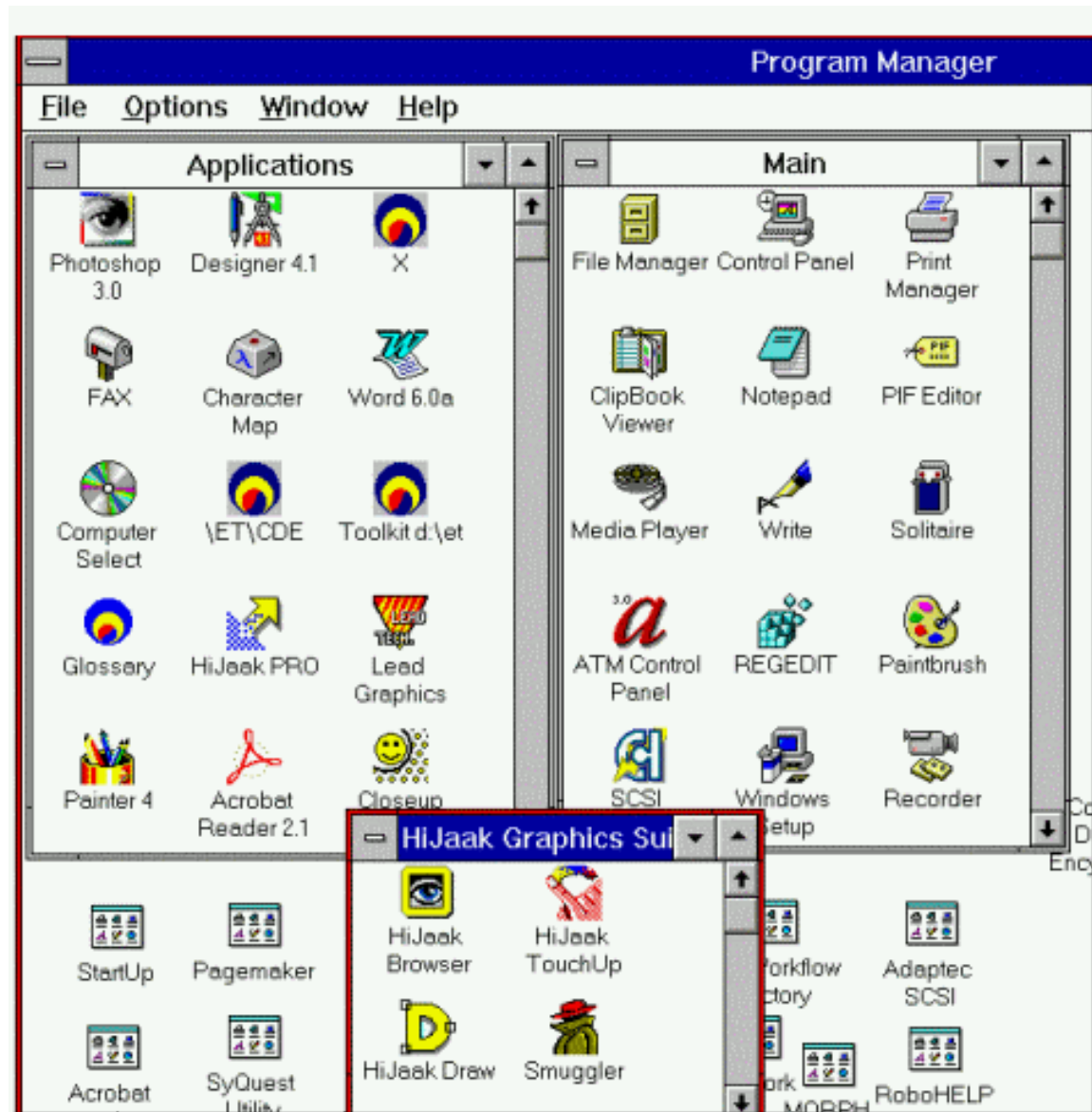
Microsoft Windows 1.0



Historique de MicroSoft Windows

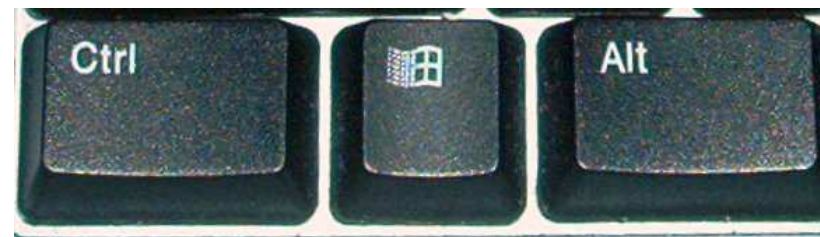
- **1992** : troisième coup de maître : **Windows 3.1**
 - Ergonomie enfin aboutie
 - Police TrueType

Microsoft Windows 3.1

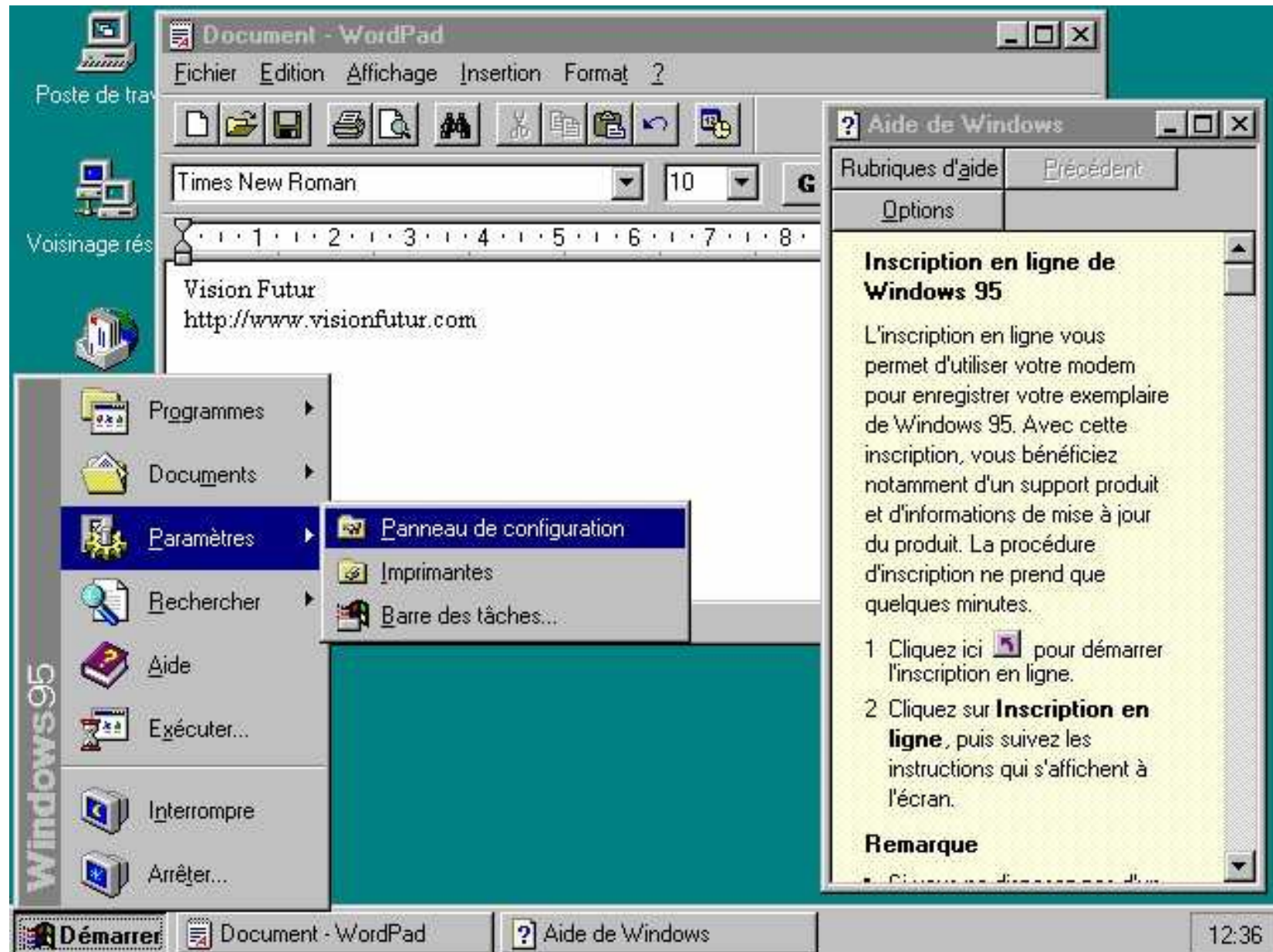


Historique de MicroSoft Windows

- **1995** : l'achèvement du succès : **Windows 95**
 - Facilité d'utilisation et ergonomie excellente
 - Introduction du multi-tâches
 - Apparition de la touche Windows
 - quasi monopole en grand public (90%)



Microsoft Windows 95



Microsoft Windows 95

Windows

Une erreur fatale 0E est apparue à 0028:C0031CE0. L'application va se terminer.

- Appuyez sur une touche pour terminer l'application.
 - Appuyez sur Ctrl+Alt+Suppr pour redémarrer votre ordinateur.
- Vous perdrez les informations non sauvegardées.

Appuyez sur n'importe quelle touche pour continuer _

Historique de Micro\$oft Windows

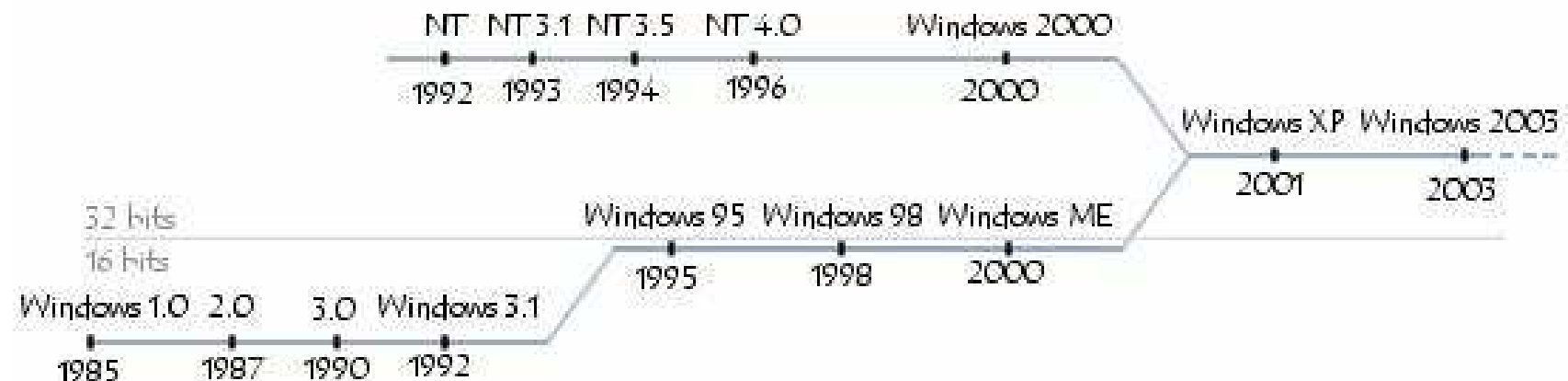
- **2010** : Bill Gates est le deuxième homme le plus riche du monde...

→ 53 000 000 000 \$



Microsoft®
Your potential. Our passion.®

Historique de MicroSoft Windows



Microsoft®

Objectifs de NT (New Technology)

1988 : étude d'un nouveau SE orienté serveur

- Portabilité car NT écrit en C/C++
 - Fonctionne aussi bien sur une machine x86 que sur une machine Alpha, p. ex.
- Mise en place de sécurité
 - Respect de la norme « C2 »
- Compatible avec la norme POSIX
 - POSIX : norme respectée par tous les SE modernes
- Multitraitement
 - Gestion multi processeurs possible

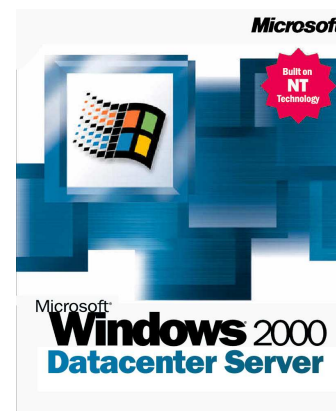


Windows 2000

Principalement : fiabiliser NT !

Puis :

- Nouvel annuaire **Active Directory**
- Nouveau système de fichier **NTFS 5**
- ...



Windows Server 2003

- Évolution de Windows 2000 Server
 - Incorporation de l'interface XP allégée
 - Ajout de nouvelles fonctionnalités
 - Amélioration de la gestion du réseau, de IIS (Internet Information Service) et de l'annuaire Active Directory
 - Réécriture partielle du code du noyau





My Documents



My Computer



My Network
Places



Internet
Explorer



Active
Directory Us...

Windows Server 2003 Enterprise Edition

- Windows Catalog
- Windows Update
- Programs
- Documents
- Settings
- Search
- Help and Support
- Run...
- Log Off Administrator...
- Shut Down...

- Accessories
- Administrative Tools
- Applications
- Startup
- Internet Explorer
- Outlook Express
- Remote Assistance

- Active Directory Domains and Trusts
- Active Directory Sites and Services
- Active Directory Users and Computers
- Certification Authority
- Cluster Administrator
- Component Services
- Computer Management
- Configure Your Server Wizard
- Data Sources (ODBC)
- DHCP
- Distributed File System
- DNS
- Domain Controller Security Policy
- Domain Security Policy
- Event Viewer
- Internet Information Services (IIS) Manager
- Licensing
- Local Security Policy
- Manage Your Server
- Microsoft .NET Framework 1.1 Configuration
- Microsoft .NET Framework 1.1 Wizards
- Microsoft SharePoint Administrator
- Network Load Balancing Manager
- Performance
- POP3 Service
- Remote Desktops
- Routing and Remote Access
- Services
- Terminal Server Licensing
- Terminal Services Configuration
- Terminal Services Manager
- Web Interface for Remote Administration



Recycle Bin



2:37 PM

Windows Server 2008

- **2008 : Windows Server 2008**
 - Gestion de IPv6 en natif
 - Ajout à chaud de composants comme les microprocesseurs
 - Installation en **Core Serveur**
 - Installation sans interface graphique, uniquement la ligne de commande
 - Windows **PowerShell**
 - Nouvelle interface en ligne de commande



Recycle Bin



Server Manager



Command Prompt



Windows Update



Internet Explorer



Notepad



Administrator

Documents

Computer

Network

Control Panel

Administrative Tools ▶

Help and Support

Run...



All Programs

Start Search



Initial Configuration Tasks

FR



22:20

Windows Server (R) 2008 Enterprise
Evaluation copy. Build 6001

Windows Server 2008 R2

- **2010 : Windows Server 2008 R2**
 - Version serveur de Windows 7
 - Adoption du noyau de Windows 7
 - Réduction de la consommation électrique
 - Système « Core parking »
 - Nouveau Windows **PowerShell**
 - Nouvelle interface en ligne de commande



Et ensuite ?

- **2012** : sortie de **Windows 8**

Plan

1- Historique

2- Qu'est-ce que Windows Server 2008 ?

3- Les versions de Windows Server 2008

4- Le système de sécurité

- La SAD
- Les DACL
- Les droits utilisateur
- Les audits

5- Notion de domaine

6- Relation d'approbation

Qu'est-ce que Windows Server 2008 ?

- Un système d'exploitation...
- ... multi tâches...
 - Plusieurs programmes peuvent fonctionner en même temps
- ... multi thread...
 - Cf. semestre 2 et ASR4
- ... multi traitement
 - Peut tourner sur un ordinateur comportant plusieurs processeurs

Plan

- 1- Historique
- 2- Qu'est-ce que Windows Server 2008 ?
- 3- Les versions de Windows Server 2008
- 4- Le système de sécurité
 - La SAD
 - Les DACL
 - Les droits utilisateur
 - Les audits
- 5- Notion de domaine
- 6- Relation d'approbation

3

Les versions de Windows Server 2008

- Pour les serveurs d'applications critiques qui nécessitent les plus hauts besoins de performances et de disponibilité

Datacenter ed.

- Pour les moyennes et grandes organisations

Enterprise ed.

- Pour les serveurs réseau polyvalents
- Pour les PME

Standard ed.

- Développement et déploiement rapides de services et d'applications Web
- Contient IIS

Web edition

Autres versions

- Pour les PME

Small Business

- Pour les TPE
- 15 utilisateurs maximum

Foundation ed.



Plan

- 1- Historique
- 2- Qu'est-ce que Windows Server 2008 ?
- 3- Les versions de Windows Server 2008
- 4- Le système de sécurité
 - La SAD
 - Les DACL
 - Les droits utilisateur
 - Les audits
- 5- Notion de domaine
- 6- Relation d'approbation

4

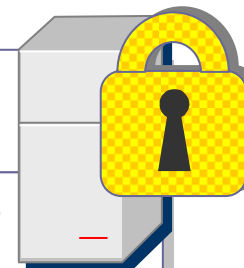
Le système de sécurité



- On peut contrôler :
 - qui accède à quoi
 - quel action un individu peut réaliser sur un objet
- On peut auditer des événements et les récupérer dans un journal d 'audit

Vue d'ensemble

Stratégies de compte	Configurent des stratégies pour les mots de passe et les comptes
Stratégies locales	Configurent l'audit, les droits d'utilisateur et les options de sécurité
Stratégies de clé publique	Configurent les agents de récupération de données cryptées, les racines de domaines, les autorités de certification approuvées, etc.
Stratégies IPSec	Configurent la sécurité IP sur un réseau
Journal des événements	Configure les paramètres des journaux des applications, des journaux système et des journaux de sécurité
Groupes restreints	Configurent l'adhésion aux groupes sensibles en termes de sécurité
Services système	Configurent les paramètres de sécurité et de démarrage des services exécutés sur un ordinateur
Registre	Configure la sécurité au niveau des clés du registre
Système de fichiers	Configure la sécurité au niveau des chemins d'accès de fichiers spécifiques



Plan

- 1- Historique
- 2- Qu'est-ce que Windows Server 2008 ?
- 3- Les versions de Windows Server 2008
- 4- Le système de sécurité
 - La SAD
 - Les DACL
 - Les droits utilisateur
 - Les audits
- 5- Notion de domaine
- 6- Relation d'approbation

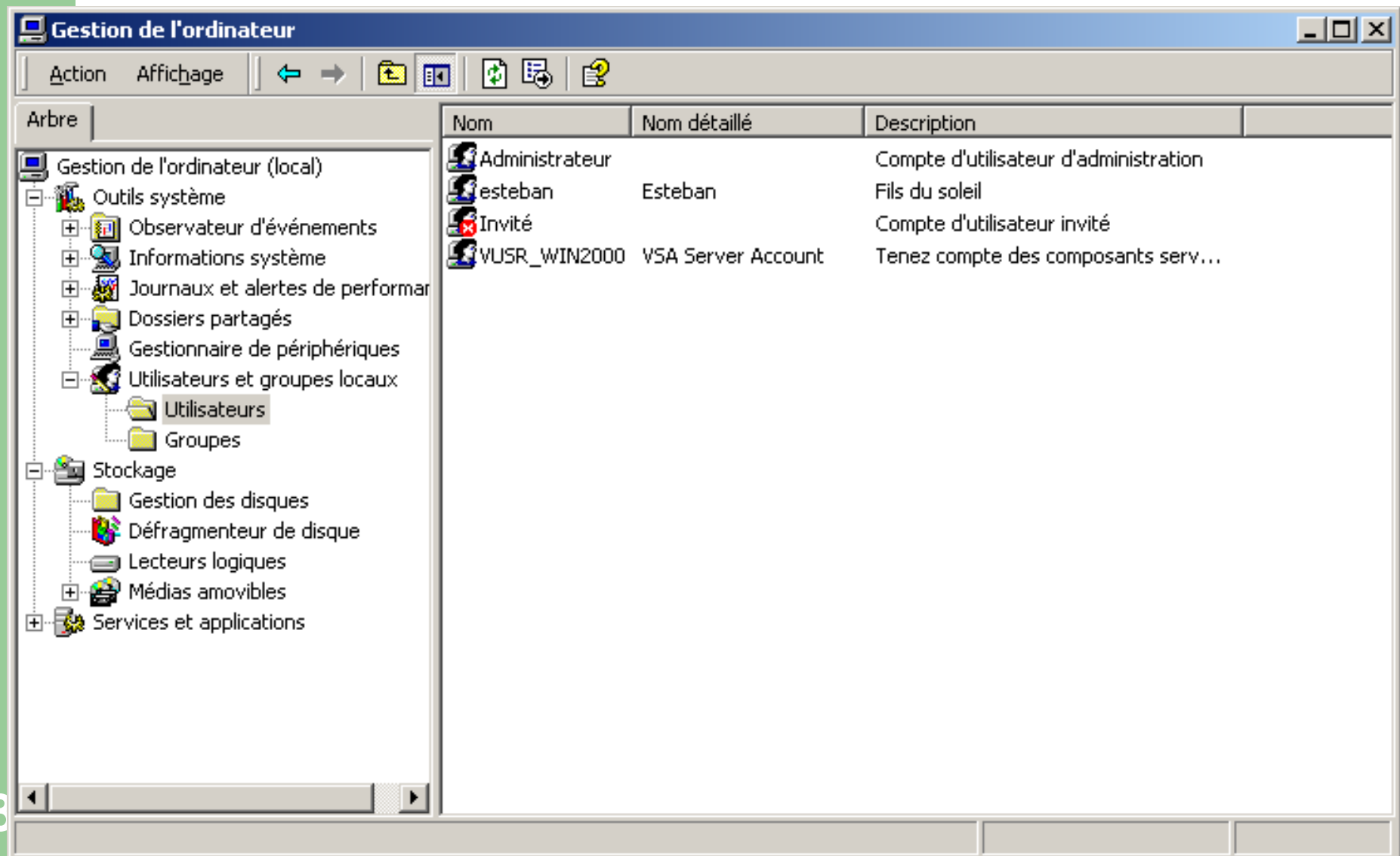
Architecture du système de sécurité

- Security Account Manager (**SAM**)
 - En charge de la **SAD** (Security Account Database)
 - SAD = base de données des utilisateurs autorisés à se connecter sur la machine
 - Chaque utilisateur étant identifié par un **SID**
 - SID=Security Identifiant, identifiant d'utilisateur



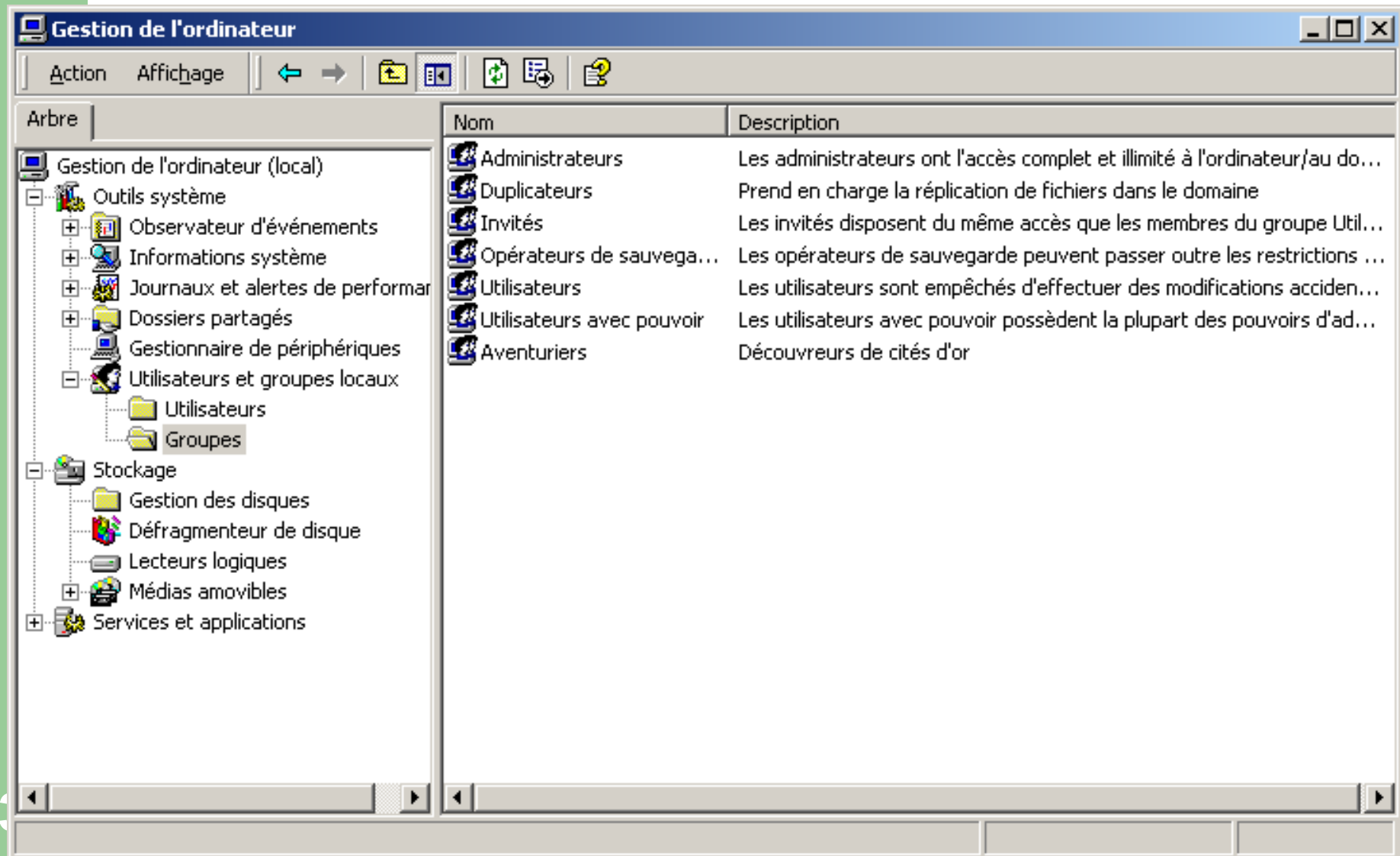
Security Account Database (SAD)

Gérée via l'application « gestion de l'ordinateur »



Security Account Database (SAD)

Gestion des groupes d'utilisateurs



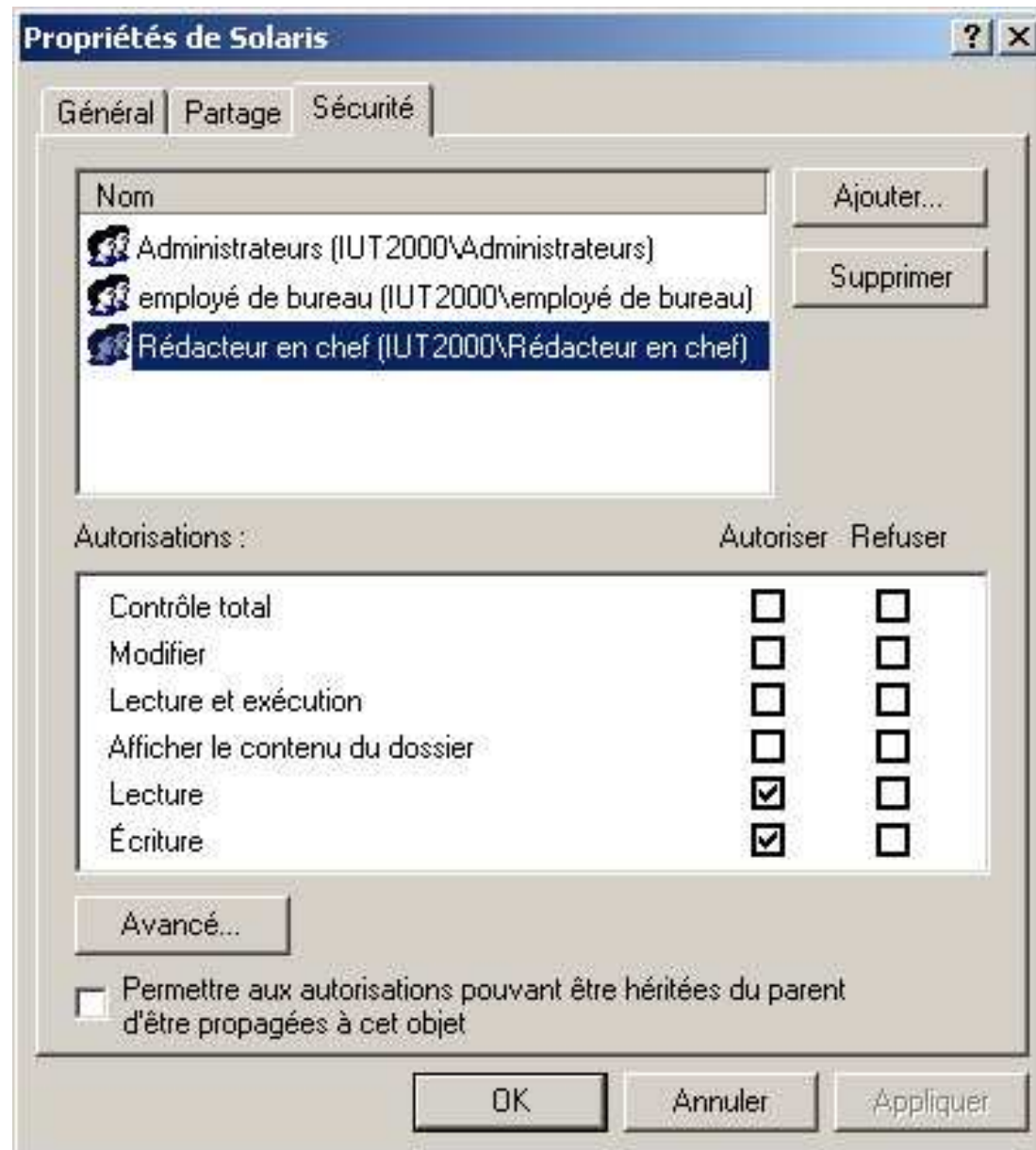
Plan

- 1- Historique
- 2- Qu'est-ce que Windows Server 2008 ?
- 3- Les versions de Windows Server 2008
- 4- Le système de sécurité
 - La SAD
 - Les DACL
 - Les droits utilisateur
 - Les audits
- 5- Notion de domaine
- 6- Relation d'approbation

Architecture du système de sécurité (suite)

- Security Reference Monitor (**SRM**)
 - Vérifie qu'un utilisateur ou un programme peut accéder à un objet donné via sa **DACL** (Discretionary Access Control List)
 - DACL=liste à contrôle d'accès associée à tout objet des trois types suivants :
 - Fichiers
 - Répertoires
 - Imprimantes

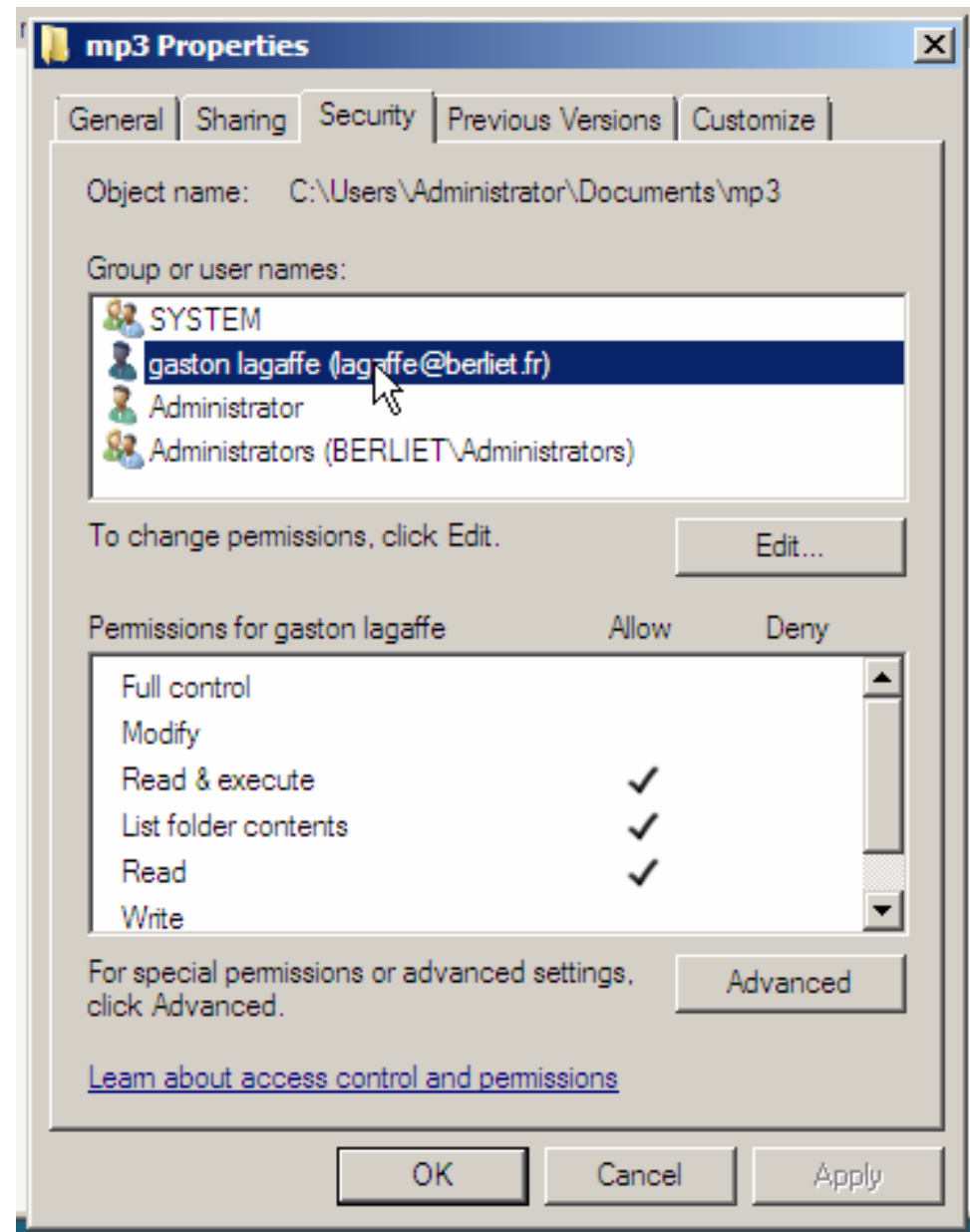
Exemple de DACL pour un dossier



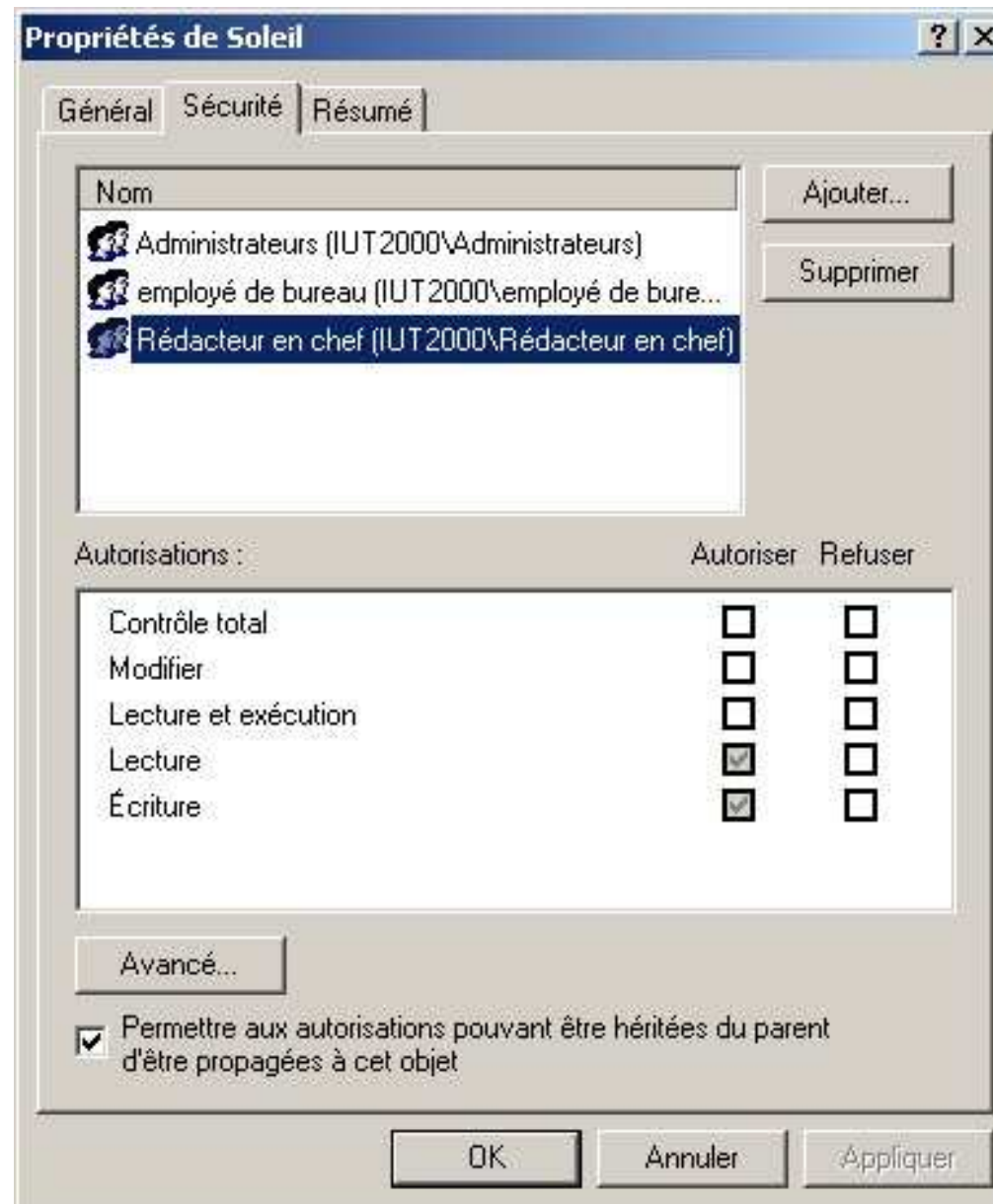
Exemple de DACL pour un dossier



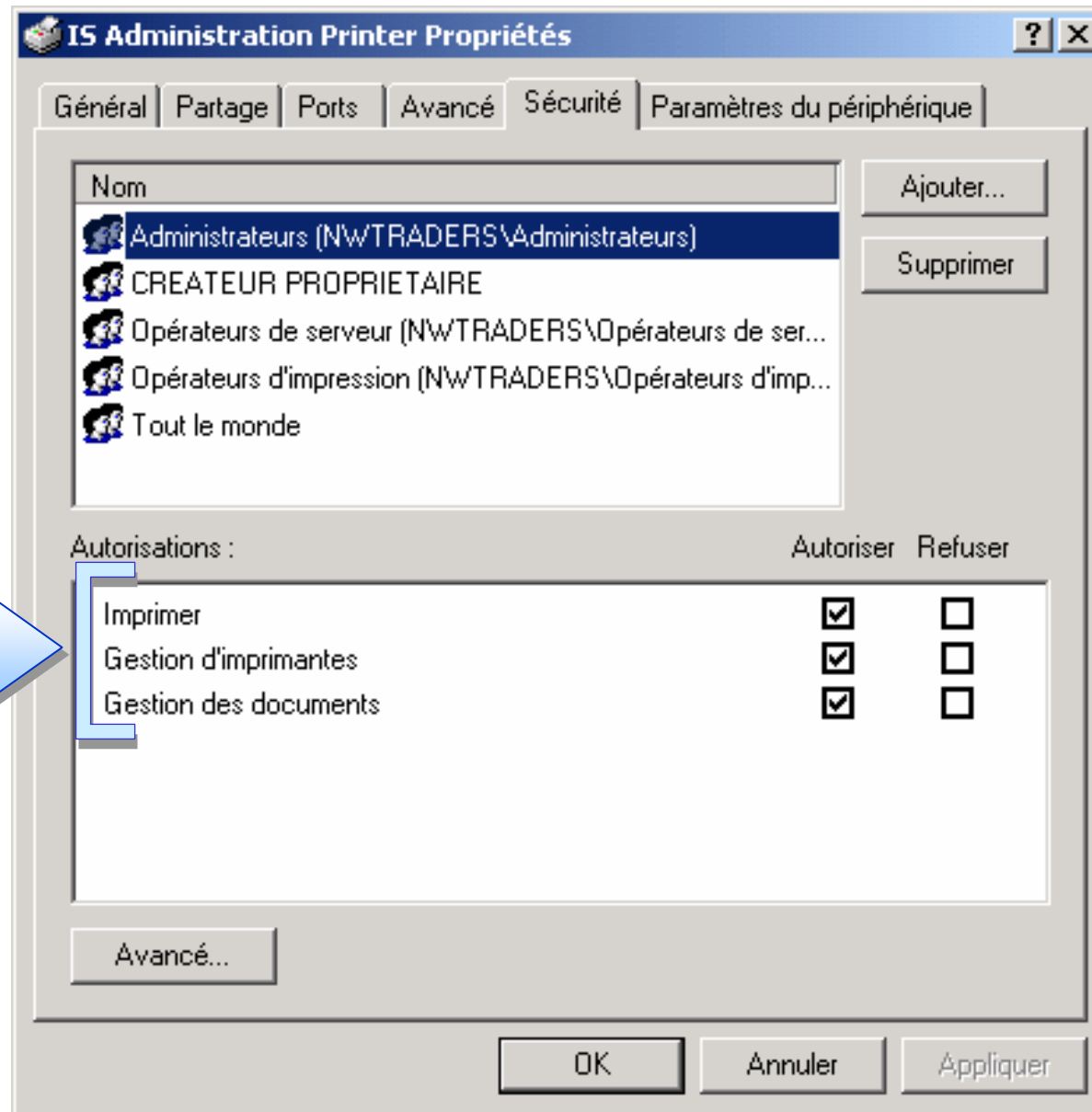
Windows Server® 2008



Exemple de DACL pour un fichier



Exemple de DACL pour une imprimante



Autorisations
d'impression

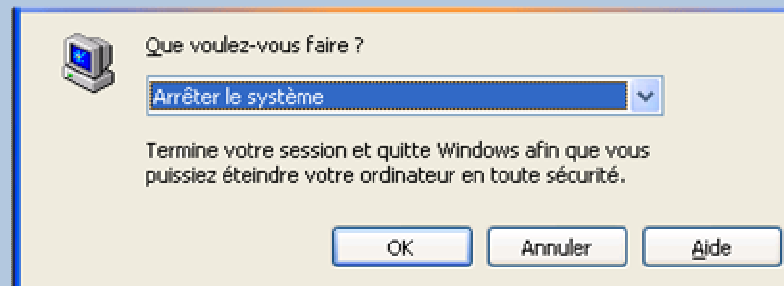
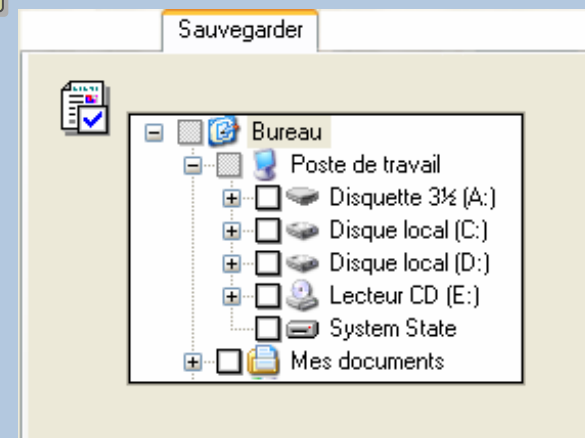
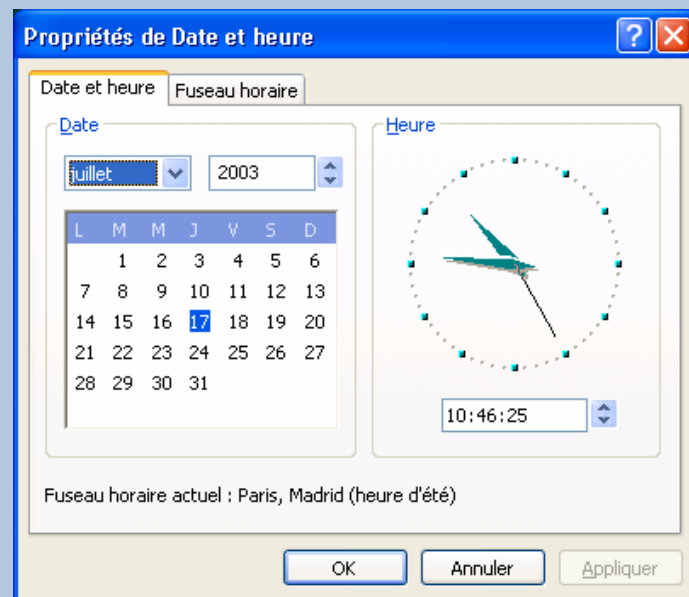
Plan

- 1- Historique
- 2- Qu'est-ce que Windows Server 2008 ?
- 3- Les versions de Windows Server 2008
- 4- Le système de sécurité
 - La SAD
 - Les DACL
 - Les droits utilisateur
 - Les audits
- 5- Notion de domaine
- 6- Relation d'approbation

Privilèges utilisateur

- Droits qui ne sont pas associés à un objet particulier
 - Sauvegarde du système
 - Arrêt de la machine
 - Changement de l'heure
 - Création de nouveaux utilisateurs
 - ...

Exemples de droits utilisateur



Privilèges utilisateur

- Certains groupes d'utilisateurs prédéfinis possèdent des droits particuliers

Administrateurs	Dispose de tous les droits
Utilisateurs	Dispose de droits limités
Utilisateurs avec pouvoir	Peut réaliser les tâches administratives de base mais n'a pas le contrôle total du système.
Opérateurs de sauvegarde	Possède des droits uniquement sur les fichiers et sur les tâches administratives de sauvegarde et de restauration.

Gestion des privilèges utilisateur

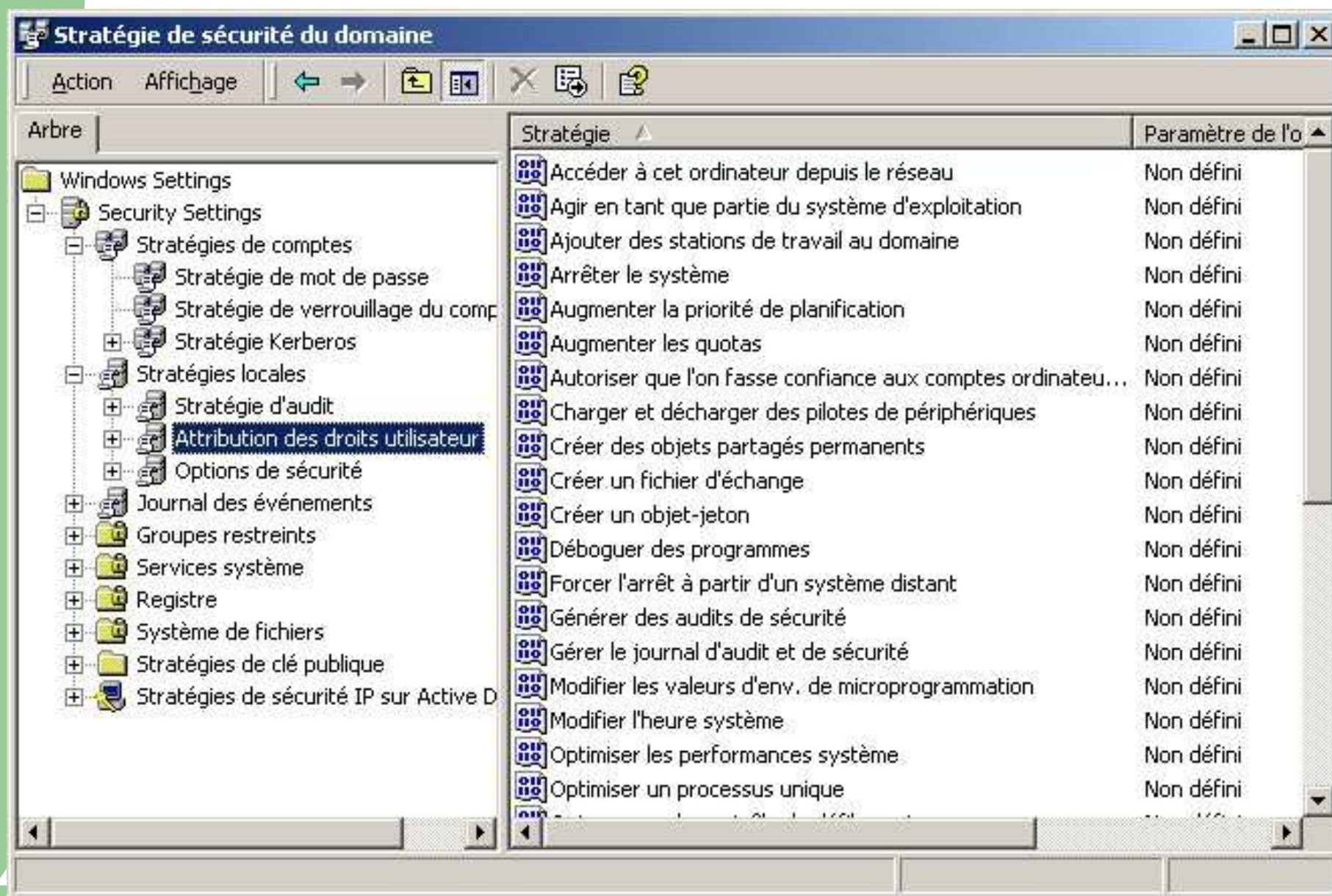


Gestion des privilèges utilisateur

- L'administrateur attribue à l'utilisateur Lagaffe le privilège de changer l'heure



Gestion des privilèges utilisateur



Plan

- 1- Historique
- 2- Qu'est-ce que Windows Server 2008 ?
- 3- Les versions de Windows Server 2008
- 4- Le système de sécurité
 - La SAD
 - Les DACL
 - Les droits utilisateur
 - Les audits
- 5- Notion de domaine
- 6- Relation d'approbation

Audits

- Suivre **les activités** des utilisateurs et du système d'exploitation
- Consigner les événements sélectionnés dans des **journaux de sécurité**

Que s'est-il passé ?

Qui l'a fait ?

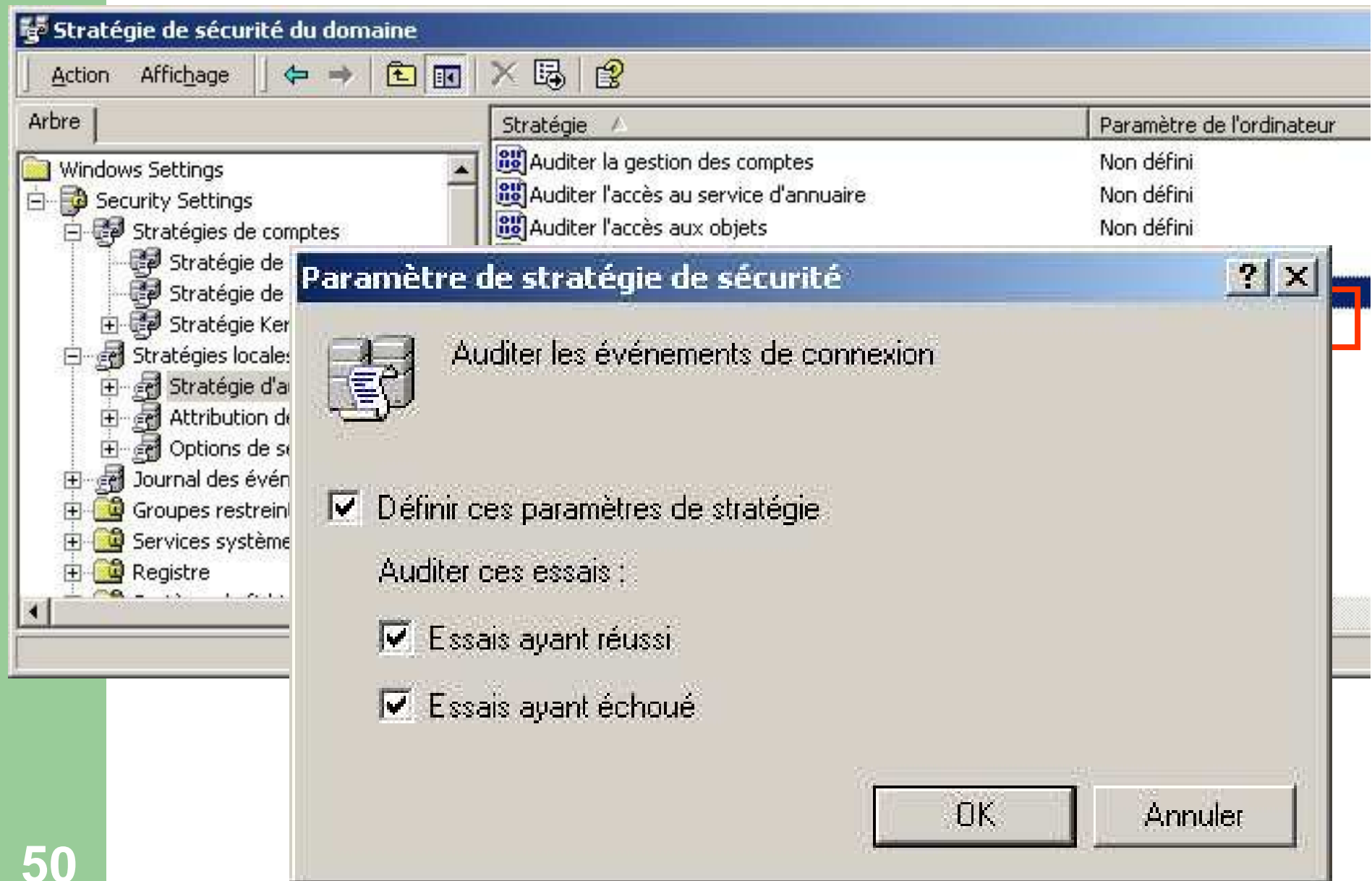
Quand ?

Quel est le résultat ?

- **On active l'audit pour :**
 - détecter l'accès non autorisé aux ressources
 - conserver un historique de l'activité
 - détecter les attaques et les menaces
 - déterminer les dégâts
 - éviter des dégâts supplémentaires

Audits

- Sous Windows 2000



Propriétés de Événement

Événement

Date : 12/09/2002 Source : Security
Heure : 16:23 Catégorie : Ouverture/Fermeture de
Type : Audit des ID événement : 540
Utilisateur : IUT2000\lagaffe
Ordinateur : SERVEUR2000

Description :

Ouverture de session réseau réussie :
Nom de l'utilisateur : lagaffe
Domaine : IUT2000
N° de la session : (0x0,0x69E97)
Type de session : 3
Processus de session : Kerberos
Package d'authentification : Kerberos

Données : ☒ Octets ☐ Mots

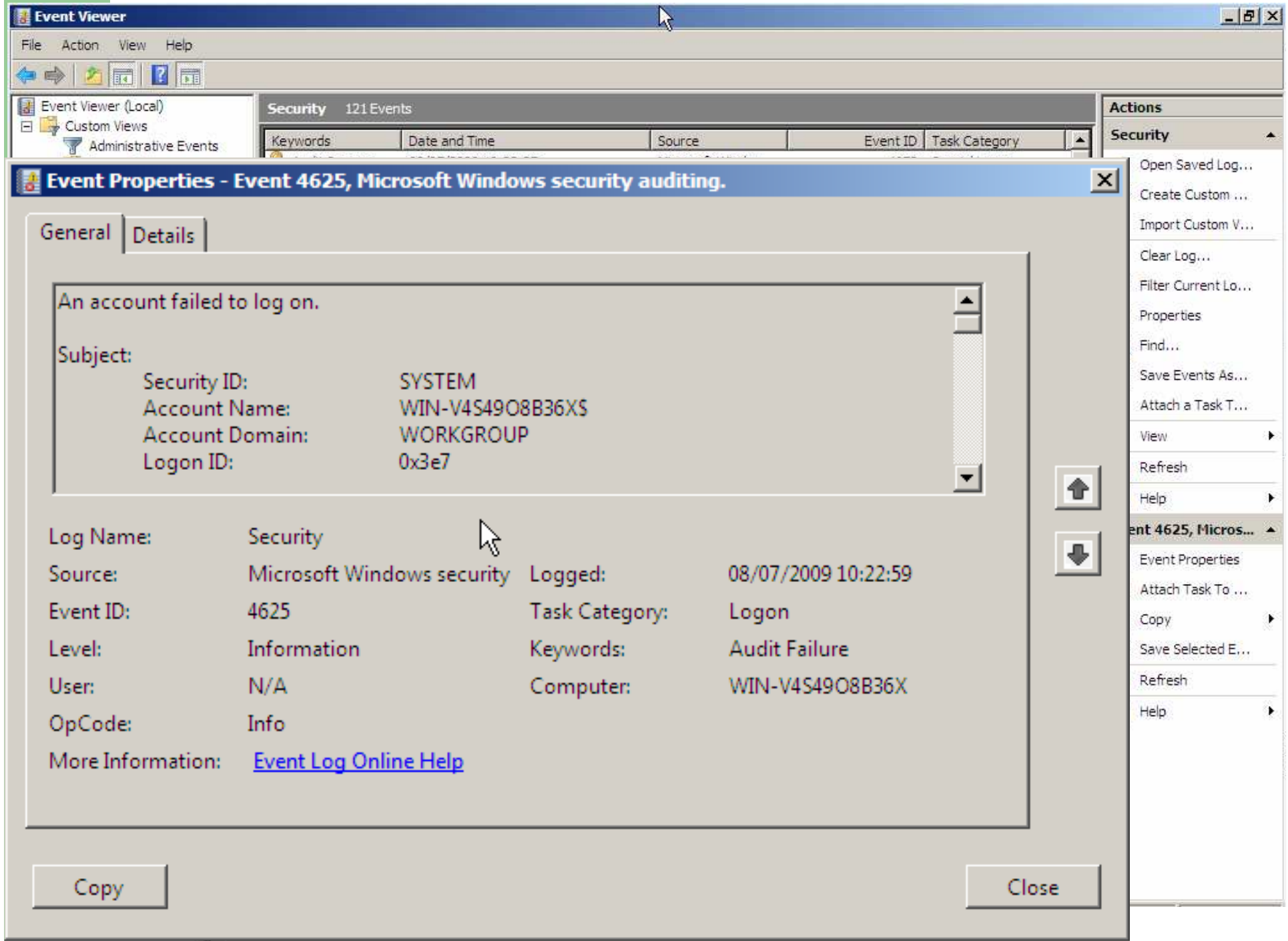
OK

Annuler

Appliquer

serveur

Catégorie	Évén...	Utilisateur
Ouvertur...	538	administrateur
Ouvertur...	538	administrateur
Ouvertur...	540	administrateur
Ouvertur...	540	administrateur
Ouvertur...	540	administrateur
Ouvertur...	538	administrateur
Ouvertur...	540	administrateur
Ouvertur...	528	administrateur
Ouvertur...	538	lagaffe
Ouvertur...	538	lagaffe
Ouvertur...	538	lagaffe
Ouvertur...	538	lagaffe
Ouvertur...	540	lagaffe
Ouvertur...	540	lagaffe
Ouvertur...	540	lagaffe
Ouvertur...	538	lagaffe
Ouvertur...	540	lagaffe
Ouvertur...	538	lagaffe



Plan

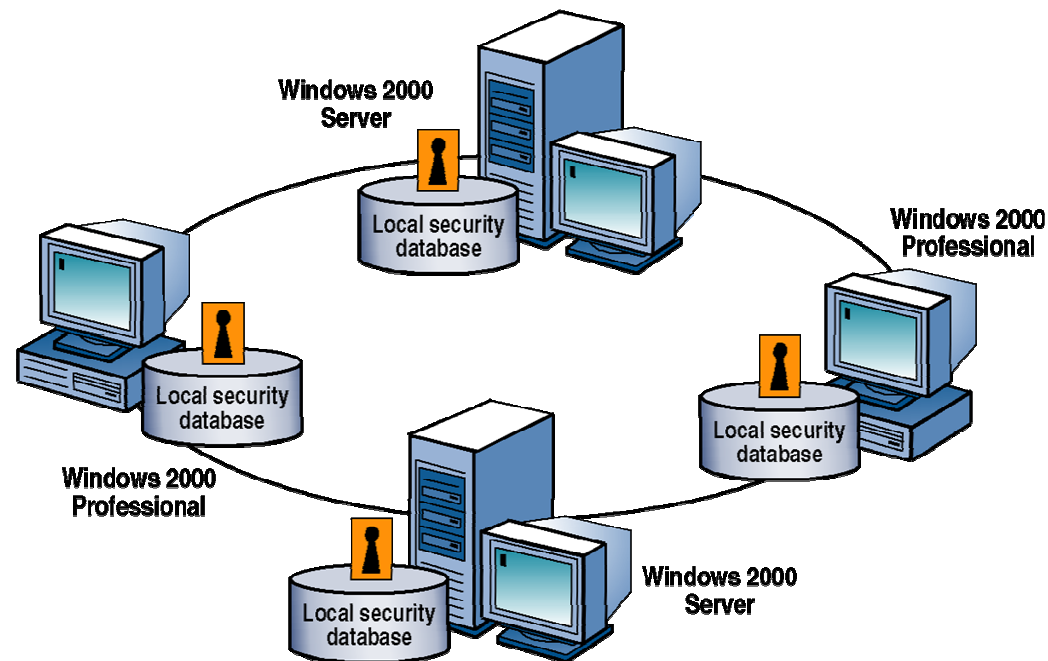
- 1- Historique
- 2- Qu'est-ce que Windows Server 2008 ?
- 3- Les versions de Windows Server 2008
- 4- Le système de sécurité
 - La SAD
 - Les DACL
 - Les droits utilisateur
 - Les audits
- 5- Notion de domaine
- 6- Relation d'approbation

Modèles d'environnement réseau

- Deux modèles pour la gestion du réseau informatique existent sous Server 2008 :
 - Le **groupe de travail** (workgroup)
 - Le **domaine**

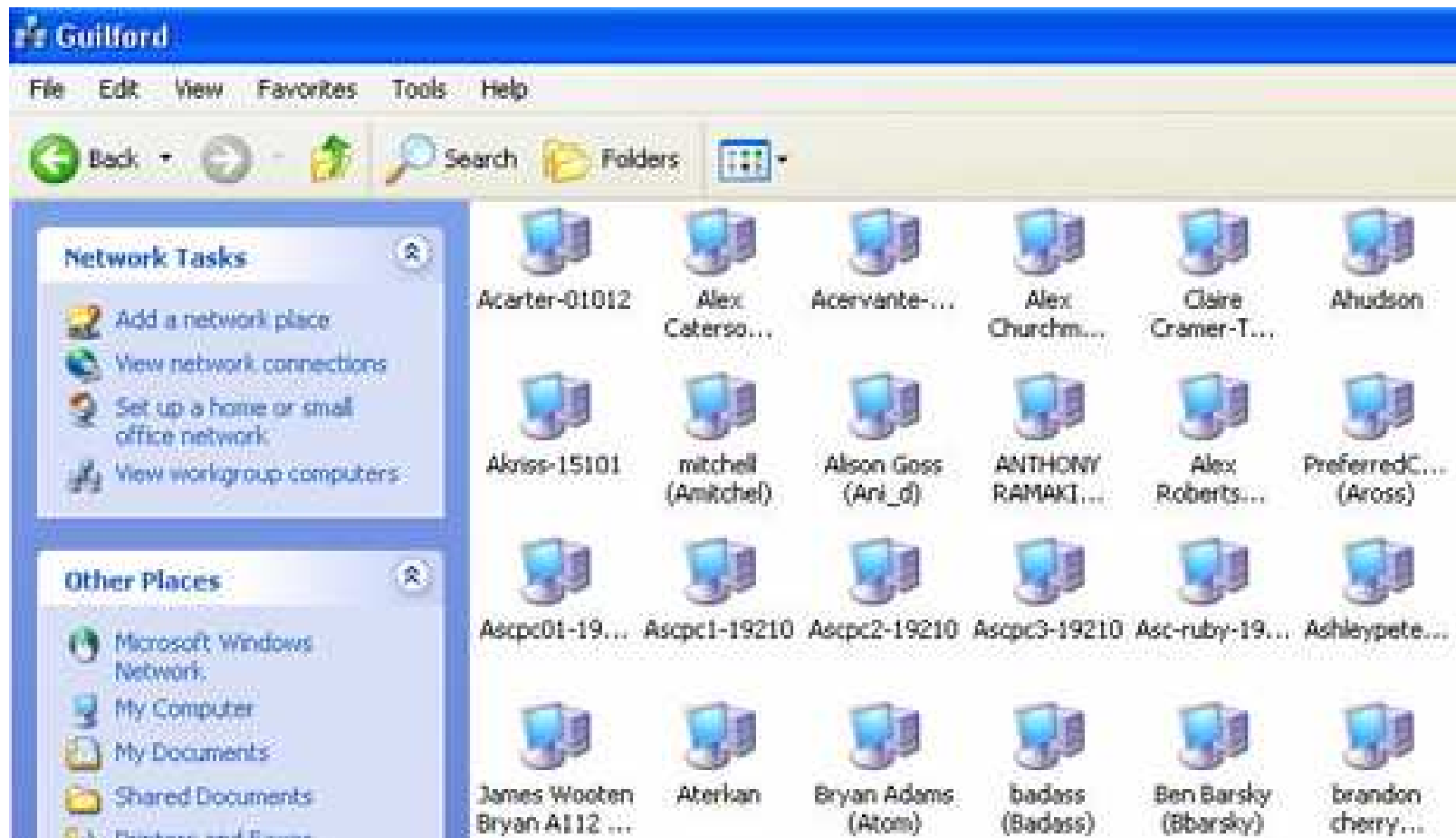
Le groupe de travail

- **Déf** : Machines reliées entre elles par un réseau
- **Aucune centralisation** des ressources ou de la sécurité
 - Chaque machine possède :
 - Sa propre SAD
 - Ses propres configurations de sécurité et des utilisateurs



Le groupe de travail

- **Avantage** : dans le **voisinage réseau** n'apparaissent **que** les ressources du groupe de travail, pas le réseau entier de l'entreprise → **navigation facilitée** pour l'utilisateur final



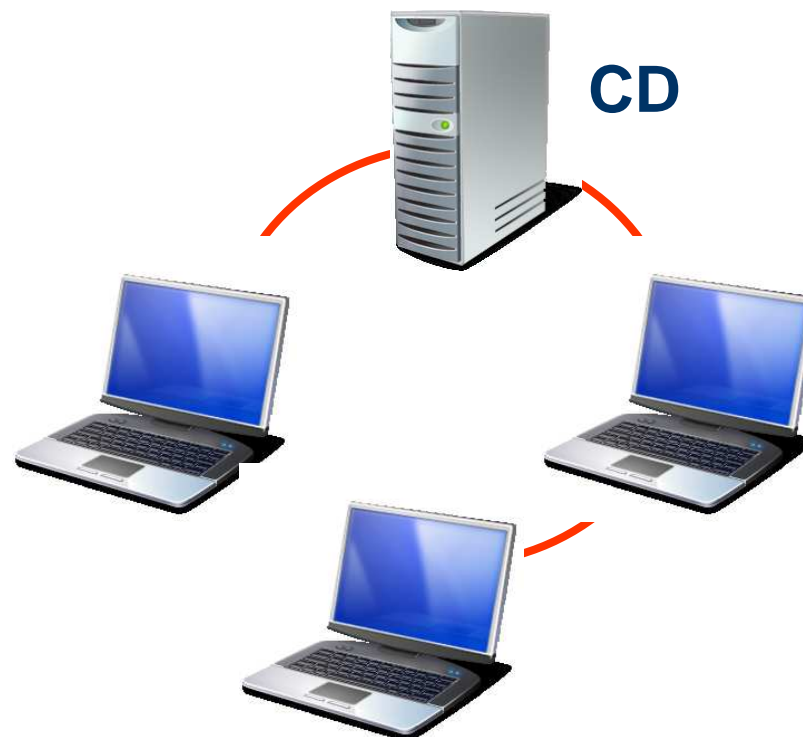
Le domaine

- Groupe de machines partageant **les même comptes utilisateur** et la **même politique de sécurité**
 - Ex : domaine du département Informatique
- Avantages:
 - Gestion centralisée des comptes utilisateur et de la sécurité
 - Réseau divisé en domaine
 - Respect de l'organisation physique et logique de l'entreprise



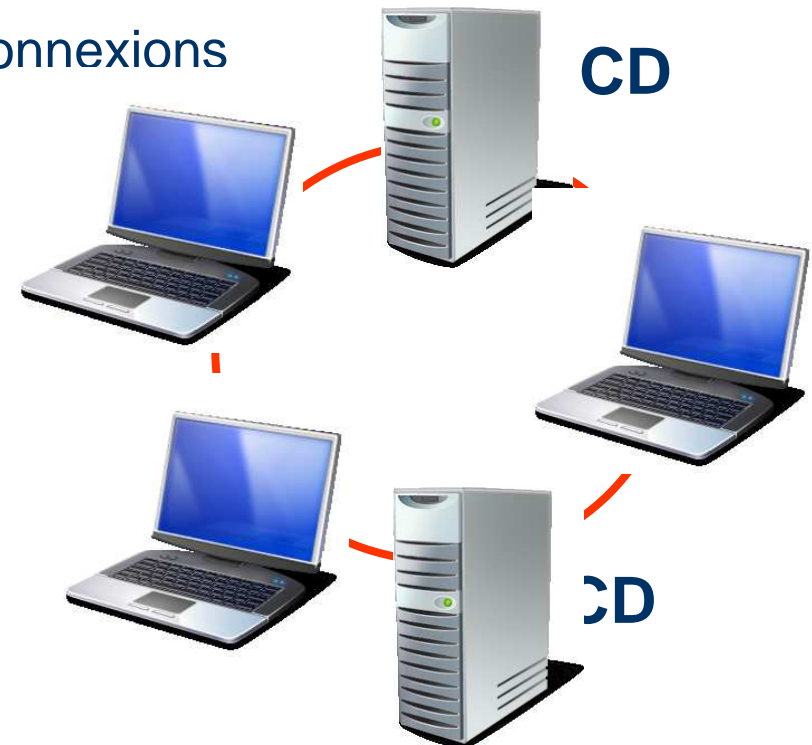
Composition d'un domaine

- Au moins un **contrôleur de domaine (CD)**
 - Contient un exemplaire **d'Active Directory**
 - Active Directory contient entre autre la liste des utilisateurs autorisés à se connecter sur n'importe quelle machine du domaine
 - Valide les demandes de connexion des utilisateurs



Composition d'un domaine (suite)

- **Plusieurs** contrôleurs de domaine conseillés
 - pour pallier une panne d'un autre CD
 - pour des raisons de rapidité
- Chaque CD contient un exemplaire d'Active Directory
 - donc tous peuvent valider les connexions



Aperçu d'Active Directory

Utilisateurs et ordinateurs Active Directory

Console Fenêtre ?

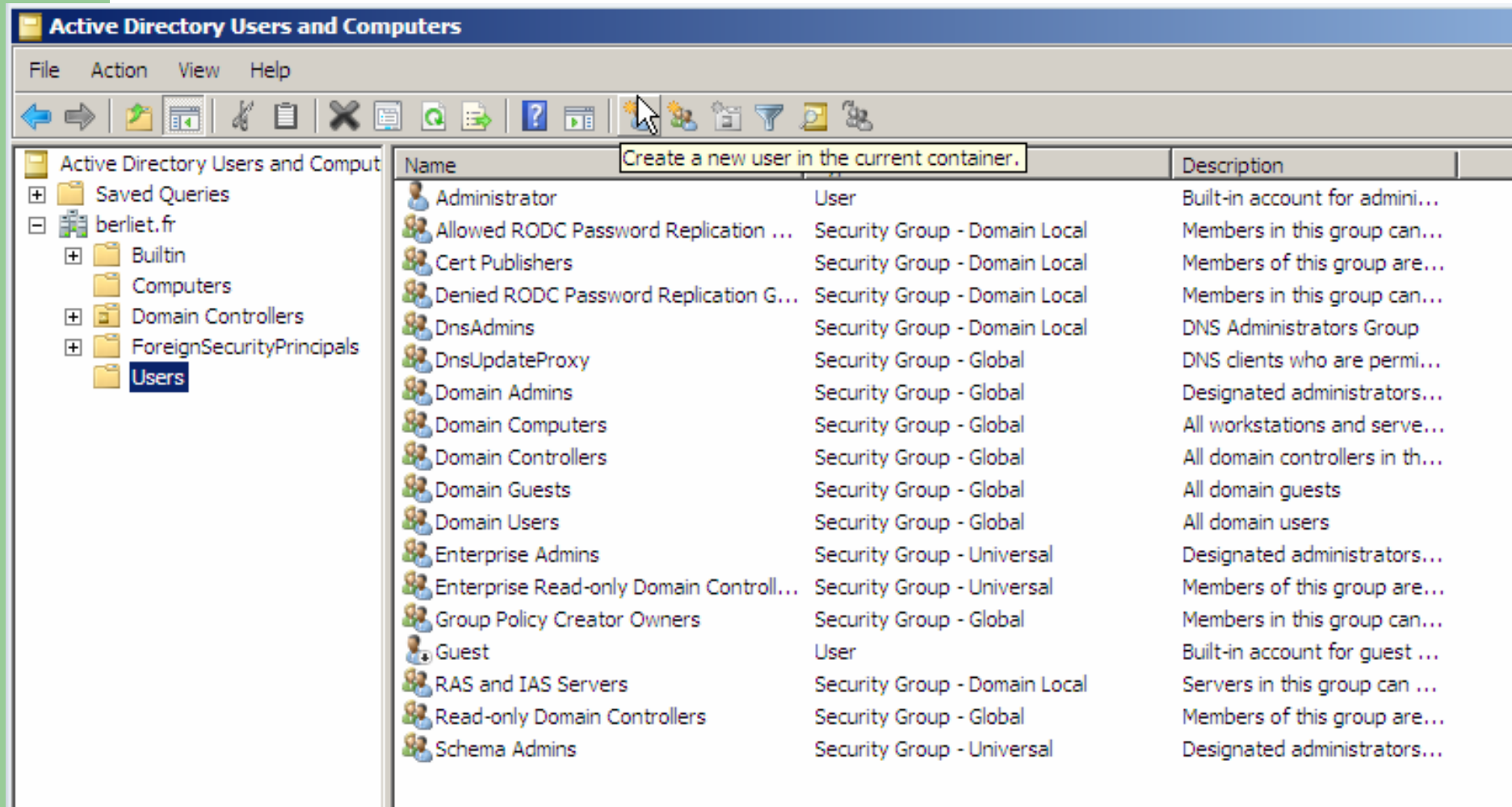
Action Affichage

Arbre

Users 22 objets

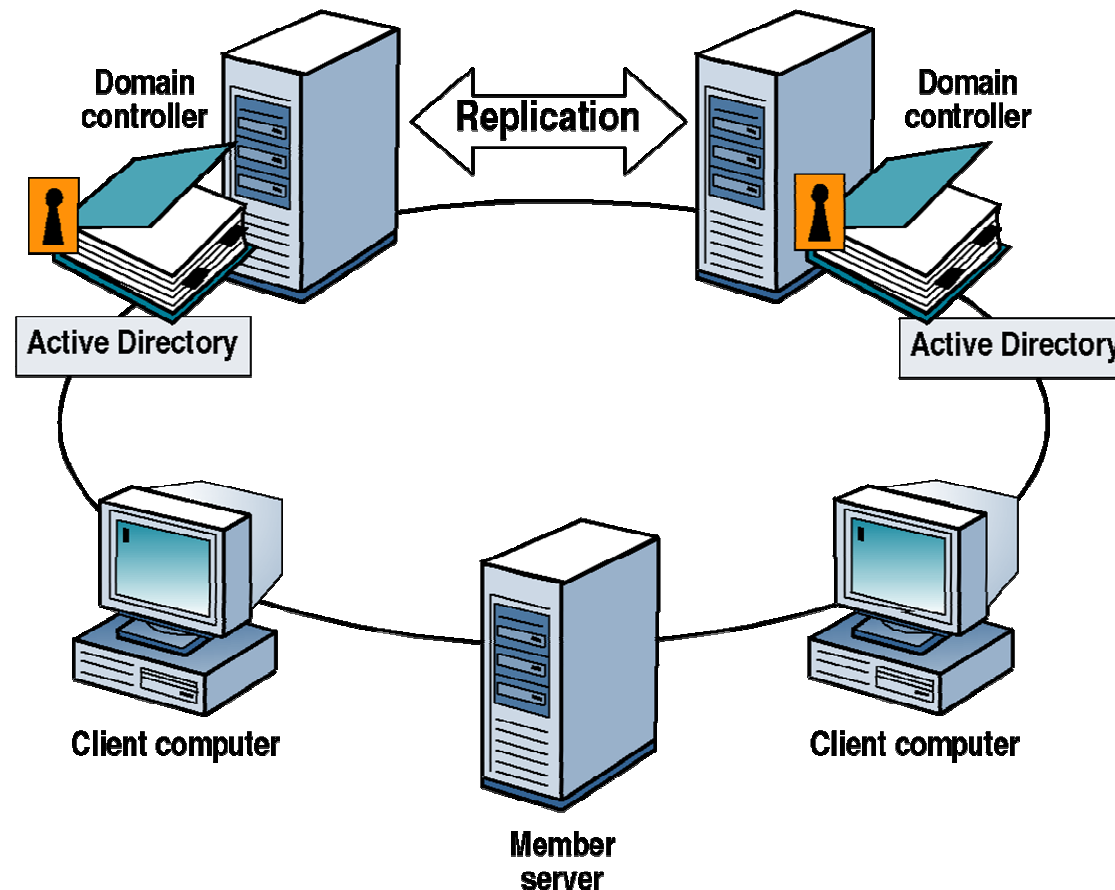
Nom	Type	Description
Administrateur	Utilisateur	Compte d'utilisateur d'administration
Administrateurs de l'entre...	Groupe de sécurité -...	Administrateurs désignés de l'entreprise
Administrateurs DHCP	Groupe de sécurité -...	Les membres qui ont un accès autorisant l'administration du
Administrateurs du schéma	Groupe de sécurité -...	Administrateurs désignés du schéma
Admins du domaine	Groupe de sécurité -...	Administrateurs désignés du domaine
Contrôleurs de domaine	Groupe de sécurité -...	Tous les contrôleurs de domaine du domaine
DnsAdmins	Groupe de sécurité -...	Groupe des administrateurs DNS
DnsUpdateProxy	Groupe de sécurité -...	Les clients DNS qui sont autorisés à effectuer des mises à j
Éditeurs de certificats	Groupe de sécurité -...	Agents de certification d'entreprise et de renouvellement
employé de bureau	Groupe de sécurité -...	Employés de bureau à la rédaction Dupuis
Gaston Lagaffe	Utilisateur	
Invité	Utilisateur	Compte d'utilisateur invité
Invités du domaine	Groupe de sécurité -...	Tous les invités du domaine
krbtgt	Utilisateur	Compte de service du centre de distribution de clés
Ordinateurs du domaine	Groupe de sécurité -...	Toutes les stations de travail et les serveurs joints au doma
Propriétaires créateurs de ...	Groupe de sécurité -...	Les membres de ce groupe peuvent modifier la stratégie de
Serveurs RAS et IAS	Groupe de sécurité -...	Les serveurs de ce groupe peuvent accéder aux propriétés
TsInternetUser	Utilisateur	Ce compte utilisateur est utilisé par les services Terminal Se
Utilisa. du domaine	Groupe de sécurité -...	Tous les utilisateurs du domaine
Utilisateurs DHCP	Groupe de sécurité -...	Les membres qui ont un accès autorisant uniquement la cor
Rédacteur en chef	Groupe de sécurité -...	
Léon Prunelle	Utilisateur	

Aperçu d'Active Directory Windows Server® 2008



Composition d'un domaine (suite)

- Des machines Windows Server 2008/2003/2000/NT...
 - Appelées « **serveurs membres** »
- ... voire des machines Windows XP/98/95
 - Appelées « **ordinateur client** »



Composition d'un domaine (suite)

- Deux types de connexion sont donc possibles :
 - Connexion locale
 - Si l'utilisateur est déclaré dans la **SAD** de la machine
 - Connexion sur le domaine
 - Si l'utilisateur est déclaré dans l'**Active Directory** du domaine



En résumé

- **Active Directory :**

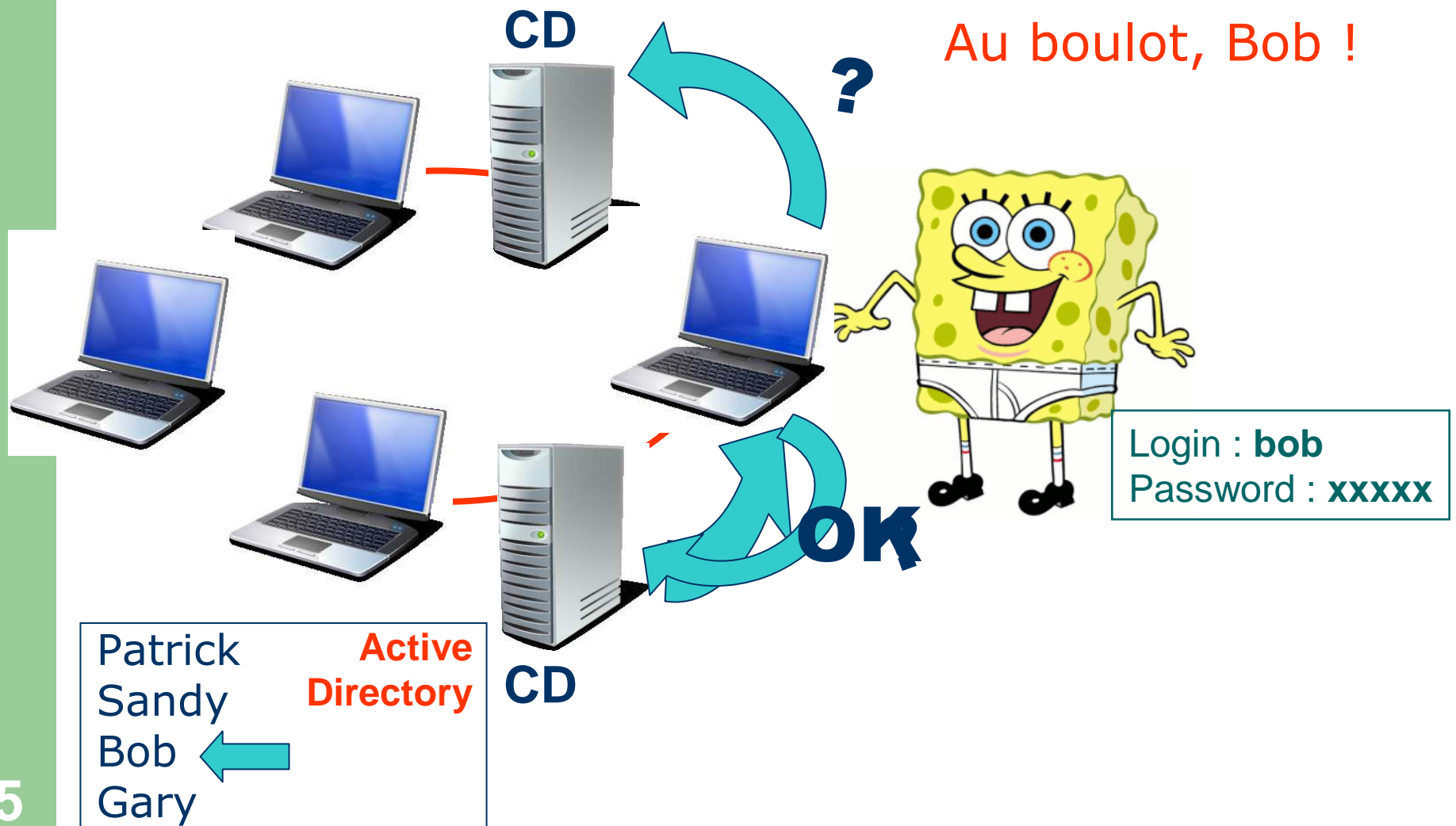
- Présent uniquement sur un contrôleur de domaine
- Permet une connexion sur toutes les machines du domaine

- **SAD :**

- Présent sur toute machine Windows Server non CD
- Permet uniquement une connexion locale

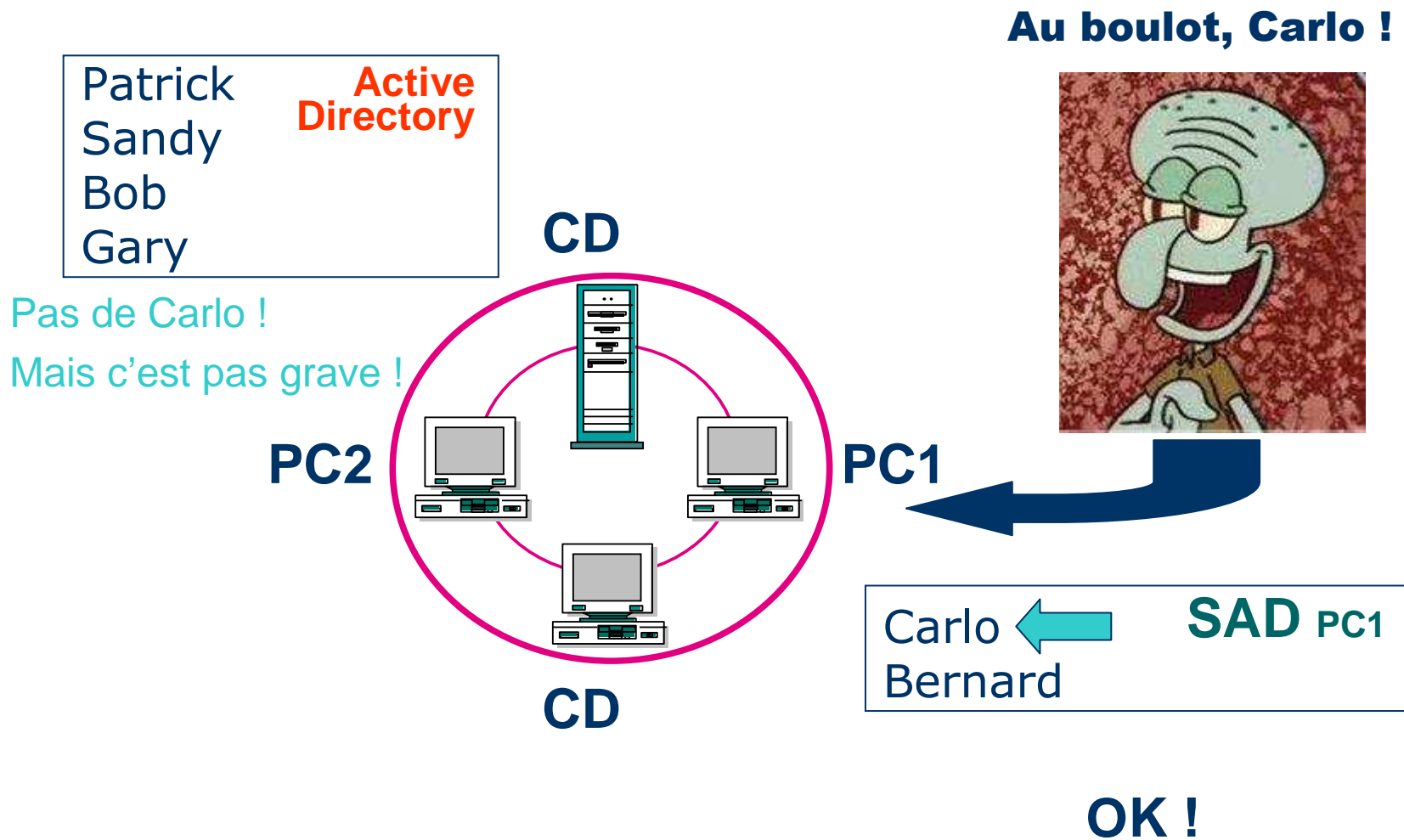
Exemple 1

- **Bob** veut se connecter sur le domaine



Exemple 2

- **Carlo** veut ouvrir une session locale sur la machine **PC1**



Plan

- 1- Historique
- 2- Qu'est-ce que Windows Server 2008 ?
- 3- Les versions de Windows Server 2008
- 4- Le système de sécurité
 - La SAD
 - Les DACL
 - Les droits utilisateur
 - Les audits
- 5- Notion de domaine
- 6- Relation d'approbation

6

Relation d'approbation

- Le capitaine **Krabs** veut se connecter sur une machine du **domaine 1**

Bob
Patrick
Sandy **AD1**

Problème.
Solution ? relation
d 'approbation !

Krabs
Lary
Jacasseur **AD2**

Domaine 1

Domaine 2

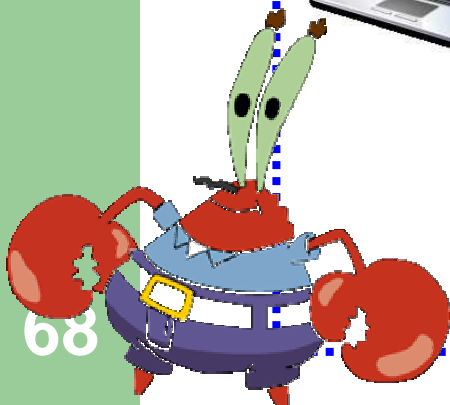
CD

Rel. App.

CD

CD

CD



Relation d'approbation

- Si le domaine **A** approuve le domaine **B**, alors :
 - ⇒ Les utilisateurs déclarés sur le domaine **A** peuvent se connecter sur le domaine **B**
 - et **réci-proquement** si la relation d'approbation est **bi-directionnelle**
- Si les domaines **A** et **B** s'approuvent et si **B** et **C** s'approuvent, alors:
 - ⇒ les domaines **A** et **C** s'approuvent
 - La relation d'approbation est **transitive**
- Utilité des relations d'approbation : permet la gestion de **forêts** et **d'arbres**
 - Voir exercice